Multi-Protocol Label Switching To Support Quality of Service Needs

Master’s Thesis in Computer Network Engineering - 15hp

AMJAD IFTIKHAR
AOON MUHAMMAD SHAH

&

FOWAD LATIF

School of Information Science, Computer and Electrical Engineering
Halmstad University
Multi-Protocol Label Switching To Support Quality of Service Needs

Master Thesis in Computer Network Engineering – 15hp

Authors:

AMJAD IFTIKHAR
AOON MUHAMMAD SHAH
FOWAD LATIF

Supervisor:

OLGA TORSTENSSON
TONY LARSSON

School of Information Science, Computer and Electrical Engineering
Halmstad University
Box 823, S-301 18 Halmstad, Sweden

February 2010
Preface

At the beginning we would like to record our gratitude to Olga Torstensson and Tony Larsson for their kind supervision and support throughout our work. They started guiding us at the very early stages up to the final level. They made us able to come up with a solution that we were working for. It was such an honor for us to work under the supervision of Olga Torstensson and Tony Larsson. Their encouragement and guidance at various stages exceptionally inspire and enrich our knowledge. We gratefully acknowledge both of them for their support.

In addition we would like to thank our parents who always encourage us and empower us to work hard. It is our pleasure to say thanks to all of our friends and the seniors who guided us and helped us throughout this period.

At the end we would gratefully thank everyone who supported us to successfully complete our project work and helped us in our thesis directly or indirectly, at the same time we also apologize that it might not be possible to acknowledge one by one here.

Amjad Iftikhar, Aoon Muhammad Shah and Fowad Latif

Halmstad University, February 2010
Introduction

Abstract

Multi-Protocol Label Switching (MPLS) is a technique that can be used to improve the performance of a computer communication network. By use of 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 and VPNs etc.

This thesis evaluates the working and performance of MPLS and its support for Quality of Service. QoS is required in the network when real time traffic is transported.

In this thesis it is described, how QoS guarantees are assigned to the IP packets and how MPLS QoS environment differs from the traditional IP routing environment. MPLS QoS works as the IP QoS, but MPLS QoS enhances the capability of network as compared to the IP QoS based network.

The thesis studies the use of MPLS in an integrated environment with DiffServ QoS model and also implements MPLS QoS in a Lab environment to compare MPLS QoS with IP QoS. Real time traffic faces longer delays in IP QoS based networks. MPLS QoS reduces the delays in real time traffic transmission.

The study results and the practical implementations show that MPLS QoS provide much better results than simple IP QoS.
# Contents

**PREFACE** .................................................................................................................. III

**ABSTRACT** .................................................................................................................. IV

**1 INTRODUCTION** ....................................................................................................... 1

1.1 **MOTIVATION** ...................................................................................................... 1

1.2 **PROBLEM DEFINITION** ..................................................................................... 2

1.3 **GOALS** .............................................................................................................. 2

**2 QUALITY OF SERVICE** .......................................................................................... 3

2.1 **PROBLEMS DUE TO WHICH QUALITY OF SERVICE IS NEEDED** ................. 3

2.2 **HISTORY OF QUALITY OF SERVICE** ............................................................... 4

2.3 **IN A WELL DIMENSIONED NETWORK, QoS IS NEEDED** ............................... 4

2.4 **TRAFFIC CONDITIONING FUNCTIONS OF QUALITY OF SERVICE** ............ 5

**3 MPLS** ....................................................................................................................... 8

3.1 **REQUIREMENTS FOR CONVERGED MPLS CORE AND MPLS OBJECTIVES** .... 9

3.2 **MPLS BASED NETWORK VS IP BASED NETWORKS (EXISTING NETWORKS)** ... 10

**4 MPLS ARCHITECTURE** ............................................................................................ 11

4.1 **LABEL SWITCH ROUTERS (LSRs)** .................................................................... 12

4.2 **PROTOCOLS IN IP AND MPLS NETWORKS** .................................................. 12

4.2.1 **Protocols in the traditional IP network** ......................................................... 12

4.2.2 **Protocols in MPLS Network** ........................................................................ 13

4.2.3 **Protocols in edge devices** ............................................................................ 13

4.3 **LABEL DISTRIBUTION PROTOCOL (LDP)** .................................................. 15

4.4 **LABEL DISTRIBUTION** ................................................................................... 15

4.5 **LABEL SWITCH PATHS (LSPs)** ....................................................................... 18

4.6 **MPLS MODES** ............................................................................................... 19

**5 MULTI-PROTOCOL LABEL SWITCHING AND QUALITY OF SERVICE** ................. 20

5.1 **INTRODUCTION** ............................................................................................... 20

5.2 **OVERVIEW OF QUALITY OF SERVICE IN IP NETWORKS** ............................ 20

5.3 **IMPROVEMENTS IN QoS USING MULTIPROTOCOL LABEL SWITCHING** ....... 21

5.4 **CLASS OF SERVICE (COS)** ............................................................................ 22

5.5 **QUALITY OF SERVICE IN MPLS NETWORKS** ............................................ 22

**6 QUALITY OF SERVICE IN MPLS NETWORK WITH DIFFSERV SERVICES** .......... 25

6.1 **E-LSPS AND L-LSPS BANDWIDTH RESERVATION** ........................................ 26

6.2 **LABEL FORWARDING IN DIFFSERV LSRs** .................................................... 26

6.3 **MPLS AND DIFFSERV INTEGRATION FOR THE PROVISION OF QoS FOR REAL TIME TRAFFIC** ........................................................................... 27
Introduction

1 Introduction

Technologies are developing day by day. Enterprises adopt new technologies to upgrade their networks and services. Enterprises need to reduce their network costs by use of a single network infrastructure that can provide a wide range of services. Companies thus want to use a single network to transfer data, voice and video instead of three different networks to reduce the cost and effort. New network infrastructures are designed according to these requirements.

Data, voice and video are different types of applications. When an ordinary data is sent across any network, it does not require any service guarantees. If real time traffic is sent on same network, then it does not allow longer delays between the segments as compared to the data. The service guarantees required by any kind of traffic are called “quality of service” (QoS). Multi-Protocol Label Switching (MPLS) can be used to support QoS in the network for real time traffic.

MPLS load balancing across different links, which solves the major issue of congestion in the network. When traditional routing is used in the network, all the network traffic is routed through the shortest available path from the source to the destination. In case of failure of the shortest path new alternative and available choices are considered. In the case of MPLS, at the time of collecting routing information, different LSPs are built from the source to the destination and all available links are used to balance the load across different links.

MPLS can provide enhanced QoS compared to pure IP routing, by use and creation of Traffic Engineering and Virtual Private Network (VPN) services. MPLS enables the networks to provide service guarantees and minimize the delay in the case of real time traffic. When MPLS is used with differentiated services (DiffServ), it can provide better services than IP QoS. MPLS forwards packets on the selected LSPs, whereas the DiffServ helps to setup and treat the packets with the service guarantees which are required by these packets.

1.1 Motivation

Traditional routing faces issues related to delay, congestion and services that the traffic needs during its flow. Routers become very busy in working with routing tables. The routing is based on the IP prefixes. The router decides the path upon which the data packets are sent. The path selected by the router is the shortest path between the source and the destination. When all the traffic is sent through the shortest available path then it can create congestion in the network. On the other hand, when dealing with the real time traffic, it requires strict service guarantees. When real time traffic is sent through an IP network, it often does not get enough resources to the real time traffic to be routed without delay, jitter and the congestion problems.

MPLS in general can provide an integrated environment to build up a converged network with the capability of providing better QoS and traffic engineering. With the growing trends of today’s technology, the small, mid sized and larger companies are frequently changing their infrastructures. Companies are migrating towards MPLS. Keeping all this in mind, enterprises are setting their minds to build their newer networks equipped with MPLS, and towards shifting the older ones to the MPLS also.
MPLS to support Quality of service Needs

1.2 Problem Definition
In simple IP routing, routers builds up and uses routing tables. Data packets are routed on the basis of IP prefixes stored in routing tables. Routers perform lookups to find out the next destination of the data packets. This process generate delays, jitter and packet drops. Ordinary data can accept long delays but real time traffic requires guarantied QoS with low delay, jitter and packet drop etc. By just applying QoS on IP routed network the optimum performance can not be achieved.

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.

This thesis is aimed to compare MPLS QoS characteristics with IP QoS. This is done with the help of a detailed theoretical study and also by practical implementation to figure out that MPLS QoS provides better services than IP QoS.

1.3 Goals
The primary goal of this paper is to provide an in-depth knowledge of what MPLS is and how it supports quality of service needs. Real time traffic needs some services when it is routed through the network. The thesis is about what MPLS is and how it provides quality of service (QoS). It highlights the following issues and gives a detailed knowledge about the following.

- How MPLS can provide support to QoS demanding traffic.
- Comparison of MPLS and its applications with the other, traditional technologies.
- Practical implementation of MPLS and its comparison with IP routing.

This study will provide a detailed view of what kind of problems MPLS is going to solve, and how the different mechanisms of MPLS work. It also highlights the features of MPLS which make it different from the older technologies and how it combines with the DiffServ model to provide QoS.
2 Quality of Service

“A capability of service reliability and resource assurance to any type of traffic in a traditional network is called Quality of Service”. QoS provides different types of service levels to treat different application needs. It provides guarantees to cope with the problems in the network like delay, jitter, packet drop rate etc. Different networks are built in order to deal with different types of network traffic. For example, the different traffic types are voice, video and best effort traffic. In order to deal with different types of network traffics service providers have to build new networks. Today’s networks of ISPs (Internet Service Provider) and larger enterprises are based on IP networks. The individual IP networks are interconnected globally with each other which are known as a network of networks called Internet. Internet is a traditional IP network which makes the different categories of data to be transferred from one side to another within very short interval of time. As the corporate world is growing day by day which in turn makes the global network (Internet) to grow with it, as a result these intranets as well as internet has to deal with different types of traffic. Internet or IP network is considered as a converged network for every kind of data (i.e. traditional data, voice and video streaming etc.). A kind of traffic which does not need any service assurance or any priorities is call Best Effort traffic. The network which offers best effort services can not guarantee the services which are needed to any traffic flow. It only provides the best services for the traffic that a network can but it does not reserve any resources for the critical data, only it deals with best services to the critical traffic when there is no congestion in the network. If congestion occurs in the network it deals the critical traffic same as that of the non critical data [10].

2.1 Problems Due to which Quality of Service is needed

- In a best effort service a network can have different problems. When the traffic is dealt with best effort services, the packets arrive are not treated with any differentiation, any kind of services are not provided. Due to which Packet drop rate can increase.

- When the buffers in or queues in the network devices like routers and switches are filled the packets arrived at the time are dropped, as a result the receiver could not get the data as it requires. When a specific data packet is dropped, the receiver requests for the retransmission of that data packet. Hence the retransmissions introduce unwanted delays.

- When the data packets reside in the queues of the devices for longer time then the expected this unwanted delay sometime causes modification in the data which is unusual while dealing with real time applications such as voice and video.

- Jitter is another problem with the network traffic. It occurs when different delay in the data packets varies when they travel from the source to the destination. This variation in delays of different data packets is known as jitter. Jitter affects the quality of voice and video streaming also.

- On internet when data is sent in the form of collection of number of packets from the source to the destination it is not necessary for all the packets to be transmitted over a single path, instead packets use different paths to reach the destination. When the packets use different paths then the delay varies from packet to packet as a result the packet could
MPLS to support Quality of service Needs

not reach the destination in the order as they were delivered. So a mechanism is required by which they could be sorted out in a proper order.

- Error recovery is also needed to check the packets. It should be checked whether the packet received contains the content what they are originally delivered by the sender or they have been rendered during the transmission [11].

2.2 History of Quality of Service

When initially IP header was created, there was a byte in the header named as Type of Service Byte (ToS) which indicates the futuristic need of usage of this byte. The founders knew that the technology grow as faster as no one can think of it, so there must be a need of such kind of services. This (ToS) byte was reserved for provisioning of quality of service.

In early developments of internet the applications running over the internet ignored the ToS byte because it is not generally needed at the time. ToS byte was not marked by the applications and during forwarding of IP datagram the network devices like router did not interpret this field instead they forward it without providing any kind of service parameters. In this byte three bits were used as type of service and three bits were used as an IP Precedence. The higher the IP precedence the traffic would be treated more preferably and the lower the IP precedence then traffic would be treated with less preference.

But during the initial stages of the internet it was not used even it’s not needed in the network. Its importance was shown with the growth of internet, when the usage of internet became more commercial and the traffic routed through internet had been increased then the need of different types of services were also grown up.

2.3 In a well dimensioned network, QoS is needed

The discussion above was about the reasons due to which a network is in severe needs of a mechanism by which all the above discussed problem can be remove from the network, so that the network traffic would not be affected during it flow from the source to the destination. Now the question arises, that if the network is fully functioning and well designed and equipped with all the necessary resources then would there be any need of Quality of Service? As technology is growing day by day and the requirements are also changing with the passage of time. So if there would be a network with enough resource, but the needs of the users are also changing frequently, on internet there will be millions of users transferring there information from one place to another which needs some kind of services. The requirements are changing day by day, so it is not possible for a network designer to design them in advance or to accommodate such types of resources which would be needed in future, so the only application of Quality of services along with the other hardware changes would make it possible.

File uploading and downloading is increasing, voice and video chats are even going to be more common which needs some kind of priorities. A threat of viruses or some kind of malicious acts is also along with the other growing technologies. One can not guarantee that which type of attack is going to be the next one for our network. To deal with all this u need to prioritize the network traffic in such a way that each individual flow can be treated in a well mannered approach.
Using quality of service the different categories of data flows can be prioritized as well as
classified in such a way that they will be treated with differently. When traffic is characterized
in such a way they the users of different categories can easily be identified. Because the
service classification can help differentiate the users who need higher degree of services with
the users those need only moderate services. Some applications are considered as more
critical where as some are non critical, this classification made the difference between both
the areas more clear. In case of internet service providers, they can differentiate their services
on the basis of this classification.

In any network when in intrinsic area of the network is considered, its more likely considered
that the traffic targeted inside the network does not need any service priorities. But when
considering the connection to the outside network or internet, the links for connecting with the
internet are more expensive according to their capacity. If an organization is using a link with
the lower data rate and the network is not equipped with quality of service parameters the link
to the outside network can not be used in an efficient way. When quality of service parameters
will be configured in the network, then on the basis of these service parameters the different
flows are classified and prioritized according to the services they need as a result only in line
traffic will be sent on the link to the internet which does not create any burst in the link [10],
[11], [12].

2.4 Traffic Conditioning Functions of Quality of Service

When QoS is implemented in the network it plays an important role at the boundaries of the
networks. 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 such as classification, marking, policing and
shaping etc. In the next section all these features are briefly discussed.

- **Classification:**

  It is referred to as the division of different flows of traffic into classes. In general similar data
packets are considered to be in one class. These classes are identified on the basis of certain
parameters. Identification criteria can be based on different parameters. One and the most
common is to classify the packets on the basis of source and destination IP addresses, source
and destination port numbers etc. The identification of different classes can also be possible
on the basis of some other header fields such as IP precedence and DSCP fields. TCP header
can also b used for classifying the traffic, by recognizing the length of an incoming packet or
by checking the MAC addresses of the source and destination the traffic can b classified.

  Access list can be used to differentiate the traffic of different classes. When the traffic is
classified into different classes then there will be three significant classes appear to be treated.

  **High Priority of Sensitive Traffic:** The traffic which requires QoS the most means which
needs to be treated without delay, jitter and other network problems, such kind of class
includes VOIP etc.

  **Best Effort Traffic:** Best effort data is what which comes after the high priority traffic class
which needs to be delivered but the time factor does not affect the class. It is necessary to
MPLS to support Quality of service Needs

safely deliver this class to the receiver but his class does not need any time sensitive guarantees. Example of this class is any kind of email.

**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. This type of traffic includes any spam emails or any code generated by the attacker.

- **Marking:**

After classification the traffic is marked to identify the specific class. Marking refers to mark the packet with IP precedence or DSCP fields inside the IP header.

Inside IP header there is a field of Type of Service (ToS) byte, three bits of ToS are used to indicate IP precedence. It specifies that how a traffic will be treated in the network. Lower the precedence lower services will be offered as well as 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 of 6 bits out of which 4 are used to set the per hop behaviors (PHB) for the traffic and two them are unused. DSCP marking is used to specify PHB and the appropriate set of QoS parameters.

- **Metering:**

Metering refers to as 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. On the basis of this step the traffic is distinguished and forwarded for shaping as well as dropping. The traffic matching the defined parameters is scheduled for shaping where as the traffic which does not meet the specific condition is dropped out.

- **Shaping:**

Traffic shaping is a mechanism applied on the traffic after metering. It is usually applied to control the traffic entering the network. The metered packets are stored and delayed inside the buffer until they are compared with the policies or traffic profiles defined. If the data packets are in accordance with the defined profile they are then shaped to send out to the interface. Shaping also means to make the QoS related guarantees needed by the traffic possible for it.

- **Policing:**

Traffic shaping and policing are somehow similar to each other. Traffic policing is also called dropping. When a specific traffic does not meet the criteria defined in the profile the traffic is dropped [12], [13].
Multiprotocol label switching is the new technique for provisioning the high speed data transfer; fast convergence and scalability to the communication networks [1], [3], [5]. MPLS has become the best choice for packet transportation, which fulfills the multiple requirements of the next generation. Many more service providers are going to deploy the MPLS as a common backbone to achieve convergence of existing technologies such as X.25; ATM/frame relay (FR) and best effort IP with the new MPLS based services, such as IP VPN. It optimizes the transmission resources by providing the differentiated services to the communication networks. MPLS provides the routing intelligence and gives the significant improvement in the switching performance of the network, regardless of what the network architecture is, IP, ATM or it can be layer 2 technology based architecture. MPLS provides the scalability for the virtual private networks (VPNs) and maintains the end-to-end quality of service (QoS) [1], [3], [5]. When compared to the other network topologies, like full mesh topology, partial mesh topology and hub and spoke topology, MPLS provides optimal routing [1], [5]. Due to the valuable applications of MPLS like virtual private network (VPNs) and traffic engineering (TE) many larger data network service providers are deploying the MPLS in their networks [1], [2], [3], [5].

Fast label switching techniques and label swapping enhance the efficiency of packet forwarding. Initially, the development of MPLS was to provide the fast packet switching but current the main goal of MPLS technology is to support the quality of service (QoS) and traffic engineering (TE). MPLS is an IETF standardized mature technology, which is extensively used by major network operators because it supports traffic engineering. Initially, the major tasks were to solve the issue of scalability of network layer routing, enhance the network performance, provisioning of reliability. MPLS fulfilled the entire mentioned tasks, so now it is being deployed by all of the major networks [8].

Traffic engineering is an application of MPLS, which gives support to enhance the efficiency and reliability of the network operations and also optimizes the utilization of network resources. Most often, the network protocols used by conventional network are based on the shortest path algorithms, indicating only one path between source and destination. In MPLS, multiple paths can be chosen simultaneously for forwarding the packets, which improve the overall performance. MPLS provides explicit routing, which is helpful in traffic engineering and to increase the traffic oriented performance. MPLS manages the bandwidth and meets the service requirements for the next generation when it is used as a traffic engineering tool [9].

In fast growing environment, the world is moving towards omnipresent deployment of internet, which requires service assurance as quality of service and reliability. These requirements increase the need for re-designing the core network. The virtual private network (VPN) technology provides the solution to use the internet backbone for private data communication. MPLS offers the alternative tunneling mechanism of virtual private network (VPN). MPLS combines layer 3 routing and layer 2 switching for flexible architecture of VPNs. VPN technology replaces the expensive private bandwidth, which is used to provide the secure communication for the remote sites [7].

The innovative technology of MPLS has its many uses, including within the services provider as well as within the enterprise. By prioritizing the internet traffic efficiently, MPLS provides quality of service and traffic engineering, which increase the performance of emerging internet applications, such as voice and video traffic [B]. MPLS network offers the quality of
service (QoS) guarantees the data transport just like the services of ATM or frame relay (FR) and there is no need to dedicate a line for the data transmission. The main purpose of development and deployment of MPLS technology was to transfigure the internet and IP backbones networks to business class transport mediums which can handle the real time services. On the other hand best effort services are not capable of handling the real time services. The initial task for the service provider was to deliver the most needed traffic engineering capabilities, but the availability of traffic engineering application helps the MPLS for its deployment. The other key causes of deployment of MPLS technology are including low cost, detailed quality of service and greater control over the network. MPLS uses the constraint-based routing distributions protocol (CR-LDP) and resource reservation protocol (RSVP) as the signaling protocols for the traffic engineering.

In early computer networks technologies such as in circuit switching, it was best suited for uni-cast transmission of real time data or voice because it supports continuous bit stream on the physical link. The main drawback was only a single dedicated link, which is used for the whole communication. When it fails, it can be the cause of interruption for the communication through the single physical link. In the current era, only packet switched networks can fix the problem of single dedicated link for the transmission. Data is divided into small chunks, which are individually routed on the different links. On the failure of a link, packets are retransmitted. In IP-based network infrastructure voice and data communication can be converged [9].

3.1 Requirements for Converged MPLS Core and MPLS Objectives

The numbers of key elements required for designing the optimized converged MPLS network and the objectives of MPLS are as follow:

- The converged MPLS backbone must handle the multiple class of service, such as voice, data and multimedia services, and it must effectively and efficiently handle the multiple class of service (CoS). The converged MPLS backbone efficiently and effectively handles the multiple class of service (CoS).

- Most carriers need fault resiliency by path protection against network failures. MPLS has the feature of traffic protection when the network failure occurs. It provides the fast re-routing (FRR) in one-to-one or many-to-one as well as it carries out end-to-end path protection.

- For successful routing of traffic, it is advantageous, and preferred by the carriers to have an efficient network, which can meet the traffic demands. MPLS offers the load balancing mechanism to minimize the maximum load at the link and hence it increases the network performance and efficiency.

- To meet the requirements and service level agreement (SLA) for customers, it is important for the network that it must be cost effective. MPLS network is a low cost network, which meets the certain given performance targets.

- The designed network must meet the service level agreement (SLA) requirements for various class of service (CoS). The MPLS designed network meets the SLA requirements to the end users, which is the key differentiator for the carriers. Service level agreement with end customer can consist of packet loss, recovery time, service availability, delay and jitter attributes [6].
3.2 MPLS Based Network VS IP Based Networks (existing networks)

- MPLS can be described as the separate entity to IP and it works in conjunction with IP networks. In traditional IP networks, routing is performed on the basis of IP routing lookup. Forwarding is based on the routing table. MPLS, without the need of particular routing protocols, reduces the number of routing lookups by changing the forwarding criteria [3], [5]. In IP routing, packets are transferred hop by hop and the router makes the forwarding decision based on the information provided in the packet header [8].

- MPLS labels the packet and forwards those packets by using the labels. Labels are assigned at the edge routers and traverse throughout the network [3]. Packets with the same destination are aggregated in traffic trunk, and the trunk is assigned the same label [A]. An IP router decides a group of packets with the same destination and assigns the next hop to the destination. In MPLS, packets with the same destination are placed in forwarding equivalence class (FEC) and the label is assigned to FEC by LSR [8].

- Traditional IP packet forwarding has several limitations as it has limited capability to deal with addressing information, and traffic for the same destination is treated similarly, which is problematic for traffic engineering in IP based networks. MPLS technology supports the traffic engineering as the elegant solution to manage the bandwidth and to fulfill the requirements for the next generation. Traffic engineering offers efficient use of available network resources, which is helpful to accommodate highly interactive applications with low delay and packet loss [9].

- Labels that are assigned to the packets are always corresponding to the layer 3 destination IP addresses as the IP based routing having the same correspondence [3].

- Regardless of layers 3 protocols, it supports the forwarding of protocols. MPLS provides the traffic engineering to the IP networks [3]. MPLS is not designed to replace the traditional IP base switching, but it is designed to apply a set of rules to IP packets [9].

- MPLS ensures the provisioning of fast routing by using the labels. Only edge routers are responsible for the routing lookups, whereas the core routers forward the packets using the labels. In IP based networks, the intermediate routers are also responsible for the routing lookups, which is time consuming and the cause of slow forwarding as compared to MPLS based network [1], [2], [4], [3], [5].
4 MPLS Architecture

MPLS network architecture is very similar to traditional IP network architecture despite all the additional capabilities of the MPLS network. MPLS is an extension of internet protocols and it offers number of applications for the networks, e.g., traffic engineering (TE), IP virtual private networks (VPNs) and it also supports the integration of IP routing, layer 2 switching [2] [3] [5]. Earlier MPLS labeled only IPv4 packets but in Cisco IOS IPv6 packet can also be labeled. When a packet is labeled, it can not be distinguished either they are IPv4 packets, IPv6 packets or even layer 2 frames, they are labeled, when they are switched in MPLS domain [5]. MPLS has its two main components in its architecture, control plane and data plane.

- **Control Plane**
- **Data Plane**

**Control Plane:** Control plane is a classic component of MPLS architecture which exchanges the label between adjacent nodes as well as controlling the routing information exchange. Label switched paths (LSPs) are set up by control plane and these LSPs are used by the labeled packets. 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 and it depends 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 by using the label exchange protocols such as MPLS label distribution protocol (LDP) and border gateway protocol (BGP).

**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 labels. Data plane uses this LFIB to forward the packets.

MPLS network architecture consists of two types of label switch routers (LSRs). The core routers (LSRs) are known as the label switch routers and the edge routers (edge LSRs) [1], [3] are known as the edge label switch routers. Customer premises equipment is always connected to the edge LSRs running MPLS, but the customer sites are responsible for the IP forwarding rather than MPLS. Edge LSRs are carrier networks, and they will be connected with many IP networks, but MPLS between carriers is not essential. MPLS might be used in inter-carrier links [1], [3].
4.1 Label Switch Routers (LSRs)

Routers that support MPLS and can receive and transmit labeled packets on the data link are known as label switch routers (LSRs). MPLS network consists of three types of label switch routers (LSRs) [1], [5].

**Ingress LSRs:** Non labeled packets are received by ingress edge LSRs and it inserts the labels to the packets and switches them to the data link [1], [5].

**Egress LSRs:** The egress LSRs receive labeled packets, and strips off the labels from the packet and switches them to the data link. The egress LSRs are also the edge routers [1], [5].

**Intermediate LSRs:** The intermediate or core routers receive the labeled packet and, by applying the swap operation, they swap the label and switch the packets to the data link. In MPLS domain a LSRs perform three common operations, these are push, pop and swap. In push operation, it inserts the label or label stack to the IP packet and switches the packet to data link and the ingress LSRs are responsible for the push operation. In pop operations, it removes label or label stack from the packet and sends it out to the data link, which is a reverse of the push operation. The swap operation is conducted by the intermediate or core LSRs and, after swapping the label, the packet is sent out on the out-going link [1], [5].

4.2 Protocols in IP and MPLS networks

4.2.1 Protocols in the traditional IP network

MPLS uses the superset of IP routing protocols whereas, in traditional IP network, the subset of IP routing protocol is used in IP routers. In IP routers, the interior gateway routing protocol (IGP) tells the router how to reach the IP destinations, and IGP deals with the routing inside the IP network. There are many routing protocols used in traditional IP network as an IGP [1].

RIP: The routing information protocol (RIP) due to its many limitations, is no longer in use.
OSPF: Open shortest path first is broadly used.

IS-IS: intermediate system to intermediate system routing protocol is very similar to OSPF, both are link state routing protocols. IS-IS is commonly used in service providers [4] [1]. Routers under the same administration will use the same interior gateway routing protocol (IGP) but, for the communication with the different administrations, use the border gateway routing protocol (e.g., BGP). In traditional IP network, routing protocols build the routing tables, consisting of the IP prefixes. Packet forwarding is based on the IP destination address in IP network, and IP is also known as the forwarding protocol. There are some other protocols in the protocol stack used by the router; the most common protocols are transmission control protocol (TCP) and user datagram protocol (UDP) [1].

### 4.2.2 Protocols in MPLS Network

As in the traditional IP network, IP routing protocols are used to forward the packets but, in MPLS network, label switched routers (LSRs) use label switching as the forwarding mechanism. Switched paths are setup throughout the network called “label switched paths” (LSPs), which are setup by label distribution throughout the network. LSP is just like an IP prefix and is, stored in the forwarding tables of the several routers, setting-up of LSP according to the IP destination prefix is known as the hop-by-hop routed MPLS. The most common label distribution protocols in MPLS network are as follows [1], [5].

- **Label distribution protocol (LDP)**
- **Resource reservation protocol (RSVP)**
- **Constraint-based Label distribution protocol (CR-LDP)**

LDP is used as label distribution protocol, which supports hop-by-hop routed MPLS. Label encapsulation and packet forwarding in MPLS network is carried out by applying a label to the packet. In packet switching, a label is applied between layer 2 and layer 3 header, which is also known as the generic label encapsulation, whereas in asynchronous transfer mode (ATM), the label is applied as the virtual channel identifier (VCI)/virtual path identifier (VPI) to the cells of the packet [1], [5]. The two common modes of MPLS are packet-based MPLS and switch-based MPLS. The edge LSRs are packet-based MPLS because edge LSRs have the full layer 3 packet handling capacity. The LSRs lacking the capacity of handling layer 3 headers, and forward the packet by using layer 2 switching is known as switch-based MPLS [1], [3], [5].

### 4.2.3 Protocols in edge devices

The edge LSRs are usually connected with the traditional IP networks and MPLS networks. Hence, edge devices run all the protocols of traditional IP network as well as MPLS. A single routing protocol in LSR supports both MPLS and traditional IP links. In MPLS label encapsulation, a label is pushed to the IP packet and sent out across the network. At the edge LSRs label is popped from the packet and forwarded as the ordinary IP packet. MPLS also allows the multiple labels stack to the packet in traffic (TE) engineering or in virtual private networks (VPNs) [1], [5].

Firstly, point of presence (PoPs) is designed for the MPLS network to provide the reliability, choice of equipment is also considered as a factor of reliability. According to the requirements, the equipment is used to meet the needs because some of the edge label switch routers (LSRs) can support only IP or MPLS edge functions, whereas some of the edge label
MPLS to support Quality of service Needs

switch routers (edge LSRs) provide the ATM and frame relay switch functions. There are number of pop designs for MPLS networks, the typical designs are as follows [1].

A PoP can consist of a single LSR with number of access links or several LSRs as an aggregation device to provide the scalability. The use of several LSRs (aggregation devices) provide a number of advantages like it reduces the routing protocols, prevents the local traffic inside the same PoP and it also reduces the number of links and virtual circuits in ATM and frame relays in MPLS networks [1].

Designing of IP routing for MPLS network is carried out by label switch paths (LSPs), like interior gateway protocol (IGP), it provides the routes for the traffic in IP routing. The interior gateway protocol (IGP) treats the MPLS network as the traditional IP network [1], [5]. MPLS traffic engineering (TE) uses the link state routing protocols such as intermediate system to intermediate system (IS-IS) or open shortest path first (OSPF) as the interior gateway protocols (IGP) because the distance vector routing protocols (RIP) do not support the traffic engineering (TE) in MPLS [1], [3], [5].

Switch based LSRs can be used as the area border routers, whereas switch based LSRs do not support the route summarization [1], [5]. Many of the issues in designing MPLS and traditional IP networks are similar with the exception of the provisioning of the label space. LSPs are assigned to the IP destination and a number of LSPs is carried out on a single link. LSPs are built corresponding to IP destination prefixes, which is known as the “hop-by-hop” routed MPLS. Labels are not required for all of the destination prefixes but, after the filtering of the forwarding table, labels are assigned to the destination prefixes [1], [5].

Label space in MPLS network is dependent on the capabilities of the equipment which is used in the network. In MPLS network, labels are merged on a single link of LSP [1], [5]. Many LSPs are carried out on a single link, different LSPs to a single destination can be merged together [3]. Hence, only one label is required for the destination [1], [5].

![Figure 2: General MPLS Architecture](image-url)
**4.3 Label Distribution Protocol (LDP)**

In MPLS network, packets are labeled and switched through the LSPs and label switched routers (LSRs) perform the swapping operation to switch the packets. A label is needed to distribute to all the adjacent LSRs. Label distribution protocol (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, BGP carries exterior routes and is already a Multiprotocol. BGP also carries label information and distributes prefixes between different autonomous systems [1], [5].

**Label forwarding instance base:** The label containing LIFB are used to forward the label throughout the MPLS network. After labeling the packets, they are switched to the particular LSPs [1], [5].

**MPLS payload:** In MPLS network, intermediate routers do not have the information about the MPLS payload because they do not need to know about payload to switch the packets to corresponding LSP. Required information to switch the packet is in the label. To make a forwarding decision, the intermediate router looks at the label and might not have the information about the MPLS payload. In MPLS domain the labels of all the packets are removed at egress routers. So egress routers must know about the MPLS payload because they forward the payload [1], [5].

**Forwarding equivalence class:** Group of Packets having the similar characteristics are considered in same class, same label is provided to these packets, that class is known as forwarding equivalence class [5]. A specific label switched path (LSP) can be used for the multiple forwarding equivalence classes (FECs) [3], [5]. Group of packets switched through the same path and with the same treatment might constitute the same FEC [5].

**4.4 Label Distribution**

The packet, which is supposed to be forwarded through MPLS network to the destination, is forwarded through the label switched paths (LSPs). The ingress LSRs receive the IP packet, inserts the one or more labels and looks up the destination address and forwards the packet. The LSRs have an interior gateway protocol (IGP) running throughout the network. Intermediate LSRs swap the label with the outgoing label and sends them out. Egress LSRs strips off the labels and forwards them to the on going way. The all of the adjust LSRs in the network must know the accurate topology of the label that which label should be best suited for corresponding prefix. When a packet enters in an MPLS domain at ingress router, it adds a label to the packet and switches the labeled packet to the adjacent intermediate LSR, this operation is known as the “push operation”. Intermediate routers are responsible to swap the label and switch the packets to adjacent LSR; this is known as “swap operation”. Before reaching to the destination, a label is stripped off by the egress router or transit router, this is called “pop operation” [1], [5].

Label allocation: In MPLS domain a router has two main functions including label allocation and distribution, which are accomplished in four steps. The routers in MPLS domain exchange information using standard protocols including open shortest path firth (OSPF), interior gateway protocol (IGP) and IS-IS as the interior gateway protocol. Labels are generated and assigned to the each IP prefix for the particular destination that is in the routing
MPLS to support Quality of service Needs

Table. After assigning a label to the IP prefix, it is stored in the label information base (LIB) table. The locally generated labels are propagated to the adjacent routers. These labels from the FIB (forward information base) and LFIB tables can be used as the next hop. The LIB, LFIB and FIB databases, based on received labels are built in each LSR, which contain label information. Label distribution protocol (LDP) uses the label information base (LIB) database, which is located in control plane. A significant label is assigned to a prefix in LIB table, which is used to map with the next hop label that is learned from the downstream LSRs. On the other hand, LFIB database in the data plane is used to forward the labeled packets. The local labels, which were previously advertised to the upstream neighbors, are mapped to the received labels from downstream neighbors. Unlike to LFIB, the FIB database in data plane is used to forward the unlabeled packets. Network topology is advertised to the routers in the network by interior gateway protocol (IGP). Any of the routers in MPLS domain can first generate a label for the corresponding destination. For example, router B generates a label 30 and assigns it to IP to reach the network X. The assigned label to a prefix for network X is stored in LIB. The LFIB containing the local label is used to make the forwarding decision. However in the example, the action remains untagged because the router B has not received the label yet for network X from the downstream router [25], [26].

![Figure 3: Label Allocation](image)

Label distribution and advertisement: MPLS imposes the label to the packets and these labels are exchanged between the adjacent routers. LDP in control plane is used to exchange the labels and stores them in the label information base (LIB) table. When a local label is assigned by an LSR, it is propagated to the adjacent routers.
After receiving update from router B, the adjacent routers A, C and E fill their LIB, LFIB and FIB tables. Label 25 for network X is stored in LIB as shown in the diagram. Label 25 is attached to the corresponding IP in FIB, and packets are forwarded as labeled packets. The local labels in LFIB are mapped to the outgoing label 25 and then they are forwarded. Router B will also receive the label from downstream adjacent router as a next hop label.

Router B maps the IP for network X FIB as well as it maps the local label 25 in LFIB to the label 47 received from the downstream router. Similarly, router E will also assign a label for network X. Router allocates a label 26 for network X, and it has received 25 from B and 47 from D to reach the network X [25], [26].
**4.5 Label Switch Paths (LSPs)**

The path through which the labeled packet is traversed in MPLS network is known as the label switch paths, or LSPs, and it consists of a sequence of LSRs. The labeled packets are switched through these LSPs in MPLS network. The LSPs are traversed from the ingress LSRs to the egress LSRs, whereas the core or intermediate LSRs are located between ingress LSRs and egress LSRs [1], [5]. The packets of the same class are aggregated as a trunk, and this traffic trunk is assigned the same label.

**LSP selection method in MPLS network:** In MPLS network, packets are transferred using labels along the label switch paths (LSPs), which are established between the ingress LSRs to the egress LSRs [1], [2]. 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. As in the traditional IP network, the best route is calculated and selected to forward the IP packet. In MPLS network, the best LSP is selected from multiple unidirectional LSPs. The bandwidth for both upward and downward directions is not same. In MPLS network, the LSP pair is selected in round-robin fashion. In the absence of required availability of the bandwidth for forwarding, the next available LSP pair is selected [1], [2], [5].

**MPLS Label:** In MPLS domain, the label assigned to a packet is of 32 bits. The structure of MPLS label can be defined as a portion of 20-bit label value [1], [4], [5]. The 16 bits are reserved and not for the normal use, whereas three bits are experimental bits, which are used for quality of service (QoS). Bit 23, is for the bottom of stack (BoS) and is used when multiple labels are required for the packets and is set as 1. Bits 24 to 32, 8 bits are used for time to live (TTL) and are located in IP header [1], [5].
MPLS Architecture

The ingress router sets the TTL (time to live), which is a counter that is decremented by LSR. When the TTL expires, the packet is discarded by the LSR. MPLS behaves like a tunnel for the payload by using the multiple labels with the packet. Extra labels are inserted at the top of label stack; the outer most labels are swapped at each hop [8]. In some instances, multiples of labels are assigned to the packets. The instances include MPLS VPNs, MPLS traffic engineering (MPLS-TE) and MPLS VPN combined with TE. In MPLS VPN Multiprotocol BGP propagate the second label to identify the VPN. MPLS traffic engineering uses RSVP to propagate the labels, which are used to identify the tunnel label switched path (LSP). MPLS VPN with the combination of MPLS traffic engineering uses multiple labels to identify the VPN underlying LSP and tunnel LSP [25], [26].

![Figure 7: MPLS header](image)

4.6 MPLS Modes

During label distribution, LSRs use three types of modes, which are as follow.

**Label distribution mode:**

In label distribution mode LSR requests the next hop LSRs in the downstream for the label binding. Each LSR receives binding from the downstream LSR and is called downstream on demand (DOD). In unsolicited downstream mode, adjacent LSRs distribute labels to each other. Downstream label distribution shows only one remote binding, whereas unsolicited distribution shows more than one remote binding between adjacent LSRs [5].

**Label retention mode:**

All received remote bindings from LSRs are kept in the label information base (LIB) and this is known as “liberal retention mode”. When the topology change occurs it triggers updates and adopts the changes [5]. If an LSR goes down, and it is supposed to be changed by a new one, the information is quickly updated in LFIB [1], [5]. In conservative label retention mode, not all of the remote bindings are stored in label information base (LIB) [5]. It stores only the remote bindings associated to adjacent next hop [1], [5].

**LSP control mode:**

LSR creates local binding with other adjacent LSRs for the forwarding equivalence class (FEC) [5].
5 Multi-Protocol Label Switching and Quality of Service

5.1 Introduction
Initially networks were designed in such a way that there must be an individual network to provide voice transmission, other one will support the rest of data transfer facilities. The data other than voice does not require to much guarantees and as a result it can be sent with best effort network models, but in case of voice the network should be capable of delivering the fine quality of voice from the sender to the destination. For reliable delivery of voice or any real time traffic different networks were used that only support the real time traffic. The approach of using different networks for data and voice is cost effective, it increases the cost of enterprise. With the improvement in technology the organizations now wanted to build a new network infrastructure with support 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 the issue is that real time traffic is when transported over a packet switched network it faces different problems as a result the voice traffic can not be received as it is sent. In the network if data traffic is sent it may face delay and all other disturbance factors. Dealing with voice in packet switched networks there must me a mechanism which provide the resources to the real time traffic so that I could not face delay or packet loss problems. To cope with this problem the best effort approach of the internet is now being modified up to such extent so that the real time traffic could be transmitted without facing network problems. Quality of service is provided in the IP networks but in order to provide the fine grained quality to the voice the Quality of service with Multi-Protocol label switching is introduced.

5.2 Overview of Quality of Service in IP Networks
Quality of service in only IP networks is not as reliable. IP is not considered as a connection oriented protocol so there are no such mechanisms that provide specified quality of service on each router as a result the services through out the transmission could not be guaranteed. In order to provide guaranteed quality of service there must be some parameters on each hop to reserve the resources and IP does not provide such mechanism.

This deficiency of IP QoS has been insufficiently removed by using two different models for IP Quality of Service.

- The DiffServ Model
- The IntServ Model.

The Differentiated services model (DiffServ) provides different services at different levels. The information about the services is appended in the IP header. Routers interpret this information and extract the fields which specify the different priorities for different types of traffic and provide the services. However the DiffServ model does not provide any prior guarantees. If congestion occurs in the network, it increases the delay and the available bandwidth is reduces.

The Integrated Services Model is provided with resource reservation protocol (RSVP) which reserves the resource for the specified traffic flow. But it is not guaranteed that the traffic will
MPLS to support Quality of service Needs

follow the path in which resources were reserved. It does not converge with the updated network topology after having any change in the network topology. This approach is not considered as scalable.

5.3 Improvements in QoS Using Multiprotocol Label Switching

The packets are forwarded in IP network on the shortest path selected, even when the shortest path is crowded enough so that it does not have enough bandwidth for the next packets. As result congestion occurs, this is not suitable when dealing with real time traffic.

IP QoS is now combined with the MPLS, a new technology to overcome the deficiencies of only IP QoS. Multiprotocol Label Switching is used in order to explicitly select the packet forwarding paths 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 as a result the transmission is considered as more reliable.

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

The labels are appended in the IP headers of the IP packets and the packets are converted into IP frames and then these frames can easily be switched on packet based networks as well as cell based networks.

When IP packets are received by the edge routers they perform the label related operations. Labels are appended and remove by the edge routers, so the edge routers are called Label Edge routers (LERs). The IP lookups are also performed at the edges, because the Label Edge routers are responsible to append or remove the label, so at the time of appending the label the router performs a IP look up to get the appropriate label corresponding to the IP address of the IP packet. On the other hand when the packet is switched to the other end, again the label edge router 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 that take part between the label edge routers are called the Label Switch Routers (LSRs). They perform the swapping as well as switching operations. 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 LSRs instead of IP lookups. The paths followed by the packets during transmission from the source to the destination are called label switched paths (LSPs). MPLS provides IP network support for ATM, frame relay etc.

The LSPs are selected explicitly; these are accomplished by two different protocols, RSVP and CR-LDP. It is considered that RSVP is the most compatible now days for signaling or for LSP selection [14].
5.4 Class of Service (COS)

Class of service is generally defined as grouping of different types of traffic in such way that the traffic in the group has the same requirements. Class of different type 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 the feature of CoS. WFQ supports relative bandwidth whereas the CBQ supports fixed bandwidth allocation. The behavior and individual packet receives is determined by the precedence bit of the IP header.

[15], generally discusses the IP CoS mapping to MPLS CoS. It is expressed that there are two methods to provide treatment to the IP packets from edges to the core. At the edges the IP header contains ToS byte.

First method to provide the CoS mapping in the core is by copying the ToS byte from IP header to the EXP field of the shim header in MPLS.

In the second method the packets are treated with IP CoS at the edges and MPLS CoS in the core, it is provided by signaling protocols in MPLS like LDP and RSVP.

According to [15] the second method is preferred instead of the first one, because in the second method congestion can be managed on the basis of hops. Resources are allocated on per class basis whereas in the first the resources are available on per edge router pair.

5.5 Quality of Service in MPLS networks

IP network was not initially designed to provide any quality of service guarantees. Internet was not initially designed to serve for voice and other services that require higher services like higher bandwidth, less delay and jitter. The internet was to only work with TCP as transport protocol and TCP served the other protocols and applications like files, emails and other data delivery services. TCP have some features to deal with congestion and timers for verification of packet delivery and retransmission. In order to deal with this congestion problem when the traffic in the Service providers network became higher that the network available bandwidth they added more bandwidth resources to deal with this problem, but soon after they discovered that the problem of congestion can not be eliminated only by adding the additional bandwidth. It was studied by the SPs that there are some more problems in the network like traffic distribution in the network, path failure and other problems. Economical factors were also there which were increased by providing additional bandwidth. Another issue was their in front of service providers was to provide an infrastructure which can provide data, voice and video services together in an integrated environment.
MPLS to support Quality of service Needs

It can easily be predicted that only MPLS can not provide the service guarantees that are required by the customers and the service providers also. The feature of QoS is also included in the MPLS for the provision of services required. In [22] a type of survey has been conducted for the enterprises in order to know the reason of popularity of MPLS and its services in the enterprise world. It is highlighted that the enterprises focused on the functionality of the MPLS and described that the SPs and their customers are attracted to move their network resource towards MPLS because it simplifies the network issues, it solves the network management, bandwidth issues and removes the complex management of PVCs. Beside all these there is another issue of migrated our networks to the MPLS is the issue of real time traffic. The enterprises nowadays need to get the integrated environment. In order to deal with their voice and video and the normal data, they require a single network medium with QoS facilities.

Quality of service for MPLS network does not differ from the procedure as it is for any other IP based network. In this complete story [22] the quality of service provision is divided into four stages.

- As it has already been discussed that the traffic classification is considered as the first step in provision of the QoS. At the edges or boundaries of the MPLS domain the traffic is classified on the basis of its importance. As boundary routers or switches are responsible for the task, but in [22] it is proposed that if instead of boundary routers or switches the QoS appliances would be installed then they would classify the traffic after deeply checking the packet and the intermediate devices will not have to work out any classification, instead they will only forward the packets.

- Traffic prioritization helps the critical traffic to be forward first, it helps to recognize the sensitivity and importance of the traffic. Traffic prioritization is set by setting CoS for a given flow of traffic. MPLS provides gold, silver and bronze as levels of priorities. The prioritization specified as CoS is mapped to MPLS service levels.

- Bandwidth management is an important feature in order to make the accurate delivery of bandwidth to all of the available classes of traffic. It should be considered that there must be an amount of bandwidth is required to pass low priority traffic. Real time traffic should be classified and the bandwidth should be reserved for it in such a way that when it exceeds the threshold it would be denied in order to pass the rest of the types of traffic. For example if number of users using VOIP then there would be a check by call managers to restrict the callers not to exceed the allocated bandwidth.

- Another feature of providing quality of service is to manage the bandwidth requirements in such a way that the traffic should not exceed the available bandwidth. The traffic is shaped in such a way that it remains in the limits of available bandwidth. For this traffic is compress and decompressed as a result the size of the files is reduced and can be accommodated in the available bandwidth. For compression and decompression dedicated devices can be used or the routers itself perform the task. If dedicated devices accomplish this task then MPLS routers only check the classification and marking as usual.

Resources are allocated in the network by applying admission control on all LSPs. The traffic policing and monitoring is accomplished at the ingress nodes of LSPs. When TE is used the bandwidth constraints are considered per link where as when DS-TE is used bandwidth constraints are considered different for different classes of traffic on a link. Best results are
MPLS and QoS

obtained by applying admission control to all types of traffic flows which use the resources in the domain. If all the traffic is engineered then the load is controlled and there would be the less probability of congestion. At ingress node the traffic flow is identified to LSP path, at signaling time the traffic flows are mapped to the classed and it provides an open possibility of quality of service guarantees to all traffic classes individually. MPLS quality of service is also compatible over previous ATM and Frame Relay networks. The feature of fast reroute in MPLS makes it very efficient for the real time traffic, as real time traffic does not allow higher delays. It enables the network to provide its services with no delay when a specified route fails. The integration of MPLS and DiffServ provide the network with low tunneling overhead. Generally pipe tunneling model is used. The traffic pass through DiffServ domain and the DiffServ domain remains transparent to the traffic flowing through it. Routing decisions are made at the ingress level of an LSP and the routing tables on the QoS aware routers become large.
6 Quality of Service in MPLS network with DiffServ Services

The rapid growth in the internet and increasing need of services and application made the it very difficult for the service providers to exactly provide the environment what actually their customers need. Now a days not only the data but the multimedia applications, voice and video, for all these it is not enough to provide best effort services. The internet is based on what a best effort service model is. On the internet the data and other applications all receive best effort delivery. The use of best effort services on internet only provides the best effort, means it doesn’t guaranty the delivery as well as the delay and loss factor is also along with it. Internet service providers are now required to provide better services that a customer needs, they are facing the problems of service guarantees, performance and scalability. They require a solution which enhances their service levels, provide some guarantees and resolve the issue of scalability. On the basis of which the ISPs can better model their networks and the customers could rely on their services and offers provided by their internet service providers. [16], [17], [18] provide the solution on the basis of customers’ and service providers’ needs. It is considered that the scalability, service guarantees and differentiation in the services of different customers are not possible in the present best effort model. MPLS is considered as an emerging technology which is considered as a solution for these problems in combination with the quality of service guarantees.

MPLS forwards packets on the basis of labels, the packets are sent towards the destination following different label switching paths, these paths are pre-selected. The network load is balance if several LSPs are discovered from any source to destination pair. The general routing by the routing protocols is based on the forwarding of packets through the shortest available path, whereas MPLS switch the packets on the paths other than the shortest calculated path, which minimizes the issue of congestion. As MPLS forwards the packets efficiently, on the other hand another issue was under discussion, i-e, how the packet will receive the services it needs. Then IETF provided two more QoS models to deal with the problem of service guarantees.

- **IntServ. (Integrated Services Model):**
- **DiffServ. (Differentiated Services Model):**

IntServ is flow based model, consist of features like admission control and provides end-to-end QoS guarantees. It treats the individual traffic flows on every hop as a result it is considered as non scalable. Discussion of MPLS doesn’t require IntServ to be discussed. The second one provides better services which treat the traffic in the form of classes. It is based on Per Hop Behaviors.

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. In [18] it has been discussed that DiffServ treats the packets in such a way that the traffic conditioning takes place at the boundaries of the network, i-e, when the traffic enters to the MPLS domain, when traffic conditioning has been taken place at the boundaries. The packets are formulated as behavior aggregates, (collection of packets with similar characteristics), inside the domain of MPLS and DiffServ these
behavior aggregates are treated according to the specific Per Hop Behavior (PHB), which is specifically identified by the DSCP field.

In the backbone networks the combination of MPLS and DiffServ acts as a key to provide QoS. Two types of LSPs are defined, E-LSPs and L-LSPs.

E-LSPs stand for EXP inferred LSPs and L-LSPs stand for Label inferred LSPs. The FEC is identified by the MPLS label whereas the desired PHB is selected from the # bit EXP field. In contrast with only DiffServ, because the DiffServ model uses 6 bits for a specific behavior aggregate to define a particular PHB and here the E-LSP used only 3 bits for the purpose. In the second L-LSP, the only label is used to identify the FEC as well as the PHB also. EXP only defines the drop priority.

Generally it can be said that when a packet is entered to a DiffServ domain, at the edges the classification and marking is done, marking of DSCP enables the transit nodes to extract the information that what type of queuing and scheduling treatment is to be done with the packet. In [19] the similarities of MPLS and DiffServ are discussed. It is said that FEC is equivalent to a BA and the label can be considered as an equivalent to that of DSCP. Both of them are independent of each other. Both provide the best services of their own. [19] Discusses that the DSCP in IP header cannot be interpreted inside the MPLS domain as a result the packets therefore cannot be differentiated on the basis of the DSCP field inside the IP header. For the solution of this E-LSPs and L-LSPs are used in order to identify the PHB. This behavior of the MPLS network enables the operation between both kinds of ISPs with MPLS and without MPLS. [16], [17], [18], [19]

### 6.1 E-LSPs and L-LSPs Bandwidth Reservation

The requirement of bandwidth with these LSPs is signaled when the LSPs are established by the LSRs. LSRs use this requirement for admission control. The establishments of LSPs with bandwidth requirement does not involve per-LSP scheduling.

The bandwidth requirement for L-LSP is used for admission control over DiffServ resources which are specified for a specific scheduling class. The bandwidth requirement for E-LSP is used by the LSRs for a set of scheduling classes and the admission control is performed over the global resources. These global resources are collectively shared by the set of scheduling classes.

### 6.2 Label Forwarding in DiffServ LSRs

Label forwarding in DiffServ LSRs is different from only DiffServ routers. In [21] the label forwarding for DiffServ LSRs is divided into different stages.

- The incoming packet is first checked for which behavior aggregate it belongs to. The PHB is determined by examining the EXP field of the shim header inserted in the packet.

- Then the outgoing PHB determination is performed. The traffic conditioning is another factor for LSRs, if it involves then the enforcement of a PHB and sending it with the forwarded packet is said to be outgoing PHB determination, if the traffic conditioning is not performed in the LSR then the outgoing PHB will be the same as the incoming PHB.
QoS in MPLS network with DiffServ Services

- By using incoming label map the labels are swapped. Label swapping comprises of label types, different supported PHB, incoming PHB determination and outgoing PHB determination.

- Another stage of forwarding DiffServ information to the downstream. It is about how to transfer the information about the DiffServ attributes to the downstream LSRs with the transmitted packet. The DiffServ information can be transmitted in the label of the transmitted packet or the IP header of the transmitted packet is encoded with the DiffServ information. In IP header it is done by copying the DSCP in to the DS field.

6.3 MPLS and DiffServ Integration for the Provision of QoS for Real Time Traffic

MPLS and DiffServ integration is a strategy as a solution for the today’s network problems. It led to the enhancement of the network performance by providing the better QoS services and new techniques to provide QoS in present and future networks.

[20] Discusses the integration of MPLS QoS with DiffServ, growing needs of core networks require a type of network which provides services for data, voice and video also. In order to design a network to deal with the data as well as the real time traffic is very easy; a simple network can provide the facilities, but the premium classes of services are the focus of network entrepreneurs. A simple IP network can also have the capability of providing the QoS in enhance the efficiency of the network for real time traffic, it can also deal differently with real time traffic as compared to the data traffic, but the sensitivity of real time traffic does not allow the service gaps which occurs in simple IP network QoS services. To deal with the provision of guaranteed QoS the research work is being continuously done in the field. With the development of MPLS it is considered as the most efficient switching technique as compared to the others, in the future MPLS is going to completely replace other types of switching fabrics. It is also considered that the QoS parameters are also efficiently dealt in the cores where MPLS and DiffServ integration services are used. [20] Focuses with the help of simulations that the integration of MPLS and DiffServ is the required solution for the current QoS problems in the core networks in order to deal with real time traffic bursts. In [20] the network was setup with 11 nodes from 0 to 10. The network topology was setup in such a way that the nodes 0, to 2 were set as source nodes and the other three 8 to 10 were set as destination nodes. The link between node 3, 4 and 5 was considered as the shortest path. Four different types of scenarios were configured as IP only, DiffServ IP, MPLS IP and DiffServ MPLS. IP only and DiffServ IP network topologies were same, the only difference between them was the prioritization and marking of packets in DiffServ IP. In MPLS and DiffServ MPLS networks the only difference was the capability of all the routers to be MPLS enabled. The DiffServ MPLS network was also configured to use CBQ.

The network performance of all the four networks was studied by the comparison of TCP and UDP flows. In order to study the effect in the network the CBR traffic generator was used and it increases the traffic flows dramatically study the effect that how different network conditions will cope with this dramatically increase. The increase in CBR traffic was according to the capacity of the shortest link between the source and the destination.
The simulation results clearly depict the differences between the different types of traffic throughputs. As the FTP and EXP traffic flows were generated during the simulation. In IP only network all type of traffic used the shortest path from source to the destination, as a result the link got congested and the packets were dropped as a result the average throughput was reduced. In DiffServ IP network the EXP flow got the better throughput because prioritization was used as result the premium traffic gets the higher availability of the resources as compared to the FTP. The throughput of the FTP was worse in DiffServ IP network because it has to wait till the buffer overflow could be managed. The other two scenarios MPLS IP and DiffServ MPLS appeared with the enhanced throughput for both the FTP and EXP flows. It is concluded in [20] that the IP/MPLS and DiffServ MPLS has reduced the delay in both FTP and EXP flows. In MPLS enabled networks all of the LSPs were use instead of the shortest path as a result it was easy to deal with the problem of congestion, whereas in IP only network the shortest path is congested and the traffic flows were dropped resulted in reduced throughput.

<table>
<thead>
<tr>
<th>Table for packet loss of FTP and EXP traffic flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Network</td>
</tr>
<tr>
<td>CBR uses 50% of the shortest path capacity</td>
</tr>
<tr>
<td>Packet Sent</td>
</tr>
<tr>
<td>FTP</td>
</tr>
<tr>
<td>IP Network</td>
</tr>
<tr>
<td>DiffServ IP Network</td>
</tr>
<tr>
<td>IP/MPLS Network</td>
</tr>
<tr>
<td>DiffServ MPLS Network</td>
</tr>
</tbody>
</table>

Figure 11: MPLS network simulation environment

The above table shows the packet loss in all of the scenarios from [20]. It was clearly depicted that the packet loss is higher in the networks with without MPLS and DiffServ.
7 MPLS Application As Virtual Private Networks

A virtual private network is a network which is built over a shared infrastructure based on some rules. The rules are defined according to the requirements of the customer and the availability of the service provider’s network. Different customer sites are interconnected through a service provider network to communicate with each other, regardless of what network resources from SPs network they are using. VPN services can be based on different network technologies, like ATM and Frame Relay based VPNs, VPNs based on tunneling and the most important category of VPN is MPLS VPN. Layer 2 VPNs use frame relay and ATM services. The VPNs using IP tunnels to provide connectivity between the customer sites are Layer 3. An example of layer 3 VPN is GRE tunnel based VPN. These days, enterprises are increasing their sites all over the world. As their sites are increasing day by day, so they need connectivity among their sites in such a way that any site could have connectivity to any other. This leads to a problem of VPN technology, as current VPN solutions are not scalable in a way to provide this type of connectivity. So MPLS VPN is considered as a more flexible, scalable and efficient technology. MPLS based VPNs provide better and simpler management, more flexible and considered as the cost effective solution for connecting different sites. The MPLS based VPNs are considered as the site-to-site VPNs; BGP is used in these VPNs, and is called MPBGP. Multiprotocol BGP (MPBGP) is responsible for the distribution of routing information in the backbone network, whereas the forwarding of packets in the backbone network is accomplished by MPLS. Both the customers sites which are connected with MPLS based VPNs are unaware of the backbone network infrastructure and the forwarding of packets inside the core network. MPLS is designed in such a way that, it enables the internet to evolve in a way to support larger traffic loads, millions of hosts, and to provide the QoS guarantees that could be wished on the internet. Traffic Engineering enables the network to support different architectures for the routing and highest QoS guarantees enable users to integrate different categories of the network traffic of a single network infrastructure. In MPLS, traffic engineering is used to calculate the number of routes for the desired destination and load is balanced across different links.

The main objective of applying VPN techniques to connect different sites is to provide better and guaranteed services to the users. In other words, the objective is to guarantee QoS to the users. VPNs are most likely implemented to provide the QoS guarantees discussed in [23]. In [24] the advantages of MPLS VPN are highlighted as a strong network. The advantages are as follows.

- The network can easily be extended in a sense that the number of VPNs can easily be increased.

- MPLS provides the necessary safety measures in the previous ATM and Frame Relay and also provides additional IPSEC features for the encryption.

- Integration of voice video and data is also a feature of MPLS VPN.

- Provides central management which reduces the load of management on the customer.

- It is considered as the cost effective solution for the customers.
MPLS Application as VPN

- Implementation of MPLS in the network reduces the processing of the network devices inside the network.

- In the backbone network, BGP forwards the packets on the basis of labels assigned by the MPLS edge routers, which makes the routing more efficient and easy.

Enterprises are continuously adopting this new avenue for their networks to scale well. The major problem with Layer 2 VPN solutions was that they could not grow well. The scalability problems of Layer 2 VPNs lead to this newer Layer 3 VPN solution. Thus layer 3 MPLS VPN with BGP solves this scalability problem and provides much more features than layer 2 VPNs. The route forwarding is accomplished by BGP over MPLS core. The extended form of BGP is used in the MPLS VPN which saves separately the routing information of different clients.

7.1 Architecture of MPLS VPN

MPLS VPN is a virtual private network which connects different customer sites in such a way that the customer boundary routers connect to the provider’s network. The routers that are placed on the edges of customer sites are called “Customer Edge Routers” (CE routers) and the routers placed at the provider’s network edges are called “PE routers”. Customer sites are configured with any of the interior gateway routing protocols, and provider’s side is also configured with any routing protocol for their intrinsic routing information distribution. The whole network is divided into two parts, a customer –controlled part C-Network and a provider-controlled part P-Network. Different parts of the customer’s network are referred to as the sites of the customer network, which are connected through VPN, and the service provider’s network or p-network is responsible to provide the connectivity between these sites. The routers at the edges of both customer’s and provider’s network are called PE routers and CE routers. PE routers interfere in the customer routing. These routers take the customer routing information from one site to the other and the rest of provider’s network (backbone) acts as a transit area for the customer routing information. Customer routing information is forwarded through the backbone network but the routers in the core network (which are called P routers) do not participate in the customer routing. In PE routers, the customer information is stored in such a way that individual routing tables are maintained for each customer.

These routing tables are also called “Virtual Routing and Forwarding” tables (VRF). The customer information is transparent to the P network, so the routing inside the backbone network takes place on the basis of global routing tables. In PE routers, the tables used for separating different customers’ routing information, these tables are called virtual routing and forwarding tables (VRFs), when the information flow through the P network to other PE router from where it is sent to the destination site of the customer, in the core network there would be a carrier protocol which distinguishes the customer routing information throughout the flow. It is possible when there will be a single routing protocol between the PE routers. The individual routing protocol between the PE routers makes it easy to make the customer information transparent to the P network.

Border Gateway Routing Protocol (BGP) is considered as the scalable and suitable protocol to be configured between the PE routers. It is expected that the service providers are required to connect a large number of customers’ sites with each other which make the routing tables in PE routers very large according to the customers. As a result, a scalable protocol is needed to handle the larger routing tables. BGP is considered as the scalable and efficient to carry out
MPLS to support Quality of service Needs

the task. BGP is required with the capability to distinguish the routing information of different customers even if they have the same address spaces. It is not possible for the BGP to separate the customer information with the original IP prefixes. In MPLS VPN, IP prefixes of the customers are extended to make them non-overlapping with each other. Route Distinguishers (RD) are introduced by MPLS VPN to make the address unique. A 64 bit RD is appended with the original IP prefix of the customer. After the addition of RD, the overlapped address can also be made unique, which is easily taken by the BGP to transport over the providers network.

When an RD is added to the original customer’s IPv4 address, it converts the address into VPN IPv4 addresses. Thus, they are called “VPNv4” addresses. These addressed are transported between PE routers; the customer sites are unaware of VPN IPv4 addresses. They only know that one site sends an IPv4 prefix to others, regardless of what the interfering networks do. BGP session is established between the provider edge routers and BGP supports both the VPNv4 and IPv4 addresses. That is why the BGP here referred to as “Multi-protocol BGP” (MPBGP). When the customer sites want to communicate with each other, one site sends an update with an IPv4 prefix to the PE router, PE then adds an RD of 64 bit to the IP prefix to use it as a unique prefix of 96-bits called, “PNv4 address”. When RD is added to the prefix, MPBGP session is established and this update is propagated to the other PE routers. PE router, on receiving VPNv4 address, strips off the RD from the income update and makes it an original IPv4 prefix and forwards it to the destination site of the customer. RDs are only responsible for making the IP prefixes unique throughout the transportation between PE routers.

In larger enterprises, a number of sites want to communicate with each other, and it is possible that there is more than one VPN which accomplishes the task. VRFs are created and associated with VPNs which hold the information of sites and their attached VPNs, IP routing table and CEF table. The routing table is controlled by a set of rules, which are also a part of VRF. VRF and customers sites have a one-to-one relationship in a VPN with each other, whereas a customer site can be a part of different VPNs. RDs only distinguish the addresses of customers; only overcoming the problem of overlapping of address spaces used by the customers, but they do not tell about the VPN membership of the customer. As a result, it is necessary to separate the routing updates of different VPNs when a customer site is attached to more than one VPN. Route Targets (RTs) are used to solve this problem. When any routing update is learned from the customer site, a list of attributes is attached to it which identifies that the routing update is from a particular VPN. Generally, RTs identify the membership of a route with a particular VPN [24].

7.2 Flow of Information in MPLS VPN

When MPLS VPN is designed, it is kept in mind that the customer routers are unaware of the MPLS VPN. In a provider’s network, the edge routers only keep the customer routing information; the rest of the provider’s network does not keep the customer routes in its routing tables. PE routers should have the capability of supporting MPLS VPN services as well as the traditional IP routing services.

The routing protocols should be individually configured between customer routers and provider routers in such a way that MPBGP is configured between PE routers. The connectivity between PE and CE routers is provided by configuring routing protocols on both PE and CE routers. CE routers are unaware of PE routing as MPLS VPN. They treat them as
MPLS Application as VPN

simple routers of their own network so any routing protocol can make it possible to provide connectivity between them. Routing protocols on PE routers for PE and CE connectivity are configured on per VRF basis. Customer site is unaware of what is going on inside a provider’s network. For customer site the MPLS VPN backbone behaves like a part of its own backbone network. For providers network the MPLS VPN do not have any meanings because the router inside the P network do not take part in MPLS VPN routing they just act as transit routers for the MPLS VPN routing updates. Any interior gateway protocol is enough to be configured between P routers for the exchange of intra network routing information. BGP is not configured on P routers because it is only needed for MPLS VPN. The core devices of MPLS VPN are the PE routers which participate in MPLS VPN as well as in normal routing of P network.

When an update from one customer site is propagated to the other it first goes to the PE router to which sender customer site is connected. A PE router takes the routing update from the CE router and populates the corresponding VRF for the received update. Then this routing update has to be forwarded to the destination customer site through MPLS VPN. Thus PE router changes its IPv4 prefix to VPNv4 route and establishes an MPBGP session and exports to the other PE router to which destination site is connected. Receiving PE router imports the routing update in its appropriate VRF on the basis of RTs attached to the route and configured on the receiving VRF. Then this route is converted from VPNv4 to IPv4 route and forwarded to the CE router [23], [24].

![MPLS VPN Architecture](image)

**Figure 8: MPLS VPN Architecture:**

### 7.3 Comparison of MPLS VPN with IP VPNs

As when compared with the overlay VPNs some of the benefits of overlay VPNs are also remain under consideration. They are considered as well known and easy to implement from both customer and SP point of view. Another benefit of overlay VPN is that SP does not participate in the customer site so purely both the network can be separated. On the other hand the MPLS VPN provides optimum routing and guaranteed QoS measured between different customer sites without any effort. MPLS VPN is considered as scalable backward compatible technology as it provides the same services and features the traditional ATM and Frame Relay VPNs were providing in addition with the additional services. In layer 2 overlay VPNs the
MPLS to support Quality of service Needs

optimum routing can be provided when there would be full mesh connectivity between different sites through virtual circuits. Different customer sites are connected through manual configuration for VC as well as bandwidth is provided on the basis of customer sites which adds an overhead of working and is not easy to manage always. Some of the problems which also remain in layer 3 overlay VPNs (IPSec and GRE) are the additional overhead with the data packets. These tunneling schemes add a lot of encapsulation with the data packets which can be 20 to 80 bytes per packet.

The best features of Overlay VPNs and the peer-to-peer VPNs are combined in MPLS VPN. When different customer sites are connected through a service provider network, routers at the edges of provider’s network are called provider edge (PE) routers and those at the edges of customer sites are called customer edge (CE) routers. In case of MPLS VPN the optimum routing is provided as the PE routers contribute in customer routing. PE routers separate each customer routes so that the customers are not required to use different address spaces, instead they can use overlapping address spaces.

Nowadays different business environments are using VPN infrastructures to connect their distributed sites. Enterprises are trying to get more of what they have deployed or what they are about to deploy. Different environments have the different requirement and on the basis of these requirements they are using various VPN technologies. These VPN technologies include layer 2 and layer 3 VPNs. Some of them are relying on the cost and use the lower cost technologies however they do not think of what the security measure are all about. But those who are thinking about their data and information fool proof security they do not think that how much a secure solution costs. Enterprises are conscious about their addressing schemes. When they want to use a public network for their private and necessary data, they are thinking about the vulnerability of their data. Somehow it is possible that a packet addressed to the destination site of customer A may be received by the same address recipient of the customer B. But MPLS provides an environment where all these reason became less important. Number of customers can use the shared infrastructure without taking care of what addressing scheme they are using. In MPLS VPN the addresses are converted into 96 bits unique address. The original IP address of the packet is modified by adding 64 bits to the IP address. The new address is call VPNv4 address.

![VPN IPv4 Address](image)

**Figure 9: VPNv4 Address.**


8 Implementation

A practical environment is developed in the laboratory and two scenarios were built in order to test the working of MPLS. A theoretical study has clarified the benefits of MPLS. At the end in the practical environment the network with two scenarios were built in such a way that first an ordinary network is built with a traditional IP routing. Then the same network is configured with the MPLS and results are obtained. The obtained results show that the network with MPLS shown the better performance as compared to the traditional IP routing.

QoS of Service is configured for both the scenarios. Generally when an ordinary data is to be transferred in the network, it does not require any service guarantees. Performance degradation factors like, delay, jitter and dropping of packets 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 can not 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.

8.1 Network Diagram

![Network Diagram](image)

Figure 13: Network Diagram
MPLS to support Quality of service Needs

8.2 Network with Traditional IP routing

The above network was divided into two portions. The core part of network consists of routers P1, P2, M1, M2, M3, M4 and M5. OSPF was configured as a routing protocol in this portion and all of these nodes were kept in area 0. The second portion of the network were two sites one is a network with the router S1 connected to the core at P1 and the other is the network with a router S2 connected to the core via P2. Both these sites have EIGRP as the routing protocol running inside. For full time connectivity both the protocols are redistributed in each other. After redistribution of OSPF in EIGRP and EIGRP in OSPF the network was in full time connectivity mode. Connectivity was checked by sending PING request from S1’s loopback to the S2’s loopback.

Quality of service (QoS) is configured on the core network in order to provide better services for the traffic coming to and from both the sites. The serial interfaces of routers P1 and P2 are configured with the QoS policies towards the output. The policies configured on P1 and P2 classify and mark the incoming traffic. As the growing networks demand quality of service to provide the services to transport different data types on the single network infrastructure like, voice, video, normal data etc. In order to transport these traffic types on a single infrastructure it is required to use such kind of service that could not face any delay more than the acceptable. Here in this practical environment we built a network with the traditional routing on the basis of routing protocols and compared its performance with the MPLS network. After configuration of routing protocols the network connectivity was checked. For ordinary data, there is no need of QoS configuration but in case of some sensitive traffic network needs to be fully equipped with QoS parameters. The following tables show different policies configured on the routers in IP network. Traffic is divided into different classes, on the basis of classed the traffic will be entertained in the network during its flow. The main purpose of this classification is to identify that which type of traffic is flowing inside the network. If any real time traffic will be in the network than it will be giver the highest precedence as a result it will be treated in the network on the priority basis. The table below just indicates how classification is done; on the basis of matching criteria a router puts the incoming traffic into a specific class. This classification is performed at the edges of the network and the rest of the routers inside the network treat incoming packets according to the behaviors attached with the packets. Generally the traffic which is more sensitive takes the benefit of the QoS more than the ordinary data. Classification is usually done with respect to traffic types, like video, voice and the best effort data. In the implementation work we classified the network traffic into five classes on the basis of their types. It is just an example to show that how policies work. We classified different protocols traffic into different classes and we gave them priorities. According to their priorities they would be treated in the network. 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.

Following tables show the QoS policies configured on the network.
Implementation

**IP Network Policies**

<table>
<thead>
<tr>
<th>Class</th>
<th>Match Criteria</th>
<th>DSCP</th>
<th>Precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>RTP</td>
<td>46</td>
<td>7</td>
</tr>
<tr>
<td>Interactive</td>
<td>EIGRP, OSPF, ICMP</td>
<td>26</td>
<td>5</td>
</tr>
<tr>
<td>Web</td>
<td>HTTP, SMTP</td>
<td>18</td>
<td>3</td>
</tr>
<tr>
<td>Class-Default</td>
<td>Any</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Next table shows the shaping policy configured on the second level routers. After classification and marking at the edges the second level routers shape the packets. Classified packets are then shaped according to the rate defined in the policy after defining the policy it is implemented on the desired interface to outbound or inbound as required.

<table>
<thead>
<tr>
<th>Class</th>
<th>Match Criteria</th>
<th>Bandwidth %</th>
<th>Average Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prec7</td>
<td>Precedence 7</td>
<td>50</td>
<td>240000/120000</td>
</tr>
<tr>
<td>Prec5</td>
<td>Precedence 5</td>
<td>35</td>
<td>160000/80000</td>
</tr>
<tr>
<td>Prec3</td>
<td>Precedence 3</td>
<td>15</td>
<td>60000/30000</td>
</tr>
<tr>
<td>Class-Default</td>
<td>Precedence 0</td>
<td>-</td>
<td>800000/400000</td>
</tr>
</tbody>
</table>
MPLS to support Quality of service Needs

8.3 MPLS based Network

The network shown above was configured with IP routing first and then tested with the MPLS enabled on the core network. QoS policies are configured on the core routers to provide service guarantees to the traffic. After that the same network was modified and MPLS was enabled on the core network routers in order to demonstrate how better the MPLS works. Then QoS is enabled on the necessary interfaces in order to work with MPLS and show the better performance than the network with IP routing. The policies configured on the routers in MPLS based network are as follows. The traffic classification was configured at both the edges.

MPLS Network Policies

<table>
<thead>
<tr>
<th>Class</th>
<th>Match Criteria</th>
<th>MPLS EXP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Precedence 7</td>
<td>5</td>
</tr>
<tr>
<td>Interactive</td>
<td>Precedence 5</td>
<td>4</td>
</tr>
<tr>
<td>Web</td>
<td>Precedence 3</td>
<td>3</td>
</tr>
<tr>
<td>Class-Default</td>
<td>Precedence 0</td>
<td>0</td>
</tr>
</tbody>
</table>

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 enabled network different labels are attached and removed from the source to the destination and it is forwarded on the basis of MPLS label. The router forwards the packet after checking the next hop label regardless of what the IP address is. The question is that how QoS parameters are read by the router when MPLS headers appended with the IP packets? As we discussed in detail 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 packet is covered with the MPLS label then the QoS parameters are also copied to the new labeled packet. The experimental bits in the MPLS packet specify the QoS behavior of the MPLS packet.
Table 4

<table>
<thead>
<tr>
<th>MPLS Network Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
</tr>
<tr>
<td>MPLS-AF1</td>
</tr>
</tbody>
</table>

Above table shows the policy maps which were configured on all the core routers. When the traffic is classified and marked at the edge routers then it is forwarded to the destination through core routers, core routers have to provide the required QoS to the labeled packets. At the edge routers the voice traffic is classified as a CRITICAL class and then MPLS EXP 5 is assigned. In the core network 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.

8.4 Traffic Statistics from IP Network

S2 is a PAGENT router. PAGENT router contains the Cisco IOS which is able to generate the automatic traffic. S2 router in the network considered as Traffic Generator to check the performance of the network. When the network was in full connectivity mode then “TGN Start” command was given, traffic generator started to generate the traffic which flew through out the network and then it was stopped by using “TGN Stop” command. After that following statistics were obtained by issuing “pkt-seq-drop-stats, show delay-stats, show jitter-stats” commands.

Table 5

<table>
<thead>
<tr>
<th>IP Network Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sent</td>
</tr>
<tr>
<td>Drop</td>
</tr>
<tr>
<td>Minimum</td>
</tr>
<tr>
<td>Delay</td>
</tr>
<tr>
<td>Jitter</td>
</tr>
</tbody>
</table>
MPLS to support Quality of service Needs

8.5 Traffic Statistics from MPLS based Network

Table 6

<table>
<thead>
<tr>
<th>MPLS Network Statistics</th>
<th>Sent</th>
<th>Received</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop</td>
<td>753</td>
<td>753</td>
<td>0</td>
</tr>
<tr>
<td>Minimum</td>
<td>0.017692</td>
<td>0.022794</td>
<td>0.017928</td>
</tr>
<tr>
<td>Maximum</td>
<td>0.000005</td>
<td>0.004931</td>
<td>0.000222</td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Above two tables are taken for the comparison of the parameters on the basis of which a network requires QoS. It can be seen from the values taken from the designed networks. In the cases of delay and jitter from both the networks, it can be seen that the network with MPLS shown less delay and jitter. The network was built inside a lab, which was not very large. It was just to demonstrate the performance of MPLS. If at this much smaller level MPLS gives the better performance than IP routed network then in the larger networks definitely IP routed network gives larger delays and other performance degradation factors as compared to the MPLS enabled network.

As for as scalability of the network is considered, it can easily be seen from our implementation that for a smaller level may b IP network can work properly but in the larger networks its does not work good, instead MPLS handles larger networks without any performance degradation.

8.6 IP Network Routing Tables

The routing tables obtained were built by the routers when they exchange packets between each other. OSPF is the routing protocol running between the routers of the core network. When routers exchange hello packets between each other and adjacencies are built, shortest path between every source and destination pair is stored in the routing tables of the routers. When the network will be large the routing tables in the routers will be larger, as a result when it is required to lookup in the routing table then it causes longer delays to search something out of a routing table. Router when builds a routing table it only stores a shortest path between every source and destination path, if sometimes route fails and router have to find out a new way so it takes more time as a result the network become busy and the performance of the networks is affected. Due to larger routing tables the network will have slower convergence as compared to the MPLS enabled network.
8.7 MPLS based network CEF Tables and Forwarding Tables

MPLS is in contrast to the IP routing, it is a switching technique based on the labels, instead of looking up in the routing tables the switching is performed on the basis of labels. Instead of routing tables CEF is built in the routers. Routing tables only store the shortest path, in case of shortest path failure the next available path is calculated again and stored in the routing table. In CEF every possible link between any two source and destination pair is stored. CEF table acts as a cache, so it works faster than the routing tables.

Once CEF is built with the help of routing table and then it is used actively. So the router does not require working with the shortest available paths. All available paths are stored in the CEF table. MPLS uses different links to send the traffic from the source to the destination to avoid network congestion. If there would be a single shortest path then it will quickly become congested as a result the network would become in the congested state. These all features make MPLS more distinguishing technology. CEF tables are shown in the Appendix B section of the report.

Following is the sample of MPLS forwarding table from one of the routers. The routers use these forwarding tables inside the MPLS domain to forward the packets on the basis of labels. Once the packet enters the MPLS domain from the non-MPLS domain its IP prefix is mapped against the appropriate label and label is appended to the packet. After that inside the core network the packets are forwarded on the basis of labels. Inside the core network the labeled packet faces different hops and at each hop the labels are swapped according to the incoming and outgoing interfaces. Following table shows the tags (Labels), outgoing interfaces and their respective IP prefixes.

Table 7

<table>
<thead>
<tr>
<th>Local Tag</th>
<th>Outgoing Tag</th>
<th>IP Prefix or Tunnel ID</th>
<th>Bytes Tag Switched</th>
<th>Outgoing Interface</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>16</td>
<td>192.168.30.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>17</td>
<td>17</td>
<td>192.168.10.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>18 Pop tag</td>
<td></td>
<td>192.168.40.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>19 Untagged</td>
<td></td>
<td>172.16.20.0/24</td>
<td>0</td>
<td>Fa0/0</td>
<td>172.16.200.1</td>
</tr>
<tr>
<td>20</td>
<td>20</td>
<td>172.16.10.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>21</td>
<td>21</td>
<td>172.16.100.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>22</td>
<td>23</td>
<td>192.168.20.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>23</td>
<td>24</td>
<td>192.168.100.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
</tbody>
</table>

Above table is a forwarding table taken from one of the routers to show how the labels are stored in the routers. Local tags are assigned by the that router itself for the corresponding IP prefix, for example 16 is local tag assigned for 192.168.30.0/24 and the outgoing interface for the packets for this IP prefix will be Serial interface 0/1/0 of that router. In the same way routers store labels for all the IP prefixes their respective outgoing interfaces and next hop. Forwarding tables for all the routers are appended with the report in the Appendix C section of the report.
9 Results

Two different scenarios were implemented in the lab, to demonstrate the performance of MPLS and IP routing. The results obtained from the designed scenarios are summarized below.

- In IP routing scenario, large routing tables were built by the individual routers which make the routing slower.
- In MPLS switching the IP routing tables were replaced by the CEF tables which make the switching process faster than the routing. Without MPLS CEF tables are built but the routing is based on IP prefixes stored in routing tables.
- Forwarding of packets in MPLS is based on labels instead of IP prefixes which reduces the processing overhead of the routers.
- In IP routing, the IGP used the shortest path to forward the packets between every source and destination pair. In MPLS environment the shortest path technique was removed and instead all available paths were used from one source to destination pair for balancing the load.
- It is deduced that the load balancing feature of MPLS removed the congestion factor from the network.
- Practical implementation proved that the quality of service works well in combination with MPLS as compared to IP quality of service.
- Performance degradation due to delay, jitter and dropping of packets is less in the network scenarios with MPLS as compared to the network scenarios without MPLS.
10 Conclusion

The theoretical part of this study helps to understand MPLS and its functionality. Authors of this research focus on QoS in MPLS network. Guaranteed QoS is required to transfer real time traffic over the network. In MPLS network QoS gives better performance as compared to the IP QoS regarding reliability of data transfer, delay and jitter etc. To validate this claim the authors of this thesis have conducted a practical comparison of MPLS and IP routing. An IP network with nine routers was built and QoS was configured. Delay, jitter and packet drops were collected by issuing commands. Then the network was reconfigured with MPLS QoS. Again delay, jitter and packet drops were collected for MPLS based network.

The statistics collected from both the networks show that the MPLS based network shows better result than the simple IP routed network. Data packets face longer delays in IP routed network. The other factors like jitter, bandwidth and reliability were also improved in MPLS QoS network.

All the necessary configurations of the routers have been recorded and presented at the end in the appendices section of the report. Two different scenarios are compared, IP routing network and MPLS based network. For both cases configurations are attached in the appendices sections. Then routing tables of IP routing network and CEF tables of MPLS network have been taken. At the end in appendix C the MPLS LDP neighbors, bindings and MPLS forwarding tables have been shown.
11 References


[10]. Srinivas Vegesna Quality of Service By Published by Cisco Press, 2001 ISBN 1578701163, 9781578701162


[12]. Leonardo Balliache, Network QoS Using Cisco HOWTO, April 2003 v0.1 Published on May 1, 2003, v0.2 May 15, 2003, v0.3 September 10, 2003

MPLS to support Quality of service Needs


[19]. International Workshop NGNT, “DiffServ and MPLS Timea Dreilinger”, Budapest University of Technology and Economics, Department of Telecommunication and Telematics, High Speed Networks Laboratory.


Appendices

Appendix A

Routers’ Configurations

IP routing based network

############################################################

S1#show run

Building configuration...

Current configuration : 1069 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
no MPLS ip
!
voice-card 0
!
!
interface Loopback0
  ip address 172.16.10.1 255.255.255.0
!
interface FastEthernet0/0
MPLS to support Quality of service Needs

ip address 172.16.100.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/1/0
no ip address
shutdown
clock rate 125000
!
interface Serial0/1/1
no ip address
shutdown
clock rate 125000
!
routing eigrp 1
network 172.16.0.0
no auto-summary
!
ip classless
ip route 172.16.100.0 255.255.255.0 172.16.10.0
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login
!
end

P1#show run

Building configuration...

Current configuration : 1694 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname P1

boot-start-marker
boot-end-marker

enable password cisco

no aaa new-model

resource policy

mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef

no MPLS ip

voice-card 0

class-map match-any Critical
match protocol rtp
class-map match-any EF
match protocol rtp
class-map match-any Interactive
match protocol eigrp
match protocol ospf
match protocol icmp
class-map match-any AF1
match protocol eigrp
match protocol ospf
match protocol icmp
class-map match-any Web
match protocol http
match protocol smtp
class-map match-any AF2
match protocol http
match protocol smtp

policy-map SETDSCP
  class EF
  set ip dscp 46
  class AF1
  set ip dscp 26
MPLS to support Quality of service Needs

class AF2
    set ip dscp 18

policy-map markingpolicy
    class Critical
        set precedence 7
        bandwidth percent 50
    class interactive
        set precedence 5
        bandwidth percent 35
    class web
        set precedence 3
    class class-default
        set precedence 0
        bandwidth percent 15

interface FastEthernet0/0
    ip address 172.16.100.254 255.255.255.0
    duplex auto
    speed auto
    service-policy input SETDSCP

interface FastEthernet0/1
    no ip address
    shutdown
    duplex auto
    speed auto

interface Serial0/1/0
    ip address 192.168.100.1 255.255.255.0
    no fair-queue
    clock rate 64000
    service-policy output markingpolicy

interface Serial0/1/1
    ip address 192.168.30.2 255.255.255.0
    clock rate 2000000
    service-policy output markingpolicy

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 classless
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login
!
end

#--------------------------------------------------------

M1#show run

Building configuration...

Current configuration : 1405 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname M1
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
!
resource policy
!
ip cef
!
voice-card 0
!
class-map match-all prec5
match precedence 5
class AF1
match ip dscp 26
class-map match-any prec7
match precedence 7
MPLS to support Quality of service Needs

class EF
  match ip dscp 46
class-map match-all prec0
  match precedence 0
class AF2
  match ip dscp 18
!
!
Policy-map SETDSCP
class EF
  set ip dscp 46
class AF1
  set ip dscp 26
class AF2
  set ip dscp 18
!
policy-map shapingdefault
class prec7
  shape peak 120000
  bandwidth percent 50
class prec5
  shape peak 80000
  bandwidth percent 35
  class class-default
  bandwidth percent 15
interface FastEthernet0/0
  no ip address
  shutdown
duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  shutdown
duplex auto
  speed auto
!
interface Serial0/1/0
  ip address 192.168.100.10 255.255.255.0
  no fair-queue
service-policy output shapingdefault
service-policy input SETDSCP
!
interface Serial0/1/1
  ip address 192.168.10.10 255.255.255.0
  ip accounting precedence input
service-policy input SETDSCP
  service-policy output shapingdefault
!
routing ospf 1
Appendix

log-adjacency-changes
network 192.168.0.0 0.0.255.255 area 0
!
ip http server
do ip http secure-server
!
control-plane
!
line con 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login
!
scheduler allocate 20000 1000
end
###########################################################

M2#show run

Building configuration...

Current configuration : 1116 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname M2
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
memory-size iomem 10
!
ip cef
!
ip host PAGENT-SECURITY-V3 21.63.1.51 90.34.0.0
!
multilink bundle-name authenticated
no MPLS ip
!
voice-card 0
!
MPLS to support Quality of service Needs

class-map match-all prec5
  match precedence 5
class AF1
  match ip dscp 26
class-map match-any prec7
  match precedence 7
class EF
  match ip dscp 46
class-map match-all prec0
  match precedence 0
class AF2
  match ip dscp 18
!
!
Policy-map SETDSCP
  class EF
    set ip dscp 46
  class AF1
    set ip dscp 26
  class AF2
    set ip dscp 18
!
policy-map shapingdefault
  class prec7
    shape peak 120000
    bandwidth percent 50
  class prec5
    shape peak 80000
    bandwidth percent 35
  class class-default
    bandwidth percent 15
no dspfarm
!
vtp domain cisco
vtp mode transparent
!
interface FastEthernet0/0
  no ip address
  shutdown
duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  shutdown
duplex auto
  speed auto
!
interface Serial0/0/0
  ip address 192.168.20.20 255.255.255.0
no fair-queue
clock rate 64000
service-policy output shaping default
service-policy input SETDSCP

! interface Serial0/0/1
  ip address 192.168.10.20 255.255.255.0
clock rate 64000
service-policy output shaping default
service-policy input SETDSCP

! router ospf 1
  log-adjacency-changes
  network 192.168.0.0 0.0.255.255 area 0
!
ip http server
no ip http secure-server
control-plane
!
line con 0
  exec-timeout 0 0
  password cisco
  login
line aux 0
line vty 0 4
  password cisco
  login
!
scheduler allocate 20000 1000
!
end

M3#show run

Building configuration...

Current configuration : 1478 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname M3
!
boot-start-marker
boot-end-marker
!
enable password cisco

no aaa new-model
memory-size iomem 10
!!
ip cef
!
ip host PAGENT-SECURITY-V3 97.32.43.85 87.84.0.0
!
multilink bundle-name authenticated
!
voice-card 0

no dspfarm
!
class-map match-all prec5

match precedence 5

class AF1
match ip dscp 26

class-map match-any prec7

match precedence 7

class EF
match ip dscp 46

class-map match-all prec0

match precedence 0

class AF2
match ip dscp 18
!
!
Policy-map SETDSCP

class EF
set ip dscp 46

class AF1
set ip dscp 26

class AF2
set ip dscp 18
!
!
policy-map shapingdefault

class prec7
shape peak 120000
bandwidth percent 50

class prec5
shape peak 80000
bandwidth percent 35

class class-default
bandwidth percent 15
!

interface FastEthernet0/0

no ip address

shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.20.30 255.255.255.0
 no fair-queue
 service-policy output shappingdefault
 service-policy input SETDSCP
!
interface Serial0/0/1
 ip address 192.168.200.30 255.255.255.0
 service-policy output shappingdefault
 service-policy input SETDSCP
!
router ospf 1
 log-adjacency-changes
 network 192.168.0.0 0.0.255.255 area 0
!
ip http server
 no ip http secure-server
!
control-plane
!
line con 0
 exec-timeout 0 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
scheduler allocate 20000 1000
!
end
###########################################################
**M4#show run**

Building configuration...

Current configuration : 1529 bytes
!
version 12.4
 service timestamps debug datetime msec
MPLS to support Quality of service Needs

service timestamps log datetime msec
no service password-encryption
!
hostname M4
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
memory-size iomem 10
!
ip cef
!
ip host PAGENT-SECURITY-V3 90.4.89.97 37.89.0.0
!
multilink bundle-name authenticated
no MPLS ip
!
voice-card 0
no dspfarm
!
class-map match-all prec5
 match precedence 5
class AF1
 match ip dscp 26
class-map match-any prec7
 match precedence 7
class EF
 match ip dscp 46
class-map match-all prec0
 match precedence 0
class AF2
 match ip dscp 18
!
!
Policy-map SETDSCP
 class EF
 set ip dscp 46
class AF1
 set ip dscp 26
class AF2
 set ip dscp 18
!
policy-map shapingdefault
 class prec7
 shape peak 120000
 bandwidth percent 50
class prec5
Appendix

shape peak 80000
bandwidth percent 35
class class-default
bandwidth percent 15
!
interface FastEthernet0/0
ip address 192.168.40.40 255.255.255.0
duplex auto
speed auto
service-policy input SETDSCP
service-policy output shapingdefault
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
ip address 192.168.30.40 255.255.255.0
service-policy input SETDSCP
service-policy output shapingdefault
!
router ospf 1
log-adjacency-changes
network 192.168.0.0 0.0.255.255 area 0
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login
!
scheduler allocate 20000 1000
!
end
##########################################################################
MPLS to support Quality of service Needs

**M5#show run**

Building configuration...

Current configuration : 1545 bytes

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname M5

boot-start-marker
boot-end-marker

enable password cisco

no aaa new-model
memory-size iomem 10

ip cef

ip host PAGENT-SECURITY-V3 10.58.87.12 64.83.0.0

multilink bundle-name authenticated
no MPLS ip

voice-card 0
no dspfarm

class-map match-all prec5
  match precedence 5
class AF1
  match ip dscp 26
class-map match-any prec7
  match precedence 7
class EF
  match ip dscp 46
class-map match-all prec0
  match precedence 0
class AF2
  match ip dscp 18

Policy-map SETDSCP
  class EF
    set ip dscp 46
class AF1
    set ip dscp 26
class AF2
    set ip dscp 18
!
policy-map shapingdefault
    class prec7
        shape peak 120000
        bandwidth percent 50
    class prec5
        shape peak 80000
        bandwidth percent 35
    class class-default
        bandwidth percent 15
!
interface FastEthernet0/0
    ip address 192.168.40.50 255.255.255.0
duplex auto
speed auto
service-policy output shapingdefault
service-policy input SETDSCP default
!
interface FastEthernet0/1
    no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
    ip address 192.168.50.50 255.255.255.0
    no fair-queue
service-policy output shapingdefault
service-policy input SETDSCP
!
interface Serial0/0/1
    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 http server
    no ip http secure-server
!
control-plane
!
line con 0
    exec-timeout 0 0
password cisco
login
MPLS to support Quality of service Needs

line aux 0
line vty 0 4
    password cisco
    login
!
scheduler allocate 20000 1000
!
end

P2#show run

Building configuration...
Current configuration : 1740 bytes
!
version 12.4
service timestamps debug datatime msec
service timestamps log datatime msec
no service password-encryption
!
hostname P2
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
memory-size iomem 10
!
ip cef
!
ip host PAGENT-SECURITY-V3 64.89.38.67 9.81.0.0
!
multilink bundle-name authenticated
!
voice-card 0
    no dspfarm
!
class-map match-any Critical
    match protocol rtp
class-map match-any EF
    match protocol rtp
class-map match-any Interactive
    match protocol eigrp
    match protocol ospf
    match protocol icmp
class-map match-any AF1
    match protocol eigrp
    match protocol ospf
    match protocol icmp
Appendix

class-map match-any Web
  match protocol http
  match protocol smtp

class-map match-any AF2
  match protocol http
  match protocol smtp

! policy-map SETDSCP
  class EF
    set ip dscp 46
  class AF1
    set ip dscp 26
  class AF2
    set ip dscp 18

! policy-map markingpolicy
  class Critical
    set precedence 7
    bandwidth percent 50
  class interactive
    set precedence 5
    bandwidth percent 35
  class web
    set precedence 3
  class class-default
    set precedence 0
    bandwidth percent 15

! interface FastEthernet0/0
  ip address 172.16.200.254 255.255.255.0
  duplex auto
  speed auto
  service-policy input SETDSCP

! interface FastEthernet0/1
  no ip address
  shutdown
duplex auto
  speed auto

! interface Serial0/0/0
  ip address 192.168.50.2 255.255.255.0
  no fair-queue
clock rate 64000
  service-policy output markingpolicy

! interface Serial0/0/1
  ip address 192.168.200.1 255.255.255.0
clock rate 64000
  service-policy output markingpolicy
MPLS to support Quality of service Needs

!
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 http server
no ip http secure-server
!
control-plane
!
line con 0
  exec-timeout 0 0
  password cisco
  login
line aux 0
line vty 0 4
  password cisco
  login
!
scheduler allocate 20000 1000
!
end
###########################################################
S2#show run

Building configuration...
Current configuration : 1146 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S2
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
oo aaa new-model
memory-size iomem 10
!
Appendix

ip cef
!
ip host PAGENT-SECURITY-V3 57.79.21.41 55.86.0.0
!
multilink bundle-name authenticated
!
voice-card 0
  no dspfarm
vtp domain CISCO
vtp mode transparent
!
vlan 10,20,30
!
interface Loopback0
  ip address 172.16.20.1 255.255.255.0
!
interface FastEthernet0/0
  ip address 172.16.200.1 255.255.255.0
duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  shutdown
duplex auto
  speed auto
!
interface Serial0/0/0
  no ip address
  shutdown
  no fair-queue
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 http server
  no ip http secure-server
!
control-plane
!
line con 0
  exec-timeout 0 0
password cisco
MPLS to support Quality of service Needs

login
line aux 0
line vty 0 4
  password cisco
login
!
scheduler allocate 20000 1000
!end

###########################################################

MPLS based network
###########################################################

P1#show run
Building configuration...

Current configuration : 2511 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P1
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
!
!
!
!
!
mpls ldp advertise-labels for 1
!
voice-card 0
!
!
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 critical
  match protocol rtp
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
MPLS to support Quality of service Needs

speed auto
!
interface Serial0/1/0
   ip address 192.168.100.1 255.255.255.0
   mpls ip
   clock rate 64000
   service-policy input set-PHB
   service-policy output output-qos
!
interface Serial0/1/1
   ip address 192.168.30.2 255.255.255.0
   mpls ip
   clock rate 200000
   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 classless
!
!
ip http server
no ip http secure-server
!
access-list 1 permit 192.168.0.0 0.0.255.255
!
control-plane
!
!
line con 0
   password cisco
   login
line aux 0
line vty 0 4
   password cisco
   login
!
scheduler allocate 20000 1000
end
###########################################################
Appendix

**M1#show run**

Building configuration...

Current configuration : 2329 bytes

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname M1
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
voice-card 0
!
!
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
```
MPLS to support Quality of service Needs

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
  no ip address
  shutdown
duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  shutdown
duplex auto
  speed auto
!
interface Serial0/1/0
  ip address 192.168.100.10 255.255.255.0
  mpls ip
  service-policy output output-qos
!
interface Serial0/1/1
  ip address 192.168.10.10 255.255.255.0
  ip accounting precedence input
  mpls ip
  service-policy output output-qos
!
router ospf 1
log-adjacency-changes
network 192.168.0.0 0.0.255.255 area 0
!
  ip classless
!
!
ip http server

Appendix

no ip http secure-server
!
!
control-plane
!
line con 0
  password cisco
  login
line aux 0
line vty 0 4
  password cisco
  login
!
scheduler allocate 20000 1000
end
###########################################################

M2#show run

Building configuration...

Current configuration : 1375 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname M2
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
!
resource policy
!
memory-size iomem 10
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
ip host PAGENT-SECURITY-V3 21.63.1.51 90.34.0.0
MPLS to support Quality of service Needs

!
!
voice-card 0
!
!
class-map match-all mpls-af1
 match mpls experimental topmost 5
!
!
policy-map output-qos
 class mpls-af1
 bandwidth percent 60
 random-detect
!
!
interface FastEthernet0/0
 no ip address
 shutdown
duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 192.168.20.20 255.255.255.0
 ip accounting precedence input
 mpls ip
clock rate 64000
 service-policy output output-qos
!
interface Serial0/1/1
 ip address 192.168.10.20 255.255.255.0
 mpls ip
clock rate 64000
 service-policy output output-qos
!
router ospf 1
 log-adjacency-changes
 network 192.168.0.0 0.0.255.255 area 0
!
ip classless
!
!
ip http server
 no ip http secure-server
!
Appendix

!
control-plane
!
!
line con 0
exec-timeout 0 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login
!
scheduler allocate 20000 1000
end

###########################################################

M3#show run

Building configuration...

Current configuration : 1712 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname M3
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
!
resource policy
!
memory-size iomem 10
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
MPLS to support Quality of service Needs

ip host PAGENT-SECURITY-V3 97.32.43.85 87.84.0.0
!
!
voice-card 0
!
!
!
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
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/1/0
ip address 192.168.20.30 255.255.255.0
Appendix

mpls ip
service-policy output output-qos
!
interface Serial0/1/1
ip address 192.168.200.30 255.255.255.0
mpls ip
service-policy output output-qos
!
router ospf 1
log-adjacency-changes
network 192.168.0.0 0.0.255.255 area 0
!
ip classless
!
!
ip http server
no ip http secure-server
!

control-plane
!
!
!
line con 0
exec-timeout 0 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login
!
scheduler allocate 20000 1000
end

########################################################################

M4#show run

Building configuration...

*Aug 28 12:21:23.455: %SYS-5-CONFIG_I: Configured from console by console
Current configuration : 1734 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
MPLS to support Quality of service Needs

hostname M4
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
!
resource policy
!
memory-size iomem 10
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
!
ip host PAGENT-SECURITY-V3 90.4.89.97 37.89.0.0
!
voice-card 0
!

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
Appendix

    shape peak 400000
policy-map output-qos
    class mpls-af1
    bandwidth percent 60
    random-detect

!  
! interface FastEthernet0/0
ip address 192.168.40.40 255.255.255.0
duplex auto
speed auto
mpls ip
service-policy output output-qos
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/1/0
no ip address
shutdown
no fair-queue
clock rate 125000
!
interface Serial0/1/1
ip address 192.168.30.1 255.255.255.0
service-policy output output-qos
!
router ospf 1
log-adjacency-changes
network 192.168.0.0 0.0.255.255 area 0
!
ip classless
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
password cisco
login
line aux 0
line vty 0 4
MPLS to support Quality of service Needs

password cisco
login
!
scheduler allocate 20000 1000
end

#############################################################################

M5#show run

Building configuration...

Current configuration : 1731 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname M5
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
!
resource policy
!
memory-size iomem 10
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
ip host PAGENT-SECURITY-V3 10.58.87.12 64.83.0.0
!
!
voice-card 0
!
!
class-map match-all mpls-af1
  match mpls experimental topmost 5
class-map match-all prec5
  match precedence 5
class-map match-any prec7

77
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 192.168.40.50 255.255.255.0
duplex auto
speed auto
mpls ip
service-policy output output-qos
!
interface FastEthernet0/1
  no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/1/0
  ip address 192.168.50.50 255.255.255.0
mpls ip
service-policy output output-qos
!
interface Serial0/1/1
  no ip address
shutdown
clock rate 2000000
!
routing ospf 1
log-adjacency-changes
MPLS to support Quality of service Needs

network 192.168.0.0 0.0.255.255 area 0
!
ip classless
!
ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
  exec-timeout 0 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login
!
scheduler allocate 20000 1000
end

#########################################################################

P2#show run

Building configuration...

Current configuration : 2212 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P2
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
oo aa new-model
!
resource policy
!
memory-size iomem 10
Appendix

mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
!
!
ip host PAGENT-SECURITY-V3 64.89.38.67 9.81.0.0
!
mpls ldp advertise-labels for 1
!
voice-card 0
!
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 Critical
match protocol rtp
class-map match-any interactive
match protocol eigrp
match protocol ospf
class-map match-any web
match protocol http
match protocol smtp
!
policy-map set-PHB
  class mpls-af1 1
  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 172.16.200.254 255.255.255.0
duplex auto
MPLS to support Quality of service Needs

speed auto
service-policy input marking-policy
interface FastEthernet0/1
   no ip address
   shutdown
duplex auto
   speed auto
!
interface Serial0/1/0
   ip address 192.168.50.2 255.255.255.0
   mpls ip
clock rate 64000
   service-policy input set-PHB
   service-policy output output-qos
!
interface Serial0/1/1
   ip address 192.168.200.1 255.255.255.0
   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 classless
!
ip http server
   no ip http secure-server
!
access-list 1 permit 192.168.0.0 0.0.255.255
!
control-plane
!
line con 0
   password cisco
   login
line aux 0
line vty 0 4
   password cisco
   login
scheduler allocate 20000 1000
Appendix

end

Appendix B

Routing Tables and CEF Tables

IP routing based network Routing Tables

S1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

D EX 192.168.30.0/24
   [170/284160] via 172.16.100.254, 00:23:39, FastEthernet0/0
D EX 192.168.10.0/24
   [170/284160] via 172.16.100.254, 04:10:48, FastEthernet0/0
D EX 192.168.40.0/24
   [170/284160] via 172.16.100.254, 04:10:48, FastEthernet0/0
   172.16.0.0/24 is subnetted, 4 subnets
D EX 172.16.200.0
   [170/284160] via 172.16.100.254, 04:10:48, FastEthernet0/0
D EX 172.16.20.0 [170/284160] via 172.16.100.254, 04:10:48, FastEthernet0/0
C  172.16.10.0 is directly connected, Loopback0
C  172.16.100.0 is directly connected, FastEthernet0/0
D EX 192.168.200.0/24
   [170/284160] via 172.16.100.254, 04:10:48, FastEthernet0/0
D EX 192.168.20.0/24
   [170/284160] via 172.16.100.254, 04:10:51, FastEthernet0/0
D EX 192.168.50.0/24
   [170/284160] via 172.16.100.254, 04:10:51, FastEthernet0/0
D EX 192.168.100.0/24
   [170/284160] via 172.16.100.254, 04:24:03, FastEthernet0/0

P1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
MPLS to support Quality of service Needs

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C  192.168.30.0/24 is directly connected, Serial0/1/1
O  192.168.10.0/24 [110/321] via 192.168.30.40, 00:22:57, Serial0/1/1
O  192.168.40.0/24 [110/65] via 192.168.30.40, 00:22:57, Serial0/1/1
  172.16.0.0/24 is subnetted, 4 subnets
O E2  172.16.200.0 [110/20] via 192.168.30.40, 00:22:57, Serial0/1/1
O E2  172.16.10.0 [110/20] via 192.168.30.40, 00:22:57, Serial0/1/1
D  172.16.10.0 [90/156160] via 172.16.100.1, 04:23:24, FastEthernet0/0
C  172.16.100.0 is directly connected, FastEthernet0/0
O  192.168.200.0/24 [110/193] via 192.168.30.40, 00:22:57, Serial0/1/1
O  192.168.20.0/24 [110/257] via 192.168.30.40, 00:22:57, Serial0/1/1
O  192.168.50.0/24 [110/129] via 192.168.30.40, 00:22:57, Serial0/1/1
C  192.168.100.0/24 is directly connected, Serial0/1/0

#~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

M1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O  192.168.30.0/24 [110/845] via 192.168.100.1, 00:22:12, Serial0/1/0
C  192.168.10.0/24 is directly connected, Serial0/1/1
O  192.168.40.0/24 [110/846] via 192.168.100.1, 00:22:12, Serial0/1/0
  172.16.0.0/24 is subnetted, 4 subnets
O E2  172.16.200.0 [110/20] via 192.168.10.20, 00:22:12, Serial0/1/1
O E2  172.16.10.0 [110/20] via 192.168.10.20, 00:22:12, Serial0/1/1
O E2  172.16.10.0 [110/20] via 192.168.100.1, 00:22:12, Serial0/1/0
O  192.168.50.0/24 [110/909] via 192.168.10.20, 00:22:12, Serial0/1/1
O  192.168.20.0/24 [110/845] via 192.168.10.20, 00:22:12, Serial0/1/0
O  192.168.200.0/24 [110/910] via 192.168.100.1, 00:22:12, Serial0/1/0
C  192.168.100.0/24 is directly connected, Serial0/1/0

#~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

83
Appendix

**M2#show ip route**

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```
O    192.168.30.0/24 [110/257] via 192.168.20.30, 00:21:43, Serial0/0/0
C    192.168.10.0/24 is directly connected, Serial0/0/1
O    192.168.40.0/24 [110/193] via 192.168.20.30, 00:21:43, Serial0/0/0
    172.16.0.0/24 is subnetted, 4 subnets
    O E2  172.16.200.0 [110/20] via 192.168.20.30, 00:21:43, Serial0/0/0
    O E2  172.16.20.0 [110/20] via 192.168.20.30, 00:21:43, Serial0/0/0
    O E2  172.16.10.0 [110/20] via 192.168.20.30, 00:21:43, Serial0/0/0
    O E2  172.16.100.0 [110/20] via 192.168.20.30, 00:21:43, Serial0/0/0
O    192.168.200.0/24 [110/128] via 192.168.20.30, 00:21:43, Serial0/0/0
C    192.168.20.0/24 is directly connected, Serial0/0/0
O    192.168.50.0/24 [110/192] via 192.168.20.30, 00:21:43, Serial0/0/0
O    192.168.100.0/24 [110/321] via 192.168.20.30, 00:21:43, Serial0/0/0
    ###################################################################

**M3#show ip route**

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```
O    192.168.30.0/24 [110/257] via 192.168.200.1, 00:21:14, Serial0/0/1
O    192.168.10.0/24 [110/128] via 192.168.20.20, 00:21:14, Serial0/0/0
O    192.168.40.0/24 [110/193] via 192.168.200.1, 00:21:14, Serial0/0/1
    172.16.0.0/24 is subnetted, 4 subnets
    O E2  172.16.200.0 [110/20] via 192.168.200.1, 00:21:14, Serial0/0/1
    O E2  172.16.20.0 [110/20] via 192.168.200.1, 00:21:14, Serial0/0/1
    O E2  172.16.10.0 [110/20] via 192.168.200.1, 00:21:14, Serial0/0/1
    O E2  172.16.100.0 [110/20] via 192.168.200.1, 00:21:14, Serial0/0/1
```
MPLS to support Quality of service Needs

C  192.168.200.0/24 is directly connected, Serial0/0/1
C  192.168.20.0/24 is directly connected, Serial0/0/0

O  192.168.50.0/24 [110/128] via 192.168.200.1, 00:21:14, Serial0/0/1
O  192.168.100.0/24 [110/257] via 192.168.200.1, 00:21:14, Serial0/0/1

#......................................................................................#

M4#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
    D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
    ia - IS-IS inter area, * - candidate default, U - per-user static route
    o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C  192.168.30.0/24 is directly connected, Serial0/0/1
O  192.168.10.0/24 [110/257] via 192.168.40.50, 00:20:42, FastEthernet0/0
C  192.168.40.0/24 is directly connected, FastEthernet0/0
    172.16.0.0/24 is subnetted, 4 subnets
O E2  172.16.200.0 [110/20] via 192.168.40.50, 00:20:42, FastEthernet0/0
O E2  172.16.20.0 [110/20] via 192.168.40.50, 00:20:42, FastEthernet0/0
O E2  172.16.10.0 [110/20] via 192.168.30.2, 00:20:42, Serial0/0/1
O E2  172.16.100.0 [110/20] via 192.168.30.2, 00:20:42, Serial0/0/1
O  192.168.200.0/24 [110/20] via 192.168.40.50, 00:20:42, FastEthernet0/0
O  192.168.20.0/24 [110/193] via 192.168.200.1, 00:21:14, Serial0/0/0
O  192.168.50.0/24 [110/129] via 192.168.40.50, 00:20:42, FastEthernet0/0
O  192.168.100.0/24 [110/128] via 192.168.30.2, 00:20:42, Serial0/0/1

#......................................................................................#

M5#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
    D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
    ia - IS-IS inter area, * - candidate default, U - per-user static route
    o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O  192.168.30.0/24 [110/65] via 192.168.40.40, 00:19:56, FastEthernet0/0
O  192.168.10.0/24 [110/256] via 192.168.50.2, 00:19:56, Serial0/0/0
C  192.168.40.0/24 is directly connected, FastEthernet0/0
Appendix

172.16.0.0/24 is subnetted, 4 subnets
O E2 172.16.200.0 [110/20] via 192.168.50.2, 00:19:56, Serial0/0/0
O E2 172.16.20.0 [110/20] via 192.168.50.2, 00:19:56, Serial0/0/0
O E2 172.16.10.0 [110/20] via 192.168.40.40, 00:19:56, FastEthernet0/0
O E2 172.16.100.0 [110/20] via 192.168.40.40, 00:19:56, FastEthernet0/0
O 192.168.200.0/24 [110/128] via 192.168.50.2, 00:19:56, Serial0/0/0
O 192.168.20.0/24 [110/128] via 192.168.50.2, 00:19:56, Serial0/0/0
C 192.168.50.0/24 is directly connected, Serial0/0/0
O 192.168.100.0/24 [110/129] via 192.168.40.40, 00:19:56, FastEthernet0/0

###########################################################

P2#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O 192.168.30.0/24 [110/129] via 192.168.50.50, 00:19:22, Serial0/0/0
O 192.168.10.0/24 [110/129] via 192.168.200.30, 00:19:22, Serial0/0/1
O 192.168.40.0/24 [110/129] via 192.168.50.50, 00:19:22, Serial0/0/0
172.16.0.0/24 is subnetted, 4 subnets
C 172.16.200.0 is directly connected, FastEthernet0/0
D 172.16.20.0 [90/156160] via 172.16.200.1, 04:24:41, FastEthernet0/0
O E2 172.16.10.0 [110/20] via 192.168.50.50, 00:19:22, Serial0/0/0
O E2 172.16.100.0 [110/20] via 192.168.50.50, 00:19:22, Serial0/0/0
C 172.16.200.0/24 is directly connected, Serial0/0/1
O 192.168.20.0/24 [110/128] via 192.168.200.30, 00:19:22, Serial0/0/1
C 192.168.50.0/24 is directly connected, Serial0/0/0
O 192.168.100.0/24 [110/129] via 192.168.40.40, 00:19:56, FastEthernet0/0

###########################################################

S2#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

86
MPLS to support Quality of service Needs

Gateway of last resort is not set

D EX 192.168.30.0/24
[170/284160] via 172.16.200.254, 04:20:27, FastEthernet0/0
D EX 192.168.10.0/24
[170/284160] via 172.16.200.254, 04:21:52, FastEthernet0/0
D EX 192.168.40.0/24
[170/284160] via 172.16.200.254, 04:24:01, FastEthernet0/0
172.16.0.0/24 is subnetted, 4 subnets
C 172.16.200.0 is directly connected, FastEthernet0/0
C 172.16.20.0 is directly connected, Loopback0
D EX 172.16.10.0 [170/284160] via 172.16.200.254, 04:05:45, FastEthernet0/0
D EX 172.16.100.0
[170/284160] via 172.16.200.254, 04:05:45, FastEthernet0/0
D EX 192.168.200.0/24
D EX 192.168.20.0/24
D EX 192.168.50.0/24
[170/284160] via 172.16.200.254, 04:24:06, FastEthernet0/0
D EX 192.168.100.0/24
[170/284160] via 172.16.200.254, 04:06:09, FastEthernet0/0

drawable

MPLS based network CEF tables

drawable

P1#show ip cef

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>drop</td>
<td>Null0 (default route handler entry)</td>
</tr>
<tr>
<td>0.0.0.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>172.16.10.0/24</td>
<td>172.16.100.1</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.20.0/24</td>
<td>192.168.30.40</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>attached</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.100.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>172.16.100.1/32</td>
<td>172.16.100.1</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.100.254/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>172.16.200.0/24</td>
<td>192.168.30.40</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.10.0/24</td>
<td>192.168.100.10</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>192.168.100.10</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.30.0/24</td>
<td>attached</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.30.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.30.2/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.30.255/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.40.0/24</td>
<td>192.168.30.40</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.50.0/24</td>
<td>192.168.30.40</td>
<td>Serial0/1/1</td>
</tr>
</tbody>
</table>
Appendix

192.168.100.0/24 attached Serial0/1/0
192.168.100.0/32 receive
192.168.100.1/32 receive
192.168.100.255/32 receive

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.200.0/24</td>
<td>192.168.30.40</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>224.0.0.0/4</td>
<td>drop</td>
<td></td>
</tr>
<tr>
<td>224.0.0.0/24</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>255.255.255.255/32</td>
<td>receive</td>
<td></td>
</tr>
</tbody>
</table>

P1#show ip cef non-recursive

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.10.0/24</td>
<td>172.16.100.1</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.20.0/24</td>
<td>192.168.30.40</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>attached</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.100.1/32</td>
<td>172.16.100.1</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.200.0/24</td>
<td>192.168.30.40</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.10.0/24</td>
<td>192.168.100.10</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>192.168.100.10</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.30.0/24</td>
<td>attached</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.40.0/24</td>
<td>192.168.30.40</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.50.0/24</td>
<td>192.168.30.40</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.100.0/24</td>
<td>attached</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.200.0/24</td>
<td>192.168.30.40</td>
<td>Serial0/1/1</td>
</tr>
</tbody>
</table>

M1#show ip cef

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>drop</td>
<td>Null0 (default route handler entry)</td>
</tr>
<tr>
<td>0.0.0.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>172.16.10.0/24</td>
<td>192.168.100.1</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>172.16.20.0/24</td>
<td>192.168.10.20</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>192.168.100.1</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>172.16.200.0/24</td>
<td>192.168.10.20</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.10.0/24</td>
<td>attached</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.10.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.10.10/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.10.255/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>192.168.10.20</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.30.0/24</td>
<td>192.168.100.1</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.40.0/24</td>
<td>192.168.100.1</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.50.0/24</td>
<td>192.168.100.1</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.100.0/24</td>
<td>attached</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.100.0/32</td>
<td>receive</td>
<td></td>
</tr>
</tbody>
</table>
MPLS to support Quality of service Needs

192.168.100.10/32 receive
192.168.100.255/32 receive
192.168.200.0/24 192.168.10.20 Serial0/1/1
224.0.0.0/4 drop
224.0.0.0/24 receive
255.255.255.255/32 receive

#......................................................................................

M1#show ip cef non-recursive

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.10.0/24</td>
<td>192.168.100.1</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>172.16.20.0/24</td>
<td>192.168.10.20</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>192.168.100.1</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>172.16.200.0/24</td>
<td>192.168.10.20</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.10.0/24</td>
<td>attached</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>192.168.10.20</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.30.0/24</td>
<td>192.168.100.1</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.40.0/24</td>
<td>192.168.100.1</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.50.0/24</td>
<td>192.168.100.1</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.100.0/24</td>
<td>attached</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.200.0/24</td>
<td>192.168.10.20</td>
<td>Serial0/1/1</td>
</tr>
</tbody>
</table>

#......................................................................................

M2#show ip cef

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>drop</td>
<td>Null0 (default route handler entry)</td>
</tr>
<tr>
<td>0.0.0.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>172.16.10.0/24</td>
<td>192.168.10.10</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>172.16.20.0/24</td>
<td>192.168.20.30</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>192.168.10.10</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>172.16.200.0/24</td>
<td>192.168.20.30</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.10.0/24</td>
<td>attached</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.10.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.10.20/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.10.255/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>attached</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.20.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.20.20/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.20.255/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.30.0/24</td>
<td>192.168.10.10</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.40.0/24</td>
<td>192.168.20.30</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.10.10</td>
<td>Serial0/0/1</td>
<td></td>
</tr>
<tr>
<td>192.168.50.0/24</td>
<td>192.168.20.30</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.100.0/24</td>
<td>192.168.10.10</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.200.0/24</td>
<td>192.168.20.30</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>224.0.0.0/4</td>
<td>drop</td>
<td></td>
</tr>
</tbody>
</table>
Appendix

224.0.0.0/24        receive
Prefix              Next Hop             Interface
255.255.255.255/32  receive

#********************************************************************

M2#show ip cef non-recursive

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.10.0/24</td>
<td>192.168.10.10</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>172.16.20.0/24</td>
<td>192.168.20.30</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>192.168.10.10</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>172.16.200.0/24</td>
<td>192.168.20.30</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.10.0/24</td>
<td>attached</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>attached</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.30.0/24</td>
<td>192.168.10.10</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.40.0/24</td>
<td>192.168.20.30</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.10.10</td>
<td>Serial0/0/1</td>
<td></td>
</tr>
<tr>
<td>192.168.50.0/24</td>
<td>192.168.20.30</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.100.0/24</td>
<td>192.168.10.10</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.200.0/24</td>
<td>192.168.20.30</td>
<td>Serial0/0/0</td>
</tr>
</tbody>
</table>

#********************************************************************

M3#show ip cef

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>drop</td>
<td>Null0 (default route handler entry)</td>
</tr>
<tr>
<td>0.0.0.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>172.16.10.0/24</td>
<td>192.168.20.20</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>172.16.20.0/24</td>
<td>192.168.200.1</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>192.168.20.20</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>172.16.200.0/24</td>
<td>192.168.200.1</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.10.0/24</td>
<td>192.168.20.20</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>attached</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.20.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.20.30/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.20.255/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.30.0/24</td>
<td>192.168.200.1</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.40.0/24</td>
<td>192.168.200.1</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.50.0/24</td>
<td>192.168.200.1</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.100.0/24</td>
<td>192.168.20.20</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.200.0/24</td>
<td>attached</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.200.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.200.30/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.200.255/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>224.0.0.0/4</td>
<td>drop</td>
<td></td>
</tr>
<tr>
<td>224.0.0.0/24</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>255.255.255.255/32</td>
<td>receive</td>
<td></td>
</tr>
</tbody>
</table>
MPLS to support Quality of service Needs

###########################################################

**M3#show ip cef non-recursive**

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.10.0/24</td>
<td>192.168.20.20</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>172.16.20.0/24</td>
<td>192.168.200.1</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>192.168.20.20</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>172.16.200.0/24</td>
<td>192.168.200.1</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.10.0/24</td>
<td>192.168.20.20</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>attached</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.30.0/24</td>
<td>192.168.200.1</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.40.0/24</td>
<td>192.168.200.1</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.50.0/24</td>
<td>192.168.200.1</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.100.0/24</td>
<td>192.168.20.20</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.200.0/24</td>
<td>attached</td>
<td>Serial0/0/1</td>
</tr>
</tbody>
</table>

###########################################################

**M4#show ip cef**

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>drop</td>
<td>Null0 (default route handler entry)</td>
</tr>
<tr>
<td>0.0.0.0/32</td>
<td>receive</td>
<td>Null0 (default route handler entry)</td>
</tr>
<tr>
<td>172.16.10.0/24</td>
<td>192.168.30.2</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>172.16.20.0/24</td>
<td>192.168.40.50</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>192.168.30.2</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>172.16.200.0/24</td>
<td>192.168.40.50</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.10.0/24</td>
<td>192.168.30.2</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>192.168.40.50</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.30.0/24</td>
<td>attached</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.30.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.30.40/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.30.255/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.40.0/24</td>
<td>attached</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.40.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.40.40/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.40.50/32</td>
<td>192.168.40.50</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.40.255/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.50.0/24</td>
<td>192.168.40.50</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.100.0/24</td>
<td>192.168.30.2</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.200.0/24</td>
<td>192.168.40.50</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>224.0.0.0/4</td>
<td>drop</td>
<td></td>
</tr>
<tr>
<td>224.0.0.0/24</td>
<td>receive</td>
<td></td>
</tr>
</tbody>
</table>

Prefix       | Next Hop       | Interface    |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>255.255.255.255/32</td>
<td>receive</td>
<td></td>
</tr>
</tbody>
</table>

###########################################################
## M4#show ip cef non-recursive

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.10.0/24</td>
<td>192.168.30.2</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>172.16.20.0/24</td>
<td>192.168.40.50</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>192.168.30.2</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>172.16.200.0/24</td>
<td>192.168.40.50</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.10.0/24</td>
<td>192.168.30.2</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>192.168.40.50</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.30.0/24</td>
<td>attached</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.40.0/24</td>
<td>attached</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.40.50/32</td>
<td>192.168.40.50</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.50.0/24</td>
<td>192.168.40.50</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.100.0/24</td>
<td>192.168.30.2</td>
<td>Serial0/0/1</td>
</tr>
<tr>
<td>192.168.200.0/24</td>
<td>192.168.40.50</td>
<td>FastEthernet0/0</td>
</tr>
</tbody>
</table>

# M5#show ip cef

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>drop</td>
<td>Null0 (default route handler entry)</td>
</tr>
<tr>
<td>0.0.0.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>172.16.10.0/24</td>
<td>192.168.40.40</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.20.0/24</td>
<td>192.168.50.2</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>192.168.40.40</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.200.0/24</td>
<td>192.168.50.2</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.10.0/24</td>
<td>192.168.40.40</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>192.168.50.2</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.30.0/24</td>
<td>attached</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.40.0/24</td>
<td>attached</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.40.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.40.50/32</td>
<td>192.168.40.40</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.40.50/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.40.255/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.50.0/24</td>
<td>attached</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.50.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.50.50/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.50.255/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.100.0/24</td>
<td>192.168.40.40</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.200.0/24</td>
<td>192.168.50.2</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>224.0.0.0/4</td>
<td>drop</td>
<td></td>
</tr>
<tr>
<td>224.0.0.0/24</td>
<td>receive</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>255.255.255.255/32</td>
<td>receive</td>
<td></td>
</tr>
</tbody>
</table>
MPLS to support Quality of service Needs

###############################################################

M5#show ip cef non-recursive

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.10.0/24</td>
<td>192.168.40.40</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.20.0/24</td>
<td>192.168.50.2</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>192.168.40.40</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.200.0/24</td>
<td>192.168.50.2</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.10.0/24</td>
<td>192.168.40.40</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>192.168.50.2</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.30.0/24</td>
<td>192.168.40.40</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.40.0/24</td>
<td>attached</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.40.40/32</td>
<td>192.168.40.40</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.50.0/24</td>
<td>attached</td>
<td>Serial0/0/0</td>
</tr>
<tr>
<td>192.168.100.0/24</td>
<td>192.168.40.40</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.200.0/24</td>
<td>192.168.50.2</td>
<td>Serial0/0/0</td>
</tr>
</tbody>
</table>

###############################################################

P2#show ip cef

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>drop</td>
<td>Null0 (default route handler entry)</td>
</tr>
<tr>
<td>0.0.0.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>172.16.10.0/24</td>
<td>192.168.50.50</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>172.16.20.0/24</td>
<td>172.16.200.1</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>192.168.50.50</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>172.16.200.0/24</td>
<td>attached</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.200.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>172.16.200.1/32</td>
<td>172.16.200.1</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.200.254/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>172.16.200.255/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.10.0/24</td>
<td>192.168.200.30</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>192.168.200.30</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.30.0/24</td>
<td>192.168.50.50</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.40.0/24</td>
<td>192.168.50.50</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.50.0/24</td>
<td>attached</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.50.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.50.2/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.50.255/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.100.0/24</td>
<td>192.168.50.50</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.200.0/24</td>
<td>attached</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.200.0/32</td>
<td>receive</td>
<td></td>
</tr>
<tr>
<td>192.168.200.1/32</td>
<td>receive</td>
<td></td>
</tr>
</tbody>
</table>

Prefix Next Hop Interface
192.168.200.255/32 receive
224.0.0.0/4 drop
224.0.0.0/24 receive
255.255.255.255/32 receive
Appendix

P2#show ip cef non-recursive

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.10.0/24</td>
<td>192.168.50.50</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>172.16.20.0/24</td>
<td>172.16.200.1</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>192.168.50.50</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>172.16.200.0/24</td>
<td>attached</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>172.16.200.1/32</td>
<td>172.16.200.1</td>
<td>FastEthernet0/0</td>
</tr>
<tr>
<td>192.168.10.0/24</td>
<td>192.168.200.30</td>
<td>Serial0/1/1</td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>192.168.50.50</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.30.0/24</td>
<td>192.168.50.50</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.40.0/24</td>
<td>192.168.50.50</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.50.0/24</td>
<td>attached</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.100.0/24</td>
<td>192.168.50.50</td>
<td>Serial0/1/0</td>
</tr>
<tr>
<td>192.168.200.0/24</td>
<td>attached</td>
<td>Serial0/1/1</td>
</tr>
</tbody>
</table>

Appendix C

MPLS Based network outputs

MPLS based network LDP Bindings

P1#show MPLS ldp bindings

P1#show mpls ldp bindings

tib entry: 172.16.10.0/24, rev 22
  local binding: tag: 23
  remote binding: tsr: 192.168.10.10:0, tag: 19
  remote binding: tsr: 192.168.40.40:0, tag: 20

tib entry: 172.16.20.0/24, rev 16
  local binding: tag: 21
  remote binding: tsr: 192.168.10.10:0, tag: 22
  remote binding: tsr: 192.168.40.40:0, tag: 22

tib entry: 172.16.100.0/24, rev 20
  local binding: tag: imp-null
  remote binding: tsr: 192.168.40.40:0, tag: 19
  remote binding: tsr: 192.168.10.10:0, tag: 18

tib entry: 172.16.200.0/24, rev 18
  local binding: tag: 22
  remote binding: tsr: 192.168.10.10:0, tag: 23
  remote binding: tsr: 192.168.40.40:0, tag: 23

tib entry: 192.168.10.0/24, rev 8
  local binding: tag: 17
MPLS to support Quality of service Needs

remote binding: tsr: 192.168.10.10:0, tag: imp-null
remote binding: tsr: 192.168.40.40:0, tag: 17

tib entry: 192.168.20.0/24, rev 10
local binding: tag: 18
remote binding: tsr: 192.168.10.10:0, tag: 20
remote binding: tsr: 192.168.40.40:0, tag: 18

remote binding: tsr: 192.168.10.10:0, tag: 17
remote binding: tsr: 192.168.40.40:0, tag: imp-null

tib entry: 192.168.30.0/24, rev 2
local binding: tag: imp-null
remote binding: tsr: 192.168.10.10:0, tag: 17
remote binding: tsr: 192.168.40.40:0, tag: imp-null

remote binding: tsr: 192.168.10.10:0, tag: 17
remote binding: tsr: 192.168.40.40:0, tag: imp-null

tib entry: 192.168.40.0/24, rev 6
local binding: tag: 16
remote binding: tsr: 192.168.10.10:0, tag: 16
remote binding: tsr: 192.168.40.40:0, tag: imp-null

remote binding: tsr: 192.168.10.10:0, tag: 16
remote binding: tsr: 192.168.40.40:0, tag: imp-null

tib entry: 192.168.50.0/24, rev 12
local binding: tag: 19
remote binding: tsr: 192.168.10.10:0, tag: 24
remote binding: tsr: 192.168.40.40:0, tag: 24

remote binding: tsr: 192.168.10.10:0, tag: imp-null
remote binding: tsr: 192.168.40.40:0, tag: imp-null
remote binding: tsr: 192.168.40.40:0, tag: 16

tib entry: 192.168.100.0/24, rev 4
local binding: tag: imp-null
remote binding: tsr: 192.168.10.10:0, tag: imp-null
remote binding: tsr: 192.168.40.40:0, tag: 16

remote binding: tsr: 192.168.10.10:0, tag: 24
remote binding: tsr: 192.168.40.40:0, tag: 24

remote binding: tsr: 192.168.10.10:0, tag: 21
remote binding: tsr: 192.168.40.40:0, tag: 23

remote binding: tsr: 192.168.10.10:0, tag: imp-null
remote binding: tsr: 192.168.40.40:0, tag: 18

remote binding: tsr: 192.168.40.40:0, tag: imp-null
remote binding: tsr: 192.168.40.40:0, tag: 16
remote binding: tsr: 192.168.40.40:0, tag: 18

P2#show MPLS ldp bindings

tib entry: 172.16.10.0/24, rev 67
local binding: tag: 23
remote binding: tsr: 192.168.40.50:0, tag: 21
remote binding: tsr: 192.168.200.30:0, tag: 23

tib entry: 172.16.20.0/24, rev 10
local binding: tag: 19
remote binding: tsr: 192.168.200.30:0, tag: 20
remote binding: tsr: 192.168.40.50:0, tag: 23

remote binding: tsr: 192.168.10.10:0, tag: 21
remote binding: tsr: 192.168.40.50:0, tag: 24

remote binding: tsr: 192.168.200.30:0, tag: 19
remote binding: tsr: 192.168.40.50:0, tag: 24

remote binding: tsr: 192.168.10.10:0, tag: 16
remote binding: tsr: 192.168.200.30:0, tag: 20
remote binding: tsr: 192.168.40.50:0, tag: 22

remote binding: tsr: 192.168.10.10:0, tag: imp-null
remote binding: tsr: 192.168.200.30:0, tag: 19
remote binding: tsr: 192.168.40.50:0, tag: 24

remote binding: tsr: 192.168.10.10:0, tag: 16
remote binding: tsr: 192.168.200.30:0, tag: 16
remote binding: tsr: 192.168.40.50:0, tag: 18
Appendix

```
tib entry: 192.168.20.0/24, rev 18
  local binding: tag: 22
  remote binding: tsr: 192.168.200.30:0, tag: imp-null
  remote binding: tsr: 192.168.40.50:0, tag: 19

tib entry: 192.168.30.0/24, rev 53
  local binding: tag: 18
  remote binding: tsr: 192.168.200.30:0, tag: 18
  remote binding: tsr: 192.168.40.50:0, tag: 16

tib entry: 192.168.40.0/24, rev 51
  local binding: tag: 17
  remote binding: tsr: 192.168.200.30:0, tag: 17
  remote binding: tsr: 192.168.40.50:0, tag: imp-null

tib entry: 192.168.50.0/24, rev 61
  local binding: tag: imp-null
  remote binding: tsr: 192.168.40.50:0, tag: imp-null
  remote binding: tsr: 192.168.200.30:0, tag: 24

tib entry: 192.168.100.0/24, rev 55
  local binding: tag: 20
  remote binding: tsr: 192.168.10.20:0, tag: 24
  remote binding: tsr: 192.168.100.1:0, tag: 23

#...................................................

M1#show mpls ldp bindings

```
tib entry: 172.16.10.0/24, rev 44
  local binding: tag: 17
  remote binding: tsr: 192.168.10.20:0, tag: 18

tib entry: 172.16.20.0/24, rev 54
  local binding: tag: 24
  remote binding: tsr: 192.168.10.20:0, tag: 24
  remote binding: tsr: 192.168.100.1:0, tag: 23

tib entry: 172.16.100.0/24, rev 46
  local binding: tag: 18
  remote binding: tsr: 192.168.100.1:0, tag: imp-null
  remote binding: tsr: 192.168.10.20:0, tag: 19

tib entry: 172.16.200.0/24, rev 52
  local binding: tag: 23
  remote binding: tsr: 192.168.10.20:0, tag: 23
  remote binding: tsr: 192.168.100.1:0, tag: 22

tib entry: 192.168.10.0/24, rev 10
  local binding: tag: imp-null
  remote binding: tsr: 192.168.10.20:0, tag: imp-null
  remote binding: tsr: 192.168.100.1:0, tag: 17

tib entry: 192.168.20.0/24, rev 12
MPLS to support Quality of service Needs

local binding: tag: 19
remote binding: tsr: 192.168.10.20:0, tag: imp-null
remote binding: tsr: 192.168.100.1:0, tag: 18

tib entry: 192.168.30.0/24, rev 42
local binding: tag: 16
remote binding: tsr: 192.168.100.1:0, tag: imp-null
remote binding: tsr: 192.168.10.20:0, tag: 17

tib entry: 192.168.40.0/24, rev 48
local binding: tag: 20
remote binding: tsr: 192.168.100.1:0, tag: 20
remote binding: tsr: 192.168.10.20:0, tag: 20

tib entry: 192.168.50.0/24, rev 50
local binding: tag: 22
remote binding: tsr: 192.168.100.1:0, tag: 21
remote binding: tsr: 192.168.10.20:0, tag: 22

tib entry: 192.168.100.0/24, rev 38
local binding: tag: imp-null
remote binding: tsr: 192.168.20.30:0, tag: 24
remote binding: tsr: 192.168.10.10:0, tag: imp-null

tib entry: 192.168.200.0/24, rev 16
local binding: tag: 21
remote binding: tsr: 192.168.10.20:0, tag: 21
remote binding: tsr: 192.168.100.1:0, tag: 19

#~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

M2#show mpls ldp bindings

tib entry: 172.16.10.0/24, rev 44
local binding: tag: 18
remote binding: tsr: 192.168.10.10:0, tag: 17
remote binding: tsr: 192.168.20.30:0, tag: 19

tib entry: 172.16.20.0/24, rev 54
local binding: tag: 24
remote binding: tsr: 192.168.20.30:0, tag: 24
remote binding: tsr: 192.168.10.10:0, tag: 24

tib entry: 172.16.100.0/24, rev 46
local binding: tag: 19
remote binding: tsr: 192.168.10.10:0, tag: 18
remote binding: tsr: 192.168.20.30:0, tag: 20

tib entry: 172.16.200.0/24, rev 52
local binding: tag: 23
remote binding: tsr: 192.168.20.30:0, tag: 23
remote binding: tsr: 192.168.10.10:0, tag: 23

tib entry: 192.168.10.0/24, rev 4
local binding: tag: imp-null
remote binding: tsr: 192.168.20.30:0, tag: 17
remote binding: tsr: 192.168.10.10:0, tag: imp-null

tib entry: 192.168.20.0/24, rev 12
local binding: tag: imp-null
remote binding: tsr: 192.168.20.30:0, tag: imp-null
remote binding: tsr: 192.168.10.10:0, tag: 19

tib entry: 192.168.30.0/24, rev 42
  local binding: tag: 17
  remote binding: tsr: 192.168.10.10:0, tag: 16
  remote binding: tsr: 192.168.20.30:0, tag: 18

tib entry: 192.168.40.0/24, rev 48
  local binding: tag: 20
  remote binding: tsr: 192.168.10.10:0, tag: 20
  remote binding: tsr: 192.168.20.30:0, tag: 21

tib entry: 192.168.50.0/24, rev 50
  local binding: tag: 22
     remote binding: tsr: 192.168.10.10:0, tag: 22
     remote binding: tsr: 192.168.20.30:0, tag: 22

tib entry: 192.168.100.0/24, rev 38
  local binding: tag: 16
     remote binding: tsr: 192.168.10.10:0, tag: imp-null
     remote binding: tsr: 192.168.20.30:0, tag: 16

tib entry: 192.168.200.0/24, rev 16
  local binding: tag: 21
     remote binding: tsr: 192.168.10.10:0, tag: imp-null
     remote binding: tsr: 192.168.20.30:0, tag: 21

#----------------------------------------------------------------------------------

M3#show mpls ldp bindings

tib entry: 172.16.10.0/24, rev 45
  local binding: tag: 19
     remote binding: tsr: 192.168.10.20:0, tag: 18
     remote binding: tsr: 192.168.200.1:0, tag: 21

tib entry: 172.16.20.0/24, rev 55
  local binding: tag: 24
     remote binding: tsr: 192.168.10.20:0, tag: 24
     remote binding: tsr: 192.168.200.1:0, tag: 23

tib entry: 172.16.100.0/24, rev 47
  local binding: tag: 20
     remote binding: tsr: 192.168.10.20:0, tag: 19
     remote binding: tsr: 192.168.200.1:0, tag: 22

tib entry: 172.16.200.0/24, rev 53
  local binding: tag: 23
     remote binding: tsr: 192.168.10.20:0, tag: 23
     remote binding: tsr: 192.168.200.1:0, tag: imp-null

tib entry: 192.168.10.0/24, rev 4
  local binding: tag: 17
     remote binding: tsr: 192.168.10.20:0, tag: imp-null
     remote binding: tsr: 192.168.200.1:0, tag: 17

tib entry: 192.168.20.0/24, rev 12
  local binding: tag: imp-null
MPLS to support Quality of service Needs

remote binding: tsr: 192.168.10.20:0, tag: imp-null
remote binding: tsr: 192.168.200.1:0, tag: 18
tib entry: 192.168.30.0/24, rev 43
  local binding: tag: 18
  remote binding: tsr: 192.168.10.20:0, tag: 17
  remote binding: tsr: 192.168.200.1:0, tag: 19
tib entry: 192.168.40.0/24, rev 49
  local binding: tag: 21
  remote binding: tsr: 192.168.10.20:0, tag: 20
  remote binding: tsr: 192.168.200.1:0, tag: 16
tib entry: 192.168.50.0/24, rev 51
  local binding: tag: 22
  remote binding: tsr: 192.168.10.20:0, tag: 22
  remote binding: tsr: 192.168.200.1:0, tag: imp-null
tib entry: 192.168.100.0/24, rev 39
  local binding: tag: 16
  remote binding: tsr: 192.168.10.20:0, tag: 16
  remote binding: tsr: 192.168.200.1:0, tag: 20
tib entry: 192.168.200.0/24, rev 16
  local binding: tag: imp-null
  remote binding: tsr: 192.168.10.20:0, tag: 21
  remote binding: tsr: 192.168.200.1:0, tag: imp-null

###########################################################

M4#show mpls ldp bindings

tib entry: 172.16.10.0/24, rev 55
  local binding: tag: 20
  remote binding: tsr: 192.168.50.50:0, tag: 21
tib entry: 172.16.20.0/24, rev 61
  local binding: tag: 24
  remote binding: tsr: 192.168.50.50:0, tag: 22
tib entry: 172.16.100.0/24, rev 57
  local binding: tag: 21
  remote binding: tsr: 192.168.50.50:0, tag: 23
tib entry: 172.16.200.0/24, rev 59
  local binding: tag: 22
  remote binding: tsr: 192.168.50.50:0, tag: 24
tib entry: 192.168.10.0/24, rev 47
  local binding: tag: 16
  remote binding: tsr: 192.168.50.50:0, tag: 16
tib entry: 192.168.20.0/24, rev 49
  local binding: tag: 17
  remote binding: tsr: 192.168.50.50:0, tag: 17
tib entry: 192.168.30.0/24, rev 42
  local binding: tag: imp-null
  remote binding: tsr: 192.168.50.50:0, tag: 18
tib entry: 192.168.40.0/24, rev 63
  local binding: tag: imp-null
Appendix

remote binding: tsr: 192.168.50.50:0, tag: imp-null
  tib entry: 192.168.50.0/24, rev 66
    local binding: tag: 23
    remote binding: tsr: 192.168.50.50:0, tag: imp-null
  tib entry: 192.168.100.0/24, rev 51
    local binding: tag: 18
    remote binding: tsr: 192.168.50.50:0, tag: 19
  tib entry: 192.168.200.0/24, rev 53
    local binding: tag: 19
    remote binding: tsr: 192.168.50.50:0, tag: 20

###########################################################################

M5#show mpls ldp bindings

tib entry: 172.16.10.0/24, rev 14
  local binding: tag: 21
    remote binding: tsr: 192.168.200.1:0, tag: 21
    remote binding: tsr: 192.168.30.1:0, tag: 20
  tib entry: 172.16.20.0/24, rev 16
    local binding: tag: 22
      remote binding: tsr: 192.168.200.1:0, tag: 23
    remote binding: tsr: 192.168.30.1:0, tag: 24
  tib entry: 172.16.100.0/24, rev 18
    local binding: tag: 23
      remote binding: tsr: 192.168.200.1:0, tag: 22
    remote binding: tsr: 192.168.30.1:0, tag: 21
  tib entry: 172.16.200.0/24, rev 20
    local binding: tag: 24
      remote binding: tsr: 192.168.200.1:0, tag: imp-null
      remote binding: tsr: 192.168.30.1:0, tag: 22
  tib entry: 192.168.10.0/24, rev 4
    local binding: tag: 16
      remote binding: tsr: 192.168.200.1:0, tag: 17
  tib entry: 192.168.20.0/24, rev 6
    local binding: tag: 17
      remote binding: tsr: 192.168.200.1:0, tag: 18
      remote binding: tsr: 192.168.30.1:0, tag: 17
  tib entry: 192.168.30.0/24, rev 8
    local binding: tag: 18
      remote binding: tsr: 192.168.200.1:0, tag: 19
      remote binding: tsr: 192.168.30.1:0, tag: imp-null
  tib entry: 192.168.40.0/24, rev 22
    local binding: tag: imp-null
      remote binding: tsr: 192.168.200.1:0, tag: 24
      remote binding: tsr: 192.168.30.1:0, tag: imp-null
  tib entry: 192.168.50.0/24, rev 2
    local binding: tag: imp-null
MPLS to support Quality of service Needs

remote binding: tsr: 192.168.200.1:0, tag: imp-null
remote binding: tsr: 192.168.30.1:0, tag: 23
tib entry: 192.168.100.0/24, rev 10
local binding: tag: 19
remote binding: tsr: 192.168.200.1:0, tag: 20
remote binding: tsr: 192.168.30.1:0, tag: 18
tib entry: 192.168.200.0/24, rev 12
local binding: tag: 20
remote binding: tsr: 192.168.200.1:0, tag: imp-null
remote binding: tsr: 192.168.30.1:0, tag: 19

#########################################################################

MPLS Forwarding Tables

#########################################################################

P1#show mpls forwarding-table

<table>
<thead>
<tr>
<th>Local</th>
<th>Outgoing</th>
<th>Prefix</th>
<th>Bytes</th>
<th>tag</th>
<th>Outgoing</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
<td>tag or VC</td>
<td>or Tunnel Id</td>
<td></td>
<td></td>
<td>switched</td>
<td>interface</td>
</tr>
<tr>
<td>16</td>
<td>Pop tag</td>
<td>192.168.10.0/24</td>
<td>0</td>
<td>16</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>17</td>
<td>Pop tag</td>
<td>192.168.40.0/24</td>
<td>0</td>
<td>17</td>
<td>Se0/1/1</td>
<td>point2point</td>
</tr>
<tr>
<td>18</td>
<td>17</td>
<td>172.16.200.0/24</td>
<td>0</td>
<td>18</td>
<td>Se0/1/1</td>
<td>point2point</td>
</tr>
<tr>
<td>19</td>
<td>18</td>
<td>172.16.20.0/24</td>
<td>0</td>
<td>19</td>
<td>Se0/1/1</td>
<td>point2point</td>
</tr>
<tr>
<td>20</td>
<td>Untagged</td>
<td>172.16.10.0/24</td>
<td>0</td>
<td>20</td>
<td>Fa0/0</td>
<td>172.16.100.1</td>
</tr>
<tr>
<td>22</td>
<td>23</td>
<td>192.168.20.0/24</td>
<td>29926</td>
<td>22</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>23</td>
<td>22</td>
<td>192.168.50.0/24</td>
<td>37840</td>
<td>23</td>
<td>Se0/1/1</td>
<td>point2point</td>
</tr>
</tbody>
</table>

#########################################################################

P2#show mpls forwarding-table

<table>
<thead>
<tr>
<th>Local</th>
<th>Outgoing</th>
<th>Prefix</th>
<th>Bytes</th>
<th>tag</th>
<th>Outgoing</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
<td>tag or VC</td>
<td>or Tunnel Id</td>
<td></td>
<td></td>
<td>switched</td>
<td>interface</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>192.168.30.0/24</td>
<td>0</td>
<td>16</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>17</td>
<td>17</td>
<td>192.168.10.0/24</td>
<td>0</td>
<td>17</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>18</td>
<td>Pop tag</td>
<td>192.168.40.0/24</td>
<td>0</td>
<td>18</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>19</td>
<td>Untagged</td>
<td>172.16.20.0/24</td>
<td>0</td>
<td>19</td>
<td>Fa0/0</td>
<td>172.16.200.1</td>
</tr>
<tr>
<td>20</td>
<td>20</td>
<td>172.16.10.0/24</td>
<td>0</td>
<td>20</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>21</td>
<td>21</td>
<td>172.16.100.0/24</td>
<td>0</td>
<td>21</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>22</td>
<td>23</td>
<td>192.168.20.0/24</td>
<td>0</td>
<td>22</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>23</td>
<td>24</td>
<td>192.168.100.0/24</td>
<td>0</td>
<td>23</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
</tbody>
</table>

#########################################################################

M1#show mpls forwarding-table
### Appendix

<table>
<thead>
<tr>
<th>Local</th>
<th>Outgoing</th>
<th>Prefix</th>
<th>Bytes</th>
<th>tag</th>
<th>Outgoing</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tag or VC</td>
<td>or Tunnel Id</td>
<td>switched</td>
<td>interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Pop tag</td>
<td>192.168.30.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>16</td>
<td>172.16.10.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Pop tag</td>
<td>172.16.100.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Pop tag</td>
<td>192.168.20.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>20</td>
<td>192.168.40.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>19</td>
<td>172.16.200.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>21</td>
<td>192.168.50.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>22</td>
<td>192.168.200.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>23</td>
<td>172.16.20.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
<td></td>
</tr>
</tbody>
</table>

M2#show mpls forwarding-table

<table>
<thead>
<tr>
<th>Local</th>
<th>Outgoing</th>
<th>Prefix</th>
<th>Bytes</th>
<th>tag</th>
<th>Outgoing</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tag or VC</td>
<td>or Tunnel Id</td>
<td>switched</td>
<td>interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Pop tag</td>
<td>192.168.100.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>16</td>
<td>192.168.30.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>17</td>
<td>172.16.10.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>18</td>
<td>172.16.100.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>20</td>
<td>192.168.40.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Pop tag</td>
<td>192.168.200.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>22</td>
<td>192.168.50.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>23</td>
<td>192.168.200.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>24</td>
<td>172.16.20.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
<td></td>
</tr>
</tbody>
</table>

M3#show mpls forwarding-table

<table>
<thead>
<tr>
<th>Local</th>
<th>Outgoing</th>
<th>Prefix</th>
<th>Bytes</th>
<th>tag</th>
<th>Outgoing</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tag or VC</td>
<td>or Tunnel Id</td>
<td>switched</td>
<td>interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>192.168.100.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Pop tag</td>
<td>192.168.10.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>19</td>
<td>192.168.30.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>18</td>
<td>172.16.10.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>19</td>
<td>172.16.100.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>16</td>
<td>192.168.40.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Pop tag</td>
<td>192.168.50.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Pop tag</td>
<td>192.168.200.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>23</td>
<td>172.16.20.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
<td></td>
</tr>
</tbody>
</table>

M4#show mpls forwarding-table
MPLS to support Quality of service Needs

<table>
<thead>
<tr>
<th>Local tag</th>
<th>Outgoing tag or VC</th>
<th>Prefix</th>
<th>Bytes tag</th>
<th>Outgoing</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>Untagged</td>
<td>192.168.10.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
</tr>
<tr>
<td>17</td>
<td>Untagged</td>
<td>192.168.20.0/24</td>
<td>0</td>
<td>Fa0/0</td>
<td>192.168.40.50</td>
</tr>
<tr>
<td>18</td>
<td>Untagged</td>
<td>192.168.100.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
</tr>
<tr>
<td>19</td>
<td>Untagged</td>
<td>192.168.200.0/24</td>
<td>0</td>
<td>Fa0/0</td>
<td>192.168.40.50</td>
</tr>
<tr>
<td>20</td>
<td>Untagged</td>
<td>172.16.10.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
</tr>
<tr>
<td>21</td>
<td>Untagged</td>
<td>172.16.100.0/24</td>
<td>0</td>
<td>Se0/1/1</td>
<td>point2point</td>
</tr>
<tr>
<td>22</td>
<td>Untagged</td>
<td>172.16.200.0/24</td>
<td>0</td>
<td>Fa0/0</td>
<td>192.168.40.50</td>
</tr>
<tr>
<td>23</td>
<td>Untagged</td>
<td>172.16.50.0/24</td>
<td>0</td>
<td>Fa0/0</td>
<td>192.168.40.50</td>
</tr>
<tr>
<td>24</td>
<td>Untagged</td>
<td>172.16.20.0/24</td>
<td>0</td>
<td>Fa0/0</td>
<td>192.168.40.50</td>
</tr>
</tbody>
</table>

M5#show mpls forwarding-table

<table>
<thead>
<tr>
<th>Local tag</th>
<th>Outgoing tag or VC</th>
<th>Prefix</th>
<th>Bytes tag</th>
<th>Outgoing</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>17</td>
<td>192.168.10.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>17</td>
<td>18</td>
<td>192.168.20.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>18</td>
<td>19</td>
<td>192.168.30.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>19</td>
<td>20</td>
<td>192.168.100.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>20</td>
<td>Pop tag</td>
<td>192.168.200.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>21</td>
<td>21</td>
<td>172.16.10.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>22</td>
<td>23</td>
<td>172.16.20.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>23</td>
<td>22</td>
<td>172.16.100.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
<tr>
<td>24</td>
<td>Pop tag</td>
<td>172.16.200.0/24</td>
<td>0</td>
<td>Se0/1/0</td>
<td>point2point</td>
</tr>
</tbody>
</table>