DOKUZ EYLÜL UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED

SCIENCES

DESIGN AND ANALYSIS OF MULTI-PROTOCOL LABEL SWITCHING NETWORKS

By

Ayşe ŞENOL

September, 2007

İZMİR

DESIGN AND ANALYSIS OF MULTI-PROTOCOL LABEL SWITCHING NETWORKS

A Thesis Submitted to the

Graduate School of Natural and Applied Sciences of

Dokuz Eylül University

In Partial Fulfillment of the Requirements for

the Degree of Master of Science in Electrical and Electronics Engineering

By

Ayşe ŞENOL

September, 2007

İZMİR

M.Sc THESIS EXAMINATION RESULT FORM

We certify that we have read this thesis and **"DESIGN AND ANALYSIS OF MULTI-PROTOCOL LABEL SWITCHING NETWORKS"** completed by AYŞE ŞENOL under supervision of **ASST. PROF. DR. ZAFER DICLE** and that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Asst. Prof. Dr. Zafer Dicle
Supervisor

Assoc. Prof. Dr. Yalçın Çebi
(Jury Member)

Asst. Prof. Dr.Reyat Yılmaz
(Jury Member)

Prof. Dr. Cahit HELVACI
Director
Graduate School of Natural and Applied Sciences

ACKNOWLEDGMENTS

I would like to give my sincere thanks to my supervisor, Asst. Prof. Dr. Zafer Dicle for his guidance, advice and encouragement along the fulfillment of this project.

I want to thank my family for their support and tolarence during this work and all my life, and to all the friends who have been helped in this thesis.

Ayşe ŞENOL

DESIGN AND ANALYSIS OF
MULTI-PROTOCOL LABEL SWITCHING NETWORKS

ABSTRACT

Service providers must consider lots of factors while designing their backbone such as ensuring high performance, scalability, robustness, coping with new age technologies. MPLS is a preferred technology by most of the service providers because of the advantages in these topics. In addition, as using MPLS, different services which service providers want to offer, e.g. voice over IP, video and TV applications, internet access, point to point services, layer 3 and layer 2 vpn services can be provided in same network. MPLS reduces networking costs and improves speed and sorts of the services.

MPLS enables carrying IP over ATM. MPLS is also convenient technology for the service providers having ATM backbones.

OSPF or IS-IS can be used as an interior gateway routing protocol in an MPLS network. Interior gateway routing protocols are used to distribute the IP forwarding routes to all the routers in the network. BGP is used to communicate between the AS of the service provider and the different ASs. LDP distributes the label information to the all routers in the network. LDP learns the network information from OSPF or IS-IS.

Keywords : MPLS, LDP, label.

ÇOK PROTOKOLLÜ ETİKET ANAHTARLAMA AĞLARININ TASARIM VE ANALİZİ

ÖZ

Servis sağlayıcıları omurgalarını tasarlarken yüksek performansı sağlama, ölçeklenebilirlik, dayanıklılık, yeni nesil teknolojilere uyum sağlama gibi bir çok unsuru göz önünde bulundurmalıdırlar. MPLS bir çok servis sağlayıcı tarafından bu özellikleri sağladığı için tercih edilen bir teknolojidir. Ek olarak, servis sağlayıcıların sunmak istedikleri, IP üzerinden ses, video ve TV uygulamaları, internet erişimi, katman 3 ve katman 2 vpn servisleri gibi hizmetler MPLS kullanılarak aynı omurga üzerinden verilebilir.

MPLS, IP üzerinde ATM taşımaya imkan verir. Bu sebeple MPLS ayrıca ATM omurgaya sahip olan servis sağlayıcılar için uygun bir teknolojidir.

OSPF veya IS-IS dahili yönlendirme protokolü olarak MPLS ağda kullanılabilir. Dahili yönlendirme protokolleri IP yönlendirme bilgisinin ağdaki tüm diğer yönlendiricilere dağıtılmasını sağlar. BGP, servis sağlayıcı AS'inin diğer AS'ler ile haberleşmesini sağlar. LDP, label bilgisini ağdaki tüm yönlendiricilere dağıtır. LDP ağ bilgisini OSPF ya da IS-IS'den öğrenir.

Anahtar sözcükler : MPLS, LDP, etiket.

CONTENTS

Page

CHAPTER ONE
INTRODUCTION

1.1 Introduction

Multi-protocol label switching, MPLS, is a standard routing and switching platform which combines the label switching and forwarding technology with routing technology of network layer rather than a service or application. Basic idea of MPLS is routing at edge and switching in core.

MPLS is a QoS enabling technology that forces application flows into connection-oriented paths and provides mechanisms for traffic engineering and bandwidth guarantees along these paths. Furthermore, when an MPLS network supports DiffServ, traffic flows can receive classbased admission, differentiated queue servicing in the network nodes, preemption priority, and other network treatment that provide bases for QoS guarantees. The IETF work in this area has been augmented by the MPLS/Frame Relay (FR), Alliance Implementation Agreement which extends MPLS to the user-network interface, and thus serves as a foundation for implementing QoS end-to-end.

In this thesis, benefits of mpls and its advantages are explained in chapter two. The chapter three is related with an overview of MPLS operating mechanism. The support of TE and QoS are explained in the chapter four. MPLS VPNs is mentioned in chapter five. A MPLS network design and analysis of this network are explained in chapter six. Last chapter is the conclusion part.

CHAPTER TWO
BENEFITS OF MPLS

2.1 Why MPLS is used?

Expectations of user and service providers change. Users want faster, better, cheaper services. Service providers want more efficient operations. Mpls brings the speed of layer 2 switching to layer 3. MPLS provides reduced networking costs and improved speed to market products.

MPLS resolves the problems of IP over Asynchronous Transfer Mode, ATM, such as complexity of control and management and scalability issues. MPLS supports multiple layer 2 technologies, enables ATM service enhancements and new services.

MPLS extends functionality of legacy ATM switches. MPLS is also a competitive alternative to IP-based MPLS solutions.

MPLS helps carriers and large corporates scale their networks as increasingly large routing tables become more complex to manage. Transit routers no longer need to handle complete routing tables.

MLPS combines flexible any-to-any communication found on PSTN or Internet with the reliability and security delivered by Private Line, Frame Relay or ATM services.

The ultimate benefit is a unified or converged network supporting all classes of service. MPLS offers diferentiated performance levels and prioritisation of delay and non-delay sensitive traffic as well as voice and multimedia applications, all on a single network.

MPLS addresses traffic management issues by prioritising time sensitive applications. MPLS is a critical addition capability for IP networks. It solves problems for which no other solutions are known. It is difficult to anticipate the longer term future and what applications may be supported because of the innovations MPLS enables.

MPLS is a secure service, utilising leading edge IP and MPLS technology to isolate packets on the network, data remains confidential and network is protected from outside intrusion. Network traffic is monitored and proactively managed, enabling the customers to back the service with industry-leading, comprehensive Service Level Guarantees.

2.2 Applications for MPLS

2.2.1 IP-ATM integration

MPLS enables IP over ATM. The LER devices are responsible for IP flow classification and label imposition. The LSR devices located in the core are responsible for forwarding at Layer 2 while participating in the exchange of Layer 3 routing information. 'Label switching' also can be done by ATM to ATM switches. This involves putting IP routing and LDP software ATM switches, MPLS allows ATM switches to optimally support Virtual Private Networks (VPNs). VPNs form the infrastructure which corporations will base their whole business structures MPLS, in combination with network to support thousands of customers' VPNs. So, MPLS with providing VPN services on both ATM and packet-based equipment. Manageability of MPLS and BGP VPN services are a major benefit.

2.2.2 IP Explicit Routing and Traffic Engineering

MPLS has been views as an IP traffic engineering tecnlogy. Best effort delivery is not (always) sufficient. MPLS provides for explicit routing. An important problem

traffic flows to make best use of available network bandwidth. MPLS uses specially set up LSPs to finely adjust IP traffic flows.

2.2.3 Class of Services

The head end LSR could place high-priority traffic in one LSP, medium-priority traffic in another LSP, best-effort traffic in a third LSP, and less-than-best-effort traffic in a fourth LSP.

2.2.4 VPNs

VPN is the capability of both private and public networks to support a communication infrastructure connecting geographically dispersed sites where users can communicate among them as if they were in a private network. IPsec VPN and MPLS VPN forms layer 3 VPN. In IPsec VPN, the customer premises equipment, (CPE), need to have VPN support (IPsec support) which causes extra costs. In MPLS VPN, there is no extra cost for CPEs since there is no need to provide VPN support for CPEs VPN. Inlike IPsec VPN, in MPLS VPN there is no need to make encryption in CPEs, no performance and delay problems emerge and there is no need for tunneling between the center and branches of the customer edge, branches can access each other directly, thus delay is reduced, the central bandwidth is not used. MPLS also allows layer 2 VPNS.

2.2.5 Layer 2 Transport

MPLS provides layer 2 transport of IP packets. MPLS becomes forwarding infrastructure for a number of services, i.e. IP services, private data (Frame Relay, ATM, Ethernet).

CHAPTER THREE
MPLS LABEL FORWARDING

3.1 Basic Concepts About MPLS

3.1.1 MPLS domain

A contiguous set of nodes which operate MPLS routing and forwarding and which are also in one Routing or Administrative Domain.

3.1.2 FEC (Forwarding Equivalent Class)

A group of IP packets which are forwarded in the same manner (same destination, same forwarding path, same class of service).

3.1.3 Labeled Packet

Labeled packet is a packet into which a label has been encoded.

3.1.4 Label Stack

Label stack is a group of labels which are carried by one labeled packet and organized as a last-in, first-out stack.

3.1.5 LSR (Label Switching Router)

LSR is an MPLS node which is capable of forwarding native L3 packets.

3.1.6 Control Component

It is to distribute label, to select routing path, to generate forwarding table, to establish and release the LSP.

3.1.7 Forwarding Component

It is to forward labeled packets based on the forwarding table.

3.1.8 LER (Label Edge Router, also named as the edge LSR)

LER is an MPLS node that connects an MPLS domain with a node which is outside of the domain, either because it does not run MPLS, and/or because it is in a different domain.

3.1.9 LSP (Label Switched Path)

The path through one or more LSRs at one level of the hierarchy followed by packets in a particular FEC.

3.2 MPLS Shim Header

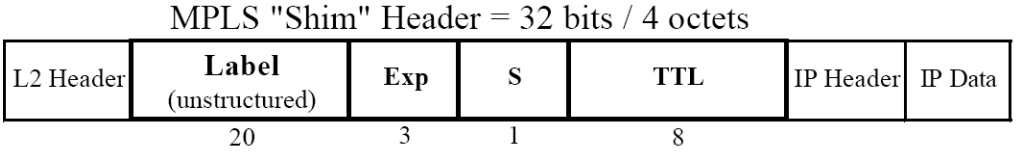

Figure 3.1 MPLS shim header

The 32-bit MPLS header contains the 20 bit label field carrying the actual value of the MPLS label (see figure 3.1). The three bit CoS field, also called exp bit, can affect

the queuing and discard algorithms applied to the packet as it is transmitted through the network. A single bit stack field that supports a hierarchical label stack. In addition an eight bit time-to-live (TTL) field that provides conventional IP TTL functionality (see figure 3.1) (V. Jolly & S. Latifi, IEEE, 2005)

When an IP packet presented to the LER, it pushes the shim header between layer 2 and layer 3 which is shown in figure 3.1.

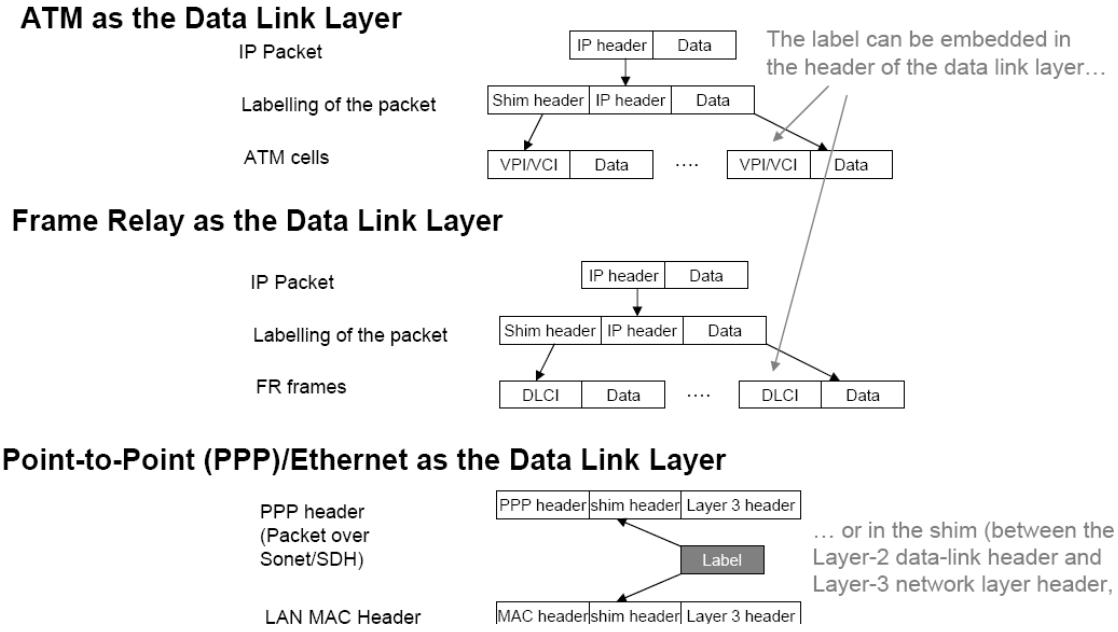

Figure 3.2 Label imposition in FR, ATM, Ethernet and PPP (Udo Payer, 2005)

The exact format of a label and how it is added to the packet depends on the layer 2 link technology used in the MPLS network. For example, a label could correspond to an ATM VPI/VCI, a Frame Relay DLCI, or a DWDM wavelength for optical networking.

3.3 LSPs

LSPs are fully established from ingress LER to egress LER. The LSP setup for an FEC is unidirectional in nature. The return traffic must take another LSP.

The paths that an LSP takes can be defined one of two ways:

Hop by Hop: LSRs along the path looks at the IP Route table to determine where the next hop for the LSP. Each LSR independently selects the next hop for a given FEC. The LSR uses any available routing protocols, such as OSPF, ATM private network-to-networkinterface (PNNI), etc.

Explicit Routing: Ingress-LSR (the LSR where the data flow to the network first starts) specifies which nodes to use to set up the LSP.

An LSP can be configured two ways: LSP can be configured manually. This requires going into each and every LSR and specifying the incoming label/interface and outgoing label/interface. This is much like ATM or Frame Relay PVCs are provisioned.

The other way, a protocol can be used to communicate label/interface binding to all LSR(this is the most practical method). Examples are LDP (Label s Distribution Protocol), RSVP-TE (RSVP with Traffic Engineering extensions), CR-LDP (Label Distribution Protocol with Constraint Based Routing), M-BGP (Multiprotocol BGP for VPNs.

Two types of LSP:

Point to point LSP: LSP follows route chosen when LSP is set up.

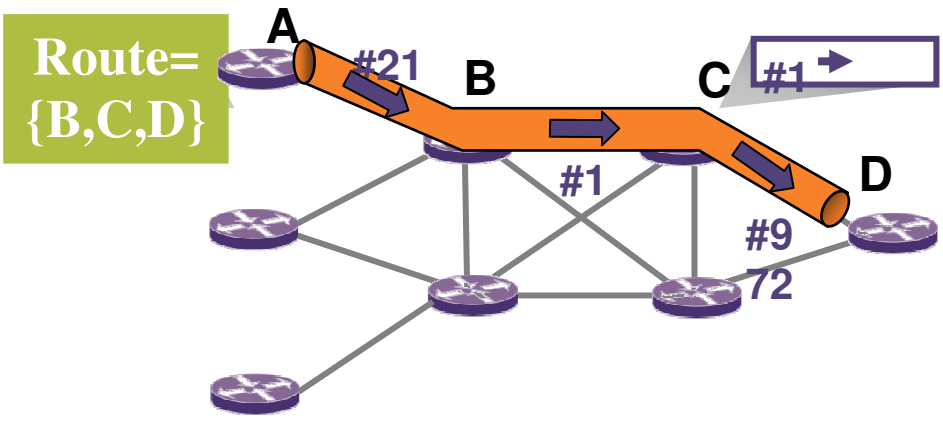

Figure 3.3 Point to point LSP

Merging LSP: LSP forms a “sink tree”. The branches of the LSP always follows the same route as normal IP forwarding; that is, the shortest path.

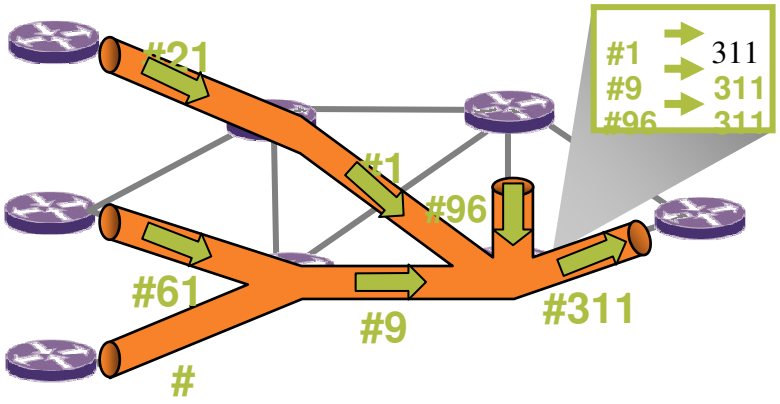

Figure 3.4 Merging LSP

3.4 Label Distribution Protocol

LDP (Label Distribution Protocol): is the control and signaling protocol of MPLS and the key technology of MPLS. LDP classifies the FEC, distributes label, transmits the result of distribution and establishs and maintains LSP.

In order that LSPs can be used, the forwarding tables at each LSR must be populated with the mappings from incoming interface, label value to outgoing interface, label value. This process is called LSP setup, or Label Distribution. There are multiple

different label distribution protocols for use in different scenarios, including the LDP, CR-LDP, RSVP, BGP4, OSPF.

3.4.1 LDP Messages

Discovery messages are used to discover and maintain the presence of new peers. Hello packets (UDP) sent to all-routers multicast address. Once neighbour is discovered, the LDP session is established over TCP

Session messages establish, maintain and terminate LDP sessions.
Advertisement messages create, modify, delete label mappings for FECs.
Notification messages provide advisory information and signal error information.

3.4.2 Signaling Mechanisms

3.4.2.1 Label Request

A LSR requests a label from its downstream neighbor so that it can bind to a specific FEC. This mechanism can be employed down the chain of LSRs up to the egress LER.

3.4.2.2 Label Mapping

In response to a label request, a downstream LSR will send a label to the upstream initiator using the label mapping mechanism. (Udo Payer, 2005)

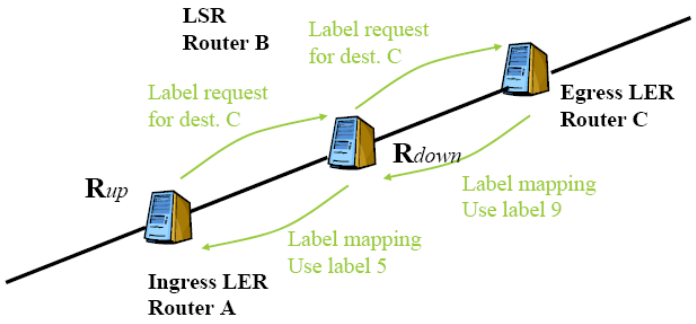

Figure 3.5 Label Request

3.5 Data Flow in MPLS Networks

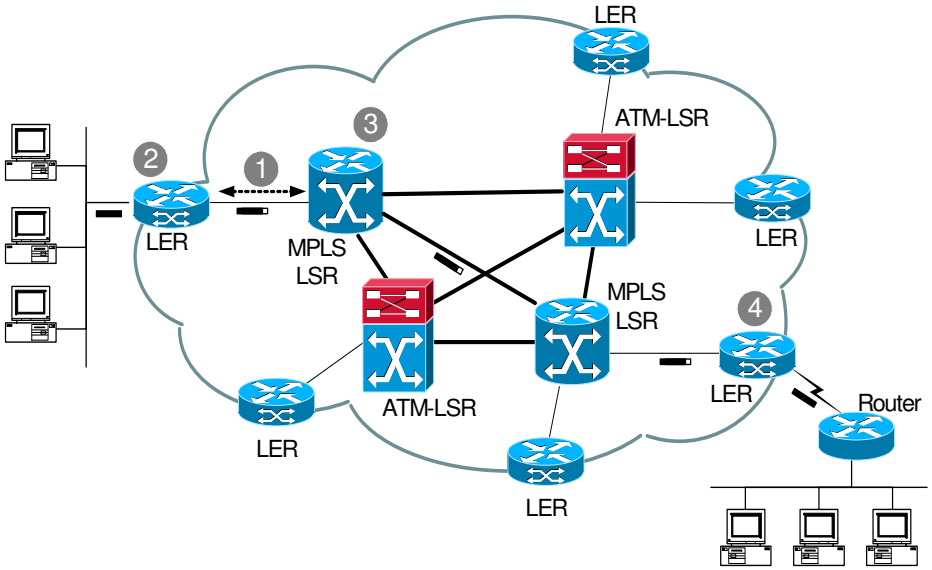

Figure 3.6 Packet flow in MPLS Network

Figure.3.6 shows a MPLS network. (1) Through LDP and traditional routing protocol (e.g. OSPF-TE, IS-IS-TE, the routing table and label mapping table for active FEC in all LSRs are established. Ingress LER (2) receives packet, performs Layer 3 value added services, and labels packet. LSR switches the packets using label swapping (3). LER at egress removes label and delivers packet.

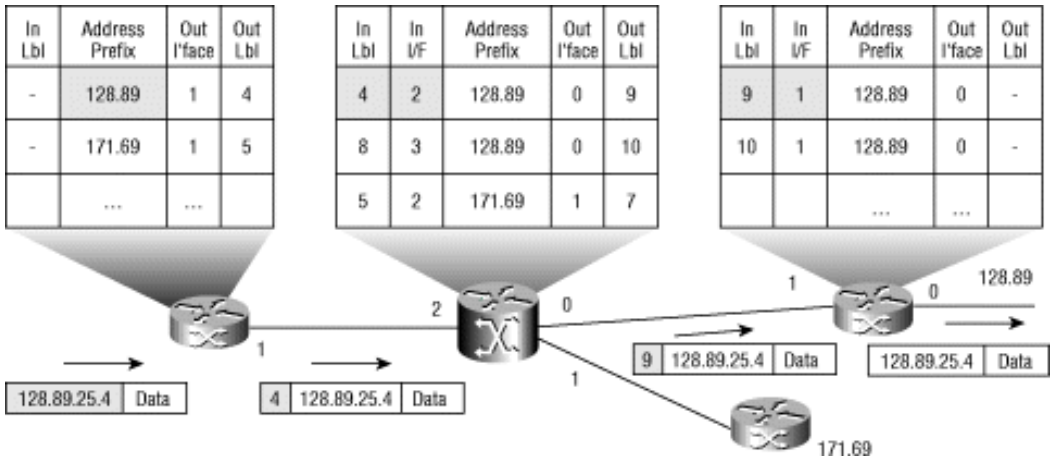

Figure 3.7 Label Swappig

Figure 3.7 shows an IP packet with destination address 128.89.25.4. Ingress LER receives initial unlabeled packet and push the first label based on predefined FEC. Label Information Base (LIB) of the ingress LER has 4, as the label value of 128.89.0.0 destination address. LER imposes label 4 into the packet before layer 3 header and sends the LSR. LSR looks up its LIB and swaps the label 4 and label 9 is imposed into packet. Egress LER recieves the packet with label 9 looks up its LIB and pops the label and sends the next router outside the MPLS nework.

3.6 Tunnels and Label Stack

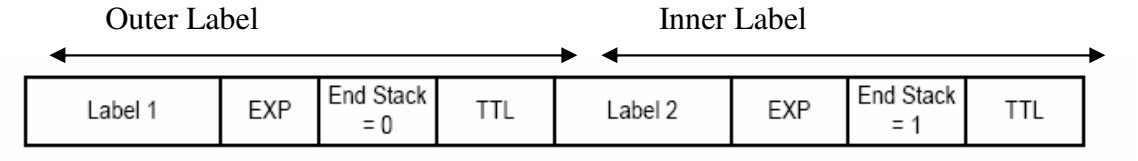

Figure 3.8 MPLS Label Stack

The MPLS shim header is also referred to as a label stack, since it may contain multiple entries. In the case of VPNs such as VPLS the inner label would be used to identify the customer VPN (Virtual Circuit ID) and the outer label the LSP.

The process of placing multiple labels on a packet is known as label stacking .

A key feature of MPLS, especially when considering VPNs, is that once the labels required for an LSP have been exchanged between the LSRs that support the LSP, intermediate LSRs transited by the LSP do not need to examine the content of the data packets flowing on the LSP. For this reason, LSPs are often considered to form tunnels across all or part of the backbone MPLS network. A tunnel carries opaque data between the tunnel ingress and tunnel egress LSRs.

This means that the entire payload, including IP headers, may safely be encrypted without damaging the ability of the network to forward data.

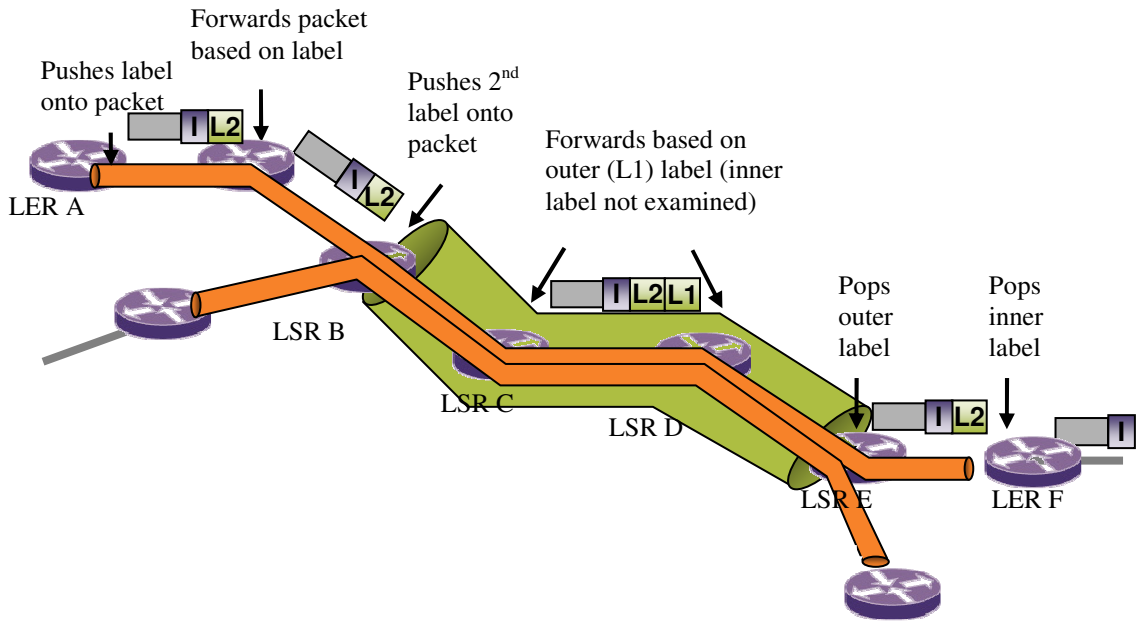

Figure 3.9 Label Stack Example

Figure 3.9 is an example of label stacking. Two LSPs are put in other LSP. This is implemented by allowing packet to have more than one label at a time. Labels form a stack. LSR always forward based on outermost or top label (last-in first out method). This technique is used to enable L2/L3 VPNs over MPLS core networks.

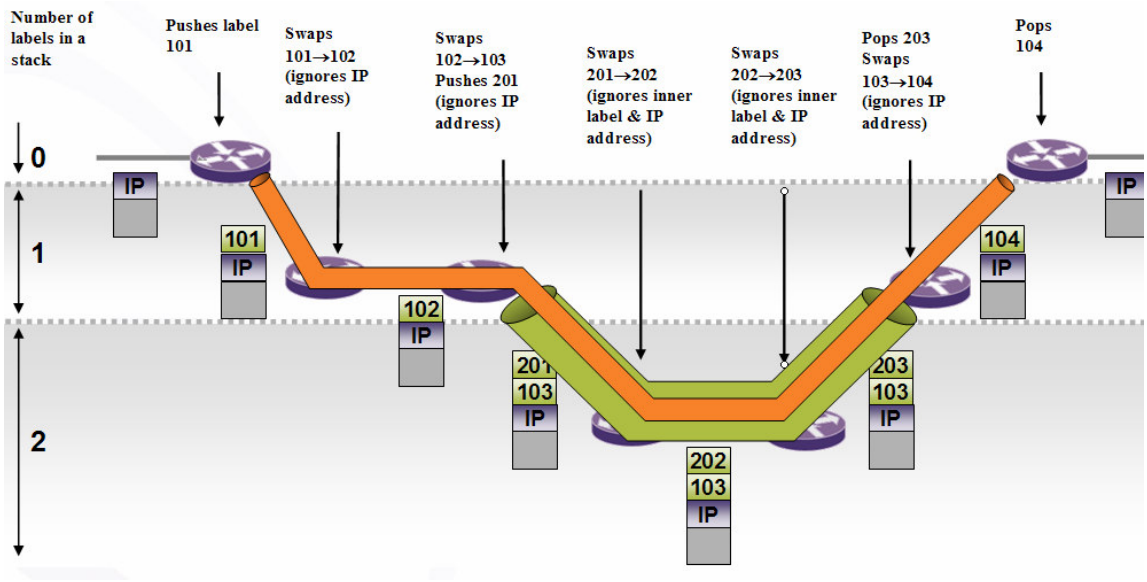

Figure 3.10 Label swapping in Label Stack

In Figure 3.10, Ingress LER pushes label 101. Next LSR swaps 101 to 102, ignores IP address. The next LSR, before the tunnel, swaps 102 into 103 and pushes 201, ignores IP address. The first LSR in tunnel, swaps 201 to 202, ignores inner label and ip address. The second LSR in tunnel swaps 202 to 203, ignores inner label and IP address. The next LSR, after the tunnel, pops 203, swaps 103 to 104 and egress LER pops 104.

In Figure3.10, both LSPs are acting as tunnels. LSR forwards the packets based only on the label attached to each packet. It does not inspect the contents of the packet or the encapsulated IP header.

An egress LSR may distribute labels for multiple FECs and set up multiple LSPs. Where these LSPs are parallel they can be routed, together, down a higher-level LSP tunnel between LSRs in the network. Labeled packets entering the higher-level LSP tunnel are given an additional label to see them through the network, and retain their first-level labels to distinguish them when they emerge from the higher-level tunnel.

Label stacks allow a finer granularity of traffic classification between tunnel ingress and egress nodes than is visible to the LSRs in the core of the network, which need only route data on the basis of the topmost label in the stack. This helps to reduce both the size of the forwarding tables that need to be maintained on the core LSRs and the complexity of managing data forwarding across the backbone.

A label stack is arranged with the label for the outer tunnel at the top and the label for the inner LSP at the bottom. On the wire (or fiber) the topmost label is transmitted first and is the only label used for routing the packet until it is popped from the stack and the next highest label becomes the top label.

For MPLS networks based on ATM equipment, it is attractive to consider using the VPI as the outer label and the VCI as the inner label. However, this places constraints on the number of outer and inner labels that may be too restrictive for an SP that needs to support many thousands of tunnels across the backbone. An alternative in such cases is to carry the inner label in a shim header below an outer VPI/VCI-based label. Although this method of label stacking in ATM means that the label stack cannot be fully implemented in standard ATM hardware, it does overcome other problems, not least of which is that some ATM hardware is incapable of performing VPI switching.

CHAPTER FOUR
MPLS TE AND QoS

4.1 Traffic Engineering

Traditional routing selects the shortest path. All traffic between the ingress and egress nodes passes through the same links causing congestion. LDP signaled paths only follows the IGP routing path. Traffic engineering allows a high degree of control over the path that packets take, allows more efficient use of network resources.
Traffic redirection is done through BGP or IGP shortcut. Resource utilization and network redundancy are improved. Load balancing is verified.

4.2 Why Traffic Engineering ?

A major goal of Internet Traffic Engineering is to facilitate efficient and reliable network operations while simultaneously optimizing network resource utilization and performance.

4.3 Classical RSVP

Classical RSVP designed in the 1990's (RFC 2205), is a generic QoS signaling protocol.

RSVP was specified as part of the IETF Integrated Services model. An Internet control protocol which uses IP as its network layer. RSVP designed originally for host to host signaling. RSVP has no concept of labels and LSPs - packets assumed to travel unlabelled. It uses the IGP to determine paths. There is no explicit route concept; reservations made along shortest path. RSVP is neither a data transport protocol nor routing protocol.

4.3.1 IntServ with RSVP

[IntServ] has defined the requirements for QoS mechanisms in order to satisfy two goals. The first goal is to serve real-time applications and the second goal is to control bandwidth-sharing among different traffic classes. Two types of service were defined to comply with the IntServ architecture: Guaranteed Service and Controlled Load Service, both focusing on an individual application's requirements.

4.3.1.1 Guaranteed Service

Guaranteed Service was defined to provide an assured level of bandwidth, a firm end-to-end delay bound, and no queuing loss; and it was intended for real-time applications such as voice and video.

4.3.1.2 The Controlled Load Service

The Controlled Load Service definition did not include any firm quantitative guarantees but rather "the appearance of a lightly loaded network."
It was intended for applications that could tolerate a limited amount of loss and delay, including adaptive real-time applications. By design, Controlled Load Service provided better performance than the Best- Effort treatment, because it would not noticeably deteriorate as the network load increased. In order to achieve their stated goals and provide the proposed services, the IntServ models included various traffic parameters such as rate and slack term for Guaranteed Service; and average rate, peak rate and burst size for Controlled Load Service. To install these parameter values in a network and to provide service guarantees for the realtime traffic, the Resource Reservation Protocol [RSVP] was developed as a signaling protocol for reservations and explicit admission control. The IntServ architecture has satisfied both necessary conditions for the network QoS, i.e., it provided the appropriate bandwidth and queuing resources for each application flow (a "microflow"). However, the IntServ implementations with RSVP

required the permicroflow state and signaling at every hop. This added significant complexity to network operation and was widely considered unscalable. Therefore, the IntServ model was implemented only in a limited number of networks, and the IETF moved to develop DiffServ as an alternative QoS approach with minimal complexity. (Vicoria Fineberg, 2003)

4.3.2 DiffServ

The DiffServ architecture has assumed an opposite approach to that of IntServ. It defined Classes of Service (CoS), called *Aggregates*, and QoS resource management functions with node-based, or *Per-Hop,* operation. The CoS definitions include a Behavior Aggregate (BA) which has specific requirements for scheduling and packet discarding, and an Ordered Aggregate (OA) which performs classification based on scheduling requirements only, and may include several drop precedence values. Thus, an OA is a coarser classification than a BA and may include several BAs. The node behavior definitions correspond to the CoS definitions. A Per Hop Behavior (PHB) is offered to a BA, whereas a PHB Scheduling Class (PSC) serves an OA; PHB mechanisms include scheduling and packet discarding, whereas PSC only concerns scheduling.

The DiffServ model is based on redefining the meaning of the 8-bit ToS field in the IP header. The original ToS definition was not widely implemented, and now the field is split into the 6-bit DiffServ Code Point (DSCP) value and the 2-bit Explicit Congestion Notification (ECN) part, as shown in Figure 4.1 below.

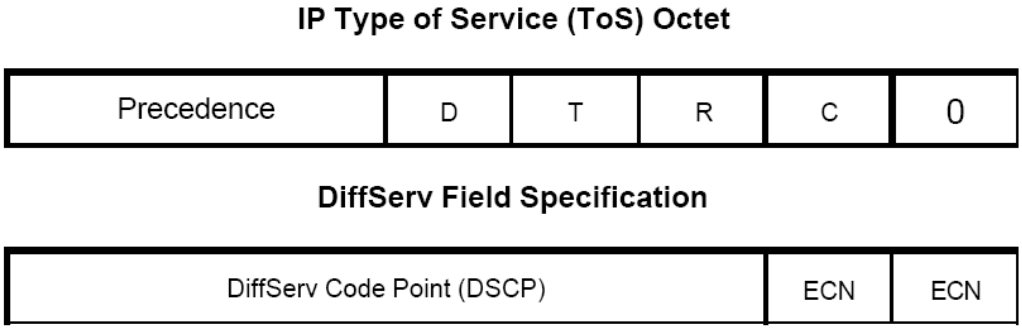

Figure 4.1 Relationship between ToS and DiffServ / ECN

In Figure 4.1, the letters indicate the following: D = Delay, T = Throughput, R = Reliability, C = Cost, ECN = Explicit Congestion Notification. The value of the DSCP field is used to specify a BA (i.e., a class), which is used by DiffServ-compliant nodes for choosing the appropriate PHB (i.e., a queue servicing treatment). Fourteen PHBs have been defined, including one for Expedited Forwarding (EF), twelve for Assured Forwarding (AF), and one for Default, or Best Effort, PHB. The twelve AF PHBs are divided into four PSCs, and each of the AF PSCs consists of three sub-behaviors related to different packet discarding treatment.

In summary, the DiffServ model allows the network to classify (combine) microflows into flow aggregates (BAs) and then to offer to these aggregates differentiated treatment in each DiffServ-capable node. This treatment is reflected in the queue servicing mechanisms which include scheduling and packet discarding. PHB is reflected in both scheduling and discarding, whereas PSC applies only to scheduling.
In the introductory section, we mentioned the two necessary conditions for QoS: guaranteed bandwidth, and class-related scheduling and packet discarding treatment. The DiffServ architecture satisfies the second condition, but not the first.

4.4 MPLS Traffic Engineering

The label switching approach was initially conceived in order to improve router performance, but this motivation has diminished with advances in router design and

achievement of line-speed forwarding of native IP packets. But later the most important advantage of the MPLS architecture over the native IP forwarding has become apparent: the connection-oriented nature of MPLS allows SPs to implement TE in their networks and achieve a variety of goals, including bandwidth assurance, diverse routing, load balancing, path redundancy, and other services that lead to QoS.

TE-REQ describes issues and requirements for Traffic Engineering implementation in MPLS networks. It provides a general definition of TE as a set of mechanisms for performance optimization of operational networks in order to achieve specific performance objectives and describes how MPLS supports TE by enabling control and measurement mechanisms.

The set of MPLS Traffic Engineering tools, defined in [RSVP-TE], OSPF-TE] and [ISIS-TE], that supports the requirements defined in [TE-REQ], is used today by many network operators to achieve major Traffic Engineering objectives defined in [TE-OVW]. TE-REQ uses the concept of an MPLS Traffic Trunk (TT) which is an aggregation of traffic flows of the same class that are placed inside an LSP. The principal distinction between a TT and an LSP is that a TT is an aggregated traffic flow, whereas an LSP is a *path* a TT takes through a network. For example, during a recovery process, a TT may be using a different LSP. TE-REQ describes a framework for mapping TTs onto LSPs by addressing three sets of capabilities:

4.4.1 TT attributes

TT attributes of particular interest are traffic parameters, priority, and preemption. Traffic parameter attributes may include values of peak rates, average rates, burst sizes and other resource requirements of a traffic trunk that can be used for resource allocation and congestion avoidance. The priority attribute allows the CR process to establish an order in which path selection is done so that higher priority TTs will have an earlier opportunity to claim network resources than lower priority TTs. The preemption

attribute determines whether a TT can or cannot preempt and can or cannot be preempted by another TT.

4.4.2 Resource Attributes That Constrain Placement of TTs

Resource attributes are topology state parameters such as Maximum Allocation Multiplier (MAM) which allows a network operator to allocate more or less resources than the link capacity in order to achieve the goals of overbooking or overprovisioning, respectively; and Resource Class Attributes which allow a network operator to classify network resources (e.g., "satellite," "intercontinental," etc.) and then apply to them resource-class based policies.

4.4.3 Constraint-Based Routing (CR)

Constraint-based Routing (CR), sometimes referred to as "QoS routing," enables a demand-driven, resource reservation-aware routing environment in which an I-LER automatically determines explicit routes for each TT it handles.

CR requires several network capabilities which include traffic-engineering extensions to Interior Gateway Protocols (IGPs) OSPF and IS-IS, i.e., OSPF-TE and ISIS-TE defined in [OSPF-TE] and [ISIS-TE] respectively, to carry additional information about the maximum link bandwidth, maximum reservable bandwidth, current bandwidth reservation at each priority level, and other values which are to allow the network management system to discover paths that meet TT constraints, resource availability and load balancing and recovery objectives algorithms that select feasible paths based on the information obtained from IGP-TEs (e.g., by pruning ineligible links and running a SPF algorithm on the remaining links resulting in a Constrained Shortest Path First (CSPF)) and generate explicit routes.

CR also requires label distribution by a traffic-engineering-enabled protocol such as RSVP-TE [RSVPTE]. RSVP-TE carries information about the explicit path identified by CR algorithms and several objects which contain signaling setup and holding priority attributes, preemption attribute, and some others.

CR also requires a bandwidth management or admission control function in each node that performs accounting of used and still available resources in the node, and provides this information to IGP-TE and RSVP-TE. With these mechanisms in place, MPLS-TE allows an SP to create stable paths with bandwidth reservation and traffic-engineer them for various network objectives. In order to guarantee bandwidth along these paths, MPLS-TE reservations must be supplemented with mechanisms that protect flows from interfering with each other during bursts beyond their reserved values. These mechanisms may include flow policing, overprovisioning, or queuing discipline that enforces fair sharing of links in the presence of contending traffic flows. Of the two necessary conditions for QoS: guaranteed bandwidth and differentiated servicing, MPLS-TE addresses the first condition, and RSVP-TE provides the means for controlling delay and delay variation for time-sensitive flows. (Vicoria Fineberg, 2003)

4.5 RSVP-TE (RFC 3209)

RSVP-TE operates on RSVP capable routers where tunneling extensions allow the creation of explicitly routed LSPs, provide smooth rerouting, preemption, and loop detection. RSVP-TE extensions to RSVP for LSP Tunnels. (draft-ietf-mpls-rsvp-lsp-tunnel-08).

Some of the major differences between the Standard RSVP and RSVP-TE protocols include the following:

Standard RSVP provides signaling between pairs of hosts; RSVP-TE provides signaling between pairs of LERs.

Standard RSVP applies to single host-to-host flows; RSVP-TE creates a state for a traffic trunk. An LSP tunnel usually aggregates multiple host-to-host flows and thus reduces the amount of RSVP state in the network.

Standard RSVP uses standard routing protocols operating on the destination address; RSVP-TE uses extended IGPs and constraint-based routing (CR). But just like Standard RSVP, RSVP-TE can support various IntServ service models and distribute various traffic conditioning parameters such as, for example, average rate, peak rate and burst size for Controlled Load Service. These features allow networks with MPLS-TE and RSVP-TE to provide various services with strict QoS requirements. One shortcoming of this solution is lack of a packet discard mechanism. A technology addressing this issue and providing another approach to QoS guarantees.

RSVP-TE Supports Downstream on Demand label distribution only. PATH messages used by sender to solicit a label from downstream LSRs. RESV messages used by downstream LSRs to pass label upstream towards the sender. RSVP-TE extends classical RSVP with new objects (TLVs) for these messages. Refresh reduction proposed as classical RSVP-TE maintains significant state information.

4.6 MPLS Support of DiffServ

Now, that both DiffServ and MPLS have been reviewed, we can discuss a technology that combines these two approaches in order to guarantee QoS. Let us recall that DiffServ provides a QoS treatment to traffic aggregates. It is a scalable and operationally simple solution as it does not require per- flow signaling and state. However, it cannot guarantee QoS, because it does not influence a packet path, and therefore, during a congestion or failure, even high-priority packets do not get guaranteed bandwidth.

MPLS, on the other hand, can force packets into specific paths and - in combination with constraint-based routing - can guarantee bandwidth for FECs. But in its basic form MPLS does not specify class-based differentiated treatment of flows.
Combining the DiffServ-based classification and PHBs with MPLS-based TE leads to true QoS in packet backbones. The mechanisms for MPLS support of DiffServ are described in RFC3270 [MPLS-DiffServ]. [MPLS-DiffServ] defines two types of LSPs: E-LSPs and L-LSPs. In an E-LSP, a label is used as the indication of the FEC destination, and the 3-bit Exp field is used as the indication of the class of a flow in order to select its PHB, including both scheduling and drop priority. Note that DiffServ uses 6 bits to define BAs and the corresponding PHBs, whereas E-LSP has only 3 bits for this function.

In an L-LSP, a label is used as the indication of both the FEC destination and its scheduling priority. The Exp field in an L- LSP is used only for the indication of the drop priority. Mappings between IP headers with DiffServ and MPLS shim headers for E-LSP and LLSP are shown in Figures 3 and 4, respectively. In these figures, the term "5-tuple" refers to the five fields in an IP packet header, including source and destination IP addresses, source and destination TCP or UDP ports, and a protocol that can be used for defining a FEC.

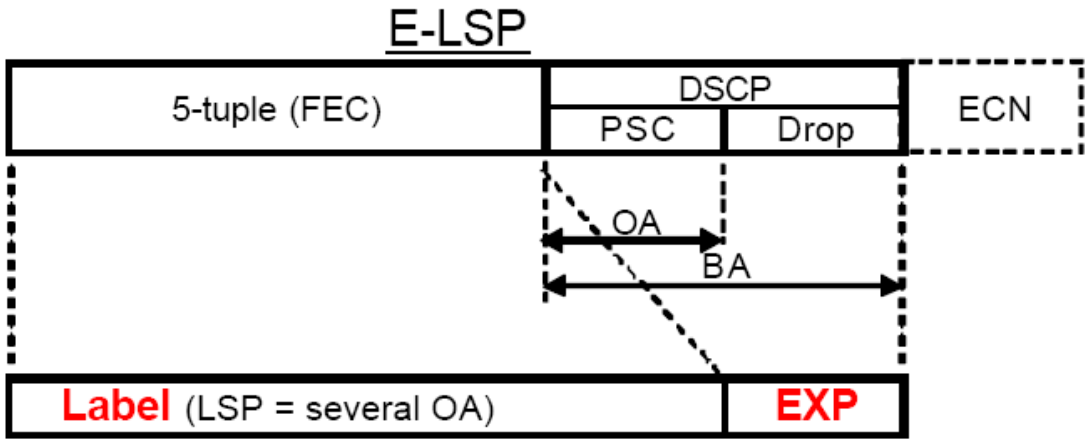

Figure 4.2 Mapping between an IP header and an MPLS shim header for an E-LSP

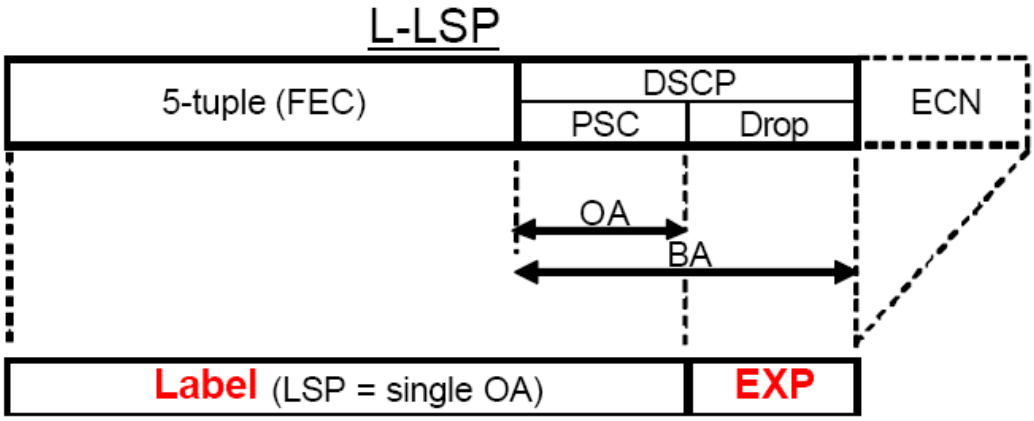

Figure 4.3 Mapping between an IP header and an MPLS shim header for an L-LSP

Note that Figures 4.2 and 4.3 represent mappings between portions of the native IP header, and the Label and EXP parts of the MPLS shim header. They are *not to-scale* and do not represent the complete structure of either header. Each type of LSP has its advantages and disadvantages. E-LSPs are easier to operate, and are more scalable because they preserve labels and use the EXP field for DiffServ features. But considering that MPLS signaling reserves bandwidth on a per-LSP basis, the bandwidth is reserved for the entire LSP without the PSC-based granularity, and there may be insufficient bandwidth in queues serving some particular PSCs. L-LSPs, on the other hand, are more cumbersome to provision, because more labels are needed to tag all PSCs of all FECs. But (because a label carries the scheduling information) when bandwidth is reserved for a given L-LSP, it is associated with the priority queue to which this LSP belongs. The next two figures illustrate how routing and QoS improve network routing by using basic MPLS and then DiffServ Support of MPLS.

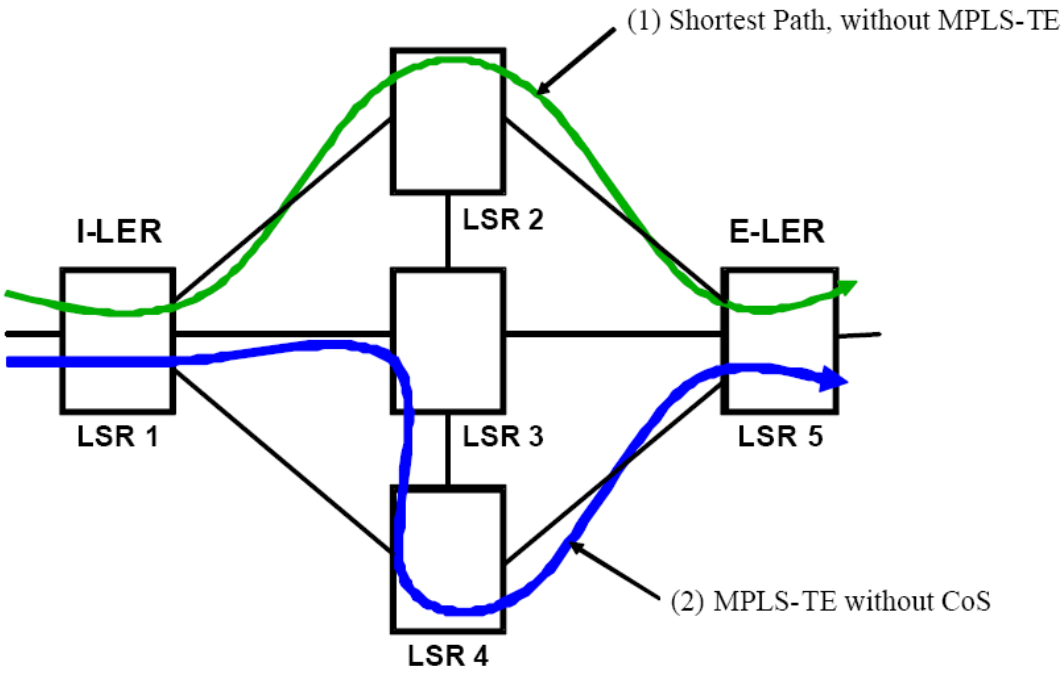

Figure 4.4 Packet flow in MPLS without DiffServ

Figure 4.4 illustrates the difference between a path taken by packets that follow shortest path routing (1) and a traffic-engineered path (2). Path (2) may have been chosen because it has sufficient bandwidth to serve a given FEC, but this bandwidth is not associated with any specific class of service, and thus priority traffic (for example, VoIP) may not have sufficient bandwidth for its particular queue.

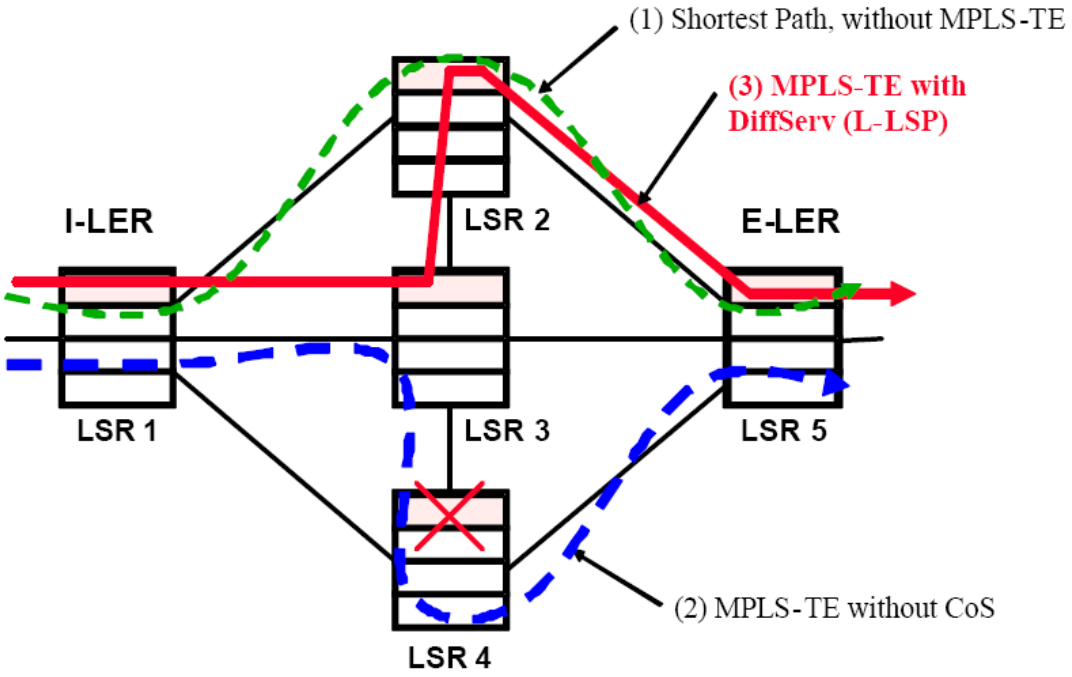

Figure 4.5 Packet flow in MPLS with DiffServ

Figure 4.5 illustrates an improvement on the architecture illustrated in Figure 5. Paths (1) and (2) of the previous figure are shown here in dashed lines for reference. In this architecture, MPLS support of DiffServ technology is deployed, and bandwidth reservations can be made with respect to specific priority queues. Let us assume that VoIP traffic uses queue-0, which is the top queue in every LSR. LSR-4 may have sufficient bandwidth across all of its queues, but it does not have enough bandwidth in queue-0, and therefore, path (2) will not provide QoS that is appropriate for the VoIP traffic. That is why we crossed the VoIP queue on LSR-4. But if an L-LSP is used with queue-0-specific bandwidth reservations, then traffic can be routed along path (3) via LSR-3 and LSR-2, and VoIP can be delivered with guaranteed QoS.

In summary, MPLS support of DiffServ satisfies both necessary conditions for QoS: guaranteed bandwidth and differentiated queue servicing treatment. MPLS satisfies the first condition, i.e., it forces applications flows into the paths with guaranteed bandwidth; and along these paths, DiffServ satisfies the second condition by providing

differentiated queue servicing. Note that MPLS support of DiffServ is still simpler and more scalable than IntServ with Standard RSVP. IntServ requires per-microflow signaling and per- microflow states in each router. In contrast, LSPs may themselves be aggregations of many microflows and thus require less signaling. Additionally, routers do not keep per- flow states. Instead, LSRs keep aggregated information on the bandwidth availability for all LSPs or for each priority queue.

The initial approaches to packet network QoS which primarily focused on throwing in bandwidth are now being replaced with sophisticated mechanisms that allow SPs to provision and operate their networks more precisely. This phenomenon is forced by two recent drivers: (1) reduction in the CAPEX for acquiring ever more bandwidth and (2) generation of additional revenues by providing value-added services with stricter SLAs. Capital Expenditures (CAPEX) are QoS driver which have been driven by traffic volumes, which have not necessarily correlated to service revenues, resulting in a difficult business model.

Advanced network services, such as VoIP, require hard QoS guarantees. While the IntServ architecture offered such guarantees, it was not scalable or practical to operate and manage. The DiffServ architecture has provided a scalable alternative but it had the drawback of providing no guarantees. Recent IETF work on combining the DiffServ and MPLS technologies in a packet network leads to enabling hard QoS assurances; and these guarantees come with better scalability and reduced complexity in comparison with IntServ. These improvements are a result of the stacking hierarchies and FEC aggregations characteristic of MPLS networks as well as the aggregated states maintained by the DiffServ-supporting nodes.

CHAPTER FİVE
MPLS VPN

5.1 VPN Requirements

Opaque transport of data between VPN sites, because the customer may be using non-IP protocols or locally administered IP addresses that are not unique across the SP network. Security of VPN data transport to avoid misdirection, modification, spoofing or snooping of the customer data. QoS guarantees to meet the business requirements of the customer in terms of bandwidth, availability and latency.

In addition, the management model for IP-based VPNs must be sufficiently flexible to allow either the customer or the SP to manage a VPN. In the case where an SP allows one or more customers to manage their own VPNs, the SP must ensure that the management tools provide security against the actions of one customer adversely affecting the level of service provided to other customers.

5.2 VPN Types

P. Brittain, Adrian Farrel,2004 define the VPN types as below.

5.2.1 Virtual Leased Lines (VLL)

VLL provide connection-oriented point-to-point links between customer sites. The customer perceives each VLL as a dedicated private (physical) link, although it is, in fact, provided by an IP tunnel across the backbone network The IP tunneling protocol used over a VLL must be capable of carrying any protocol that the customer uses between the sites connected by that VLL.

5.2.2 Virtual Private LAN Segments (VPLS)

VPLS provide an emulated LAN between the VPLS sites. As with VLLs, a VPLS VPN requires use of IP tunnels that are transparent to the protocols carried on the emulated LAN. The LAN may be emulated using a mesh of tunnels between the customer sites or by mapping each VPLS to a separate multicast IP address.

5.2.3 Virtual Private Routed Networks (VPRNs)

VPRNs emulate a dedicated IP-based routed network between the customer sites. Although a VPRN carries IP traffic, it must be treated as a separate routing domain from the underlying SP network, as the VPRN is likely to make use of non-unique customer-assigned IP addresses. Each customer network perceives itself as operating in isolation and disjoint from the Internet. It is, therefore, free to assign IP addresses in whatever manner it likes. These addresses must not be advertised outside the VPRN since they cannot be guaranteed to be unique more widely than the VPN itself.

5.2.4 Virtual Private Dial Networks (VPDNs)

VPDNs allow customers to outsource to the SP the provisioning and management of dial-in access to their networks. Instead of each customer setting up their own access servers and using PPP sessions between a central location and remote users, the SP provides a shared, or very many shared access servers. PPP sessions for each VPDN are tunneled from the SP access server to an access point into each customer's network, known as the access concentrator. The last of these VPN types is providing a specialized form of access to a customer network. The IETF has specified the Layer 2 Tunneling Protocol (L2TP), which is explicitly designed to provide the authentication and multiplexing capabilities required for extending PPP sessions from a customer's L2TP .

5.3 MPLS For VPNs

MPLS is rapidly emerging as a core technology for next-generation networks, in particular optical networks. It also provides a flexible and elegant VPN solution based on the use of LSP tunnels to encapsulate VPN data. VPNs give considerable added value to the customer over and above a basic best effort IP service, so this represents a major revenue-generating opportunity for SPs.

Different implementation models for MPLS-based VPNs imply different interactions between elements of a VPN solution.

5.3.1 LSP Tunnels

The basis of any MPLS solution for VPNs is the use of LSP tunnels for forwarding data between SP edge routers that border on a given VPN. By labeling the VPN data as it enters such a tunnel, the LSR neatly segregates the VPN flows from the rest of the data flowing in the SP backbone. This segregation is key to enabling MPLS to support the following characteristics of a VPN tunneling scheme, as identified in RFC 2764.

Multiple protocols on the VPN can be encapsulated by the tunnel ingress LSR since the data traversing an LSP tunnel is opaque to intermediate routers within the SP backbone.

Multiplexing of traffic for different VPNs onto shared backbone links can be achieved by using separate LSP tunnels (and hence separate labels) for each data source.

Authentication of the LSP tunnel endpoint is provided by the label distribution protocols. See the section *VPN Security* for more details.

QoS for the VPN data can be assured by reserving network resources for the LSP tunnels. MPLS supports both Intserv and Diffserv. The implications of using each of these reservation styles are examined in the next section. Protection switching and automatic re-routing of LSP tunnels ensure that failure of a link or router that affects a VPN can be corrected without management intervention. These protection mechanisms operate at several different levels, including refresh/keep-alive messages on a hop-by-hop basis within the label distribution protocols, re-routing of LSP tunnels, pre-provisioning of alternative routes, and wavelength failure detection and management for optical networks.

5.3.2 VPN Connectivity Using LSP Tunnels

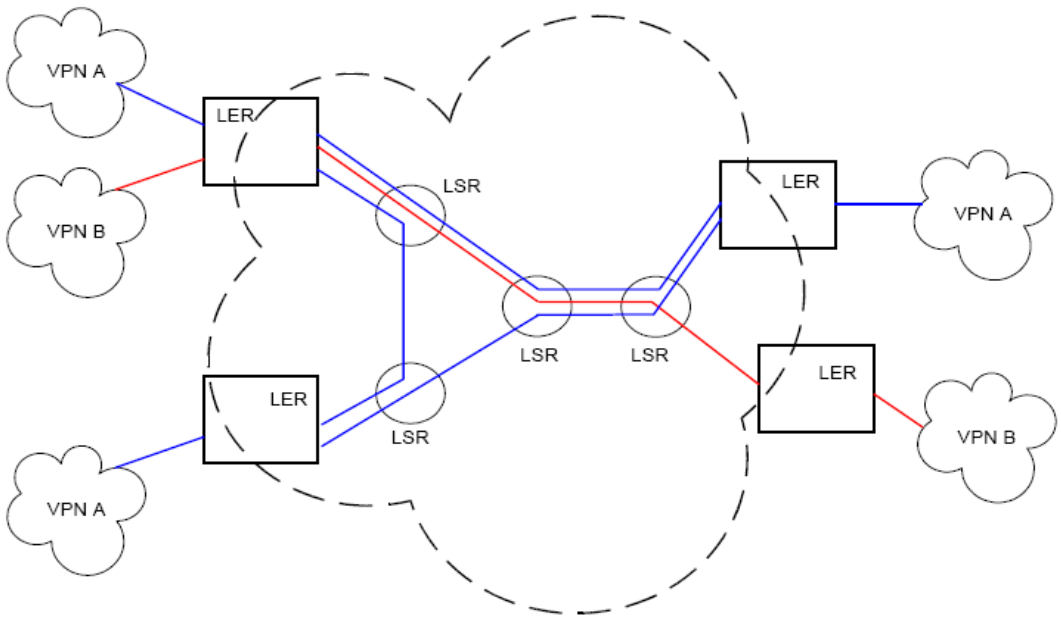

Figure 5.1 VPN Networks connected to the MPLS Network

Figure 5.1 shows simple interconnection between five VPN sites belonging to two different VPNs. A total of four LSPs are required in this topology, one to connect the two sites in VPN B, and three to connect the three sites in VPN A

CHAPTER SİX
DESIGN AND ANALYSIS OF AN MPLS NETWORK

6.1 A MPLS Backbone in Turkey

6.1.1 Network Scenario

In this chapter, a scenario of an MPLS network will be mentioned. Since economy of the East part of Turkey has been weak, the available infrastructure of the telecommunication is inadequate. There is a big industrialization project in the East and a great many of the firms are investigating in. A new service provider, let's name A Telekom (AT), considers the future needs and designs MPLS network in the East region connected to İstanbul.

6.1.2 Network Expectations

AT wants to offer L2 & L3 VPN services, broadband internet services, carrying the FR & ATM traffic, VOIP applications.

AT considers the quality and variety of its services and need to have a backbone which supports new age technologies.

AT decides to use MPLS technology which fills its all design need and expectations.

AT ensures that the layer 3 MPLS VPN design can deal with the current requirements as well as the predicted future service requirements.

AT improves the layer 3 MPLS VPN service with qos promises, supporting it to be marketed as the service of choice for the customers.

AT offers high-availability commitments to VPN users without additional capital expenses.

6.2 AT's Network Design Objectives

AT determines the cities included in industrialization project. Considering these throughputs, AT specifies the number and type of the devices (routers), the number and the capacity of the links in the network.

Figure 6.1 Turkey map

Figure 6.1 shows the cities in Turkey. There are two huge organized industrial regions in Diyarbakır and Erzurum. According to the survey of AT, the total traffic amount of these cities are expected over 8 Gbps. A great many of the traffic is internet traffic, remainig traffic is vpn traffic to İstanbul and abroad.

AT's network devices located in İstanbul, Erzurum and Diyarbakır must support MPLS technology. While choosing the brand of the routers, there are some factors to be considered, such as performance, cost, scalability and robustness. Performance is a very important factor in network design. The all routers and all of the links used inside

the network have to be capable of answering future needs. Factors which are considered measuring performance of the network are response time, traffic amount, usage rate and the protocols used in the network. Response time is considered as the service rate sensing the customers. Response time is related with the link failures, congestions, routing time of the routers, protocols used in the network. When the amount of traffic in links approaches full capacity, performance decreases. Providing the flexibility, a certain amount of the link capacity must be reserved. The protocols running in the network must be perceived correctly. The unnecessary routing information dispertion decreases the performance of the routers.

Scalability is the another factor in network design. A scalable network can be broaden with respect to future needs. Providing this situation requires a hierarchic design. Topology of the network must be scalable, must be in a hierarchic design.

Robustness can be described as the failures and problems occurred in the network do not influence services in the network. This is managed by providing backup links, equipments and cards.

The AT network is structered into three types of POPs (Points f Presence). Each type (t), is classified as either core router (t1 router), large (t2 router) and small (t3 router). The type of the POP depends on the density of the combined traffic throughput requirements.

T1 POPs are the high capacity core P routers of the backbone. AT decides to install the core routers in Erzurum and İstanbul and t2, t3 routers in İstanbul, Erzurum, Diyarbakır. The combined interconnection traffic of routers is carried by t1 routers.

AT also invests its transmission infrastructure, owns fiber and is running a long distance optical based on dense wavelength division multiplexing (DWDM) technology. This translates to availability of raw high-speed links (OC-48 (2.488 Gbps) and OC-192 (10 Gbps)) for provider router (P router) and PE router interconnection, at relatively low

cost and provisioning time. AT can activate additional capacity by enabling additional wavelengths (lambdas) in a relatively short time frame. AT takes advantage of this to enforce an overengineering policy for core router links.

The high-speed core links are provided to routers as native lambdas straight from the DWDM equipment without any intermediate SONET add/drop multiplexer (ADM). SONET framing is in use between the routers and the DWDM equipment. These links do not benefit from any protection at the optical level. Some links interconnecting P routers and PE routers are provided through a SONET infrastructure overlaid over the optical infrastructure. The SONET links are protected by means of SONET protection provided by bidirectional line switch rings (BLSRs) with four fibers, also called BLSR/4.

Intra-POP connectivity is achieved via packet over SONET (PoS) or switched gigabit ethernet (ge). Because of the relatively low cost of switched gigabit ethernet technology and the negligible cost of fibers within a premises, AT also maintains an overengineered intra-POP capacity.

The AT backbone POP topology, interconnected through OC-12 (622 Mbps), OC-48 (2.4 Gbps), OC-192 and ge links and every link in the network has a backup link.

PE routers providing Internet and Layer 3 MPLS VPN services from major locations are also deployed, as well as some additional P routers acting as an aggregation layer inside the POP for these PE routers. Aggregation P routers reduce the number of IGP adjacencies that have to be maintained by the backbone P routers to two, because each core P router has to peer with only two aggregation P routers (in addition to the other core P routers in the backbone) instead of with all the PE routers in the POP (whose number can be fairly high, and growing, in a Level 1 POP).

Since the expected traffic amount of t1 routers between Erzurum and İstanbul is min 8 Gbps, the t1 routers in same city are connected to each other via 10 ge links and t1

routers between İstanbul and Erzurum are connected each other via OC-192 links. T2 routers are composed of P routers that connected to the t1 routers via 10ge links and other routers via OC-12, OC-48 links. T3 routers connected to the t2 routers via OC-12 or OC-48 links. Diyarbakır traffic is combined in t2 routers and carried over t1 routers in Erzurum. Table 6.1 summarizes the various types of links used in the AT network, along with their main characteristics and localization.

Table 6.1 Link Types and Characteristics in the AT Backbone

Link Type	**Speed**	**Protection**	**Localization**
OC-192 DWDM	10 Gbps	None	t1 POP-t1 POP
OC-48 DWDM	2.5 Gbps	None	t1 POP-t2 POP t2 POP-t2 POP
OC-48 SONET	2.5 Gbps	SONET protection	t1 POP-t2 POP t2 POP-t3 POP
OC-12 SONET	622 Mbps	SONET protection	t2 POP-t3 POP
Gigabit Ethernet	10 Gbps	None	Intra-t2 POP

6.3 Analysis of Link Failures

The use of SONET protection covers only the case of a link failure within the SONET network but not an IP router interface failure (sometimes considered a link failure) or a router failure. On the other hand, AT considers router interface failures and router failures rare enough that they are acceptable and do not the use of additional recovery mechanisms such as Automatic Protection Switching (APS).

The DWDM equipment lets the company provide 1+1 optical protection. Such a protection scheme relies on specialized optical equipment performing traffic bridging along the primary and secondary light paths, each of which follows diverse paths. Upon a link failure, such as a fiber cut or optical equipment failure, the receiving side quickly detects the failure and switches the traffic received from the primary light path to the secondary. This type of mechanism, usually qualified as "single-ended," is undoubtedly efficient because it does not require any extra signaling mechanisms or coordination between the sender and receiver (just the receiving side performs the switching function). Hence, the rerouting time is very fast (a few milliseconds). Moreover, a strictly equivalent quality of service (QoS) is guaranteed upon a network element failure because the secondary path is identical to the primary path (although it might be longer to be diverse from the primary path). On the other hand, this requires dedicating half of the fiber capacity for backup recovery. Furthermore, such a protection scheme implies that additional optical equipment needs to be purchased.

Hence, AT decided to use all the network bandwidth to route the primary traffic and rely on some upper-layer protection mechanisms to offer equivalent rerouting time at significantly lower costs. All the light paths provided to the IP/MPLS layer for inter-Level 1 links and Level 1-to-Level 2 links therefore are unprotected. This is perfectly in line with the previously described core network overengineering strategy adopted by AT.

Although DWDM offers the ability to provide high bandwidth in a very cost-effective fashion, it has a downside. Multiple links share some common resources and equipment whose failure may impact several links. This is called Shared Risk Link Group (SRLG), and the production design should take it into account.

During the past several years, AT has gathered various network failure statistics. These statistics have been used to assess AT's design requirements for its backbone network.

6.4 Internal and External IP Routing and Label Switching

AT runs OSPF as its interior gateway routing protocol. Because of the complexity of the network, there is some hierarchy including OSPF regions in OSPF topology. By convention, area 0 represents the core or "backbone" region of an OSPF-enabled network. The other OSPF area numbers may be designated to serve other regions of an enterprise (large, business) network, however every additional OSPF area must have a direct connection to the backbone OSPF area. The backbone area has the identifier 0.0.0.0. Backbone area is configured including link interfaces. The OSPF metric values of the network must be decided during the design of the network according to the link ranges between routers. In AT network, there are also other areas, NSSA or STUB regions, such as ADSL network devices (SSGs) of the same SP. NSSA or STUB OSPF areas prevents the circulating of the routing information including small regions.

AT runs BGP to provide connectivity between different AS's. BGP builds up internal or external neighborhood via the AS of the neighbor router. The IBGP is used inside an autonomous system. IBGP is used inside the confines of its own AS, can not be used in conjunction with a different AS. EBGP works just the opposite of IBGP. It transports information to other BGP enabled systems. However, EBGP is generally not used within the same AS. In rare cases, EBGP can be used in place of interior protocols (IGRP, RIP, etc.) through the specification of static routes. EBGP runs as its exterior gateway routing protocol. There are two EBGP routers in the network which have neigborhoods with the abroad AS's. IBGP usage in AS is not preferred, but if the some other AS's have to transit their traffic from the AS, IBGP must run in the network. If not, all EBGP routes must be injected to the route tables of the internal gateway routing protocols's. This causes a serious decrease in the routers' performances in AS.

Label distribution protocol (LDP) is used within the mpls backbone to enable label switching from one edge of the AT network to the other. LDP distrubutes labels to the destination addresses in accordance with the link information learning via OSPF. Layer

3 VPN traffic and layer 2 VPN traffic is label switched. Internet traffic coming from static routes and SSG (Service Selection Gateway) routers is forwarded by normal IP forwarding procedures. Internet traffic coming from BGP routes can be forwarded by mpls procedures.

AT's network is addressed from the 18 subnet block. This block includes all PE, P routers and other equipments in AT network. As a network design decision, there are different subnet ranges for MPLS router loopback interfaces, link network interfaces, route reflector network interfaces, customer service interfaces. AT also use the private address block for its internal infrastructure. The use of private addresses provides some protection from the Internet because it is not a routable address space. So, the internal AT network is hidden from the outside. However, the customers who have static routes can send traffic to AT through default route.

6.5 IP MPLS Bacbone of AT

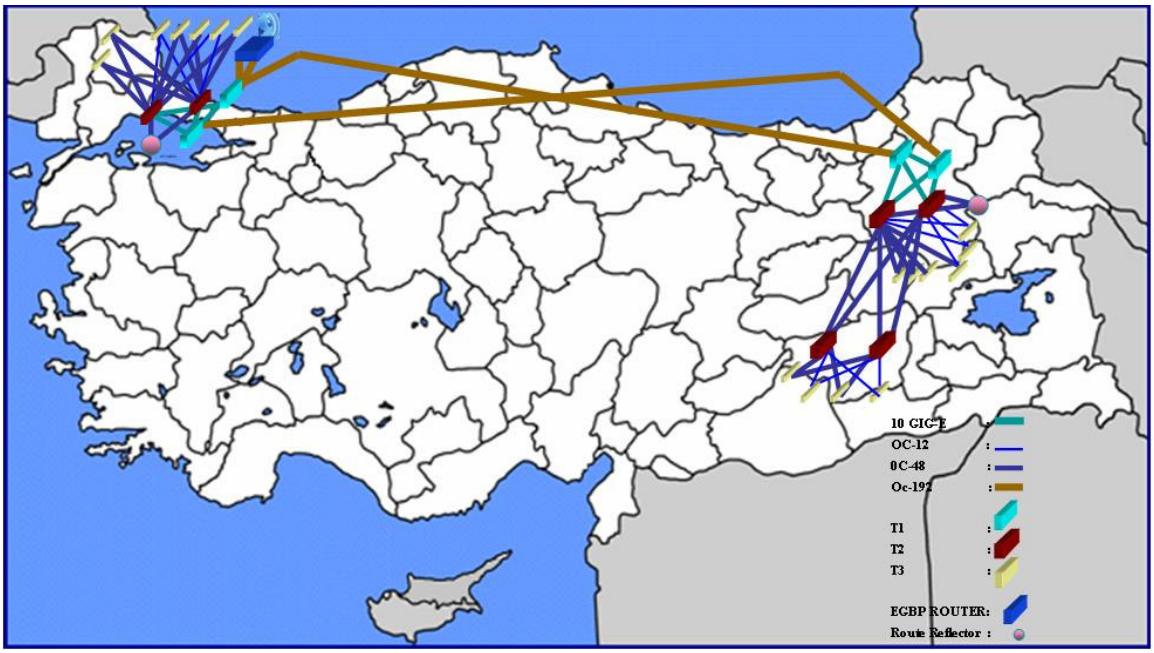

Figure 6.2 General view of AT Network

A general view of the AT backbone is shown in the Figure 6.2. Therefore, Turkey is separated into three main regigions. In these regions, main routers are connected to each other via 10 ge links in LAN. Four routers are the core routers which İstanbul and Erzurum have two of them. OC-192 links connects the core routers each other. The traffic of the regions flows through these OC-192 links. There is a backup link of every link in the network.

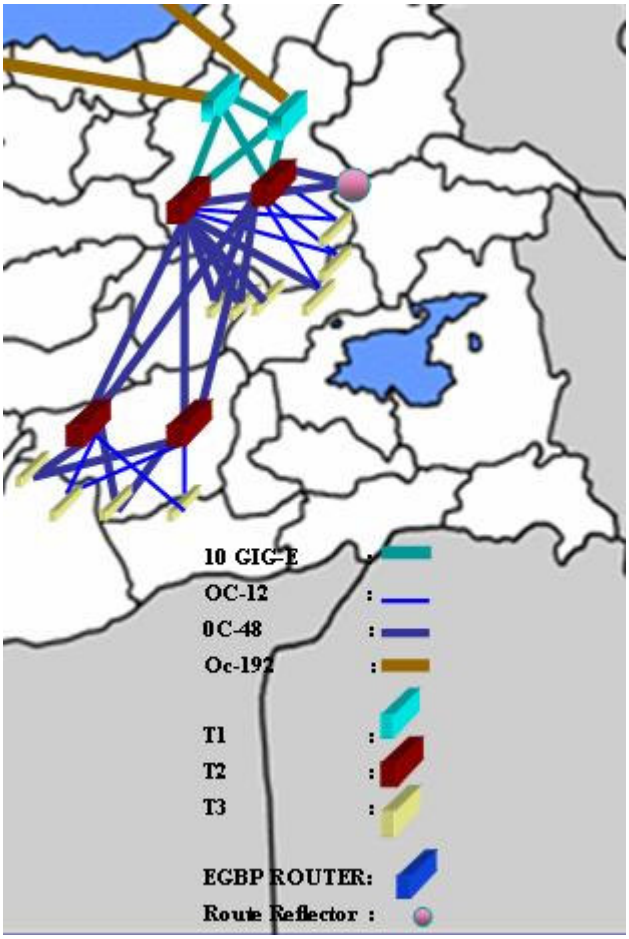

Figure 6.3 A close view of east site of AT Network.

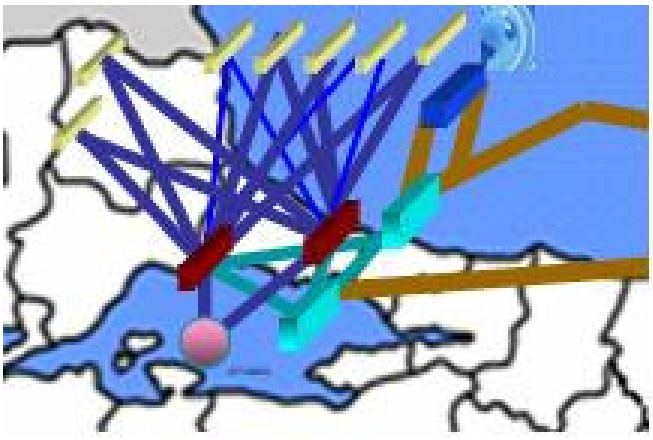

Figure 6.4 A close view of west site of AT Network.

The Figure 6.3 and 6.4 shows a close view of AT Network.

One router is used as EBGP router in the network. This EBGP router is connected to the core routers via OC-192 links. The customers are not connected to EBGP router. The EBGP router announces the default link announce. Therefore, the traffic of the addresses which is absent in BGP or OSPF routing table, is sent to the EBGP routers.

In the network, OSPF area 0.0.0.0 is used including all the routers in the network. The routers which have the services .e.g. ADSL, GSHDSL, DIAL-UP is belong to both 0.0.0.0 area and other area incluing BRASs.

9875 is used as the AS number of the AT. EBGP routers are connected to the different AS's.

Two route reflectors located in Istanbul and Erzurum are used in the backbone. These two routers communicate each other via IBGP. BGP regions including all other routers are composed and these regions operate as the server of RRs.

LDP runs as the label distribution protocol.

AT is planning to run TE protocols as the need of new age technologies increase.

CHAPTER 7
CONLUSION

In order to deliver the variety of services demanded and to ensure that these are delivered fast, safe and secure, the new network has been developed and designed with MPLS technology. MPLS Technology was developed to help service providers leverage the best aspects of IP technology and combine it with the best features of ATM and Frame Relay Circuit Technology. By using VPN in addition to MPLS we can offer a wide selection of nationwide services across a secure and single infrastructure.

MPLS increases the performance of the large networks such as AT. Main working principle of MPLS is forwarding at edge and switching in the core. If the number of the routers in a network is small, most of the routers will be edge router and the traffic will be send at layer 3 level. On the other hand, in large networks, label switching can be done efficiently in the core. If the number of routers increases in a network, MPLS performance increases.

MPLS is also suitable for large networks because of the diminishing the routing information in routers since transit routers are no longer need to handle complete routing tables.

Since the LDP and RSVP-TE are still open to be developed, running these protocols may cause some problems. Comparing with the advantages and benefits of this technology, these problems may be unimportant for service provides.

MPLS is a standards-based technology that can improve network performance and QoS for selected traffic. Service providers enhance the variety of the services, the class of the services and customer portfolio through MPLS. Service providers can market various services such as metro ethernet, IP/TV, layer 3 and layer 2 VPNs, VOIP. MPLS offers multiple classes of service, each associated with different types of traffic. For instance, an enterprise's mission-critical applications (such as VOIP applications) might be in a gold class of service, less-important applications might be in a silver service, recreational applications (such as games, instant messaging, and P2P) might be in a best effort service.

The service providers existing long years may have FR and/or ATM backbones. Service providers are increasingly looking to MPLS to provide the basis of their next-generation core networks since Frame Relay and ATM services continue to generate significant and growing revenues. These facts demonstrate the importance of providing continued support for the customers of Frame Relay and ATM services as migrating to the core networks to MPLS. The provision of this support reinforces the need for Frame Relay and ATM access to MPLS core networks. MPLS enables the integration the FR and ATM backbone.

REFERENCES

Andersson L. (2001), *LDP Specification.*

Bernet, Y. (2001) *Networking Quality of Service and Windows Operating Systems*. New Riders.

Blake S. (1998) An Architecture for Differentiated Services, RFC2475 .

Braden R.(1994), *Integrated Services in the Internet Architecture: an Overview*, RFC1633.

Brittain P., Adrian Farrel. (2004). *MPLS Vitual Private Networks.*

Faucheur F. (2002*) MPLS Support of Differentiated Services.*

Faucheur F.(2003), *Requirements for Support of Diff-Serv-aware MPLS Traffic Engineering.*

Fineberg V.(2002). A Practical Architecture for Implementing End-to-End QoS in an IP Network, IEEE Communications Magazine.

Grossman D.(2002), *New Terminology and Clarifications for DiffServ*, RFC3260.

Jolly V. & Latifi S.(2005). An *Overview of MPLS and Constraint Based Routing*, IEEE.

Martin W. Murhammer & Lee K. K. & Motallebi P. & Borghi P., (1999) IP *Network Design Guide ,* IBM.

Nichols K (1998) Definition *of the Differentiated Services Field (DS field) in the IPv4 and IPv6 headers*, RFC2474.

Payer U.(2005), DiffServ, IntServ.

Rosen E.(2001), A. Viswanathan, R. Callon, *Multiprotocol Label Switching Architecture.*

Smit H.(2002), T. Li, *IS-IS Extensions for Traffic Engineering.*