DOKUZ EYLÜL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

MULTI-PROTOCOL LABEL SWITCHING AND MPLS VPN SOLUTIONS

by
Mümin GÜNGÖR

July, 2006
İZMİR

MULTI-PROTOCOL LABEL SWITCHING
AND
MPLS VPN SOLUTIONS

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

Mümin GÜNGÖR

July, 2006
İZMİR

M.Sc THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **"MULTI-PROTOCOL LABEL SWITCHING AND MPLS VPN SOLUTIONS"** completed by **Mümin Güngör** under supervision of **Asst. Prof. Dr. Zafer Dicle** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

.....

Supervisor

.....

(Jury Member)

.....

(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.

Mümin Güngör

MULTI-PROTOCOL LABEL SWITCHING AND MPLS VPN SOLUTIONS

ABSTRACT

MPLS is an improved method for forwarding packets through a network using information contained in labels attached to IP packets. The labels are inserted between the Layer 3 header and the Layer 2 header in the case of frame-based Layer 2 technologies, and they are contained in the virtual path identifier (VPI) and virtual channel identifier (VCI) fields in the case of cell-based technologies such as ATM.

MPLS combines Layer 2 switching technologies with Layer 3 routing technologies. The primary objective of MPLS is to create a flexible networking fabric that provides increased performance and stability. This includes traffic engineering and VPN capabilities, which offer quality of service (QoS) with multiple classes of service (CoS).

MPLS 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.

Keywords: MPLS, label, VPI, VCI, traffic engineering, quality of service, class of service, virtual private network, label switched path.

ÇOK PROTOKOLLÜ ETİKET ANAHTARLAMA VE MPLS SANAL ÖZEL NETWORK ÇÖZÜMLERİ

ÖZ

MPLS, IP paketlerine bazı bilgiler içeren etiketler eklenerek paketlerin networkde gönderilmesini daha efektif yapmak için geliştirilmiştir. Bu etiketler 3. katman ve 2. katman başlıkları arasına yerleştirilirler, frame temelli 2. katman teknolojilerinde sanal yol tanımlayıcısı (VPI), cell temelli teknolojilerde de sanal kanal tanımlayıcısında bulunurlar.

MPLS 2. katman anahtarlama teknolojisi ile 3. katman yönlendirme teknolojisinin birleşimidir. MPLS'in birinci amacı esnek bir network oluşturarak performansı ve kararlılığı arttırmaktır. Trafik mühendisliği ve sanal özel networkler bu amacın içindedirler ve servise kalitesi ve çoklu servis sınıfları bu sayede gerçekleşir.

Mpls ayrıca etiket anahtarlamalı yolların (LSP) tünellerini VPN datayı enkapsüle etmek için kullandığından esnek ve zarif bir VPN çözümü sunar. VPNler müşterilerine basit best effort IP servisi üzerinden ek özellikler verir. Bu özellikler sayesinde de internet servis sağlayıcılarına daha iyi hizmet sunma imkanı ve daha fazla kazanç sağlamaktadır.

Anahtar Sözcükler : MPLS, etiket, VPI, VCI, trafik mühendisliği, servis kalitesi, servis sınıfları, sanal özel network, etiket anahtarlamalı yol.

CONTENTS

CHAPTER ONE
INTRODUCTION

1.1 Introduction

Over the last few years, the Internet has evolved into a ubiquitous network and inspired the development of a variety of new applications in business and consumer markets. These new applications have driven the demand for increased and guaranteed bandwidth requirements in the backbone of the network. In addition to the traditional data services currently provided over the Internet, new voice and multimedia services are being developed and deployed. The Internet has emerged as the network of choice for providing these converged services. However, the demands placed on the network by these new applications and services, in terms of speed and bandwidth, have strained the resources of the existing Internet infrastructure. This transformation of the network toward a packet- and cell-based infrastructure has introduced uncertainty into what has traditionally been a fairly deterministic network.

In addition to the issue of resource constraints, another challenge relates to the transport of bits and bytes over the backbone to provide differentiated classes of service to users. The exponential growth in the number of users and the volume of traffic adds another dimension to this problem. Class of service (CoS) and QoS issues must be addressed to in order to support the diverse requirements of the wide range of network users.

With over 250 million new users projected in the next decade and with the implementation of Internet protocol version 6 (IPv6), carriers and service providers struggle to scale their current infrastructures for the inevitable demand on their networks.

In order to meet the growing demand for bandwidth, Internet service providers (ISPs) need higher performance switching and routing products. Although most carrier and service provider core networks run on impressive asynchronous transfer mode

(ATM) backbones, most connections to these providers continue to be slow frame relay and point-to-point connections, introducing latency and sometimes bottlenecks at the edge access points. Core network routers also contribute to latencies, as each must make its own individual decision on the best way to forward each incoming packet. Traditionally, IP has been routed over ATM using IP over ATM via virtual circuits (VCs) or multiprotocol over ATM (MPOA). These forwarding methods proved to be cumbersome and complicated. The need for a simpler forwarding method —one with the traffic management features and performance of traditional switches combined with the forwarding intelligence of a router— is definitely felt.

All of these needs can be met with multiprotocol label switching (MPLS), because it integrates the key features of both Layer 2 and Layer 3. Most importantly, it is not limited to any Layer 2 or Layer 3 protocol. In particular, MPLS has several applications and can be extended across multiple product segments (such as an MPLS router, an IP services switch/router, a multiservice switch, an Optical Ethernet switch, as well as optical switches).

In sum, despite some initial challenges, MPLS will play an important role in the routing, switching, and forwarding of packets through the next-generation network in order to meet the service demands of the network users.

1.2 Aim of Thesis

MPLS is an improved method for forwarding packets through a network using information contained in labels attached to IP packets. The labels are inserted between the Layer 3 header and the Layer 2 header in the case of frame-based Layer 2 technologies, and they are contained in the virtual path identifier (VPI) and virtual channel identifier (VCI) fields in the case of cell-based technologies such as ATM.

MPLS combines Layer 2 switching technologies with Layer 3 routing technologies. The primary objective of MPLS is to create a flexible networking fabric that provides increased performance and stability. This includes traffic

engineering and VPN capabilities, which offer quality of service (QoS) with multiple classes of service (CoS).

The best way to describe the function of MPLS is to draw an analogy to a large national firm with campuses located throughout the United States. Each campus has a central mail-processing point through which mail is sent, both around world and to other campuses. From the start, the mailroom has been under orders to send all intercampus correspondence via standard first-class mail. The cost of this postage is calculated into the company's operational budget.

However, some departments have been complaining for several months that they require overnight delivery and package-tracking services. As a manager, you establish a system to send three levels of mail between campuses: first-class (normal) mail, priority (important) mail, and express mail (urgent). In order to offset the increased expense of the new services, you bill the departments that use these premium services at the regular rate of postage, plus 10 percent.

In this analogy, units of priority mail and express mail are processed by way of placement into specific envelopes with distinctive labels. These special labels and packets assure both prioritized handling and tracking capability within the postal network. In order to avoid slowdowns and bottlenecks, the postal facilities in the network create a system that uses sorting tables or sorting databases to identify and expedite these packets.

In an IP network, you can think of routers as post offices or postal sorting stations. Without a means to mark, classify, and monitor mail, there would be no way to process different classes of mail. In order to designate different classes of service or service priorities, traffic must be marked with special labels as it enters the network. MPLS and MPLS network components accomplish this mission.

This thesis is study of various implementation approaches of Multiprotocol Label Switching (MPLS) with existing technologies. In the first five chapters of this thesis,

theoretical aspects of MPLS are explained. These chapters are mainly concerned with the MPLS standard, its origin, overview of its working and various services it can provide. Chapter 3 explains how MPLS works and its standarts and principles. In chapter 4, working of MPLS with the existing protocols is explained. ATM , Frame Relay , and Ethernet and PPP are covered in these chapters. In chapter 5, MPLS services like Virtual Private Networks (VPN), Quality of Services (QoS), Traffic Engineering (TE) are touched on. Chapters 6,7, cover VPNs history,characters and properties. In chapter 6, why we need VPNs, why they born are explained and consist of VPN's kind and properties. MPLS VPNs are focused in chapter 7 and their advantage and compare of other VPNs are explained in this chapter. Last part is conclusion.

Contribution of this thesis is divided into two parts. First part is study of various implementation approaches of MPLS with existing protocols. First part is covered in chapters 2,3,4,5. Second part is VPNs and their characters and properties. It is covered chapters 6,7. Last part is conclusion.

CHAPTER TW0
MPLS HISTORY and BACKGROUND

2.1 Origin of MPLS

This chapter covers the reasons behind the origin of MPLS and limitations of the technologies, which ate supposed to be replaced by MPLS.

During the early days of the Internet IP was prevalent protocol for the connectionless flow of packets. On the other hand, Time Division Multiplexing (TDM) and Frequency Division Multiplexing (FDM) were used for the connection-oriented transfer of data in telephone networks. The network was divided into two parts; best effort connectionless service offered by IP and guaranteed bandwidth provided by TDM based Synchronous Transfer Mode.

Since IP is based on statistical multiplexing, it makes better use of available bandwidth. In order to make use of this feature in all parts of the network and unite the flow of data and voice traffic, ATM was proposed. ATM makes use of the good features of both the worlds. It is based on statistical multiplexing and has a wide range of control and signaling protocols. Main purpose of these protocols is to provide different kinds of services such as Variable Bit Rate, Constant Bit Rate etc.

These protocols make use of different concepts like Call Admission Control, Bandwidth reservation etc. to achieve the desired features.

Although ATM was perfect in theory but there were some problems in real world implementation of ft. IP was prevalent in data communication networks and it was hard to replace it with an entirely new protocol like ATM. Also the cost of ATM equipments was too high to put it into access networks and user premises. Therefore ATM was deployed as link layer technology in the IP backbones, m this case a number of routers were connected to each other through an ATM network to form a mesh. This technique of using ATM as layer 2 switching technology for IP packets is called Overlay model. This is because here IP packets are overlaid on the top of an ATM network. There were several problems with the overlay model:

Scalability - In order to create a fully meshed network, each router has to be joined to every other router via an ATM virtual circuit. This creates the need for N(N-l)/2 virtual circuits. This kind of network topology is not scalable and leads to explosive growth in the number of virtual circuits.

Conversion from IP packets to ATM cells - Each IP packet should be broken down into ATM cells before being transferred through the network. This leads to additional overhead of segmentation and reassembly. This problem is also called as "cell tax".

Overhead of two different protocols — Since ATM is designed from scratch as a replacement to IP, it does not have any thing in common with IP. Also ATM provides wide varieties of Quality of Service and Class of Service, so it is quite complex protocol. In order to deploy IP over ATM, network administrators should have knowledge of both of these protocols.

High-speed routers - With the rapid increase in forwarding speed of routers, an ATM switch can be bottleneck in the network. Because of the bandwidth limitation in ATM Segmentation and Reassembly interfaces, the switching speed of an ATM switch cannot be increased to indefinitely.

All these problems with overlay model have lead the researchers to find an alternative. The main source of these problems is incompatibility of IP and ATM. So the solution was to invent a technology, which can provide the features of ATM without compromising the existing IP based protocols.

2.2 Companies Solutions

Various companies came with their proprietary solution for these problems. Some of the examples are Cell Switching Router from Toshiba, IP Switching from Ipsilon, Tag switching from Cisco and Aggregate Route bases switching from IBM.

2.2.1 The Cell Switching Router (CSR)

The Cell Switching Router (CSR) approach was developed by Toshiba and presented to the IETF in 1994. It was one of the earliest public proposals for using IP protocols to control an ATM switching fabric. CSR is designed to function as a router for connecting logical IP subnets in a classical 'IP over ATM' environment. Label switching devices communicate over standard ATM virtual circuits. CSR labeling is data-driven (i.e., labels are assigned on the basis of flows that are locally identified). The Flow Attribute Notification Protocol (FANP) is used to identify the dedicated VCs between CSR's and to establish the association between individual flows and individual dedicated VCs. The objective of the CSR is to allow 'cut through' forwarding of flows, i.e., to switch the ATM cell flow that constitutes the packet rather than reassembling it and making an IP level forwarding decision on it. CSRs have been deployed in commercial and academic networks in Japan.

2.2.2 IP Switching

IP Switching, developed by Ipsilon (who are now part of Nokia), was announced in early 1996 and has been delivered in commercial products. IP Switching enables a device with the performance of an ATM switch to act as a router, thereby overcoming the limited packet throughput of traditional routers. The basic goal of IP

Switching is to integrate ATM switches and IP routing in a simple and efficient way (by eliminating the ATM control plane). IP Switching uses the presence of data traffic to drive the establishment of a label. A label binding protocol (called the Ipsilon Flow Management Protocol or IFMP) and a switch management protocol (called General Switch Management Protocol or GSMP) are defined. GSMP is used solely to control an ATM switch and the virtual circuits made across it.

2.2.3 Tag Switching

Tag Switching is the label switching approach developed by Cisco Systems. In contrast to CSR and IP Switching, Tag Switching is a controldriven technique that does not depend on the flow of data to stimulate setting up of label forwarding tables in the router. A Tag Switching network consists of Tag Edge Routers and Tag Switching Routers, with packet tagging being the responsibility of the edge router. Standard IP routing protocols are used to determine the next hop for traffic. Tags are 'bound' to routes in a routing table and distributed to peers via a Tag Distribution Protocol. Tag switching is available on a number of products from Cisco.

2.2.4 Aggregate Route-based IP Switching (ARIS)

Aggregate Route-based IP Switching (ARIS),IBM's label switching approach, is similar architecturally to Tag Switching. ARIS binds labels to aggregate routes (groups of address prefixes) rather than to flows (unlike CSR or IP Switching). Label bindings and label switched paths are set up in response to control traffic (such as routing updates) rather than data flows, with the egress router generally the initiator. Routers that are ARIScapable are called Integrated Switch Routers. ARIS was designed with a focus on ATM as the Data Link Layer of choice (it provides loop prevention mechanisms that are not available in ATM). The ARIS Protocol is a peer-to-peer protocol that runs between ISRs directly over IP and provides a means to establish neighbors and to exchange label bindings. A key concept in ARIS is the "egress identifier". Label distribution begins at the egress router and propagates in an orderly fashion towards the ingress router.

2.3 MPLS Working Group

All these techniques had one concept in common. That is, to make enhancements to the existing TCP/IP protocol suite to make it connection-oriented so that real time traffic can be supported and quality of service can be improved. But the problem was that although the concept was same, implementation was not. Each approach was trying to push its own implementation. In order to solve the problems of interoperability, IETF started one working group in 1997 called MPLS working group. Goal of this working group was to develop a vendor independent version of layer 3 switching technique. This group went though different existing solutions and finalized the MPLS standard in 1999. Although MPLS is vendor independent, it is quite similar to tag switching by Cisco. MPLS works at layer 2.5 i.e. between IP and any link layer. It can support any network layer protocol as well as any link layer technique including ATM, Frame Relay, PPP and Ethernet.

Next chapter gives an overview of working of MPLS as described by the IETF MPLS working group. Goal of the chapter is to explain basic working of MPLS and how it can benefit the existing network.

CHAPTER THREE
WORKING OF MPLS

3.1 MPLS ELEMENTS

Multiprotocol Label Switching (MPLS) is a layer 3 switching technique. The basic idea in MPLS is to forward the packets based on a short, fixed length identifier termed as label. The domain in which MPLS is effective is called MPLS domain. There are three kinds of routers in an MPLS domain namely ingress routers, Label Switching Routers (LSR) and egress routers. As the names imply, an ingress router is the first router encountered by any packet when it enters the MPLS domain and egress router is situated at the exit of this domain. All other routers are called LSRs. Ingress routers and egress routers are commonly referred to as Label Edge Routers (LERs). The path taken by a packet inside an MPLS domain is known as Label Switched Path (LSP). Next subsection explains the label switching procedure specified by MPLS.

3.1.1 Forwarding Equivalance Class

Forwarding Equivalence Class (FEC) determines the level of granularity in a given network. When establishing connection, some criteria should be used to associate the flow of packets with the connection. In the simplest case this criteria may be source and destination IP addresses. In this case any packet for a given combination of source and destination IP addresses will be treated in the same way by the network. A network with finer granularity can take port addresses into account also.

In other words, a forwarding equivalence class is a subset or collection of packets such that the network treats all the packets in this subset identically; the entire network is a collection of such disjoint subsets. The reason a router forwards all packets within a given FEC the same way is that the mapping between the information carried in the network layer header of the packets and entries in the forwarding table is many to one. That is, packets with different content of their network layer headers could be mapped into the same entry in the forwarding table.

Forwarding Equivalence Class is used to control the size of the forwarding table as well as to decide the QoS provided by the network.

Examples of forwarding equivalence class :

- A set of unicast packets whose Layer 3 destination addresses match a certain address prefix
- A set of unicast packets whose destination addresses match a particular IP address prefix with similar type of service (ToS) bits
- A set of unicast packets whose destination addresses match a particular IP address prefix and have the same destination TCP port number
- A set of multicast packets with the same source and destination Layer 3 addresses
- A set of multicast packets with similar source and destination Layer 3 addresses and the same incoming interface

3.1.2 Label Switching

MPLS is based on the concept of label switching, i.e. every node in the MPLS domain forwards by means a label lookup. Whenever a packet enters an MPLS domain, it first encounters an ingress router. The ingress router checks if there is already a connection established for the packet. If it is then the packet is forwarded along the appropriate path, otherwise a connection is first established and the packet is temporarily buffered.

When an LSR receives a packet, it performs forwarding as opposed to routing. Routing is usually done by IP based router. The difference is that forwarding is the process of swapping an incoming label with a new label depending on the entry in the forwarding table, while routing requires a search through the routing table to find the optimal path to the destination. In other words, in case of forwarding, search for the optimal path is done only for the first packet of the flow and all other packets are just forwarded along the same path. This concept makes MPLS based networks to be connection-oriented.

An LSR has two planes: the data plane and the control plane. The data plane consists of cross connect table or Next Hop Label Forwarding Entry (NHLFE), consisting of entries for label swapping. This table provides the information about incoming label and corresponding outgoing label. The control plane consists of FEC (Forwarding Equivalence Class) data and FEC to NHLFE cross merge database. FEC contains the details about the packets on a particular flow like source and destination IP addresses. It can also contain any Quality of Serive (QoS) and Class of Service (CoS) requirements imposed by the flow, the way packet should be processed, outgoing queue to be used etc. FEC to NHLFE database maps each FEC to a set of NHLFEs. The basic idea is that more than one flow might need identical treatment by the LSR, so there is only one entry for all those flows in FEC but each flow has separate entry in NHLFE. LSR also contain a table with a list of free labels.

When a packet enters an LSR, it first goes to the data plane through the appropriate port mapping. After that, the LSR performs label swapping by placing the outgoing label in place of the incoming label. In the next step, appropriate processing is done and packet is queued to the next hop. This procedure is explained below in detail with example.

Figure 3.1 explains the various planes present in an LSR. In our example, a packet comes in the data plane of the LSR with incoming label value of 1450. This label value is searched throughout the NHLFE using indexing in the hardware; indexing is done in order to improve the performance of the router. Indexing in hardware is usually implemented using Translation Lookaside Buffers (TLBs). This technique has the advantage of searching all the entries in the table in parallel. Once an entry is found with the incoming label value of 1450, the outgoing label value is read from that entry. After that the incoming label value in the MPLS header of the packet is replaced by the outgoing value (which is 1006 in this example), m the next step, mapping is peformed from NHLFE to FEC data using FEC-NHLFE table as explained below.

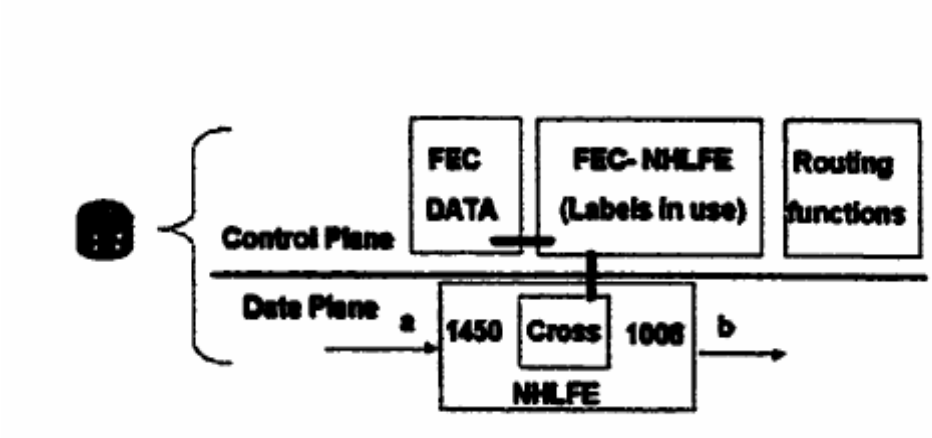

Figure 3.1 Various planes and associated tables in an LSR

The three tables outline the working of various tables in LSR. Table 3.1 displays a possible FEC database. In this example, destination IP address and port number are used as the criteria for the formation of an FEC. Therefore, all packets destined to the same host and using same port number will receive identical treatment throughout the network. The table also contains the description of the processing to be done with the packets belonging to an FEC.

Table 3.1 A Sample FEC Database

FEC	PORT	Processing requirements
129.107.22.1	80	Controlled Load
129.107.23.1	69	Best Effort
129.107.24.1	230	Guaranteed Bandwidth

Table 3.2 shows various entries of an NHLFE database. Each entry in this table has two parts incoming label and outgoing label. Incoming label is taken from the MPLS header of any packet entering the LSR and is used for searching the appropriate entry in the table. For example, if a packet with incoming label of 2200 comes in an LSR with the following NHFLF table, first entry would match for that packet. So LSR will put a label value of 4400 before sending the packet to next hop. This process is called label swapping or label switching and hence the name Multiprotocol Label Switching. Once label

switching is done, LSR searches for the appropriate FEC entry in the FEC database. This is done with the help of FEC to NHLFE table, which is shown in table 3.3, Continuing with out example, a packet with an incoming label value of 2200 should have a destination IP address of 129.107.23.1 as shown in the first entry of FEC to NHLFE table. This is because only packets with this destination address are mapped to this entry at the time of label allocation and binding.

Table 3.2. A Sample NHFFE Database

Incoming label	Outgoing label
2200	4400
2300	4500
2400	4600

After an entry is found in FEC to NHLFE database using the incoming and outgoing label values from NHLFE table, appropriate entry in FEC database is searched. This is performed by using FEC value from the entry in FEC to NHLFE database. FEC database is searched for the respective FEC vales and once the entry is found, appropriate processing of the packet is done. In our example, second entry of FEC table is the one for the current packet, the packet will be given best effort treatment while forwarding.

Table 3.3. A Sample FEC to NHLFE Database

FEC	Incoming label	Outgoing label
129.107.23.1	2200	4400
129.107.22.1	2300	4500
129.107.24.1	2400	4600

3.1.2 Label Distrubution

Before explaining the process of label distribution, let us introduce the methodology: downstream and upstream router. Figure 3.2 shows a sample network with five routers numbered 1 through 5. The concept of upstream and downstream router is relative: when a packet flows from router 1 to router 4, then router 1 is called upstream router with respect to router 4 and router 4 is called downstream router with respect to router 1. Similarly, when packets are going from router 3 to router 1, then router 2 is immediate

downstream router with respect to router 3 and router 3 is immediate upstream router with respect to router 2. In short, a router can be either downstream or upstream depending on the direction of flow as well as the reference router.

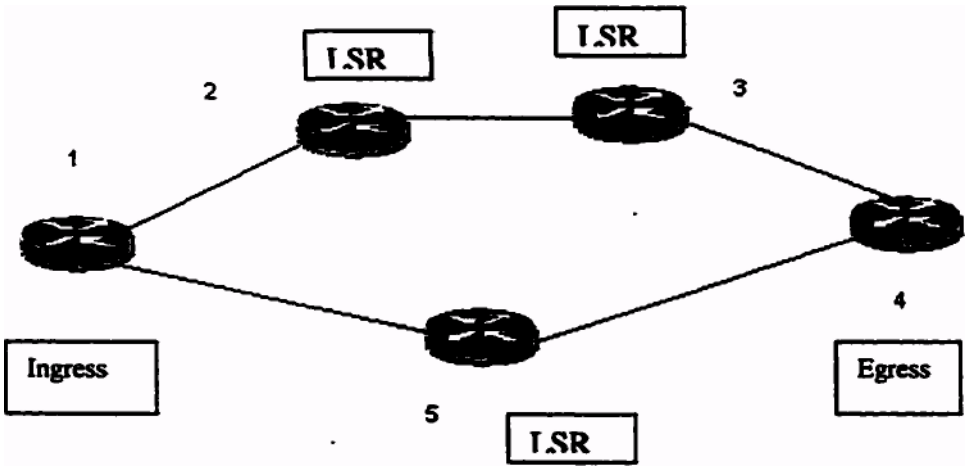

Figure 3.2 A Simple Network

Therefore, in general, a router is called upstream router if a packet comes to it before reaching the reference router. Similarly, a router is called downstream router if it gets the packets after referenced router gets the same packet.

Initial setup for the formation of an LSP can occur in one of the two modes: independent control mode and ordered control mode. In case of independent control mode a router performs label binding and sends this information to other routers in the network. Routes also listen to information from the other routers. In case of ordered control, an LSR may transmit the information about label binding to the next upstream router only when either it has the label binding information from the next downstream router or it is working as egress router.

An LSR can distribute label binding information in two ways. When the LSR sends the binding information in response to an explicit request from another LSR, it is called downstream-on demand label distribution. If LSR distributes label bindings to other LSRs that have not explicitly requested them then it is called downstream-unsolicited label distribution.

Here is the explanation of the four combinations of label distributions. As shown in Figure 3.3, router A sends a request to router B for binding a label to FEC F. Router B is working in independent control mode, so it replies immediately without waiting for reply from router C. Reply of router B to router A is independent downstream on demand because a request was sent by downstream router for the binding of the label. Similarly, router B sends a message to router C informing that it will use label M for FEC F.

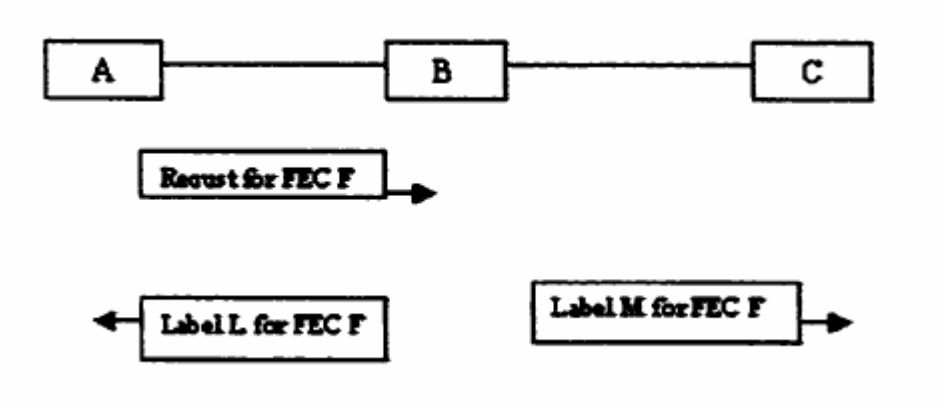

Figure 3.3 Independent downstream-on demand and independent downstream unsolicited label distribution

The explanation given above was an example of independent downstream-unsolicited binding. The main advantage of independent control is that binding time is less and label assignment occurs just after the advertising of the addresses. The problem with this approach is that the assignment might not be consistent.

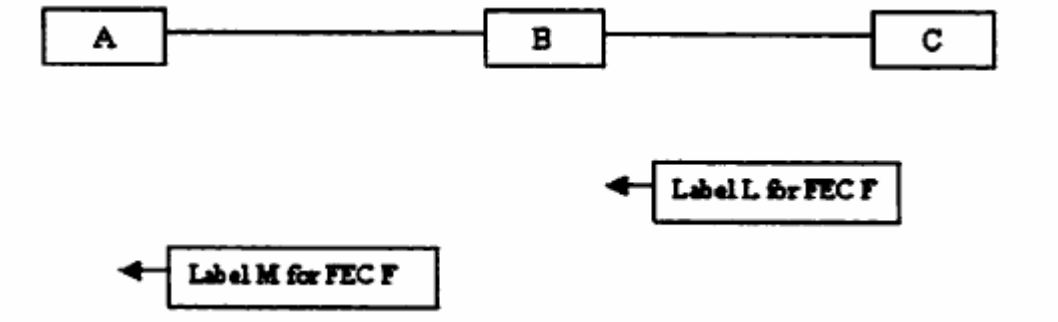

Figure 3.4 Ordered control downstream on-demand label distribution

Figure 3.4 gives an overview of ordered control downstream on-demand label distribution mode. First router A sends a request for label binding to router B. Since the routers are working in ordered control mode, router B can not send label binding information to router A unless it receives a response form route C. When router C receives a label binding request from router B, it sends a reply to router B. Here router C is working as egress router therefore it can send reply immediately. Once router B receives a reply from C, it chooses a label from its label pool, binds that label with the FEC F and sends a message to router A. The advantage of using ordered control is that all the routers along the path always use the same FEC as the initial advertiser, guaranteeing consistency. The drawback is that establishment of an LSP takes much more time that that in independent control.

After getting the information about the label distribution, an LSR generates cross-connect tables and starts forwarding the packets.

3.1 Connection Establishment

In order to establish a connection or setup an LSP, the ingress router can decide to use one of the various combinations available for the label binding and distribution. Here is the explanation of using ordered downstream on-demand binding, which is the most common one.

First of all the ingress router generates a request packet and sends it to the next hop towards the destination router. MPLS uses two methods for route selection: hop- by-hop routing and explicit routing. In case of hop-by-hop routing, OSPF is generally used at each router for deciding the next hop to the destination router. While in case of explicit routing, an explicit route to the destination is decided by a designated router, usually the ingress router. Constrained Shortest Path First (CSPF) can be used for the selection of explicit route. The path selection process and other relevant details are explained later.

The request packet contains the details of the new connection to be established. It can also contain any QoS requirements or constraints imposed by the end hosts. This

packet flows through the network, signaling all the router in the path about the new flow until it reaches an egress router.

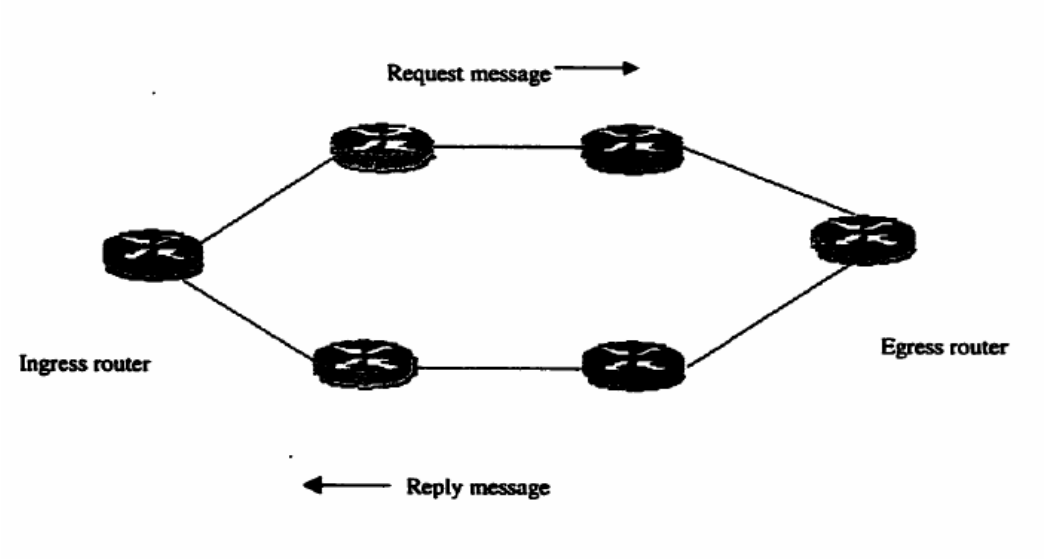

Figure 3.5 Connection establishment process through MPLS network

When an egress router receives the request packet, a new packet is generated. The purpose of this packet is to do label binding. Egress router chooses a label and puts this label in the newly generated packet. Now the packet flows in the upstream direction towards the ingress router. When a router receives this packet, it updates its forwarding table by using the information contained in the packet. After that it chooses one label from its local database and updates the label Meld of the packet. In the next step, this router sends the updated packet to the next upstream router. Once this packet is received by ingress router, it updates its forwarding table and forwards the buffered packet. During the flow of the packet through the network, every router uses its forwarding table to find out the label to be placed and the next hop for the packet. In this way, a connection is established from the ingress router to the egress router. The exact details of the name and type of the two packets are dependent on the distribution protocol being used. Two distribution protocols namely LDP and RSVP are explained later.

3.5 MPLS Header Format

There are four fields in the MPLS header; label, Exp, S and TTL. Label is used as identifier in an LSR to find out the next hop and other details about the forwarding. Exp field is short form for experimental bits and can used for providing class of service to differentiate different classes of service. When used as differentiated service code points (DSCP) it provides 8 classes of service. S is used as a stacking bit to indicate if this is the last label of the stack. TTL field is of 8 bits and is used to avoid formation of loops. These bits are copied from IP header by the Ingress router and copied back by the egress router.

There are three places where an MPLS label can be placed in the IP packet When using either Ethernet or PPP as link layer technology, MPLS label should be placed between Ethernet (or PPP) header and IP header.

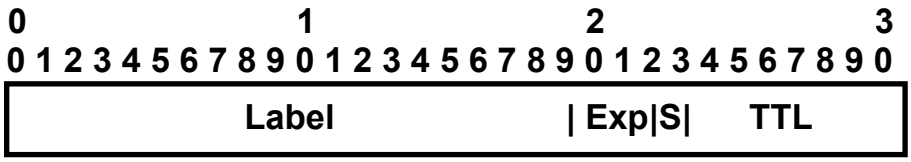

Figure 3.6. MPLS header and size of each field in bits

In case of Frame Relay, DLCI field of the header can be used to place the MPLS label. Similarly, VPI/VCI fields of ATM header can be used for MPLS label when ATM is used as data link layer technology. It should be noted that in case of Frame Relay and ATM, when the corresponding header field is replaced by MPLS label, the switch becomes a router in the sense that the routing and signaling protocols used by the switch become IP/MPLS based. So this type of network just makes use of Frame Relay or ATM hardware and IP/MPLS based software replaces the original software. This approach leads to avoidance of N squared mesh problem (Number of ATM Permanent Virtual Circuits required for a mesh network of surrounding routers increases with a square of the number of routers).

3.6 RSVP

In order to perform LSP setup and label distribution, there should be some kind of label distribution protocol. The purpose of this protocol is to signal the network about the new LSP to be established as well as to do the label binding along the selected path.

For the label allocation and binding, MPLS has two options namely RSVP and LDP. RSVP stands for Resource Reservation Protocol and is a part of TCP/IP protocol suite. In order to work with MPLS, some modifications to this protocol are required. This is because RSVP was developed for IP and does not have provision for carrying label information.

For the distribution and binding of labels using RSVP, two message types are used viz. PATH message and RESV message. The ingress router starting the connection establishment process uses PATH message. The PATH message starts the connection establishment process and is sent to potential participants of a session. The RESV message is sent in response to the PATH message to confirm the formation of a connection.

An ingress router, after determining the QoS requirement of the flow, generates a PATH message and places sufficient information in it. After this, message is sent to next hop along a particular path and all the routers in that path check to see if they have enough resources to fulfill the requirements. As explained earlier the selection of path can be done in one of the two ways: hop-by-hop routing and explicit routing. A combination of these two can also be used. After an egress router receives a PATH packet, it generates an RESV packet The RESV packet has all the information contained in the PATH packet together with the label binding information. This packet travels upstream towards the ingress router and gets updated at each intermediate router while simultaneously updating the forwarding tables of those routers. Here are the components that a PATH message can have:

- LABEL_REQUEST object
- EXPUCT_ROUTE object

- RECORD_ROUTE object
- SESSION_ATTRIBUT object
- CoS FLOWSPEC object

The presence of LABEL_REQUEST object is an indication that this message is a request for label binding. The LABEL_REQEST object also contains a field for Layer 3 Protocol ID (L3ID) that identifies the layer 3 protocol being used. This is because MPLS can work with any network layer protocol. Also it is not possible to find out the layer 3 protocol from the data link layer header because that header contains MPLS as the next higher layer protocol.

When the ingress router uses explicit routing, an EXPLCIT_ROUTE object should be present in the PATH message. This The ERO (Explicit Route Object) consists of an ordered sequence of "hops" where the sequence specifies an explicit route. Technically this ERO is a sequence of <type,Iength,value> triples, where each triple depicts a particular abstract node. This abstract node can be IPv4 address prefix, Ipv6 address prefix or Autonomous System number. By using full IP addresses an explicit route can be specified as a sequence of routes. When this PATH message travels from node to node, each node removes the triple corresponding to it and forwards the packet according to the next triple value.

Purpose of RECORD.ROUTE object is to find out the route taken by the PATH message. This object contains a series of subobjects, which contain information about the intermediate routers. There are three advantages of getting the information about the route traversed by PATH message. First of all, this message helps in detection of loops in the explicit route. Second, it provides a means of collecting the detailed path information hop-by-hop about the LSP setup session. And the last use is to generate an EXPLICIT ROUTE object for LSP setup in the next PATH message. Remaining two packet types are used for specifying the other attributes of the flow such as Class of Service.

RS VP does not have routing capability and therefore it makes use of routing operations provided the network layer protocol (IPv4 or IPv6) to determine the best path to the destination router. Also RSVP supports only downstream-on-demand label distribution method.

3.7 Label Distribution Protocol

LDP, which stands for Label Distribution Protocol is a new protocol, designed by IETF for the distribution and binding of labels in an MPLS network. LDP makes use of UDP and TCP for the exchange of information with other routers.

LSRs that make use of LDP for the distribution of label and FEC mapping information are called LDP peers [33] and for exchanging this information they form an LDP session. There are four types of LDP messages:

- Discovery message
- Session message
- Advertisement message
- Notification message

The purpose of Discovery message is to announce the presence of an LSR. Each LSR in the network sends a Discovery message periodically to all the routers in the network. Session messages are used to establish, maintain and delete sessions between LDP peers. After two LSRs become LDP peers they can exchange information about label binding. Similarly Advertisement messages are used to create, change or delete label mappings for FECc. Notification messages are used for providing status, diagnostic and error information. Usage of these message types is explained in more detail below.

The first phase in the operation of LDP is meeting with the neighbors. For this each router sends a discovery message to all the routers in the network. This message is sent as a multicast message over UDP to all the routers in the network (port number 646).

Once the neighbor discovery step is over, the LSP with the numerically largest IP address initiates a TCP connection and other routers listen. Session message is used for this purpose. This message proposes several parameters for the session, including distribution method, LDP method and other parameters required for the label distribution. Negotiation for the above parameters is possible during this phase.

After the establishment of session, label binding and mapping can take place any time between any LSP peers, by using Advertisement messages. As explained before, the establishment of LSP can be either in independent mode or ordered mode. Similarly it can be either downstream unsolicited or downstream on demand.

Label Switched Routers can choose one of the two label retention policies: conservative label retention and Uberal label retention. In case of conservative label retention, an LSR can retail a label mapping only if it corresponds to the next hop in the IP forwarding path. In this case if the regular forwarding path fails because of the failure of one or more routers then only the LSR can ask for an alternate path. The information that an LSR has is the bare minimum required for forwarding the packets along the selected path. Liberal retention mode gives freedom to retain some of the label mapping information even if they are not required. In this case a router retains all the information it gets from the adjacent routers and can use it for the formation of an alternate path if the primary fails, thus no processing is required in case of failure.

For choosing label values, LDP follows the MPLS standard. There are two types of label spaces namely per interface and per platform, m case of a per interface label space, labels are associated with an interface. Therefore different interfaces can have same label values. Per platform label space means that each LSR has only one label space that is shared among all of its interfaces. This approach requires each LSR to maintain only one label pool.

3.6 Constraint-based Routing

Goal of constraint-based routing is to compute a path from one given node to another, such that the path doesn't violate the constraints and is optimal with respect to some scalar metric. Once the path is computed, constraint-based routing is responsible for establishing and maintaining forwarding state along such a path.

Constraint-based routing includes constraints, which may be either performance constraints or administrative constraints.

3.8.1 Components of Constraint-based Routing

1. There should be the ability to compute a path at the source such that this path follows a set of constraints imposed as well as is optimal for some scalar metric like hop count or delay.

2. There should a mechanism to distribute the information about network topology and attributes associated with links throughout the network. This information should be available to every node in the network because potentially any node in the network may originate traffic that has to be routed via constraint-based routing.

3. Once we have computed the path with CSPF (Constrained Shortest Path First), the next thing we need to do is to establish the forwarding state along the path, as well as reserving resources along the path. So we need explicit routing capability.

4. The last mechanism required is updating of available resources as well as link attributes after the path has been established.

Path computation at the source can be performed using CSPF. CSPF is similar to OSPF except that while adding a node to the list, link corresponding to that node is examined to see if that link satisfies the imposed constraint. This list is the list of nodes, which fall in the shortest path as selected by the shortest path first algorithm.

The third requirement can be achieved either by RSVP-TE or CRLDP. These two are described below.

3.8.2 RSVP-TE and CR-LDP

RSVP-TE is an extension to RSVP to enable explicit routing. Plain RSVP can establish LSP only along the path computed by plain IP routing. This is because with plain RSVP the path taken by RSVP message is controlled by the destination-based forwarding paradigm, and path taken by this message determines LSP.

To accomplish explicit routing for RSVP messages, an object called Explicit Route Object (ERO) is used. This object is carried in the path message and contains the explicit route that message has to take. The ERO consists of an ordered sequence of "hops" where the sequence specifies an explicit route. Technically this ERO is a sequence of <typelength,value> triples, where tach triple depicts a particular abstract node. This abstract node can be IPv4 address prefix, Ipv6 address prefix or Autonomous System number. By using full IP addresses an explicit route can be specified as a sequence of routes.

When this PATH message travels from node to node, each node removes the triple corresponding to it and forwards the packet according the next triple value.

CR-LDP contains a set of extensions to LDP that provides ability to forward along a specific path. To establish label-forwarding state along an explicit route, CR-LDP introduces a new object, called Explicit Route (ER). The structure of this object, as well as its handling by LSRs, is almost identical to the ERO used in RSVP-TE. This ER object is carried as a < type, length, value> triple in the LDP LABEL REQUEST message.

CHAPTER FOUR
WORKING OF MPLS WITH EXISTING PROTOCOL

4.1 WORKING OF MPLS WITH ATM

4.1.1 Conventional IP over ATM

In this model, a group of routers are connected with each other via an ATM network. DP based network of routers and ATM based switches are not aware of each other's presence. To the routers it seems they were connected to other routers using some layer 2 technology. Similarly ATM network does not have any understanding of IP based protocols like OSPF, RSVP etc.

As explained in the Introduction part, this model suffers from some of the major drawbacks and these drawbacks were the motivating factors for the invention of MPLS.

There are three ways of using MPLS with ATM: MPLS over ATM (Tunneling through ATM), MPLS interworking with ATM, and MPLS over ATM hardware (Label-Controlled ATM). These three approaches are explained in next few sections.

4.1.2 MPLS Over ATM

MPLS over ATM is similar to conventional IP over ATM. A group of IP/MPLS LSRs is connected to each other through an ATM network, rn this case the underlying ATM network is completely transparent to IP/MPLS based LSRs. Working of ATM is completely transparent to MPLS and vice versa. As shown in the diagram below, an ATM network is surrounded by a number of LSRs. These LSRs communicate with each other without bothering about the ATM network and are peers of each other.

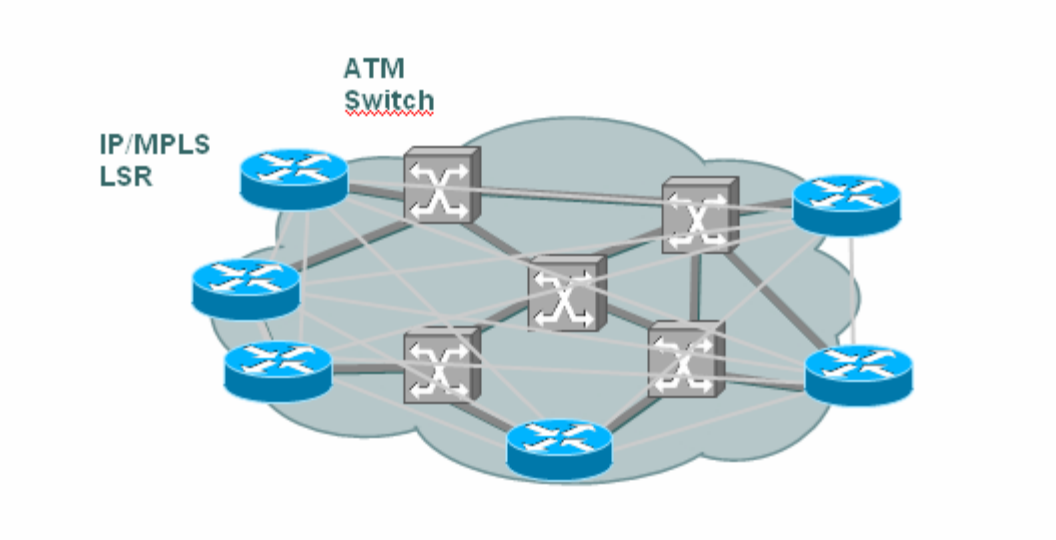

Figure 4.1 Tunneling of MPLS using ATM

This model suffers with the ail the disadvantages, which IP over ATM has, together with the added complexity of MPLS specific protocols. The ATM network works like a tunnel to MPLS based packets. This is also called tunneling model or overlay model. This solution does not require any change to existing ATM network. Only IP based routers are upgraded to work as IP/MPLS LSRs.

4.1.3 MPLS Interworking with ATM

In case of MPLS interworking with ATM, MPLS and ATM networks work as peers as opposed to overlay model. The two networks transfer data to each other with appropriate conversion of routing and signaling protocols. This model requires the use of IWF (interworking function) to perform necessary conversions from one protocol to other.

In this kind of implementation, packets from one type (ATM or MPLS) are converted to other type (MPLS or ATM). The functionality required to perform this conversion is implemented in INE. This conversion process is defined as ATM-MPLS-ATM encapsulation mode.

1. Single Cell Mode: in this mode, each ATM cell is converted to a MPLS frame with the information of ATM cell stored within the MPLS frame.

2. Concatenated Cell Mode: In this case, multiple ATM cells are encapsulated within a single MPLS frame. This technique is much more efficient than the first one.

3. Frame mode: bi this case, AAL-5 PDU fragment (a multiple of 48 bytes) is encapsulated within an MPLS frame. Although this method is most efficient of the three, it suffers from the loss of cell header transparency. Also no support is provided for AAL types 1,2,3 and 4.

Since the implementation of INE is fairly complex and impractical, this approach is rarely used.

4.1.4 MPLS over ATM Hardware

The last approach is to use integrated model. In this model existing ATM network is upgraded to IP/MPLS based network. Upgrade of only some part of software is required while the switch hardware remains intact.

As shown in the figure below, an ATM switch now behaves like an MPLS based LSR. Although it still forwards 53-byte cells, the control and signaling protocol used by this switch are that of MPLS. In this case IP/MPLS LSR and ATM switch work as peers. Definitions:

- ATM-LSR — Label Switch Router consisting of an ATM switch and IP/MPLS based software for label distribution and forwarding. VCI or VC3/VPI fields are used for putting the label. ATM specific routing or addressing is not required in this kind of switch.

- LC-ATM interface - Label Switching Controlled ATM (LC-ATM) interface is an interface of an ATM switch working as ATM-LSR. This means that the interface is capable of sending and receiving 53 byte cells but the switch supports IP/MPLS based control software.

- Frame-based LSR - It is also called Packet-based LSR. It is a Label Switch Router, capable of forwarding complete frames through one or more of its interfaces. A Frame-based LSR can also have LC-ATM interface(s). This wfll be the case when a Frame-based LSR is connected to one or more ATM-LSR. In any case, a Frame-based LSR should always have at lease one frame based or packet based interface.

When an ATM based network is upgraded to work like IP/MPLS based network, all the core routers start functioning as ATM-LSR with one or more LC-ATM interface(s). Edge routers of this network work as Frame-based LSRs with at least one LC-ATM interface for communicating with ATM switches. The edge routers of this network perform dual functionality. They receive frames or IP/MPLS packet from the adjacent LSR and they receive cells from adjacent ATM-LSR. So these LSRs should have capability of converting packets to cells and cells to packets. The diagram below conveys the same idea in pictorial way. m this diagram , packet based LSRs are connected to ATM network through LC-ATM interfaces. They are also connected to customer sites using some kind of layer 2 technique (Ethernet or PPP).

In order for MPLS to work properly in an ATM based network, some changes are required. First of all, the switches should support IP/MPLS based protocols like OSPF, LDP, ICMP, RSVP etc. This can be done by upgrading the existing software to support these protocols. Besides that an LC-ATM interface should support at least two kinds of communications: label-controlled communication using VCI or VPWCI fields of a cell, and unlabeled IP packet based communication for carrying control messages. First type of communication is the most common one and is used for forwarding packets on a particular flow. This is used only after the connection is established and makes use of either VCI or VPI/VCI fields of a cell for carrying the MPLS label information.

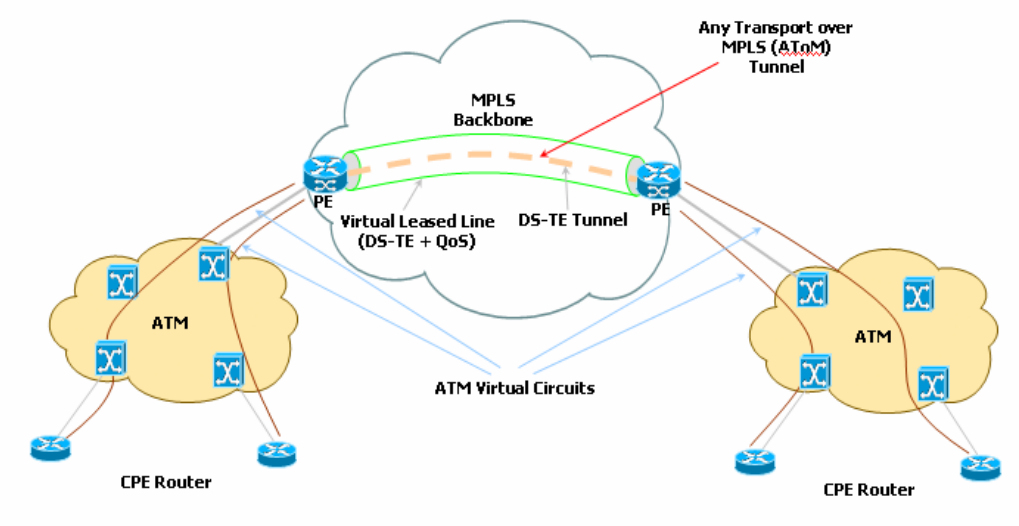

Figure 4.2 Use of MPLS over ATM Hardware

Second type of communication is required for transferring control and signaling information. When a connection request is made for a particular flow, some kind of label distribution and binding protocol is required. LDP is usually used in ATM based networks. LDP requires support of UDP and TCP packet types. In case of a simple IP based MPLS network, conventional connectionless IP packets are used for transferring these kinds of messages. But in case of an ATM network, everything is connection-oriented. Therefore some VPI/VCI values should already be configured for these kinds of messages, so that it will be possible to distinguish control messages from regular messages. Specifies that VCI values of 0-32 should be used for these messages.

4.2 MPLS OVER FRAME RELAY

This chapter covers working of MPLS in Frame Relay network and explains the procedure for deployment of such a network.

Implementation of MPLS over Frame Relay is similar to its implementation over ATM. Software on existing Frame Relay switches is upgrades to support IP/MPLS based forwarding, while the hardware components remain the same. Here is the summary of relevant terms:

- LSR: An LSR stands of Label Switching Router and it can be any device, which is capable of MPLS based forwarding and label switching,
- LC-FR: It is a Frame Relay based interface in which DLCI field of the header contains MPLS label.
- FR-LSR: It is a Frame Relay switch, which is capable of MPLS based forwarding and label switching. Each such switch has one or more LC-FR interfaces.
- FR-LSR domain: It is a set of FR-LSR routers, connected through one or more LC-FR interfaces.

When the packet flows through a Frame Relay network, MPLS label is put in the DLCI field of the of the Frame Relay data link layer. This label is used throughout the Frame Relay network for forwarding decisions. If the packet contains other labels, they are put in a separate MPLS shim header and are not used in this part of the network.

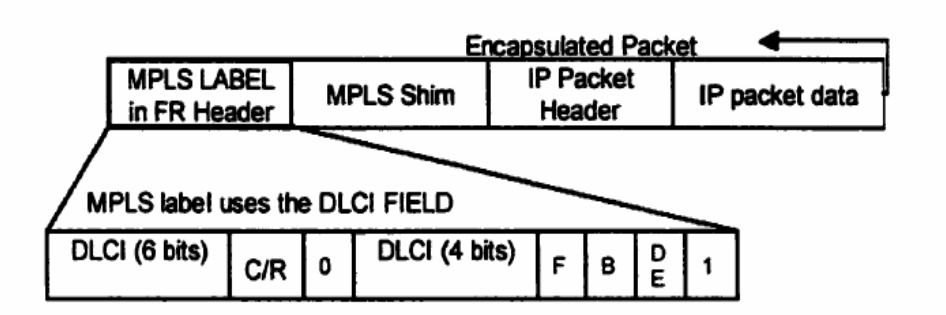

Figure 4.3 Placement of MPLS label in Frame Relay Header

While traversing the Frame Relay network, the packets are forwarded depending on the label value in the DLCI field. Since the IP header of the packets is not accessed by the switches, there should be some mechanism to ensure that TTL field is updated properly so that loop can be prevented.

For updating the TTL value of a packet, the ingress router uses a hop count value [7]. Hop count value is the number of hops before the packet reaches the egress router of that segment of the network. The hop count value is calculated at the time connection is established. This is done by using a hop count object [7] in LDP messages. When the LDP message flows upstream, every LSR in the path increments the hop count

object value by 1. If at any point, the hop count value exceeds the maximum count, the packet is dropped. When the ingress LSR receives the LDP object, it updates the TTL field of each packet before forwarding it.

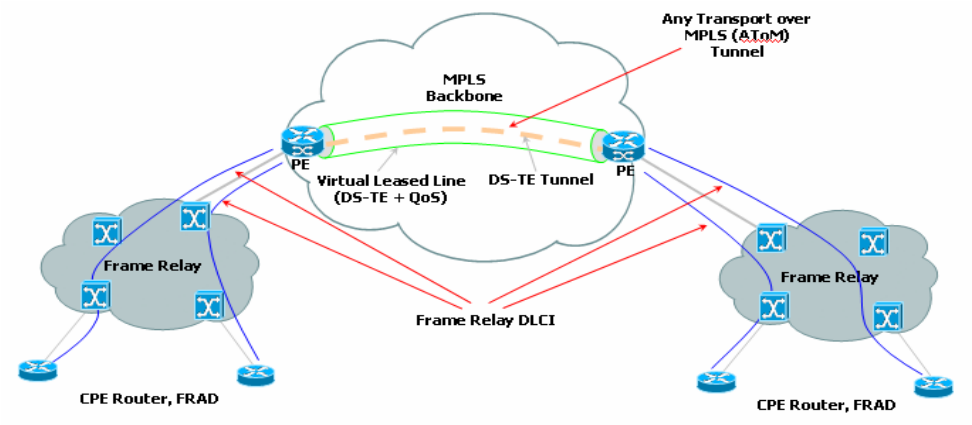

Figure 4.4 Frame Relay over MPLS

When ingress LSR receives a packet for which there is no flow established, it starts the connection establishment process by using either RSVP or LDP. A request is sent to the appropriate path, selected either by OSPF or through explicit routing. This request message flows along the path and is forwarded by the core LSRs of the network. When this request is received by an edge LSR, a new entry is created in Label Information Base (LIB). After this, a label is chosen from the pool of unallocated labels and mapping message is sent to the next upstream router. Hop count object value of this message is initialized to 1.

In order to do MPLS based forwarding of packets, all the Frame Relay switches should be upgraded to support layer 3 protocols such OSPF, RSVP, BGP besides MPLS. However, it is possible to have Frame Relay switches, which support control component of both DP/MPLS as well as control components defined by ITU and Frame Relay forum. This technique is particularly useful in cases where the switch should support both Frame Relay based forwarding and MPLS forwarding.

The method of label distribution can be either ordered control or independent control. Also the mode of label retention is left up to the specific implementation.

4.3 MPLS OVER ETHERNET AND PPP

This chapter gives overview of implementation of MPLS when link layer protocol is either Ethernet or Point-to-Point Protocol (PPP).

When MPLS is used with Ethernet, it becomes a 2.5 layer protocol. Edge router of this kind of network is responsible for connection establishment. All the routers inside the network just forward the packet depending on the incoming label value. Therefore only edge routers look at the IP header for establishing the connection and updating the value of TTL.

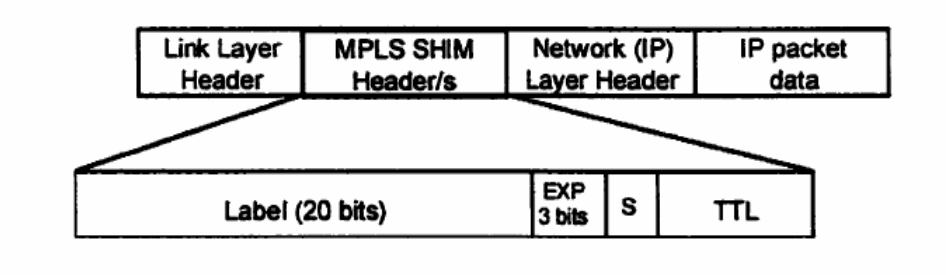

Figure 4.5 Placement of MPLS Shim Header in a TCP/IP Packet over Ethernet

MPLS over PPP can be used in similar way. In each of these cases, MPLS does not depend on the link layer being used. At the ingress of the network, edge router puts a shim header between IP header and Ethernet or PPP header. This header contains various fields required for forwarding in the core of the network. MPLS header is explained in more detail in previous part of this document.

CHAPTER FIVE
MPLS SERVICES

5.1 TRAFFIC ENGINEERING

Traffic engineering is the process of managing the flow of traffic through the network such that optimal use of network resources is made while supporting the network's customers and their QoS needs. Traffic Engineering in MPLS focuses on two aspects: traffic oriented objectives and resource-oriented objectives.

Traffic oriented objectives deal with minimizing traffic loss, minimizing delay and jitter, maximizing throughput and attainment of Service Level Agreements (SLA). Resource oriented objectives deal with the network resources such as link capacity, routers, available bandwidth etc.

As explained in the previous section. Constraint-based routing takes care of both of these objectives by choosing a path that supports the required Service Level Agreements (hence meeting traffic oriented objectives) while still being optimal (hence fulfilling resource oriented objectives).

5.2 QUALITY OF SERVICE AND CLASS OF SERVICE

Quality of Service (QoS) is provided by means of bandwidth reservation, admission control and traffic engineering. By using Constraint-based routing it is possible to reserve the bandwidth for a particular flow. Similarly by using traffic engineering, load can be distributed uniformly throughout the network. This helps in avoiding congestion in some part of the network.

Class of Service (CoS) is a technique for providing different treatment to different traffic types. The most common technique of differentiating traffic is Differentiated Services, which is explained in the next section. Giving different treatment includes using different queues for different traffic types, giving priority to

time critical traffic and dropping some particular type of traffic in case of congestion. For example, if there is congestion at a particular router, then the buffer starts overflowing and some of the packets need to be dropped. If using differentiated services, then the traffic with the least priority can be dropped first.

5.3 MPLS VPN

The overlay VPN model, most commonly used in a service provider network, dictates that the design and provisioning of virtual circuits across the backbone must be complete prior to any traffic flow. In the case of an IP network, this means that even though the underlying technology is connectionless, it requires a connection-oriented approach to provision the service.

From a service provider's point of view, the scaling issues of an overlay VPN model are felt most when having to manage and provision a large number of circuits/tunnels between customer devices. From a customer's point of view, the Interior Gateway Protocol design is typically extremely complex and also difficult to manage.

On the other hand, the peer-to-peer VPN model suffers from lack of isolation between the customers and the need for coordinated IP address space between them.

With the introduction of Multiprotocol Label Switching (MPLS), which combines the benefits of Layer 2 switching with Layer 3 routing and switching, it became possible to construct a technology that combines the benefits of an overlay VPN (such as security and isolation among customers) with the benefits of simplified routing that a peer-to-peer VPN implementation brings. The new technology, called MPLS/VPN, results in simpler customer routing and somewhat simpler service provider provisioning, and makes possible a number of topologies that are hard to implement in either the overlay or peer-to-peer VPN models. MPLS also adds the benefits of a connection-oriented approach to the IP routing paradigm, through the

establishment of label-switched paths, which are created based on topology information rather than traffic flow.

CHAPTER SIX
VIRTUAL PRIVATE NETWORKS (VPNs)

6.1 Need For Virtual Private Networks

There are two alternatives when it comes to connecting various branch offices of a corporation spread around the globe. Either use private leased lines to connect all the branches with each other or use the available public Internet. The same techniques can be used for the communication between a company and its trusted partners.

The advantages of using private lines for communication are numerous. We get the guaranteed bandwidth, which is available 24 hours a day. At the same time, since it is private network, security threats are much lower. But at the same time there are some problems with this approach. First thing is that it might be very uneconomical to afford this kind of networks especially when the networking is required on a global scale. Also for providing full connectivity among various sites, the number of lines required increase as the square of number of sites. Besides that the network is not scalable. Considering an these problems, a lot of companies are moving towards the use of Internet for the private communication.

It is not possible to use the public Internet for private communication without making any enhancements to it. This is because the Internet does not have enough provisions for security. Also most part of the Internet is based on best effort service, which might not be the desirable feature for private communication. Therefore some changes are required to the existing Internet before it can be used for private communication. For this purpose, logical channels are set up through the Internet, which look like the private network to the end user while still avoiding all the disadvantages of use of private network. These are called Virtual Private Network. Advantages of use of VPNs:

1. They are economical because Internet is being used.
2. They are scalable.

3. User can ask for different Quality of Services by using various Service Level Agreements.
4. They are easy to deploy

6.2 Connection-Oriented VPNs

Connection-oriented VPNs can be built on Layer 2 or Layer 3 infrastructures. VPNs built using connection-oriented, point-to-point overlays such as Frame Relay and ATM virtual connections are examples of Layer 2 connection-oriented VPN networks.

VPNs built using a full or partial mesh of tunnels utilizing IPSec (with encryption for privacy) or Generic Routing Encapsulation (GRE) are examples of Layer 3 connection-oriented VPN networks.

Access VPNs are circuit-switched, connection-oriented VPNs that provide a temporary secure connection for remote access between individuals (mobile users or telecommuters) and a corporate intranet or extranet over a shared service provider network with the same policies as a private network. Access VPNs that use dial access into an ISP point of presence (PoP) with transport over the public Internet and ultimate access into a corporate intranet.

The key deficiency of connection-oriented VPNs is scalability. Specifically, connection-oriented VPNs without meshed connections between customer sites are not optimal. Furthermore, in the case of Layer 3 IP VPNs, you cannot truly guarantee a firm QoS (Quality of Service) over the public Internet. From the perspective of telecom management, the complexity associated with provisioning ATM or Frame Relay Virtual Circuits is comparable to the complexity of provisioning private lines.

Virtual circuit-based VPNs require service providers to build and manage separate virtual circuits or logical paths between each pair of communicating sites within each

user group. This requirement equates to building a mesh of virtual circuits for each customer.

6.2.1 Layer 2 Connection-Oriented VPNs

Layer 2 connection-oriented networks form the basis of the overlay VPN model. In the overlay VPN model, the service provider provides the virtual circuits, and the routing information is exchanged directly between the CPE routers.

6.2.1.1 TDM-Based Networks

Most service providers offer private-line networks to enterprise customers. This involves digital multiplexing, in which two or more apparently simultaneous channels are derived from a bit stream by interleaving bits from successive channels. Typically, service providers or carriers offer DS1 and DS3 circuits in North America. E1 and E3 circuits are commonly found in Europe and Asia Pacific.

As shown in Figure 6.1, Customers A and B share the physical infrastructure of the carrier, but they are logically separated from each other by port mappings and electronic cross-connections provisioned by the carrier. The cross-connections are typically provisioned on a DACS (Digital Automatic and Crossconnect System). However, physical crossconnects are also used extensively.

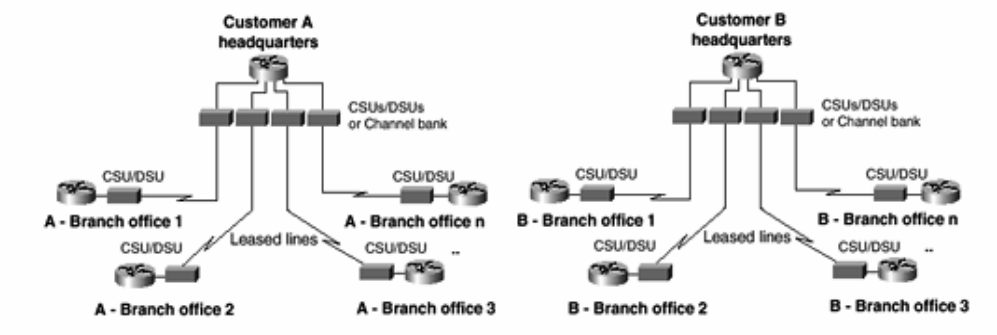

Figure 6.1 Leased Line VPN—Logical View

The TDM network is the simplest form of a Virtual Private Network that assures high-quality fixed bandwidth to customers. Most carriers offer bandwidth as multiples of 64 kbps, which is the bandwidth of a single DS0 channel.

6.2.1.2 Frame-Based VPNs

Frame-based VPNs such as Frame Relay and X.25 use logical paths as defined by switched and permanent virtual circuits. As shown in Figure 6.2, multiple closed user groups or customers share the service provider's switched infrastructure. Customers perceive virtual circuits that have been exclusively provisioned for their private use. These PVCs or SVCs can be provisioned with a fixed CIR and port speed (local loop access line bandwidth).

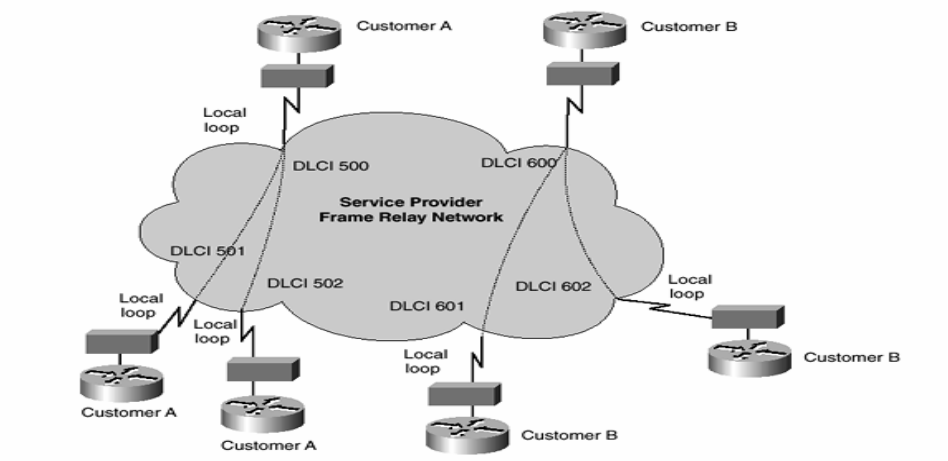

Figure 6.2 Logical Frame Relay VPN Architecture

Figure 6.2 shows the physical Frame Relay network. Customers A and B both connect to various Frame Relay points of presence (POPs) using TDM local loops. The Frame Relay protocol is run between the local CPE FRAD (router) and the Frame Relay switch. The Frame Relay interworking function converts Frame Relay frames into ATM cells for transport across the ATM backbone.

6.2.1.3 Cell-Based VPNs

Cell-based VPNs such as ATM and SMDS use logical paths as defined by switched and permanent virtual circuits. As shown in Figure 6.3, multiple closed user groups or customers share the Service Providers Switched infrastructure. Customers perceive virtual circuits that have been exclusively provisioned for their private use. These PVCs or SVCs can be provisioned with a class of service such as CBR, VBR-RT, VBR-NRT, ABR, or UBR. ATM also enables the provisioning of soft PVCs, which are a hybrid of SVCs and PVCs.

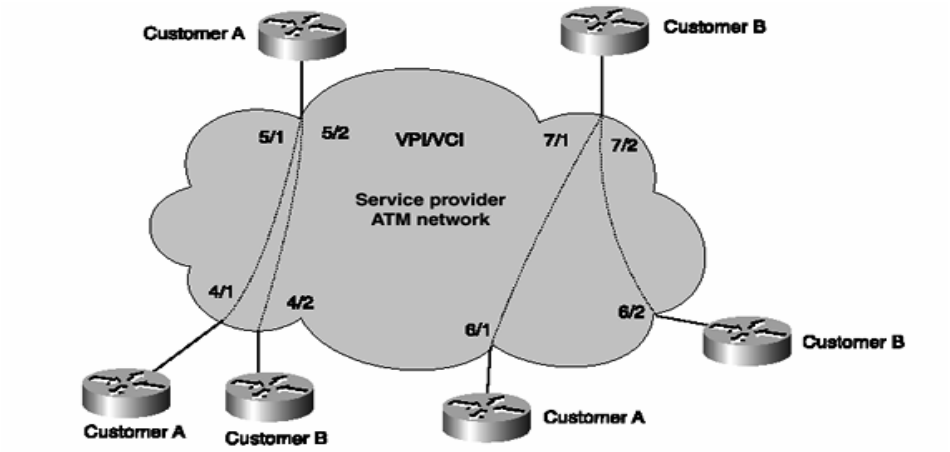

Figure 6.3 Logical ATM VPN Architecture

6.2.2 Layer 3 Connection-Oriented VPNs

Layer 3 connection-oriented networks form the basis of the tunneled VPN model. The GRE and IP Security (IPSec) models provide a point-to-point tunneled model over an IP intranet or the public Internet, whereas virtual private dialup networks (VPDNs) provide a hybrid combination of dialup along with a secure tunnel connection over the Internet to an enterprise aggregation point such as a home gateway.

6.2.2.1 GRE Tunneled VPNs

Generic Route Encapsulation (GRE) tunnels can be used to create point-to-point IP connections. A combination of these GRE tunnels can be used to build a VPN. However, the lack of inherent security by virtue of the lack of encryption makes GRE tunnels susceptible to security violations.

As shown in Figure 6.4, GRE tunnels are useful for building VPNs within a service provider's private IP backbone network. They are also useful for tunneling non-IP Layer 3 traffic across a private IP network.

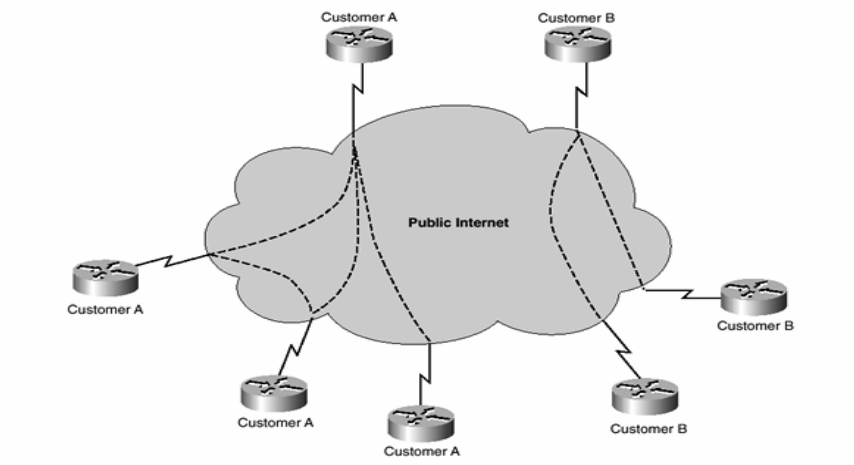

Figure 6.4 GRE and IPSec Tunneled VPNs

6.2.2.2 IPSec Tunneled VPNs

IPSec is a highly secure technology that uses a combination of encryption and a tunneling mechanism, which protects packet payloads as they traverse an IP network. IPSec is normally implemented over untrusted public IP networks such as the Internet. A combination of point-to-point IPSec tunnels can be used to construct a VPN over a public IP network. Most IPSec architectures are implemented on the CPE, and service providers would normally provide Managed IPSec VPN services. An example of an IPSec network topology is shown in Figure 6.4. For mobile users

and telecommuters who require secure remote access, IPSec is the only practical option at present to enable secure remote access VPNs.

6.2.2.3 Virtual Private Dialup Network

Telecommuters and mobile users remotely access corporate networks over the Public Switched Telephone Network (PSTN) or ISDN. As shown in Figure 6.5, Virtual PrivateDialup Network (VPDN) services are mostly implemented over a service provider's private IP backbone. The protocols used to implement VPDN service over an IP network include Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocol (L2TP).

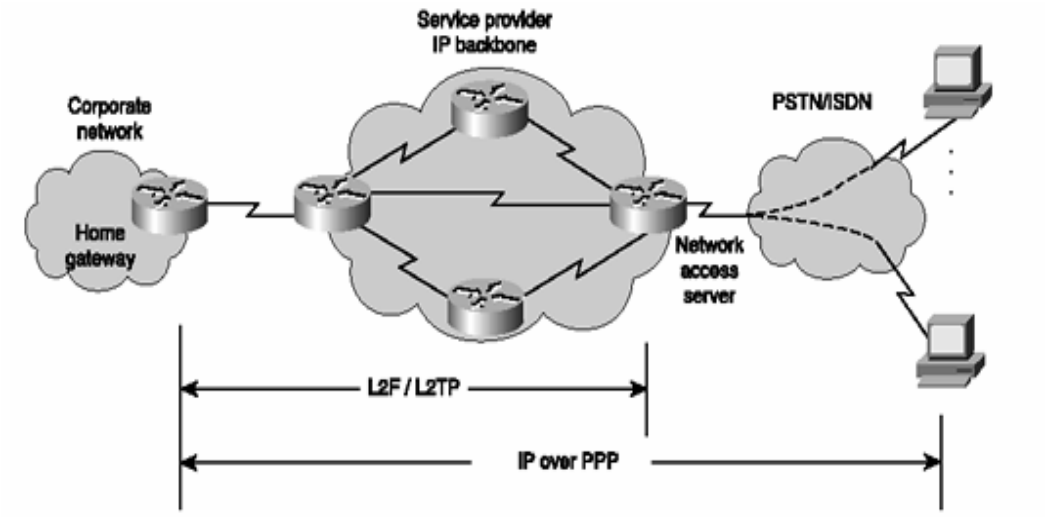

Figure 6.5 Virtual Private Dialup Network (VPDN)

The remote users initiate a dial-up connection to the Network Access Server (NAS) using PPP. The NAS authenticates the call and forwards the call via L2F or L2TP to the customer's home gateway. The home gateway accepts the call forwarded by the NAS, performs additional authentication, authorization, and terminates the user PPP session. The AAA (Authentication, Authorization and Accounting) function can also be performed by an AAA server such as a TACACS+ server. All PPP session parameters are negotiated between the dial-up user and the home

gateway. Access VPNs such as VPDNs suffer from certain limitations in the sense that they are not scalable and do not provide any-to-any connectivity.

The Point-to-Point Tunneling Protocol (PPTP) along with Microsoft Point-to-Point Encryption (MPPE) allow Cisco VPNs to use PPTP as the tunneling protocol. PPTP is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across an IP-based network. PPTP utilizes voluntary tunneling (also referred to as client-initiated tunneling), which allows clients to configure and establish encrypted tunnels to tunnel servers without an intermediate NAS participating in tunnel negotiation and establishment.

PPTP utilizes MPPE as its encryption technology over a dialup line or a VPN tunnel. MPPE works as a subfeature of Microsoft Point-to-Point Compression (MPPC). MPPE uses either 40- or 128-bit keys. All keys are derived from the user's clear-text authentication password. The MPPE algorithm is stream cipher; therefore, the encrypted and decrypted frames are the same size as the original frame. The Cisco implementation of MPPE is fully interoperable with that of Microsoft and uses all available options, including historyless mode.

6.3 Connectionless VPNs

Connectionless VPNs do not require a predefined logical or virtual circuit provisioned between two endpoints to establish a connection between the two endpoints.

6.3.1 Conventional IP VPNs

Many carriers provide a managed IP services offering that basically lets customers hook up their CPE IP routers to a service provider's private IP backbone. Most IP service providers run an IP network over a Layer 2 infrastructure such as an ATM or Frame Relay network. An example of a conventional IP VPN is shown in Figure 6.6.

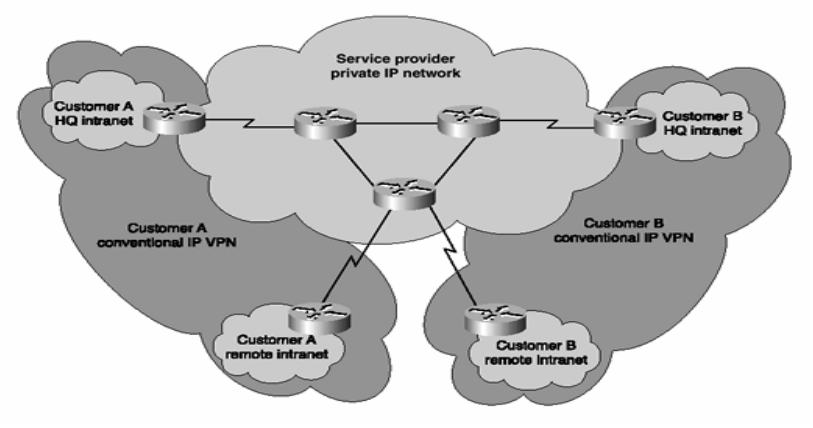

Figure 6.6 Conventional IP Router-Based VPN Network

The service provider typically configures multiple routing protocols or runs multiple routing processes on its backbone routers for various customers. Typically, the Cisco Routing engine supports the operation of multiple routing protocols in a single router in order to connect networks that use different routing protocols. The routing protocols available are inherently designed to operate independently of each other. Each protocol collects different types of information and reacts to topology changes in its own way. For example, RIP uses a hop count metric and EIGRP uses a five-element vector of metric information.

More importantly, a Cisco router can typically handle simultaneous operation of up to 30 dynamic IP routing processes. The combination of routing processes on a router can consist of the following protocols (with the limits noted):

- Up to 30 IGRP routing processes
- Up to 30 OSPF routing processes
- One IS-IS process
- One RIP routing process
- One BGP routing process
- Up to 30 EGP routing processes

Customers perceive a private IP VPN by virtue of a combination of access lists, routing protocols, and processes.

The biggest issue facing managed IP service providers is scalability and complexity of implementation. The number of available routing protocols and routing processes supported per router platform sometimes forces service providers to deploy separate routers for each customer VPN at the service provider's point of presence.

6.3.2 MPLS VPNs

MPLS VPNs are connectionless. MPLS separates traffic and provides privacy without the need for Layer 2 tunneling protocols and encryption. This eliminates significant complexity during the provisioning process.

MPLS solves the scalability issues encountered by Frame Relay and ATM deployments by allowing service providers to provision multiple VPNs for multiple customers without the chore of provisioning tens to hundreds of virtual circuits for each and every closed user group or customer. An example of an MPLS VPN is shown in Figure 6.7. Customers A and B share the service provider infrastructure while having the ability to form their own closed user groups with utmost security. They also can run their own routing protocols.

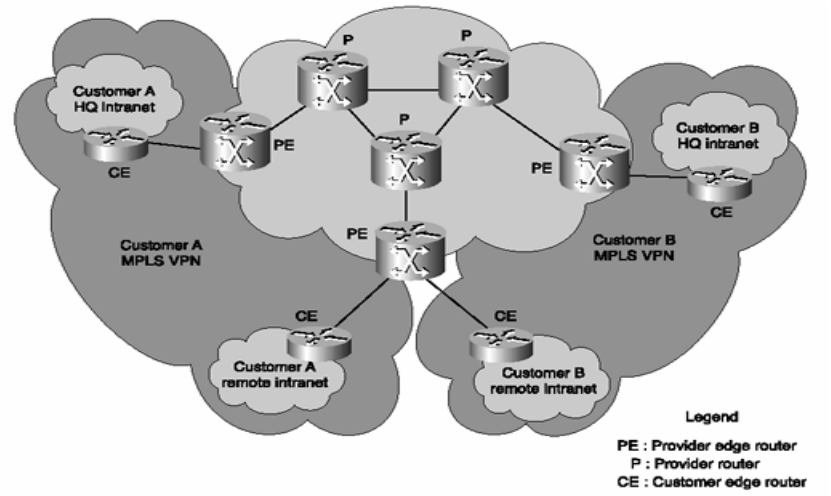

Figure 6.7 MPLS Virtual Private Network

The MPLS model requires the CPE routers to directly exchange routing information with provider edge routers, as opposed to exchanging routing information with all other CPE routers that are members of the VPN. Members of the

VPN are identified as belonging to the closed user group by means of labels. These labels carry next-hop information, service attributes, and a VPN identifier, which keeps communications within a VPN private.

At the ingress into the provider network, incoming packets from the CPE router are processed, and labels are assigned based on the physical interface these packets were received from. Labels are applied using VRF (VPN Routing and Forwarding) tables. The forwarding tables are predetermined, and incoming packets are examined only at the ingress LSR. The core devices or Provider (P) LSRs merely forward these packets based on labels.

MPLS makes service provider-routed backbones VPN-capable and provides Layer 3 visibility even across Layer 2 infrastructures. This makes it possible to create closed user groups and associate services with them.

CHAPTER SEVEN
MPLS FOR VIRTUAL PRIVATE NETWORKS (VPNs)

7.1 Elements of an MPLS VPN solution

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.

The rest of this chapter gives an overview of the basic elements of an MPLS-based VPN solution and the applicability of MPLS to different VPN types. Subsequent chapters examine the trickier aspects of MPLS for VPNs in greater detail.

Let us consider how MPLS can provide a VPN solution by examining how it would work at several different levels. We start with the data forwarding mechanics and work our way up to the network management considerations. Different implementation models for MPLS based VPNs imply different interactions between these elements of a VPN solution. See the section VPN Implementation Models for further details.

7.1.1 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.

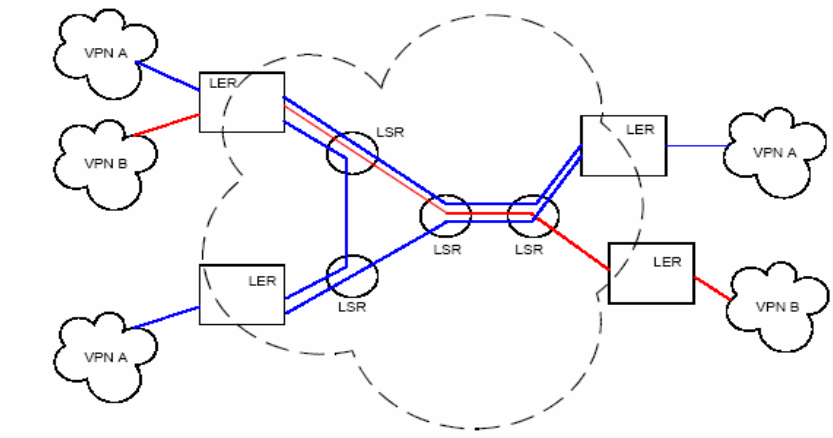

Figure 7.1 VPN Connectivity Using LSP Tunnels

Figure 3 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.

7.1.2 VPN Traffic Engineering

An LSP tunnel forms an excellent encapsulation scheme for VPN data flowing between two LSRs. But how do LSRs determine which LSPs to set up to provide connectivity for VPNs. In effect, how do LSRs decide which other LSRs provide access to the VPNs which they themselves serve. Even once this has been done, how should the different VPNs be mapped into LSP tunnels a separate tunnel for each VPN, or a single tunnel for all VPNs.

These are complex questions that do not have a single "right" answer. There is a number of factors that determine what VPN Traffic Engineering (TE) scheme best suits the performance and scalability requirements of a particular customer and their SP.

• *Identifying VPN peers*

This is the first problem facing an LSR that has been configured to support a VPN. The simplest scheme is to use explicit manual configuration of the VPN peers. This is the traditional solution providing obvious and deterministic control of resources and security, but it does not scale well as the size and complexity of the VPN increases.

Alternative schemes automate the process of discovering VPN peers using a directory or by overlaying VPN membership information on one or more routing protocols used on the SP network. This greatly simplifies the configuration task for a VPN since it means that each SP edge router need only be configured with information about the VPNs serviced by each of its customer interfaces. There is

clearly a potential security trade-off here as rogue routers can pretend to give access to a VPN.

In comparison, an IPSEC-based solution [15] requires that each SP Edge router also be configured with security attributes for each peer in the VPN, which greatly increases the configuration complexity.

• *Multiplexing VPNs on an LSP*

Although LSRs in the core of the SP network do not have to examine the data flowing on VPN LSP tunnels, they are still aware of the existence of these tunnels. This can represent a scalability problem if a separate mesh of LSP tunnels is used for each VPN, because the core LSRs must at least maintain a forwarding table entry and associated resource reservation for each tunnel.

If the SP supports thousands of VPN customers, the core LSRs could be required to maintain millions of LSPs. This is the same problem faced by VPN solutions based on ATM or Frame relay technology. Depending on the network topology, this large number of labels may also be beyond the capacity of the LSR switching hardware.

An alternative approach is to multiplex the traffic from multiple VPNs that share the same ingress and egress SP edge routers within a single LSP tunnel between those LSRs. This is achieved using label stacks, with a single outer tunnel set up across the core and an inner LSP that identifies the VPN for which the data is bound. The lower label in the stack is known only to the ingress and egress LSRs.

This use of label stacks reduces the number of LSP tunnels exposed to the network core, but it ties VPNs together. The multiplexed VPNs cannot be routed separately or given different prioritization or drop priority by the core LSRs. The VPNs must also share a single network resource reservation within the network core,

which may make it harder for the SP to guarantee the SLA for each individual customer.

In figure 7.2, two VPNs are connected across the MPLS network between a pair of LERs. The traffic for each VPN is carried on a distinct LSP shown as a red and a green line in the diagram. These two VPNs are nested within an outer LSP shown in blue.

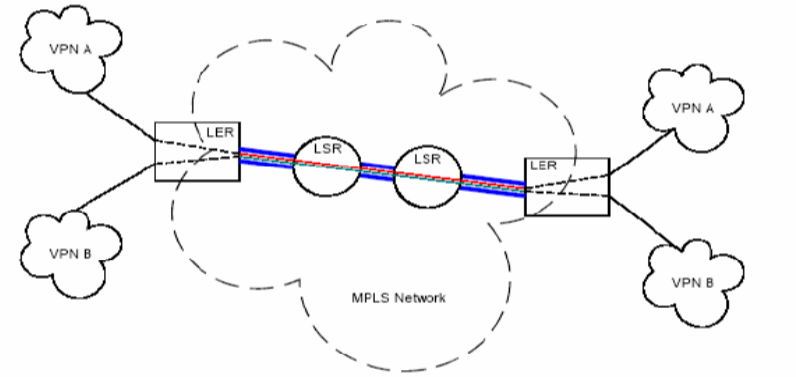

Figure 7.2 Nested LSPs Providing VPN Connectivity

• *Separating QoS classes*

Multiplexing VPNs within a single tunnel helps to reduce the signaling load and forwarding table size in the core LSRs as the number and size of the VPNs increase. However, once the data for multiple streams has been clustered together in a single LSP, it is hard to provide distinct management of the different flows. The encoding of an MPLS label allows three bits to encode the Differentiated Services Control Point (DSCP). Thus a total of eight classes of service (CoS) can be set for packets within any one LSP. These bits can define queuing rules and drop priorities for packets carried on the LSP. In the case of an ATM-based network there is just one bit available to encode the DSCP and this is usually used simply to indicate the drop preference.

If a customer or SP needs to be able to differentiate more than eight DSCPs across the core, multiple outer LSP tunnels must be set up. Each outer tunnel carries a different CoS range and can be routed separately across the core. The interaction between setting up multiple outer tunnels across the core to carry more CoSs, and the need to minimize the number of such tunnels using VPN multiplexing on a single tunnel is examined in more detail in the VPN Multiplexing and Class of Service section below. The IETF draft draft-ietf-mpls-diff-ext [12] defines methods of signaling LSPs for CoS usage and ways of determining the interpretation of the DSCP bits.

• *TE across the backbone*

MPLS TE can be used to distribute the load within a network and to guarantee bandwidth and QoS by controlling the routing of the outer VPN LSP tunnels across the SP backbone network. This is essentially the same problem as TE for non-VPN traffic, and hence is outside the scope of this paper.

7.1.3 Network Management

The management of a VPN falls into two categories.

• Defining the logical topology of the VPN.

• Mapping the VPN onto the SP's physical network, including routing the VPN data across the core network.

The second of these functions is always the preserve of the SP. The first feature may, however, be managed by the SP or by the customer on a self-serve basis.

7.2 Applicability of MPLS to VPN Types

MPLS LSP tunnels can be used to provide all or part of an implementation of any of the four types of VPN. The suitability of an MPLS solution to each VPN type is described below, including the scalability and management challenges such solutions present.

7.2.1 MPLS for VLL

Conceptually, this is the easiest application of MPLS to VPNs. Each point-to-point VLL is provisioned as an LSP tunnel between the appropriate customer sites. The customer is explicitly looking for the equivalent of leased lines, so it is very important that the SP meets any bandwidth guarantees in the SLA. This means that the LSP tunnels used in a VLL solution may have to be dedicated to that specific customer rather than multiplexing the VLL traffic with other VPNs. It is also possible to subdivide the resources of an outer tunnel to provide the QoS for inner LSPs.

The point-to-point connectivity of a VLL means that each VLL is most easily provisioned at the edge LSRs by manual configuration rather than an automatic scheme for detecting the VLL peers.

7.2.2 MPLS for VPLS

The most immediately obvious means of implementing a VPLS is to map the LAN segment to a unique IP multicast address perhaps using IP encapsulation of the VPN IP traffic. Such a solution could use existing IP multicast technologies, rather than MPLS. Indeed, such approaches are offered by many ISPs today.

However, technologies such as MOSPF and (non-labels) RSVP do not provide the full TE capabilities of MPLS, so the SP has less control over how the VPLS traffic is routed across the backbone network.

Very large SPs with many VPLS customers may also eventually find that there are too few administratively scoped IPv4 multicast addresses to represent each of the VPN LAN segments that they need to support, forcing them either to move to IPv6 or to multiplex several VPLSs on one multicast address. There are 224

administratively scoped IP multicast addresses (239./8), but an SP may well wish to reserve only a portion of this address space for VPN services.

Current MPLS label distribution protocols are specified for unicast destination IP addresses only. This means that an MPLS-based implementation of a VPLS is, necessarily for now, based on one of the following network topologies.

- A full mesh of LSP tunnels connecting the customer sites, with each SP edge LSR responsible for the fan-out to all peers.
- Point-to-point or multipoint-to-point LSP tunnel connections to a "hub" LSR that handles fan-out to all sites using point-to-point LSP tunnels.

In both cases, but especially for the mesh of LSP tunnels, the MPLS-based topology may use more network bandwidth in total that the IP-multicast based solution. This is because multiple copies of each packet may be sent across any given link, each copy carried within one of several different LSP tunnels for the VPLS that transit that link. However, SPs may still choose to implement a VPLS using MPLS in order to exploit the TE capabilities of MPLS to give them better control of how the VPLS traffic is routed between SP edge LSRs.

Future standardization work on MPLS may extend the TE capabilities to cover point-to-multipoint or multipoint-to-multipoint LSP tunnels. Such an extension would allow MPLS-based implementations of a VPLS to avoid the bandwidth overhead compared to an IP-multicast based implementation.

7.2.3 MPLS for VPRN

LSP tunnels provide an excellent solution to VPRNs. A VPRN is routed, rather than requiring point-to-multipoint connectivity. This means that even if the SP edge routers set up a full mesh of LSP tunnels to all the other SP edge routers for a given VPRN, they can route each packet onto a single LSP tunnel according to the destination address for that packet rather than fanning out copies to all peers for that

VPRN. This avoids the bandwidth wastage that can occur when using an MPLS-based VPLS, as described in the previous section.

Note that the routing protocols used on a VPRN are independent of the routing protocols used on the SP backbone. It is perfectly possible for an SP to use OSPF and BGP4 but for a VPN customer to use a much simpler protocol such as RIP.

7.2.4 MPLS for VPDN

MPLS could be used as the underlying transport mechanism between the LAC and LNS in an L2TP-based VPDN. This is no different from using MPLS to transport any other data that uses public IP addresses. The essential function of a VPDN is provided by L2TP. For this reason, no further consideration is given in this paper to the use of MPLS for VPDNs.

CONCLUSION

MPLS was designed specifically for highly scalable solutions, enabling tens of thousands of VPNs over the same network. MPLS-based VPNs use the peer model and Layer 3 connectionless architecture to leverage a highly scalable VPN solution. The peer model requires a customer site to peer with only one provider edge (PE) router as opposed to all other CPE or customer edge (CE) routers that are members of the VPN. The connectionless architecture allows the creation of VPNs in Layer 3, eliminating the need for tunnels or VCs.

MPLS VPNs offer the same level of security as connection-oriented VPNs (such as Frame Relay and ATM). Packets from one VPN do not cross into another VPN involuntarily. Security is provided at the edge of the provider network, ensuring that packets received from a customer are placed on the correct VPN. At the backbone, VPN traffic is kept separate. Spoofing (an attempt to gain access to a PE router) is nearly impossible, because the packets received from customers are IP packets that must be received on a particular interface or subinterface to be uniquely identified with a VPN label.

Specific point-to-point connection maps or topologies are not required. Sites can be added to VPN intranets and extranets to form closed user groups. When VPNs are managed in this manner, it enables membership of any given site in multiple VPNs, maximizing flexibility in building intranets and extranets. MPLS functionality resides in the provider network, requiring little or no configuration on the customer premises. MPLS is transparent to the CPE router and customer CPE devices and do not need to run MPLS.

QoS mechanisms present the industry with a true end-to-end QoS solution, allowing providers to guarantee SLA compliance. MPLS makes QoS services more scalable and extends their reach end-to-end across multiple technologies.

Routing with Resource Reservation (RRR) using extensions to the RSVP protocol lets providers maximize the utilization of network resources and operate their IP networks as efficiently as possible. RRR allows the network operator to apply and enforce explicit routing, which overrides the traditional IP forwarding techniques and provides fast restoration and protection mechanisms. Underutilized links can be forced to carry traffic, thereby resulting in an optimum routing scenario.

CoS is an important requirement for many IP VPN customers. It provides the ability to address two fundamental VPN requirements:

- Predictable performance and policy implementation
- Support for multiple levels of service in an MPLS VPN

Network traffic is classified and labeled at the edge of the network before traffic is aggregated according to policies defined by subscribers and implemented by the provider and transported across the provider core. Traffic at the edge and core of the network can then be differentiated into different classes by drop probability or delay.

The term Virtual Private Network (VPN) is used to identify a closed user group within a network. The IP-based VPN is rapidly becoming the foundation for the delivery of consolidated data, voice, and video services. IPSec and MPLS technologies are emerging to form the predominant foundations for delivery of consolidated services.

Connection-oriented VPNs can be built on Layer 2 or Layer 3 infrastructures. Frame Relay and ATM virtual connections are examples of Layer 2 connection-oriented VPN networks. IPSec Layer 2 tunneling protocol (L2TP), Layer 2 forwarding (L2F) protocol, and Generic Routing Encapsulation (GRE) are examples of Layer 3 connection-oriented VPN networks. Access VPDNs are also examples of connection-oriented VPNs.

Connectionless VPNs do not require a predefined logical or virtual circuit provisioned between two endpoints to establish a connection between the two

endpoints. Layer 3 connectionless networks form the basis of the peer-to-peer model. In the peer-to-peer model, the customer routing information is exchanged between the CPE and the service provider routers. Conventional IP VPNs and MPLS VPNs are examples of connectionless VPNs.

Two distinct technologies have emerged as the preeminent building blocks from which to create VPNs: MPLS and IPSec. Service providers should deploy one of these VPN architectures primarily based on the customers and market segments they serve, the value-added services they want to offer, and their own network priorities.

REFERENCES

Gallaher, R. (2003). MPLS Training Guide: Building Multi-Protocol Label Switching Networks. Rockland: Syngress Publishing, Inc.

Wait, J. (Ed). (2003). Traffic Engineering with MPLS. Indianapolis; Cisco Press

Alwayn, V. (2002). Advanced MPLS Design and Implementation. Indianapolis; Cisco Press

Ryan, J. (1998) Multi Protocol Label Switching. Retrieved 1998, from http://www.techguide.com

Gray, D., Boalte, J. & Rajagopal, A., (2002). MPLS on the IP Backbone. A Wiltel Communications Technical Brief for IP VPN.

Adolfo Rodriguez& John Gatrell& John Karas& Roland Peschke ,TCP/IP Tutorial and Technical Overview,IBM,2001

Andrew S. Tanenbaum , Computer Networks,Second Edition, Prentice- Hall PTR, 1999

Ericsson Training Book , Voice Over IP , Telefonaktiebolaget LM Ericsson , 2000

Mani Subramanian , Network Management Principles and Practice, 2000

Martin W. Murhammer&Kok-Keong Lee&Payam Motallebi&Paolo Borghi, IP Network Design Guide , IBM , 1999

S. Keshav ,An Engineering Approach to Computer Networking, , Reading, MA: Addison-Wesley, 1997.

S. Shenker& C. Partridge& R. Guerin , Specification of Guaranteed Quality of Service, RFC 2212.

Uyless Black, Voice over IP , Prentice-Hall PTR,1999

V. Jacobson , Compressing TCP/IP Headers for Low-Speed Serial Links , RFC 1144 ,1990.