PROYECTO FIN DE CARRERA

TEMA: Network performance

TÍTULO: Quality of Service (QoS) in MPLS Networks

AUTOR: Roberto Jesús Rodríguez Pinto
TUTOR: Matti Puska
DEPARTAMENTO: Information Technology
CENTRO DE LECTURA: Helsinki Metropolia of Applied Sciences

Fecha de Lectura: Septiembre 2013
Calificación: 3

RESUMEN DEL PROYECTO:

Las redes de Telecomunicaciones han estado en constante expansión, y se han ido ofreciendo cada vez más servicios al usuario final. Los viejos mecanismos de transmisión de paquetes se han ido volviendo obsoletos debido a los nuevos requisitos de los servicios.

Inicialmente las redes se diseñaron para enviar dos tipos de tráfico: voz y datos. Estos datos no requerían de muchas garantías ya que no eran sensibles al retardo y a la pérdida de paquetes, normalmente estos datos no eran críticos, y se podían enviar sin necesidad de modelos de red avanzados.

Esto fue así hasta que llegaron los servicios de voz. Los servicios de voz eran bastante diferentes al modelo existente de paquetes, ya que la red tenía que de ser capaz de entregar una calidad mínima desde el emisor hasta el receptor. Para un envío fiable de voz, sólo se usaban redes que

operaban exclusivamente en tiempo real. El hecho de tener que usar redes diferentes para voz y para datos incrementaba muchísimo el coste tanto para los proveedores como para los consumidores.

Por tanto se empezó a estudiar la posibilidad de construir una infraestructura de red que diera soporte a ambos servicios, voz y datos (y también vídeo), y tanto los proveedores de red como los consumidores implementaron una red de conmutación de paquetes que fuera capaz de enviar datos así como tráfico en tiempo real.

Ahora bien, el tráfico en tiempo real, cuando se transporta sobre una red de conmutación de paquetes, se enfrenta a diferentes problemas, tales como retardo, pérdida de paquetes, y otros factores que perturban el servicio. Por tanto, el tráfico en tiempo real requiere de unas garantías de tráfico estrictas para que esto no suceda.

¿Por qué son tan estrictas estas garantías para el tráfico en tiempo real? Por ejemplo, si navegamos a través de la web, estamos solicitando una página web, y los datos se han de enviar desde un servidor hasta un cliente. Si durante la transmisión hubiera algún paquete que se extraviara, o se descartara, dicho paquete se volvería a mandar desde el emisor. Para el usuario final no es tan importante que la página se demore en cargar algunos segundos más de lo normal. Ahora bien, si el usuario estuviese hablando con alguien a través de un programa de VoIP, como por ejemplo Skype, uno o dos segundos de retraso en una conversación podrían ser catastróficos, ya que ninguno de los dos interlocutores serían capaz de mantener una conversación fluida. Para poder ofrecer soporte a estos nuevos servicios, las redes tuvieron que evolucionar. Para este propósito fue diseñado MPLS.

MPLS es un mecanismo de transmisión de paquetes que se usa en redes de telecomunicaciones de alto rendimiento que dirige y transmite datos usando caminos preestablecidos. En una red que implemente MPLS, se asignan etiquetas a los paquetes que circulan por dicha red. Las decisiones de reenvío se realizan únicamente en función de las etiquetas que portan los paquetes, sin que sea necesario examinar el contenido del paquete o su cabecera. Este proceso es mucho más rápido y efectivo que encaminar dichos paquetes usando los prefijos IP, y permite la creación de circuitos punto a punto a través de cualquier medio de transporte, y usando cualquier protocolo (siendo los más comunes IP y ATM). MPLS es hoy en día una solución clásica y un estándar para el transporte de información en las redes. Ha sido un gran avance a la hora de enviar la información de todo tipo usando redes de conmutación de paquetes.

MPLS también soporta ingeniería de tráfico (TE - Traffic Engineering). La ingeniería de tráfico es un mecanismo que consiste en seleccionar las mejores rutas para el tráfico de datos con objeto de balancear la carga de tráfico entre los diferentes enlaces de una red. En una red con múltiples caminos, los algoritmos de enrutamiento tales como OSPF o EIGRP se usan para calcular la ruta más corta, pero los mecanismos de ingeniería de tráfico son los que se encargan de decidir, en función de la sobrecarga de los enlaces, si finalmente se usa el camino más corto o bien, si la red está muy saturada, es necesario buscar rutas alternativas que no tengan tanta carga.

Pero todo esto no fue suficiente para poder ofrecer al tráfico en tiempo real las garantías que necesitaba. De hecho, estos mecanismo mejoraban la red, pero no realizaban cambios sobre cómo se trataba el tráfico. De modo que para poder ofrecer estas garantías a los servicios de voz en las redes de conmutación de paquetes, se fue necesario diseñar un mecanismo que pudiera asignar los recursos necesarios al tráfico en tiempo real. Para poder proporcionar estos servicios al tráfico de voz, se introdujo el concepto de Calidad de Servicio sobre las redes que operaban con MPLS.

La calidad de servicio (Quality of Service, QoS) es la capacidad de ofrecer distintas prioridades a diferentes aplicaciones, usuarios, o flujos de datos, o bien garantizar unos ciertos requisitos a dichos flujos de datos. El tráfico se distribuye en diferentes clases, cada una de las cuales se trata de forma diferente. De esta forma, el tráfico que posea la prioridad más alta se transmite primero, y en caso de haber suficiente ancho de banda, se transmitirá el tráfico restante. Obviamente esto es una aproximación al concepto, en la práctica la calidad de servicio está pensada para garantizar que cada tipo de tráfico se trate de la forma en que especifiquen sus condiciones.

Para poder cumplir este objetivo, hay diferentes mecanismos (o políticas) que permiten realizar control y ajustes sobre los flujos de tráfico. Las posibilidades son infinitas, dependiendo de cómo se quiera estructurar la red. Usando este mecanismo se pueden ofrecer al usuario las garantías necesarias para el tráfico en tiempo real, y distribuir el tráfico en categorías dentro de la red, ofreciendo un mejor servicio tanto para los datos en tiempo real como para los que no lo son.

Una red o protocolo que soporte QoS debe acordar un contrato de tráfico con la red y reservar una capacidad en los nodos de dicha red, por ejemplo durante la fase de establecimiento de la conexión. Durante esta sesión, la red puede monitorizar y/o controlar que se cumplen los requisitos, por ejemplo, la tasa de tráfico entregada, o el retardo, y ajustar dinámicamente las prioridades en los nodos.

Todo esto permite que la red se use de forma eficiente y que las aplicaciones que exigen comunicación en tiempo real (tales como las comunicaciones de voz, videoconferencias o incluso juegos en línea) tengan unas garantías de tráfico y que puedan operar con total normalidad de cara al usuario final que las está usando.

En conclusión, las redes han estado y están evolucionando muy rápido, y es muy importante diseñar los mejores métodos para enviar la información lo más rápido posible y al mismo tiempo incrementar la fiabilidad de las comunicaciones. Con la evolución constante de la tecnología, los routers y otros equipos de red poseen nuevas capacidades que años antes eran bastante difíciles de implementar.

Helsinki Metropolia University of Applied Sciences
Degree Programme in Information Technology

Roberto Rodríguez Pinto
Quality of Service in MPLS Networks

Bachelor’s Thesis. 18 May 2010
Supervisor: Matti Puska
Language advisor: Salla Petäjä

Helsinki Metropolia University of Applied Sciences Abstract

Author Title Number of Pages Date	Roberto Jesús Rodríguez Pinto Quality of Service (QoS) in MPLS Networks 53 (total number of pages including appendices) 18 May 2010
Degree Programme	Information Technology
Degree	Bachelor of Engineering
Principal lecturer	Matti Puska

Multiprotocol Label Switching (MPLS) is a packet-carrying mechanism, and it can be used to improve the performance of telecommunications networks. By using MPLS, data packets can be switched on the basis of labels rather than routed on the basis of destination address. MPLS supports different features like QoS, Traffic Engineering, VPNs, etc.

This thesis evaluates the performance of Quality of Service in a MPLS network. QoS is required when real time traffic flows are transported, because this traffic is more sensitive to delay and packet drops and should be treated with preference.

This thesis studies the use of QoS in a MPLS network, describes how QoS guarantees are assigned to the packets and data flows and also implements a network scenario in a lab environment.

Keywords	MPLS, IP, QoS, Real-time traffic

Telecommunications networks have been always expanding and thanks to it, new services have appeared. The old mechanisms for carrying packets have become obsolete due to the new service requirements, which have begun working in real time.

Real time traffic requires strict service guarantees. When this traffic is sent through the network, enough resources must be given in order to avoid delays and information losses.

When browsing through the Internet and requesting web pages, data must be sent from a server to the user. If during the transmission there is any packet drop, the packet is sent again. For the end user, it does not matter if the webpage loads in one or two seconds more. But if the user is maintaining a conversation with a VoIP program, such as Skype, one or two seconds of delay in the conversation may be catastrophic, and none of them can understand the other.

In order to provide support for this new services, the networks have to evolve. For this purpose MPLS and QoS were developed.

MPLS is a packet carrying mechanism used in high performance telecommunication networks which directs and carries data using pre-established paths. Now, packets are forwarded on the basis of labels, making this process faster than routing the packets with the IP addresses.

MPLS also supports Traffic Engineering (TE). This refers to the process of selecting the best paths for data traffic in order to balance the traffic load between the different links. In a network with multiple paths, routing algorithms calculate the shortest one, and most of the times all traffic is directed through it, causing overload and packet drops, without distributing the packets in the other paths that the network offers and do not have any traffic.

But this is not enough in order to provide the real time traffic the guarantees it needs. In fact, those mechanisms improve the network, but they do not make changes in how the traffic is treated. That is why Quality of Service (QoS) was developed.

Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

Traffic is distributed into different classes and each of them is treated differently, according to its Service Level Agreement (SLA). Traffic with the highest priority will have the preference over lower classes, but this does not mean it will monopolize all the resources. In order to achieve this goal, a set policies are defined to control and alter how the traffic flows. Possibilities are endless, and it depends in how the network must be structured.

By using those mechanisms it is possible to provide the necessary guarantees to the real-time traffic, distributing it between categories inside the network and offering the best service for both real time data and non real time data.

Las Redes de Telecomunicaciones siempre han estado en expansión y han propiciado la aparición de nuevos servicios. Los viejos mecanismos para transportar paquetes se han quedado obsoletos debido a las exigencias de los nuevos servicios, que han comenzado a operar en tiempo real.

El tráfico en tiempo real requiere de unas estrictas garantías de servicio. Cuando este tráfico se envía a través de la red, necesita disponer de suficientes recursos para evitar retrasos y pérdidas de información.

Cuando se navega por la red y se solicitan páginas web, los datos viajan desde un servidor hasta el usuario. Si durante la transmisión se pierde algún paquete, éste se vuelve a mandar de nuevo. Para el usuario final, no importa si la página tarda uno o dos segundos más en cargar. Ahora bien, si el usuario está manteniendo una conversación usando algún programa de VoIP (como por ejemplo Skype) uno o dos segundos de retardo en la conversación podrían ser catastróficos, y ninguno de los interlocutores sería capaz de entender al otro.

Para poder dar soporte a estos nuevos servicios, las redes deben evolucionar. Para este propósito se han concebido MPLS y QoS

MPLS es un mecanismo de transporte de paquetes que se usa en redes de telecomunicaciones de alto rendimiento que dirige y transporta los datos de acuerdo a caminos preestablecidos. Ahora los paquetes se encaminan en función de unas etiquetas, lo cual hace que sea mucho más rápido que encaminar los paquetes usando las direcciones IP.

MPLS también soporta Ingeniería de Tráfico (TE). Consiste en seleccionar los mejores caminos para el tráfico de datos con el objetivo de balancear la carga entre los diferentes enlaces. En una red con múltiples caminos, los algoritmos de enrutamiento actuales calculan el camino más corto, y muchas veces el tráfico se dirige sólo por éste, saturando el canal, mientras que otras rutas se quedan completamente desocupadas.

Ahora bien, esto no es suficiente para ofrecer al tráfico en tiempo real las garantías que necesita. De hecho, estos mecanismos mejoran la red, pero no realizan cambios a la hora de tratar el tráfico. Por esto es por lo que se ha desarrollado el concepto de Calidad de Servicio (QoS).

La calidad de servicio es la capacidad para ofrecer diferentes prioridades a las diferentes aplicaciones, usuarios o flujos de datos, y para garantizar un cierto nivel de rendimiento en un flujo de datos.

El tráfico se distribuye en diferentes clases y cada una de ellas se trata de forma diferente, de acuerdo a las especificaciones que se indiquen en su Contrato de Tráfico (SLA). EL tráfico con mayor prioridad tendrá preferencia sobre el resto, pero esto no significa que acapare la totalidad de los recursos. Para poder alcanzar estos objetivos se definen una serie de políticas para controlar y alterar el comportamiento del tráfico. Las posibilidades son inmensas dependiendo de cómo se quiera estructurar la red.

Usando estos mecanismos se pueden proporcionar las garantías necesarias al tráfico en tiempo real, distribuyéndolo en categorías dentro de la red y ofreciendo el mejor servicio posible tanto a los datos en tiempo real como a los que no lo son.

CONTENTS

1 Introduction

1.1 Motivation

Telecommunications networks are always expanding and new services are provided. The old mechanisms for carrying packets now become obsolete due to the new service requirements.

As the networks grows in size, the routers become very busy working with routing tables based on IP prefixes. Also, routers decide the shortest path between the source and destination, and when all the traffic is sent through the shortest path, it can create congestion in the network. In order to deal with this, new mechanisms to improve the networks are needed.

On the other hand, real time traffic requires certain guarantees. When real time traffic is sent through a network, it has to share the resources with other traffic types, and does not get enough resources to be routed without delay, jitter and congestion problems.

MPLS can provide an integrated environment to build up a converged network with the capability of providing QoS and Traffic Engineering. Companies are migrating towards MPLS, and enterprises are building their newer networks equipped with MPLS and shifting the older ones to the MPLS also.

It is considered that MPLS can provide a better support to the QoS. The network configured with MPLS can be used to handle performance factors of the network in a better way as compared to just IP routing.

1.2 Goals

The primary goal of this paper is to provide a knowledge of what MPLS is, and how it supports QoS needs. The project is also focused on analyzing the most important points and advantages of QoS in MPLS networks, such as Traffic Engineering (MPLS TE), Differentiated Services (DiffServ), Differentiated Services Code Point (DSCP), Per-Hop Behaviors (PHBs), and classification, scheduling and traffic policies.

This document will also offer a comparison between services of different classes in a congested network, plus a reference guide for design and set up scenarios with IP / MPLS focusing on the QoS components. Furthermore, instructions and material to support a lab exercise will be provided, as well as many ideas for future development.

2 Background information

2.1 Multiprotocol Label Switching

2.1.1 History of MPLS

MPLS was originally proposed by a group of engineers from Ipsilon Networks [1][2], and it was defined only to work over ATM. Cisco introduced a related technology named "Label switching" and they handed over to the IETF (Internet Engineering Task Force) for standardization. Finally, the IETF developed a protocol that combined features from several vendors.[3]

2.1.2 MPLS overview

Multiprotocol Label Switching (MPLS) is a packet-carrying mechanism used in high-performance telecommunications networks which directs and carries data using pre-established paths. MPLS makes it easy to create "virtual links" between distant nodes. It can encapsulate packets of various network protocols.

MPLS is a highly scalable, protocol agnostic, data-carrying mechanism. In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end-to-end circuits across any type of transport medium, using any protocol. The primary benefit is to eliminate dependence on a particular Data Link Layer technology, such as ATM (Asynchronous Transfer Mode), Frame Relay, SONET (Synchronous Optical Network) or Ethernet, and eliminate the need for multiple Layer 2 networks to satisfy different types of traffic.[4]

MPLS is nowadays a classic solution and a standard for carrying information in the networks. It has been a great solution for sending the information using packet routing. MPLS offers high-performance-networks: with speed, quality of service and resource reservation protocols.

2.1.3 MPLS architecture

MPLS network architecture is very similar to traditional IP network architecture, but MPLS is an extension of internet protocols and it offers a number of applications for the networks, e.g. Traffic Engineering (TE) or IP Virtual Private Networks (VPN).

MPLS as well as routers have two main components in their architecture, control plane and data plane. See the figure below.

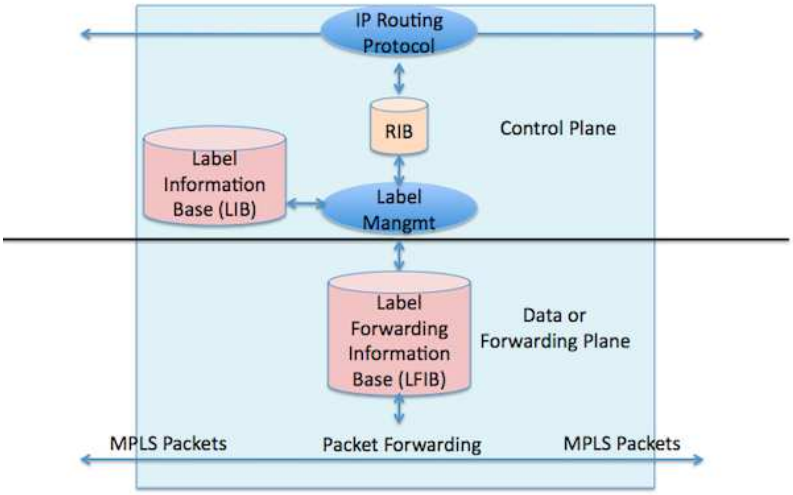

Figure 1: Control plane and data plane[5]

Control Plane: This is a classic component of MPLS architecture, and it exchanges the label between adjacent nodes and controls the routing information exchange. The Label Information Base (LIB) in an LSR holds all the local labels assigned by that LSR, and a mapping between those labels and the labels received from neighboring LSRs. Label Switched Paths (LSP) are established by the control plane and the labeled packets use them. For the efficient data transmission across the network, LSPs are set up dynamically, under the supervision of the control plane. Routing protocols and signaling protocols are the two main components of the control plane. Control plane exchanges routing information depending on the routing protocols, such as Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP) and Intermediate System to Intermediate System (IS-IS). Control plane exchanges labels using protocols such as Label Distribution Protocol (LDP) and Border Gateway Protocol (BGP). [6]

Data Plane: Data plane is a forwarding engine, which is not dependent on the routing protocols as well as label exchange protocols. Data plane uses the label forwarding information base (LFIB) table to store the information of the labels and forward the packets. The Label Forwarding Information Base (LFIB) holds only those local labels that are currently being used for forwarding. It also has a mapping between these labels and the outgoing labels received from neighbor LSRs, but additionally it also holds the egress interface to be used in forwarding, and the IP next hop address.

The routers in a MPLS network are called Label Switch Routers (LSR) and they can be core routers or edge routers. Also, the edge routers can be ingress routers or egress routers. See the figure below.

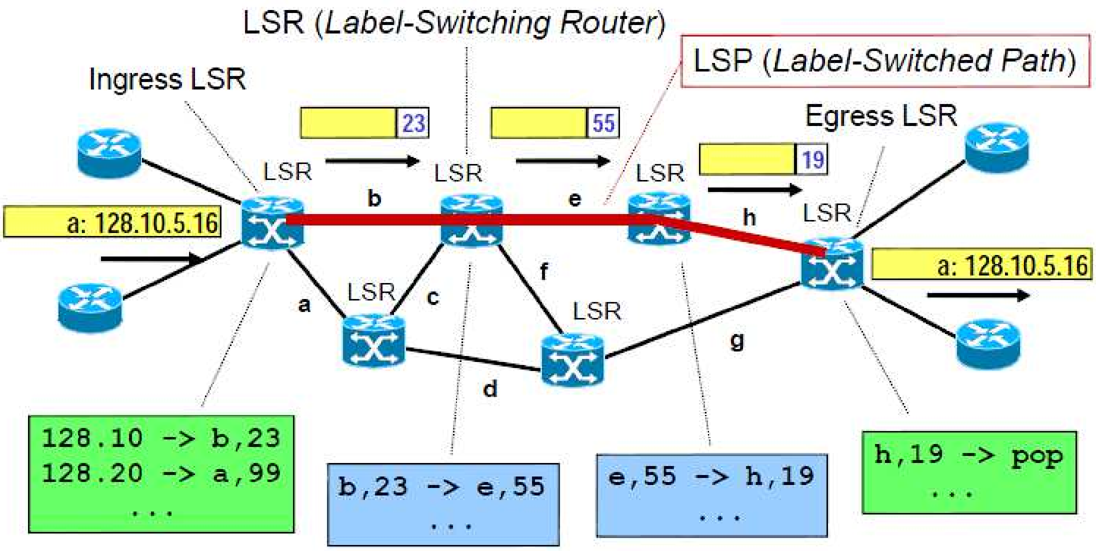

Figure 2: MPLS architecture [7]

Ingress LSR: The ingress LSRs receive non labeled packets from outside the MPLS network, insert labels to the packets and switch those labeled packets to the data link.

Egress LSR: The egress LSRs receive labeled packets from the MPLS network, and remove the labels from the packet and switches them to the data link.

Intermediate LSRs: The intermediate or core routers receive the labeled packet, swap the label if necessary, and switch the packets to the next LSR on the MPLS network. In a MPLS domain

the LSRs perform three common operations: push, pop and swap labels. In push operation, they insert the label or the label stack to the packet, and send the packet to the next LSR.
In pop operations, they remove the label or the label stack from the packet (which is a reverse of the push operation) and then they send it to the next LSR or outside the MPLS network.

When IP packets are received by the edge routers they perform the label related operations.
Labels are appended and removed into the IP header by the Label Edge Routers (LER). The IP lookups are also performed at the LER, because at the same time of appending the label the router performs a IP lookup to get the appropriate label corresponding to the IP address of the packet.

On the other hand when the packet is switched to the end, again the LER performs the IP lookup to get the IP address corresponding to the appended label in the frame. After getting the IP address the label is removed and the original IP packet is forwarded to the destination. The routers between the source LER and the destination LER are called Label Switch Routers (LSR). When a labeled packet is received by the LSR it swaps the label with the suitable label for the next hop and switches it to the next hop. A label lookup is performed on the LSR instead of IP lookup. The paths followed by the packets during transmission from the source to the destination are called Label Switched Paths (LSP).

2.1.4 Label Switched Paths

The path through which the labeled packet is traversed in MPLS network is known as the Label Switched Path, or LSP, and it consists of a sequence of LSRs. The labeled packets are switched through these LSPs in a MPLS network. The LSPs are traversed from the ingress LSR to the egress LSR, whereas the core or intermediate LSRs are located between them. The packets of the same class are aggregated as a traffic trunk, and this traffic trunk is assigned the same label.

To enhance the efficiency of the network, multiple LSPs are established throughout the network. The existing network is based on the two sided operation, which has also been adopted for MPLS. It is possible through the establishment of both upward LSP and downward LSP and is known as the “LSP pair".

In the traditional IP network, the route to forward the packet is calculated and the best is selected. In the MPLS network, the best LSP is selected from multiple unidirectional LSPs.[8]

2.1.5 Protocols in MPLS Networks

As in the traditional IP network, IP routing protocols are used to forward the packets but, in MPLS network, the LSRs use label switching as the forwarding mechanism. Label Switched Paths (LSP) are setup by label distribution throughout the network and the most common label distribution protocols are Label Distribution Protocol (LDP), Resource Reservation Protocol (RSVP) and Constraint-Based Label Distribution Protocol (CR-LDP).

2.1.6 Label Distribution Protocol

In MPLS network, packets are labeled and switched through the LSPs, and LSRs perform the swapping operation to switch the packets. A label is needed to distribute to all the adjacent routers. LDP was developed to distribute the labels throughout the network.

It can work with Interior Gateway Protocols (IGPs) like Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System to Intermediate System (IS-IS) and Routing Information Protocol (RIP) but with the exception of Border Gateway Protocol (BGP) because it carries exterior routes and is already a multiprotocol.

Groups of packets having the similar characteristics are considered in the same class, known as Forwarding Equivalence Class (FEC) and the same label is provided to these packets. A specific label switched path (LSP) can be used for the multiple Forwarding Equivalence Classes (FECs). Groups of packets switched through the same path and with the same treatment might constitute the same FEC.

The packet, which is supposed to be forwarded through MPLS network to the destination, is forwarded through the LSP. The ingress LSRs receive the IP packet, inserts the one or more labels and looks up the destination address according to the specific FEC, and forwards the packet.

The LSRs have an interior gateway protocol (IGP) running throughout the network. Intermediate LSRs swap the labels with the outgoing label and forward them. Egress LSRs strips off the labels and forwards them.

When a packet enters in an MPLS domain, the ingress LER adds a label to the packet and switches the labeled packet to the adjacent intermediate LSR. This operation is known as push operation. Intermediate LERs are responsible to swap the label and switch the packets to adjacent LSR; this is known as swap operation. Before exiting the MPLS network, the label is removed by the egress LER or transit router, this is called pop operation.

2.1.7 MPLS TE

According to [9], Traffic Engineering (TE) refers to the process of selecting the best paths for data traffic in order to balance the traffic load on the different links. Usually, routing algorithms (e.g. OSPF) calculate the shortest path available, and they put all the traffic into those links. However, most of the times the network has alternative paths to send the information, and traffic can be distributed among all those links. Traffic engineering is really important in networks where multiple parallel or alternate paths are available.

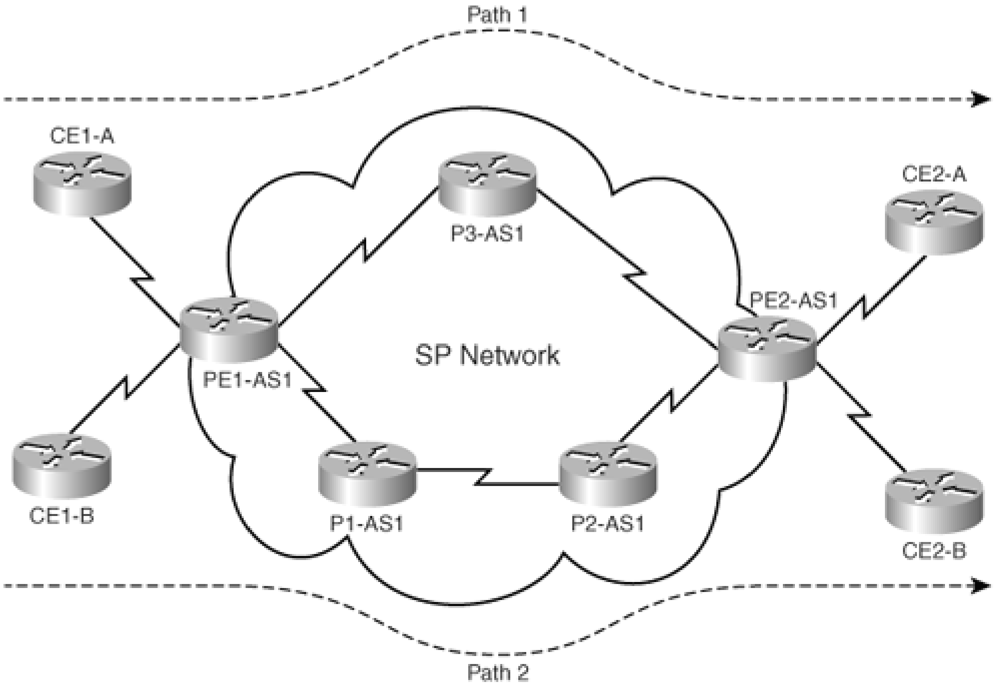

Figure 3: Two paths on a network [10]

Prior to MPLS TE, traffic engineering was performed either by IP or by ATM, depending on the protocol in use between two edge routers in a network.

TE with IP was mostly implemented by manipulation of interface cost when multiple paths existed between two endpoints in the network. In addition, static routes enabled traffic steering along a specific path to a destination.

With ATM networks, the solution is a lot more feasible; Permanent Virtual Circuits (PVCs) can be configured between source and destination with the same cost, but this would create a full mesh of PVCs between a group of routers. However, ATM has a problem in implementing TE: if a link or node goes down, the network is flooded with control messages.

The main advantage of implementing MPLS TE is that it provides a combination of ATM's TE capabilities along with the class of service (CoS) differentiation of IP. In MPLS TE, the head end router in the network controls the path taken by traffic to any particular destination inside the network.

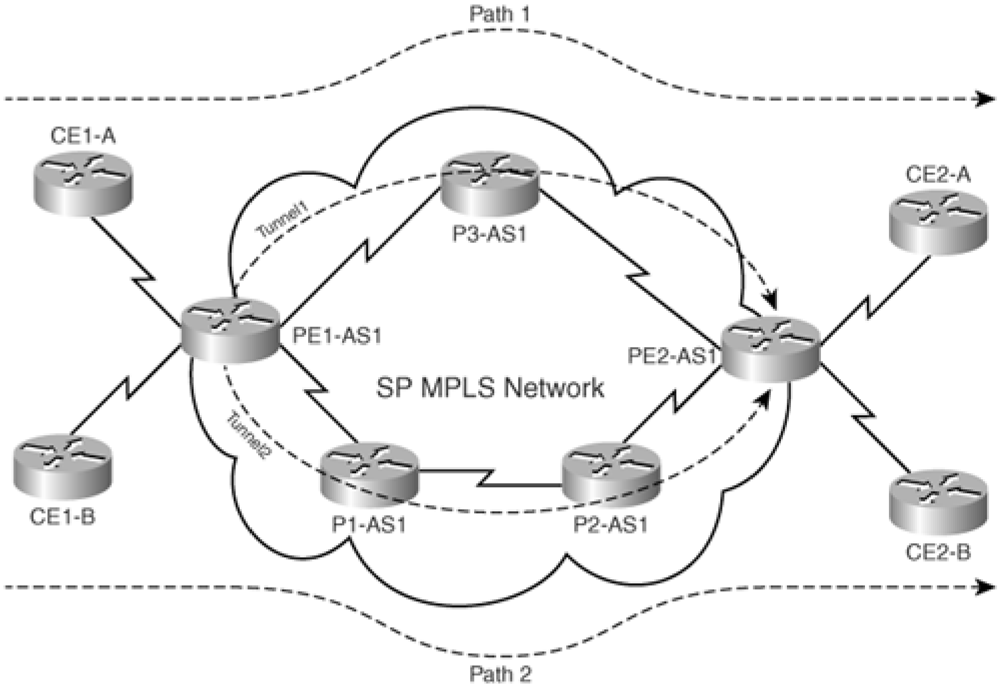

Figure 4: MPLS TE [11]

With MPLS, it is not necessary to create a full mesh of Virtual Circuits, and the network transforms into the label switched domain, in which the TE label switched paths (LSPs) or TE tunnels define paths that can be used by traffic.

2.2 Quality of Service

2.2.1 QoS overview

In the field of computer networking and other packet-switched telecommunication networks, the traffic engineering term Quality of Service (QoS) refers to resource reservation control mechanisms rather than the achieved service quality. Quality of Service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. Quality of Service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP, online games and IP-TV (Internet Protocol Television), since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication. In the absence of network congestion, QoS mechanisms are not required.[12]

2.2.2 Quality of Service in Multiprotocol Label Switching

Initially networks were designed to transmit two types of traffic, voice and data. The data does not require too much guarantees because it is not sensitive to delay and packet loss: usually this data is non critical data, not very sensitive to delay and drop, for example HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol) traffic, and it can be sent with best-effort network models.[13]

With voice is different, because the network has to be capable of delivering minimal quality from the sender to the destination. For reliable delivery of voice, only networks supporting real time traffic were used. Using different networks for data and voice increases the cost of enterprise.

So the organizations wanted to build a network infrastructure with support for both data and voice (and video also), then the service providers and the customers implemented a packet switched network which has the ability to send data as well as the real time traffic.

But real time traffic, when transported over a packet switched network, faces different problems, such as delay, packet loss, and other disturbance factors. Then, if we want to deal with voice in packet switched networks, we need a mechanism to provide the resources needed to the real time traffic.

In order to provide the fine grained quality to the voice, the Quality of Service with Multiprotocol Label Switching is introduced.

2.2.3 Improvements in QoS using Multiprotocol Label Switching

In IP networks, packets are forwarded on the shortest path selected, even when the shortest path is crowded and does not have enough bandwidth. As a result, congestion occurs, and this is not suitable when dealing with real time traffic, because this traffic is very sensitive to delay and packet loss and it needs priority over the normal data, which is less sensitive.

IP QoS is now combined with MPLS, and as a result, it is a new technology to overcome the deficiencies of IP QoS only. Multiprotocol Label Switching is used in order to select the packet forwarding path, to reduce the delay, jitter and packet loss problems. In MPLS, packets are not forwarded on the shortest path to the destination, instead packets are switched in such a way that the congestion does not occur and the transmission is considered more reliable.

Explicit paths are selected to forward traffic in MPLS, which improves the performance of the network. Generally, it combines the connection oriented and connectionless oriented model. It can be also implemented for both cell based (ATM) and packet based networks. The packets are traversed in the network or switched through the network according to labels, instead of routing the packets according to IP addresses.

As it is said before, the paths through which the packets are sent, are called Label Switched Paths (LSPs). Those LSPs are selected explicitly, and it is considered that RSVP (Resource Reservation Protocol) is the most compatible nowadays for signaling or for LSP selection.

2.2.4 DiffServ Aware Traffic Engineering

DS-TE (DiffServ Aware Traffic Engineering) is an extension made to Multiprotocol Label Switching Traffic Engineering (MPLS-TE) that make it DiffServ aware.

By using Traffic Engineering it is possible to guarantee enough bandwidth for each data link, so many authors think that QoS is not always necessary. However, in complex networks where voice and data is transmitted over the same channel, QoS is always necessary. With traditional protocols there is no way to make tunnels that assign bandwidth in the basis of the traffic classes. This is because the LSR maintain only one pool in a common interface for the packets that travel through the tunnels.

The DS-TE model implements TE classes in which the LSR have many pools grouped by class type. The RSVP is modified for check new tunnels and make sure they do not interfere with other tunnels. DS-TE uses the common resource reservation mechanism in the control plane. For the data plane, it is necessary to maintain queuing process mechanisms and packet drop policies in order to guarantee traffic classes.[14][15]

The bandwidth reservable on each link for constraint-based routing (CBR) purposes can now be managed through two bandwidth pools: a global pool and a sub-pool. The sub-pool can be limited to a smaller portion of the link bandwidth. Tunnels using the sub-pool bandwidth can then be used in conjunction with MPLS Quality of Service (QoS) mechanisms to deliver guaranteed bandwidth services end-to-end across the network.[16]

2.2.5 Class of Service

Class of Service (COS) is defined as a group of different types of traffic in which all of them have the same requirements. Different types of traffic flows are classified in order to get their QoS requirements. When CoS grouping takes place, the QoS parameters for different traffic classes are easily extracted out.

Weighted Fair Queuing (WFQ) and Class Based Queuing (CBQ) are used to support CoS.
WFQ supports relative bandwidth whereas CBQ supports fixed bandwidth allocation.

The behavior for an individual packet is determined by the precedence bit of the IP header, and usually is the IP CoS mapping to MPLS CoS. There are two methods to provide treatment to the IP packets from edge to core.

The first method to provide the CoS (Class of Service) mapping in the core is by copying the ToS (Type of Service) byte from IP header to the EXP field of the header in MPLS.
The second method is using signaling protocols in MPLS, like LDP and RSVP, and is preferred instead of the first one.

2.2.6 Traffic conditioning functions of QoS

When QoS is implemented, it plays an important role at the boundaries of the network. Inside the network the data packets are forwarded on per flow basis, however QoS on per flow basis is not scalable technique, because there are thousands of data flows and it is not possible to provide QoS to individual flows. The edge routers are responsible for the differentiation of non identical flows and apply the QoS policy. The quality of service policy is based on different conditioning functions described below.

Classification
It is a mechanism for dividing different flows of traffic into classes, in order to treat each class of traffic differently. In general similar data packets are considered to be in one class. These classes are identified according to certain parameters, the most common is classifying the packets according to source and destination IP addresses, port numbers, etc. Also, it is possible to use other header fields such as IP precedence and DSCP fields. TCP header can also be used for classifying the traffic, by recognizing the length of an incoming packet or by checking the MAC (Media Access Control) addresses of the source and destination.

After classifying a traffic flow, a predetermined policy can be applied to it in order to guarantee a certain quality or to provide best-effort delivery. This may be applied at the ingress point (the point at which traffic enters the network) with a granularity that allows the traffic-shaping control mechanism to separate traffic into individual flows and shape them differently [17].

When the traffic is classified, there are three significant classes to be treated.

High Priority of Sensitive Traffic: This is the traffic which requires QoS the most. It must be treated properly to minimize delay, jitter and other network problems. This class includes VoIP (Voice Over IP), video streaming, etc.

Best Effort Traffic: his class of traffic needs to be delivered fast, but the time factor does not affect so much. It is necessary to safely deliver this class to the receiver but his class does not need any time sensitive guarantees. This class includes email, HTTP traffic, etc.

Low Priority Traffic or Unnecessary Traffic: The data which does not need any priority or any significance, it is not required to deliver it to the appropriate destination.

Marking

Marking is a process of changing the packet QoS level according to a policy. This refers to mark the packet with a different QoS level, setting a different Differential Services Code Point (DSCP) value to enforce contracted service level[18]. The marking configuration is usually very tightly tied to the policing configuration. It is also possible to mark traffic as in-rate and out-of rate as a result of policing traffic.

Inside IP header there is a field called Type of Service (ToS), and three bits of ToS are used to indicate IP precedence. It specifies how the traffic will be treated in the network. The lower the precedence, the lower services will be offered; as well as the higher the precedence, more sensitive the traffic is and is treated with more services and care. The marking of IP precedence is done by the router or the application which is communicating with any other.

Marking is accomplished by another field called Differentiated Service Code Point (DSCP). It consists on the first 6 bits into the 8-bit Differentiated Services (DS) field of the IP packet header and IPv6 packet header. The DS field is the same as the ToS (Type of Service) field [19].

As an example, if the traffic which belongs to a certain class exceeds the reserved bandwidth for this class, it is stored in the router's buffers. If those buffers become full, the router starts to drop packets. But if the router is not transmitting too much data in other traffic classes, some packets could be sent to a low level class or even treated with best-effort model. So packets that were dropped before, now are sent to the network.

Metering

Metering refers to the measurement of the traffic, whether it meets the defined policy parameters or not. It keeps track of all the data packets and verifies the type of data traffic.

This is quite useful because sometimes it is necessary to keep a record of which bandwidth is used. For example, a company may have a fixed bandwidth but sometimes there are peaks on traffic and there is too much data being transmitted. A network provider can offer to the clients the possibility of exceed the bandwidth for a certain amount of time. It is necessary to make a metering process in order to keep a record of which traffic is exceeded and if the service is enough. Usually the companies are growing and they need more network capabilities, but only when it is really necessary. In order to determine when is necessary or not, metering process is here.

Shaping

Traffic shaping is a mechanism applied on a set of packets for delay them in order to control the volume of traffic sent into a network. It is usually applied at the network edges to control traffic entering the network. The metered packets are stored and delayed inside the buffer until they are compared using the policies or traffic profiles defined. If the data packets are in accordance with the defined profile, they are sent out to the interface. This process has a disadvantage, and it is that sometimes the buffers could be full and then drop packets is the only solution. In order to prevent this, the extra traffic of a certain class is remarked as a different category (lower class) and treated with best-effort methods if necessary.

Policing

Traffic policing is also called dropping. When a specific traffic does not meet the criteria defined in the profile, the traffic is dropped. Traffic shaping and policing are somehow similar to each other, but the difference between them is that shaping only delays packets, and policing can drop them.

2.2.7 QoS in MPLS network with DiffServ

MPLS forwards the packets on the basis of labels, and those packets are sent to the egress edge following different pre-selected LSPs (Label Switching Paths). The network load is balanced if several LSPs are discovered from any source to a destination. Traditional routing is based on the shortest available path, whereas MPLS switch the packets on the paths other than the shortest calculated, which minimizes congestion.[20]

As MPLS forwards the packets efficiently, another issue is under discussion: how the packet will receive the services it needs. Then IETF provided two more QoS models to deal with the problem of service guarantees.[21]

- IntServ (Integrated Services)
- DiffServ (Differentiated Services)

IntServ is flow based model, and reserves the exact amount of bandwidth needed to support the flow between source and destination. Those reservations are negotiated along the entire network, in all devices following the route. If a device has resources to support the flow, then a reserved path is set up. The protocol for sending messages in the forward direction is RSVP (Resource Reservation Protocol). Also, it sends messages in the reverse direction if all devices agree to reserve the resources needed.

However, IntServ has a disadvantage: the bandwidth cannot be reassigned. IntServ and RSVP must coordinate to set up an RSVP path, and then remember the information about the flow. This is a hard task on the Internet, where a router could handle millions of flows, so this model is not good for internet but best for smaller networks (or when used with DiffServ and another techniques).

DiffServ is a model that enhances the best-effort services. It differentiates traffic by different criteria; and it marks packets so that network nodes can provide different levels of service via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows. A policy management system controls service allocation.

In the context of MPLS, differentiated services model is considered as the best model for the solutions of the problems faced by the internet service providers. As MPLS switches the packets efficiently on the other hand the DiffServ model treats the packets in such a way that all the packets get the services they require.

RFC 2638 [22] states that a differentiated services architecture should "keep the forwarding path simple, push complexity to the edges of the network to the extent possible, provide a service that avoids assumptions about the type of traffic using it, employ an allocation policy that will be compatible with both long-term and short-term provisioning, and make it possible for the dominant Internet traffic model to remain best-effort."

For this purpose, packets with similar characteristics are included into DS behavior aggregates. Inside the domain of MPLS and DiffServ these behavior aggregates are treated according to the specific PHB.

PHB (Per Hop Behavior) is a forwarding behavior applied to a particular DS behavior aggregate. A DS behavior aggregate is a collection of packets with the same DSCP value crossing a link in a particular direction. When a behavior aggregate arrives at a node, the node maps the DSCP to the appropriate PHB, and this mapping defines how the node will allocate resources to the behavior aggregate.

2.2.8 Implementing Quality of Service Policies with DSCP

According to [23], the DiffServ architecture defines the DiffServ (DS) field, which supersedes the ToS field in IPv4 to make per-hop behavior (PHB) decisions about packet classification and traffic conditioning functions, such as metering, marking, shaping, and policing.

The RFCs do not dictate the way to implement PHBs; this is the responsibility of the vendor. For instance, Cisco implements queuing techniques that can base their PHB on the IP precedence or DSCP value in the IP header of a packet. Based on DSCP or IP precedence, traffic can be put into a particular service class. Packets within a service class are treated the same way.

The six most significant bits of the DiffServ field are called the DSCP (Differentiated Services Code Point. The last two Currently Unused (CU) bits in the DiffServ field were not defined for DiffServ but they are now used as Explicit Congestion Notification (ECN) bits. Routers at the edge of the network classify packets and mark them with either the IP Precedence or DSCP value in a DiffServ network. Other network devices in the core that support DiffServ use the DSCP value in the IP header to select a PHB behavior for the packet and provide the appropriate QoS treatment.

The picture below shows the structure of the Ethernet Frame and the IP Packet, and the location of the DSCP and IP Precedence fields.

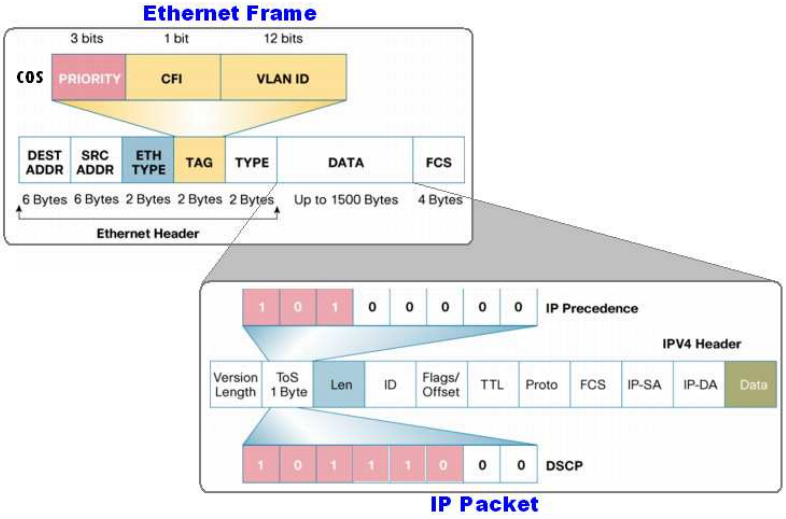

Figure 5: IP precedence and DSCP [24]

The standardized DiffServ field of the packet is marked with a value so that the packet receives a particular forwarding treatment or PHB, at each network node.

The default DSCP is 000 000. Class selector DSCPs are values that are backward compatible with IP precedence. When converting between IP precedence and DSCP, match the three most significant bits. For example, IP Prec 5 (101) maps to DSCP (101000)

The DiffServ standard utilizes also the most significant bits (DS5, DS4, DS3) for priority settings, but further clarifies the definitions offering finer granularity through the use of the next three bits in the DSCP. DiffServ reorganizes and renames the precedence levels into these categories.

Table 1: Precedence levels

Precedence level	Description
7	Stays the same (link layer and routing protocol keep alive)
6	Stays the same (used for IP routing protocols)
5	Expedited Forwarding (EF)
4	Class 4
3	Class 3
2	Class 2
1	Class 1
0	Best effort

RFC2598[25] defines the Expedited Forwarding (EF) PHB: "The EF PHB can be used to build a low loss, low latency, low jitter, assured bandwidth, end-to-end service through DS (DiffServ) domains. Such a service appears to the endpoints like a point-to- point connection or a "virtual leased line." This service has also been described as Premium service." Codepoint 101110 is recommended for the EF PHB, which corresponds to a DSCP value of 46.

With this system, a device prioritizes traffic by class first. Then it differentiates and prioritizes same-class traffic, taking the drop probability into account.

3 Implementation

A practical environment was developed in the laboratory and a scenario was built in order to test different traffic flows over a MPLS network. A theoretical study has clarified the benefits of QoS and MPLS. The obtained results show the behavior of different traffic flows over a network with those technologies.

Generally when an ordinary data is to be transferred in the network, it does not require any service guarantees. Performance degradation factors such a delay and packet dropping do not harm the ordinary data as compared to the sensitive traffic like voice and video.

The ordinary data packets when dropped can be re-transmitted by the transport protocol. When real time traffic is to be transferred it is considered much more sensitive for these factors. Longer delays, drops and jitter cause loss of important information which cannot be re-transmitted. As a result these types of applications require some service guarantees.

For this purpose QoS is configured in the networks to provide required guarantees to the sensitive applications.

3.1 Network setup

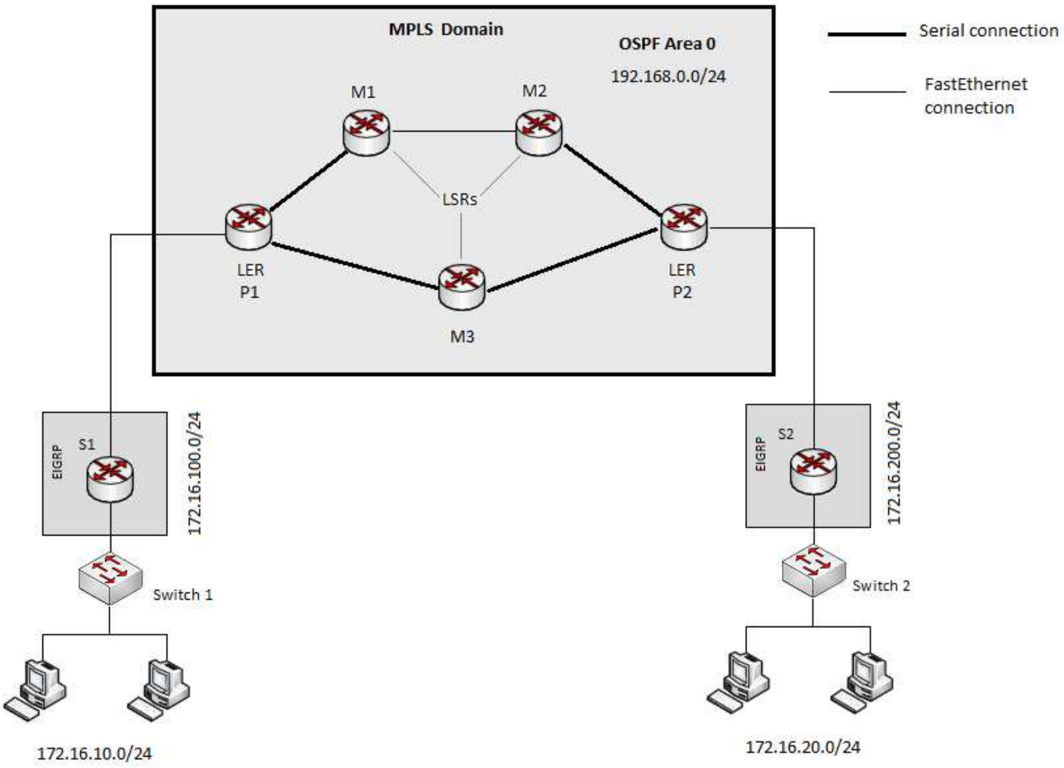

Figure 6:Network diagram

This network topology is a possible scenario between two offices of the same company. The left network could be one office, and the right-side network could be another office. Both branches are connected by a network which operates using MPLS technology.

The backbone MPLS consists of routers P1, P2, M1, M2 and M4. OSPF was chosen as the routing protocol, and all of the nodes were kept in area 0. OSPF has a fast convergence, low bandwidth utilization, authenticated routing updates, and many other advantages, so is the best option for larger networks[26]. At the left side, Network #1 has the router S1 connected to the MPLS backbone at P1, and Network #2 has the router S2 connected to the MPLS backbone via P2. This is a basic example of an MPLS network, it has multiple paths, and their length is different. For laboratory exercises, this is the best network setup.

Both these offices have EIGRP as the customer routing protocol running inside. The reason of choosing EIGRP is because as it is said in [27], it is very easy to configure, and does not require as much effort as OSPF in order to use it. Also, it works very well in networks up to a certain size. So it is a good option for the routers inside an office. Furthermore, in a real scenario the backbone network can be configured with OSPF, but other networks can use different routing protocols.

In order to provide full connectivity, both routing protocols were redistributed in each other in the edges of the MPLS network. Connectivity was checked making a ping test from one computer to another, and in order to check that the two routes were working, the interface in M4 was put down, so the traffic automatically switched to the other route, as expected.

Quality of service (QoS) was configured on the core network in order to provide better services for the traffic coming to and from both the sites. In order to limit the bandwidth in the P1-M3-P2 link, a serial interface was set between P1-M3 and also between M3-P2, and all the measurements were done in the serial interface of P1. Serial interface is slower than Fast Ethernet, and less amounts of packets are required in order to generate congestion. Those serial interfaces of routers P1 and P2 were configured with the QoS policies P2 for classifying and marking the incoming traffic.

Using both mechanisms we can provide the necessary guarantees to the most critical traffic, and distributing it between categories inside the network, offering the best service for both real time data and non real time data.

The following tables show the policies configured.

Traffic is divided into different classes, on the basis of those classes the traffic will be treated in a different way.

The main purpose of this classification is to identify which type of traffic is flowing inside the network. If any real time traffic is inside the network, it will be given the highest precedence. As a result, it will be treated inside the network according to the priority basis. The table below just indicates how classification is done: depending on the matching criteria, a router puts the incoming traffic into a specific class.

Table 2: Network policies

Network policies		
Class	Match criteria	MPLS EXP
Critical	Precedence 7	5
Interactive	Precedence 5	4
Web	Precedence 3	3
Class-Default	Precedence 0	0

This classification is performed at the edges of the MPLS network, between the ingress node and the egress node. The rest of the routers inside the MPLS network treat incoming packets according to the behaviors attached with the packets. Generally the most sensitive takes the benefit of the QoS policies more than the ordinary data.

Classification is usually done according to traffic types, like video, voice and the best-effort data. In the implementation work, the network traffic was classified into five classes on the basis of their types. It is just an example to show how policies work. Different protocols are classified into different classes and different priorities were given to them. According to their priorities they would be treated in the network in different way. The highest priority will be treated at first and it gets all the resources that it requires, then the other traffic classes are treated respectively.

In a traditional network where MPLS is not enabled, the QoS parameters are obtained through IP precedence and DSCP bits. When MPLS is enabled in the network, MPLS label is attached with the packet. When a packet traverses the MPLS network differed labels are attached and removed in the packet, from the source to the destination, and the packet is forwarded on the basis of the MPLS label. The router forwards the packet after checking the next hop label regardless of what the IP address is.

The question is, how QoS parameters are read by the router when the MPLS headers are appended with the IP packets? As discussed about the MPLS label and its structure, it consists of 32 bits in which there are experimental bits. When label is attached to the incoming IP packet to convert it into labeled packet, the IP precedence bits are mapped to the experimental bits of the MPLS header. When an IP datagram is covered with the MPLS label then the QoS parameters are also copied to the new labeled datagram. The experimental bits in the MPLS packet specify the QoS behavior of the MPLS packet.

According to [28] Internet Engineering Task Force (IETF) defines a series of priority classes according to the table below.

Table 3: Traffic priority classes [29]

Traffic priority class	IETF name
EF	Expedited Forwarding (EF)
AF4	Video/Priority Data (AF41, 42 or 43)
AF3	Mission Critical Data (AF31, 32 or 33)
AF2	Transaction Data (AF21, 22 or 23)
AF1	General Data (AF11 and 12)
BE	Default

For this lab example the priority used is AF1 (general data), and all the critical traffic was put on this class.

Table 4: Network policies

Network Policies		
Class	Match Criteria	Bandwidth (%)
MPLS-AF1	EXP 5	60%

The table above shows the policy maps that were configured on the core routers. When the traffic is classified and marked at the edge routers, it is forwarded to the destination through the backbone routers, and they have to provide the required QoS to the labeled packets. At the edge routers the real time traffic is classified in MPLS-AF1 class and MPLS EXP 5 is assigned. In the core network, in order to provide maximum bandwidth to the voice traffic, the above policies are configured on all routers to provide 60% of the link bandwidth for the packets with EXP 5.

For making the tests, different software was used in order to put different types of traffic on the network. For real time traffic the applications were VLC (for video streaming) and SJphone (for phone calls). VLC is the best option here because it allows sending a video stream between two computers using Real Time Protocol (RTP). For loading the network with non-critical traffic, JPerf[30] was used in order to send generic UDP (User Datagram Protocol) packets. And for the maintenance traffic, routers are OSPF messages, and Echo ICMP Request ad Response messages were sent manually.

3.2 Traffic Statistics

There is no point in analyzing the behavior of the network traffic if there is no congestion. All packets reach the destination without any problem. But this is different if we have limited bandwidth and too much traffic is put on the network.

Example 1

For the first example, the network was transferring UDP data for almost all of its capacity. Then, a user in one of the offices needs to show the video of a new product to some clients in the other office. At the same time, other two users between the offices decide to make a phone call.

In this case, the video communication and the phone call were established and some non-critical packets were dropped in order to give maximum priority to the video stream. A capture was made at some point during the transmission of the two types of data. Here are the statistics:

Table 5: Traffic statistics for example 1

Traffic statistics			
Class	Output bytes	5 minute offered rate (bps)	Packets dropped
MPLS-AF1	18160720	475000	9144
class-default	10710868	318000	1706

As it is observed in the output bytes field and in the bandwidth offered field, class AF1 (critical data) has a 60% of the total bandwidth. Also, some critical packets were dropped because the 60% limit was exceeded. This behavior is according to the policies set.

Example 2

In this example, a video communication was established, and a constant flow of Echo ICMP Requests was sent.

Table 6: Traffic statistics for example 2.

Traffic statistics			
Class	Output bytes	5 minute offered rate (bps)	Packets dropped
MPLS-AF1	45164805	1757000	42338
class-default	77727	177000	0

In this case the non critical data is below the 40% limit, and the network was dropping critical packets instead of non-critical ones. In the statistics, there was no packet drops on the default class, and all the Echo ICMP Responses were coming back.

3.3 Results

A scenario was implemented in the lab, to demonstrate the performance of MLS and QoS policies. The results obtained are summarized below.

- Practical implementation proved that the Quality of Service works well in combination with MPLS.
- If there is no congestion in the network, there is no need to implement QoS policies. But usually the network is a limited resource, and QoS is needed.
- QoS policies allow to create different classes of traffic, and give different priorities to them.
- Usually, highest priority is given to the critical traffic, such as video, phone calls, etc.
- If there is congestion on the network, traffic with the highest priority has the highest precedence.
- Implementing different traffic classes allow certain traffic types to have the maximum resources on the network.
- The statistics collected show that a proper QoS policy configuration is required in order to manage the most critical data.

4 Conclusion

The theoretical part of this study helps to understand QoS in a MPLS network, and have a look at its functionality. Guarantied QoS is required to transfer real time traffic over the network.

This document provides information about the advantages of QoS in a MPLS network, and offers a further look into some concepts such as Traffic Engineering (MPLS-TE), Differentiated Services (DiffServ), Differentiated Services Code Point (DSCP) and Per Hop Behaviors (PHBs), plus information about some traffic conditioning functions used in traffic management, like classification, policing, marking and shaping.
This document also offers a practical lab exercise for illustrating the concepts explained here, and gives some examples of how is the behavior of the network with those technologies.

All the necessary configurations of the routers have been recorded and presented at the end in the appendices section of the report, plus some useful information.

The statistics collected show that a proper QoS policy configuration is required in order to manage the most critical data, plus offer the best service to the user and adapt to the new technologies, which demands the best strategies in order to manage the traffic.

Networks are evolving too fast, and it is very important to design the best methods for sending the information as quick as possible and at the same time enhance the reliability of the network communications. As technology evolves, router and network devices have better technologies implemented and now they have abilities that a few years ago were quite difficult to implement.

Nowadays, traffic engineering is a key point on a network, and how to use alternate paths and distribute traffic is very important. For future implementations, the lab exercise offered in this document could be a testing scenario for distribute traffic and use the QoS techniques at the same time. There is a lot of work to do on this area yet, and new services will appear as well as better techniques for manage the new traffic profiles.

5 References

1. The phenomenon of Ipsilon. Technology Inside. February 8, 2007 http://technologyinside.com/2007/02/08/networks-part-2-the-flowering-and-dying-of-ipsilon/. Accessed May 25 2010.

2. A brief history of the development of MPLS. Linux Management. February 17, 2007. http://www.eastman-watch.cn/a-brief-history-of-the-development-of-mpls/. Accessed May 25, 2010.

3 INE CCIE blog. May 25, 2010. http://www.networkworld.es/El-IETF-y-la-UIT-aparcan-sus-diferencias-para-trabajar-junto/seccion-/articulo-185959 Accessed May 25, 2010.

4 DIATEL UPM. MPLS Documentation. February 2010. Accessed May 25, 2010.

5. INE CCIE blog. May 25, 2010. http://blog.ine.com/wp-content/uploads/2010/02/MPLS-Arch1.png. Accessed May 25, 2010.

6. Bell, John. osdir.com. June 1, 2010 http://osdir.com/ml/network.protocols.mpls/2007-08/msg00035.html.

7. DIATEL UPM. MPLS Documentation. February 2010. Accessed May 25, 2010.

8 DIATEL UPM. MPLS Documentation. February 2010. Accessed May 25, 2010.

9. The MPLS FaQ. MPLSRC. URL: http://www.mplsrc. com/faq2.shtml#MPLS%20Traffic %20Engineering. Accessed May 25, 2010.

10. MPLSRC http://ptgmedia.pearsoncmg.com/images/chap9_1587051990/elementLinks /09fig01.gif. Accessed May 25, 2010.

11. MPLSRC http://ptgmedia.pearsoncmg.com/images/chap9_1587051990/elementLinks /09fig02.gif. Accessed May 25, 2010.

12 QoS packet marking. Cisco. http://www.cisco.com/en/US/tech/tk543/tk757/tsd_technology_support_protocol_home.html. Accessed May 25, 2010.

13 QoS packet marking. Cisco. http://www.cisco.com/en/US/docs/routers/7600 /ios/12.2SR/configuration/guide/mplsqos.pdf. Accessed May 25, 2010.

14. Luis Morales. Investigación de redes VPN con tecnología MPLS. UDLAP. Date: May 16, 2006. http://catarina.udlap.mx/u_dl_a/ tales/documentos/lis/morales_d_l/capitulo3.pdf. Accessed May 25, 2010.

15. Nichols, K. "Definition of the Differentiated Services (DS Field) in the IPv4 and IPv6 headers" RFC2474. December 1998 Accessed May 27, 2010.

16. Cisco. MPLS Traffic Engineering - DiffServ Aware (DS-TE). www.aironet.info. Date: 2004. http://www.aironet.info/en/ US/docs/ios/12_2s/feature/guide/fsdserv3.pdf. Accessed May 27, 2010.

17. Traffic shaping. Wikipedia. http://en.wikipedia.org/wiki/Traffic_shaping# Traffic_Classification. Accessed May 25, 2010.

18. QOS Policing and Marking with Catalyst 4000/4500 IOS-Based Supervisor Engines. Cisco. http://www.cisco.com/en/US/products/hw/switches/ps663/products_tech_note09186a00800946 e9.shtml. Accessed June 2, 2010.

19. Differentiated Services. Wikipedia. http://en.wikipedia.org/wiki/DSCP#Classification_and _Marking. Accessed June 1, 2010.

20 Tom Sheldon and Big Sur Multimedia. Differentiated Services (DiffServ) Date: 2001 http://www.linktionary.com/d/diffserv.html. Accessed May 25, 2010.

21 F. Le Faucheur, L.Wu, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, J.heinanen, “Multi-Protocol Label Switching (MPLS) Support of Differentiated Services”, RFC 3270, May 2002.

22. K. Nichols, V. Jacobson, Cisco, L. Zhang. RFC2638. www.faqs.org. July 1999 http://www.faqs.org/rfcs/rfc2638.html. Accessed May 25, 2010.

23. Cisco. Implementing QoS policies with DSCP. http://www.cisco.com/en/US/tech /tk543/tk757/technologies_tech_note 09186a00800949f2.shtml. Accessed May 25, 2010.

24. www.pbxphreak.com. http://www.pbxphreak.com/QoS/images/COS-TOS-IP-Precedence-DSCP.PNG. Accessed May 25, 2010.

25. V. Jacobson, K. Nichols, Cisco Systems, K. Poduri, Bay Networks. An Expedited Forwarding PHB. www.ietf.org. June 1999 http://www.ietf.org/rfc/rfc2598.txt. Accessed June 2, 2010.

26. Iskra Djonova-Popova. OSPF. www.ceenet.org. http://www.ceenet.org/workshops99/ Iskra_Djonova-Popova/ospf99/sld032.htm. Accessed June 1, 2010.

27. Jeff Doyle. EIGRP vs. OSPF. www.networkworld.com. June 15, 2007. http://www.networkworld.com/community/node/16276. Accessed May 25, 2010.

28. Private IP service. www.verizonbusiness.com http://www.verizonbusiness.com/external/ service_guide/reg/cp_private_ip_service.htm. Accessed May 25, 2010.

29. Private IP service. www.verizonbusiness.com http://www.verizonbusiness.com/external/ service_guide/reg/cp_private_ip_service.htm. Accessed May 25, 2010.

30 Nicholas Richasse. JPerf. Google. http://code.google.com/p/xjperf/. Accessed May 14, 2010.

Appendices

Appendix 1: Configuration data

Core router (e.g. M3) #show running-config

```
M3_R3#sh run
Building configuration...

Current configuration : 1846 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname M3_R3
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
!
dot11 syslog
ip source-route
!
!
ip cef
!
no ipv6 cef
multilink bundle-name authenticated
!
```

```
voice-card 0
 no dspfarm
!
archive
 log config
  hidekeys
!
class-map match-all mpls-af1
 match mpls experimental topmost 5
class-map match-all prec5
 match  precedence 5
class-map match-any prec7
 match  precedence 7
 match protocol eigrp
 match protocol ospf
class-map match-all prec0
 match  precedence 0
class-map match-all prec3
 match  precedence 3
!
policy-map shapingdefault
 class prec7
   shape peak 120000
 class prec5
   shape peak 80000
 class prec3
   shape peak 30000
 class class-default
   shape peak 400000
policy-map output-qos
 class mpls-af1
   bandwidth percent 60
    random-detect
!
interface FastEthernet0/0
```

```
 ip address 192.168.150.254 255.255.255.0
 duplex auto
 speed auto
 mpls ip
 service-policy output output-qos
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.100.1 255.255.255.0
 no fair-queue
!
interface Serial0/0/1
 ip address 192.168.200.2 255.255.255.0
 mpls ip
 clock rate 2000000
 service-policy output output-qos
!
interface Serial0/1/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
router ospf 1
 log-adjacency-changes
 network 192.168.0.0 0.0.255.255 area 0
```

```
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end
```

Label Edge Router (e.g. P1) #show running-config

```
P1_R1#sh running-config
Building configuration...



Current configuration : 2118 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P1_R1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
```

```
no aaa new-model
memory-size iomem 10
!
dot11 syslog
ip source-route
!
ip cef
!
no ipv6 cef
multilink bundle-name authenticated
!
mpls ldp advertise-labels for 1
!
voice-card 0
 no dspfarm
!
archive
 log config
  hidekeys
!
class-map match-any critical
 match protocol rtp
class-map match-all mpls-af1
 match mpls experimental topmost 5
class-map match-all mpls-af11
 match mpls experimental topmost 5
class-map match-any interactive
 match protocol eigrp
 match protocol ospf
 match protocol icmp
class-map match-any web
 match protocol http
 match protocol smtp
!
policy-map set-PHB
```

```
 class mpls-af11
  set qos-group 1
  set discard-class 1
policy-map output-qos
 class mpls-af1
    bandwidth percent 60
     random-detect
policy-map markingpolicy
 class interactive
  set mpls experimental 4
 class web
  set mpls experimental 3
 class critical
  set mpls experimental 5
!
interface FastEthernet0/0
 ip address 172.16.100.254 255.255.255.0
 duplex auto
 speed auto
 service-policy input markingpolicy
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.100.2 255.255.255.0
 mpls ip
 clock rate 2000000
 service-policy input set-PHB
 service-policy output output-qos
!
interface Serial0/0/1
```

```
 ip address 192.168.30.2 255.255.255.0
 mpls ip
 clock rate 64000
 service-policy input set-PHB
 service-policy output output-qos
!
router eigrp 1
 redistribute ospf 1 metric 10000 100 255 1 1500
 network 172.16.0.0
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 redistribute connected subnets
 redistribute eigrp 1 subnets
 network 192.168.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end
```

office router, non MPLS (e.g. S1) #show running-config

```
S1_MID#sh run
Building configuration...
```

```
Current configuration : 865 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1_MID
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
!
interface Loopback0
 ip address 172.16.10.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 172.16.100.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.18.254 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.100.1 255.255.255.0
 clock rate 2000000
!
interface Serial0/0/1
```

```
 no ip address
 shutdown
 clock rate 2000000
!
router eigrp 1
 network 172.16.0.0
 no auto-summary
!
ip forward-protocol nd
ip route 172.16.100.0 255.255.255.0 172.16.10.0
!
ip http server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

Policy information example #1 in M3, serial interface

```
P1_R2#show policy-map interface serial0/0/1
 Serial0/0/1

  Service-policy input: set-PHB

    Class-map: mpls-af11 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: mpls experimental topmost 5
      QoS Set
        qos-group 1
          Packets marked 0
        discard-class 1
          Packets marked 0

    Class-map: class-default (match-any)
      80 packets, 5588 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

  Service-policy output: output-qos

    Class-map: mpls-af1 (match-all)
      13256 packets, 18160720 bytes
      5 minute offered rate 475000 bps, drop rate 68000 bps
      Match: mpls experimental topmost 5
      Queuing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/1706/0
      (pkts output/bytes output) 11550/15754200
      bandwidth 60% (926 kbps)
        Exp-weight-constant: 9 (1/512)
        Mean queue depth: 31 packets
        class    Transmitted     Random drop     Tail drop       Minimum      Maximum    Mark
                   pkts/bytes    pkts/bytes      pkts/bytes        thresh       thresh   prob

        0          0/0             0/0             0/0             20           40  1/10
        1          0/0             0/0             0/0             22           40  1/10
        2          0/0             0/0             0/0             24           40  1/10
        3          0/0             0/0             0/0             26           40  1/10
        4          0/0             0/0             0/0             28           40  1/10
        5       11550/15754200    170/231880    1536/2095104       30           40  1/10
        6          0/0             0/0             0/0             32           40  1/10
    7          0/0         0/0         0/0          34       40  1/10

    Class-map: class-default (match-any)
      13738 packets, 10710868 bytes
      5 minute offered rate 318000 bps, drop rate 170000 bps
      Match: any

      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 64/9144/0
      (pkts output/bytes output) 4592/4294453
P1_R2#
```

Policy information example #2 in M3, serial interface

```
P1_R2#show policy-map interface serial0/0/1
 Serial0/0/1

  Service-policy input: set-PHB

    Class-map: mpls-af11 (match-all)
      11904 packets, 964224 bytes
      5 minute offered rate 32000 bps, drop rate 0 bps
      Match: mpls experimental topmost 5
      QoS Set
        qos-group 1
          Packets marked 11904
        discard-class 1
          Packets marked 11904

    Class-map: class-default (match-any)
      328 packets, 22466 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

  Service-policy output: output-qos
```

```
Class-map: mpls-af1 (match-all)
  44116 packets, 45164805 bytes
  5 minute offered rate 1757000 bps, drop rate 1534000 bps
  Match: mpls experimental topmost 5
  Queueing
  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 42/42338/0
  (pkts output/bytes output) 1778/1809352
  bandwidth 60% (926 kbps)
    Exp-weight-constant: 9 (1/512)
    Mean queue depth: 41 packets
    class    Transmitted      Random drop      Tail drop        Minimum        Maximum     Mark
              pkts/bytes     pkts/bytes       pkts/bytes         thresh        thresh     prob

    0           0/0             0/0             0/0              20          40  1/10
    1           0/0             0/0             0/0              22          40  1/10
    2           0/0             0/0             0/0              24          40  1/10
    3           0/0             0/0             0/0              26          40  1/10
    4           0/0             0/0             0/0              28          40  1/10
    5          1868/1911584       187/190918     45614/46725271          30            40  1/10
    6           0/0             0/0             0/0              32          40  1/10
    7           0/0             0/0             0/0              34          40  1/10

Class-map: class-default (match-any)
  404 packets, 77727 bytes
  5 minute offered rate 177000 bps, drop rate 94000 bps
  Match: any

  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 404/29136
```