Universidad Austral de Chile

Facultad de Ciencias de la Ingeniería

Escuela de Electricidad y Electrónica

Procedimiento de configuración de QoS para red MPLS-VPN en los accesos, XDSL, Frame-Relay, Acceso MPLS Nativo, Acceso ATM STM1 y Acceso 10/100 MS.

Tesis para optar al título de
Ingeniero Electrónico

Profesor Patrocinante:
Sr. José Mardones F.
Ingeniero Electrónico

Luis Alberto Riquelme Ocares

Valdivia, Noviembre 2006

Profesor Patrocinante:

JOSÉ MARDONES FERNÁNDEZ ----------

Profesores informantes:

ALEJANDRO VILLEGAS ----------

PEDRO REY CLERICUS ----------

Dedicatoria y Agradecimientos

Dedicada: ***A Mi Familia.***

"No hay palabras que puedan describir mi profundo agradecimiento hacia mi familia, quienes durante todos estos años confiaron en mí, comprendiendo mis ideales y el tiempo que no he estado con ellos".

Quiero agradecer a mi padre José Laureano Riquelme Ocares, quién siempre me entregó el apoyo, cariño y comprensión, permitiéndome, gracias a su esfuerzo salir y enfrentar cada inconveniente que se me presentó en el camino.

En segundo lugar quisiera agradecerle a mi hijo Matías, quien con su amor e inocencia infla mi pecho y lo llena de orgullo motivandome a ser cada día mejor.

Agradezco también a todos mis profesores por parte de la Escuela de Electricidad y Electrónica y del Instituto de Electrónica de la Universidad Austral de Chile, que siempre, con respeto y cordialidad confiaron en mí y en mis capacidades como alumno, en especial agradezco a mis profesores patrocinante e informantes.

Luis

Resumen

Hoy en día existe una gran variedad de servicios que ofrecen aplicaciones de telefonía, datos, videoconferencia etc. en un mismo paquete, por lo mismo, las empresas que se han dedicado a proveer estos servicios a sus clientes se han preocupado de que cada una de las aplicaciones ofrecidas cumpla con los estándares de calidad. Es por esto que se implementa a niveles de acceso la quality of Service (Qos), siendo está una alternativa eficiente para optimizar una red que comparte el ancho de banda.

En el presente trabajo de Titulación se entrega una descripción detallada del procedimiento de configuración de Quality of Service para red MPLS en diferentes accesos como red intermedia entre el usuario final y la red Mpls, considerando las configuraciones a realizar en los distintos router CE ubicados en los extremos de la red MPLS.

Los diferentes accesos que se contemplan en este estudio de procedimiento de configuracion de QoS son para xDSL (ADSL, G.SHDSL), Frame Relay, Mpls Nativo (Red Metro), Multiservicios y STM1

Sumary

Nowadays it exists a great variety of services that offer applications of telephony, data, videoconferencia etc. in a same package, by the same, the companies that have been dedicated to provide these services to their clients have worried that each one of the offered applications fulfills the quality standards. It is by that quality is implemented at access levels of Service (Qos), being is an efficient alternative to optimize a network that shares the bandwidth. In the present work of Degree of Service for network MPLS in different accesses like intermediate network between the end user and the network Mpls is given to a detailed description of the procedure of configuration of Quality, considering the configurations to make in the different ones to router EC located in the ends of network MPLS. The different accesses that are contemplated in this study of procedure of configuration of QoS are for xDSL (ADSL, G.SHDSL), Frame Relay, Mpls Nativo (Network Meter), Multiservicios and STM1

Introducción

El rápido crecimiento de las redes de datos, Internet y los distintos servicios ofrecidos como telefonía IP, Voz sobre IP, video Conferencia y Tráfico crítico, estimula la necesidad de los Proveedores de Servicios de Telecomunicaciones a poseer sofisticadas redes, aptas para ofrecerles y satisfacerles las necesidades a sus clientes.

El tráfico, en términos de bits por segundos, al interior de una red Lan y Wan ha crecido ostensiblemente en la última década, ocasionando frecuentemente problemas de congestión. Dado que las redes de datos han crecido en capacidad y mejorado en tecnología, las diferentes aplicaciones de voz y datos han convergido sobre las redes de datos como medio de transporte.

Normalmente las redes trabajan con la filosofía del mejor esfuerzo: cada usuario comparte ancho de banda con otros y por lo tanto, la transmisión de sus datos tradicionales con las transmisiones de sus datos importantes concurre por el mismo medio. Los datos empaquetados son encaminados de la mejor forma posible, conforme las rutas y bandas disponibles. Cuando hay congestionamiento, los paquetes son descartados sin diferenciación de la aplicación a la que corresponde, por lo tanto no hay garantía que el servicio sea realizado con éxito. Entretanto, aplicaciones como voz sobre IP y videoconferencia necesitan de tales garantías.

Con la implantación de calidad de servicio (QoS), es posible ofrecer mayor garantía y seguridad para las aplicaciones avanzadas, cuando el tráfico de estas aplicaciones pasa a tener prioridad en relación con aplicaciones tradicionales.

El presente trabajo de tesis se enfoca a abordar el tema de la calidad de servicio para una red MPLS con diferentes accesos, destacando cada uno de ellos y la respectiva configuración a realizar que permite la clasificación, el marcado y la priorización de los paquetes.

Objetivos

El presente trabajo de titulación persigue los siguientes objetivos:

Entregar una introducción al diseño de los servicios QoS MPLS-VPN y detallar exhaustivamente la configuración relativa a la porción de Calidad de Servicio (QoS) a implementar en los routers (CE) que se ubican en dependencias de los usuarios finales.

Respecto a lo anterior, hacer referencia a los tipos de redes considerados como acceso entre dependencias del usuario y la red MPLS correspondientes a accesos Xdsl (ADSL y G.SHDSL), Frame Relay, ATM STM-1, Ethernet 10/100 (MS) y accesos Ethernet MPLS Nativo.

Entregar información clara y especifica de las características de una red Mpls, de tal manera de introducir al procedimiento de configuración de QoS para los diferentes accesos mencionados.

Metodo de Trabajo

El tema estudiado aborda el procedimiento de configuración de Calidad de Servicio para los diferentes accesos ya mencionados.
Se inicia estudiando el concepto de QoS (Capítulo I) destacando la importancia de la implementación de ésta cuando hay tráfico diferenciado que comparte un mismo ancho de banda. El capitulo II permite introducirnos al concepto de una red MPLS, en el cual se describen su topología y funcionamiento.

Los capitulo III, IV, V, VI, VII, están orientados netamente a indicar la configuración de calidad de servicio que se realiza para cada acceso, pero antes introduciendo a cada uno de ellos. Para luego terminar con las conclusiones y los comentarios finales.

Restricción y Consideraciones

La configuración de conectividad básica hacia la red MPLS se incluirá en la investigación, no así la configuración de los PE dentro de la red MPLS.

Los roueter CE considerados en la investigación corresponden principalmente a equipamiento CISCO.

Indice

Contenido **Pagina**

Capítulo I

1. QoS (Quality of Service)

1.1 Calidad de Servicio.

La implantación de calidad de servicio (QoS) en redes IP es esencial para el éxito de aplicaciones avanzadas, como telemedicina, videoconferencia y VoIP (voz sobre IP o telefonía sobre IP). Estas aplicaciones demandan, además de gran ancho de banda, un servicio diferenciado. En muchos casos es necesario garantizar que la transmisión de los datos sea realizada sin interrupción o pérdida de paquetes

Normalmente las redes trabajan con la filosofía del mejor esfuerzo: cada usuario comparte ancho de banda con otros y por lo tanto, la transmisión de sus datos corriente con las transmisiones de sus datos importantes concurre con las transmisiones de los demás usuarios. Los datos empaquetados son encaminados de la mejor forma posible, conforme las rutas y bandas disponibles. Cuando hay congestionamiento, los paquetes son descartados sin diferenciación de la aplicación a la que corresponde, por lo tanto no hay garantía que el servicio sea realizado con éxito . Entretanto, aplicaciones como voz sobre y videoconferencia necesitan de tales garantías.

Con la implantación de calidad de servicio (QoS), es posible ofrecer mayor garantía y seguridad para las aplicaciones avanzadas, una vez que el tráfico de estas aplicaciones pasa a tener prioridad en relación con aplicaciones tradicionales.

Con el uso del QoS los paquetes son marcados para distinguir los tipos de servicios y los enrutadores son configurados para crear filas distintas para cada aplicación, de acuerdo con las prioridades de las mismas. Así, una faja de ancho de banda, dentro del canal de comunicación, es reservada para que, en el caso de congestionamiento, determinados tipos de flujos de datos o aplicaciones tengan prioridad en la entrega.

Existen dos modelos de implementación de QoS: servicios integrados (IntServ) y servicios diferenciados (DiffServ). InterServ es basado en reserva de recursos, en cuanto DiffServ es una propuesta en la cual los paquetes son marcados de acuerdo con las clases de servicios predeterminadas.

1.2 Generación de pérdidas, retardos y jitter.

Las pérdidas tienen dos causas fundamentales: los errores de transmisión, debido por ejemplo al ruido en el canal de comunicación y las pérdidas de paquetes en los buffer.

Con la tecnología actual de transmisión, por ejemplo la transmisión óptica, y con algoritmos de recuperación de errores en las capas debajo de IP, las pérdidas debidas a los errores de transmisión son muy poco significativas.

La política 'best effort' implica que si existe más tráfico del que puede ser transportado por un enlace, el sobrante se envía a una cola de donde se irán sacando los paquetes para ser enviados. Si esta cola se llena, los paquetes son descartados.
En cuanto al retardo, el problema es similar. Existen tres fuentes fundamentales de retardo: el retardo de transmisión, el retardo de procesamiento en los enrutadores o switches, y el retardo de las colas de los enlaces. Los dos primeros con la tecnología existente son cada vez menos relevantes. Por otra parte los retardos en enrutadores o switches vienen derivados fundamentalmente del procesamiento de los paquetes. Uno de los procesamientos que genera un retardo es la búsqueda en las tablas de ruteo para decidir el próximo enrutador al que debe enviarse el paquete. Hoy en día estos procesos que antes se hacían por software pueden ser hechos por hardware y a altas velocidades de procesamiento.

El jitter, en telefonía IP o voz sobre Ip es muy importante, por lo que la variación de los retardos de los paquetes debe ser siempre muy baja para no afectar las aplicaciones de telefonía sobre una red de Datos.

De lo anterior concluimos que el problema fundamental para asegurar calidad de servicio es mantener las colas 'casi vacías'. Ahora bien la pregunta es entonces ¿porqué se llenan las colas?. Las colas se llenan porque la capacidad del enlace es momentáneamente menor que la cantidad de tráfico que pretende usar dicho enlace. Una solución obvia a este problema es asegurar una capacidad tal en todos los enlaces de manera que nunca la velocidad de arribo de paquetes sea mayor que la capacidad del enlace. Pero aquí interviene nuevamente la economía. No es razonable económicamente sobredimensionar toda la red. Pero por otra parte si se realizara ¿por cuanto tiempo estaría sobredimensionada?. En estas últimas consideraciones es donde se agregan complicaciones por la naturaleza de IP.

1.3 ¿ Cómo solucionar los problemas de calidad de servicio y aprovechar los recursos de la red?

Como vimos antes es necesario buscar formas que eviten la congestión en la red. Entendemos por congestión en este contexto la situación en la cual la diferencia entre la tasa de arribo de paquetes y la capacidad del enlace es de tal magnitud que no pueden ser satisfechos los envíos de paquetes. Por lo tanto la congestión se generar porque no se tiene capacidad suficiente para transportar todo el tráfico y satisfacer sus requerimientos de calidad de servicio o porque el tráfico está mal distribuido en la red sobrecargando ciertos enlaces y dejando sub-utilizados otros. Este último punto se resuelve aplicando políticas de Ingeniería de Tráfico.
El primer problema que origina la congestión (falta de capacidad) se puede solucionar por dos mecanismos:

Si la red no tiene capacidad suficiente se debe redimensionar la capacidad de la red. Este problema comúnmente se conoce como planificación de capacidades y no será abordado en esta tesis.

En muchos casos no se tiene capacidad suficiente para asegurar QoS al total del tráfico. Sin embargo, dentro del tráfico en muchos casos existen diferentes tipos de tráfico con

diferentes requerimientos. Si se divide la capacidad de los enlaces separando el tráfico de distintas clases por diferentes 'partes' de la capacidad de cada enlace, se puede lograr cumplir con los requerimientos de QoS de cada clase. Esto se puede lograr a través de la aplicación conjunta de tres mecanismos:

1. Dividir el volumen total del tráfico en clases con requerimientos diferentes.

2. Aplicar mecanismos para controlar el volumen de tráfico de cada clase que ingresa la red.

3. Aplicar políticas de despacho y descarte de paquetes en los enlaces de forma de dividir la capacidad total del enlace en las capacidades necesarias para cumplir los requerimientos de cada clase.

En este último enfoque, se basan modelos de QoS sobre IP como por ejemplo el modelo de Servicios Diferenciados DiffServ.

1.4 Una Arquitectura para ofrecer QoS en IP: DiffServ

La primera arquitectura propuesta para ofrecer QoS en IP fue la arquitectura de Servicios Integrados o IntServ (rfc 1633). Esta arquitectura se basaba en garantizar QoS a través de reservar recursos de punta a punta en la red (de host a host) para cada flujo. Esta arquitectura utiliza el protocolo RSVP (rfc 2205), para efectuar la reserva de recursos y para mantenerla a lo largo de la red. Esta arquitectura si bien garantiza QoS, no es escalable y es impracticable en un backbone del corazón de Internet. Para solucionar el problema de escalabilidad de IntServ en la segunda mitad de la década de los 90 en el IETF comenzó a desarrollarse la arquitectura de servicios diferenciados o DiffServ. Esta arquitectura se basa en dividir el tráfico en clases, controlar la cantidad de tráfico que cada cliente envía a la red de cada clase de tráfico y asegurar requerimientos de QoS utilizando en cada enlace políticas de scheduling y dropping.

En la aplicación de QoS, es necesario configurar las siguientes tecnicas de QoS:

- Clasificacion y Marcado
- Shaping y policing
- Tecnicas de Encolamiento
- Call admisión Control

Clasificacion y Marcado.

Como se mencionó anteriormente, es necesario proporcionar los recursos necesarios a las aplicaciones críticas. La idea de separar el tráfico se llama DiffServ, y consiste en un proceso de dos Partes

1. Detectar el Tráfico de Interés
2. Marcar el Tráfico de Interés

Para marcar el tráfico, se debe analizar en detalle la estructura del paquete IP. Al inerior del mismo existe el campo llamado Type of Service (ToS). Este campo consta de un Byte, leidos de izquierda a derecha. La utilización de los bit es hecha en base a dos técnicas.

- IP Precedence: se utilizan los tres primeros bits
- DSCP (Differenciated Service Code Point): se utilizan los seis primeros bits

Por tanto, al momento de establecer o distinguir el tráfico de interes, se procede a colocar una marca en el campo ToS del paquete IP asocada al nivel de importancia que le merece.

Otra forma de marcar tráfico, es a nivel de Ethernet, al interior del mismo, existe el campo TAG y dentro de él otro denominado “Class Of Service” (COS).

El subcampo COS consta de tres bits, leídos de Izquierda a derecha. La utilización de estos bits es hecha de manera similar a lo que es TOS.

Detección del Tráfico de Interés

Para la deteccion del tráfico de interés, se recomienda hacerlo en el router que limita con la red Wan.

El policing es para limitar la tasa de tráfico al ingreso del router, provocando retransmisiones a nivel de TCP, mientras que el shaping limita la tasa de tráfico a la salida con buffering (delay, drop).

Tecnicas de Encolamiento

En el normal de los casos, es decir sin congestión, los equipos despacharán los paquetes hacia la red según orden de llegada, lo que se conoce como **FIFO (first Input First Output)**. En el caso de experimentar congestión el router debe almacenar temporalmente los paquetes en buffer, para luego despacharlos según los criterios establecidos por el tipo de encolamiento empleado.

La tecnica de encolamiento **WFQ (weighted Fair Queuing)**, es una técnica de priorización dinámica, ya que la información a su llegada al router es clasificada según: dirección IP (fuente/destino), Puerto (fuente/destino), Ip precedence, posteriormente se le asigna un peso relativo de acuerdo a cada clasificación. Finalmente el router despachará primero aquellos paquetes de los flujos que tengan un peso relativo más importante.

La tecnica de encolamiento **CBWFQ (Class Based Weighted Fair Queuing)**, es cuando la información es clasificada por dirección IP (fuente/destino), Puerto (fuente/destino), Ip precedence. El tráfico es separado en tantos grupos como aplicaciones existan y cada grupo puede recibir una porcion de ancho de banda asignada arbitrariamente.

La tecnica de encolamiento **LLQ (Low Latency Queuing),** cola de baja latencia, la información a su arribo al router es clasificada según: dirección IP (fuente/destino), Puerto (fuente/destino), Ip precedence. Al igual que CBWFQ, el tráfico puede ser separado en tantos grupos como aplicaciones existan y cada una de ellas puede recibir una porción de ancho de banda asignada arbitrariamente.
Existe una cola de prioridad absoluta, la cual será aplicada al tráfico de voz, con ellas las aplicaciones de telefonía no estarían sujetas al descarte de paquetes o retardo variable. Este tipo de técnica de encolamiento es la que se hace mención en este documento.

El Call Admisión Control, CAC, es un concepto usado generalmente en el transporte de voz, es un mecanismo de restricción de llamadas antes de generarla cuando no hay recursos.

En este documento se entrega una introducción al diseño de los servicios QoS MPLS-VPN desde la perspectiva de la red privada de cliente y se detalla exhaustivamente la configuración relativa a la porción de Calidad de Servicio (QoS) a implementar en los routers (CE) que se ubican en dependencias de clientes y que mediante diferentes accesos que aquí se estudiaran se interconectan con una red Mpls.

Capítulo II

2. Descripción de red MPLS

2.1 Introducción

La gran demanda de los usuarios finales por mayores anchos de banda, servicios diferenciados, aplicaciones más interactivas y consumidoras de recursos de la RED, es que los proveedores de servicios deben mantenerse en constante investigación para posteriormente implementar servicios escalables en el tiempo, con cualidades diferenciadoras de las planteadas por la competencia.

Con respecto a la implantación de nuevas tecnologías en los Service Providers, en muchos casos, este resultado responde a las mayores exigencias solicitadas por sus clientes, como por los aspectos diferenciadores que ofrecen los proveedores de sus competidores, lo que puede producir una merma en la cantidad de clientes con servicios contratados. Por tanto, en general, el disponer de nuevas tecnologías para clientes, se traduce en la mantención de los clientes actuales y más aún, en la posibilidad de atraer nuevos clientes ofreciéndoles servicios diferenciados. Al referirme a lo mencionado, la implementación de una nueva tecnología de los Proveedores de Servicios no implica que sus actuales redes no cumplan o no sean capaz de soportar la demanda o las exigencias de mercado anteriormente mencionadas, si no que deben evaluar un Upgrade de sus redes actuales en función de las exigencias de sus clientes, realizando un estudio de las posibilidades de crecimiento del Backbone actual a tecnologías emergentes de tercera generación.

Junto a los avances tecnológicos en transmisión por fibra óptica (principalmente DWDM), que lleva a conseguir anchos de banda de magnitudes muy superiores, y en tecnología de integración de circuitos ASIC (Application Specific Integrated Circuits), que permite aumentar enormemente la velocidad de proceso de información en la red, hemos de considerar la arquitectura MPLS, sustrato para la inclusión en la red de nuevas aplicaciones y para poder ofrecer diferentes niveles de servicio, en un entorno de mayor fiabilidad y con las necesarias garantías.

MPLS es un estándar emergente del IETF que surgió para integrar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los 90. Como concepto, MPLS es a veces un tanto difícil de explicar. Como protocolo es bastante sencillo, pero las implicaciones que supone su implementación real son enormemente complejas. Según el énfasis (o interés) que se ponga a la hora de explicar sus características y utilidad, 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, incluso, ¿para eliminar por completo el routing? En realidad, MPLS hace un poco de todo eso, 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.

2.2 MPLS y Su Estado del Arte

2.2.1 MPLS: Definición

MPLS significa Multiprotocol Label Switching ó conmutación multiprotocolo de etiquetas. En una red MPLS, a los paquetes entrantes se les asigna una etiqueta, por un router de borde de etiquetas (Edge- Label Switch Router ó E-LSR). Los paquetes son enviados a destino a través de una Ruta de Etiquetas Conmutada (Label Switched Path)

donde cada LSR toma decisiones de envío basado solamente en el contenido de las etiquetas. En cada salto, el LSR extrae la etiqueta actual y aplica una nueva etiqueta la cual indica el próximo salto y como enviar el paquete.
Las Rutas de Etiquetas Conmutadas se establecen por operadores de red para una variedad de propósitos, tales como garantizar un cierto nivel de desempeño, para enrutar tráfico eficientemente en una red en congestión o para crear túneles IP para VPN basadas en la red. De todas maneras, LSPs no son diferentes a las rutas de conmutación de circuitos de las redes ATM o Frame-Relay, excepto que éstas son independientes de la tecnología particular utilizada en la capa 2 del modelo OSI.

Una Ruta de Etiquetas Conmutada puede ser establecida a través de múltiples transportes nivel 2, tales como ATM, Frame-Relay o Ethernet. Es más, una de las reales promesas de MPLS es la habilidad de crear circuitos end-to-end, con características de desempeño específicas, a través de cualquier medio de transporte, eliminando la necesidad de la sobreposición de redes ó mecanismos de control sólo de nivel 2.

Con esta tecnología se puede realizar conmutación del tráfico IP encapsulado en etiquetas (Labels), de forma que el FORWARDING (envío) se realiza a nivel de etiquetas, con el objetivo de obtener buenos tiempos de respuesta, calidades de servicio(QoS), Redes Privadas Virtuales (VPN) e Ingeniería de Tráfico.

2.2.2 Objetivos de MPLS

El objetivo inicial de la conmutación basada en etiquetas fue traer la velocidad de capa 2 a la capa 3. Los métodos de conmutación de etiquetas permiten a los routers tomar decisiones de envío de datagramas basándose en el contenido de una etiqueta simple, en vez de efectuar la compleja búsqueda en tablas de rutas basándose en las direcciones destino del paquete IP (esto se conoce como ROUTE LOOKUP). Esta justificación inicial para tecnologías como MPLS ya no es percibida por el beneficio

principal ya que los actuales switches capa 3 (routers basados en ASIC) están disponibles para realizar ROUTE LOOKUP a muy altas velocidades.
Sin embargo, MPLS trae otros beneficios para las redes basadas en IP, como son:

- Ingeniería de Tráfico (Traffic Engineering). Permite configurar la ruta de tráfico que se escogerá en la red, y la disponibilidad de configurar características de desempeño para deferentes clases de tráfico.

- Redes Privadas Virtuales (VPNs): Usando VPNs, lo proveedores de servicio pueden crear túneles IP a través de la red, sin la necesidad de encriptación o aplicaciones extremo usuario.

- Eliminación de Múltiples Capas: Típicamente la mayoría de las redes de los carriers emplean el modelo de sobreposición de capas donde ATM se usa en la capa 2 e IP en la capa 3. Usando MPLS, los carriers pueden migrar muchas funciones del plano de control de ATM a la capa 3, por tanto, simplificar la administración y complejidad de la red. Eventualmente, las redes de los carriers son capaces de migrar del ATM a otra tecnología, con lo cual se elimina el "cell-tax" inherente de las redes ATM al transportar tráfico IP.

2.2.3 Estado del Estándar MPLS

MPLS es un estándar del organismo Internet Engineering Task Force (IETF), surgido para agrupar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes. La mayoría de los estándares MPLS están actualmente en su fase de "Internet Draft", aunque muchos de ellos han cambiado a la categoría RFC-STD.
No existe un único estándar MPLS. En un momento existirá un conjunto de RFCs que permitirán un sistema MPLS. Por ejemplo, actualmente una hoja técnica de un router IP listará cerca de 20 RFCs en la cual el router debe cumplir. Al ir al sitio WEB de IETF

(http://www.ietf.org) y hace un click en "I-D Keyword Search" ingresando "MPLS" como criterio de búsqueda, se encontrará más de 100 documentos en categoría de borrador existentes en el sitio Web. Estos borradores pueden almacenarse por hasta 6 meses.

Algunos de estos borradores han sido adoptados por el IETF WG para MPLS. El nombre del archivo para estos borradores tienen el prefijo "draft-ietf-". Algunos de estos borradores están actualmente en la vía de convertirse en un estándar IETF.

2.2.4 Componentes MPLS

2.2.4.1 Etiqueta de MPLS

El borrador Internet "Multiprotocol Label Switching Architecture" define una etiqueta como sigue: "Una etiqueta es un identificador de largo fijo y corta longitud la cual es usada para identificar una FEC. La etiqueta la cual es colocada a un paquete particular representa la Clase Equivalente de Envío (Forwarding Equivalence Class ó FEC) a la cual es asignada.

Además, el borrador Internet "A Framework for MPLS" menciona: "En el nivel más sencillo, una etiqueta puede pensarse como nada más que un acceso expedito al encabezado de un paquete, para clasificar la decisión de envío que el router hace para el paquete. En este contexto, la etiqueta es un "acceso directo" para un flujo agregado de datos de usuario.

La etiqueta de MPLS, según el formato SHIM HEADER, está formada de la siguiente forma:

Figura 1: Encabezado MPLS, según formato SHIM

- La etiqueta MPLS de 32-bits está localizada después del encabezado de la capa 2 y antes del encabezado del paquete IP. La etiqueta MPLS contiene los siguientes campos:

- El campo Etiqueta (LABEL) (20 bits) que transporta el valor real de la etiqueta MPLS.

- El campo CoS (3 bits) puede afectar el algoritmo de encolamiento y descarte aplicado al paquete durante su tránsito por la red.

- El campo Stack (S) de 1 bit para soportar una pila para etiquetado jerárquico.

- El campo Time-to-Live (TTL) de 8 bits provee la funcionalidad convencional del paquete IP.
  También se llama encabezado "SHIM".

2.2.4.2 Definición de Label Switched Path

Un LSP es una ruta específica para tráfico a través de una red MPLS. Un LSP se crea usando protocolos de distribución de etiquetas (Label Distribution Protocols ó LDPs) tales como RSVP-TE ó CR-LDP. Cualquiera de estos protocolos establecerán una ruta a través de una red MPLS y reservarán los recursos necesarios para satisfacer los requerimientos de servicio predefinido para la ruta de datos.

Los LSPs deben contrastarse con las troncales de tráfico. Del RFC 2702 se tiene: "Una troncal de tráfico es una agregación de flujos de tráfico de la misma clase la cual es ubicada dentro de un LSP. Sin embargo, es importante enfatizar que existe una distinción fundamental entre una troncal de tráfico y la ruta y el real LSP, a través del cual éste atraviesa. En la práctica, los términos LSP y troncal de tráfico son a menudo

usado como sinónimos. La ruta por la cual atraviesa la troncal puede cambiarse. En este respecto, las troncales de tráfico son similares a los circuitos virtuales de las redes ATM y Frame-Relay.

2.2.4.3 Protocolo de Distribución de Etiquetas ó Label Distribution Protocol (LDP)

Un LDP es una especificación la cual permite a un Label Switch Router (LSR) distribuir etiquetas hacia sus pares LDP. Cuando un LSR asigna una etiqueta a una clase equivalente de envío (Forwarding Equivalence Class ó FEC) éste necesita dar a conocer a sus pares relevantes de sus etiquetas y su significado y el LDP se usa para este propósito. Ya que un conjunto de etiquetas desde el LSR de ingreso hasta el LSR de salida en un dominio MPLS define un LSP y ya que las etiquetas son mapeos de la capa de enrutamiento de red a rutas conmutadas de la capa de enlace
de datos, LDP ayuda a establecer un LSP usando un conjunto de procedimientos para distribuir las etiquetas entre los pares LSR.

Los LSRs usan etiquetas para enviar tráfico. Un paso fundamental para la conmutación de etiquetas es que los LSRs deben estar de acuerdo en qué etiquetas deberían utilizar para enviar el tráfico. Éstas sirven para el entendimiento de la distribución de etiquetas.

LDP es la parte principal de MPLS. Mecanismos similares para intercambio de etiquetas existieron en otras implementaciones de proveedores anteriores, como Flow Management Protocol (IFMP) de Ipsilon, Aggregate Route-based IP Switching (ARIS) de IBM, y Tag Distribution Protocol de Cisco Systems. LDP y las etiquetas son la base para la conmutación de etiquetas.

LDP tiene las siguientes características básicas:

- Provee un mecanismo de descubrimiento de LSR para habilitar a otro par LSR encontrarse mutuamente y establecer una comunicación.
- Define cuatro clases de mensajes: DISCOVERY, ADJACENCY, LABEL ADVERTISEMENT, y NOTIFICATION

- Opera sobre TCP para entregar los mensajes en forma confiable (con la excepción de los mensajes DISCOVERY)

En LDP, la distribución y asignación de etiquetas pueden efectuarse de varios modos diferentes.

- No solicitado aguas abajo (unsolicited downstream) ó asignación de etiquetas aguas abajo según demanda (downstream-on-demand).

- Control de LSP independiente u ordenado.

- Retención de etiquetas conservadoras ó liberales.

2.2.5 Diferencias entre CR-LDP y RSVP-TE

Existen actualmente dos mecanismos propuestos para la ingeniería de tráfico de MPLS (MPLS Traffic Engineering ó MPLS-TE) que están siendo considerado por el IETF MPLS Working Group, como lo es CR-LDP y RSVP-TE. Por tanto, son dos mecanismos diferentes para lograr el mismo objetivo. Cisco, Avici, Argon, Ironbridge, Juniper y Torrent están soportando RSVP, mientras que Ericsson, Ennovate, GDC y Nortel son los principales promotores de la propuesta CR-LDP.
Recientemente, muchos proponentes de CD-LDP anunciaron que también soportarán MPLS RSVP-TE.

CR-LDP y RSVP-TE son mecanismos de señalización usados para soportar TE a través de un Backbone MPLS. RSVP es un protocolo de señalización de QoS que es un estándar IETF y ha sido usado en algunas implementaciones a usuarios por algún tiempo. RSVP-TE propone extender el RSVP para soportar distribución de etiquetas y enrutamiento explícito mientras que CR-LDP propone extender el LDP (diseñado para distribución de etiquetas salto a salto para soportar señalización QoS y enrutamiento explícito). Los túneles MPLS TE no están limitados por los procedimientos de selección de ruta IP y por tanto, diseminarán el tráfico de red más uniformemente a través del Backbone aprovechando todos los enlaces disponibles. Un protocolo de señalización se requiere para configurar estas rutas explícitas de MPLS o túneles.

Existen muchas similitudes entre CR-LDP y RSVP-TE para las redes MPLS basadas en Paquetes. Los objetos de ruta explícita que se usan son muy similares. Ambos protocolos usan procedimientos de establecimiento de LSP en forma ORDENADA Ambos protocolos incluyen alguna información de QoS en los mensajes de señalización para habilitar la asignación de recursos y establecimiento de LSP en forma automática.

Los proveedores que soportan RSVP siguen el paradigma que si existe un protocolo que puede ser fácilmente extendido para soportar un nuevo conjunto de funciones mientras que también continúa siendo compatible con el protocolo original, es menos doloroso en la introducción de la tecnología en redes en producción. Ellos argumentan que ya que el protocolo ha estado en uso por algún tiempo, se entiende mejor para implementadores y la comunidad de usuarios. RSVP-TE está basado en extensiones de RSVP que es el protocolo usado para señalización de QoS y por tanto calza bien con la propuesta y el trabajo realizado por varios estándares IETF y ha sido ampliamente implementado. Uno de los mitos comunes de RSVP es que no es escalable. La experiencia ha demostrado a los usuarios e implementadores que el uso tradicional de RSVP en tratar de rastrear el estado de los flujos iniciados por usuarios extremo-a-extremo, es tan escalable como cualquier otro protocolo de señalización. La cantidad de estado que un protocolo de señalización debe mantener es principalmente una función del número de flujos y que es verdadero para cualquier protocolo de señalización, no

sólo RSVP. En MPLS-TE, la agenda es mantener el estado de troncales con ingeniería de tráfico y no flujos extremo-a-extremo iniciados por usuarios.

Como el debate continúa, existen algunos beneficios principales de una propuesta sobre otra. Una de las motivaciones principales para usar RSVP para soportar rutas explícitas es la suposición que muy a menudo las rutas explícitas se usarán en conjunto con la reserva de recursos a lo largo de esas rutas. Esta suposición está basada en el uso esperado de rutas explícitas en tales aplicaciones como también en proveer envío en el soporte de enrutamiento basado en QoS. En tales casos, usar RSVP para soportar rutas explícitas permite tanto el establecimiento de una ruta
explícita como la asignación de recursos para tráfico que será enviado a lo largo de la ruta. Esto es consumado sólo usando RSVP, más que teniendo un protocolo para establecimiento rutas explícitas y otro para hacer reserva de recursos a través de esas rutas. Usar RSVP, entonces, impulsa el trabajo existente realizado por el IETF sobre QoS.

2.2.6 Defínción de Clase de Equivalencia de Envío ó "Forwarding Equivalency Class"

FEC es un conjunto de paquetes la cual será enviada de la misma manera (por ejemplo, sobre la misma ruta con el mismo tratamiento de envío). Típicamente, los paquetes pertenecientes a la misma FEC seguirán la misma ruta en el dominio MPLS. Cuando se asigna un paquete a una FEC, el LSR de entrada puede ver el encabezado IP y también otra información, como la interface por donde se recibe el paquete. La FEC a la cual el paquete es asignada se identifica con una etiqueta.

Un ejemplo de una FEC es un conjunto de paquetes UNICAST donde la dirección de red de destino calza con un prefijo IP particular. Un conjunto de paquetes MULTICAST con la misma dirección de red fuente y destino es otro ejemplo de una FEC. Otro

ejemplo es un conjunto de paquetes UNICAST cuya dirección destino calza con un prefijo IP particular y donde todos los bits Tipo de Servicio (TOS) son iguales.

2.2.7 Construcción de las rutas conmutadas de etiquetas ó Label Switched Paths.

Un LSP es un conjunto de LSRs en la cual los paquetes pertenecen a una cierta FEC para alcanzar sus destinos. Ya que MPLS permite jerarquías de etiquetas conocidas como pilas de etiquetas (STACK de etiquetas), es posible tener diferentes LSPs en diferentes niveles de etiquetas para un paquete alcanzar su destino.

Como un ejemplo, considerar el siguiente escenario:

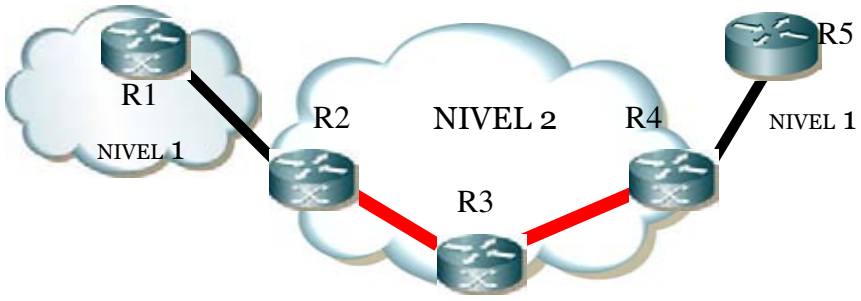


Figura 2: STACK de Etiquetas

En la figura anterior, R1 y R5 son LSRs donde el paquete P debe viajar para alcanzar su destino. Los números 1 y 2 son profundidades en la pila de etiquetas. R1 y R5 son Border GW Routers y R2, R3 y R4 son Interior GW Routers. Para el propósito del envío de etiquetas R1 y R5 son pares en el nivel del Border Gateway y R2, R3, R4 son pares en el nivel Interior Gateway. Cuando R1 recibe el paquete P con una etiqueta que tiene el nivel de profundidad 1, éste cambiará la etiqueta de P con la correspondiente etiqueta que será usada por R5. Ya que el paquete tiene que viajar por R2, R3 y R4, R1 pondrá una nueva etiqueta y la profundidad de la pila será de nivel 2. Por tanto, se tienen 2

LSPs en este caso. Uno está en nivel 1 desde R1 a R5 y existe un segundo nivel desde R2 a R4.

Para construir un LSP los LSRs hacen uso de los protocolos de enrutamiento y las rutas aprendidas de estos protocolos. Ellos pueden usar otros protocolos como RSVP, pero no es necesario.

El establecimiento del LSP puede ser de control Independiente o ordenado. Control independiente del establecimiento LSP es cuando la conmutación de etiqueta es usada para soportar el enrutamiento basado en el destino. Aquí, cada LSR puede tomar una decisión independiente para asignar una etiqueta a una FEC y anunciar esa asignación a sus vecinos. Esta forma de establecimiento de un LSP continúa la convergencia del enrutamiento casi inmediatamente. En el control ordenado, el proceso de asignación de etiquetas se efectúa de forma ordenada de un extremo de un LSP al otro. El establecimiento del LSP puede ser iniciado por el inicio o final del LSP.

El enlace de etiquetas puede ser creado local o remotamente, por LSRs aguas abajo o aguas arriba. Éstos pueden crearse en respuesta a tráfico de control o datos y el enlace puede ser distribuido por un protocolo independiente (LDP) o por otro con extensiones (por ejemplo, BGP).

2.2.8 Relación entre MPLS y un protocolo de enrutamiento interior

Los protocolos Interior Gateway Protocols (IGP), tales como OSPF y IS-IS, se usan para definir la alcanzabilidad y el enlace/mapeo entre una FEC un la dirección del próximo salto. MPLS aprende información de enrutamiento del IGP (como, OSPF, IS-IS). Generalmente un protocolo de enrutamiento tipo Estado de Enlace ya está operado en las grandes corporaciones o en redes de proveedores de servicio. No se requiere realizar cambios a los protocolos de enrutamiento IGP para soportar MPLS, MPLS-TE, MPLS QoS, o MPLS-BGP VPNs.

2.2.9 Protocolos soportados por MPLS

Por definición, Multiprotocol Label Switching soporta múltiples protocolos. A nivel de capa de red MPLS soporta IPv6, IPv4, IPX y AppleTalk, A nivel de enlace de datos MPLS soporta Ethernet, Token-Ring, FDDI, ATM, Frame-Realy y enlaces punto a punto. Esencialmente puede trabajar con cualquier protocolo de control otro fuera de IP sobre cualquier protocolo de enlace de datos.

2.3 MPLS Y ATM

2.3.1 Diferencias entre MPLS y ATM

MPLS trae las capacidades de ingeniería de tráfico (TE) del ATM a una red basada en paquetes. Opera marcando paquetes IP con etiquetas que especifican una ruta y prioridad. Combina la escalabilidad y flexibilidad del enrutamiento con el desempeño y administración de tráfico de la conmutación de la capa 2. Puede operar sobre casi cualquier medio de transporte (ATM, FR, Ethernet), en vez de estar atado a un método de encapsulación específico de la capa 2.

2.3.2 Convivencia MPLS y ATM

MPLS no reemplaza a ATM, sino que se complementa con esa tecnología. MPLS elimina la complejidad de mapear direcciones IP e información de enrutamiento directamente en las tablas de conmutación ATM. El paradigma de la conmutación de etiquetas de MPLS es el mismo mecanismo que los switches ATM usan para el envío de celdas ATM. Para un ATM-LSR la función de intercambio de etiquetas se desarrolla en el componente de envío del ATM. La información de la etiqueta se transporta en el encabezado del ATM, específicamente en los campos VPI/VCI. MPLS puede operar sobre Routers como también sobre switches ATM. MPLS provee el componente de control del IP en routers y switches ATM. Para switches ATM PNNI, ATM ARP Server y

NHRP Server son reemplazados con MPLS por direcciones IP. El plano de control ATM se mantiene. PNNI aún se usa en switches ATM para proveer servicios ATM. Por tanto, un switch IP+ATM entrega lo mejor de ambos mundos (ATM para conmutación rápida y protocolos IP para Históricamente, para un nivel de desempeño determinado, el precio de un router tiende a ser mayor que su equivalente Switch ATM. Con IP+ATM LSRs el desempeño de envío está determinado por las capacidades de los switches ATM, mientras que la funcionalidad es comparable con la de un router. Además, switches IP+ATM pueden también tener características de precio/desempeño similares a los switches ATM.

2.3.3 "Ships in the night": Definición

Algunos proveedores soportan correr MPLS y ATM en el mismo dispositivo. En general, estos dos procesos operan independientemente. Un cambio en una ruta MPLS no tiene significación sobre los VCs ATM. Esta práctica es usualmente referida como "ships in the night" ya que dos procesos actúan independientemente. Sin embargo, en algunos casos, existe algún tipo de interacción entre ambos procesos. Por ejemplo, algunos proveedores soportan un mecanismo donde la reserva de recursos de un LSP se detecta por el mecanismo de control ATM para evitar problemas de conflictos de recursos.

"Ships in the night" será utilizado como un mecanismo de transición en la medida que las redes cambien su plano de control ATM a MPLS. Las redes inicialmente conservarán ATM para transportar tráfico de datos sensible a retardos, como voz y video, y para conectarse a nodos no habilitados con MPLS, mientras que simultáneamente operando MPLS para transportar datos.
Según la evolución de la característica MPLS-QoS, se piensa que no será necesario mantener la infraestructura para flujos ATM separados y por tanto las redes sólo transportarán tráfico basado en etiquetas MPLS.

2.4 MPLS Traffic Engineering

2.4.1 Objetivo de MPLS-TE

Traffic Engineering se refiere al proceso de seleccionar rutas escogidas por tráfico de datos con el objeto de balancear carga sobre varios enlaces, routers y switches en la red. TE es lo más importante en redes donde existen disponibles múltiples rutas alternativas.
El principal objetivo de Internet TE es facilitar las operaciones eficientes y confiables de la red mientras que simultáneamente optimizar la utilización de los recursos de red y el desempeño del tráfico.

El objetivo de TE es calcular la ruta desde un nodo al otro (source routing), tal que la ruta no viole los compromisos definidos y es la mejor respecto a alguna métrica escalar. Una vez que la ruta está calculada, TE (en el caso de MPLS basado en paquetes) es responsable por el establecimiento y mantención del estado de envío a lo largo de esa ruta.

2.4.2 Componentes de MPLS-TE

Para soportar TE, a pesar del enrutamiento explícito de fuente (source routing), los siguientes componentes deberían estar disponibles:

- Habilidad de calcular la ruta tomando en cuenta todos compromisos. Para hacer esto, la fuente necesita tener toda la información ya sea disponible localmente o obtenida de otros routers en la red (por ejemplo, topología de red).

- Habilidad de distribuir la información de la topología de red y sus atributos asociados con los enlaces a través de toda la red una vez que se calcula la ruta, y necesita una forma de soportar el envío a lo largo de toda la ruta.

- Habilidad de reservar los recursos de red y modificar los atributos de los enlaces (como resultado que cierto tráfico escoge ciertas rutas)

MPLS-TE promueve varios aspectos fundamentales en la tecnología.

- Algoritmo de la ruta más corta primero soportando los compromisos (constraint shortest path first algorithm) usado para el cálculo de la ruta. Esta es una versión modificada del algoritmo SPF con extensiones para soportar los compromisos (constraints support)

- Extensiones de RSVP o CR-LDP usado para establecer el estado de envío a lo largo de la ruta, como también reservar recursos a lo largo de la ruta.

- IGPs tipo Estado de Enlace con extensiones (OSPF con LSAs Opacos, IS-IS con Link State Packets TLV (type, length, value)), que mantienen rastreo de la propagación de los cambios topológicos.

2.4.3 Fusión en los Flujos de Tráfico MPLS

MPLS permite el mapeo de paquetes IP a una FEC para realizar sólo una vez, en el ingreso del dominio MPLS. Una FEC es un conjunto de paquetes que pueden ser manejados equivalentemente con el propósito de envío y por tanto conviene para el enlace con una única etiqueta.
Desde el punto de vista del envío, los paquetes en el mismo subconjunto son tratados por el LSR de la misma forma, aún si los paquetes difieren entre sí con respecto a la información en el encabezado de la capa de red. La relación del mapeo entre la información transportada por el encabezado de la capa de red de los paquetes y las entradas en la tabla de envío del LSR es muchas a una. Esto significa que paquetes con diferente contenido en sus encabezados de capa de red pueden ser mapeados a la misma FEC.

2.5 Recuperación de fallas en MPLS

Cuando se cae un enlace es importante reenrutar todos los TRUNKs que eran enrutados por ese enlace. Ya que la ruta escogida por un Trunk está determinada por el LSR al comienzo de la ruta MPLS, el reenrutamiento debe efecturarse por el LSR que inicia la ruta. Para realizarlo, el LSR puede contar con la información obtenida por el IGP o por RSVP/CR-LDP.

Sin embargo, otra técnica existente para evitar la carga de involucrar a los LSR inciadores de rutas de todos los LSPs que atraviesan ese enlace se llama Reenrutamiento Rápido.

2.6 Diferencias entre MPLS usando OSPF e IS-IS

Esto no es un tópico de MPLS, sino más bien está relacionado con los protocolos de enrutamiento interiores (IGP). Las extensiones de MPLS, definidas en los RFCs del IETF, soportan a ambos protocolos. MPLS y BGP-VPN de los desarrollos del mundo real operan con ambos protocolos.

Existe gran debate de cuál IGP es mejor. Este debate está usualmente centrado en la escalabilidad. Se piensa que IS-IS es más escalable que OSPF. Es decir, una única área OSPF puede soportar hasta 150 routers mientras que una única área IS-IS puede soportar hasta 500 routers. En la actualidad, se han implementado redes OSPF e IS-IS muy grandes.

Finalmente, es importante comprender los beneficios y detractores de cada protocolo. Luego, usar los requerimientos de la red/clientes para escoger el protocolo IGP más adecuado y que mejor satisface las necesidades.

2.7 MPLS VPNs

2.7.1 Habilitación de VPNs en MPLS

Debido a que MPLS permite la creación de circuitos virtuales o túneles a través de una red IP, es natural pensar en el uso de MPLS para proveer servicios tipo Virtual Private Network. Usando MPLS VPN se permite la aislación de tráfico, parecido al servicio Frame-Relay o ATM. MPLS actualmente no tiene mecanismos para encriptación de paquetes, de forma que si un usuario requiere encriptación, debe usarse algún otro método, tal como IPsec. La mejor forma de pensar MPLS VPN es considerarla como un equivalente a un circuito virtual ATM o Frame-Relay.

2.7.2 Terminología

Dentro de una red MPLS-VPN se tiene una terminología diferente a la que actualmente se maneja para el Backbone/Edge MPLS.
Por ello, se define lo siguiente:

- Equipo P: Equipo Proveedor (Provider), el cual tiene como función la conmutación de etiquetas a nivel de L2 y mantiene el plano de control de L3. Equipo de CORE. Sus funciones son idénticas al equipo LSR.

- Equipo PE: Provider Edge. Corresponde al equipo de borde de la red MPLS. Forma parte de los equipos del Proveedor de la red MPLS. Significa que sus funciones son de poner y sacar las etiquetas, determinando la ruta (camino) LSP que se establecerá sobre la red MPLS. Además, debe establecer sesiones iBGP entre los otros PEs para pasarse la información de cada VPN-IPv4 y separarla en cada VRF (VPN Routing & Forwarding). En general, esta función se implementa en los equipos E-LSR (Edge LSR) ó LER (Label Edge Router).

- Equipo CE: Equipo perteneciente a la red del cliente. Este equipo trafica datos IP puros, con los protocolos de enrutamiento conocidos del mercado (RIPv1, RIPv2, OSPF, rutas estáticas, EIGRP, etc.).

2.7.3 Alternativas existentes para implementar VPNs sobre MPLS

Existen muchas propuestas para usar MPLS en la provisión de VPNs basadas en IP. Una propuesta (RFC2547-MPLS/BGP VPNs) habilita MPLS-VPNs mediante extensiones de BGP. En este enfoque BGP propaga información de VPN-IPv4 usando Extensiones Multiprotocolo de BGP (MP-BGP) para manejar estas direcciones extendidas. Se propaga la información de alcanzabilidad (direcciones VPN-IPv4) entre el Edge LSR (Provider Edge Router). La información de alcanzabilidad para una VPN determinada se propaga sólo a los miembros de esa VPN. MP-BGP identifica los receptores válidos para la información de enrutamiento para la VPN. Las rutas aprendidas en la VPN se propagan a todos los miembros de ella.

Otra propuesta para usar MPLS para crear IP-VPNs está basada en la idea de mantener tablas de rutas separadas para varias VPNs y no involucrar a BGP (Network Based IP-VPN Architecture Using Virtual Routers).

La mayoría de las primeras implementaciones MPLS-VPNs están basadas en el RFC2547.

2.7.4 Servicios disponibles con MPLS VPN

Al habilitar la Red con el servicio tipo MPLS VPN, se puede ofrecer servicios de interoperabilidad entre diferentes puntos de acceso a la red MPLS. Es decir, sea un usuario X y usuario Y, ambos con equipos CE de acceso a la red MPLS. Debido a la versatilidad en la implementación de VPNs de nivel 3 sobre la Red, entonces, pueden acceder al servicio tipo ASP (Application Service Provider), donde la casa matriz del usuario X y la casa matriz del usuario Y puede tener acceso a la red del Proveedor de Contenido, sin tener que usar otro acceso adicional al que actualmente existe de su casa matriz. Esto es válido para cualquier equipo CE que accede al Backbone MPLS.

De esta forma, se puede facilitar la administración para el Proveedor pues sólo por un acceso, puede fácilmente ofrecerse el servicio de Intranet (conexiones de los sitios remotos de un mismo cliente entre sí), servicio Extranet (conexiones de clientes con asociados comerciales), servicio Internet (conexión de la(s) sucursal(es) de con Internet).

2.8 MPLS Quality of Service

2.8.1 Soporte de Protocolos QoS en MPLS.

MPLS soporta el mismo QoS que IP. Estos mecanismos son: IP Precedence, Committed Access Rate (CAR), Random Early Detection (RED), Weighted RED, Weighted Fair Queuing (WFQ), Class-based WFQ, and Priority Queuing. Otros mecanismos propietarios y no estandarizados también están soportados, pero no garantiza la interoperabilidad con otros proveedores.

Ya que MPLS también soporta la reserva de recursos a nivel 2, MPLS puede entregar una granularidad fina de calidad de servicio, en forma muy similar a las redes de ATM y Frame-Relay.

2.8.2 Integración de MPLS y DiffServ

Se espera que ambos enfoques se implementen en las redes de los proveedores de servicio. DiffServ puede soporta hasta 64 clases, mientras que la etiqueta de MPLS soporta hasta 8 clases. Esta pequeña etiqueta tiene 3 bits en el campo definido para uso experimental. Esto define el siguiente problema. Este campo experimental de sólo 3 bits de largo como puede compatibilizarse con los 6 bits del campo usados en el enfoque DiffServ. Existen varios escenarios donde entregar una solución alternativa.

Existen dos alternativas que solucionan este problema llamados modelos Label-LSP y Exp-LSP. Sin embargo, estos modelos introducen complejidad a la arquitectura.
El modelo DiffServ esencialmente define la interpretación de los bits TOS. Debido a que los bits del IP Precedence se mapean a los bits Experimentales (EXP) con la misma interpretación, entonces es aplicable el modelo DiffServ. En el caso que bits adicionales se usen en el modelo DiffServ, se puede usar el valor de etiqueta para interpretar el significado de los bits remanentes. Reconociendo que 3 bits son suficientes para identificar el números de clases requeridas, los bits restantes en el modelo DiffServ son usados para identificar la prioridad de descarte y estas prioridades de descarte pueden mapearse a un L-LSP en el cual se usará para identificar la prioridad de descarte mientras los EXP bits identifican la clase a la cual el paquete pertenece.

Muchos proveedores de servicio tienen o se ajustarán a un pequeño número de clases. Esta pequeña mejora será difícil de provisionar, administrar y vender. Esto será una estrategia para llegar al mercado rápidamente con un servicio de valor agregado.

Las clases siguientes pueden ser apropiadas para el desarrollo inicial de MPLS QoS:

- High-priority, low-latency "Premium" class– (Gold Service)
- Guaranteed-delivery "Mission-Critical" class– (Silver Service)
- Low-priority "Best-Effort" class– (Bronze Service)

2.8.3 Integración de MPLS y ATM QoS

MPLS hace posible aplicar QoS a través de una gran red ruteada o switcheada debido a que los proveedores de servicio puedan designar un conjunto de etiquetas que tengan significado especial, tal como clase de servicio. Las redes tradicionales ATM y Frame-Relay implementan CoS con circuitos virtuales punto a punto, pero esto no escala en redes IP. Mapeando los flujos de tráfico en los bordes en clases de servicio que habilitan a los proveedores para hacer ingeniería y administrar las clases a través de toda la red.

Si los proveedores de servicios administran las redes basados en clases de servicio (no en conexiones punto-a-punto), se pueden reducir en forma importante la cantidad de detalle que se debe rastrear e incrementar la eficiencia sin perder funcionalidad. Comparado con la administración por circuito, los servicios CoS habilitados en MPLS provee virtualmente todos los beneficios sin
agregar complejidad. Usando MPLS para establecer IP CoS se agrega el beneficio de eliminar la configuración por circuito virtual. Por tanto, la red completa es más sencilla de provisionar y realizar ingeniería.

2.9 MPLambdaS

2.9.1 Provisión de Rutas Ópticas usando MPLS

Los conceptos fundamentales, software y hardware de MPLS evolucionarán para soportar Multiprotocol Lambda Switching (MPLambdaS). MPLS separa el plano de control del plano de datos. La tecnología MPLS soporta a routers y switches ATM y los cuerpos estandarizadores están trabajando en usar MPLS sobre optical cross-connect (OXC), llamadas conmutación de etiquetas ópticas ó optical label switching (MPLambdaS).

MPLambdaS está basado en el enrutamiento de longitudes de onda individuales (lambdas). Más que el intercambio de etiquetas sobre la base de hacerla por paquete y por salto, las lambdas son intercambiadas entre la puerta de entrada y salida de OXC. Rutas ópticas se provisionarán con extensiones (Label Object) para MPLS-TE y OSPF/IS-IS. Esto puede lograrse incrustando la funcionalidad de MPLS-IP en elementos ópticos, tales como OXC. MPLambdaS puede ser la clave para unificar el plano de control para todos los elementos ópticos. Esto puede ayudar en la provisión de servicios y rutas ópticas mientras se habilita la rápida recuperación de la red IP y la ingeniería de tráfico.

2.9.2 Función del "Optical Internetworking Forum"

El foro de Internetworking Óptico es una organización abierta de la industria de equipamiento de proveedores, proveedores de servicios de telecomunicaciones y usuarios finales dedicados a promover el desarrollo global de productos ópticos y fomentar el desarrollo e implementación de productos y servicios interoperables para conmutación de datos y enrutamiento usando tecnologías de Networking ópticas.

El OIF fomenta la cooperación entre participantes de la industria de telecomunicaciones incluyendo equipamiento de proveedores, proveedores de servicio y usuarios finales, promover el desarrollo global de productos ópticos de internetworking, promover a nivel nacional y mundial la compatibilidad e interoperabilidad, facilitar ingreso de información para los cuerpos estandarizadores a nivel nacional e internacional e identifica, seleccionar, defender los bosquejos de publicaciones de especificaciones de optical internetworking a los cuerpos estandarizadotes nacionales e internacionales.

Capitulo III

3. Accesos xDSL

3.1 Introducción a las tecnologías xDSL.

xDSL es un grupo de tecnologías de comunicación que permiten transportar información multimedial a mayores velocidades que las obtenidas actualmente simplemente utilizando las líneas telefónicas convencionales (par de cobre).

Estas Tecnologías nacen por la necesidad de cubrir las limitaciones de de la red telefónica, soportan un gran ancho de banda con unos costos de inversión relativamente bajos y además trabajan sobre la red telefónica ya existente, convirtiendo la línea analógica convencional en una línea digital de alta velocidad, la conexión del cliente y el nodo de la red que permite un flujo de información es tanto simétrico como asimétrico

xDSL es una tecnología en la que se necesita un dispositivo módem xDSL terminal en cada extremo del circuito de cobre, que acepte flujo de datos en formato digital y lo superponga a una señal analógica de alta velocidad. Todas utilizan la modulación para alcanzar elevadas velocidades de transmisión.

Esta tecnología opera sobre conexiones que no superen los 6 km de distancia entre el nodo y el lugar de conexión del abonado, dependiendo exclusivamente de:

- Velocidad alcanzada
- Calidad de las líneas
- Distancia
- Calibre del cable
- Esquema de modulación utilizado.

La ventaja de las técnicas xDSL consiste en soportar mas de un canal sobre un único par de cables. Basándose en esto, los operadores telefónicos proporcionan habitualmente tres canales: dos para datos (bajada y subida) y uno para voz.

A continuación veremos una gráfica donde se muestran los diferentes anchos de banda de las diferentes xDSL existentes al transmitir por el par de cobre.

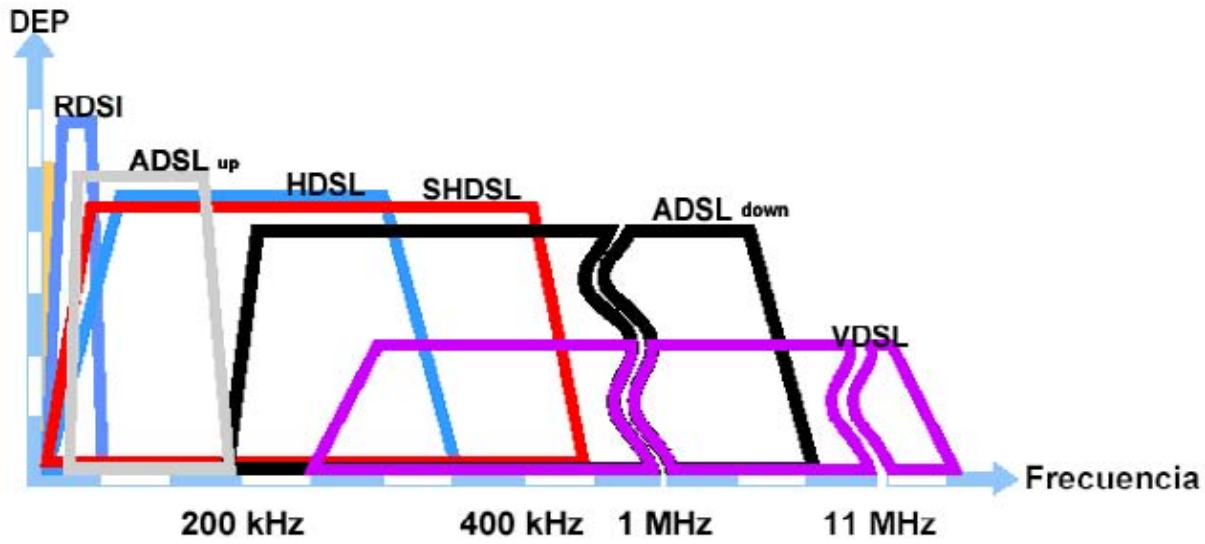


FIGURA 3: bandas de operación de xDSL

3.2 Evolución de las diferentes tecnologías xDSL.

Hay varias tecnologías xDSL, cada diseño especifica y justifica fines y necesidades de venta y mercado. Algunas formas de xDSL son propiedad, otras son simplemente modelos teóricos y otras son usadas como estándar.

A continuación se indican algunas de las tecnologías xdsl, de las cuales se describirá ADSL y G.SHDSL que son las tecnologías de accesos que se tratará en este documento como red intermedia entre usuario y la Red MPLS.

SDSL *(Symetric Digital Subscriber Line):* es una versión de HDSL y como tal es simétrica. Permite ancho de banda simétrico tanto en el sentido del NSP al cliente

como en sentido contrario. El código de línea utilizado es 2B1Q y puede transmitir hasta 1.54 Mbps.

HDSL *(High speed Digital Subscriber Line)*: Consiste en la transmisión de 2Mbps sobre pares de cobre utilizados en telefonía. El código de línea utilizado es 2B1Q. Sus aplicaciones son muy variadas, es decir, es aplicable siempre que se requieran transmitir 2Mbps entre usuarios, por ejemplo: acceso al servicio de líneas alquiladas, acceso a estaciones base de telefonía móvil, etc.

HDSL-2 *(High speed Digital Subscriber Line 2)* -> Es una alternativa a HDSL que ofrece un servicio simétrico a las velocidades T1, requerirá una modulación mas agresiva, distancias mas cortas y líneas telefónicas mejores, utiliza el código de línea 2B1Q, transmite a 1,5 Mbps, pero su mayor ventaja es que esta diseñada para no interferir a otros servicios.

G. SHDSL *(Symetric High speed Digital Subscriber Line)* -> El SHDSL se puede considerar como una mejora sustancial del HDSL, que está llamado a reemplazarlo. Se estima que en los próximos años el HDsL habrán sido sustituido por SHDSL.

ADSL *(Asymetric Digital Subscriber Line)*-> Sistema más utilizado y desplegado en la actualidad, apareció a entre 1989 y 1990, la carga útil es de 8 Mbps hacia el abonado y 640 kbps en sentido inverso.

VDSL (*Very High speed Digital Subscriber Line)* -> Extendiendo los límites de la tecnología del ADSL podemos conseguir utilizar mayor ancho de banda sobre el par de cobre, hasta llegar a los 11 MHz. Por supuesto, estos anchos de banda sólo son factibles para alcances más reducidos de los que hemos visto en ADSL. Mientras el objetivo de alcance en ADSL era cubrir el área de servicio de la central, en VDSL las áreas cubiertas son mucho menores.

3.3 G.SHDSL y ADSL.

3.3.1 ¿Qué es G.SHDSL ?

(Single-pair High-speed Digital Subscriber Line)

También conocido como G.991.2, el G.SHDSL es un standard internacional para el DSL simétrico, desarrollado por la ITU. El G.SHDSL provee los medios para enviar y recibir streams de datos simétricos de alta velocidad sobre un par de cobre a velocidades de entre 192 kbps y 2.31 Mbps. El G.SHDSL fue desarrollado para incorporar las características de otras tecnologías DSL, como el ADSL y el SDSL y puede transportar señales de T1, E1, ISDN, ATM e IP. el cual ofrece un conjunto de características muy ricas (por ejemplo, tasas adaptables) y ofrece mayores distancias con un 30% más de longitud del cable que SDSL y que cualquier estándar actual.

El G.SHDSL fue ratificado por la ITU en Febrero de 2001.

3.3.2 Características.

El G.SHDSL está diseñado para el transporte de datos de forma simétrica a regímenes que se adaptan a las características del canal y que van desde 192 kbps a 2.3Mbps.

Mientras las aplicaciones de HDSL se limitan a transportar servicios de Multiplex por División en el Tiempo (TDM), desde el principio, el G.SHDSL está siendo utilizado para transportar cargas tanto TDM como ATM.

El sistema G. SHDSL podría ser entre dos y tres veces más rápido que la mayor parte de las conexiones DSL clásicas (llega hasta los 4,6 Mbps, con 2 pares de cobre). Otra de las ventajas del G.SHDLS es que permite tener al usuario en una distancia mayor, distancia limitada hoy en día a unos 4,5 kilómetros.

3.3.3 Estándares de la tecnología.

Hasta ahora, SHDSL ha sido estandarizado por tres cuerpos de estandarización, los diferentes estándares de normalización son los siguientes:

ANSI: T1E1.4/2001-174 para Norteamérica
ETSI TS 101524 para Europa
ITU-T (G.991.2) para todo el mundo

ETSI así como ITU están trabajando actualmente en mejoras.

La otra tecnología xDSL que se analiza como acceso intermedio entre el usuario final y la red MPLS, me refiero a ADSL, solo se realizara una definición y mencion de sus características, ya que es bastante conocida como para incluirla en este documento.

3.4 ¿Que es la ADSL?

Asymmetric Digital Subscriber Line (Linea de Abonado Digital Asimétrica).

Tecnología que permite separar canales de transmisión (Ascendentes) y recepción (descendentes) en forma independiente, además entrega la capacidad necesaria para enviar desde la central hacia el abonado (sentido descendente) canales de transmisión de varios Mbps. ADSL nos permite hablar por teléfono y transmitir datos al mismo tiempo.

3.4.1 Funcionamiento del ADSL

El ADSL es una técnica de modulación de la señal que permite una transmisión de datos a gran velocidad a través de un par de hilos de cobre.

La primera diferencia entre la modulación de los módems de 56K y los de ADSL es que esto modulan a un rango de frecuencias superior a los normales [24… 1.104] KHz para los ADSL y [300… 3.400] Hz para los modems tradicionales, esto supone que ambos tipos de modulación pueden estar activos en un mismo instante ya que trabajan en rangos de frecuencia distintos.

3.4.2 Evolución

Durante la primera etapa existían dos tipos de modulación para el ADSL:

- CAP: Carrierless Amplitude/Phase (Modulación por amplitud de fase sin portadora).
- DMT: Discrete MultiTone (Modulación por Multitonos Discretos).

Los organismos de estandarización se decidieron por la DMT, que lo que hace es usar varias portadoras en vez de una sola que es lo que hace la modulación vocal. Cada una de estas portadoras se modula en cuadratura, es decir, igualmente separadas entre ellas y cada una tiene una banda asignada independiente y diferente de la de las demás. La cantidad de datos que conducirá cada portadora es proporcional al la relación Señal/Ruido, en cada una de las bandas de las portadoras, cuanto mayor sea este valor mayor cantidad de datos transportaran, puesto que el motivo por que este valor sea elevado viene de que la cantidad de Ruido en esa zona en bajo, con lo cual los datos transmitidos por esa zona tendrán menor probabilidad de llegar corruptos a su destino. Esta estimación se calcula en el momento de establecer la conexión a través de una 'secuencia de entrenamiento'.

La técnica de modulación de ambos módems es idéntica, la diferencia viene en que el MODEM de la central (ATU-C DSLAM) puede disponer de 256 subportadoras, mientras que el del usuario (ATU-R o Equipo Adsl Final) sólo dispone de 32. Lo cual nos demuestra que la velocidad de bajada siempre es superior a la de subida. Más adelante lo comprobaremos viendo los servicios que ofrecen distintas compañías.

Cabe destacar que en un cable formado por pares de hilos de cobre la atenuación de la señal por culpa del cable aumenta con la longitud del mismo, por ello vemos que dependiendo de la distancia del abonado con respecto a su central urbana, la velocidad máxima que ésta es capaz de suministrar al usuario será diferente. Como curiosidad decir que a una distancia de 2 Km. de la central, la velocidad máxima que puede tener el usuario es de 2 Mbps en sentido de bajada y 0.9 Mbps en sentido de subida.

3.5 DSLAM

(Digital Subscriber Line Access Multiplexer).

Como hemos visto antes, en xDSL para establecer la conexión entre el equipo remoto y la central se requiere de un DSLAM que cumple la función de multiplexar los diferentes accesos xDSL de los usuarios y concentrar el tráfico hacia una WAN.

Gracias a la aparición de esta tecnología el despliegue de los módems en las centrales ha sido mucho más sencillo, lo que ha conseguido que el ADSL se haya extendido tanto.

En la figura siguiente podemos ver la estructura de uno de estos armarios.

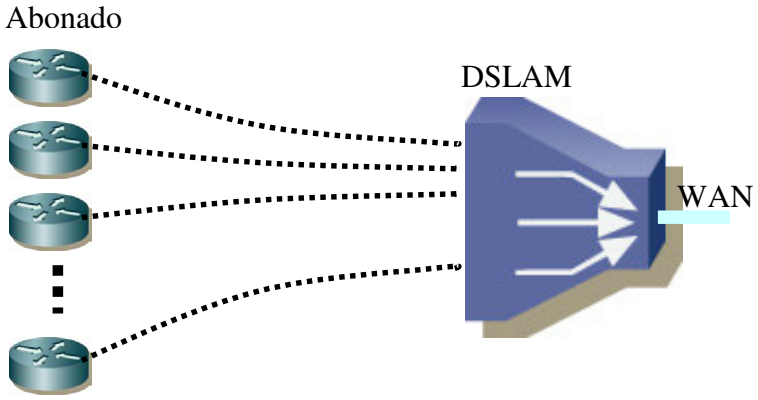


Figura 4: Estructura de un armario DSLAM

3.6 ATM sobre ADSL

Las ventajas del ADSL son el gran ancho de banda en el acceso, dicho ancho de banda se encuentra activo de forma permanente. Pero para obtener el máximo rendimiento que esa tecnología nos proporciona las redes de comunicación de banda ancha utilizan el ATM ('Asychronuos Transfer Mode') para la comunicación. Desde el principio, dado que el ADSL se concibió para el envío de información a gran velocidad, se pensó en el envío de dicha información en celdas ATM sobre los enlaces ADSL.

Esto tiene una sencilla explicación, puesto que si usamos en un enlace ADSL el ATM como protocolo de enlace podemos definir varios canales virtuales permanentes (PVC), cada uno dedicado a un servicio diferente. Esto aumenta la potencia de esta tecnología, pues añade flexibilidad para múltiples servicios a un gran ancho de banda. Finalmente otra ventaja añadida es que en ATM se contemplan diferentes velocidades de transferencia con distintos parámetros para la calidad del servicio, así podemos dar un tratamiento diferente a cada una de estas conexiones, lo que a su vez permite dedicar el circuito mas adecuado por sus parámetros de calidad de servicio a cada tipo de aplicación, ya sea voz, video o datos.

3.7 Evolución de la red de acceso

Los nuevos estándares del ADSL han conseguido unas velocidades de transferencia espectaculares, teniendo en cuenta el medio físico por el que circulan. En concreto los módems son capaces de transmitir a 8,192Mbps en sentido descendente y 0,928 Mbps en sentido ascendente.

Con estas cifras el despliegue de esta tecnología supone una autentica revolución en la red de acceso de la operadoras del servicio telefónico dichas líneas pasan de ser de banda estrecha capaces de transmitir voz o datos con módems de bajas velocidades, a ser redes de banda ancha multiservicio.

La red de acceso deja de ser el gran obstáculo que tenían las operadoras para el desarrollo y oferta de nuevos servicios, inimaginables hasta hace pocos años…

3.8 Características de Accesos xDSL:

ADSL	G.SHDSL
Asimétrica	Single-pair High-speed Simétrico
Soporta Pots	No soporta Pots
Hasta 768 Kbps en subida	Hasta 2304 Kbps en subida
Hasta 6000 Kbps en bajada	Hasta 2304 Kbps en bajada
A 3 km: 768 / 1024 Kbps	De 2,5 a 3 km 2304 / 2304 Kbps
Dslam: Alcatel, Adtran Huawei…	Dslam: Alcatel, Adtran, Huawei, Zyxel…

Las velocidades indicadas en la tabla, incluyen la compensación por pérdidas de encabezado ATM (encapsulamiento), por lo tanto, la sensación de velocidad percibida por el usuario es levemente menor.

3.9 Configuración básica de Router xDSL.

Se muestra en la figura la implementación de un acceso xDSL genérico

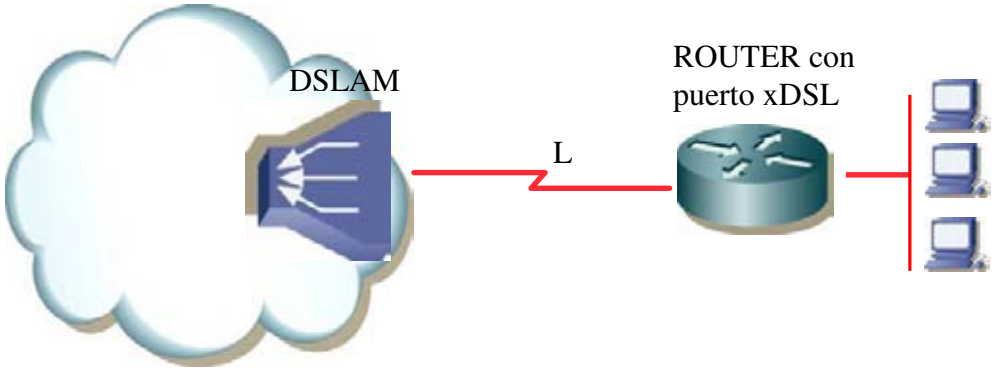


Figura 5: Diagrama Acceso xDSL

A continuación se indican la configuración básica del Router xDSL para establecer conexión con el Dslam. Se reitera que el equipamiento a utilizar en las diferentes descripciones corresponden a Router Cisco.

3.10 Configuración de Router ADSL

Dentro de la interface nativa, el comando mas importante es el que indica la velocidad , en este caso la interface esta configurada auto, de manera de adaptarse a la velocidad de la puerta. Hay casos en que la interface nativa debe ser forzada a la velocidad de la puerta.

```
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 dsl operating-mode auto
 dsl power-cutback 0
!
interface ATM0.1 point-to-point
 ip address 10.220.37.30 255.255.255.252
 pvc 8/35
  encapsulation aal5snap
 !
!
```

3.11 Configuración Router G.SHDSL

```
!
interface ATM0/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 dsl equipment-type CPE
 dsl operating-mode GSHDSL symmetric annex B
 dsl linerate 2312
!
interface ATM0/0.1 point-to-point
 ip address 10.220.49.214 255.255.255.252
 pvc 8/35
  encapsulation aal5snap
   !
!
```

3.12 Procedimiento de configuración de QoS para red MPLS en acceso xDSL.

3.12.1 Descripción del servicio

En este tipo de servicio, el acceso corresponde a un acceso del tipo xDSL (ADSL o G.SHDSL). La aplicación está constituido por un router (CE en la notación de MPLS) en dependencias de usuario y que forma parte activa de las funciones a implementar para obtener una diferenciación de servicios en el contexto de QoS. Este router CE está conectado, a través de un acceso directo de tipo ADSL o G.SHDSL (interfaces de aspecto ATM desde el punto de vista del router), a la red MPLS, y a través de ésta se conecta al resto de puntos de su red privada, en lo que se denomina un servicio MPLS-VPN. El resto de los puntos de la red privada de cliente pueden utilizar diferentes medios de acceso para conectarse a la red MPLS.

El router CE realiza la clasificación, marcado y los procesos de encolamiento correspondientes para entregar una separación adecuada de los servicios VoIP, Video Conferencia, Data Gold, y tráfico Best Effort. Se define el CE como administrado por el provedor del servicio, por lo que los criterios de clasificación del tráfico (servicios) del Usuario , expresados en la configuración, son controlados.

La red proporcionará un circuito virtual (PVC) de categoría privilegiada por sobre el resto de los PVC de datos. A los servicios QoS MPLS-VPN se asignan PVC de categoría rt-VBR.

En el siguiente esquema se representa la configuración de este tipo de acceso.

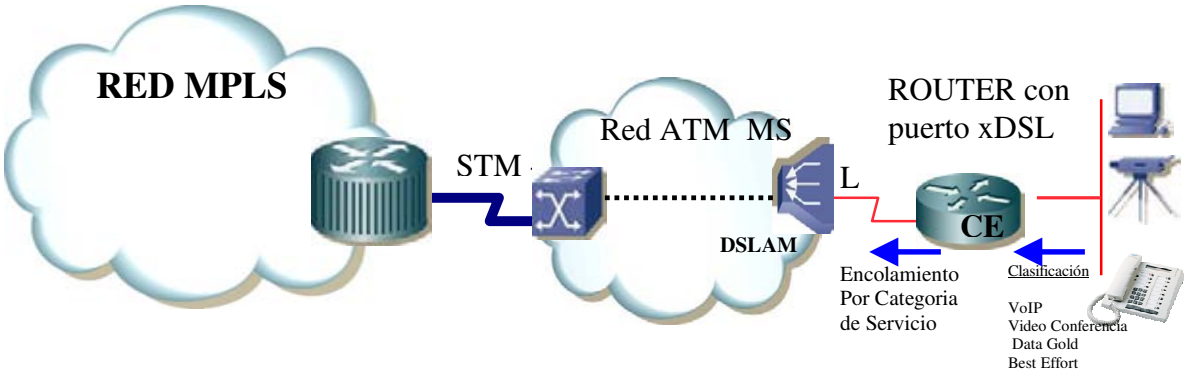


Figura 6: Servicio QoS MPLS-VPN con acceso tipo xDSL.

3.12.2 Criterios de diseño

Restricción de la velocidad de acceso:

Para valores de ancho de banda de la clase de servicio (BWClase) menores a 768[Kbps] la velocidad de acceso (velocidad de línea) debe tener un valor fijo de 768[Kbps] (a criterio del proveedor del servicio).

Servicio	Ancho de Banda de Clase mínimo (Kbps)
Solo Datos	-
Datos + VoIP	192 (sin fragmentación)
Datos + Video Conferencia	**768**
Datos + Video Conferencia + VoIP	**768**

Recordar que debido a la pérdida de capacidad en el momento de encapsulamiento sobre celdas ATM, el ancho de banda de la clase de servicio BWClase (velocidad que el cliente percibe como velocidad del enlace de acceso) es menor que el valor correspondiente a la velocidad de línea en xDSL. De hecho, existe la regla de aumentar en un 25% el ancho de banda del acceso por este motivo:

$$\text{Velocidad de línea xDSL (AR)} = 1{,}25 \in BW_{Clase}$$

Como datos originales, se tiene el número de canales de voz máximo (n) y su codec respectivo utilizado por el servicio VoIP (valores que son utilizados para estimar el ancho de banda que consume el servicio VoIP, BW_{VoIP}), el número de sesiones simultáneas máximas de Video Conferencia y su ancho de banda nominal (BW_{VCnom}), dependiente de la velocidad de la Video Conferencia y su codec. Además se especifica a priori la intensidad de tráfico de datos de la categoría Data Gold (BW_{DG}) que debe priorizarse por sobre el resto de los datos.

Las restricciones que se imponen sobre la asignación de recursos son:

$$BW_{VoIP\ Clase} \leq \tfrac{1}{2}\ BW_{Clase}$$

$$BW_2 \geq 1{,}2 \cdot BW_{VCnom}$$

$$BW_1 + BW_2 + BW_3 = 0.95 \cdot BW_{Clase}$$

donde BW_{Clase} es la velocidad de la Clase de Servicio (velocidad contratada por usuario) y BW_{VoIP} = n€codec. Los valores BW_1, BW_2 y BW_3 son valores de ancho de banda que se utilizarán en la configuración del router CE y no reflejan necesariamente valores reales de ancho de banda utilizados por las categorías de servicios.

3.12.3 Configuración Router CE

Las tareas asignadas al router CE consisten en Clasificación del tráfico de las diferentes categorías de servicios, Marcado de los paquetes IP de los diferentes servicios, Priorización (Scheduling) de los flujos correspondientes a cada categoría, y Modelado del tráfico (Shaping) para el ajuste a la tasa de transmisión digital de la clase de servicio correspondiente.

3.12.3.1 Clasificación del tráfico por categorías de servicio

La clasificación del tráfico se realizará utilizando el campo IP Precedence de la cabecera del paquete IP. Cada categoría de servicio tendrá un valor diferente y sus valores específicos corresponden a:

Categoría de Servicio	**Acrónimo**	**Acrónimo Valor de IP Precedence**
Tráfico de Voz sobre IP	VoIP	5
Tráfico de Video Conferencia	VideoC	3
Aplicaciones Críticas del Negocio	DATA-GOLD	2
Resto del Tráfico de Datos	BE	0

El objetivo final de la clasificación consiste en encauzar los flujos reales de cada servicio entregado al usuario (VoIP, Video Conferencia, etc.) en los canales que a lo largo de toda la red están especialmente acondicionados para ello. Es importante que esta clasificación sea rigurosa para impedir, por ejemplo, la suplantación de tráfico priorizado por tráfico no relevante por parte del usuario.

3.12.3.2 Configuración de los criterios de clasificación (listas de acceso)

La clasificación se realiza utilizando criterios de identificación de los servicios mediante las listas de acceso correspondientes. Cada servicio puede ser caracterizado por una lista de acceso más específica que las mostradas a continuación y su definición específica debe ser tema a abordar en el proceso de instalación del servicio en particular.

Ejemplo de criterios de clasificación

```
!
ip access-list extended VideoC
remark Regla que incluya el stream de Video
permit udp host 10.10.10.155 any range 3230 3235
```

```
!
ip access-list extended VideoC-Control
remark Regla que incluya la comunicacion de control de la VC
permit tcp host 10.10.10.155 any range 3230 3231
!
ip access-list extended VoIP
remark Regla que incluya el trafico de Voz
permit udp 10.10.10.0 0.0.0.15 any range 16384 32767
!
ip access-list extended VoIP-Control
remark Regla que incluya la comunicacion de control de Voz
permit tcp 10.10.10.0 0.0.0.15 any eq 1720
!
ip access-list extended data-gold
remark Lista de Acceso que identifica las conexiones DLSw
permit tcp any any eq 2065
permit tcp any any eq 2067
permit tcp any eq 2065 any
permit tcp any eq 2067 any
!
!
```

NOTA: los criterios expuestos en las listas de acceso mostradas más arriba, son criterios de calce genéricos y deben ser afinados con más detalle a la hora de la habilitación de un servicio.

3.12.3.3 Creación de las clases para las diferentes categorías de servicio

Las clases que clasifican el tráfico se configuran de la siguiente forma.

```
!
class-map match-all VideoC
match access-group name VideoC
!
class-map match-all VoIP
match access-group name VoIP
!
class-map match-all DATA-GOLD
match access-group name data-gold
!
class-map match-all VoIP-Control
match access-group name VoIP-Control
!
class-map match-all VideoC-Control
match access-group name VideoC-Control
!
```

3.12.4 Marcado de los paquetes por categoría de servicio

El marcado de los paquetes se realiza utilizando las clases definidas anteriormente y se aplica de entrada en todas las interfaces que miran hacia la LAN del cliente y reciben el tráfico que va a ser cursado hacia la WAN.

3.12.4.1 Creación del policy-map CLASIFICACION

Esta configuración realiza el marcado de los paquetes

Ejemplo:

```
!
policy-map CLASIFICACION
description Clasificacion y Marcado de paquetes según servicio
class VoIP
set ip precedence 5
class VideoC
set ip precedence 3
class DATA-GOLD
set ip precedence 2
class VoIP-Control
set ip precedence 2
class VideoC-Control
set ip precedence 2
class class-default
set ip precedence 0
!
!
```

3.12.4.2 Aplicación del policy-map a la interfaz

El marcado de los paquetes se debe aplicar de entrada en todas las interfaces que miran hacia la LAN del cliente.

Ejemplo:

```
!
interface FastEthernet0
ip address 192.168.105.199 255.255.255.0
service-policy input CLASIFICACION
!
```

3.12.5 Caso especial: Marcado de paquetes de voz en el caso de un Voice Gateway

Si el router CE es un Voice Gateway, vale decir, el router tiene conectadas interfaces de voz (FXO,FXS, E&M, E1) el marcado de paquetes debe realizarse directamente en los "dial-peer voice" del tipo VoIP correspondientes.

Por ejemplo:

```
dial-peer voice 3 voip
destination-pattern 15..
session target ipv4:172.16.65.182
ip precedence 5
```

Algunas versiones de sistema operativo no permiten la configuración anterior, y en ese caso la configuración alternativa será:

```
dial-peer voice 3 voip
destination-pattern 15..
session target ipv4:172.16.65.182
ip qos dscp cs5 media
```

A través de ambas configuraciones, los paquetes correspondientes a VoIP ya van marcados con Precedence 5, por lo que pueden ser clasificados en la clase VoIP en el policy-map de salida.

3.12.6 Modelado del tráfico (Traffic Shaping)

En este caso, no se aplica explícitamente comandos de traffic shaping, pero cada sub-interfaz ATM de los routers con acceso xDSL controla directamente el flujo máximo de paquetes, o celdas para ser más específico, mediante la definición de las características de tráfico del circuito virtual (PVC) (contrato de tráfico).
Los parámetros de tráfico a configurar en la definición del PVC son:

$$\text{Peak Cell Rate (PCR)} = 1{,}25 \text{ €} BW_{Clase}\,[\text{Kbps}]$$
$$\text{Average Cell Rate} = 1{,}25\text{€ } BW_{Clase}\,[\text{Kbps}]$$

donde BW_{Clase} es el valor de la velocidad contratada por cliente.

3.12.6.1 Configuración de los parámetros del Shaping

En la sub-interfaz ATM correspondiente, en la definición del PVC, se aplica la 'velocidad' de éste y que debe coincidir con la velocidad del acceso.

```
!
interface ATM0.10 point-to-point
pvc 0/99
vbr-rt 240 240 32
tx-ring-limit 3
!
```

El comando, 'tx-ring-limit 3' es obligatorio cuando se utiliza este tipo de QoS. Su efecto es el de disminuir el tiempo de encendido de los mecanismos de encolamiento y priorización.

3.12.7 Priorización del tráfico por categoría de servicio

La priorización propiamente tal se realiza en la sub-interfaz ATM. Esta priorización queda definida en el policy-map de nombre 'HACIA_RED' y se aplica directamente en la sub-interfaz ATM.

Para el cálculo de los parámetros a configurar en el sistema de priorización se da por conocidos, aportados por el diseño previo, el valor de la intensidad de tráfico de las "aplicaciones críticas del negocio" (BW_{DG}), del número máximo de canales de voz simultáneos (n) y del codec utilizado, del número máximo de sesiones de Video Conferencia y de su codec (velocidad nominal) (BW_{VCnom}).

3.12.7.1 Configuración del máximo porcentaje reservable de ancho de banda

Los equipos router pueden asignar a las diferentes categorías de servicio un cierto porcentaje de la tasa de acceso, cuyo valor por omisión es un 75%. Este valor se modifica con el comando de interfaz 'max-reserved-bandwidth XX', donde XX es el porcentaje máximo del 'bandwidth' de la interfaz a asignar con las clases. Este comando es obligatorio y se aplica directamente en la interfaz de salida.

Ejemplo:

```
!
interface ATM0.10 point-to-point
ip address 10.10.10.1 255.255.255.0
pvc 0/100
max-reserved-bandwidth 95
!
```

3.12.7.2 Creación de las clases por precedencia

La clasificación previa al encolamiento se realiza mediante la definición de las siguientes clases (configuración obligatoria)

```
!
class-map match-all Prec-3
match ip precedence 3
!
class-map match-all Prec-2
match ip precedence 2
!
class-map match-all Prec-5
match ip precedence 5
!
```

3.12.7.3.- Creación del policy-map de salida: configuración de la categoría VoIP (Precedence 5)

```
policy-map HACIA_RED
description Esquema de priorizacion por tipo de IP Precedence
class Prec-5
priority BW1
!
```

Para la clase Prec-5 (correspondiente a VoIP) se destina tanto ancho de banda como canales de voz simultáneos vayan a ser servidos. Como referencia, se estima un consumo de 45[Kbps] por canal de voz al utilizar el codec G.729. El valor $BW_1 = n€45$ se configura en la línea

```
priority 90 (BW1 = 90[Kbps])
```

3.12.7.4 Creación del policy-map de salida: configuración de la categoría VideoC (Precedence 3)

En el mismo policy-map se configura la clase para el tratamiento del tráfico con precedencia 3 (categoría VideoC). Al interior de esta clase se debe especificar dos parámetros de forma obligatoria: “bandwidth” y “police”

```
!
policy-map HACIA_RED
description Esquema de priorizacion por tipo de IP Precedence
class Prec-3
bandwidth BW2
police BW2-max
!
```

Para la clase Prec-3, que define el tratamiento para el tráfico de Video Conferencia, se asigna una ponderación alta para que pueda ser priorizado adecuadamente sobre el tráfico de datos. El valor para el parámetro ‘bandwidth’ corresponde al máximo valor de ancho de banda disponible, cuyo valor viene dado por:

$$BW_2 = 0.95 \cdot 1{,}25 \cdot BW_{Clase} - BW_1 - BW_3$$

donde el valor de BW_3 es determinado en la siguiente sección.

El valor para $BW_{2\text{-}max}$, que corresponde al máximo tráfico alcanzado por la sesión de video Conferencia, se calcula como:

$$BW_{2\text{-}max} = 1{,}3 \in BW_{VCnom}$$

Es decir, se recortará el tráfico, por razones de evitar sobreventa del servicio, un 30% por sobre el valor nominal utilizado por la Video Conferencia. Por ejemplo, una Video Conferencia correspondiente a BW_{VCnom} = 384[Kbps], el valor para $BW_{2\text{-}max}$ resulta ser de 500[Kbps].

3.12.7.5 Creación del policy-map de salida: configuración de la categoría DATA_GOLD (Precedence 2)

En el mismo policy-map se configura la clase para el tratamiento del tráfico con precedencia 2 correspondiente al tráfico de categoría Data-Gold. Al interior de esta clase se debe especificar el parámetro "bandwidth", respetando las restricciones.

```
!
policy-map HACIA_RED
description Esquema de priorizacion por tipo de IP Precedence
class Prec-2
bandwidth BW3
set atm-clp
!
```

donde

$$BW_3 = 1{,}25 \in BW_{DG}$$

Este tráfico será marcado como descartable por la red ATM, por lo que se enciende el bit CLP de las celdas ATM correspondientes a esta clase.
Considerar que el valor del comando 'bandwidth' funciona como un ponderador y no corresponde al valor real del tráfico de la Video Conferencia.

3.12.7.6 Creación del policy-map de salida: configuración de la categoría BE (Precedence 0)

Finalmente, en el mismo policy-map se configura la clase por defecto, clase que encausará todo el tráfico que no ha calzado en las clases anteriores. Utilizará todo el ancho de banda restante. Este tipo de tráfico también será descartable por la red ATM. Su configuración corresponde a:

```
!
policy-map HACIA_RED
class class-default
```

```
fair-queue
set atm-clp
!
```

3.12.7.7 Aplicación del policy-map "HACIA_RED" a la Interfaz de salida hacia la red MPLS

```
!
interface ATM0.10 point-to-point
pvc 0/100
service-policy output HACIA_RED
!
```

3.12.8 Ejemplo de la configuración del router CE

En el siguiente ejemplo se considera una clase de servicio de 768[Kbps], dos canales de voz codificadas con G.729, una sesión de Video Conferencia de 384[Kbps] y un tráfico de aplicaciones críticas de 64[Kbps][10].

Como comentario relativo a los accesos xDSL, siempre se debe sobre dimensionar la velocidad de línea (acceso) en un 25% por sobre el valor de la velocidad contratada. Esto debido a pérdidas producidas por el llenado de celda en el encapsulamiento RFC 2684 (ex RFC-1483), que se manifiesta en que no siempre calza de manera exacta un paquete, IP en este caso, en un número entero de celdas, por lo que la mayoría de las veces hay celdas viajan a medio llenar por la línea xDSL.

La configuración más relevante del router CE se muestra a continuación.

```
!
class-map match-all VideoC
match access-group name VideoC
!
class-map match-all VoIP
match access-group name VoIP
!
class-map match-all Prec-3
match ip precedence 3
!
class-map match-all Prec-2
match ip precedence 2
!
class-map match-all Prec-5
match ip precedence 5
!
class-map match-all DATA-GOLD
match access-group name data-gold
!
class-map match-all VoIP-Control
match access-group name VoIP-Control
!
class-map match-all VideoC-Control
match access-group name VideoC-Control
!
!
policy-map HACIA_RED
description Esquema de priorización por tipo de IP Precedence
```

```
class Prec-5
priority 90
class Prec-3
bandwidth 742
police 500000
class Prec-2
bandwidth 80
set atm-clp
class class-default
fair-queue
set atm-clp
!
policy-map Clasifica
description Clasificacion y Marcado de paquetes segun servicio
class VoIP
set ip precedence 5
class VideoC
set ip precedence 3
class DATA-GOLD
set ip precedence 2
class VoIP-Control
set ip precedence 2
class VideoC-Control
set ip precedence 2
class class-default
set ip precedence 0
!
interface ATM0
no ip address
no atm ilmi-keepalive
dsl equipment-type CPE
dsl operating-mode GSHDSL symmetric annex A
!
interface ATM0.10 point-to-point
ip address 10.10.10.1 255.255.255.0
pvc 0/100
protocol ip 10.10.10.2 broadcast
vbr-rt 960 960 32
encapsulation aal5snap
max-reserved-bandwidth 95
service-policy output HACIA_RED
!
!
!
interface FastEthernet0
ip address 192.168.105.199 255.255.255.0
service-policy input Clasifica
!
!
ip access-list extended VideoC
remark Regla que incluya el stream de Video
permit udp host 10.10.10.155 any range 3230 3235
!
ip access-list extended VideoC-Control
remark Regla que incluya la comunicacion de control de la VC
permit tcp host 10.10.10.155 any range 3230 3231
!
ip access-list extended VoIP
remark Regla que incluya el trafico de Voz
permit udp 10.10.10.0 0.0.0.15 any range 16384 32767
!
ip access-list extended VoIP-Control
remark Regla que incluya la comunicacion de control de Voz
permit tcp 10.10.10.0 0.0.0.15 any eq 1720
!
ip access-list extended data-gold
remark Lista de Acceso que identifica las conexiones DLSw
permit tcp any any eq 2065
permit tcp any any eq 2067
permit tcp any eq 2065 any
permit tcp any eq 2067 any
!
```

```
!
end
```

3.12.9 Configuración Red ATM

La configuración del servicio se realiza de forma similar como la que aplica a los servicios xDSL tradicionales, excepto que el PVC se define de categoría rt-VBR y se deshabilita "Traffic Policing" en la puerta de entrada a la red.

El valor de ancho de banda del PVC debe ser 1,25 €BW_{Clase}.
Se recalca el hecho de NO habilitar el "Traffic Policing" debido a que el marcado de celdas está en manos del router CE y no en la red MS.

3.12.10 Configuración DSLAM

La configuración del PVC en el DSLAM corresponde a la misma configuración aplicada a los servicios xDSL enrutados, excepto en que aquí se utiliza un PVC de categoría Real Time VBR en vez de un PVC de categoría UBR+.

El valor de ancho de banda del PVC debe ser 1,25 €BW_{Clase}.
El valor de la velocidad de línea (dada en Kbps de celdas ATM) debe ser igual a 768[Kbps] para valores de BW_{Clase} menores a 768[Kbps], y debe ser igual a 1,25€BW_{Clase} para valores de BW_{Clase} mayores o iguales a 768[Kbps].

Capitulo IV

4. QoS Sobre accesos Frame-Relay

4.1 Frame Relay

4.1.1 Introducción:

Frame Relay comenzó como un movimiento a partir del mismo grupo de normalización que dio lugar a X.25 y RDSI: El ITU (entonces CCITT). Sus especificaciones fueron definidas por ANSI, fundamentalmente como medida para superar la lentitud de X.25, eliminando la función de los conmutadores, en cada "salto" de la red. X.25 tiene el grave inconveniente de su importante "overhead" producido por los mecanismos de control de errores y de flujo.

Hasta hace relativamente poco tiempo, X.25 se ha venido utilizando como medio de comunicación para datos a través de redes telefónicas con infraestructuras analógicas, en las que la norma ha sido la baja calidad de los medios de transmisión, con una alta tasa de errores. Esto justificaba los abundantes controles de errores y sus redundantes mecanismos para el control de flujo, junto al pequeño tamaño de los paquetes. En resumen, se trataba de facilitar las retransmisiones para obtener una comunicación segura.

Frame Relay, por el contrario, maximiza la eficacia, aprovechándose para ello de las modernas infraestructuras, de mucha mayor calidad y con muy bajos índices de error, y además permite mayores flujos de información.

Frame Relay se define, oficialmente, como un servicio portador RDSI de banda estrecha en modo de paquetes, y ha sido especialmente adaptado para velocidades de hasta 2,048 Mbps., aunque nada le impide superarlas.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto. De hecho, su

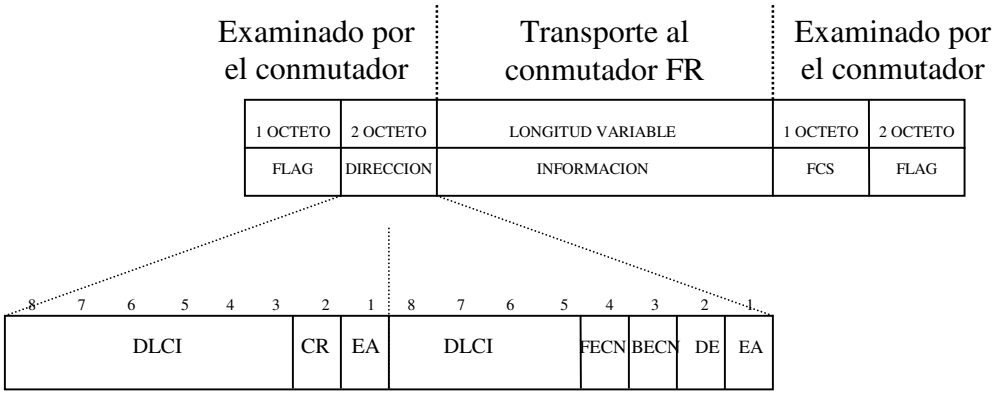
gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red. El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben de llegar ordenadas al destinatario, ya que todas siguen el mismo camino a través de la red.

4.1.2 Tecnología:

Las redes Frame Relay se construyen partiendo de un equipamiento de usuario que se encarga de empaquetar todas las tramas de los protocolos existentes en una única trama Frame Relay. También incorporan los nodos que conmutan las tramas Frame Relay en función del identificador de conexión, a través de la ruta establecida para la conexión en la red. Este equipo se denomina FRAD o "Ensamblador/Desensamblador Frame Relay" (Frame Relay Assembler / Disassembler) y el nodo de red se denomina FRND o "Dispositivo de Red Frame Relay" (Frame Relay Network Device).

La información transmitida en una trama Frame Relay puede oscilar entre 1 y 8.250 bytes, aunque por defecto es de 1.600 bytes.

Figura 7:Trama Frame Relay



DLCI: Identificador de conexión de enlace de datos

EA: Dirección Extendida

CR: Instrucción/respuesta

FECN: Notificación de congestión explicita de envío.

BECN: Notificación de congestión explicita de reenvío

Lo más increíble de todo, es que, a pesar del gran número de formas y tamaños Frame Relay funciona perfectamente, y ha demostrado un muy alto grado de interoperatibilidad entre diferentes fabricantes de equipos y redes. Ello es debido a que, sean las que sean las opciones empleadas por una determinada implementación de red o equipamiento, siempre existe la posibilidad de "convertir" los formatos de Frame Relay a uno común, intercambiando así las tramas en dicho formato.

Las redes Frame Relay son orientadas a conexión, como X.25, SNA e incluso ATM. El identificador de conexión es la sucesión de dos campos HDLC (High-level Data Link Control), en cuyas especificaciones originales de unidad de datos (protocolo de la capa 2), se basa Frame Relay. Entre los dos campos HDLC que forman el "identificador de conexión de enlace de datos" o DLCI (Data Link Connection Identifier) se insertan algunos bits de control (CR y EA).

A continuación se añaden otros campos que tienen funciones muy especiales en las redes Frame Relay. Ello se debe a que los nodos conmutadores Frame Relay carecen de una estructura de paquetes en la capa 3, que por lo general es empleada para implementar funciones como el control de flujo y de la congestión de la red, y que estas funciones son imprescindibles para el adecuado funcionamiento de cualquier red.

Los tres más esenciales son DE o "elegible para ser rechazada" (Discard Eligibility), FECN o "notificación de congestión explícita de envío" (Forward Explicit Congestion Notification), y BECN o "notificación de congestión explícita de reenvío" (Backward Explicit Congestion Notification). El bit DE es usado para identificar tramas que pueden ser rechazadas en la red en caso de congestión. FECN es usado con protocolos de sistema final que controlan el flujo de datos entre en emisor y el receptor, como el mecanismo "windowing" de TCP/IP; en teoría, el receptor puede ajustar su tamaño de "ventana" en respuesta a las tramas que llegan con el bit FECN activado. BECN, como es lógico, puede ser usado con protocolos que controlan el flujo de los datos extremo a extremo en el propio emisor.

Según esto, la red es capaz de detectar errores, pero no de corregirlos (en algunos casos podría llegar tan solo a eliminar tramas).

No se ha normalizado la implementación de las acciones de los nodos de la red ni del emisor/receptor, para generar y/o interpretar estos tres bits. Por ejemplo, TCP/IP no tiene ningún mecanismo que le permita ser alertado de que la red Frame Relay esta generando bits FECN ni de como actuar para responder a dicha situación. Las acciones y funcionamiento de las redes empleando estos bits son temas de altísimo interés y actividad en el "Frame Relay Forum" (equivalente en su misión y composición al "ATM Forum").

Frame Relay también ha sido denominado "tecnología de paquetes rápidos" (fast packet technology) o "X.25 para los 90´", y esto es cierto en gran medida.

El protocolo X.25 opera en la capa 3 e inferiores del modelo OSI, y mediante la conmutación de paquetes, a través de una red de conmutadores, entre identificadores de conexión. En cada salto de la red X.25 se verifica la integridad de los paquetes y cada conmutador proporciona una función de control de flujo. La función de control de flujo impide que un conmutador X.25 no envíe paquetes a mayor velocidad de la que el receptor de los mismos sea capaz de procesarlos. Para ello, el conmutador X.25 receptor no envía inmediatamente la señal de reconocimiento de los datos remitidos, con lo que el emisor de los mismos no envía más que un determinado número de paquetes a la red en un momento dado.

Frame Relay realiza la misma función, pero partiendo de la capa 2 e inferiores. Para ello, descarta todas las funciones de la capa 3 que realizaría un conmutador de paquetes X.25, y las combina con las funciones de trama. La trama contiene así al identificador de conexión, y es transmitida a través de los nodos de la red en lugar de realizar una "conmutación de paquetes".

Lógicamente, todo el control de errores en el contenido de la trama, y el control de flujo, debe de ser realizado en los extremos de la comunicación (nodo origen y nodo destino). La conmutación de paquetes en X.25, un proceso de 10 pasos, se convierte en uno de 2 pasos, a través de la transmisión de tramas...

4.1.3 Un caso práctico:

Si el usuario "A" desea una comunicación con el usuario "B", primero establecerá un Circuito Virtual (VC o Virtual Circuit), que los una. La información a ser enviada se segmenta en tramas a las que se añade el DLCI.

Una vez que las tramas son entregadas a la red, son conmutadas según unas tablas de enrutamiento que se encargan de asociar cada DLCI de entrada a un puerto de salida y un nuevo DLCI.

4.1.4 Parámetros

A la hora de contratar un enlace Frame Relay, hay que tener en cuenta varios parámetros. Por supuesto, el primero de ellos es la velocidad máxima del acceso (Vt), que dependerá de la calidad o tipo de línea empleada.

Pero hay un parámetro más importante: se trata del CIR (velocidad media de transmisión o Committed Information Rate). Es la velocidad que la red se compromete a servir como mínimo. Se contrata un CIR para cada PVC o bien se negocia dinámicamente en el caso de SVC's.

El Committed Burst Size (Bc) es el volumen de tráfico alcanzable transmitiendo a la velocidad media (CIR).

Por último la ráfaga máxima o Excess Burst Size (Be) es el volumen de tráfico adicional sobre el volumen alcanzable.

Para el control de todos estos parámetros se fija un intervalo de referencia (tc). Así, cuando el usuario transmite tramas, dentro del intervalo tc, a la velocidad máxima (Vt), el volumen de tráfico se acumula y la red lo acepta siempre que este por debajo de Bc. Pero si se continúa transmitiendo hasta superar Bc, las tramas empezarán a ser marcadas mediante el bit DE (serán consideradas como desechables).

Por ello, si se continúa transmitiendo superando el nivel marcado por Bc+Be, la red no admitirá ninguna trama más.

4.1.5 Configuración Básica de Un Router Cisco con Acceso Frame Relay

A continuación de indica una configuración genérica de un Router cisco con una conexión wan por acceso Frame Relay.

```
interface FastEthernet0
 ip address 192.168.105.199 255.255.255.0
 service-policy input Clasifica
!
interface Serial0
 no ip address
 encapsulation frame-relay
!
interface Serial0.1  point-to-point
 ip address "Direccion Ip y mask Asignada a esta interface del Router"
 frame-relay interface-dlci 602
```

A continuación se empieza a describir la configuración necesaria para la implementación de QoS sobre un Router instalado en un extremo que se interconecta al red MPLS mediante un acceso Frame Relay.

4.2.- QoS en Accesos Frame Relay para Redes MPLS

4.2.1.- Descripción del servicio

En este tipo de servicio, el acceso corresponde a un acceso del tipo Frame Relay a través de una red troncal de multiservicios. La implementación del circuito esta constituido por un router en dependencias de usuaro final (CE en la notación deMPLS) y que forma parte activa de las funciones a implementar para obtener una diferenciación de servicios en el contexto de QoS. Este router CE está conectado a la red MPLS a través de un acceso tipo Frame Relay, y a través de aquella se conecta al resto de puntos de su red privada, en lo que se denomina un servicio MPLS-VPN. El resto de los puntos de la red privada de cliente pueden utilizar diferentes medios de acceso para conectarse a la red MPLS.

La actividad más importante que el router CE realiza es la clasificación, marcado y los procesos de encolamiento correspondientes para entregar una separación adecuada de

los servicios VoIP, Video Conferencia, Data Gold, y tráfico Best Effort. Este router se define como administrado por la empresa proveedora del servicio, por lo que los criterios de clasificación del tráfico (servicios) del usuario, expresados en la configuración, son totalmente controlados.

La red MS (acceso Frame Relay en un extremo y ATM en el otro) proporciona un circuito virtual (PVC) de categoría privilegiada por sobre el resto de los PVC de datos. A los servicios QoS MPLSVPN se asignan PVC de categoría Low Delay/rt-VBR.

En el siguiente esquema, se representa la configuración de este tipo de acceso.

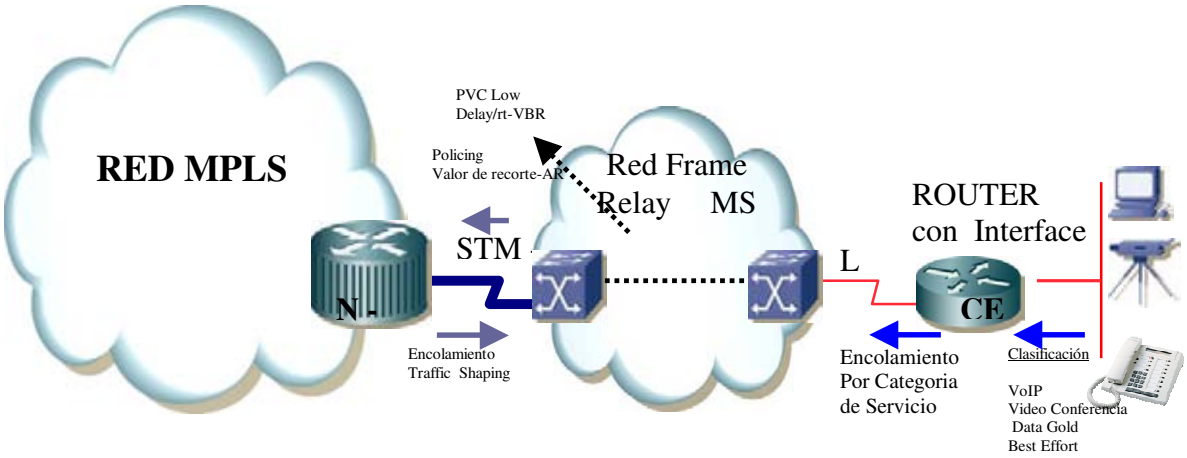


Figura 8: Topología Servicio QoS Mpls VPN con acceso Frame Relay

4.2.2.- Criterios de diseño

Restricción de la velocidad de acceso (AR) Frame Relay:

Servicio	Velocidad de acceso Mínima [Kbps]
Solo Datos	-
Datos + VoIP	384 (sin fragmentación)
Datos + Video Conferencia	768
Datos + Video Conferencia + VoIP	768

Como datos originales, provenientes del diseño a implementar, se tiene el número de canales de voz máximo (n) y su codec respectivo utilizado por el servicio VoIP (valores

que son utilizados para estimar el ancho de banda que consume el servicio VoIP, BW_{VoIP}), el número de sesiones simultáneas máximas de Video Conferencia y su ancho de banda nominal (BW_{VCnom}), dependiente de la velocidad de la Video Conferencia y su codec. Además se especifica a priori la intensidad de tráfico de datos de la categoría Data Gold (BW_{DG}) que debe priorizarse por sobre el resto de los datos.

Las restricciones que se imponen sobre la asignación de recursos son

$$BW_{VoIP} \leq \frac{1}{2} BW_{Clase}$$

$$BW_2 \geq 1{,}2 \cdot BW_{VCnom}$$

$$BW_1 + BW_2 + BW_3 = 0.95 \cdot BW_{Clase}$$

donde BW_{Clase} es la velocidad de la Clase de Servicio (que en este caso corresponde exactamente a la velocidad del acceso AR de Frame Relay) y BW_{VoIP} = n€codec. Los valores BW_1, BW_2 y BW_3 son valores de ancho de banda que se utilizarán en la configuración del router CE y no reflejan necesariamente valores reales de ancho de banda utilizados por las categorías de servicios.

4.2.3.- Configuración Router CE

Las tareas asignadas al router consisten en Clasificación del tráfico de las diferentes categorías de servicios, Marcado de los paquetes IP de los diferentes servicios, Priorización (Scheduling) de los flujos correspondientes a cada categoría, y Modelado del tráfico (Shaping) para el ajuste a la tasa de transmisión digital de la clase de servicio correspondiente.

4.2.3.1.- Clasificación del tráfico por categorías de servicio

La clasificación del tráfico se realizará utilizando el campo IP Precedence de la cabecera del paquete IP. Cada categoría de servicio tendrá un valor diferente y sus valores específicos corresponden a

Categoría de Servicio	Acrónimo	Valor de IP Precedence
Tráfico de Voz sobre IP	VoIP	5

Tráfico de Video Conferencia	VideoC	3
Aplicaciones Críticas del Negocio	DATA-GOLD	2
Resto del Tráfico de Datos	BE	0

El objetivo final de la clasificación consiste en encauzar los flujos reales de cada servicio entregado a cliente (VoIP, Video Conferencia, etc.) en los canales que a lo largo de toda la red están especialmente acondicionados para ello. Es importante que esta clasificación sea rigurosa para impedir, por ejemplo, la suplantación de tráfico priorizado con tráfico no relevante por parte del usuario.

4.2.3.1.1.- Configuración de los criterios de clasificación (listas de acceso)

La clasificación se realiza utilizando criterios de identificación de los servicios mediante las listas de acceso correspondientes. Cada servicio puede ser caracterizado por una lista de acceso más específica que las mostradas a continuación y su definición específica debe ser tema a abordar en el proceso de instalación del servicio en particular.

Ejemplo de criterios de clasificación

```
!
ip access-list extended VideoC
remark Regla que incluya el stream de Video
permit udp host 10.10.10.155 any range 3230 3235
!
ip access-list extended VideoC-Control
remark Regla que incluya la comunicacion de control de la VC
permit tcp host 10.10.10.155 any range 3230 3231
!
ip access-list extended VoIP
remark Regla que incluya el trafico de Voz
permit udp 10.10.10.0 0.0.0.15 any range 16384 32767
!
ip access-list extended VoIP-Control
remark Regla que incluya la comunicacion de control de Voz
permit tcp 10.10.10.0 0.0.0.15 any eq 1720
!
ip access-list extended data-gold
remark Lista de Acceso que identifica a las conexiones DLSw como DG
permit tcp any any eq 2065
permit tcp any any eq 2067
permit tcp any eq 2065 any
permit tcp any eq 2067 any
!
!
!
```

NOTA: los criterios expuestos en las listas de acceso mostradas más arriba, son criterios de calce genéricos y deberán ser afinados con más detalle en la habilitación del servicio.

4.2.3.1.2.- Creación de las clases para las diferentes categorías de servicio

Las clases que clasifican el tráfico se configuran de la siguiente forma.

```
!
class-map match-all VideoC
match access-group name VideoC
!
class-map match-all VoIP
match access-group name VoIP
!
class-map match-all DATA-GOLD
match access-group name data-gold
!
class-map match-all VoIP-Control
match access-group name VoIP-Control
!
class-map match-all VideoC-Control
match access-group name VideoC-Control
!
!
!
```

4.2.3.2.- Marcado de los paquetes por categoría de servicio

El marcado de los paquetes se realiza utilizando las clases definidas anteriormente y se aplica de entrada en todas las interfaces que miran hacia la LAN del cliente y reciben el tráfico que va a ser cursado hacia la WAN.

4.2.3.2.1.- Creación del policy-map CLASIFICACION

Esta configuración realiza el marcado de los paquetes

Ejemplo:

```
!
policy-map CLASIFICACION
description Clasificacion y Marcado de paquetes segun servicio
class VoIP
set ip precedence 5
class VideoC
set ip precedence 3
class DATA-GOLD
set ip precedence 2
class VoIP-Control
set ip precedence 2
class VideoC-Control
set ip precedence 2
class class-default
set ip precedence 0
!
!
```

4.2.3.2.2.- Aplicación del policy-map a la interfaz

El marcado de los paquetes se debe aplicar de entrada en todas las interfaces que miran hacia la LAN del cliente.

Ejemplo:

```
!
interface FastEthernet0
ip address 192.168.105.199 255.255.255.0
service-policy input CLASIFICACION
!
```

4.2.3.3.- Caso especial: Marcado de paquetes de voz en el caso de un Voice Gateway

Si el router CE es un Voice Gateway, vale decir, el router tiene conectadas interfaces de voz (FXO, FXS, E&M, E1) el marcado de paquetes debe realizarse directamente en los "dial-peer voice" del tipo VoIP correspondientes.

Por ejemplo:

```
dial-peer voice 3 voip
destination-pattern 15..
session target ipv4:172.16.65.182
ip precedence 5
!
```

Algunas versiones de sistema operativo no permiten la configuración anterior, y en ese caso la configuración alternativa será:

```
dial-peer voice 3 voip
destination-pattern 15..
session target ipv4:172.16.65.182
ip qos dscp cs5 media
```

A través de ambas configuraciones, los paquetes correspondientes a VoIP van marcados con Precedence 5, por lo que pueden ser clasificados en la clase VoIP en el policy-map de salida.

4.2.3.4.- Modelado del tráfico (Traffic Shaping)

Para la correcta aplicación del sistema de encolamiento y priorización Class Based Weigthed Fair Queuing (CBWFQ) aquí expuesto, es necesario habilitar traffic-shaping en la sub-interfaz Frame Relay de salida. Esencialmente la configuración del shaping no "recortará" tráfico, sino que es configurado sólo para salvar lo anterior.

Los parámetros de Traffic Shaping a configurar deben ser:

cir = AR
bc = cir/100
be = 0
mincir = AR

donde AR es el valor de la velocidad digital del acceso utilizado (velocidad de la interfaz serial que encapsula Frame Relay). AR Parámetro de configuración obligatoria. Define

el ancho de banda disponible para destinar al encolamiento LLQ y CBFWQ. El ancho de banda que se destina con los comandos 'priority' y 'bandwidth' se va descontando del valor de mincir.

4.2.3.4.1.- Configuración de los parámetros del Shaping

Se define un map-class para Frame Relay que luego será aplicado en la sub-interfaz correspondiente.

```
!
map-class frame-relay CFR
frame-relay cir 1984000
frame-relay bc 19840
frame-relay be 0
frame-relay mincir 1984000
!
```

4.2.3.4.2.- Aplicación de Traffic Shaping

Se habilita el modelamiento de tráfico en la interfaz nativa Frame Relay y luego se aplica el mapclass.

Ejemplo:

```
!
interface Serial0
no ip address
encapsulation frame-relay
frame-relay traffic-shaping
!
interface Serial0.62 point-to-point
ip address 26.0.0.6 255.0.0.0
frame-relay interface-dlci 602
class CFR
!
```

4.2.3.5.- Priorización del tráfico por categoría de servicio

La priorización propiamente tal se realiza en la sub-interfaz serial. Esta priorización queda definida en el policy-map de nombre 'HACIA_RED' y se aplica en la definición de Traffic Shaping de la subinterfaz. Es obligatorio aplicar traffic shaping de Frame Relay para así poder utlilizar las funcionalidades MQC.

Para el cálculo de los parámetros a configurar en el sistema de priorización se dan por conocidos, aportados por el diseño previo, el valor de la intensidad de tráfico de las "aplicaciones críticas del negocio" (BW_{DG}), del número máximo de canales de voz

simultáneos (n) y del codec utilizado, del número máximo de sesiones de Video Conferencia y de su codec (velocidad nominal) (BW_{VCnom}).

4.2.3.5.1.- Creación de las clases por precedencia

La clasificación previa al encolamiento se realiza mediante la definición de las siguientes clases (configuración obligatoria)

```
!
class-map match-all Prec-3
match ip precedence 3
!
class-map match-all Prec-2
match ip precedence 2
!
class-map match-all Prec-5
match ip precedence 5
!
```

4.2.3.5.2.- Creación del policy-map de salida: configuración de la categoría VoIP (Precedence 5).

```
!
policy-map HACIA_RED
description Esquema de priorizacion por tipo de IP Precedence
class Prec-5
priority BW1
!
```

Para la clase Prec-5 (correspondiente a VoIP) se destina tanto ancho de banda como canales de voz simultáneos vayan a ser servidos. Como referencia, se estima un consumo de 30[Kbps] por canal de voz al utilizar el codec G.729. El valor BW1 = n€30 se configura en la línea:

```
priority 90 (BW1 = 90[Kbps])
```

4.2.3.5.3.- Creación del policy-map de salida: configuración de la categoría VideoC (Precedence 3).

En el mismo policy-map se configura la clase para el tratamiento del tráfico con precedencia 3 (categoría VideoC). Al interior de esta clase se debe especificar dos parámetros de forma obligatoria: “bandwidth” y “police”

```
!
policy-map HACIA_RED
description Esquema de priorizacion por tipo de IP Precedence
class Prec-3
bandwidth BW2
police BW2-max
¡
```

Para la clase Prec-3, que define el tratamiento para el tráfico de Video Conferencia, se asigna una ponderación alta para que pueda ser priorizado adecuadamente sobre el tráfico de datos. El valor para el parámetro 'bandwidth' corresponde al máximo valor de ancho de banda disponible, cuyo valor viene dado por:

$$BW_2 = 0.95 \cdot BW_{Clase} - BW_1 - BW_3$$

donde el valor de BW3 es determinado en la siguiente sección.

El valor para $BW_{2\text{-}max}$, que corresponde al máximo tráfico alcanzado por la sesión de Video Conferencia, se calcula como:

$$BW_{2\text{-}max} = 1{,}3 \cdot BW_{VCnom}$$

Es decir, se recortará el tráfico, por razones de evitar sobreventa del servicio, un 30% por sobre el valor nominal utilizado por la Video Conferencia. Por ejemplo, una Video Conferencia correspondiente a $BW_{VCnom} = 384$[Kbps], el valor para $BW_{2\text{-}max}$ resulta ser de 500[Kbps].

4.2.3.5.4.- Creación del policy-map de salida: configuración de la categoría DATA_GOLD (Precedence 2).

En el mismo policy-map se configura la clase para el tratamiento del tráfico con precedencia 2 correspondiente al tráfico de categoría Data-Gold. Al interior de esta clase se debe especificar el parámetro "bandwidth", respetando las restricciones dadas anteriormente.

```
!
policy-map HACIA_RED
description Esquema de priorizacion por tipo de IP Precedence
class Prec-2
bandwidth BW3
set fr-de
!
```

donde

$$BW_3 = BW_{DG}$$

Este tráfico será marcado como descartable por la red Frame Relay, por lo que se enciende el bit DE de las tramas Frame Relay correspondientes a esta clase.

4.2.3.5.5.- Creación del policy-map de salida: configuración de la categoría BE (Precedence 0)

Finalmente, en el mismo policy-map se configura la clase por defecto, clase que encausará todo el tráfico que no ha calzado en las clases anteriores. Utilizará todo el ancho de banda restante. Este tipo de tráfico también será descartable por la red Frame Relay. Su configuración corresponde a:

```
!
policy-map HACIA_RED
class class-default
fair-queue
set fr-de
!
```

4.2.3.5.6.- Aplicación del policy-map "HACIA_RED" de salida hacia la red MPLS

En este caso especial de Frame Relay, el policy-map se aplica en la definición de traffic shaping

```
map-class frame-relay CFR
service-policy output HACIA_RED
!
```

4.2.3.6.- Ejemplo de la configuración del router CE

En el siguiente ejemplo se considera un acceso AR = 768[Kbps], dos canales de voz codificadas con G.729, una sesión de Video Conferencia de 384[Kbps] y un tráfico de aplicaciones críticas de 64[Kbps].

La configuración más relevante del router CE se muestra a continuación.

```
!
class-map match-all VideoC
 match access-group name VideoC
!
class-map match-all VoIP
 match access-group name VoIP
!
class-map match-all Prec-3
 match ip precedence 3
!
class-map match-all Prec-2
 match ip precedence 2
!
class-map match-all Prec-5
 match ip precedence 5
!
```

```
class-map match-all DATA-GOLD
 match access-group name data-gold
!
class-map match-all VoIP-Control
 match access-group name VoIP-Control
!
class-map match-all VideoC-Control
 match access-group name VideoC-Control
!
!
policy-map HACIA_RED
 description Esquema de priorizacion por tipo de IP Precedence
 class Prec-5
  priority 60
class Prec-3
 bandwidth 605
 police 500000
class Prec-2
 bandwidth 64
 set fr-de
class class-default
 fair-queue
 set fr-de
!
policy-map Clasifica
 description Clasificacion y Marcado de paquetes segun servicio
 class VoIP
  set ip precedence 5
 class VideoC
  set ip precedence 3
 class DATA-GOLD
  set ip precedence 2
 class VoIP-Control
  set ip precedence 2
 class VideoC-Control
  set ip precedence 2
 class class-default
  set ip precedence 0
!
!
!
interface FastEthernet0
 ip address 192.168.105.199 255.255.255.0
 service-policy input Clasifica
!
interface Serial0
 no ip address
 encapsulation frame-relay
 frame-relay traffic-shaping
!
interface Serial0.62 point-to-point
 ip address 26.0.0.6 255.0.0.0
 frame-relay interface-dlci 602
  class CFR
!
!
!
ip access-list extended VideoC
 remark Regla que incluya el stream de Video
 permit udp host 10.10.10.155 any range 3230 3235
!
ip access-list extended VideoC-Control
 remark Regla que incluya la comunicacion de control de la VC
 permit tcp host 10.10.10.155 any range 3230 3231
!
ip access-list extended VoIP
 remark Regla que incluya el trafico de Voz
 permit udp 10.10.10.0 0.0.0.15 any range 16384 32767
!
ip access-list extended VoIP-Control
 remark Regla que incluya la comunicacion de control de Voz
 permit tcp 10.10.10.0 0.0.0.15 any eq 1720
```

```
!
ip access-list extended data-gold
 remark Lista de Acceso que identifica las conexiones DLSw
 permit tcp any any eq 2065
 permit tcp any any eq 2067
 permit tcp any eq 2065 any
 permit tcp any eq 2067 any
!
!
map-class frame-relay CFR
 frame-relay cir 768000
 frame-relay bc 7680
 frame-relay be 0
 frame-relay mincir 768000
 service-policy output HACIA_RED
!
end
```

Capitulo V

5.- Accesos MPLS Nativo (Ethernet 10/100/1000)

5.1 Accesos MPLS Nativo.

El acceso Mpls nativo al backbone Mpls instalado en un usuario corresponde a una conectividad directa al backbone MPLS a través de los equipos de borde la red. Esto quiere decir que el router de borde de la Red MPLS (PE) se extiende mediante una red Vlan asociada al PE a través de Switches de alta conectividad.

Este tipo de acceso tiene instalado switches de capa 2 destinados a recibir accesos directos de clientes 10/100/ Mbps y Gigabit Ethernet, llamados accesos MPLS nativos. Este tipo de topologías también es denominado Red Metro.

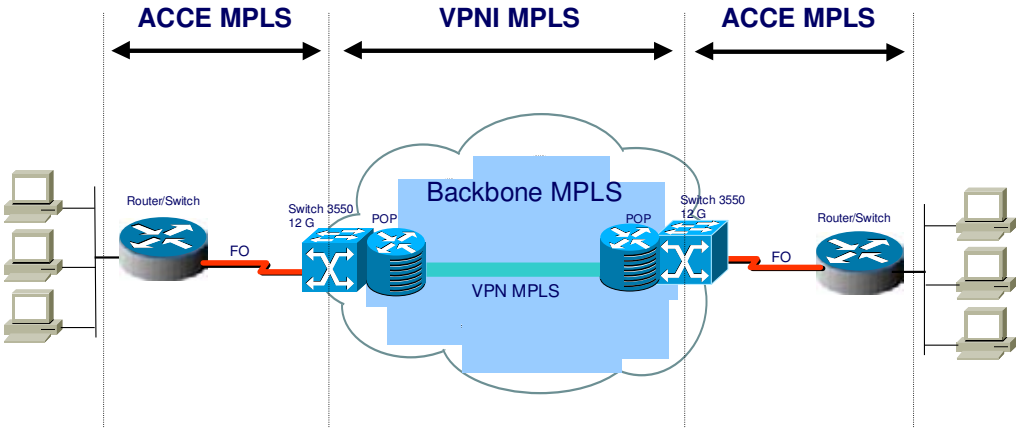


Figura 9: Topología red MPLS Nativo

Generalmente los usuarios que optan por este tipo de acceso son las grandes corporaciones que por diferentes aplicaciones que poseen, voz, video, data Gold, mail voice y otras tantas, necesitan cubrir y sentirse seguros que sus aplicaciones no se verán afectados por escasez de ancho de banda.

Incluso las grandes empresas optan por estos accesos en sus casas matrices o donde lo requieran, ya que necesitan cubrir una alta demanda de tráfico para sus diferentes sucursales que tienen a lo largo del país o del mundo. Todo esto porque hoy en día las

empresas tienen centralizados sus aplicaciones informáticas (servidores, Voice Mail, IpPBX, etc.)

5.2.- Descripción del servicio

En este tipo de servicio, el acceso desde dependencias del usuario corresponde a un acceso mediante la red METRO Ethernet, conectando las dependencias de cliente a la red MPLS. El servicio está constituido, además, por un router (CE en la notación de MPLS) en dependencias de usuario y que forma parte activa de las funciones a implementar para obtener una diferenciación de servicios en el contexto de QoS.

Este router CE está conectado directamente la red MPLS, y a través de ésta se conecta al resto de puntos de su red privada, en lo que se denomina un servicio

QoS MPLS-VPN. El resto de los puntos de la red privada de cliente pueden utilizar diferentes medios de acceso para conectarse a la red MPLS.

El router CE realiza la clasificación, marcado y los procesos de encolamiento correspondientes para entregar una separación adecuada de los servicios VoIP, Video Conferencia, Data Gold, y tráfico Best Effort. Se define como administrado por el proveedor del servicio, por lo que los criterios de clasificación del tráfico (servicios) del cliente expresados en la configuración, son controlados.

La red METRO Ethernet proporciona un trayecto privilegiado a cada categoría de servicio diferenciadas a través de IP Precedence.

En el siguiente esquema, Figura N° 5,se representa la configuración de este tipo de acceso.

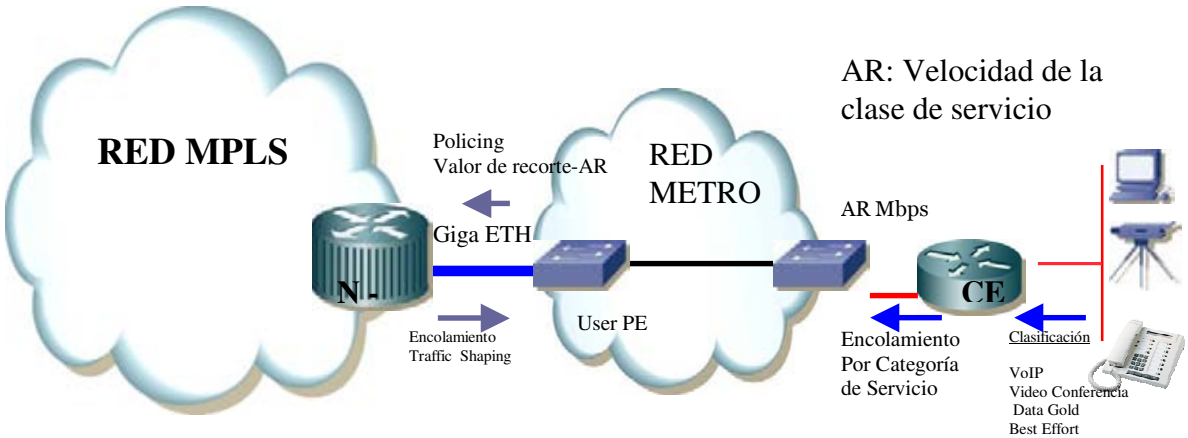


Figura 10 : Servicio QoS MPLS-VPN con acceso tipo MPLS Nativo (Ethernet 10/100/1000).

5.3.- Criterios de diseño

Como datos originales, provenientes del diseño de la implemetacion del servicio, se tiene el número de canales de voz máximo (n) y su codec respectivo utilizado por el servicio VoIP (valores que son utilizados para estimar el ancho de banda que consume el servicio VoIP, BW_{VoIP}), el número de sesiones simultáneas máximas de Video Conferencia y su ancho de banda nominal (BW_{VCnom}), dependiente de la velocidad de la Video Conferencia y su codec. Además se especifica a priori la intensidad de tráfico de datos de la categoría Data Gold (BW_{DG}) que debe priorizarse por sobre el resto de los datos.

Las restricciones que se imponen sobre la asignación de recursos son:

$$BW_{VoIP} \leq \frac{1}{2} BW_{Clase}$$

$$BW_2 \geq 1{,}2 \cdot BW_{VCnom}$$

$$BW_1 + BW_2 + BW_3 = 0.95 \cdot BW_{Clase}$$

donde BW_{Clase} es la velocidad de la Clase de Servicio (velocidad contratada por cliente) y BW_{VoIP} = n€codec. Los valores BW1, BW2 y BW3 son valores de ancho de banda que se utilizarán en la configuración del router CE y no reflejan necesariamente valores reales de ancho de banda utilizados por las categorías de servicios.

5.4.- Configuración Router CE

Las tareas asignadas al router consisten en Clasificar el tráfico en los diferentes servicios, Marcado de los paquetes IP de los diferentes servicios, Priorización (Scheduling) de los flujos de servicios, y Modelado del tráfico (Shaping) para el ajuste a la tasa de transmisión digital de la clase de servicio correspondiente.

5.4.1.- Clasificación del tráfico por categorías de servicio

La clasificación del tráfico se realizará utilizando el campo IP Precedence de la cabecera del paquete IP. Cada categoría de servicio tendrá un valor diferente y sus valores específicos corresponden a:

Categoría de Servicio	Acrónimo	Valor de IP Precedence
Tráfico de Voz sobre IP	VoIP	5
Tráfico de Video Conferencia	VideoC	3
Aplicaciones Críticas del Negocio	DATA-GOLD	2
Resto del Tráfico de Datos	BE	0

El objetivo final de la clasificación consiste en encauzar los flujos reales de cada servicio entregado a cliente (VoIP, Video Conferencia, etc.) en los canales que a lo largo de toda la red están especialmente acondicionados para ello. Es importante que esta clasificación sea rigurosa para impedir, por ejemplo, la suplantación de tráfico priorizado por tráfico no relevante por parte del usuario.

5.4.1.1.- Configuración de los criterios de clasificación (listas de acceso).

La clasificación se realiza utilizando criterios de identificación de los servicios mediante las listas de acceso correspondientes. Cada servicio puede ser caracterizado por una lista de acceso más específica que las mostradas a continuación, además de presentarse diferentes métodos, por lo que su definición específica debe ser tema a abordar en el proceso de instalación del servicio en particular.

Ejemplo de criterios de clasificación:

Lista de acceso para el tráfico VoIP

```
Router#conf ter
Router(config)#ip access-list extended [name]
Router(config-ext-nacl)# permit [protocolo] [source] [wildcard] [destination]
[wildcard]
```

Ejemplo:

```
router2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
router2(config)#ip access-list extended VoIP
router2(config-ext-nacl)#remark Regla que incluya el trafico de Voz
router2(config-ext-nacl)# permit udp 10.10.10.0 0.0.0.15 any range 16384 16383
```

De similar manera, se configura las restantes listas de acceso para las demás categorías de servicio.

```
!
ip access-list extended VideoC
 remark Regla que incluya el stream de Video
 permit udp host 10.10.10.155 any range 3230 3235
!
```

```
ip access-list extended VoIP
 remark Regla que incluya el trafico de Voz
 permit udp 10.10.10.0 0.0.0.15 any range 16384 16383
!
ip access-list extended DATA_GOLD
 remark Lista de Acceso que identifica el tráfico GOLD
 permit tcp host 10.1.1.200 any
!
```

NOTA: los criterios expuestos en las listas de acceso mostradas, son criterios de calce genéricos y deberán ser afinados con más detalle en la habilitación de algún servicio.

5.4.1.2.- Creación de las clases para las diferentes categorías de servicio

Las clases que clasifican el tráfico se configuran de la siguiente forma.

```
!
class-map match-all VideoC
 match access-group name VideoC
!
class-map match-all VoIP
 match access-group name VoIP
!
class-map match-all DATA-GOLD
 match access-group name DATA_GOLD
!
```

5.4.2- Marcado de los paquetes por categoría de servicio

El marcado de los paquetes se realiza utilizando las clases definidas anteriormente y se aplica de entrada en todas las interfaces que miran hacia la LAN del cliente.

5.4.2.1.- Creación del policy-map CLASIFICACION

Esta configuración realiza el marcado de los paquetes

Ejemplo:

```
!
policy-map CLASIFICACION
 description Clasificacion y Marcado de paquetes segun servicio
 class VoIP
  set ip precedence 5
 class VideoC
  set ip precedence 3
 class DATA-GOLD
  set ip precedence 2
 class class-default
  set ip precedence 0
!
```

5.4.2.2.- Aplicación del policy-map a la interfaz

El marcado de los paquetes se debe aplicar de entrada en todas las interfaces que miran hacia la LAN del cliente.

Ejemplo:

```
!
interface FastEthernet0
 ip address 192.168.105.199 255.255.255.0
 service-policy input CLASIFICACION
!
```

5.4.3.- Caso especial: Marcado de paquetes de voz en el caso de un Voice Gateway

Si el router CE es un Voice Gateway, vale decir, el router tiene conectadas interfaces de voz (FXO, FXS, E&M, E1) el marcado de paquetes debe realizarse directamente en los "dial-peer voice" del tipo VoIP correspondientes.

Por ejemplo:

```
dial-peer voice 3 voip
 destination-pattern 15..
 session target ipv4:172.16.65.182
 ip precedence 5
```

Algunas versiones de sistema operativo no permiten la configuración anterior, y en ese caso la configuración alternativa será:

```
dial-peer voice 3 voip
 destination-pattern 15..
 session target ipv4:172.16.65.182
 ip qos dscp cs5 media
```

A través de ambas configuraciones, los paquetes correspondientes a VoIP ya van marcados con IP Precedence 5, por lo que pueden ser clasificados en la clase VoIP en el policy-map de salida.

5.4.4.- Modelado del tráfico (Traffic Shaping)

Se debe aplicar un modelamiento de tráfico hacia la salida a fin de evitar que la red MPLS descarte el exceso que está por sobre la clase de servicio contratada por cliente (BW_{Clase}).

5.4.4.1.- Configuración de los parámetros del Shaping

Para lograr que el tráfico proveniente desde la LAN no supere el ancho de banda contratado, reflejado en la clase de servicio, se debe configurar un primer 'policy-map' llamado HACIA_RED_PADRE

```
!
```

```
policy-map HACIA_RED_PADRE
class class-default
shape average BWClase
!
```

Donde BW_{Clase} corresponde al ancho de banda definido en la clase de servicio contratada.

Por ejemplo para una clase de servicio de BW_{Clase} = 2Mbps, la configuración será:

```
!
policy-map HACIA_RED_PADRE
 class class-default
  shape average 2000000
!
```

5.4.5.- Priorización del tráfico por categoría de servicio

La priorización propiamente tal se realiza en la sub-interfaz de salida hacia la red. Esta priorización queda definida en el policy-map de nombre "HACIA_RED_HIJO" que será configurado dentro del policy-map "HACIA_RED_PADRE". Este último será el que se aplica a la interfaz de conexión
hacia la red METRO.

Para el cálculo de los parámetros a configurar en el sistema de priorización se da por conocidos, aportados por el diseño previo, el valor de la intensidad de tráfico de las "aplicaciones críticas del negocio" (BW_{DG}), del número de canales de voz simultáneos (n) y del codec utilizado, del número de sesiones de Video Conferencia y de su codec (velocidad nominal) (BW_{VCnom}).

5.4.5.1.- Configuración del máximo porcentaje reservable de ancho de banda

Los equipos router pueden asignar como máximo un cierto porcentaje de la tasa de acceso AR a las diferentes categorías de servicio, cuyo valor por omisión es un 75%. Este valor se modifica con el comando de interfaz 'max-reserved-bandwidth XX', donde XX es el porcentaje máximo del 'bandwidth' de la interfaz a asignar con las clases. Este comando se aplica directamente en la interfaz de salida, dejando para nuestro caso un 95% de reserva.

Ejemplo :

```
!
int ethernet 0/0
 max-reserved-bandwidth 95
```

```
!
```

NOTA: Este valor de 95% se considerará fijo para todo tipo de diseño.

5.4.5.2.- Creación de las clases por precedencia

La clasificación previa al encolamiento se realiza mediante la definición de las siguientes clases (configuración obligatoria)

```
!
class-map match-all Prec-3
 match ip precedence 3
!
class-map match-all Prec-2
 match ip precedence 2
!
class-map match-all Prec-5
 match ip precedence 5
!
```

5.4.5.3.- Creación del policy-map de salida: configuración de la categoría VoIP (Precedence 5)

```
!
policy-map HACIA_RED_HIJO
 description Esquema de priorizacion por tipo de IP Precedence
 class Prec-5
  priority BW1
!
```

Para la clase Prec-5 (correspondiente a VoIP) se destina tanto ancho de banda como canales de voz simultáneos vayan a ser servidos. Como referencia, se estima un consumo de 35[Kbps] por canal de voz al utilizar el codec G.729. El valor BW1 = n€35 se configura en la línea

```
priority 105 (BW1 = 105[Kbps])
```

5.4.5.4.- Creación del policy-map de salida: configuración de la categoría VideoC (Precedence 3)

En el mismo policy-map se configura la clase para el tratamiento del tráfico con precedencia 3 (categoría VideoC). Al interior de esta clase se debe especificar dos parámetros de forma obligatoria: “bandwidth” y “police”

```
!
policy-map HACIA_RED_HIJO
 description Esquema de priorizacion por tipo de IP Precedence
 class Prec-3
  bandwidth BW2
  police BW2-max
!
```

Para la clase Prec-3, que define el tratamiento para el tráfico de Video Conferencia, se asigna una ponderación alta para que pueda ser priorizado adecuadamente sobre el tráfico de datos. El valor para el parámetro 'bandwidth' corresponde al máximo valor de ancho de banda disponible, cuyo valor viene dado por:

$$BW_2 = 0.95 \cdot BW_{Clase} - BW_1 - BW_3$$

donde el valor de BW_3 es determinado en la siguiente sección.

El valor para $BW_{2\text{-}max}$, que corresponde al máximo tráfico alcanzado por la sesión de video Conferencia, se calcula como:

$$BW_{2\text{-}max} = 1{,}3 \cdot BW_{VCnom}$$

Es decir, se recortará el tráfico, por razones de evitar sobreventa del servicio, un 30% por sobre el valor nominal utilizado por la Video Conferencia. Por ejemplo, una Video Conferencia correspondiente a $BW_{VCnom} = 384$[Kbps], el valor para $BW_{2\text{-}max}$ resulta ser de 500[Kbps].

5.4.5.5.- Creación del policy-map de salida: configuración de la categoría DATA_GOLD (Precedence 2)

En el mismo policy-map se configura la clase para el tratamiento del tráfico con precedencia 2 correspondiente al tráfico de categoría Data-Gold. Al interior de esta clase se debe especificar el parámetros "bandwidth", respetando las restricciones mencionadas en primera instancia.

```
!
policy-map HACIA_RED_HIJO
 description Esquema de priorizacion por tipo de IP Precedence
 class Prec-2
  bandwidth BW3
!
```

donde

$$BW_3 = BW_{DG}$$

5.4.5.6.- Creación del policy-map de salida: configuración de la categoría BE (Precedence 0)

Finalmente, en el mismo policy-map se configura la clase por defecto, clase que encausará todo el tráfico que no ha calzado en las clases anteriores. Utilizará todo el ancho de banda restante. Este tipo de tráfico también será descartable por la red ATM. Su configuración corresponde a:

```
!
policy-map HACIA_RED_HIJO
 class class-default
  fair-queue
!
```

5.4.5.7.- Aplicación del policy-map "HACIA_RED_HIJO" dentro del policymap "HACIA_RED_PADRE"

Para el correcto funcionamiento de la priorización y del modelamiento de tráfico a un ancho de banda máximo, es necesario configurar anidados los policy-map que definen ambas tareas.

```
!
policy-map HACIA_RED_PADRE
 class class-default
  shape average 2000000
  service-policy HACIA_RED_HIJO
!
```

5.4.5.8.- Aplicación del policy-map "HACIA_RED_PADRE" a la interfaz de salida hacia la red MPLS

```
!
int ethernet 0/0
 service-policy output HACIA_RED_PADRE
 max-reserved-bandwidth 95
!
```

5.4.6.- Ejemplo de la configuración del router CE

En el siguiente ejemplo se considera un acceso de clase de servicio BW_{Clase} = 2[Mbps], 3 canales de voz codificadas con G.729, una sesión de Video Conferencia de 384[Kbps] y un tráfico de aplicaciones críticas de 256[Kbps].

La configuración más relevante del router CE se muestra a continuación:

```
!
class-map match-all VideoC
 match access-group name VideoC
!
class-map match-all VoIP
 match access-group name VoIP
!
class-map match-all Prec-3
 match ip precedence 3
!
class-map match-all Prec-2
 match ip precedence 2
!
class-map match-all Prec-5
 match ip precedence 5
!
class-map match-all DATA-GOLD
 match access-group name data-gold
!
!
policy-map HACIA_RED_HIJO
 description Esquema de priorizacion por tipo de IP Precedence
 class Prec-5
  priority 105
 class Prec-3
  bandwidth 1539
  police 500
 class Prec-2
  bandwidth 256
 class class-default
  fair-queue
!
policy-map HACIA_RED_PADRE
 class class-default
  shape average 2000000
   service-policy HACIA_RED_HIJO
!
policy-map Clasifica
 description Clasificacion y Marcado de paquetes segun servicio
 class VoIP
  set ip precedence 5
 class VideoC
  set ip precedence 3
 class DATA-GOLD
  set ip precedence 2
 class class-default
  set ip precedence 0
!
!
interface FastEthernet0/1
 ip address 192.168.105.199 255.255.255.0
 service-policy input Clasifica
!
!
interface Ethernet 0/0
 ip address 192.168.100.1 255.255.255.0
 service-policy output HACIA_RED_PADRE
 max-reserved-bandwidth 95
!
```

```
!
ip access-list extended VideoC
 remark Regla que incluya el stream de Video
 permit udp host 10.10.10.155 any range 3230 3235
!
ip access-list extended VoIP
 remark Regla que incluya el trafico de Voz
 permit udp 10.10.10.0 0.0.0.15 any range 16384 32767
!
ip access-list extended DATA_GOLD
 remark Lista de Acceso que identifica el tráfico GOLD
 permit tcp host 10.1.1.200 any
!
!
end
```

Capitulo VI

6.- Accesos ATM STM-1

6.1.- Descripción del servicio

En este tipo de servicio, el acceso desde dependencias de los usuarios corresponde a un acceso ATM STM-1. El servicio está constituido por un router (CE en la notación de MPLS) en dependencias del usuario y que forma parte activa de las funciones a implementar para obtener una diferenciación de servicios en el contexto de QoS. Este router CE está conectado, a través de la red ATM MS, a la
red MPLS, y a través de ésta se conecta al resto de puntos de su red privada, en lo que se denomina un servicio MPLS-VPN. El resto de los puntos de la red privada de cliente pueden utilizar diferentes medios de acceso para conectarse a la red MPLS.

El router CE realiza la clasificación, marcado y los procesos de encolamiento correspondientes para entregar una separación adecuada de los servicios VoIP, Video Conferencia, Data Gold, y tráfico Best Effort. Se define como administrado por el proveedor del servicio, por lo que los criterios de clasificación del tráfico (servicios) del cliente expresados en la configuración, son controlados.

La red ATM proporciona un circuito virtual (PVC) de categoría privilegiada por sobre el resto de los PVC de datos. A los servicios QoS MPLS-VPN se asignan PVC de categoría rt-VBR. En el siguiente esquema, se representa la configuración de este tipo de acceso.

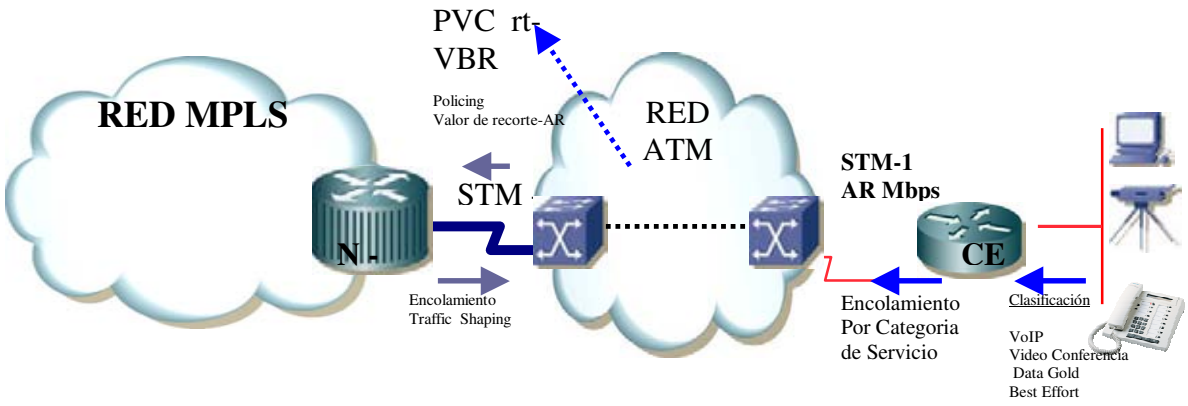


Figura 11: Servicio QoS MPLS-VPN con acceso tipo ATM-STM-1.

6.2.- Criterios de diseño

Como datos originales, provenientes del diseño a implementar en un usuario, se tiene el número de canales de voz máximo (n) y su codec respectivo utilizado por el servicio VoIP (valores que son utilizados para estimar el ancho de banda que consume el servicio VoIP, BW_{VoIP}), el número de sesiones simultáneas máximas de Video Conferencia y su ancho de banda nominal (BW_{VCnom}), dependiente de la velocidad de la Video Conferencia y su codec. Además se especifica a priori la intensidad de tráfico de datos de la categoría Data Gold (BW_{DG}) que debe priorizarse por sobre el resto de los datos.

Las restricciones que se imponen sobre la asignación de recursos son:

$$BW_{VoIP} \leq \frac{1}{2} BW_{Clase}$$

$$BW_2 \geq 1{,}2 \cdot BW_{VCnom}$$

$$BW_1 + BW_2 + BW_3 = 0.95 \cdot BW_{Clase}$$

donde BW_{Clase} es la velocidad de la Clase de Servicio y BW_{VoIP} = n€codec. Los valores BW_1, BW_2 y BW_3 son valores de ancho de banda que se utilizarán en la configuración del router CE y no reflejan necesariamente valores reales de ancho de banda utilizados por las categorías de servicios.

6.3.- Configuración Router CE

Las tareas asignadas al router consisten en Clasificar el tráfico en los diferentes servicios, Marcado de los paquetes IP de los diferentes servicios, Priorización (Scheduling) de los flujos de servicios, y Modelado del tráfico (Shaping) para el ajuste a la tasa de transmisión digital de la clase de servicio correspondiente.

6.3.1.- Clasificación del tráfico por categorías de servicio

La clasificación del tráfico se realizará utilizando el campo IP Precedence de la cabecera del paquete IP. Cada categoría de servicio tendrá un valor diferente y sus valores específicos corresponden a:

Categoría de Servicio	Acrónimo	Valor de IP Precedence
Tráfico de Voz sobre IP	VoIP	5
Tráfico de Video Conferencia	VideoC	3
Aplicaciones Críticas del Negocio	DATA-GOLD	2
Resto del Tráfico de Datos	BE	0

El objetivo final de la clasificación consiste en encauzar los flujos reales de cada servicio entregado a cliente (VoIP, Video Conferencia, etc.) en los canales que a lo largo de toda la red están especialmente acondicionados para ello. Es importante que esta clasificación sea rigurosa para impedir, por ejemplo, la suplantación de tráfico priorizado por tráfico no relevante por parte del cliente.

6.3.1.1.- Configuración de los criterios de clasificación (listas de acceso)

La clasificación se realiza utilizando criterios de identificación de los servicios mediante las listas de acceso correspondientes. Cada servicio puede ser caracterizado por una lista de acceso más específica que las mostradas a continuación y su definición específica debe ser tema a abordar en el proceso de instalación del servicio en particular.

Ejemplo de criterios de clasificación:

```
!
ip access-list extended VideoC
remark Regla que incluya el stream de Video
permit udp host 10.10.10.155 any range 3230 3235
!
ip access-list extended VideoC-Control
remark Regla que incluya la comunicacion de control de la VC
permit tcp host 10.10.10.155 any range 3230 3231
!
ip access-list extended VoIP
remark Regla que incluya el trafico de Voz
permit udp 10.10.10.0 0.0.0.15 any range 16384 32767
!
ip access-list extended VoIP-Control
remark Regla que incluya la comunicacion de control de Voz
permit tcp 10.10.10.0 0.0.0.15 any eq 1720
!
ip access-list extended data-gold
remark Lista de Acceso que identifica las conexiones DLSw
permit tcp any any eq 2065
permit tcp any any eq 2067
```

```
permit tcp any eq 2065 any
permit tcp any eq 2067 any
!
!
!
```

NOTA: los criterios expuestos en las listas de acceso mostradas más arriba, son criterios de calce genéricos y deberán ser afinados con más detalle en la habilitación del servicio entre el proveedor del servicio y su cliente.

6.3.1.2.- Creación de las clases para las diferentes categorías de servicio

Las clases que clasifican el tráfico se configuran de la siguiente forma.

```
!
class-map match-all VideoC
 match access-group name VideoC
!
class-map match-all VoIP
 match access-group name VoIP
!
class-map match-all DATA-GOLD
 match access-group name data-gold
!
class-map match-all VoIP-Control
 match access-group name VoIP-Control
!
class-map match-all VideoC-Control
 match access-group name VideoC-Control
!
!
```

6.3.2.- Marcado de los paquetes por categoría de servicio

El marcado de los paquetes se realiza utilizando las clases definidas anteriormente y se aplica de entrada en todas las interfaces que miran hacia la LAN del cliente.

6.3.2.1.- Creación del policy-map CLASIFICACION

Esta configuración realiza el marcado de los paquetes
Ejemplo:

```
!
policy-map CLASIFICACION
 description Clasificacion y Marcado de paquetes segun servicio
 class VoIP
  set ip precedence 5
 class VideoC
  set ip precedence 3
 class DATA-GOLD
  set ip precedence 2
 class VoIP-Control
  set ip precedence 2
 class VideoC-Control
  set ip precedence 2
 class class-default
  set ip precedence 0
!
```

6.3.2.2.- Aplicación del policy-map a la interfaz

El marcado de los paquetes se debe aplicar de entrada en todas las interfaces que miran hacia la LAN del cliente.

Ejemplo:

```
!
interface FastEthernet0
 ip address 192.168.105.199 255.255.255.0
 service-policy input CLASIFICACION
!
```

6.3.3.- Caso especial: Marcado de paquetes de voz en el caso de un Voice Gateway

Si el router CE es un Voice Gateway, vale decir, el router tiene conectadas interfaces de voz (FXO, FXS, E&M, E1) el marcado de paquetes debe realizarse directamente en los "dial-peer voice" del tipo VoIP correspondientes.

Por ejemplo:

```
dial-peer voice 3 voip
 destination-pattern 15..
 session target ipv4:172.16.65.182
 ip precedence 5
```

Algunas versiones de sistema operativo no permiten la configuración anterior, y en ese caso la configuración alternativa será:

```
dial-peer voice 3 voip
 destination-pattern 15..
 session target ipv4:172.16.65.182
 ip qos dscp cs5 media
```

A través de ambas configuraciones, los paquetes correspondientes a VoIP ya van marcados con Precedence 5, por lo que pueden ser clasificados en la clase VoIP en el policy-map de salida.

6.3.4.- Modelado del tráfico (Traffic Shaping)

En este caso, no se aplica explícitamente traffic shaping, pero cada sub-interfaz ATM de los routers controla directamente el flujo máximo de paquetes, o celdas para ser más específico, mediante la definición de las características de tráfico del circuito virtual (PVC) (contrato de tráfico).

Los parámetros de tráfico a configurar en la definición del PVC son:

$$\text{Peak Cell Rate (PCR)} = 1{,}25 \text{ €} BW_{Clase} \text{ [Kbps]}$$
$$\text{Average Cell Rate} = 1{,}25 \text{ €} BW_{Clase} \text{ [Kbps]}$$

donde BW_{Clase} es el valor de la velocidad contratada por cliente.

6.3.4.1.- Configuración de los parámetros del Shaping

En la sub-interfaz ATM correspondiente, en la definición del PVC, se aplica la 'velocidad' de éste y que debe coincidir con la velocidad de la clase de servicio.

```
!
interface ATM0.10 point-to-point
 pvc 0/100
  vbr-rt 10000 10000
  tx-ring-limit 3
!
!
```

Este comando, 'tx-ring-limit 3' es obligatorio cuando se utiliza este tipo de QoS. Su efecto es el de disminuir el tiempo de encendido de los mecanismos de encolamiento y priorización.

6.3.5.- Priorización del tráfico por categoría de servicio

La priorización propiamente tal se realiza en la sub-interfaz serial. Esta priorización queda definida en el policy-map de nombre 'HACIA_RED' y se aplica directamente en la sub-interfaz ATM.

Para el cálculo de los parámetros a configurar en el sistema de priorización se da por conocidos, aportados por el diseño previo, el valor de la intensidad de tráfico de las "aplicaciones críticas del negocio" (BW_{DG}), del número de canales de voz simultáneos (n) y del codec utilizado, del número de sesiones de Video Conferencia y de su codec (velocidad nominal) (BW_{VCnom}).

6.3.5.1.- Configuración del máximo porcentaje reservable de ancho de banda

Los equipos router pueden asignar como máximo un cierto porcentaje de la tasa de acceso AR a las diferentes categorías de servicio, cuyo valor por omisión es un 75%. Este valor se modifica con el comando de interfaz 'max-reserved-bandwidth XX', donde

XX es el porcentaje máximo del 'bandwidth' de la interfaz a asignar con las clases. Este comando se aplica directamente en la interfaz de salida.
Ejemplo:

```
!
interface ATM0.10 point-to-point
 ip address 10.10.10.1 255.255.255.0
 pvc 0/100
 max-reserved-bandwidth 95
!
```

NOTA: Este valor de 95% se considerará fijo para todo tipo de diseño.

6.3.5.2.- Creación de las clases por precedencia

La clasificación previa al encolamiento se realiza mediante la definición de las siguientes clases (configuración obligatoria)

```
!
class-map match-all Prec-3
 match ip precedence 3
!
class-map match-all Prec-2
 match ip precedence 2
!
class-map match-all Prec-5
 match ip precedence 5
!
```

6.3.5.3.- Creación del policy-map de salida: configuración de la categoría VoIP (Precedence 5)

```
!
policy-map HACIA_RED
description Esquema de priorizacion por tipo de IP Precedence
class Prec-5
priority BWLLQ
!
```

Para la clase Prec-5 (correspondiente a VoIP) se destina tanto ancho de banda como canales de voz simultáneos vayan a ser servidos. Como referencia, se estima un consumo de 45[Kbps] por canal de voz al utilizar el codec G.729. El valor $BW_1 = n€45$ se configura en la línea:

```
priority 90 (BW1 = 90[Kbps])
```

6.3.5.4.- Creación del policy-map de salida: configuración de la categoría VideoC (Precedence 3)

En el mismo policy-map se configura la clase para el tratamiento del tráfico con precedencia 3 (categoría VideoC). Al interior de esta clase se debe especificar dos parámetros de forma obligatoria: "bandwidth" y "police"

```
!
policy-map HACIA_RED
 description Esquema de priorizacion por tipo de IP Precedence
class Prec-3
 bandwidth BW2
 police BW2-max
!
```

Para la clase Prec-3, que define el tratamiento para el tráfico de Video Conferencia, se asigna una ponderación alta para que pueda ser priorizado adecuadamente sobre el tráfico de datos. El valor para el parámetro 'bandwidth' corresponde al máximo valor de ancho de banda disponible, cuyo valor viene dado por:

$$BW_2 = 0.95 \cdot 1{,}25\ BW_{Clase} - BW_1 - BW_3$$

donde el valor de BW_3 es determinado en la siguiente sección.

El valor para $BW_{2\text{-}max}$, que corresponde al máximo tráfico alcanzado por la sesión de vides Conferencia, se calcula como:

$$BW_{2\text{-}max} = 1{,}3 \in BW_{VCnom}$$

Es decir, se recortará el tráfico, por razones de evitar sobreventa del servicio, un 30% por sobre el valor nominal utilizado por la Video Conferencia. Por ejemplo, una Video Conferencia correspondiente a BW_{VCnom} =384[Kbps], el valor para $BW_{2\text{-}max}$ resulta ser de 500[Kbps].

6.3.5.5.- Creación del policy-map de salida: configuración de la categoría DATA_GOLD (Precedence 2)

En el mismo policy-map se configura la clase para el tratamiento del tráfico con precedencia 2 correspondiente al tráfico de categoría Data-Gold. Al interior de esta clase se debe especificar el parámetro "bandwidth", respetando las restricciones dadas anteriormente.

```
!
policy-map HACIA_RED
 description Esquema de priorizacion por tipo de IP Precedence
 class Prec-2
  bandwidth BW3
  set atm-clp
!
```

donde

$$BW_3 = 1{,}25 \text{ € } BW_{DG}$$

Este tráfico será marcado como descartable por la red ATM, por lo que se enciende el bit CLP de las celdas ATM correspondientes a esta clase.

6.3.5.6.- Creación del policy-map de salida: configuración de la categoría BE (Precedence 0)

Finalmente, en el mismo policy-map se configura la clase por defecto, clase que encausará todo el tráfico que no ha calzado en las clases anteriores. Utilizará todo el ancho de banda restante. Este tipo de tráfico también será descartable por la red ATM. Su configuración corresponde a:

```
!
policy-map HACIA_RED
 class class-default
  fair-queue
  set atm-clp
!
```

6.3.5.7.- Aplicación del policy-map "HACIA_RED" a la interfaz de salida hacia la red MPLS

```
!
interface ATM0/0.10 point-to-point
 pvc 0/100
  service-policy output HACIA_RED
!
```

6.3.6.- Ejemplo de la configuración del router CE

En el siguiente ejemplo se considera un acceso de clase de servicio BW_{Clase} = 25[Mbps], 120 canales de voz codificadas con G.729, diez sesiones de Video Conferencia de 384[Kbps] y un tráfico de aplicaciones críticas de 1[Mbps].

Como comentario relativo a los accesos ATM, siempre se debe sobre dimensionar la velocidad del PVC en un 25% por sobre el valor de la velocidad contratada (BW_{Clase}).

Esto debido a pérdidas producidas por el llenado de celda en el encapsulamiento RFC 2684 (ex RFC-1483), que se manifiesta en que no siempre calza de manera exacta un paquete IP, en este caso, en un número entero de celdas, por lo que la mayoría de las veces hay celdas viajan a medio llenar por el enlace ATM.

La configuración más relevante del router CE se muestra a continuación.

```
!
class-map match-all VideoC
 match access-group name VideoC
!
class-map match-all VoIP
 match access-group name VoIP
!
class-map match-all Prec-3
 match ip precedence 3
!
class-map match-all Prec-2
 match ip precedence 2
!
class-map match-all Prec-5
 match ip precedence 5
!
class-map match-all DATA-GOLD
 match access-group name data-gold
!
class-map match-all VoIP-Control
 match access-group name VoIP-Control
!
class-map match-all VideoC-Control
 match access-group name VideoC-Control
!
!
policy-map HACIA_RED
 description Esquema de priorizacion por tipo de IP Precedence
 class Prec-5
  priority 5400
 class Prec-3
  bandwidth 23037
  police 5000
 class Prec-2
  bandwidth 1250
  set atm-clp
 class class-default
  fair-queue
  set atm-clp
!
policy-map Clasifica
 description Clasificacion y Marcado de paquetes segun servicio
 class VoIP
  set ip precedence 5
 class VideoC
  set ip precedence 3
 class DATA-GOLD
  set ip precedence 2
 class VoIP-Control
  set ip precedence 2
 class VideoC-Control
  set ip precedence 2
 class class-default
  set ip precedence 0
!
interface ATM0/0
 no ip address
 no atm ilmi-keepalive
!
```

```
interface ATM0/0.10 point-to-point
 ip address 10.10.10.1 255.255.255.0
 pvc 0/100
  protocol ip 10.10.10.2 broadcast
  vbr-rt 31250 31250
  encapsulation aal5snap
  max-reserved-bandwidth 95
  service-policy output HACIA_RED
!
!
!
interface FastEthernet0
 ip address 192.168.105.199 255.255.255.0
 service-policy input Clasifica
!
!
ip access-list extended VideoC
 remark Regla que incluya el stream de Video
 permit udp host 10.10.10.155 any range 3230 3235
!
ip access-list extended VideoC-Control
 remark Regla que incluya la comunicacion de control de la VC
 permit tcp host 10.10.10.155 any range 3230 3231
!
ip access-list extended VoIP
 remark Regla que incluya el trafico de Voz
 permit udp 10.10.10.0 0.0.0.15 any range 16384 32767
!
ip access-list extended VoIP-Control
 remark Regla que incluya la comunicacion de control de Voz
 permit tcp 10.10.10.0 0.0.0.15 any eq 1720
!
ip access-list extended data-gold
 remark Lista de Acceso que identifica las conexiones DLSw
 permit tcp any any eq 2065
 permit tcp any any eq 2067
 permit tcp any eq 2065 any
 permit tcp any eq 2067 any
!
!
!
end
```

6.4.- Configuración Red ATM

La configuración del servicio se realiza de forma similar como la que aplica a los servicios ATM MPLS, excepto que el PVC se define de categoría rt-VBR y se deshabilita "Traffic Policing" en la puerta de entrada a la red.

Capitulo VII

7.- Accesos 10/100 MS MPLS

7.1.- Descripción del servicio

En este tipo de servicio, el acceso desde dependencias del usuario corresponde a un Ethernet vía F.O. mediante transceivers, conectados a un Switch o a una puerta que interconecte con las red MS. El servicio está constituido, además, por un router (CE en la notación de MPLS) en dependencias del usuario y que forma parte activa de las funciones a implementar para obtener una diferenciación de servicios en el contexto de QoS. Este router CE está conectado, a través de la red ATM MS, a la red MPLS, y a través de ésta se conecta al resto de puntos de su red privada, en lo que se denomina un servicio MPLS-VPN. El resto de los puntos de la red privada de cliente pueden utilizar diferentes medios de acceso para conectarse a la red MPLS.

El router CE realiza la clasificación, marcado y los procesos de encolamiento correspondientes para entregar una separación adecuada de los servicios VoIP, Video Conferencia, Data Gold, y tráfico Best Effort. Se define como administrado por el proveedor del servicio por lo que los criterios de clasificación del tráfico (servicios) del usuarios expresados en la configuración, son controlados.
La red ATM proporciona un circuito virtual (PVC) de categoría privilegiada por sobre el resto de los

PVC de datos. A los servicios tipo QoS MPLS-VPN se asignan PVC de categoría rt-VBR.
En el siguiente esquema, Figura ,se representa la configuración de este tipo de acceso.

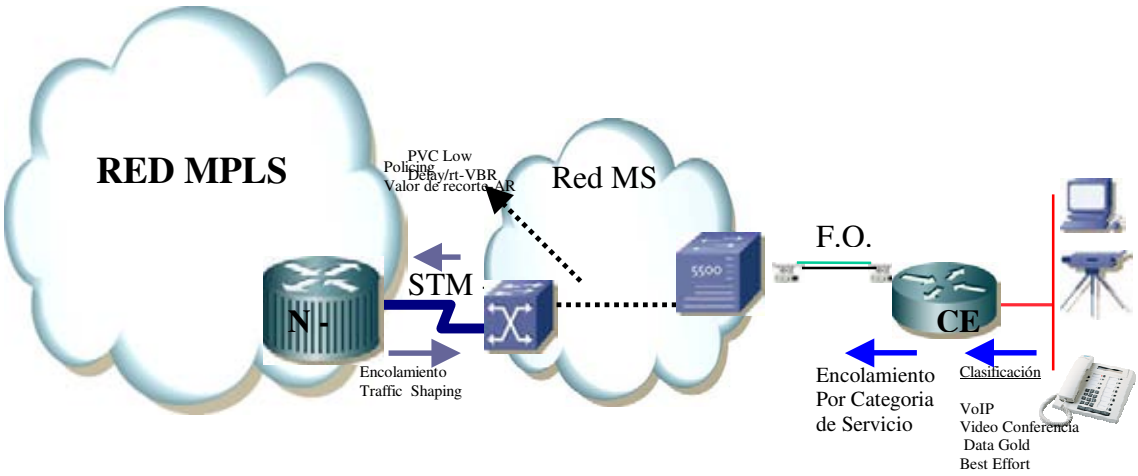


Figura 12: Servicio QoS MPLS-VPN con acceso tipo 10/100 MS MPLS.

7.2.- Criterios de diseño

Se tiene el número de canales de voz máximo (n) y su codec respectivo utilizado por el servicio VoIP (valores que son utilizados para estimar el ancho de banda que consume el servicio VoIP, BWVoIP), el número de sesiones simultáneas máximas de Video Conferencia y su ancho de banda nominal (BWVCnom), dependiente de la velocidad de la Video Conferencia y su codec. Además se especifica a priori la intensidad de tráfico de datos de la categoría Data Gold (BWDG) que debe priorizarse por sobre el resto de los datos.

Las restricciones que se imponen sobre la asignación de recursos son

$$BW_{VoIP} \leq \tfrac{1}{2}\, BW_{Clase}$$

$$BW_2 \geq 1{,}2 \cdot BW_{VCnom}$$

$$BW_1 + BW_2 + BW_3 = 0.95 \cdot BW_{Clase}$$

donde BW_{Clase} es la velocidad de la Clase de Servicio (velocidad contratada por cliente) y BW_{VoIP} = n€codec. Los valores BW_1, BW_2 y BW_3 son valores de ancho de banda que se utilizarán en la configuración del router CE y no reflejan necesariamente valores reales de ancho de banda utilizados por las categorías de servicios.

7.3.- Configuración Router CE

Las tareas asignadas al router consisten en Clasificar el tráfico en los diferentes servicios, Marcado de los paquetes IP de los diferentes servicios, Priorización (Scheduling) de los flujos de servicios, y Modelado del tráfico (Shaping) para el ajuste a la tasa de transmisión digital de la clase de servicio correspondiente.

7.3.1.- Clasificación del tráfico por categorías de servicio

La clasificación del tráfico se realizará utilizando el campo IP Precedence de la cabecera del paquete IP. Cada categoría de servicio tendrá un valor diferente y sus valores específicos corresponden a

Categoría de Servicio	Acrónimo	Valor de IP Precedence
Tráfico de Voz sobre IP	VoIP	5
Tráfico de Video Conferencia	VideoC	3
Aplicaciones Críticas del Negocio	DATA-GOLD	2
Resto del Tráfico de Datos	BE	0

El objetivo final de la clasificación consiste en encauzar los flujos reales de cada servicio entregado a cliente (VoIP, Video Conferencia, etc.) en los canales que a lo largo de toda la red están especialmente acondicionados para ello. Es importante que esta clasificación sea rigurosa para impedir, por ejemplo, la suplantación de tráfico priorizado por tráfico no relevante por parte del usuario.

7.3.1.1.- Configuración de los criterios de clasificación (listas de acceso)

La clasificación se realiza utilizando criterios de identificación de los servicios mediante las listas de acceso correspondientes. Cada servicio puede ser caracterizado por una lista de acceso más específica que las mostradas a continuación, además de presentarse diferentes métodos, por lo que su definición específica debe ser tema a abordar en el proceso de instalación del servicio en particular.

Ejemplo de criterios de clasificación

Lista de acceso para el tráfico VoIP

```
Router#conf ter
Router(config)#ip access-list extended [name]
Router(config-ext-nacl)# permit [protocolo] [source] [wildcard] [destination]
[wildcard]
```

Ejemplo:

```
router2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
router2(config)#ip access-list extended VoIP
router2(config-ext-nacl)#remark Regla que incluya el trafico de Voz
router2(config-ext-nacl)# permit udp 10.10.10.0 0.0.0.15 any range 16384 16383
```

De similar manera, se configura las restantes listas de acceso para las demás categorías de servicio.

```
!
ip access-list extended VideoC
remark Regla que incluya el stream de Video
permit udp host 10.10.10.155 any range 3230 3235
!
ip access-list extended VoIP
remark Regla que incluya el trafico de Voz
permit udp 10.10.10.0 0.0.0.15 any range 16384 16383
!
ip access-list extended DATA_GOLD
remark Lista de Acceso que identifica el tráfico GOLD
permit tcp host 10.1.1.200 any
!
```

7.3.1.2.- Creación de las clases para las diferentes categorías de servicio

Las clases que clasifican el tráfico se configuran de la siguiente forma.

```
!
class-map match-all VideoC
 match access-group name VideoC
!
class-map match-all VoIP
 match access-group name VoIP
!
class-map match-all DATA-GOLD
 match access-group name DATA_GOLD
!
```

7.3.2.- Marcado de los paquetes por categoría de servicio

El marcado de los paquetes se realiza utilizando las clases definidas anteriormente y se aplica de entrada en todas las interfaces que miran hacia la LAN del cliente.

7.3.2.1.- Creación del policy-map CLASIFICACION

Esta configuración realiza el marcado de los paquetes

Ejemplo:

```
!
policy-map CLASIFICACION
 description Clasificacion y Marcado de paquetes segun servicio
```

```
 class VoIP
  set ip precedence 5
 class VideoC
  set ip precedence 3
 class DATA-GOLD
  set ip precedence 2
 class class-default
  set ip precedence 0
!
```

7.3.2.2.- Aplicación del policy-map a la interfaz

El marcado de los paquetes se debe aplicar de entrada en todas las interfaces que miran hacia la LAN del cliente.

Ejemplo:

```
!
interface FastEthernet0
 ip address 192.168.105.199 255.255.255.0
 service-policy input CLASIFICACION
!
```

7.3.3.- Caso especial: Marcado de paquetes de voz en el caso de un Voice Gateway

Si el router CE es un Voice Gateway, vale decir, el router tiene conectadas interfaces de voz (FXO, FXS, E&M, E1) el marcado de paquetes debe realizarse directamente en los "dial-peer voice" del tipo VoIP correspondientes.

Por ejemplo:

```
dial-peer voice 3 voip
destination-pattern 15..
session target ipv4:172.16.65.182
ip precedence 5
```

Algunas versiones de sistema operativo no permiten la configuración anterior, y en ese caso la configuración alternativa será:

```
dial-peer voice 3 voip
destination-pattern 15..
session target ipv4:172.16.65.182
ip qos dscp cs5 media
```

A través de ambas configuraciones, los paquetes correspondientes a VoIP ya van marcados con Precedence 5, por lo que pueden ser clasificados en la clase VoIP en el policy-map de salida.

7.3.4.- Modelado del tráfico (Traffic Shaping)

Se debe aplicar un modelamiento de tráfico hacia la salida a fin de evitar que la red MPLS descarte el exceso que está por sobre la clase de servicio contratada por cliente.

7.3.4.1.- Configuración de los parámetros del Shaping

Para lograr que el tráfico proveniente desde la LAN no supere el ancho de banda contratado, reflejado en la clase de servicio, se debe configurar un primer 'policy-map' llamado HACIA_RED_PADRE

```
!
policy-map HACIA_RED_PADRE
class class-default
shape average BWClase
!
```

Donde BW_{Clase} corresponde al ancho de banda definido en la clase de servicio contratada. Por ejemplo para una clase de servicio de BW_{Clase} = 2Mbps, la configuración será:

```
!
policy-map HACIA_RED_PADRE
class class-default
shape average 2000000
!
```

7.3.5.- Priorización del tráfico por categoría de servicio

La priorización propiamente tal se realiza en la sub-interfaz de salida hacia la red. Esta priorización queda definida en el policy-map de nombre "HACIA_RED_HIJO" que será configurado dentro del policy-map "HACIA_RED_PADRE". Este último será el que se aplica a la interfaz de conexión

hacia la red MS. Para el cálculo de los parámetros a configurar en el sistema de priorización se da por conocidos, aportados por el diseño previo, el valor de la intensidad de tráfico de las "aplicaciones críticas del negocio" (BW_{DG}), del número de canales de voz simultáneos (n) y del codec utilizado, del número de sesiones de Video Conferencia y de su codec (velocidad nominal) (BWV_{Cnom}).

7.3.5.1.- Configuración del máximo porcentaje reservable de ancho de banda

Los equipos router pueden asignar como máximo un cierto porcentaje de la tasa de acceso AR a las diferentes categorías de servicio, cuyo valor por omisión es un 75%.

Este valor se modifica con el comando de interfaz 'max-reserved-bandwidth XX', donde XX es el porcentaje máximo del 'bandwidth' de la interfaz a asignar con las clases. Este comando se aplica directamente en la interfaz de salida, dejando para nuestro caso un 95% de reserva.

Ejemplo :

```
!
int ethernet 0/0
max-reserved-bandwidth 95
!
```

NOTA: Este valor de 95% se considerará fijo para todo tipo de diseño.

7.3.5.2.- Creación de las clases por precedencia

La clasificación previa al encolamiento se realiza mediante la definición de las siguientes clases (configuración obligatoria)

```
!
class-map match-all Prec-3
match ip precedence 3
!
class-map match-all Prec-2
match ip precedence 2
!
class-map match-all Prec-5
match ip precedence 5
!
```

7.3.5.3.- Creación del policy-map de salida: configuración de la categoría VoIP (Precedence 5)

```
!
policy-map HACIA_RED_HIJO
description Esquema de priorizacion por tipo de IP Precedence
class Prec-5
priority BW1
!
```

Para la clase Prec-5 (correspondiente a VoIP) se destina tanto ancho de banda como canales de voz simultáneos vayan a ser servidos. Como referencia, se estima un consumo de 35[Kbps] por canal de voz al utilizar el codec G.729 El valor BW1 = n€35 se configura en la línea

```
priority 105 (BW1 = 105[Kbps])
```

7.3.5.4.- Creación del policy-map de salida: configuración de la categoría VideoC (Precedence 3)

En el mismo policy-map se configura la clase para el tratamiento del tráfico con precedencia 3 (categoría VideoC). Al interior de esta clase se debe especificar dos parámetros de formaobligatoria: "bandwidth" y "police"

```
!
policy-map HACIA_RED_HIJO
description Esquema de priorizacion por tipo de IP Precedence
class Prec-3
bandwidth BW2
police BW2-max
!
```

Para la clase Prec-3, que define el tratamiento para el tráfico de Video Conferencia, se asigna una ponderación alta para que pueda ser priorizado adecuadamente sobre el tráfico de datos. El valor para el parámetro 'bandwidth' corresponde al máximo valor de ancho de banda disponible, cuyo valor viene dado por:

$$BW_2 = 0.95 \cdot 1.25 \cdot BW_{Clase} - BW_1 - BW_3$$

donde el valor de BW3 es determinado en la siguiente sección.

El valor para BW2-max, que corresponde al máximo tráfico alcanzado por la sesión de Video Conferencia, se calcula como:

$$BW_{2\text{-max}} = 1{,}3 \in BW_{VCnom}$$

Es decir, se recortará el tráfico, por razones de evitar sobreventa del servicio, un 30% por sobre el valor nominal utilizado por la Video Conferencia. Por ejemplo, una Video Conferencia correspondiente a BW_{VCnom} = 384[Kbps], el valor para BW2-max resulta ser de 500[Kbps].

7.3.5.5.- Creación del policy-map de salida: configuración de la categoría DATA_GOLD (Precedence 2).

En el mismo policy-map se configura la clase para el tratamiento del tráfico con precedencia 2 correspondiente al tráfico de categoría Data-Gold. Al interior de esta clase se debe especificar el parámetros "bandwidth".

```
!
policy-map HACIA_RED_HIJO
description Esquema de priorizacion por tipo de IP Precedence
class Prec-2
bandwidth BW3
!
```

donde

$$BW_3 = BW_{DG}$$

7.3.5.6.- Creación del policy-map de salida: configuración de la categoría BE (Precedence 0)

Finalmente, en el mismo policy-map se configura la clase por defecto, clase que encausará todo el tráfico que no ha calzado en las clases anteriores. Utilizará todo el ancho de banda restante. Este tipo de tráfico también será descartable por la red ATM. Su configuración corresponde a

```
!
policy-map HACIA_RED_HIJO
class class-default
fair-queue
!
```

7.3.5.7.- Aplicación del policy-map "HACIA_RED_HIJO" dentro del policymap "HACIA_RED_PADRE"

Para el correcto funcionamiento de la priorización y del modelamiento de tráfico a un ancho de banda máximo, es necesario configurar anidados los policy-map que definen ambas tareas.

```
!
policy-map HACIA_RED_PADRE
class class-default
shape average 2000000
service-policy HACIA_RED_HIJO
!
```

7.3.5.8.- Aplicación del policy-map "HACIA_RED_PADRE" a la interfaz de salida hacia la red MPLS

```
!
int ethernet 0/0
 service-policy output HACIA_RED_PADRE
 max-reserved-bandwidth 95
!
```

7.3.6.- Ejemplo de la configuración del router CE

En el siguiente ejemplo se considera un acceso de clase de servicio BW_{Clase} = 2[Mbps], 3 canales de voz codificadas con G.729, una sesión de Video Conferencia de 384[Kbps] y un tráfico de aplicaciones críticas de 256[Kbps].
La configuración más relevante del router CE se muestra a continuación.

```
!
class-map match-all VideoC
match access-group name VideoC
!
class-map match-all VoIP
match access-group name VoIP
!
class-map match-all Prec-3
match ip precedence 3
!
class-map match-all Prec-2
match ip precedence 2
!
class-map match-all Prec-5
match ip precedence 5
!
class-map match-all DATA-GOLD
match access-group name data-gold
!
!
policy-map HACIA_RED_HIJO
description Esquema de priorizacion por tipo de IP Precedence
class Prec-5
priority 105
class Prec-3
bandwidth 1539
police 500
class Prec-2
bandwidth 256
class class-default
fair-queue
!
policy-map HACIA_RED_PADRE
class class-default
shape average 2000000
service-policy HACIA_RED_HIJO
!
policy-map Clasifica
description Clasificacion y Marcado de paquetes segun servicio
class VoIP
set ip precedence 5
class VideoC
set ip precedence 3
class DATA-GOLD
set ip precedence 2
class class-default
set ip precedence 0
!
interface FastEthernet0/1
ip address 192.168.105.199 255.255.255.0
service-policy input Clasifica
!
!
interface Ethernet 0/0
ip address 192.168.100.1 255.255.255.0
service-policy output HACIA_RED_PADRE
max-reserved-bandwidth 95
!
!
ip access-list extended VideoC
remark Regla que incluya el stream de Video
permit udp host 10.10.10.155 any range 3230 3235
```

```
!
ip access-list extended VoIP
remark Regla que incluya el trafico de Voz
permit udp 10.10.10.0 0.0.0.15 any range 16384 32767
!
ip access-list extended DATA_GOLD
remark Lista de Acceso que identifica el tráfico GOLD
permit tcp host 10.1.1.200 any
!
!
end
```

7.5.- Plataformas Routers como equipo CE

Las recomendaciones planteadas en este apartado consideran la capacidad de los equipos para realizar las funciones anteriormente descritas.

La siguiente tabla resume los modelos de equipos a utilizar para QoS MPLS junto con sus principales características.

Conclusiones

Luego de analizar los diferentes capítulos estudiados en este trabajo de titulación, se menciona lo siguientes comentarios finales.

El tráfico, en términos de bits por segundos, al interior de una red Lan y Wan ha crecido ostensiblemente en los últimos años ocasionando frecuentemente problemas de congestión. Dado que las redes de datos han crecido en capacidad y mejorado en tecnología, las diferentes aplicaciones de voz y datos han convergido sobre las redes de datos como un único medio de transporte.

Por tanto, para solucionar el problema del congestionamiento en la redes de datos, podemos aumentar el ancho de banda u Optimizar las redes. Una solución obvia a este problema es asegurar una capacidad tal en todos los enlaces de manera que nunca la velocidad de arribo de paquetes sea mayor que la capacidad del enlace. Pero aquí interviene nuevamente la economía. No es razonable económicamente sobredimensionar toda la red. Pero por otra parte si se realizara ¿por cuánto tiempo estaría sobredimensionada?, lo primero es una solución mas costosa y no es escalable en el tiempo, mientras que con el uso del QoS los paquetes son marcados para distinguir los tipos de servicios y los enrutadores son configurados para crear filas distintas para cada aplicación, de acuerdo con las prioridades de las mismas. Así, una faja de ancho de banda, dentro del canal de comunicación, es reservada para que, en el caso de congestionamiento, determinados tipos de flujos de datos o aplicaciones tengan prioridad en la entrega.

QoS es un Conjunto de técnicas para controlar: el retardo y su variación (jitter), el uso del ancho de banda y el descarte de paquetes, permitiendo la utilización controlada y administrada de la infraestructura de la red, otorgando una diferenciación de los recursos de red utilizados por diferentes tipos de flujos,.

Si no se diseña con cautela, una o más categorías de flujos pueden ver deteriorado su nivel de servicio

Referente al capitulo II, MPLS integra, sin discontinuidad, los niveles de trasporte y de red, combinando las funciones de control del routing con la simplicidad y rapidez de la conmutación.

- MPLS resuelve algunos de las problemas presentes en las redes IP sobre ATM:
  - Manejo de 2 redes separadas (IP/ATM)
  - Escalabilidad
- Mezcla la inteligencia de *routing* con la rapidez del *switching*.

Por estas características de la red Mpls, tanto como las empresas provedoras de servicios y sus clientes obtienen diversas ventajas tales como:
Para clientes:

- Accesos Universales: Accesos de distinto tipo, lo que no es posible en la MS. Ej. VPNs con accesos InterLAN, xDSL, F/R y GigE, que se comportan como una sola red "ruteada".
- Importante Capilaridad de Acceso: Uso de la red MS como acceso a la red MPLS
- Reducción de Costos: Eliminación o cambio de servicios costosos, hacia servicios Ethernet (10M, 100M, 1000M), que es más barato.

Para los Proveedores de servicios

- Incorporar a la oferta de Productos, una nueva solución, basada en tecnología de última generación.
- Permitir en el mediano plazo una reducción de los montos de inversión en el crecimiento de las plataformas tecnológicas (menores costos por puerta al ser tecnología Ethernet v/s ATM).
- Reducción de Costos por ancho de banda.
- Reducción de routers en Casa Matriz y cabeceras regionales (ruteo en red y sólo accesos Ethernet) -> menores costos en equipo.

De los diferentes accesos incorporados en este estudio, el más adecuado para las empresas, al momento de la elección, dependerá estrictamente del diseño de la red y la

capacidad de tráfico que se necesita soportar, siempre pensando en la escabilidad en el tiempo.

Por esto, es de gran importancia que los administradores de redes sepan dimensionar y gobernar adecuadamente sus redes.

REFERENCIAS BIBLIOGRAFICAS

ftp://ftp.isi.edu/in-notes/rfc3031.txt

http://www.ietf.org/html.charters/mpls-charter.html

http://www.isi.edu/rsvp/DOCUMENTS/ietf_rsvp-qos_survey_02.txt

http://www.ietf.org/internet-drafts/draft-rosen-rfc2547bis-02.txt.

PAPER Davie, B. and Rekhter, Y., "MPLS:
Technology and Applications"

Otra fuente de información sobre este tópico, es la página WEB de Daniel Awduche, cuya dirección
es: http://www.awduche.com
El Sr. Awduche es autor y co-autor de varios documentos sobre este tema.

http://www.oiforum.com

http://www.mplsrc.com

...ADSL Forum (http://www.adsl.com/)

http://www.cisco.com/univercd/home/home.htm

http://www.dsllife.com/tutorial/SHDSL_wp.pdf

http://www.etsi.org/technicalactiv/xdsl/xdsl%5Ftutorial.htm

http://www.earthweb-connect.com/what_is_broadband.htm

http://www.cisco.com/en/US/netsol/ns110/ns10/ns12/ns262/netqa09186a008009d557.html

http://www.cisco.com/en/US/partner/tech/tk652/tk698/technologies_tech_note09186a00800f6cf8.html

http://www.cisco.com/en/US/partner/tech/tk543/tk544/technologies_tech_note09186a00800a4754.html

http://www.cisco.com/en/US/partner/tech/tk39/tk48/technologies_tech_note09186a0080094ba1.Html

ANEXO A

Plataformas Routers como equipo CE para acceso xDSL

Las recomendaciones planteadas en este apartado consideran la configuración de los equipos para realizar las funciones anteriormente descritas.

La siguiente tabla resume los modelos de equipos a utilizar para QoS MPLS junto con sus principales características. Los router considerados corresponden equipamiento Cisco.

PLATAFORMA	IOS	FEATURE SET	Nombre IOS	RAM [MBytes]	FLASH [MBytes]
828	12.3(2)XE	IP PLUS	c828-sy6-mz.12.3-2.XE	24	8
827-4V	12.3(2)XC1	IP VOICE/PLUS	c820-sv6y6-mz.12.3-2.XC1	48	12
837	12.3(2)XC1	IP/FW/PLUS 3DES	c837-k903sy6-mz.12.3-2.XC1	48	12
1711	12.3(2)XC	IP/ADSL/FW/IDS PLUS IPSEC 3DES	c1700-k903sy7-mz.12.3-2.XC	64	16
1712	12.3(2)XC	IP/ADSL/FW/IDS PLUS IPSEC 3DES	c1700-k903sy7-mz.12.3-2.XC	64	16
1751	12.3(4)T2	IP/ADSL PLUS	c1700-sy7-mz.12.3-4.T2	64	16
1751-V	12.3(4)T2	IP/ADSL PLUS	c1700-sy7-mz.12.3-4.T2	64	16
1760	12.3(4)T2	IP/ADSL PLUS	c1700-sy7-mz.12.3-4.T2	64	16
2610XM-2611XM	12.3(4)XD	IP BASE	c2600-ipbase-mz.12.3-4.XD	64	16
2610XM-2611XM	12.3(4)XD	IP VOICE	c2600-ipvoice-mz.12.3-4.XD	96	32
2620XM-2621XM	12.3(4)XD	IP BASE	c2600-ipbase-mz.12.3-4.XD	64	16
2620XM-2621XM	12.3(4)XD	IP VOICE	c2600-ipvoice-mz.12.3-4.XD	96	32
2650XM-2651XM	12.3(4)XD	IP BASE	c2600-ipbase-mz.12.3-4.XD	64	16
2650XM-2651XM	12.3(4)XD	IP VOICE	c2600-ipvoice-mz.12.3-4.XD	96	32
c3640	12.3(4)XD	IP PLUS	c3640-is-mz.12.3-4.XD	96	32
c3640A	12.3(4)XD	IP PLUS	c3640-is-mz.12.3-4.XD	96	32
c3660	12.3(2)T4	IP PLUS	c3660-is-mz.12.3-2.T4	128	32

Ejemplos de IOS por modelo de router Acceso xDSL.

Plataformas Routers como equipo CE para acceso Frame Relay

Las recomendaciones planteadas en este apartado consideran las configuraciones de los equipos para realizar las funciones anteriormente descritas.

La siguiente tabla resume los modelos de equipos a utilizar para QoS MPLS junto con sus principales características.

PLATAFORMA	IOS	FEATURE SET	Nombre IOS	RAM [MBytes]	FLASH [MBytes]
1711	12.3(2)XE	IP/ADSL/FW/IDS PLUS IPSEC 3DES	c1700-k9o3sy7-mz.12.3-2.XE	64	16
1712	12.3(2)XE	IP/ADSL/FW/IDS PLUS IPSEC 3DES	c1700-k9o3sy7-mz.12.3-2.XE	64	16
1751-V	12.3(5)	IP/VOICE PLUS	c1700-sv3y-mz.12.3-5	48	16
1751-V	12.3(5)	IP BASE	c1700-ipbase-mz.12.3-5	48	16
1760	12.3(4)T	IP VOICE	c1700-ipvoice-mz.12.3-4.T	96	32
1760	12.3(4)T2	IP BASE	c1700-ipbase-mz.12.3-4.T2	48	16
2610-2613	12.3(5)	IP/H323 PLUS BASIC	c2600-is3x-mz.12.3-5	64	16
2610-2613	12.3(5)	IP	c2600-i-mz.12.3-5	32	8
2610XM-2613XM	12.3(5)	IP PLUS	c2600-is-mz.12.3-5	64	32
2610XM-2613XM	12.3(5)	IP	c2600-i-mz.12.3-5	32	8
c2620 c2621	12.3(3c)	IP	c2600-i-mz.12.3-3c	32	8
c2620 c2621	12.3(3c)	IP PLUS	c2600-is-mz.12.3-3c	64	32
c2620XM c2621XM	12.3(5)	IP	c2600-i-mz.12.3-5	32	8
c2620XM c2621XM	12.3(5)	IP PLUS	c2600-is-mz.12.3-5	64	32
c2650XM c2651XM	12.3(5)	IP	c2600-i-mz.12.3-5	32	8
c2650XM c2651XM	12.3(5)	IP PLUS	c2600-is-mz.12.3-5	64	32
c3640	12.3(5)	IP	c3640-i-mz.12.3-5	48	16
c3640	12.3(5)	IP PLUS	c3640-is-mz.12.3-5	96	32
c3640A	12.3(5)	IP	c3640-i-mz.12.3-5	48	16
c3640A	12.3(5)	IP PLUS	c3640-is-mz.12.3-5	96	32
c3660	12.3(5)	IP	c3660-i-mz.12.3-5	64	16
c3660	12.3(5)	IP PLUS	c3660-is-mz.12.3-5	96	32
c7200	12.3(5)	IP PLUS	c7200-is-mz.12.3-5	128	48

Ejemplos de IOS por modelo de Router para Acceso Frame Relay.

Plataformas Routers como equipo CE para acceso Mpls Nativo

Las recomendaciones planteadas en este apartado consideran la capacidad de los equipos para realizar las funciones anteriormente descritas.

La siguiente tabla resume los modelos de equipos a utilizar para QoS MPLS junto con sus principales características.

PLATAFORMA	IOS	FEATURE SET	Nombre IOS	RAM	FLASH
2610-2613	12.1(5)T15	IP PLUS IPSEC	c2600-is56i-mz.12.1-5.T15	48	16
2610 XM 2611XM	12.3(5)	IP PLUS	c2600-is-mz.12.3-5	64	16
C 3640	12.3(2)T4	IP PLUS	c3640-is-mz.12.3-2.T4	96	32
C 3660	12.3(5)	IP PLUS	c3660-is-mz.12.3-5	96	32
C 3725	12.3(5)	IP PLUS	c3725-is-mz.12.3-5	128	32
C 3745	12.3(2)T4	IP/H323	c3745-ix-mz.12.3-2.T4	128	32
C 1751-V	12.3(5)	IP/Voice PLUS	c1700-sv3y-mz.12.3-5	48	16
C 1760	12.2(15)ZL1	IP PLUS	c1700-sy-mz.12.2-15.ZL1	64	16
C 7200	12.3(5)	IP PLUS	c7200-is-mz.12.3-5	128	48
C 7200	12.1(5)T5	IP PLUS	c7200-is-mz.12.1-5.T5	128	16

Ejemplos de IOS por modelo de router Acceso Nativo MPLS.

Plataformas Routers como equipo CE

Las recomendaciones planteadas en este apartado consideran la capacidad de los equipos para realizar las funciones anteriormente descritas.

La siguiente tabla resume los modelos de equipos a utilizar para QoS MPLS junto con sus principales características.

PLATAFORMA	IOS	FEATURE SET	Nombre IOS	RAM	FLASH
2610-2613	12.1(5)T15	IP PLUS IPSEC	c2600-is56i-mz.12.1-5.T15	48	16
2610 XM 2611XM	12.3(5)	IP PLUS	c2600-is-mz.12.3-5	64	16
C 3640	12.3(2)T4	IP PLUS	c3640-is-mz.12.3-2.T4	96	32
C 3660	12.3(5)	IP PLUS	c3660-is-mz.12.3-5	96	32
C 3725	12.3(5)	IP PLUS	c3725-is-mz.12.3-5	128	32
C 3745	12.3(2)T4	IP/H323	c3745-ix-mz.12.3-2.T4	128	32
C 1751-V	12.3(5)	IP/Voice PLUS	c1700-sv3y-mz.12.3-5	48	16
C 1760	12.2(15)ZL1	IP PLUS	c1700-sy-mz.12.2-15.ZL1	64	16
C 7200	12.3(5)	IP PLUS	c7200-is-mz.12.3-5	128	48
C 7200	12.1(5)T5	IP PLUS	c7200-is-mz.12.1-5.T5	128	16

Ejemplos de IOS por modelo de router Acceso STM1 y MS

ANEXO B

Dimensionamiento de Ancho de Banda Y Uso de Codec

Una red de telefonía IP, conserva el modelo topológico empleado en el ámbito de los datos. Lo anterior se explica fácilmente, pues a la misma red de datos se le incorporan teléfonos IP, Gateways y Servidores.
Por lo tanto para dimensionar el uso de codec en una red y su acceso Wan, se deben considerar dos cosas.

- Tipo de Codec (más usados G711 y G729)
- Tipo de acceso (frame Relay, ATM, Ethernet, Etc.)

Consideraciones en el Tipo de Acceso

En el tipo de acceso a emplear hay que tener en cuenta la dimensión del encabezado y trailer que se le suma al “payload”.

- 20 Bytes para protocolo IP
- 8 Bytes para protocolo UDP
- 12 Bytes para protocolo RTP
- En caso de ocupar cRTP, lo anterior se reduce a 2 Bytes
- 6 Bytes par protocolo MultiLink PPP
- 6 Bytes para Frame Relay (F.R.F. 12)
- 1 Bytes para “end of frame “ para protocolo ATM
- 1 Bytes para “end of frame “ para protocolo Frame Relay
- 18 Bytes para Ethernet, lo que incluye F.C.S

El tipo de codec consiste en cuanto se comprimen los canales de voz para reducir su tasa de transmisión.

Informacion de Codec				Calculode Ancho de Banda					
Codec y bit rate (Kbps)	Codec Sample Size (Bytes)	Codec Sample Interval(ms)	Mean Opinion Score (MOS)	Voice y Payload Size(Bytes)	voice Payload Size (ms)	Packets Per Second (PPS)	Bandwitdth MP or FRF.12 (Kbps)	Bandwitdth w/cRTP MP or FRF.12 (Kbps)	Bandwidth Ethernet (Kbps)
G711 (64 Kbps)	(80 Bytes)	10 ms	4,1	160 Bytes	20 ms	50	82,8 Kbps	67,6 Kbps	87,2 Kbps
G729 (8 Kbps)	10 Bytes	10 Bytes	3,92	20 Bytes	20 ms	50	26,8 Kbps	11,6 Kbps	31,2 Kbps

Para establecer el dimensionamiento del ancho de banda en el acceso es necesario realizar el siguiente calculo.

- Largo del paquete de Voz(bits) = (largo del encabezado capa 2 + largo del encabezado IP/UDP/RTP + largo del payload) * 8

- PPS = (tasa de transmisión codec) / (Largo del Payload)

- BW = Largo del paquete de voz * PPS

=====>

BW Total = Ancho de banda * nº de Teléfonos