MEE09:44

BLEKINGE INSTITUTE OF TECHNOLOGY
School of Engineering
Department of Telecommunication Systems

Investigation of different VPN Solutions And Comparison of MPLS, IPSec and SSL based VPN Solutions

(Study Thesis)

Name: **Sheikh Riaz Ur Rehman**
Personal Number: **750929-0735**
Email: **rure06@student.bth.se**

Supervisor: **Adrian Popescu**

Examiner: **Adrian Popescu**

Abstract

The rapid growth of e-business in past few years has improved companies efficiency and revenue growth. E-business applications such as e-commerce, remote access has enabled companies to manage processes, lower operating costs and increased customer satisfaction. Also the need rises for the scalable networks that accommodate voice, video, and data traffic. With the increased dependability of networks the security issues are raised and networks become more and more vulnerable to different types of security threats. To overcome security issues different security technologies are in action by vendors and technologists. Also for the survival of many businesses to allow open access to network resources, today's networks are designed with the requirement of availability to the Internet and public networks, therefore, information confidentiality is the major issue in these networks to ensure that the network resources and user data are as secure as possible.

With the requirement of network security, concept of Virtual private network was established. A Virtual Private Network (VPN) can be defined as a network in which connectivity between multiple customers' sites is deployed on a shared network with the same security as a private network. Different VPN technologies and protocols architectures are available in market among are MPLS VPN architecture, IPSec VPN architecture, and SSL VPN architecture. Like With the introduction of Multiprotocol Label Switching (MPLS), which combines the benefits of Layer 2 switching and Layer 3 routing, it became possible to construct a technology that combines the benefits of an overlay VPN with the benefits of peer-to-peer VPN implementation in which routing is simple. MPLS/VPN is a new and simple technology, which provides simpler to routing and also makes number of topologies easy to implement which are otherwise difficult to implement. All architectures have benefits and drawbacks, also each of them can be implemented separately or in combination of other according to customer security requirement and performance of the network.

ACKNOWLEDGEMENT

After the all praise to Almighty Allah, first of all I would like to thank my supervisor Dr. Adrian Popescu, who has given me chance to do my thesis work with him.

I would also like to show my appreciation and love for my parents who have always motivated and appreciated my efforts and my elder brother Dr. Moez Ur Rehman who guided and supported my during my studies in Sweden.

TABLE OF CONTENTS

Abstract 3

ACKNOWLEDGEMENT 5

TABLE OF CONTENTS 6

CHAPTER 1 9
Security and VPN Overview 9
1.1 VPN Terminology: 9
1.1.1 Trusted VPN: 9
1.1.2 SECURE VPNs: 10
1.1.3 Hybrid VPNs: 10
1.2 Different VPN Technologies 11
SUMMRY 12

CHAPTER 2 133
INTRUDUCTION to MPLS 133
2.1 MPLS Introduction 13
2.2 MPLS VPN 13
2.2.1 Layer 2 MPLS VPN 13
2.2.2 Layer 3 MPLS VPN 14
2.3 MPLS Traffic Engineering 14
2.3.1 MPLS Traffic Engineering Application 15
2.4 MPLS Services 15
2.5 MPLS Benefits 17
2.5.1 Benefits of MPLS to Service Providers 17
2.5.2 Benefits of MPLS to Enterprise Networks 17
2.6 Examine MPLS and Layer 3 Routing Limitations 18
2.6.1 Layer 3 Routing Limitations 18
2.7 Traditional IP Forwarding 18
2.7.1 Traditional IP Forwarding and Traffic Engineering 19
2.8 MPLS Architecture 19
2.8.1 Control Plane 20
2.8.2 Data Plane 20
2.9 MPLS Modes of Operation 20
2.9.1 Frame-mode MPLS 20
2.9.2 Cell-Mode MPLS 21
2.10 Label Headers 21
2.11 Label Switched Router Types 22
2.11.1 Label Switched Routers 22
2.11.2 Edge LSR 22
2.11.3 LSR 23
2.12 MPLS Forwarding 23
2.13 Summary 24

CHAPTER 3 25
MPLS Base VPN Architecture 25
3.1 Overview 25
3.2 MPLS VPN Architecture and Components 25
3.2.1 MPLS VPNs 25
3.2.2 MPLS VPN Architecture 25
3.3 MPLS VPN Routing Model 26
3.4 Propagation of Routing Information across the P-Network 27
3.5 Route Distinguisher 28
3.5.1 MP-IBGP and MP-EBGP 29
3.5.2 Route Distinguisher Number 29
3.6 Route Target 29
3.7 Packet Forwarding in MPLS VPN 30
3.8 Penultimate Hop Popping 32
3.9 Summary 32

CHAPTER 4 33
IPsec VPN 33
4.1 Introduction 33
4.2 Application of IPsec 34
4.2.1 Secure branch office connectivity over the Internet 34
4.2.2 Establishing Intranet VPN 34
4.2.3 Establishing Extranet VPN 35
4.2.4 Remote access VPN 35
4.2.6 Teleworkers 36
4.2.7 Security Enhancement of electronic commerce: 37
4.3 Benefits of IPsec 37
4.4 Applications in Routing 37
4.5 Architecture of IPSec 38
4.5.1 Documentation 38
4.6 IPsec Services 39
4.7 Security Associations 40
4.8 Transport and Tunnel Modes 42
4.8.2 Tunnel Mode 42
4.9 Authentication Header 42
4.9.1 Transport and tunnel Modes in AH 44
4.10 Encapsulating Security Payload 45
4.10.1 Transport and Tunnel Modes in ESP 46
4.11 Combining Security Association 48
4.11.1 Transport adjacency 48
4.11.2 Iterated Tunneling 49
4.12 Security Association's Combinations 50
4.13 Key Management 52
4.14 SUMMRY 53

Chapter 5 54

Secure Socket Layer (SSL) VPN 54
5.1 Introduction 54
5.2 SSL Architecture 54
5.2.1 Record Protocol 56
5.2.3 Change Cipher Spec Protocol 57
5.2.4 Alert Protocol 57
5.2.5 Handshake Protocol 58
5.3 Cryptographic Computations 58
5.3.1 Master secret 58
5.3.2 Cryptographic parameter generation 59
5.4 SSL VPN 59
5.5 Summary 59

Chapter 6 60
Comparison between Different VPN Models 60
6.1 Introduction 60
6.2 Criteria for Evaluating IP VPN Architectures for the Enterprise 60
6.2.1 High Availability 60
6.2.2 Security 61
6.2.3 QoS 61
6.2.4 Scalability 61
6.2.5 Management 61
6.2.6 Cost of Ownership 61
6.3 MPLS Based VPN 62
6.4 IPSec Based VPN 63
6.5 SSL Based VPN 64

Conclusion 67

REFERENCES 69

CHAPTER 1
Security and VPN Overview

In this thesis report I will describe three major technologies used in Virtual Private Networks in the computer networks. In recent years, enterprises, medium businesses and personal usage of Internet is increased dramatically.
The wide verity of VPN services and products are offered by competing vendors. This made organizations/enterprises confused about what to choose in connection with features like network protection etc.

First I will briefly describe and define the different kinds of VPNs and their usage in this chapter. From next chapters I will try to explore each mode in greater detail.

1.1 VPN Terminology:

A virtual private network is a private data and voice network that uses the public communication infrastructure while maintaining privacy by using security procedure and tunneling protocols.
VPNs are cheaper alternative of, leased lines and the expensive owned networks, by using the shared public networks. Now a days companies are using VPNs for intranet and extranet for both voice and data communication [1].

First in this chapter we will describe three major VPN types.

1: Trusted VPNs
2: Secure VPNs
3: Hybrid VPNs
Then we describe some VPN protocols.

1: GRE
2: PPTP
3: MPLS
4: IPSec
5: SSL

1.1.1 Trusted VPN:

In this kind of VPN the privacy in these legacy VPNs was only achieved by that the service provider assurance that the given circuit to the customer not be used by any other customer. Customer implements their own IP addressing scheme and security policies. In this scenario any one who have physical access to the network can see the customer's traffic in service provider networks. So the VPN customer must have the trust on the service provider that he will maintain the integrity of the communication link and uses

best business practices to avoid security risks, thus these VPNs are called “Trusted VPNs” [1].

Trusted VPN Technologies

Competing service providers are offering many types of trusted VPNs. Trusted VPNs are generally categorized into layer 2 VPN and layer 3 VPNs.

Layer 2 Trusted VPN

1: ATM circuits
2: Frame relay Circuits
3: Transport of layer 2 Frames over MPLS.

Layer 3 Trusted VPNs

1: MPLS with constrained distribution of routing information through BGP [1].

1.1.2 SECURE VPNs:

After increase usage of Internet and companies started relying on Internet as a communication medium, customers and service providers both concerned with secure communication. The legacy trusted VPNs had lack of real security, so the vendors started to create protocols that encrypt traffic at the edge of one network or at the originating device and transfer over the Internet like any other data and decrypt at receiving end of corporate network or at receiving end user device.
The encrypted data transfer, emulates that it is transferred in a secure tunnel between two networks. Even if attacker sees the traffic, he cannot read it, and any change in data is not possible without the notice of legitimate receiving network, hence will be rejected, if changed during transmission.
Networks that are constructed using encryption technologies are called “Secure VPNs” [1].

Secure VPN Technologies

1: IPSec with Encryption in either tunnel or transport modes.
2: IPSec Inside of L2TP
3: SSL3.0 or TLS

1.1.3 Hybrid VPNs:

More recently service providers have begun to offers a trusted VPN by using Internet instead of the public switched telephone networks for communication. Even these type of trusted VPNs also don’t provide security, but these VPN provide network segmentations for WAN. Management of these VPNs can be controlled by single site and can also provide QoS guarantee. With these trusted VPNs, secure VPN can also be combined to

provide security also and called hybrid VPNs. In this type of VPN security management is achieved by customers himself or can be taken by provider also.
Usually the part of hybrid VPNs are secure but it's up to the customer security needs and full hybrid VPNs can be secure.

Hybrid VPN Technologies

1: Any supported Trusted VPN combined with any secure VPN technology [1].

1.2 Different VPN Technologies

In the previous section we described the three major VPN types including trusted VPN, secure VPN, and hybrid VPN.
With the increased organization reliance on VPN**,** number of VPN protocol, GRE, PPTP, L2TP, MPLS VPN, IPSec and SSL VPN, and procedures were defined and used by vendors and some of them were standardized by IETF (Internet Engineering Task Force) [17].

The VPN protocols can also be categorized in two major groups [17].

1) Site to Site VPN
2) Remote access VPN

Site-to-Site VPN
Site-to-site VPN Protocols are used to establish network connection between two or more organization's offices using shared medium such as Internet, to securely transmit network traffic. Protocol most commonly used in site-to-site VPN are, GRE, MPLS VPN, and IPsec.

Remote Access VPN
Remote access VPN protocols are used to establish connection between mobile users and organization's network by using shared medium such as Internet for securely transmitting network traffic. Protocols most commonly used in remote access VPN are PPTP, L2TP, IPsec and SSL VPN.

GRE (Generic Routing Encapsulation): GRE is a simple protocol which is used for multiprotocol and for IP multicast transportation, if there is only IP connectivity between two or more sites. Simple VPN can be created by GRE. GRE is an encapsulation protocol which encapsulates packets inside of transport protocol. But GRE does not have any cryptographic mechanisms thus does not provide encryption natively. GRE provide reliable and powerful tunnel but it has lack of security especially across untrusted networks. IPSec can be used in combination with GRE to provide security not only for IP traffic but also for non-IP traffic and also support multicasting.

PPTP (Point to Point Tunneling Protocol): Microsoft developed PPTP it is one of the first remote access VPN technology and still popular. WINDOWS operating system

support PPTP is main reason of its popularity. The PPTP encapsulate PPP frames between the VPN client and VPN server. PPTP uses GRE to encapsulate user data. The PPTP uses an ISP to provide low cast access to enterprise network to Dial-up users by creating a tunnel from client to server. Almost every vender support PPTP and it provide grater interpretability; also client software is easily available. Initial Implementation has some security vulnerabilities. PPTP also may not work with PAT and firewall, if they are now aware of PPTP characteristics.

MPLS VPN: MPLS VPN technology is most scalable VPN technology. We will discuss MPLS and MPLS VPN in **CHAPTER 2** and **CHAPTER 3** respectively in grater detail.

IPSec VPN: IPSec is used to provide secure data transmission over IP network it can provide authenticity, integrity, confidentiality to the transmitted data; we will discuss IPSec in **CHAPTER 4.**

SSL VPN: SSL VPNs are useful to secure web based VPN. We will discuss SSL in grater detail in **CHAPTER 5**

SUMMRY

In this chapter first we described the VPN definition and then types and VPN technologies in each type. In the last section we also described VPN categorization as site-to-site VPN and remote access VPN and technologies included in each category.

CHAPTER 2
INTRUDUCTION to MPLS

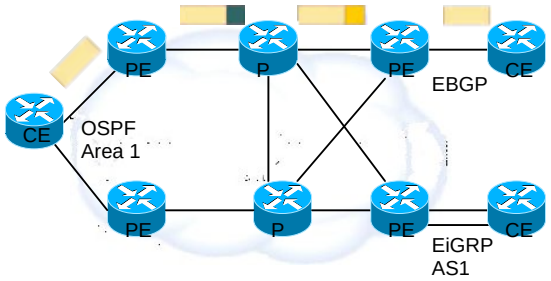
In previous chapter we described MPLS as trusted VPN technology; in this chapter we discuss the benefits of MPLS, how MPLS enhance network services of organizations and service provider by first by understanding the basic concept of MPLS.

2.1 MPLS Introduction

IP networks can provide additional services by enabling MPLS, services include are virtual private networks (VPNs), by encapsulating OSI Layer 3 VPN packets or OSI Layer 2 VPN frames using MPLS labels. MPLS also provides traffic engineering and other services that are not available in traditional IP networks.

To use MPLS all devices in the forwarding paths must support MPLS functionality. This requirement is for both the provider (P) core devices and for provider-edge (PE) devices. If MPLS supported features such as MPLS VPNs or MPLS Traffic Engineering (MPLS TE) are deployed than all the participating devices must support these features.

Usually customer-edge (CE) devices don't need to support MPLS functionality, because MPLS switching is performed in the provider core network. However, some advanced solutions (like Carrier Supporting Carrier [CsC]) do require CE devices to support MPLS [2][3].



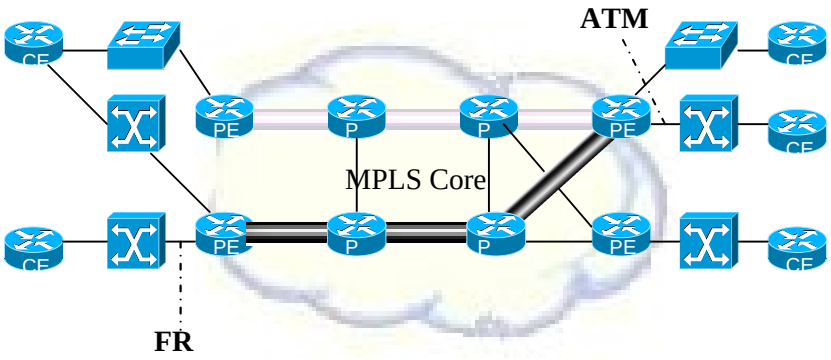
Basic MPLS Architecture

2.2 MPLS VPN

2.2.1 Layer 2 MPLS VPN

Layer 2 MPLS VPN technologies is used to provide VPNs by encapsulating the entire VPN frame with the use of MPLS labels, and forward the frames through the MPLS backbone. Layer 2 MPLS VPNs are usually implemented in a point-to-point configuration.

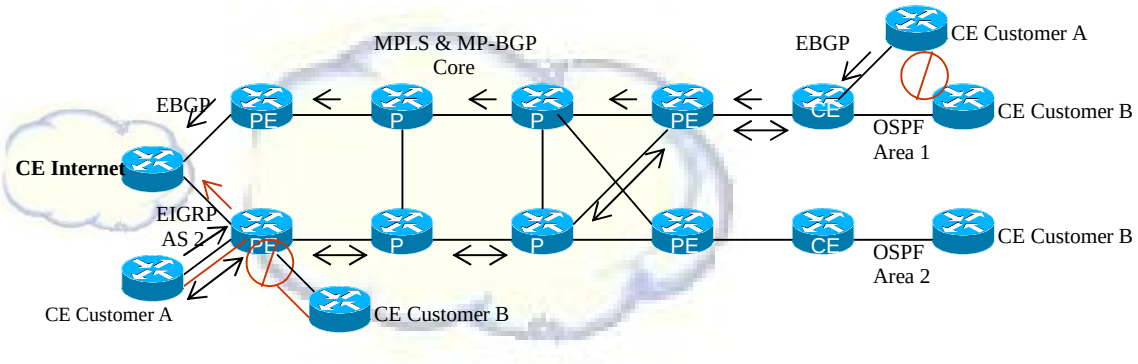
The figure illustrates some of possibilities in implementing Layer 2 MPLS VPNs. Some Layer 2 services provided by MPLS networks are, PPP over MPLS, HDLC over MPLS Point-to-point Ethernet over MPLS, ATM Cell Relay over MPLS, Frame Relay over MPLS, TDM over MPLS [4][5].



Layer 2 MPLS VPN

2.2.2 Layer 3 MPLS VPN

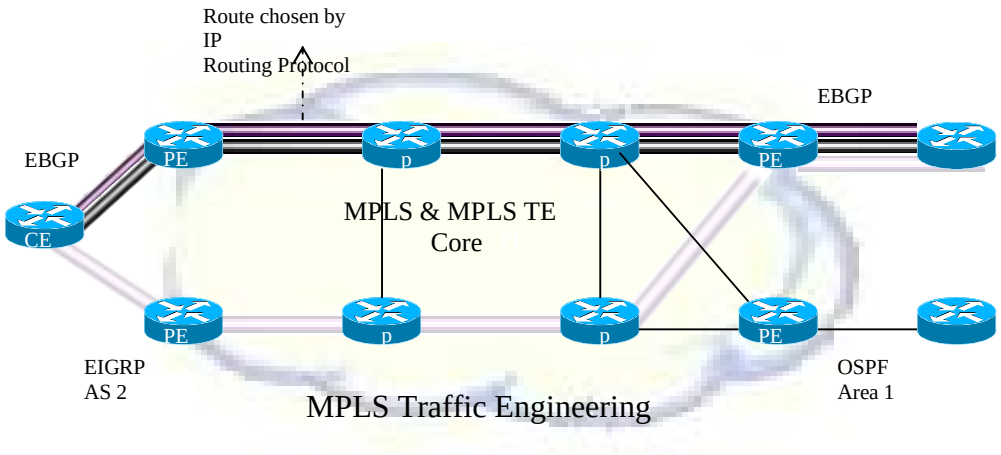
Layer 3 MPLS VPNs provide VPN IP peering between VPN devices and provider devices. Privacy is implemented using per-VPN routing tables (VRFs) that prevent different VPNs from being able to communicate.
The figure illustrates the basic characteristics of a Layer 3 MPLS VPN where any-to-any connectivity is provided to sites belonging to the same VPN. Layer 3 MPLS VPNs ensure optimal forwarding inside the MPLS backbone. In Traditional VPNs similar services can be implemented only by a full mesh of connections.
The MPLS VPN backbone uses MP BGP to propagate VPN routing information across the backbone [4][5].



Layer3 MPLS VPN

2.3 MPLS Traffic Engineering

MPLS Traffic Engineering (MPLS TE) is used to optimize resource utilization of networks with redundant links and unequal cost paths. Additionally, MPLS TE provides mechanisms for fast recovery in case of link, or path, or router failures. Traffic engineering feature with other QoS mechanisms can provide guarantees to VPNs or different traffic classes [3].



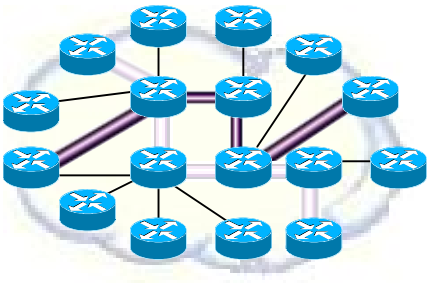
2.3.1 MPLS Traffic Engineering Application

All applications and technologies which have guaranteed bandwidth requirement, delay, or jitter levels can take benefits of MPLS TE feature by efficiently utilizing exciting resources. TE feature does not provide more bandwidth or resource, instead utilize resources efficiently especially by utilizing underused redundant paths in network. MPLS TE also aware of Diffserv and strict bandwidth guarantee and can provide specific DSCP or IP precedence to specific MPLS TE tunnels, these tunnels can also provide guaranteed bandwidth to selected traffic flow.
Both MPLS TE and QoS mechanisms should be used together throughout the core MPLS network to enable strict bandwidth, delay, and jitter levels [3].

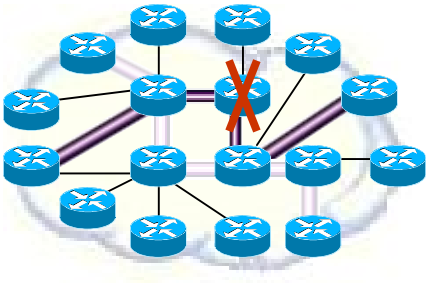
2.4 MPLS Services

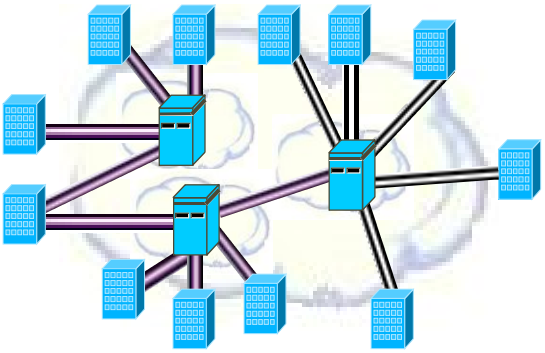
The figure illustrates various services that can be deployed individually or in a combination in MPLS Environment. Single infrastructure can be used for providing Internet access, Layer 2 MPLS VPNs, and Layer 3 MPLS VPNs; in combination with QoS guarantees and optimize resource utilization inside the backbone.

Traffic Optimization

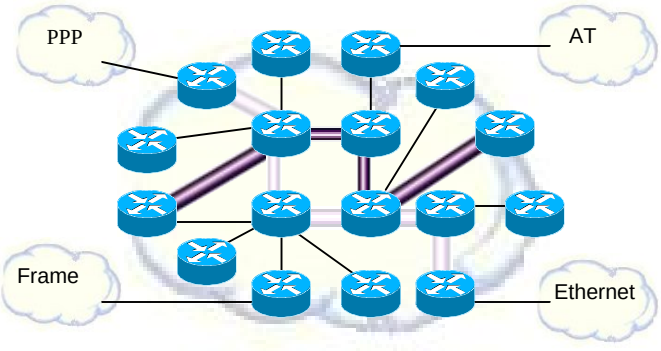


Resilience



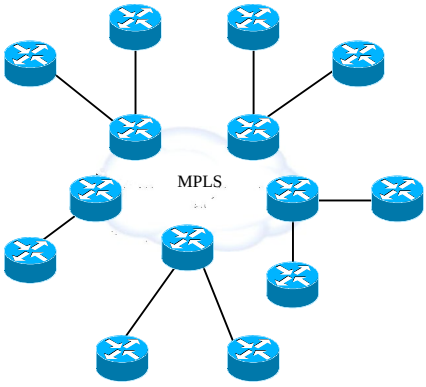


Layer 3 MPLS VPN

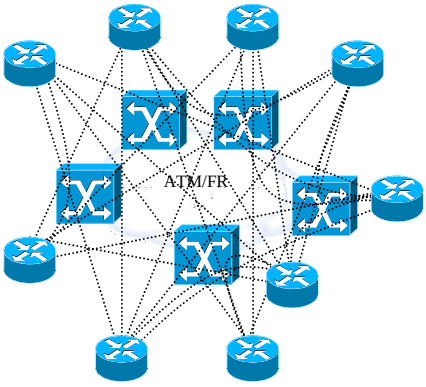


Single Converged Network

Layer-3 MPLS VPNs provide much more scalability in operation (forwarding of packets across optimal paths) and manageability (adding, relocating or removing customer sites) in comparison to traditional overlay VPN technologies such as ATM or Frame Relay, as MPLS rely on routing protocols and TDP/LDP to generate a full mesh of LSPs, instead in an overlay VPN scenario (as shown in the figure above) would require the provisioning of a full mesh of PVCs to provide similar solution.



MPLS VPN Example



Overlay VPN Example

Also Layer-3 MPLS VPNs only requires configuration changes on a single provider edge router to add a new site; the routing protocols will build new LSPs. In fully meshed

overlay VPN adding a new site requires changes on all involved ATM/FR switches as well as all attached customer routers.

2.5 MPLS Benefits

2.5.1 Benefits of MPLS to Service Providers

Initially service providers found application of MPLS technology in their networks with reduced cost of operations and enhanced services. Service providers started to offer new services, like layer 3 MPLS VPNs and layer 2 MPLS VPN using ATM or Frame Relay. With Layer 3 MPLS VPN, complex VPN topologies such as overlapping VPNs, central service VPNs, extranet, and management VPNs can be implemented easily, which were more difficult in overlay VPN technologies. MPLS VPN services can be integrated with other services, such as Internet access, IPsec-based remote access, firewalled Internet access, dial-up access, and centralized management of IP services [7].

2.5.2 Benefits of MPLS to Enterprise Networks

Initially MPLS was intended for service providers, but Enterprises are also taking benefits of the evolving MPLS features.

Traditional WAN based Enterprise networks can benefit from MPLS TE feature to optimized utilization of link and the throughput of the network. Also MPLS TE and Fast ReRoute feature can improve convergence time after link failure.
Inside enterprise networks Layer 2 MPLS VPNs can be used to extend existing networks transparently, across long distance links. Inside the enterprise networks Layer 3 MPLS VPNs can segment a large flat enterprise network into smaller segments can provide easy management and also isolation provides additional security between VPNs.

If two merging companies, also merging their networks which were previously using the same private address space, Layer 3 MPLS VPNs provides the solution.

Some Enterprises such as airports which offers their network infrastructure to their customers e.g. airlines, duty free shops travel agents, and other shops, can become service providers by implementing MPLS-enabled backbone to provide networking service these customers and other departments[7].

2.5.3 Benefits to Organizations using MPLS-based services provided by service providers

The following is a list of some of the advantages of using MPLS-based services over traditional WAN-based VPNs like layer 2 overlay VPNs:

Layer 3 MPLS VPNs provide optimized any-to-any connectivity without any additional cost (i.e. no per-VC cost, no per-distance cost).

Layer 2 and Layer-3 MPLS VPNs can be augmented by IP-aware advanced QoS mechanisms.

Layer 2 VPNs (AToM) can provide identical services to traditional ATM and Frame Relay networks and also some new Layer-2 services (e.g. interworking between virtually any pair of supported layer-2 technologies [Ethernet, PPP, Frame Relay, ATM]).

Layer 3 MPLS VPNs support various simple and complex VPN topologies (intranet, extranet, centralized services, Internet access, management VPN) integration with IPsec-based VPNs.

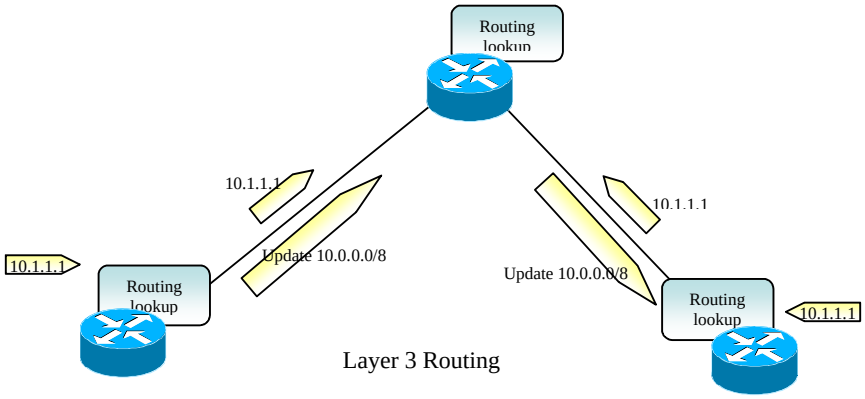
Layer 3 MPLS VPNs can reduce the cost of operation for the Enterprise network by offloading the network management to the service provider (i.e. SP can manage CE devices, address assignment through centralized DHCP, DNS, etc.) [7].

2.6 Examine MPLS and Layer 3 Routing Limitations

Before moving further first we should understand Layer 3 routing limitations, which is important to get clear understanding of MPLS basic concepts and additional services provided by MPLS. In this topic, we will describe the limitations of L3 routing; describe the difference between the data plane and the control plane in MPLS, describe the difference between frame-mode and cell-mode MPLS, describe how label headers are used in MPLS, describe the different types of label switched routers used in a MPLS network [3].

2.6.1 Layer 3 Routing Limitations

This section describes the limitations of L3 routing.



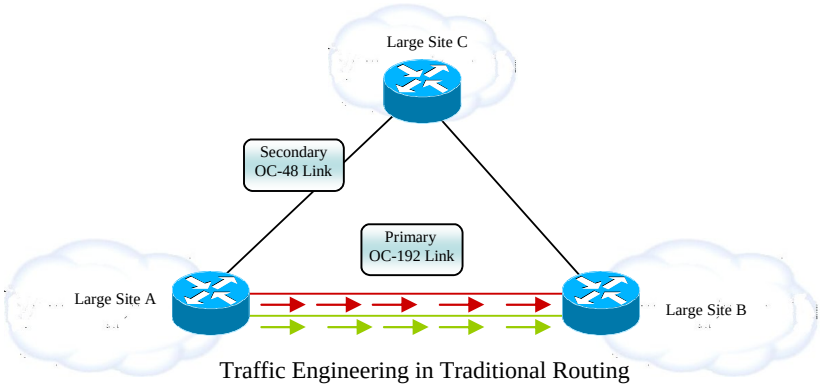
Layer 3 Routing

2.7 Traditional IP Forwarding

Traditional IP forwarding has several drawbacks, routing protocols distributes L3 routing information. Every routing protocol uses destination address for forwarding and every router performs routing lookups. Forwarding decisions are independently taken by each router in the network. This forwarding criterion can be improved by using MPLS to reduce the number of routing lookups.

In an IP over ATM network, some time L2 and L3 topologies does not match because L2 devices have static information about how to interconnect the L3 devices and suboptimal route is chosen [2].

2.7.1 Traditional IP Forwarding and Traffic Engineering

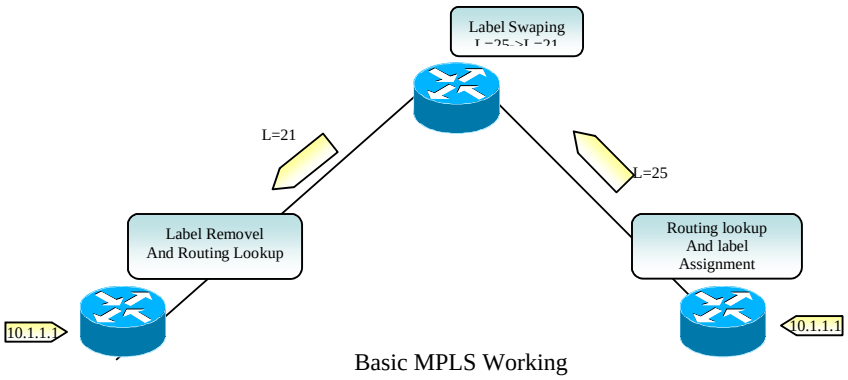


Traffic Engineering in Traditional Routing

Destination-based IP routing does not provide any mechanism for load balancing across unequal paths. In this case backup link can underutilized or unused while having over utilized primary link. All of the traffic going between sites A and B uses only the primary link because the destination network is only one hop away. Traditional IP forwarding does not have a scalable solution for utilizing the backup link. Load balancing and Policy-based routing are solutions to forward packets based on other parameters, but due to their performance limitations, these solutions are not suitable for networks with high traffic volume.

2.8 MPLS Architecture

MPLS is a forwarding mechanism which forward packets based on labels. These labels may be IP destination addresses, QoS and source address. MPLS designed support the forwarding of other protocols also. MPLS enabled routers assign labels to define paths between end points, so, only routers on the edge of the network perform a routing lookup. The routing lookup is performed by the router which first receives the packet. In figure the label 25 is given to packet. Instead of routing table lookup, core MPLS router simply looks the label and switches the packet. Then router forwards the packet by swapping the labels. On the edge of the MPLS network last router forward the packet towards its destination after removing the label.



Basic MPLS Working

MPLS is a switching method that uses labels to forward L2 and L3 traffic. MPLS router's function is divided into two major parts: the control plane and data plane. Control plane in MPLS exchanges L3 routing information and labels. By using routing protocols, such as OSPF, EIGRP, IS-IS, and BGP, L3 routing information. The label exchange mechanism simply propagates labels that are used for L3 destinations. In this example the Label Distribution protocol receives a label of 17 to be used for packets with a destination address of 10.x.x.x.

The data plane is a label-based forwarding engine; it is independent of routing protocol or label exchange protocol. It contains Label Forwarding Information Base to forward packets based on labels. Label exchange protocols used in the control plane populate the LFIB. The label generated by the Label Distribution Protocol is stored in the Label Information Base. Since the label is from a next hop router it is then populated to the Label Forwarding Information Base (LFIB) table. A local label is generated and sent to upstream neighbors. In this example, the label is 16. The data plane then forwards all packets with a label of 16 through the appropriate interfaces and replaces the label with a label of 17 [2][3].

2.8.1 Control Plane

The control plane contains a routing protocol and exchanges layer 3 routing information. It also contains label distribution protocol and exchanges labels [3].

2.8.2 Data Plane

The data plane forwards packets based on labels or destination addresses. It contains a Forwarding Information Base (FIB) that is populated by the routing protocol and a Label Forwarding Information Base (LFIB)[3].

2.9 MPLS Modes of Operation

This section describes the difference between frame-mode and cell-mode MPLS.

2.9.1 Frame-mode MPLS

MPLS is designed to use for any media and L2 encapsulation. Most of the L2 encapsulations are frame based. In frame-based MPLS, an additional 32 bits label field is inserted between the L2 and L3 headers. MPLS over ATM can use frame mode MPLS or in headers of every ATM cell labels can be inserted. In frame-mode MPLS, when the edge router receives a normal IP packet, it does a routing lookup. The forwarding table shows that a label should be attached to the packet. A label is then imposed between the L2 frame header and L3 packet header. The labeled packet is then sent out. In cell-mode MPLS, the ATM's header Virtual Path Identifier/Virtual Channel Identifier fields (VPI/VCI) are used to hold the labels for forwarding decisions. The original 32-bit label is still preserved in the frame, but not used in the label switching decision [2][3].

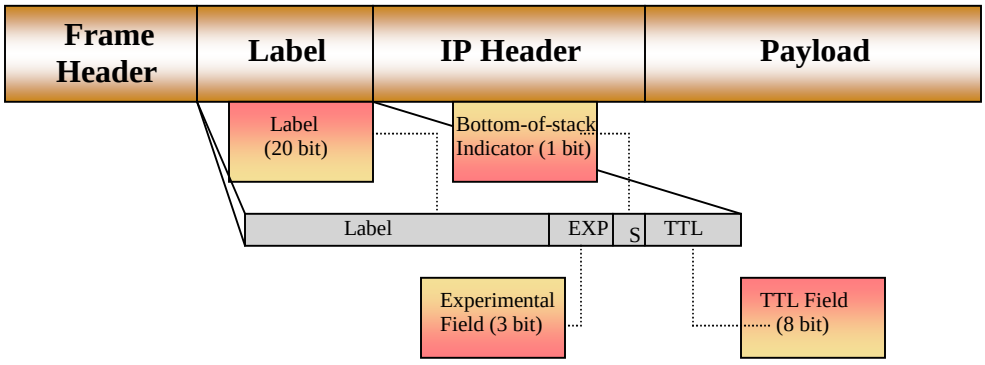
2.9.2 Cell-Mode MPLS

Cell-mode MPLS is very similar to frame-mode MPLS, the only difference is that ATM LSRs forward cells and not the packets. The ingress edge LSR lookup a forwarding table and assigns a label to the packet at the edge of the MPLS domain. This packet is then segmented into cells and each cell's VPI/VCI field is assigned the label value. The cells are then forwarded to the LSR in the center of the domain. The core ATM LSR receives the ATM cells and uses their VCI/VPI fields to forward the cells based on information in the LFIB.
The ATM LSR can handle individual cells only. The cells' VPI/VCI fields are assigned new label values and are then forwarded to their next hop destination. On the egress ATM edge LSR the cells are reassembled back into a frame. During the reassembly the label values are lost in each cell.
After removing the label and forwarding lookup the router forwards the packet out of the MPLS domain [2][3].

2.10 Label Headers

This section describes how label headers are used in MPLS.

MPLS Label Format



MPLS Label Format

MPLS label header length is 32 bits which begins with a 20-bit label that is only locally significant and usually changes on every hop. After the label field header has 3-bit long experimental field is used to define a class of service which is similar to the IP precedence field of the encapsulated IP packet. Some routers automatically copy the IP precedence value to this field during label imposition, and copy back from this field to the IP precedence during label disposition. However, this behavior can be changed to meet QoS policy needs. After experimental bits a 1-bit is for bottom-of-stack indicator is used to determine whether the label is the last label before the IP header because MPLS allows multiple labels can be imposed on a single packet by every router in a path. If the

current label is the last label this bit is set to 1. Last 8-bits of MPLS label are TTL field, which decrements at every hop to prevent indefinite loop [2][3].

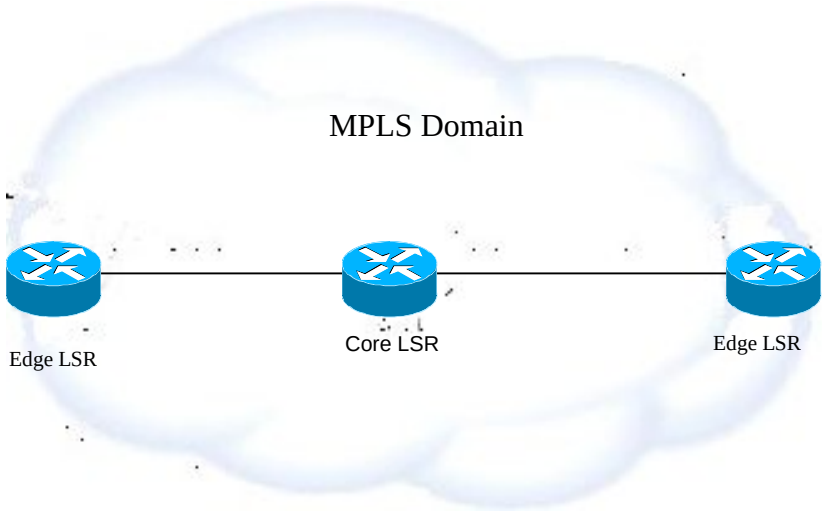
2.11 Label Switched Router Types

This section describes the different types of label switched routers used in a MPLS network.

2.11.1 Label Switched Routers

In MPL networks two types of label switched routers are defined; LSRs and Edge LSRs. On the edge of the MPLS domain, Edge LSRs impose labels to simple IP Packet and forward labeled packet into the MPLS core network. And before sending the packet outside the MPLS domain these LSRs dispose the label and send IP packet towards the destination network. In ATM networks where Cell-Mode MPLS is used, ATM LSRs provide the similar functionality. ATM edge LSRs also segment packets into cells and assign labels to the ATM cell header or, they reassemble ATM cells back into packets. LSRs exist inside the MPLS domain. An LSR will primarily forward labeled packets by swapping a label. LSRs and edge LSRs, both are capable of label switching and IP routing. All interfaces of LSRs should be enabled for MPLS, but for edge LSRs all interfaces are not necessarily enabled for MPLS. ATM switches running an IP routing protocol and MPLS, can forward cells based on MPLS labels are ATM LSRs [2].

2.11.2 Edge LSR



Edge LSR in MPLS Domain

The main function of Edge LSRs is, label imposition of IP packets and forward labeled packet into an MPLS domain, and label deposition from packets and forward IP packets out of an MPLS domain. ATM edge LSRs also segment packets into cells.

2.11.3 LSR

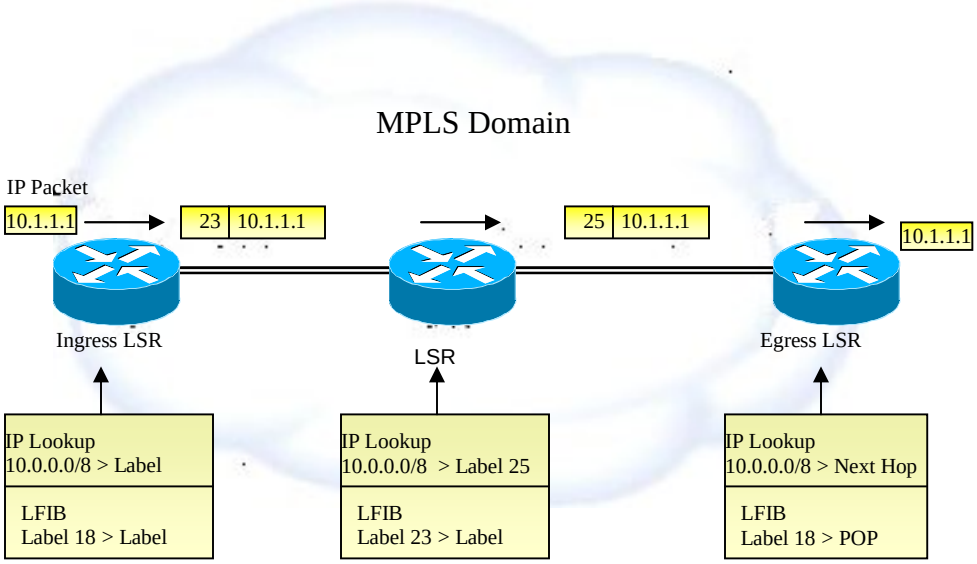
LSRs are in the core MPLS network; perform label swapping to forward packets or cells.

The Process of MPLS Forwarding

This section describes the basic concepts of MPLS and explains L3 IP routing limitations.

2.12 MPLS Forwarding

MPLS forwarding is based on exchanged labels. An MPLS-enabled router can insert, swap, or remove a label. In this example, on the edge of the MPLS domain, the ingress edge LSR performs a routing table lookup and assigns a label of 23 to the packet. The packet is then forwarded to the LSR in the core of the domain. The middle LSR router accepts the packet with a label of 23 and swaps the label based on the contents of the label forwarding table. It has the capability to perform a routing table lookup, but it does not have to. The packet is sent on with a new label of 25. The egress router removes the label and does a forwarding table lookup to forward the packet out of the MPLS domain [2].



2.13 Summary

MPLS services deployed in the enterprise WAN can make the enterprise network more efficient in terms of traffic forwarding, costs, scalability, and operations. These services can be either out-sourced to a service provider or deployed in-house. Whichever model is used to deploy MPLS, the advantages are many and empower the enterprise network to dynamically respond to a quickly changing environment. Distributed applications demand more flexible topologies and efficient forwarding, while the abundance of acquisitions and company merges calls for an efficient way of integrating dissimilar networks. All this needs to be achieved in a network that allows the enterprise to minimize operational expenses while maximizing scalability efficiency.

The deployment of MPLS services, such as L3 VPNs and Traffic Engineering, in the enterprise

WAN can provide effective solutions for the highly demanding requirements of current enterprise networks.

CHAPTER 3
MPLS Base VPN Architecture

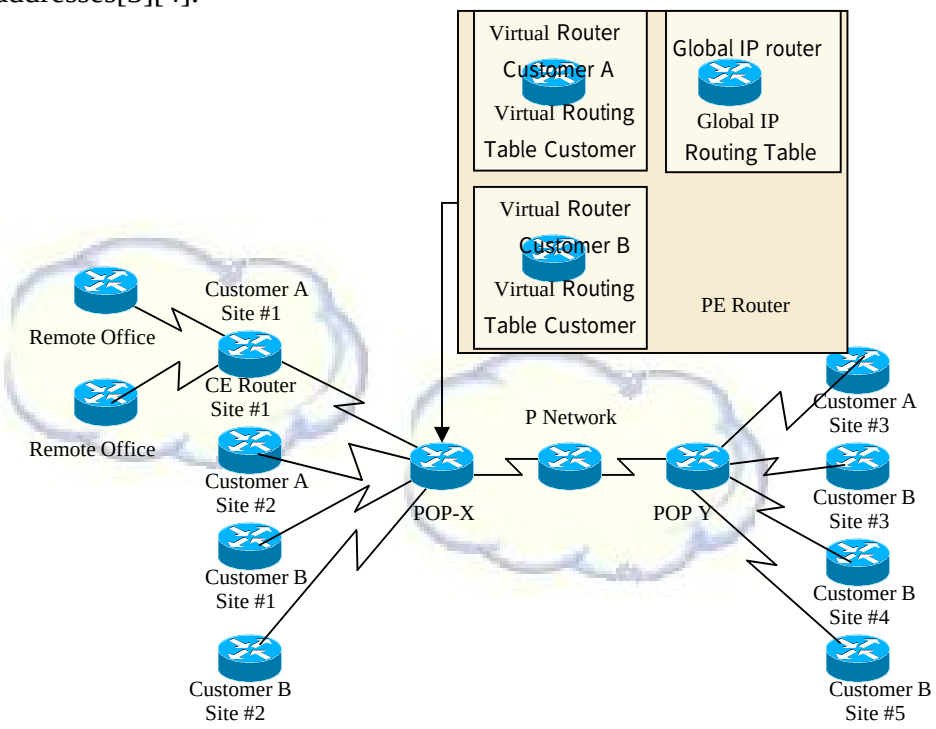
3.1 Overview

In This chapter we will the MPLS VPN architecture and components. We will also study the routing in MPLS VPN design and implementation. Also we describe the MPLS VPN packet forwarding mechanism.

3.2 MPLS VPN Architecture and Components

3.2.1 MPLS VPNs

MPLS VPNs provide a peer-to-peer VPN architecture that combines the best features of both the overlay and peer-to-peer implementations. In the MPLS VPN architecture, PE routers participate in customer routing, guaranteeing optimum routing between customer sites, maintain the routes for each customer in a separate virtual routing context, resulting in complete isolation between different customers, so that they can use overlapping addresses[3][4].



MPLS VPN Architecture Components

3.2.2 MPLS VPN Architecture

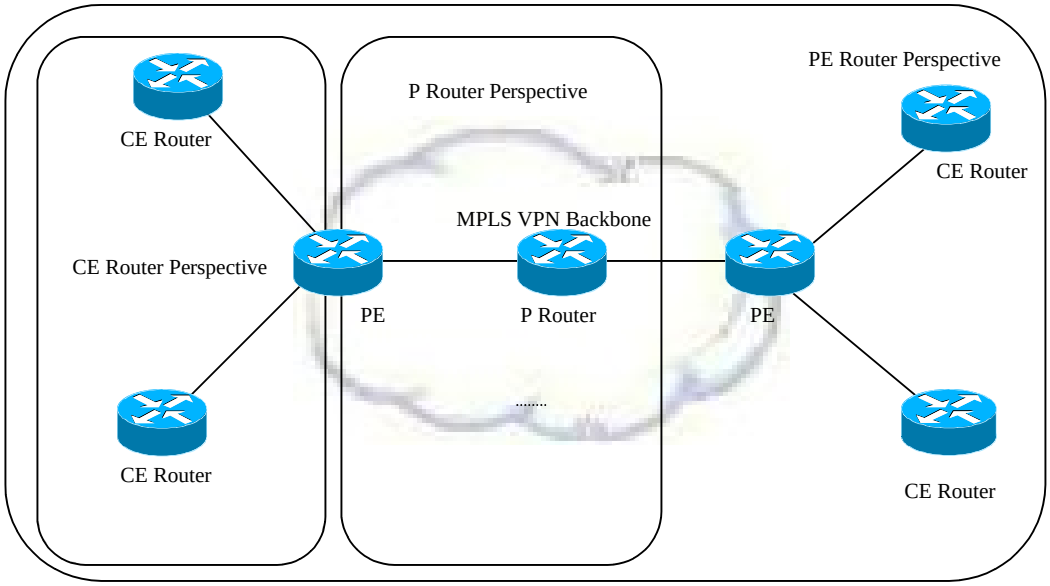
In MPLS VPN PE router architecture is similar to point-of-presence (POP) in the peer to peer model. The only difference is that in MPLS VPN single device provide the whole

architecture. As shown in above figure virtual routers are created assigning independent routing table to each customer and these virtual routers act as a dedicated PE routers in peer-to-peer model, Global IP routing tables are used to perform routing across the provider network. In traditional peer-to-peer architecture intra POP P router used as Global IP router do the same function [3][4].

3.3 MPLS VPN Routing Model

CE routers have standard IP routing software instead of MPLS VPN aware software in MPLS VPN implementation. Provider (P) routers are unaware of VPN routes and provide only label switching between provider edge PE routers. It's the PE routers which not only support traditional Internet but also support MPLS VPN services. In CE routers perspective MPLS VPN backbone is just a standard corporate backbone. So CE exchange routing updates with PE, which is a normal customer's routers to them. Provider edge router redistributes routes between VPN and individual sites. Standard BGP backbone design rules can be implemented in the customer's network. MPLS network service provider's backbone topology is transparent to the customer because the P router is hidden to the customer.

P routers only run the IGP with other P routers and with PE routers, and they exchange information about core subnets, and doesn't carry VPN routes [4][5].

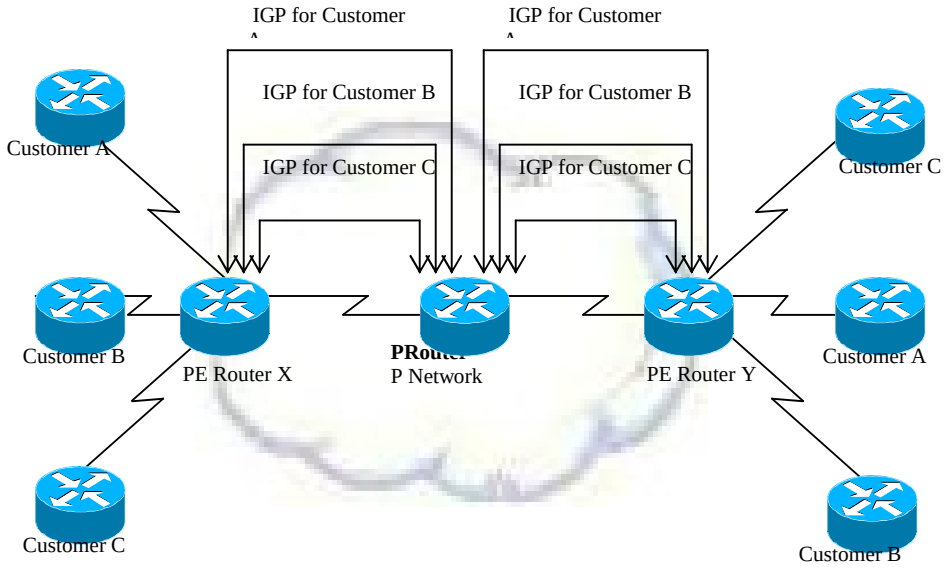


MPLS VPN Routing Paradigm

It isn't necessary to run BGP on P router for MPLS operation but to provide Internet connectivity that is not migrated to MPLS. The provider edge routers see all routing aspects of MPLS VPN in the MPLS VPN architecture. PE exchange IPv4 VPN routes via various routing protocols with the CE. PE also exchanges VPNv4 (customer) routes via VPNv4 enabled internal Multi Protocol BGP (MP BGP) sessions with other PE routers. PE also with other PE and with P routers exchange core routes through core IGP.

3.4 Propagation of Routing Information across the P-Network

Although virtual routing tables isolates customers but there are sites attached to different PE router needs information in these routing tables. Therefore we need a routing protocol that can transport all customers' routes across the provider network without compromising address spaces independency of individual customer.

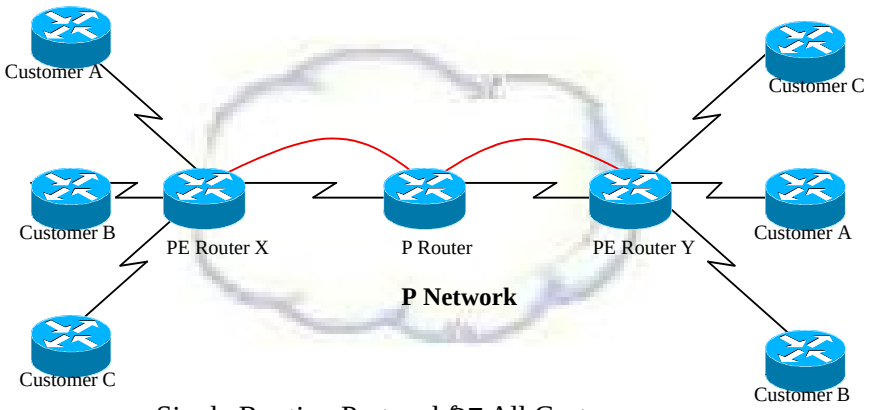


Dedicated IGP for Propagation of Routing Information

Solution to this issue is that, for each customer to use a separate routing protocol. The provider edge routers can be connected through point-to-point tunnels (and per customer routing protocol will run between PE routers) or P routers could participate in the customer routing.

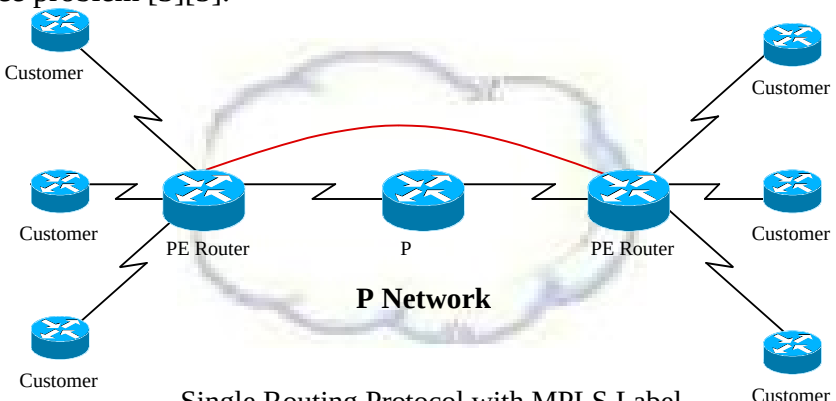
This is not a scalable solution for service provider environment because PE routers need to run a large number of routing protocols and the P routers have to carry all customer routes.

Another approach is deploy a single routing protocol for route propagation for customer routes across the provider network bus as in previous solution this solution also have some scalability problem because P routers are still involved in customer routing.



Single Routing Protocol for All Customers

Another problem in this solution is that if the customers are using overlapping address space in the routing information of all customers will be mixed in one routing protocol process.
So we need a solution for customer route propagation is to use a one routing protocol between PE routers without the involvement of the P routers to exchange all customer routes. MPLS labels forward packets between the PE routers in network. Because the number of routing protocol will not increase with the increased number of customers and provider router doesn't carry customer routes, so the scalability issue is resolved. Only well-known protocol BGP can provide required scalability due to vary large number of customer routes. But even this solution doesn't provide the solution to the overlapping address space problem [3][5].

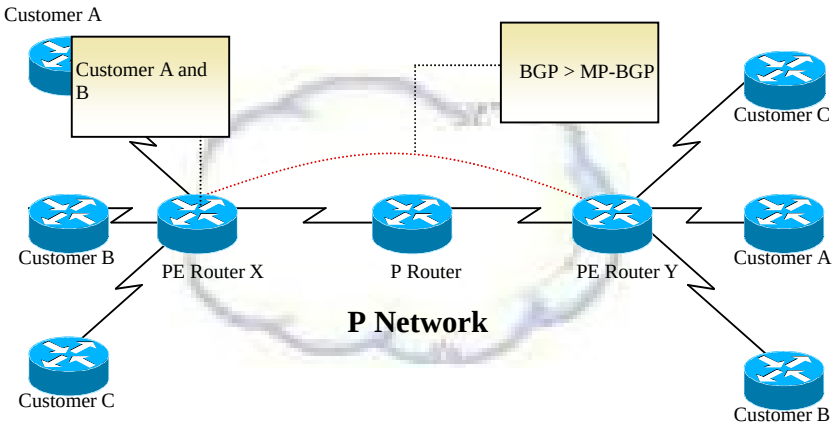


Single Routing Protocol with MPLS Label

3.5 Route Distinguisher

An important feature of MPLS VPN architecture is, support of overlapping customer address spaces, which traditional peer-to-peer VPN solution does not support.
By deploying single routing protocol for all customer routes exchange between PE routers, several identical prefixes propagated by BGP become an issue.

Solution to this problem is to expand customer IP prefix which are previously using the same subnet, by using the new prefix that will make each one unique. By adding 64-bit prefix in MPLS VPN to convert 32-bit non-unique customer addresses into 96-bit unique VPNv4 addresses. These added 64-bits are known as Route Distinguisher.
For BGP to carry the 96-bit routes need enhancement. Multi protocol BGP is the enhanced version of BGP. MP BGP treats 96-bits as a new address family of the VPNv4.
PE when exchange routes with CE routers uses the traditional IP version 4 address by prefixing route distinguisher to these routes internally converted to VPNv4 routes. MP BGP propagates these VPNv4 routes to egress PE routes [3] [5].



Multi Protocol BGP

Route distinguisher is removed before the egress PE propagates these routes to the CE.

3.5.1 MP-IBGP and MP-EBGP

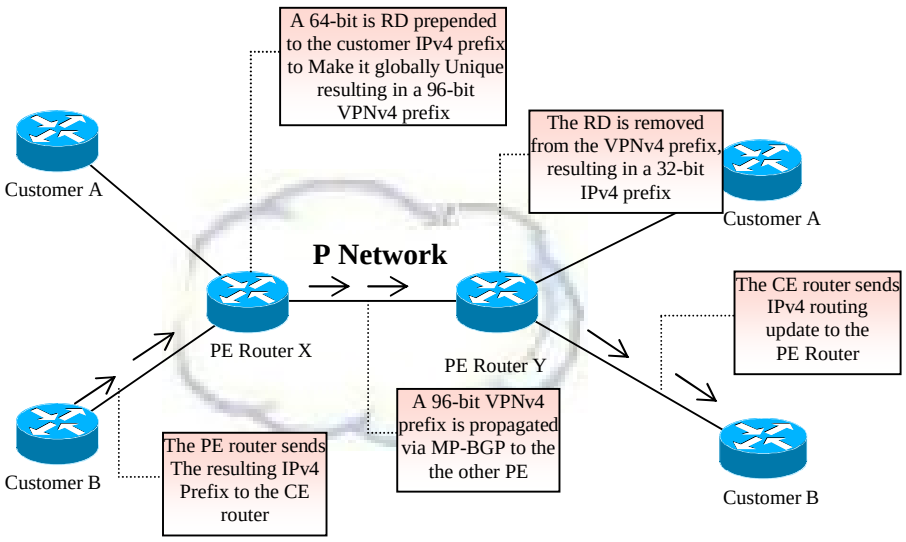
If MP BGP session is between two PE routers which are in same autonomous system it is a MP-IBGP session. Same rules of BGP attribute e.g. AS path and next hope on IBGP session applies. If VPNv4 routes exchange across the autonomous system, it will be a MP-EBGP session [4][5].

3.5.2 Route Distinguisher Number

Route distinguisher is arbitrary configurable number and users allocate numbers for selection. It just differentiates two identical IPv4 routes as two VPNv4 routes from two customers and doesn't have any technical significance.
Route distinguisher is viewed as VRF identifier because of one-to-one mapping of route distinguisher and VRF in MPLS VPN implementation.
RD can also serve as VPN identifier if there is only one route distinguisher per customer. But if customer site belongs to more then one VPN it is not implemental [7].

3.6 Route Target

Route distinguisher which is prepended to an IPv4 route is a single entity and it has no ability to show that the site belong to more then VPN.
If a router has membership in several VPNs then a set of VPN identifiers are attached to that route, so the route targets were introduce to support this requirements[4][5].



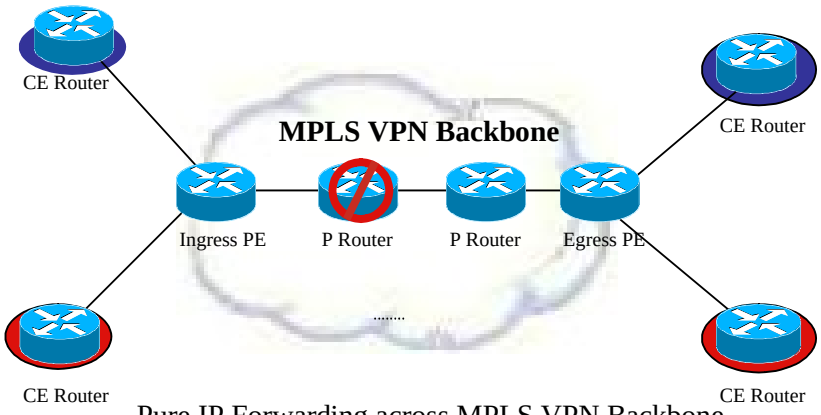
Route Distinguisher

Now complex and simple both type of topologies requires route targets to indicate membership of VPN due to MPLS VPN architecture's generic nature.
RT is extended BGP communities that are attached to a VPNv4 BGP route to indicate its VPN membership. With standard BGP communities, a set of extended communities can be attached to a single BGP route for complex VPN topologies.
A route can carry more then one route targets each shows a membership of different VPN.

Example
When PE-router converts customer routes from IPv4 routes to a VPNv4 routes it attaches the route target to this route.
The route targets attach to the route are called export Route Target and in PE router for each virtual routing table route targets are separately configured, a set of VPN
The export route targets identify a set of VPNs. A set of VPN associated with sites in the virtual routing table are identified by route targets.
When PE routers receive the VPNv4 routes, they select routes to import them into their virtual routing table by import route targets.
In PE router virtual routing table there are many import route targets are configured which identifies the VPNs from which the routes are accepted by virtual routing table.

3.7 Packet Forwarding in MPLS VPN

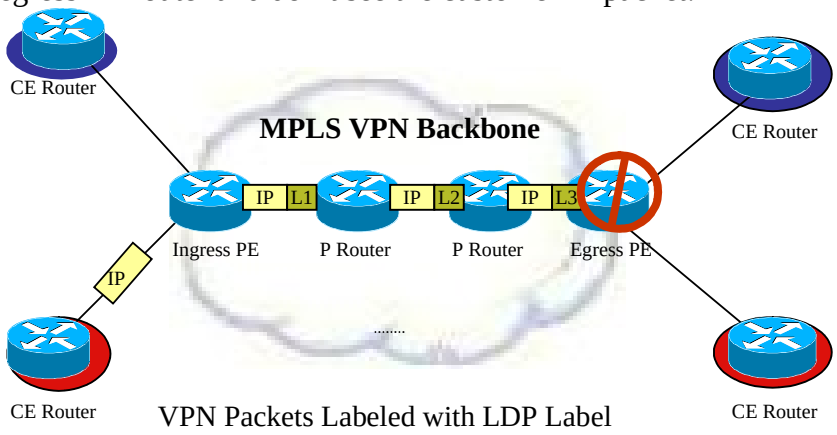
In this section we describe MPLS VPN Packet forwarding process.
Customer sends pure IP traffic and CE doesn't require to be MPLS VPN aware but run simple IP software so the traffic between CE and PE is simple IP packet. In forwarding across the MPLS VPN backbone, If PE forwards this simple IP packet to other PE, the forwarding will fail because P router is unaware of customer routes.



Pure IP Forwarding across MPLS VPN Backbone

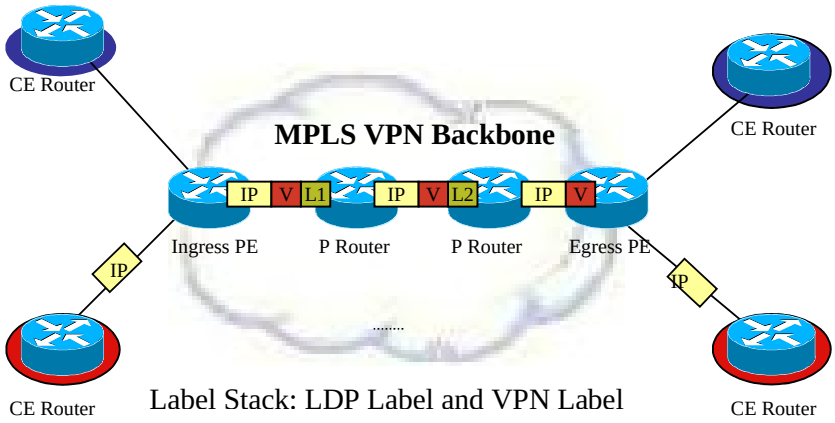
So we use MPLS label switch path (LSP) between PE router and for each LSP also define label [5].

We use Label Distribution Label Protocol for label assignment on egress PE routers in packet forwarding across MPLS backbone. Core routers see only the labeled packet towards the egress PE router and don't see the customer IP packet.



VPN Packets Labeled with LDP Label

The core routers see only the labeled packet and perform simple label switching on packets towards the egress PE routers and don't see the customer IP packet. But egress PE router doesn't perform VRF lookup on customer IP packet because it does not have any VPN information. MPLS label stack indicate what to do with VPN packet to egress router. Two labels are attached to incoming IP packet by ingress PE router in label stack. The top label in the stack guarantee the packet delivery to the egress PE router through MPLS VPN backbone and it is next hop label for PE router. Egress PE router assign a VPN label is second label in stack and provide route to incoming IP packet. Egress PE router only performs label lookup if the second label directly points an outgoing interface on VPN packet. Or the egress router first performs label lookup to find the VRF and in VRF it performs IP lookup if second label points VRF [5].



Label Stack: LDP Label and VPN Label

3.8 Penultimate Hop Popping

In frame-based MPLS networks, we can remove top label in stack one hop before the egress router. This process is called Penultimate Hop Popping. The last router in the network through LSP pops the LSP label and egress PE router receives only VPN labeled packet. Usually label lookup performed in the egress PE router on the packet for forwarding the packet to CE router. Hence full IP lookup performed only once in the ingress PE router [3].

3.9 Summary

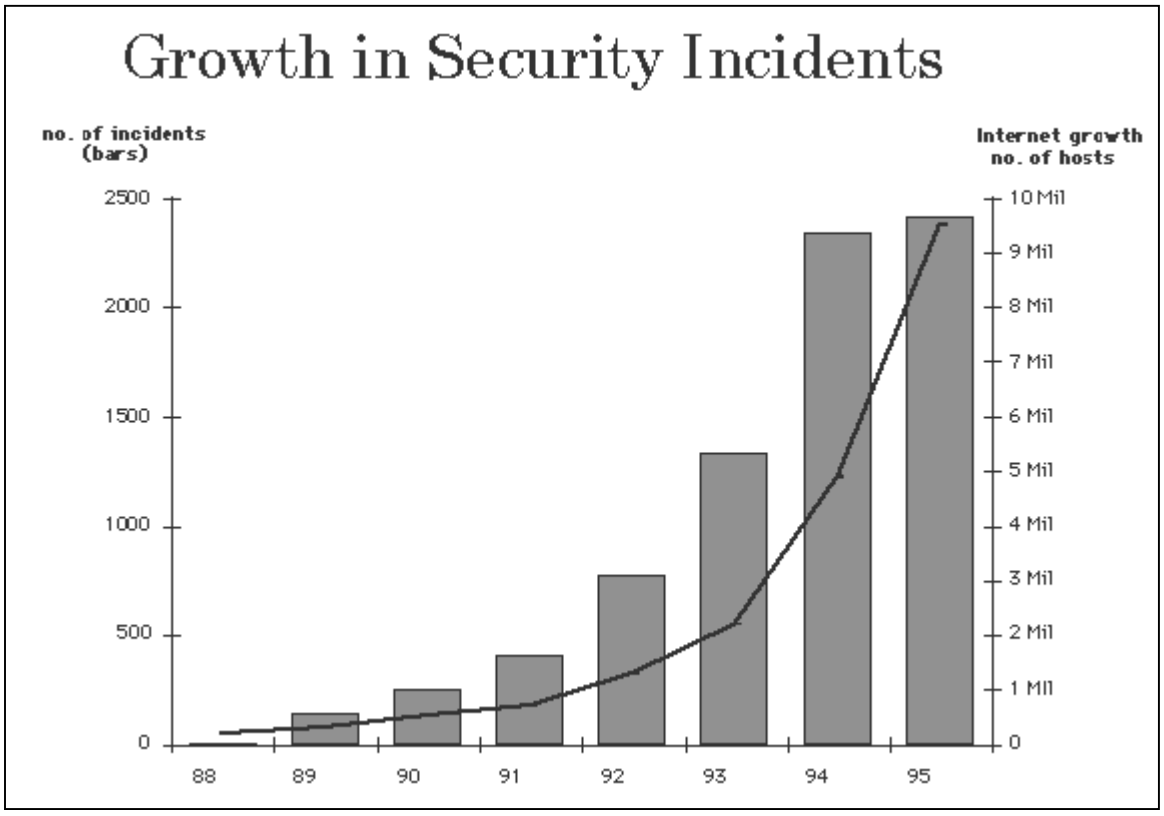
In this chapter we describe the detail architecture of MPLS VPN and also analyze the MPLS VPN design and at the end we examined the detail packet forwarding in MPLS VPN environment.

CHAPTER 4
IPsec VPN

4.1 Introduction

IPsec is protocol suit which consists, the set of IETF standards. According to report "Security in the Internet Architecture" by IAB that the Internet needs more and better security. The need, to secure end to end user traffic through authentication and encryption methods, to stop network infrastructure's unauthorized monitoring and network traffic control.

In 2003 CERT lists 137,529 reported security incidents. The number of security incidents reported to the CERT center was growing dramatically, from less than 100 in 1988 to almost 2,500 in 1995, which justifies the IAB concerns. Figure 1 [8] shows the Internet growth and the corresponding reported security incidents growth [8][14].



Security Incidents Growth [8]

The data for 1995 and partial data for 1996 show in above figure taken from cert official website, a slowing of the rate at which incidents are reported to the CERT/CC (perhaps because of sites' increased security efforts or the significant increase in other response teams formed to handle incidents). However, the rate continues to increase for serious incidents, such as root compromises, services outages, and packet sniffers.

IP spoofing, attacks are the most serious attacks in which packets with false IP addresses are created and it exploits IP based authentication. Other major attack is packet sniffing,

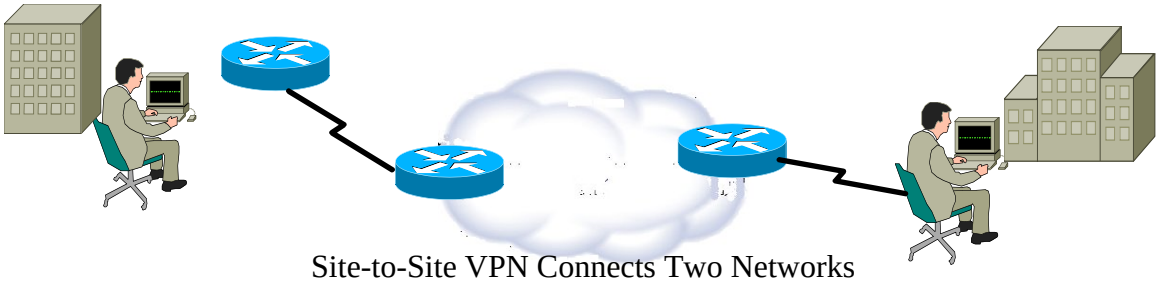
in which transmitted information such as login information for future use and data can be read by intruder.
To address these issues, authentication and encryption are mandatory security features in the IPv6 by IAB. But these security features also work with the IPv4. And now a day almost every network products have IPSec capabilities [14].

4.2 Application of IPsec

IPsec is a flexible standard that have capability to protect communication of individual systems or entire networks. VPNs can be created across the Internet and public or private networks, and the endpoints can have, direct connection, wireless connectivity and over dialup and connections. IETF standards provide interoperability with different vendors. IPsec usages include the following:

4.2.1 Secure branch office connectivity over the Internet

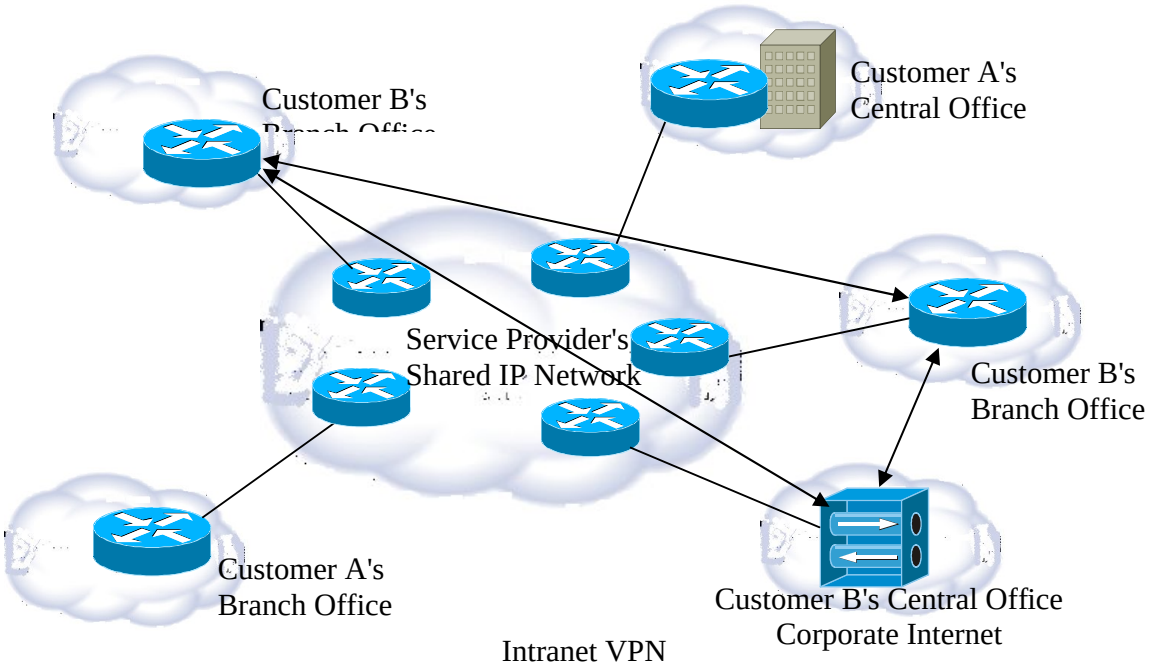
Site-to-site VPNs are between two network entities, and behind each entity is a trusted network. Remote access VPNs provide aggregation of remote users; however, there are no trusted networks at the remote locations
A company can build a secure site-to-site virtual private network over a public WAN, and behind each site there is a trusted network. Through this business heavily rely on the Internet, which minimize the cost of owning and managing a private network [7].



Site-to-Site VPN Connects Two Networks

4.2.2 Establishing Intranet VPN

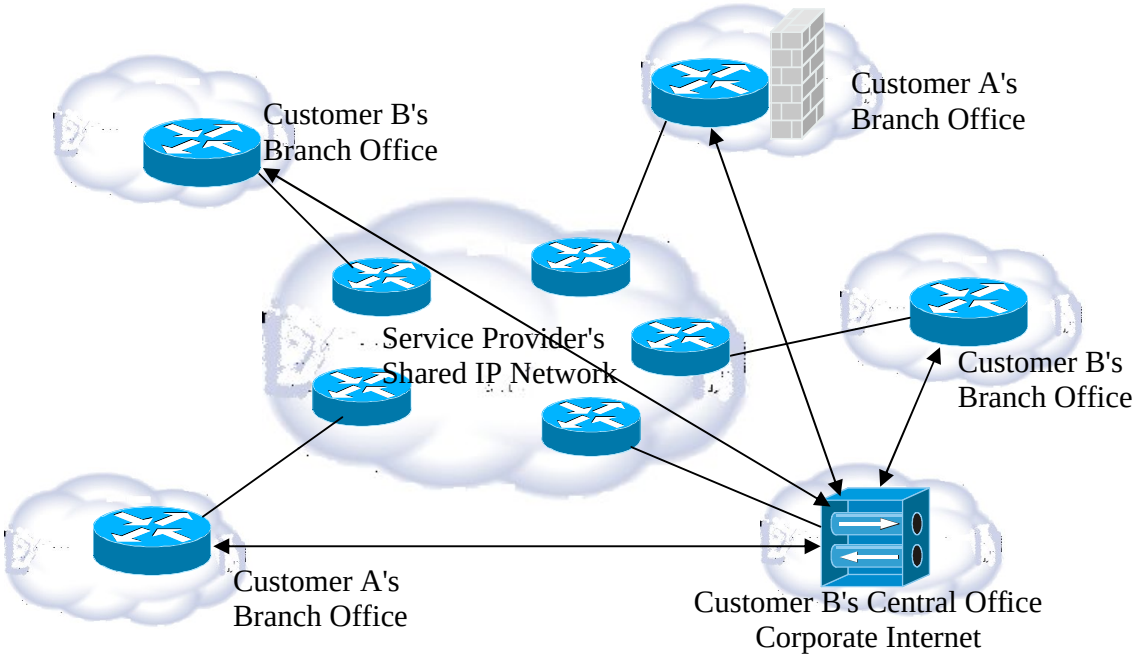
IPsec can be used to secure connectivity within organization intranet. In intranet VPNs, multiple intranets shares the same IP infrastructure (ISP); for branch to branch connectivity usually hub and spoke topology is used, full mesh or partial mesh can also be used but it have some scalability issues, remote sites connected through the corporate central site[7][14].



Intranet VPN

4.2.3 Establishing Extranet VPN

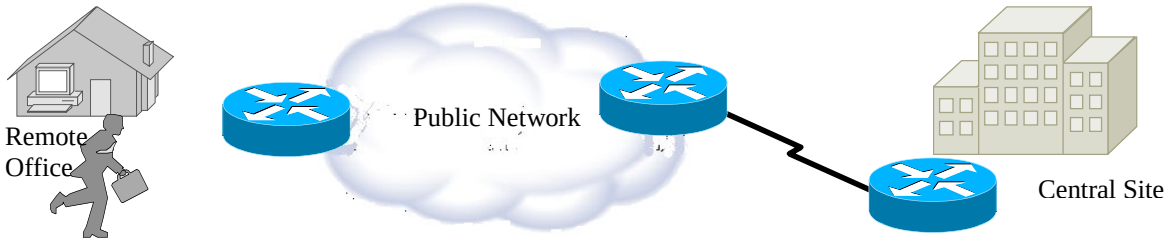
Extranet VPNs connects network of one company with the network of partners and/or suppliers. Which uses Internet for connectivity and share IP infrastructure, also through IPsec tunnels connects two or more Intranets. In extranet VPN full mesh, partial mesh or secure hub topologies can be used [14].



Extranet VPN

4.2.4 Remote access VPN

If there is no trusted network at remote location, a remote user with IPsec enabled equipment can make a local call to an ISP, to access a company network. Through this remote user access secure enterprise network with reduced toll charges [7].

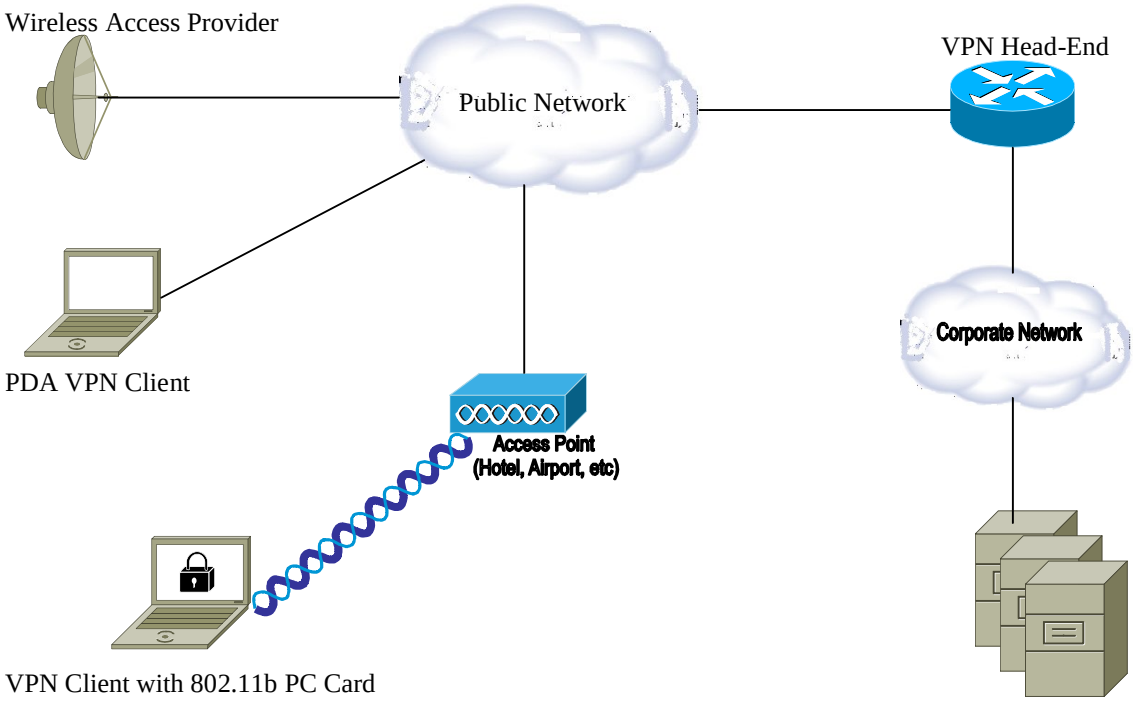


Remote Access VPN Connects Remote Users to Central Site

4.2.5 Wireless Access VPN

Many wireless connections especially hot spot such airports hotels do not implement any security especially if using public services such as hotels and airports. So the man-in-the-middle attack becomes easy in these environments than in wired connections. Even though WLAN have security mechanism but it does not provide good security and hacker with a little knowledge can break the security in few minutes and also these security protocols only secure the wireless part of networks.

So the use of IPsec not only extends the security to the wired part but also better protect the communication over the wireless link [7].



4.2.6 Teleworkers

Many organizations use IPsec to enable corporate reachability for home users, teleworkers, and small offices. An IPsec implementation should solve the following issues: clients are dynamically assigned IP addresses, and clients are protected from threats from the Internet by a personal or dedicated firewall, intrusion detection, or virus scanning. The corporate network is protected from possible incidents on clients sites by using a firewall; intrusion detection; virus scanning; split tunneling, which prevents clients from becoming gateways into the corporate networks; and strong authentication of clients, using two- or three-factor authentication [7].

4.2.7 Security Enhancement of electronic commerce:
Most of the electronic commerce and Web applications have built-in security protocols, but even then IPsec provides extra layer of security to these applications [14].

4.3 Benefits of IPsec

1 IPsec implementation in any networking device provides strong security to all traffic crossing the perimeter.

2 IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP, and the firewall is the only means of entrance from the internet into the organization.

2 If firewall is the only entrance from the internet into the network IPsec implementation in firewall provide more resistance to bypass firewall.

3 IPsec works on network layer and its transparent to user application and user applications and servers systems need not to be changed for IPsec implementation.

4 Because IPsec is transparent to end users, so users training on security mechanism are not necessary.

5 IPsec can provide security for individual users such as teleworkers or for sensitive application setting up a secure virtual sub network within an organization [9][14].

4.4 Applications in Routing

IPsec not only protects end systems and networks but it also provides protection to internetworking routing architecture.
1 IPsec feature of data origin authentication guarantees that the routing advertisement is coming from an authorized router.

2 If a router wants to make a neighbor relationship with a router in other domain with IPSec router can check that the advertisement is coming from an authorized router.

3 It also sees if the initial packet and redirect message are from same router.

4 It also checks the forged routing updates.

Without IPsec security measure, an intruder can divert or traffic to unauthorized user or disrupt communications by sending traffic to unknown destination. Routing updates of routing protocol between IPsec enabled peer provide great security to these updates [14].

4.5 Architecture of IPSec

The IPsec specifications are very complex. To get a clear understanding of architecture we will start with documents that define IPsec. Then we will move on concept of SA and service provides by IPsec [9][14].

4.5.1 Documentation

There are several documents that define IPsec specifications. The most significant since November 1998, till date are RFCs 2401 (obsoleted by 4301), 2402(obsoleted by 4302 and 4305), 2406 (obsoleted by 4303 and 4305), and 2408 (obsoleted by 4306):
These feature's support is optional for IPv4 but mandatory for IPv6. Extension header is used with main IP header in both IPv4 and IPv6 to implement these security features. For authentication the extension header is used and for encryption the Encapsulating Security Payload ESP header is used.
There are many other drafts have been published by the IETF working group of IP Security Maintenance and extensions (ipsecms) previously known as IP security Protocol working group [14].

"Architecture: Covers the general concepts, requirements, definitions and procedures for defining IPsec technology.

ESP: ESP documents contain the issues related to the data encryption and authentication and packet format for encryption and authentication option.

Authentication Header: AH documents the issues related to the use of AH data authentication and packet format.

Encryption Algorithm: A series of documents describing how various encryption algorithms are used for ESP.

Authentication Algorithm: A series of documents describing how various authentication algorithms are used for the AH and authentication option of the ESP.

Key Management System: Document specifies the manual or automated key management system.

Domain of interpretation DOI: Contains values for the other documents in connection with each other. These include identifiers for authentication and encryption algorithms and authorized operational parameters such as key management [14]".

4.6 IPsec Services

IPsec provides different security services at the Network layer. System or networks enabled with IPsec select required security protocols for the services, and use cryptographic keys to provide the requested services. Authentication Header provide authentication by attaching header to the packet and Encapsulating Security Payload provides encryption and optional authentication. IPsec provides the following services [14]:

Access Control

Confidentiality: IPSec sender encrypts the data before transmission and receiving end decrypts the data. The encryption enables the data confidentiality.

Data Integrity: IPSec sender appends the checksum to the data before transmission and receiver verify the checksum after reception for possible data alteration during transmission.

Data Origin Authentication: With data origin authentication IPSec receiver authenticate the source of data.

Table below show the services provided by the AH and ESP protocol.

	AH	**ESP(Encryption only)**	**ESP (Encryption, Authentication)**
Access Control	Yes	Yes	Yes
Connection Integrity	Yes		Yes
Data Origin Authentication	Yes		Yes
Rejection of Replayed packets	Yes	Yes	Yes
Confidentiality		Yes	Yes
Limited Traffic flow Confidentiality		Yes	Yes

Table 4.1

4.7 Security Associations

SAs are set of information shared by network equipment that defines authentication and cryptographic mechanisms of inbound and outbound traffic. Although both IPsec and IKE uses SAs, but IPSec security SAs are independent of IKE SAs and are also unidirectional, hence required tow SAs for communication for each direction [9].

One per direction per protocol SA is needed for protected data. SAs are uniquely identified by three parameters:

Destination address: Currently, as a destination address of endpoint of SA, only unicast addresses are allowed. End point can be router, firewall or any user end system.

Security protocol: Security Protocol shows that SA is an AH SA or an ESP SA.

Security parameter index (SPI): SPI is a bit string assigned to SA and have only local significance. The receiving system by the help of SPI in the AH or ESP header, selects the SA for packet processing.

SAD

Security Association Database is a database in every which defines the parameters associated with each SA. A security association is defined by these parameters [9].

SAD Data Items

The following data items MUST be in the SAD [9]:

“Security Parameter Index (SPI): SPI is a 32-bit value to uniquely identify the SA selected by the receiving end of an SA. The SPI in SAD entry is used to construct the AH or ESP header of packet. SPI also map traffic to the appropriate SA

Sequence Number Counter: It is a 64-bit counter used to generate the Sequence Number field in AH or ESP headers. We can also use 32-bit numbers if negotiated but default is 64-bit sequence numbers.

Sequence Number Counter: It is a flag which specifies the generation of auditable event and stops transmitting more packets or restarts the counter upon sequence number counter overflow.

Anti-Replay Window: a 64-bit counter and a bit-map (or equivalent) used to determine whether an inbound AH or ESP packet is a replay. If anti-replay has been disabled by the receiver for an SA then the Anti-Replay Window is ignored for that SA.

AH Information: AH information defines AH authentication algorithm, keys for negotiation and keys lifetime etc.

ESP Information: ESP Encryption algorithm, integrity algorithm key, mode, Initialization Vector, etc.

Lifetime of SA: SA must be replaced or terminated after a specific time interval. Time or byte count can be used as lifetime simultaneously, and which ever expire first will take precedence.

IPsec protocol mode: Indicates weather traffic on this SA is in tunnel mode or transport mode of AH or ESP.

Stateful fragment checking flag: Indicates whether or not state full fragment checking applies to this SA".

Path MTU: It is an observed path MTU on link.

Tunnel header IP source and destination address: Source and destination addresses of tunnel must be either IPv4 addresses or IPv6 addresses.

SA Selectors:

IPsec provides the considerable flexibility in implementing IPsec services to traffic. Different SAs can be combined to get desired protection. IPsec allows differentiating traffic which need protection and traffic which can by pass IPsec protection mechanism. Protected traffic is related to specific SAs in the Security Policy Database (SPD). SPD contains entries that define IP traffic and related SA.
Each SPD entry by a set of IP and upper layer protocol field values. These values are called SA selectors. Usage of selectors determines by the context of IPsec implementation [9][14].

SPD entry is determined by the following Selectors [9]:

Remote IP Address (IPv4 or IPv6): This is a single IP address, or a list of addresses, or a range of addresses, or a list of ranges. If more than one remote system sharing the same SA, the address ranges are used e.g., behind a security gateway.

Local IP Address (IPv4 or IPv6): This is a single IP address, or a list of addresses, or a range of addresses, or a list of ranges. If more than one source system sharing the same SA, the address ranges are used e.g., behind a security gateway.

User ID: If the IPsec is running on same operating system as user then this field is used and is not in IP or upper layer header.
Data Sensitivity Level: Used for systems providing information security level as secret or classified.

Next Layer Protocol: This is a protocol specific number of next layer protocol in the IPv4 "Protocol" field and in the IPv6 "Next Header" field.

IPsec Protocol (AH or ESP or AH/ESP): It can be obtained from the IPv4 protocol or IPv6 header field.

IPv4 Type of Service (TOS): This is a specific IPv4 TOS value and is obtained from IPv4 header.

IPv6 Class: This is an IPv6 class or wildcard value and is obtained from IPv6 header.

4.8 Transport and Tunnel Modes

IPsec has two modes of operations: transport and tunnel mode. The operation of these modes can be best understood in the context of AH and ESP description.

4.8.1 Transport mode

IPsec transport mode provides protection to only the IP payload, and the original IP headers remain the same. Only few bytes are added to each packet in this mode

Devices on the public network can see the final source and destination of the packet, which allows enabling special processing, for example, quality of service (QoS) on the intermediate network based on the information in the IP header. Because the Layer 4 header is encrypted, the examination of the packet is limited. For end-to-end communication between client and server or between two workstations transport mode is used [9].

4.8.2 Tunnel Mode

IPsec Tunnel mode provides the protection to the entire original IP datagram, so entire packet becomes the payload in a new IP packet. When IPSec enabled one or both ends of a security association are security gateways such as router or firewall, tunnel mode is used. The source gateway forward the encrypted data through the IPsec tunnel, and the destination gateway decrypts the data and forwards original data to the destination system.

When one or both ends of a security association are security gateways such as router or firewall, tunnel mode is used.
IPsec tunnel mode is most used mode in IPsec deployment. Tunnel mode implementations can be achieved without the modification of the operating system, or any applications on PCs, servers, and hosts [9].

4.9 Authentication Header

The Authentication Header provides data integrity and the data or user authentication. The data integrity ensures that modification of a packet is not possible during transmission. The authentication ensures that the user or application are authentic and filter traffic accordingly; it also prevents the address spoofing attacks. Reply attacks can also be prevented by the AH, but it does not provide confidentiality.
Authentication uses of a message authentication code (MAC), hence the two parties must share a secret key [10].

AH

Next Header	Payload Length	Reserved
Security Parameter Index(SPI)		
Sequence Number		
Authentication Data (Variable length)		

AH consists of the following fields [10][14]:

“Next Header (8 bits): Identified the type of header immediately following this header.

Payload Length (8 bits): Length of Authentication Header in 32-bit words, minus 2.

Reserved (16 bits): This field is for future use.

Security Parameter Index (32 bits): Is used for security association identification.

Sequence Number (32 bits): It is a monotonically increasing counter value.

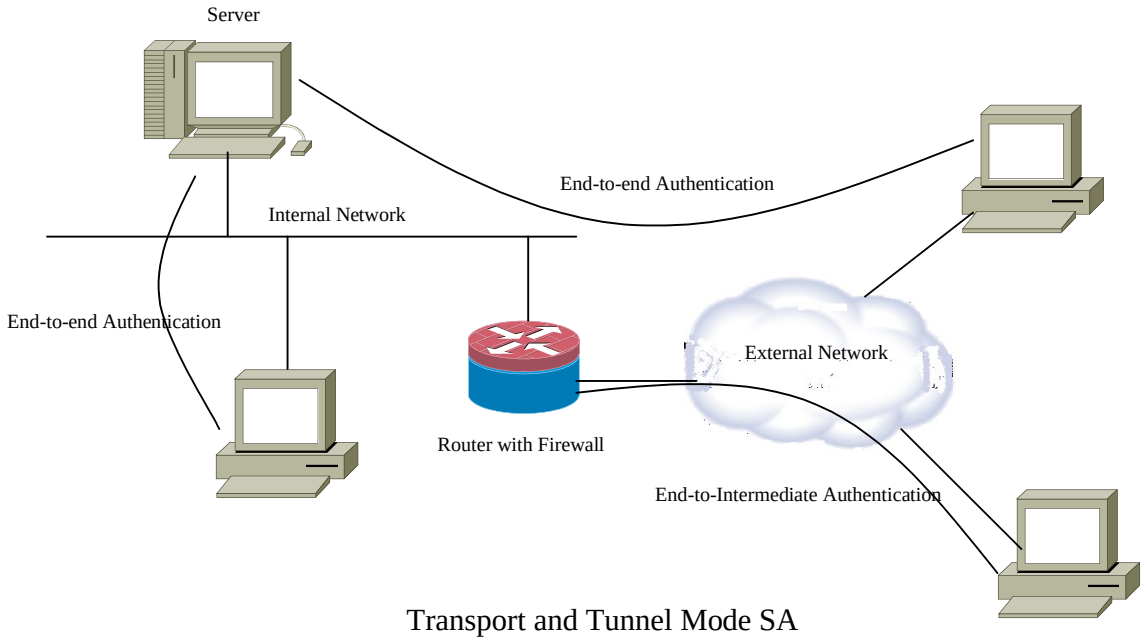
Authentication Data (variable): A variable-length field (must be an integral number of 32-bits words) that contains the Integrity Check Value (ICV), or MAC, for this packet” [10].

Anti-Reply Service

Replay attack is attack in which a hacker sniffs the packet containing username or password and retransmits it to the destination to get into the destination system as a legitimate user for further escalation. The sequence number field of header thwarts this attack. When first packet sent, the sender initializes a sequence number counter to 0, every time the packet sent from this sender for same SA the sequence number field increments. The first usable value is 1. If anti reply is enabled the sender don’t allow the sequence number cycle past 2*32-1 back to zero so prevent the multiple packets with same sequence number. When this limit reaches the sender terminates the current SA and negotiates the new SA [10].

4.9.1 Transport and tunnel Modes in AH

Figure shows the two scenarios to implement the IPsec authentication service. In scenario one, server and client workstation are using authentication services for secure transmission. Authentication services can be used between both server and client workstations on same network or on different networks. The authentication process is secure, as the workstation and the server share a protected secret key. This is a transport mode SA scenario. If a remote workstation authenticates itself to the corporate firewall, for access to the entire internal network or a server that may be don't support the authentication feature, is a tunnel mode SA scenario [10][14].



Transport and Tunnel Mode SA

AH Transport mode

In Transport mode AH in IPv4, the AH is inserted after the original IP header and before the IP payload; this is shown in the figure. Entire packet is authenticated, except the mutable fields in the IPv4 header that are set to zero for MAC calculation.

AH is viewed as an end-to-end payload in IPv6; and is not examined or processed by intermediate routers. In IPv6 AH comes after the IPv6 base header and Extension headers. Then, entire packet except the mutable fields is authenticated [10][14].

IP Header	Payload

Original IPv4 Packet

IP Header	AH	Payload

IPv4 AH Transport Mode

IP Header	Extension Header	Payload

Original IPv6 Packet

IP Header	Extension header	AH	Destination	payload

IPv6 AH Transport Mode

AH Tunnel mode

For tunnel mode AH, the AH is inserted between the original IP header and a new outer IP header, and the entire original IP packet is authenticated, (Figure). The inner IP header contains the final source and destination addresses, while an outer IP header may contain different IP address (e.g., address of firewalls or other security gateways).

In tunnel mode, the entire inner IP packet, including the entire internal IP header, is protected by AH. The outer IP header and the outer IP extension header (IPv6) are authenticated except for mutable fields [10][14].

New IP Header	AH	Original IP Header	Payload

IPv4 Tunnel Mode

New IP Header	Extension Header	AH	Original IP Header	Extension Header	Payload

IPv6 Tunnel Mode

4.10 Encapsulating Security Payload

ESP main function is to provide confidentiality service by encrypting the data, but ESP can also provide authentication [11][14].

ESP Format

Figure shows the packet format of an ESP. ESP packet contains the following fields:

“Security Parameters Index: SPI is 32 bits value to identify SA.

Sequence Number: Sequence number is 32 bits counter value that provides an anti-replay function.

Payload Data (variable): This is a transport layer segment in transport mode or IP packet in tunnel mode that is protected by encryption.

Padding (0-250 bytes):
There are many purposes for padding field.

In block cipher encryption algorithm requires the plaintext must be a multiple of some number of bytes, the Padding field expands the plain text to the required length. The Pad Length and Next Header field must be in 32-bit blocks. To conceal the actual length of payload can be achieved by padding.

Pad Length (8 bits): This field specifies the number of pad bytes prior to this field.

Next Header (8 bits): This defines the first header in the payload e.g., transport layer protocol such as TCP or an extension header in IPv6.

Authentication data (variable): It is a variable-length field that contains the Integrity Check Value computed for ESP packet without the Authentication Data field. This field must be an integral number of 32 bit words)".

Encryption and Authentication Algorithms

ESP encrypts the Payload, Padding, Pad Length, and Next Header fields. If the algorithm used to encrypt the payload requires cryptographic synchronization data, such as an Initialization vector (IV), then these data may be carried explicitly at the beginning of the Payload Data field. Although an IV is considered as part of cipher text but it is usually not encrypted.
The current specification dictates that compliant implementation must support DES in cipher block chaining (CBC) mode. Other algorithms which can be used for encryption are these

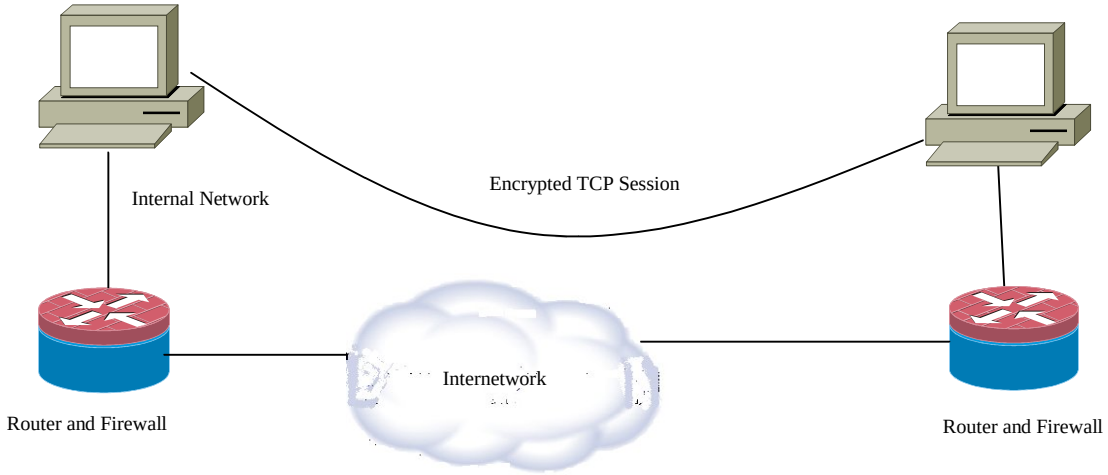
Three Key triple DES
RC5
IDEA
Three key triple IDEA
CAST
Blowfish

ESP supports the use of MAC with a default length of 96 bits. Also ESP implementation must support HAMC-MD5-96 and HAMC-SHA-1-96 [12][14].

4.10.1 Transport and Tunnel Modes in ESP

IPsec ESP services can be used, as show in figure. In the figure A, ESP transport mode encryption and optionally authentication are provided directly between two hosts. In Figure b tunnel mode ESP services are used to set up a virtual private network. A

company has four private networks interconnected through the Internet. Internal network hosts transport the data through Internet but do not interact with other hosts on the Internet. In this configuration hosts does not need to implement security and the secure tunnels are terminated on the security gateway to each internal network [11][14].



ESP in Transport Mode

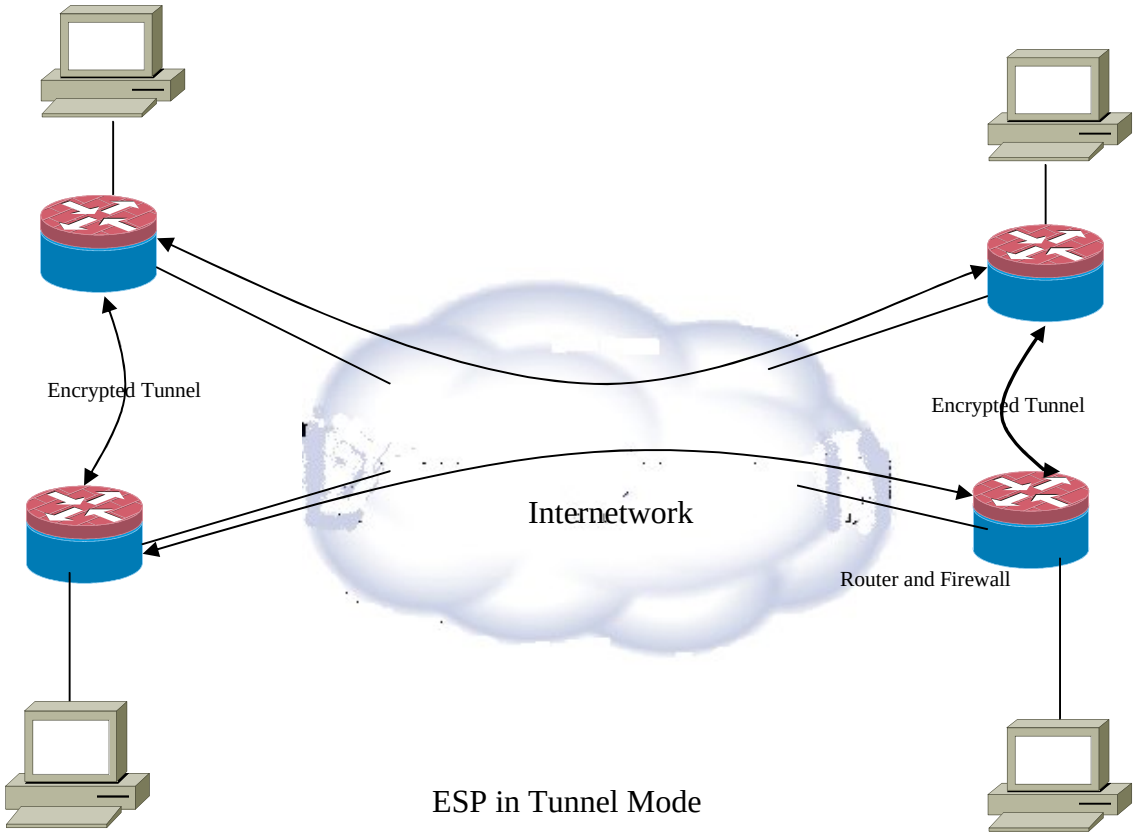
Transport Mode ESP

As shown in figure Transport mode ESP encrypts and optionally authenticate the data portion of IP packet e.g. TCP segment. The ESP header is inserted into the IP packet immediately after the original IP header and before the transport layer header (e.g. TCP, UDP, and ICMP) and an ESP trailer and if authentication is selected, the ESP Authentication Data field is added after the data field. The transport layer segment and the ESP trailer are encrypted. And entire cipher text plus the ESP header are authenticated.

ESP is an end-to-end payload in IPv6; and examined or processed by intermediate routers. Therefore, the ESP header comes after the IPv6 base header and other extension headers. And the entire transport layer segment and the ESP trailer are encrypted. Entire cipher text plus the ESP header is authenticated.

Transport mode operation provides confidentiality for any application that uses it, thus avoids the need to implement confidentiality in every individual application. Because fewer bits are which saves bandwidth so this mode is efficient, but traffic analysis on the transmitted packets can reveal the source and destination address in original IP packet [11].

Tunnel Mode ESP



ESP in Tunnel Mode

Tunnel mode ESP encrypts an entire IP packet (figure). In this mode the ESP header is prefixed to the original IP packet and then the packet and the ESP trailer is encrypted. A new IP header is added before the ESP header for routing on intermediate systems but it can reveal the original IP source and destination address. However, the tunnel mode can only work in configurations which includes security gateway such as firewall or router. This reduces the host configuration and key distribution tasks [11][14].

4.11 Combining Security Association

A single SA can only AH or ESP protocol. Sometime we need both AH and ESP for specific flow. Also some traffic flows require different IPSec services between hosts, security gateways or firewalls. To achieve the required security service we need to implement number of SAs. These combined security associations are called security association bundle. End points for these bundles can be same or different equipment [14].

We can combine security association in two ways.

4.11.1 Transport adjacency

In this, we apply more then one SA to same IP packet, without tunneling. In this method, processing is performed on only one IPSec instance of the final destination, because only one level of combination is allowed and there is now added benefit of further nesting [14].

4.11.2 Iterated Tunneling

In this method we apply multiple layers of security protocols through IP tunneling. Each tunnel can have different originating end, and terminating end along the path because of multiple level of nesting.
Transport adjacency and iterated tunneling can be combined e.g. we apply tunnel SA between security gateways and transport SA between hosts behind these SAs.

The main consideration of applying SA bundles is the order of authentication and encryption processing [14].

Authentication and Confidentiality
We have several approaches for combining encryption and authentication mechanisms for transmitting IP packets with confidentiality and authentication.

ESP with Authentication Option
As shown in figure, first ESP is applied the user data for confidentiality and the authentication field is added to that data. We can implement this approach both in transport mode ESP and tunnel mode ESP. In both cases we apply authentication mechanism to cipher text.

Transport Adjacency
Two bundled transport SAs is method of applying encryption before authentication, the inner SA will be ESP SA without its authentication option and outer SA will be AH SA.
The encryption is applied only on IP payload due to transport SA. Then encrypted packed include the IP header and ESP, and then AH is applied to that encrypted packet in transport mode. This method is advantages over ESP SA with authentication option because it also covers source and destination addresses, but has more overheads due to two SAs processing.

Transport-Tunnel Bundle

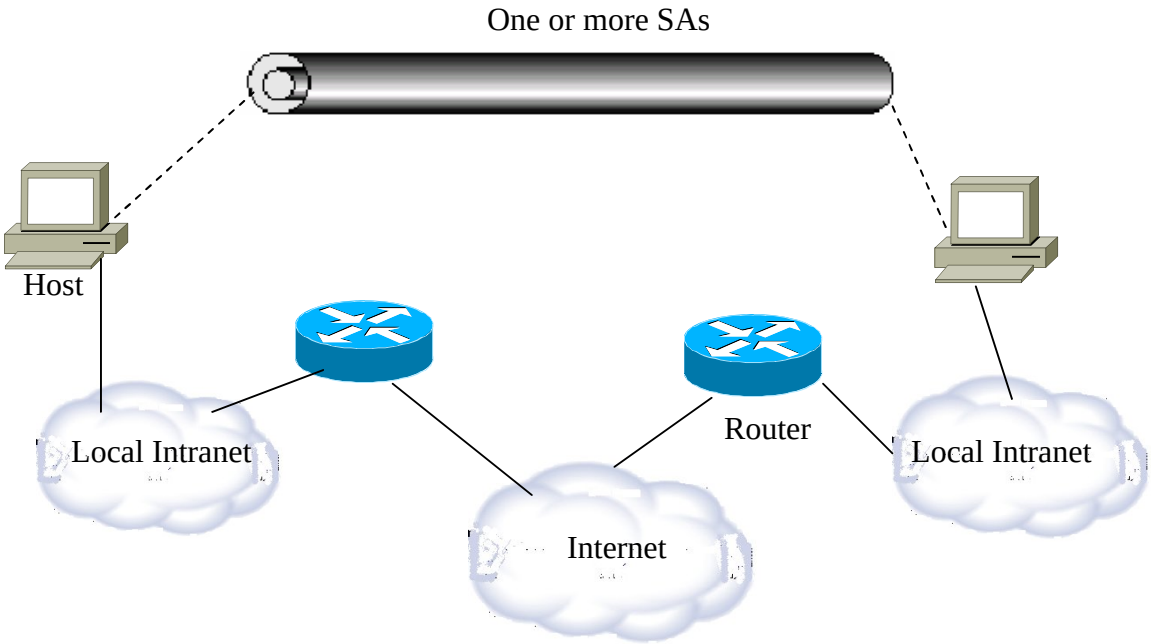
In transport tunnel bundle authentication is applied before encryption, because message alteration becomes impossible without detection due to encryption. Also if it is required to store authentication information with message for future reference this can help, otherwise encryption before authentication require to re-encrypt the message to check the validity of authentication.

To apply authentication before encryption we use two bundle SAs, inner one is transport AH SA and outer is tunnel ESP SA. So the IP payload is authenticated first and the authentic payload and IP header is encrypted by ESP in tunnel mode, hence the entire authenticated IP packet is encrypted and a new IP header is attached to the packet [14].

4.12 Security Association's Combinations

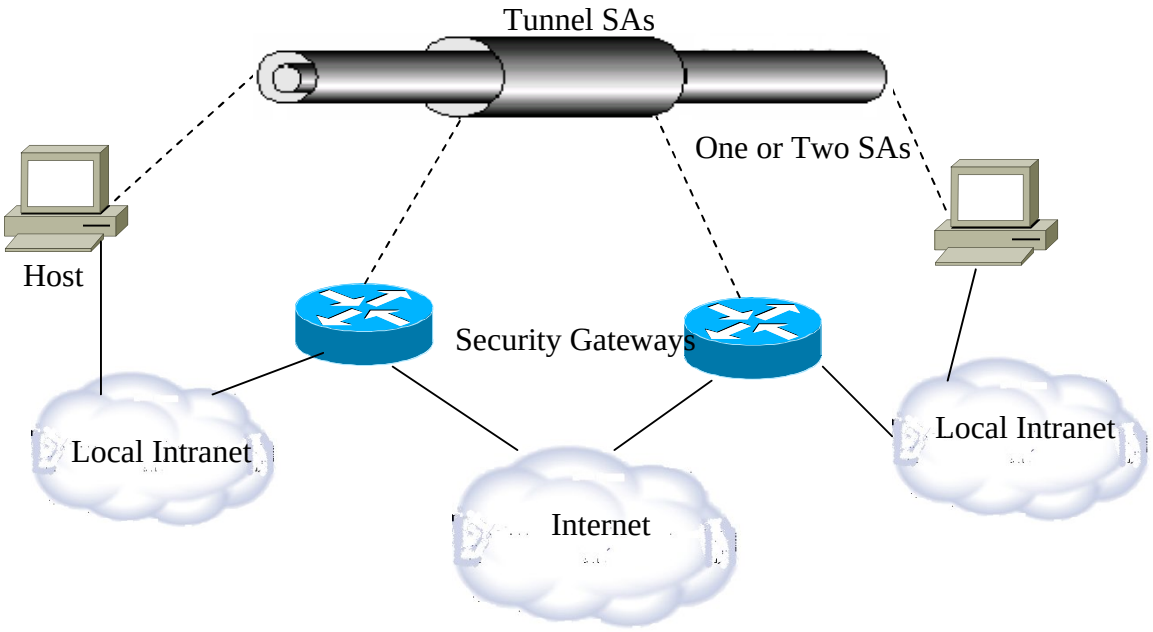
There are four combination examples for SAs that must be supported by IPSec enabled hosts or IPSec enabled security gateways such as router and firewalls [14].

Case 1: IPSec Security between end systems. The appropriate secret key is required for end systems communication via an SA.



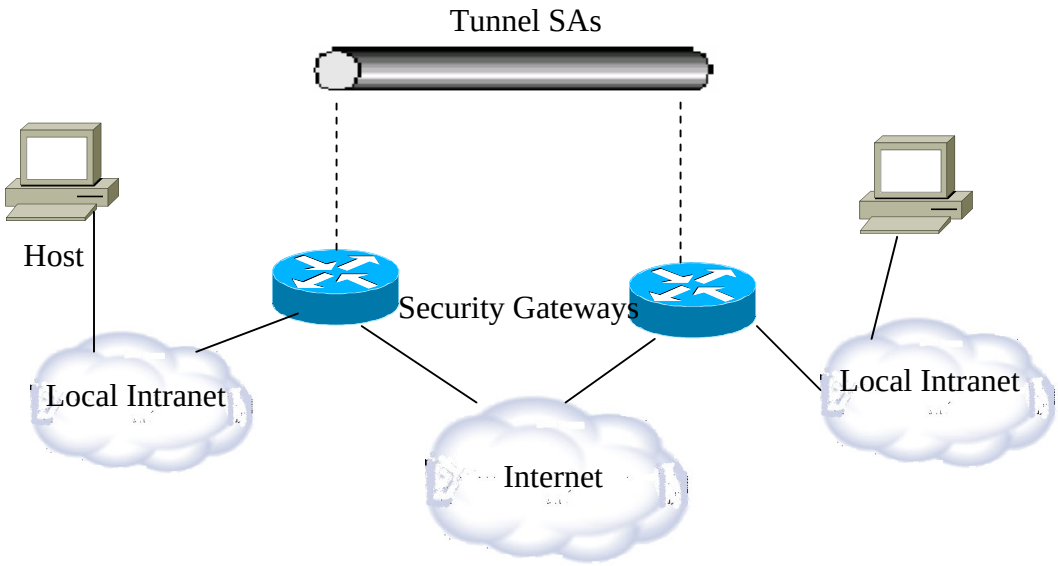
Case 1

Case 2: IPSec provide security between security gateways. No protection is provided between "gateways to host" traffic. Single SA tunnel is required because the IPSec security mechanism protect entire inner packet. This is a simple VPN.



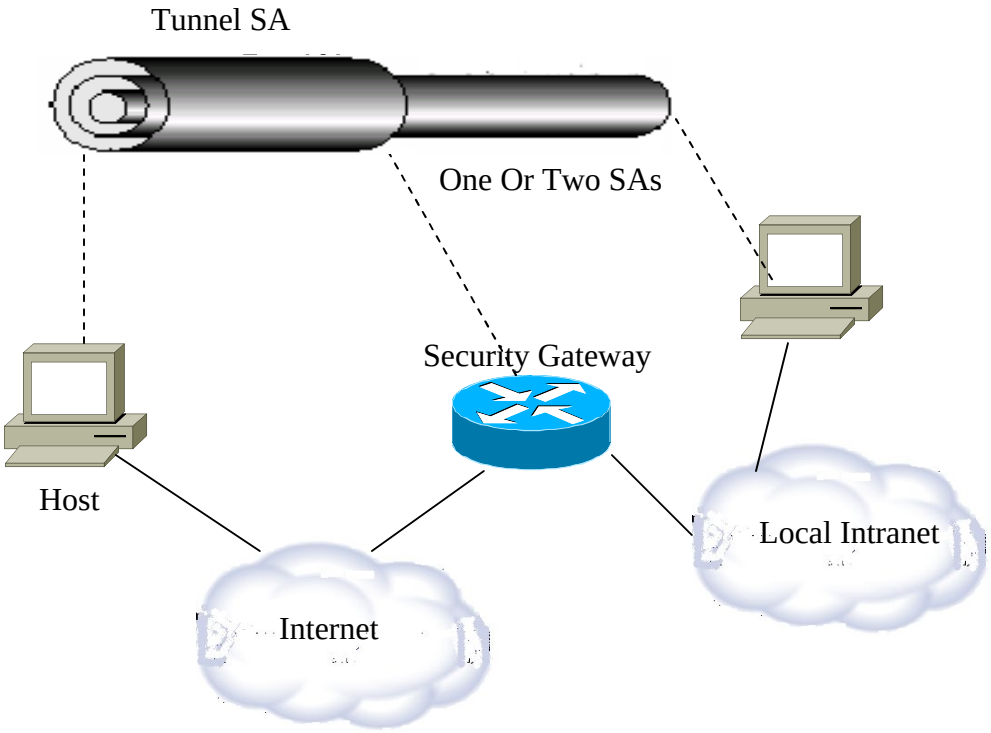
Case 2

Case 3: By adding two or more SAs, first gateway to gateway tunnel provides authentication or confidentiality or both for all traffic between end systems. And for end to end protection hosts can use any additional SAs.



Case 3

Case 4: In this case a remote host can access through corporate security to the internal network visa Internet. Required mode is tunnel between host and firewall.



Case 4

4.13 Key Management

The security of the cryptographic system depends on the determination and distribution of secret keys. Key management involves generation, distribution and storage of keys. The identity trust on other party is required if IPsec is used to protect communications. The exchange of secret keys is needed for symmetric cryptography. Two types of key management support are mandatory in IPsec architecture documents.

Manual Key: A system administrator manually configures each system with its own keys and keys of other communicating systems. This is not a scalable method and also re-keying is burdensome but practical for small environment.

Automated Key: Through the automated key generation and distribution for SAs keys are created and exchanged on demand and also destructed after completion of key lifetime.

The automated key management protocol for IPsec is ISAKMP/Oakley.

Oakley Protocol:

Oakley is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security. Oakley is generic and does not state specific formats.

(ISAKMP): Internet Security Association and Key Management Protocol is a framework for key management and provide the support for specific protocol and formats of negotiation of security attributes [13].

4.14 SUMMRY

In this chapter first I analyzed feature and application of IPSec. Then I presented detail architecture and protocol into IPSec suite.

Chapter 5
Secure Socket Layer (SSL) VPN

5.1 Introduction

Netscape developed SSL for secure web transactions to promote e-commerce. Netscape continued the development of SSL until version 3.0, which released as an Internet draft in 1996. In January 1999, the IETF adopted the SSL protocol for common standard and called it Transport Layer Security (TLS). TLS is also called SSLv3.1 and backward compatible with SSLv3.0. Although SSL was developed to provide secure web access but it also provide secure access to other applications including SMTP, POP3 and IMAP.

5.2 SSL Architecture

SSL is two layer protocols as show in FIG (5.1) which provides a reliable end-to-end secure communication by using TCP.

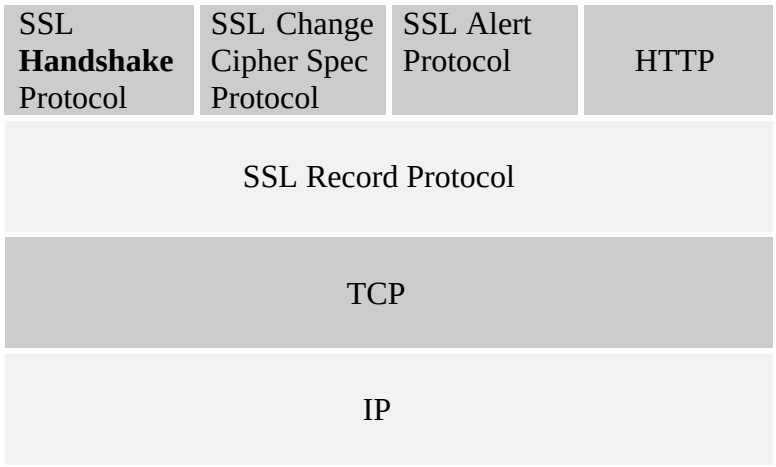


Fig 5.1: SSL Protocol STACK

The SSL Record Protocol provides security services to different higher-layer protocols. Particularly, Hypertext Transfer Protocol (HTTP) can operate on top of SSL, which provides the secure transfer services for Web client/server interaction. Three higher-layer protocols are defined as part of SSL [14][15]:

Handshake Protocol
Change Cipher Spec Protocol, and
Alert Protocol

These protocols are used in managing of SSL exchanges.

Connection and Session

SSL connection and SSL session are two important concept mentioned in SSL specification.

Connection: A connection is a transport to users that provides an appropriate type of service. The connections are temporary and peer to peer relationship, and every connection is associated with one session.
The following elements are included in connection state [14][15][16]:

"Server and client random
This is a byte sequence chosen by the server and client for each connection.

Server write MAC secret
The secret of the MAC used in operations on data written by the server.

Client write MAC secret.
The secret of the MAC used in operations on data written by the client.

Server write key
This is the biggest key to encrypt data encrypted by the server and decrypted by the client.

Client write key
This is the biggest key to encrypt data encrypted by the client and decrypted by the server.

When the block cipher in CBC mode is used, an initialization vector (IV) of every key is retained. First Handshake protocol initialize this field after that, the final cipher text block from each record is stored for use with the next record.

Sequence Number
Each party will be a set of numbers for sent and received messages for each connection. When a party sends or receives a change cipher spec message, the sequence number is set to zero. It should not exceed 2 ^ 64-1".

Session: Sessions are used to avoid the process intensive new security parameters for each connection. An SSL session is an association of a client and a server, created by the Handshake Protocol. Multiple connections share security parameters defined by session.

Between pair of parties such as on HTTP client and servers), there may be multiple secure connections and in practice there is only one session between them but there may be multiple simultaneous sessions between parties.

There are number of states associated with each session. Established session is in a current operating state for both read and write (i.e. receive and send). During the Handshake Protocol, pending read and writes states are created, upon successful conclusion of the Handshake Protocol; the pending states become the "current state".

The following parameters define the session state. (Definitions taken from the SSL specification) [14][15]:

Session Identifier

This is arbitrary byte sequence chosen by the server to identify active session states.

Peer Certificate
This is X509.v3 [x509] certificate for the peer. This element of the state may be null.

Compression method
The algorithm used to compress data before encryption.

Cipher spec
Cipher spec protocol states algorithms for data encryption such as null, DES, etc. and the data authentication algorithm such as MD5 or SHA.

Master secret
48-byte shared secret between client and server.

Resumable
This is a flag indicating whether the session can be used to initiate new connections.

5.2.1 Record Protocol

The SSL Record Protocol provides two services:

Confidentiality:

Message Integrity:

Overall operation of SSL Record Protocol is depicted in fig. The Record Protocol first fragments the date which need secure transmission into manageable blocks, optionally apply compression on to the data, and calculate a MAC for verification, encrypts the data, adds a header, and transmits the data in a TCP segment. On receiving end, received data are decrypted, verified, decompressed (if applied), and fragmented data is reassembled and then delivered to higher level users.

The first step in operation is fragmentation. Each fragment is up to 16384 bytes or less. Then fragmented data is compressed, and compression must be lossless and content length may not increase more that 1024 bytes. No compression algorithm is specified in SSLv3 and current version of TLS.

Then a message authentication code is computed for the compressed data. A shared secret key is used for message authentication code computation.

Then compressed message and the HMAC are encrypted using symmetric encryption. Different encryption protocols are permitted including, IDEA, RC4, DES-40, DES, 3DES, and FORTEZZA etc [14] [16].

In the stream encryption, HMAC computation takes place before encryption and then the compressed message plus the HMAC is encrypted.

For block encryption, after the HMAC computation padding may be required to yield bytes that are multiple of 8 before encryption.

The last step of SSL Record Protocol operation is to prepend a header. The header has the following fields [14][15]:

Content Type (8 bits): This field defines the higher layer protocol used to process the enclosed fragment.

Major Version: This 8 bits version field indicates the major version of SSL in use e.g. value is 3 for SSLv3.

Minor version: This 8 bits field indicates the minor version of SSL in use e.g. value is 0 for SSLv3.

Compressed Length: This is 2 byte field which state the length of the plaintext or compressed fragment.

5.2.3 Change Cipher Spec Protocol

The change cipher spec protocol consists on a single encrypted and compressed message, which signals transitions in ciphering strategies. This message is sent by both client and server and on reception instructs the record layer to copy the pending state into the current state, which updates the cipher suite to be used on this connection. The message consists of a single byte of value 1[14][15].

5.2.4 Alert Protocol

The Alert Protocol conveys SSL related alerts to the communicating peer. Current state specifies the encrypted and compressed alert messages.
"Each message in this protocol consists of two bytes. First byte has warning value of 1 or fatal value of 2 to transmit a message of severity. Both bytes indicates specific alert with code contained in byte"[16].

Error Alert
Error handling is very simple when an error is detected; the detecting party sends a message to the other party. Alert messages which have fatal level immediately terminate the connection. All other connections on this session may continue, but the session identifier becomes invalid, and no new connection can be established with this failed session.
Both communicating end, are required to discard any keys, session identifier and other things associated with this connection [16].

5.2.5 Handshake Protocol

Handshake protocol is very complex protocol, through which client and servers authenticate each other and also negotiate MAC algorithm, encryption algorithm and generation of cryptographic key to protect data in SSL environment. This protocol is used before the transmission of actual user data. Client and server exchanges series of messages by handshake protocol and every message has three fields format.

“Type: It’s a one byte message which indicates message type.

Length: It’s three byte which indicates message length in bytes.

Content: It has variable length which indicates the associated parameters with this message” [16].

Four phase of logical connection establishment between client and server [14].

Phase 1: Establish security capability
This phase establish security capabilities to initiate logical connection between client and server. Client initiate exchange by sending Hello message and server reply with Hello message. Both client and server use same parameters for hello message.

Phase 2: Server Authentication and Key Exchange

If server needs authentication it sends its certificate in this phase. The key exchange method requires the certificate message.

Phase 3: Client Authentication and key exchange

After receiving the server message client verify the validity of certificate and hello message parameters. Then client sends one or more messages to server. Some time server also request a certificate from client and client sends a certificate message to server and initiate this phase. Client sends no certificate alert to server if it does not have any valid certificate. Client key exchange message is also sent in this phase.

Phase 4: Finish

Both client and server send finish message which verifies that the authentication and key exchange were successful, and secure connection has been established. Now the client and server exchange the application layer data.

5.3 Cryptographic Computations

5.3.1 Master secret

Master secret between client and server is 48 byte value, which is generated once for this session by exchange of secure keys. First Diffie-Hellman or RSA is used for pre master secret exchange and then both parties calculate master secret [14][16].

5.3.2 Cryptographic parameter generation

Master secret generate client and server MAC secret, client and server write key and client and server write initialization vector in order for cipher specs. Hashed master secret into sufficient length sequence of bytes generates this parameter [14].

5.4 SSL VPN

SSL provide secure communication and is transparent to the upper layer application of OSI model. HTTP is the most successful application which uses SSL protocol.

SSL Provides these VPN features

1) SSL provide s authentication, confidentiality, and integrity by using cryptographic algorithms.
2) The SSL/TLS VPN users can access organization's resources remotely from any where by using just there PC without installing any VPN client software.
3) SSL VPN need no special consideration to transport traffic over the network having a firewall and NAT traffic because it works on TCP port 443 which is allowed on these devices.

SSL VPN did not standardized, but SSL VPN technology uses SSL/TLS provide secure transport mechanism. Today remote access commonly used SSL VPN technologies include reverse proxy, port forwarding, SSL VPN tunnel client and integrated terminal services [17].

5.5 Summary

First in this chapter we described SSL protocol and SSL VPN, we also described SSL architecture and different protocol working in this architecture. At the end we covered SSL VPN and its features.

Chapter 6
Comparison between Different VPN Models

In previous chapters of this report we explored different layer 3 VPN architecture mainly MPLS VPN, IPSEC VPN and SSL VPN that can be selected for WAN by any organization according to their requirement. Appropriate selection of VPN architecture mainly effects on scalability, security, support for voice and video, and support for multicast. Business requirement of an organization provide the information which VPN architecture is optimal for their network.

6.1 Introduction

To choose VPN architecture for organization there is need to consider the business requirements of organization, due to wide verity of VPN option like MPLS, IPSec, and SSL architecture and their usage scenario. In most cases combinations of these architectures provide the required services, needed to the organization. The selected architecture has different effects and aspects, which includes that the VPN solution is network based or customer premises based. Whether a solution is provided as managed service as in MPLS-based VPN or VPN originated and terminated in the MPLS enabled service provider network. Other solutions also can be provided as manage solution by service provides but are usually managed by organization itself as IPsec and SSL architecture and VPN originate and terminate at the customer premises equipment.

In this chapter we will describe usage scenario of each MPLS, IPSec, and SSL VPN technology and their strength and limitation. At the end of the chapter a table will be provided to compare the above mentioned three technologies [20].

6.2 Criteria for Evaluating IP VPN Architectures for the Enterprise

To provide secure and cost effective connectivity over a shared network infrastructure, VPN solution must have the following attributes, [19][20]

1) High Availability
2) Network Security
3) Scalability
4) QoS
5) Management

Every VPN solution has these attributes but with different degree, so the organization has to decide which attribute they required most for their business. In next section we will discuss these attributes in detail.

6.2.1 High Availability

High availability means high network reliability and redundancy of both, link and network equipment which can deliver network traffic all the time. Sometime it is provided by Service level agreement SLA. SLA is a contractual guarantee provide by service provider to organization about network uptime and performance. Optionally for different types of traffic multiple levels of services can be provided by SLA [19].

6.2.2 Security

An organization want to know that there VPN traffic will not flow on to another organization's VPN and will remain private because organization is using shared infrastructure of service provider network which provide service to multiple organization on their core network. Hence VPN solution may use, encapsulation, encryption, tunneling, authentication for sensitive data, further different criteria is used for routing table security and traffic separation such as different routing table for each VPN, constraint based routing and access control for this purpose [19].

6.2.3 QoS

QoS is an important consideration when deploying any VPN architecture. QoS is relevant to end-to-end delay, jitter (variation in delay) and packet loss. For different types of traffic such as voice, video, and data different levels of services are required which is defined by class of service (CoS) attribute.

For mission critical applications, organizations choose service provider that offer support for multiple CoS for different tunnels. VPN solution by enabling QoS mechanism of CoS classify traffic and assign priority to tunnels which carries delay sensitive and mission critical traffic such as voice and video [19].

6.2.4 Scalability

Need of bandwidth and connectivity of organization can change over time and in some cases suddenly, as the business expansion, mergers and for encouragement of telecommunicating. Bandwidth and connectivity requirements can also boosts if extranet connectivity to partners and customer is needed. To be responsive to these growing needs and organization choose a service provider who can accommodate the unplanned changes and growth of VPN [19].

6.2.5 Management

The VPN architecture chosen by an organization affect the manageability and related cost. The organization wants the easy VPN which have reduced management cost. Organizations neither have to spend lot of resources and efforts to train a management personal, nor have they to spend overhauling of equipment. VPN Management services needed to an organization are includes:

1) VPN Provisioning
2) SLAs support
3) Installing VPN enabled devices and software
4) Implementing policies related to security and QoS
5) Preserving Current configuration regarding routing etc.
6) Providing services addition, removal and change, also providing performance management, fault management, and reporting etc [19].

6.2.6 Cost of Ownership

Organizations also have concerns that total cost of ownership of VPN solutions should not exceeds the benefits of the solution to the company and they don't have to change the every network equipment for the VPN solution deployment [20].

In next few sections we describe three VPN solution and their usage scenario and strengths.

6.3 MPLS Based VPN

As we studied in chapter 2 MPLS is switching technology which has intelligence of routing. Service providers can enjoy the benefits of MPLS with their existing IP and IP over ATM architecture or can combine MPLS with other layer 2 technologies. Layer 3 MPLS VPN is a conventional peer-to-peer model and BGP is used for distribution of VPN related information.
Scalability is key advantage of MPLS VPN as it support of small to vary large size VPN deployments. MPLS also provide QoS, quick correction of faulty or failed link, traffic engineering etc [19].

MPLS USAGE Guidelines

1) If the organization wants service level agreement SLA MPLS VPN is the best choice.
2) If the organization's security requirement is just to separate traffic of different VPN as in ATM and frame relay network MPLS is good choice.
3) If organization have full mesh or partial mesh topology MPLS is suitable for them.
4) If voice, video and data is converged on a single network then required QoS for mission-critical and delay sensitive data can be better provided by MPLS.
5) In out sourcing organization WAN [19].

MPLS Strength

1) Network Security: MPLS separate traffic of different VPN by using route distinguisher on the same core. Per VPN routing tables separate routing information of each client.

2) Scalability: MPLS based VPN deployment provide easy change, growth and migration to organization. Adding new site in VPN, MPLS only requires to establish peering between provider and the new site and does not need the configuration changes at other site, in contrast to other VPN architectures where end-to-end or full mesh peering is required.

3) SLA Support: If the VPN environment require strict performance and resiliency then SLA is very important. QoS mechanism, traffic engineering and bandwidth guarantee provides SLA support in MPLS VPN [19][20].

6.4 IPSec Based VPN

As we explored detailed protocol and feature of IPSec is an IETF standard and is not a single protocol but suit of security related protocol and these protocols provide layer 3 CPE based VPN architecture. IPSec provides following function to protect data traveling across public network.

Data confidentiality
Data Integrity
Data origin Authentication
Antireply Services

To achieve the security functionality IPSec defines Authentication Header for data authentication and Encapsulating Security Payload for data confidentiality. Data Encryption Standard (DES), Triple DES and AES are supported symmetric encryption algorithm by ESP. IKE is used in negotiating security parameter between potential peer before transmission of actual data which need protection.
It is possible in IPSec that traffic can be specified which need protection and which does not needs and also access control is possible in manner that who can receive protected traffic. Usually IPSec VPN service of an organization are in hub and spoke topology where headquarter is hub and all branches are spokes and have a point to point connection to the hub. Both site-to-site and remote access VPN designs are supported in IPSec [19][17].

IPSec Usage Guidelines:

Organizations should consider the following factors when choosing IPSec:

1) Encryption and authentication of user and device are required security features.
2) Deployment of IPSec VPN on existing IP network is possible which save equipment and operational cost of building a new infrastructure.
3) Provide access to corporate resources to geographically dispersed mobile workers and teleworkers.
4) Little or nor change is required in existing IP infrastructure if organization want to add new site into network, so the deployment is rapid. If required topology is hub and spoke IPSec works well [19].

User Experience

For site-to-site and remote access VPNs, users have slightly different experience. In site-to-site VPN an IPSec enabled router or security gateway at branch office initiate an IPSec session with central site. A secure VPN tunnel is created after negotiation and authentication of session between the central site and branch office. This whole process is transparent to user, and user just uses the services and applications of central site as these services are local. In remote access VPN user needs software VPN client and provide the host name or IP address of destination. After successful setup of tunnel users can access application at central site as locally [19].

IPSec Strengths

Strong Security: IPSec provide very strong security e.g. authentication of user, confidentiality of data and data integrity. For user's authentication pre-shared keys and digital certificates.
Mobile and Tele workers support: IPSec VPN device at headquarter create VPN tunnel with thousand of mobile and tele workers at different location.
Easy deployment: Service provider involvement is not required to setup VPN. However service providers managed services can be advantageous for the organization because it reduce cost and also provide extra value added services and reduce the risk.
Low Cost: Overall Cost of network infrastructure is reduced by using low cost internet for network traffic transport [19][20].

6.5 SSL Based VPN

As we studied in chapter 4 SSL provides source connectivity to WEB based application by using WEB browser to any Internet user without client software. SSL as alternative to IPSec Remote access VPN and provide location independence to SSL users. SSL provide both encryption and authentication to traffic flow between parties.

SSL Indicator

1) WEB browser originated connection.
2) If there is no control or limited control of IT department on remote systems.
3) If short duration access from home, library or airport is needed to organization network.
4) If limited access is provided to remote host on organization network [18][19].

User knowledge

There is not any difference for Web browser users.

SSL strength

The strengths of SSL for secure remote access include
Reduced Overhead Of training: Almost every WEB browser support SSL.
Access from Anywhere: SSL enabled WEB browser can be used form any PC with internet access. Eliminate the VPN client software installation.
Client Ubiquity: WEB browsers have built-in client software, installed on almost every end system.
Transparent Wireless Roaming: IP address is not associated with SSL sessions [19][20].

Below is the comparison table of MPLS VPN, IPSec VPN and SSL VPN [19].

	MPLS-Based VPN	IPSec-Based VPN	SSL-Based VPN
Topology Support	Site-to-site VPN: Hub-and-spoke or full-mesh	Site-to-site VPN: Mainly hub-and-spoke	Remote-access VPN
Security *Session Authentication*	Establishes VPN membership during provisioning, based on logical port and unique route descriptor Defines access to a VPN service group during service configuration; denies unauthorized access	Authenticates through digital certificate or pre-shared key Drops packets that do not conform to the security policy	Authenticates through digital certificate
Confidentiality	Separates traffic, which achieves same results delivered in trusted Frame Relay or ATM network environments	Uses a flexible suite of encryption and tunneling mechanisms at the IP network layer	Encrypts traffic using the public key infrastructure (PKI)
QoS and SLAs	Enables SLAs with a scalable, robust QoS mechanism and traffic-engineering capability	Does not address QoS and SLAs directly	Not applicable; service provider network is unaware of SSL traffic
Scalability	Highly scalable because no site-to-site peering is required Capable of supporting tens of thousands of VPNs over the same network	Acceptable scalability in most typical hub-and-spoke deployments Difficult for a very large, fully meshed IPSec VPN deployment; require s planning and coordination to address key distribution, key management, and peer configuration	Not applicable; service provider network is unaware of SSL traffic
Management *Site-to-site support* *Remote access Support*	 Yes Yes, if used in conjunction with IPSec	 Yes Yes	 No Yes
Provisioning	Requires one-time provisioning of customer edge and provider edge devices to enable the site to become a member of a MPLS VPN group	Reduces operational expense through centralized network-level provisioning for CPE based service offering Uses centralized provisioning for network based service offering	Not applicable; service provider network is unaware of SSL traffic
Service deployment	Needs MPLS-enabled network elements at the core and edge of the service provider network	Can be deployed across any existing IP networks or the Internet	Not applicable; service provider network is un aware of SSL traffic
VPN client	Is not required because MPLS VPN is a network-based VPN service; users do not need VPN clients to interact with the network	Is required for client-initiated IPSec VPN deployments Cisco VPN client software is supported by Microsoft Windows, Solaris, Linux, and Macintosh operating systems	Is not required; relies on Web browser
Place in network	Core network	Local loop, edge, and off-net	Local loop, edge, and off-net
Transparency	Resides at the network layer Transparent to applications	Resides at the network layer Transparent to applications	Resides at the session layer Works only with applications coded for SSL

VPN Architectures Comparison Table [20]

Conclusion

MPLS VPN provides a level of security similar to GRE tunnels, ATM or frame relay. The MPLS VPN model enforces traffic separation by assigning unique VRFs to each VPN of the customer. Thus users is in specific VPN cannot see traffic outside their VPN When the strict security is required such as confidentiality authentication and integrity IPSec or other technology that uses encryption or hashing. MPLS provide and great features of QOS service and Traffic engineering. In the networks where great demand of QOS features MPLS VPN is the choice.

IPSec Provides authentication, integrity and confidentiality, Hence MPLS IPSec VPN provides a high level of confidentiality and protect the sensitive traffic over Internet. Networks which require closed security IPSec VPN is the main choice. Some QoS does not work well with IPSec due to encryption, Like cRTP is incompatible with IPSec, even legitimate IPSec protected packets delayed or dropped by Anti-Replay mechanism, solution to this is to create separate SAs for data traffic and voice traffic. QoS implementation in IPSec require great deal of work.

The SP uses MPLS to provide the MPLS VPNs by separating the IP cloud of the VPNs from other VPN clouds and the Internet. IP Separation is first security mechanism the defense against most security threats such as break-ins and DoS attacks.
Then VPN traffic crossing the VPN backbone can be secure by use of IPSec Confidentiality feature. The use of tunnels endpoints discovery (TED) or dynamic multipoint VPN (DMVPN) makes an IPSec implementation more manageable.

Integration of IPSec and MPLS

Typical IPSec implementations in combination with MPLS VPNs include:

1) Site-to-Site VPN is implemented between CE routers to provide packet authentication, integrity and confidentiality across an untrusted service provider network. All other untrusted IPSec sessions should also be terminated inside the customer network such as remote access across the Internet, IPSec over dialup network.
2) If the MPLS VPN provider is regarded as the only trusted transport network, then the service provider can offer additional services based on IPSec to accommodate the secure usage of other transport network so the infrastructure of service provider can be used to terminate IPSec-based remote access into MPLS VPN.

Typical Usage Scenario IPSec and MPLS VPNs provide complementary services that maximize the security of a VPN.
MPLS provides VPN functionality by isolating the routing environment of a customer network but still utilizing a shared IP infrastructure. IPsec adds advanced cryptographic mechanisms to provide packet authentication, integrity assurance,

confidentiality and reply prevention. MPLS additionally provides protection to customer IPSec devices because it isolates them from the internet.

The main use of IPSec is to implement site to site VPN and remote access VPN. In customer managed IPSec both site to site and remote access IPSec sessions are terminated inside the customer network. In service provider managed, site-to-site VPNs are typically only provided using MPLS. Remote-access VPNs still use IPSec but the sessions are terminated inside the service provider network in appropriate MPLS VPN.

For remote access VPN organization can combine the features of SSL and IPsec VPN.

REFERENCES

[1] *"VPN Technologies: Definitions and Requirements"*, Paper, VPN Consortium, July 2008.

[2] E. Rosen, A. Viswanathan, R. Callon, "*Multiprotocol Label Switching Architecture"*, RFC 3031, January 2001.

[3] Vivek Alwayn "Advanced MPLS Design and Implementation", Cisco Press, Sep 25, 2001, ISBN-10: 1-58705-020-X; ISBN-13: 978-1-58705-020-6.

[4] E. Rosen, Y. Rekhter, "*BGP/MPLS IP Virtual Private Networks (VPNs)"*, RFC 4364, February 2006.

[5] Ivan pepelnjak, Jim Guichard, *"MPLS and VPN Architectures (Networking Technology)"*, Cisco Press, November 2000, ISBN: 1587050021 978-1587050022.

[6] Paul Brittain, Adrian Farrel, *"MPLS VIRTUAL PRIVATE NETWORKS"*, a review of the implementation options for MPLS VPNs, White paper.

[7] www.cisco.com last viewed on 18-01.2009

[8] CERT (Computer Emergency Response Team) official website, http://www.cert.org/ last viewed on September 15, 2008.

[9] S. Kent, K. Seo, "*Security Architecture for the Internet Protocol"*, RFC 4301, December 2005.

[10] S. Kent, "*IP Authentication Header"*, RFC4302, December 2005.

[11] S. Kent, "*IP Encapsulating Security Payload (ESP)"*, RFC4303, December 2005.

[12] V. Manral, *"Cryptographic Algorithm Implementation Requirements for (ESP) and (AH)"* RFC 4835, April 2007.

[13] C. Kaufman, Ed, *"Internet Key Exchange (IKEv2) Protocol*", RFC 4306, December 2005.

[14] William Stallings *"Cryptography and Network Security: Principles and Practice (3rd Edition)"* Prentice Hall, August 2002, ISBN: 0130914290, 978-0130914293.

[15] The SSL protocol Version 3.0 at http://wp.netscape.com/eng/ssl3/ssl-toc.html

[16] T. Dierks, E. Rescorla, *"The Transport Layer Security (TLS) Protocol Version 1.1"*, RFC 4346 April 2006

[17] Jazib Frahim, Qiang Huan, *"SSL Remote Access VPN"*, Cisco Press, June 2008, ISBN: 978-1-58705-242-2, 1-58705-242-3

[18] Steven Song, *"SSL VPN Security White Paper"*, White Paper, http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html.

[19] Matthew Finlayson, Jon Harrison, Richard Sugarman, *"VPN Technologies -A Comparison"*, http://www.dataconnection.com, White paper, *2003-2004.*

[20] Cisco Systems, *"Managed VPN - Comparison of MPLS, IPSec, and SSL Architectures"*, White paper, Cisco Systems.