CHAPTER 12

Virtual Private Networks

Introduction

Business has changed in the last couple of decades. Companies now have to think about having a global presence, global marketing, and logistics. Most of the organizations have branches spread across different geographies of the world. Wherever you are located, all these branches need to be connected with their headquarters data center for information. With the changing culture and environment, the demand of the sales force to be able to connect to the headquarters data center from either their homes or hotels is increasing and seamless connectivity to the main data center has become a necessity. Hence, there is one demand that the companies are asking for from their network team: a fast, safe, secure, and trustworthy network that helps in communicating with all their offices wherever they are located.

When the companies want to connect their network with outside partners, external vendors, or even with external telecommuter and sales employees, there are two options: one private, dedicated lease line or share a part of bandwidth with an existing line such as the Internet.

Dedicated leased lines ranging from ISDN (144 Kbps) to Optical Carrier (192 Gbps) fiber enable the companies to connect a geographically dispersed office as shown in Figure 12-1. For example, X.25, Frame Relay, Asynchronous Transmission Mode (ATM), and MPLS (Multiprotocol Label Switching) are examples of private WAN networks.

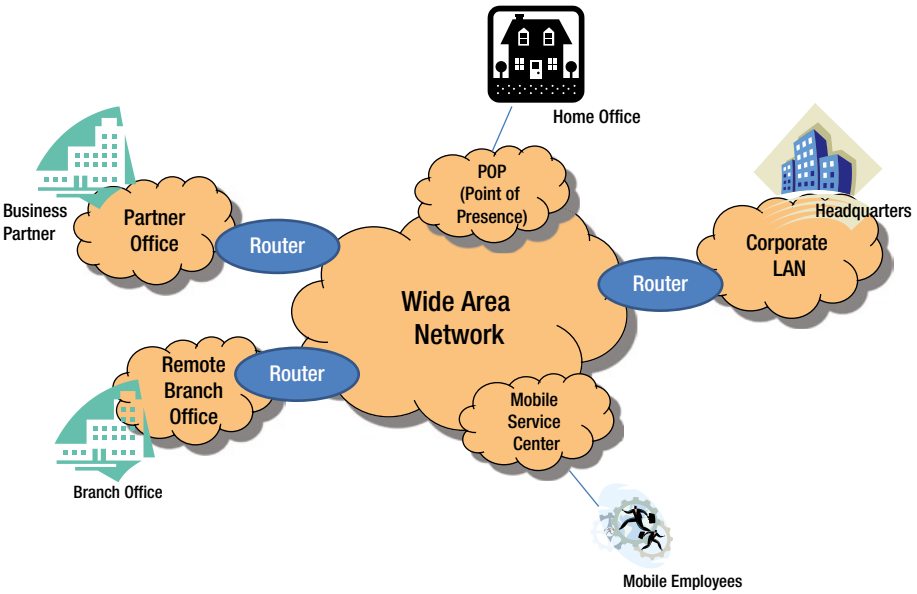

Figure 12-1. *Typical Business Scenarios*

For secured connection, it is always recommended to have your own private dedicated line between different points. However, this option is very expensive as you have to connect different places by different cables and laying cable across geographies is an expensive affair and maintaining these lines is even more expensive. Additionally, a leased line is not a viable option as the locations of the offices may change or for a mobile work force that is constantly on the go. The other option is to share the line with others which is cheap, but not always secure. To overcome this problem, the concept of Virtual Private Network (VPN) was developed. VPN creates a tunnel between the two end hosts and data is transmitted securely through this tunnel but on a public shared network.

A VPN is a private network, as shown in Figure 12-2 (similar to a leased line) but uses the public network (Internet) to connect to remote sites. VPN creates a "virtual" tunnel connection routed through the Internet from the company's trusted network to the remote office or to a mobile work force. With VPN, you can send data via the public network which emulates a private link between the two parties or two networks.

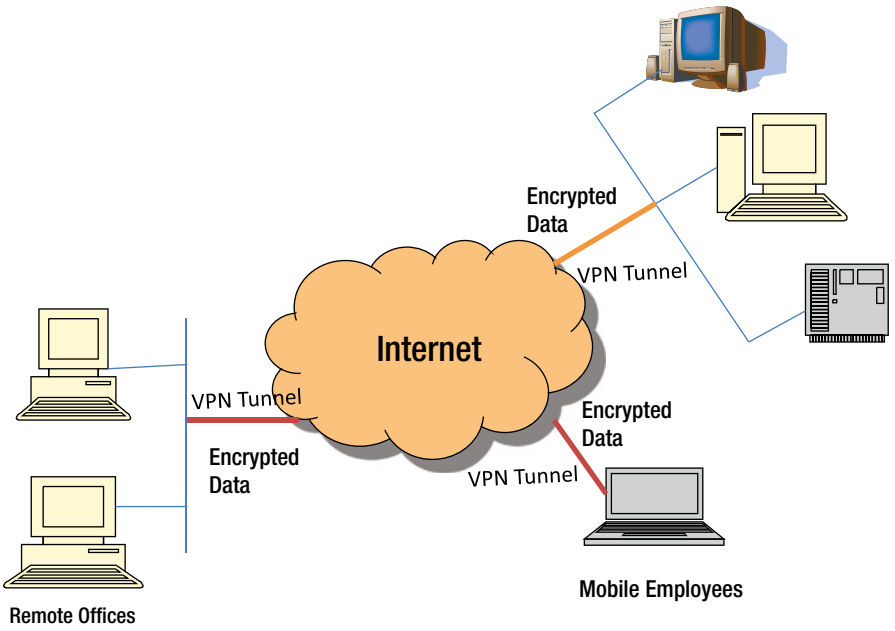

Figure 12-2. *Virtual Private Network scenario*

A secure VPN encrypts data before passing it through the tunnel to ensure privacy. Data integrity and authenticity are also maintained before the creation of the tunnel. Thus, VPN protects data with privacy, integrity, and authenticity. With VPN, you can provide many services such as the Internet, e-mail, applications, and database services to users in remote locations with secured communication.

Advantages of VPN

A Virtual Private Network (VPN) allows two computers to communicate securely over the public network such as the Internet. This allows for connecton of employees, partners, and other small branch offices to the corporate network securely and at low cost. For example, a sales person on the road can access a product database securely from a laptop

or mobile device as if she is sitting in the office. A company's small branch office can connect to the corporate office using VPN across the Internet and access information on the network as if it is all in the same network. Following are some of the advantages of using VPN:

- **Cost savings:** Using private networks used to be the only solution for WAN connectivity. However, it was expensive and not always feasible, not easily scalable, and lacked security features. A VPN solution making use of the Internet is an inexpensive alternative, allowing the full advantage of cost savings of the Internet and providing a superior level of security.
- **Smooth and Seamless Integration:** VPN allows seamless integration with the existing network infrastructure. There is no need to change your network architecture or any network software component.
- **Secure Remote Access:** One of the primary objectives of the VPN is to provide remote users secured access to the organization's trusted network. VPN technology allows the same connectivity whether it is network to network, host to host, client to server, dial-up connections, or home office or mobile users.
- **Extranet Connections:** In today's global economy, most organizations have one or more partners for mutual growth and success of the business. Companies have to connect to their external partners to share certain information, sometimes even critical, confidential information. Hence, they need to have a secured connection between the two partners. VPN solutions allow secured connection between the two parties allowing even proprietary information to be shared.
- **Low Maintenance:** VPN eliminates much of the day-to-day maintenance such as key management and SNMP.

VPN Types

When data is routed through the Internet, it will pass through different service providers' network and equipment. The service provider may or may not provide any security. The customer data needs to be transported securely where the customer does not trust the service provider's network and prefers creating a "virtual" tunnel to pass the traffic securely. In such cases, the service provider merely acts as a transporter of IP traffic.[1]

Primarily, VPN supports two types of communication:

- Remote Access (host-to-site) VPN
- Site-to-site (intranet and extranet) VPN

Remote Access (Host-to-Site) VPN

Remote Access (Host-to-Site) VPN is a connection between a user and the LAN inside a company where the user is an employee who needs to connect to the corporate network from outside the company. This type of connection is used mainly by telecommuting or sales force employees who want to connect to the corporate LAN from remote locations. The remote employees, once they connect to the Internet, use their VPN client to connect to the corporate LAN. The VPN client first connects to the VPN gateway server, a network device located in the DMZ. The VPN gateway server authenticates the user and then creates a "virtual" tunnel between the remote host and the gateway for a secured connection. Once the virtual tunnel is created, the channel becomes secured and the remote host can connect to any server in the trusted network to start sending data. This type of Remote Access provides a secure, encrypted communication between two parties that are connected via the Internet. This is depicted in Figure 12-3, where a remote employee is accessing a corporate network from his house. He is authenticated at the corporate network level. Once he is inside the network, he can access any resources within the network. However, any data flows out of the network are secured and travel through the VPN tunnel.

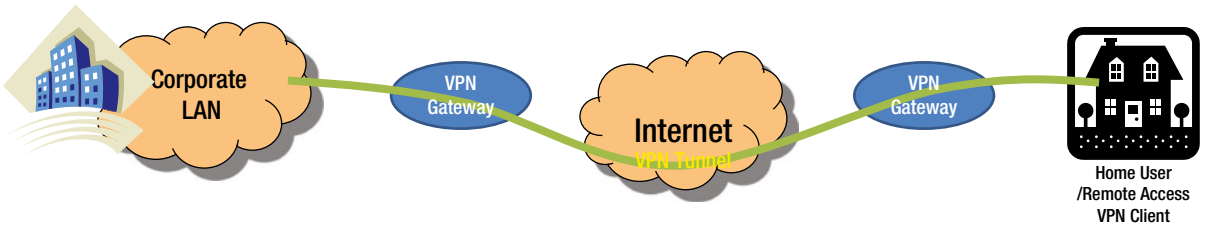

Figure 12-3. *Remote Access VPN*

Host-to-Host VPN

Some refer to host-to-host VPNs as remote access with one small change. In host-to-host VPN, two hosts are connected through a VPN tunnel. The tunnel is directly established between two hosts for a secured data transfer. Before the data transmission, the user is authenticated and the encrypted keys are exchanged between the two parties and then the transmission of data begins. The VPN tunnel ensures data authenticity, data integrity, and data confidentiality.

As shown in Figure 12-4, two hosts are connected over the internet. This type of connection is allowed when an employee or a partner wants to connect to a specific network resource (server/database) securely. He/she may not be allowed to access any other resources within the network.

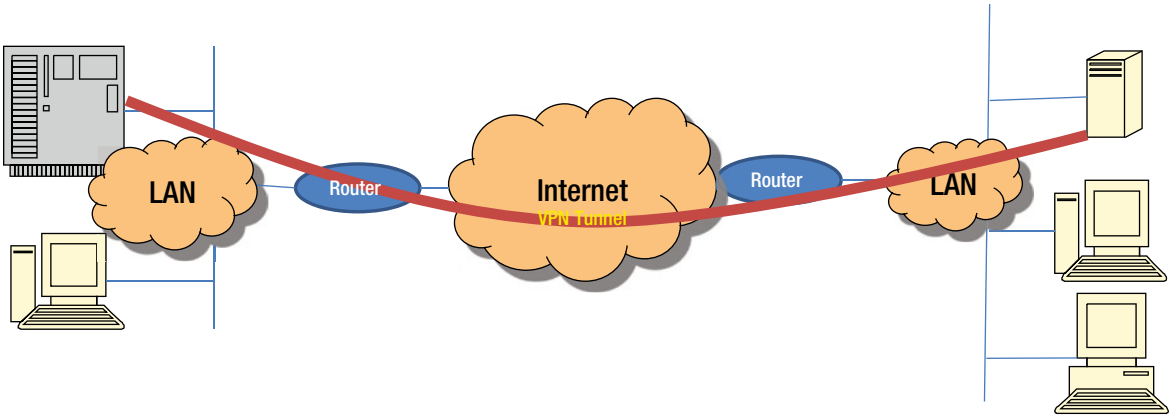

Figure 12-4. *Host-to-Host VPN*

Site-to-Site (Intranet and Extranet) VPN

Site-to-site VPN connects one network to another network over the Internet, such as connecting a remote branch office to the corporate headquarters LAN. In this setup, the tunnel is created between two VPN gateways. The VPN gateway of the remote branch negotiates a connection with the VPN gateway of the corporate headquarters network and establishes a secured tunnel. The remote hosts will not have any VPN clients but they send normal TCP/IP traffic through the VPN gateways. The VPN gateway is responsible for authentication of the user/network, encryption, and integrity of data. Once the VPN gateway receives the encrypted data, it strips the headers, decrypts the content, and relays normal data toward the target host inside the trusted network. Thus, the VPN tunnel is created between two sites allowing the company's network and resources available to the remote location. This solution is ideal for small offices located in remote parts of the world.

As shown in Figure 12-5, two networks are connected as if they are one. Any device on one network can communicate with the device on the other network securely as if the other device is part of the same network. Whenever the data leaves one network, it passes through the secured VPN tunnel.

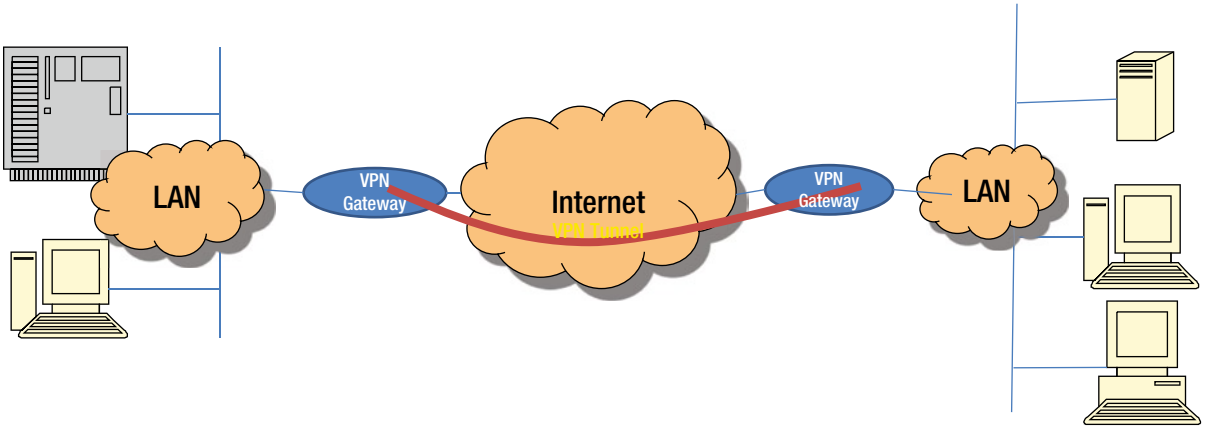

Figure 12-5. *Site-to-site VPN*

There are two types of site-to-site VPNs:

- **Intranet-based VPN** – A company with a small number of remote offices, wishing to connect all of them together to make it into a single network can use this type of connection. A seamless connection is established between all the remote branches of the company which helps in sharing of systems and network resources. This gives the feeling that all the different networks of the various branches are one single network.
- **Extranet-based VPN** – A company may wish to connect with its partner's network. One company's LAN is connected with another company's LAN to share certain information across the companies for better business relationships and processes. For example, in case of supply chain relationship, companies allow their partners to connect to their network to share the database and other relevant information. The extranet-VPN allows the companies to share certain information with their partners, such as just a customer database application and nothing else. If the team working on this database application consists of 10 people from one company and 5 people from the partner company, then a secure VPN is created only between this small network of 10 systems and the other 5 systems. No other network resources are shared except for the database application. It allows the companies to work together in a secure and shared environment while still allowing their internal network to be secure and available for only the internal users.

VPN and Firewall

A firewall is used to control the access into the network so that it can stop the spread of "fire" in the surrounding area whereas VPN provides the secured channel between the two parties who are exchanging information. A combination of VPN and Firewall would ensure only authorized applications and users are accessing the information. VPN Firewall, as shown in Figure 12-6, ensures that malicious intentions are impeded and only authentic traffic enters into the VPN.

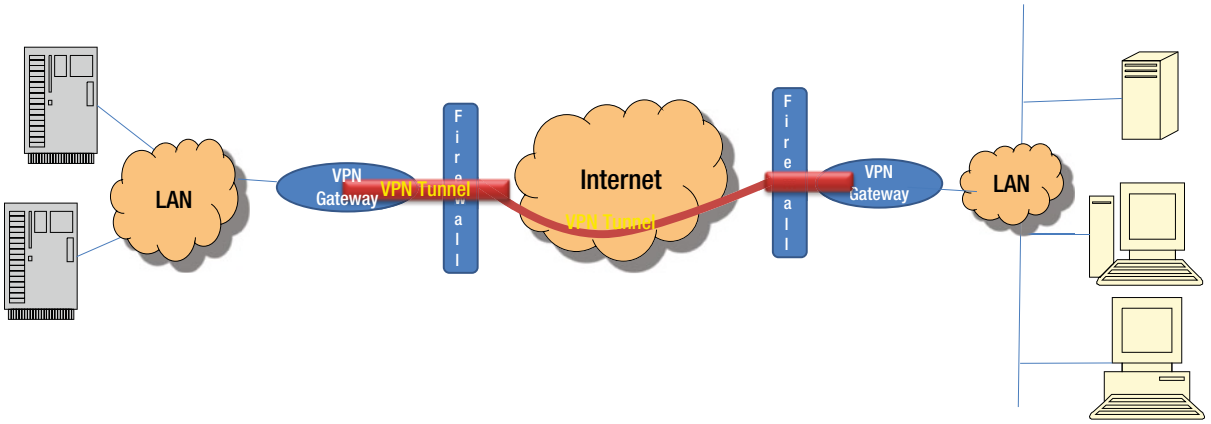

Figure 12-6. *VPN and Firewall Deployment*

VPN and firewall can be deployed separately. Normally VPN is deployed after the firewall. First check of entry is firewall. A firewall provides proper policy and access check and then allows the traffic to pass through the VPN tunnel. Some of the VPN gateway vendors are now providing firewall functions also. This has an added advantage of using a single device to configure both as VPN gateway and firewall.

VPN Protocols

VPN supports secured communication over a public network. Before the data transmission, the secured channel should be established. Each party should know how they securely communicate, how they encrypt the data, and how they exchange decryption keys so that each party can transmit information securely. VPN connection has two phases. In the first phase of connection, both parties establish secured connection by identifying themselves as genuine parties and exchanging the keys to support data encryption, decryption, and data integrity. In the second phase, actual data transfer happens with the encrypted data where only two parties know the keys. For secured connection, VPN protocols should support:

- Tunneling
- Data Authentication
- Data Integrity
- Data Encryption
- Anti-replay services

Tunneling

VPN Tunneling is the encapsulation of one type of data packet within another data packet. A specific data packet of one protocol is wrapped into another protocol and then transmitted between a VPN client and a server. For example, an IP packet is wrapped around a PPTP (VPN protocol) and transmitted. PPTP is a tunneling VPN protocol. PPTP protocol itself manages user authentication, data integrity, and data encryption.

Data Authentication and Data Integrity

Data authentication guarantees the authenticity of the two parties who are communicating with each other. It authenticates that the data is actually being received from a genuine user who has sent the data. Integrity means that the data received has not been modified during transmission.

Anti-Replay Services

Anti-replay services are services in which the receiver device can reject duplicate packets or late arrival packets in order to protect against replay attacks.

Data Encryption

Encryption is the mechanism commonly used for protecting confidentiality and privacy of data over the public network. The sender encrypts the data using a particular method, which is normally called a key, and the receiver decrypts the message using the same method and the same key.

The implementation of a VPN is based on one of the protocols listed in Table 12-1.

Table 12-1. *VPN Protocol Architecture*

Site-to-site VPN	Remote Access
Internet Protocol Security (IPSec)	Point to Point Transport Protocol (PPTP)
Generic Routing Encapsulation (GRE) Or IP Tunneling	Layer Two Protocol (L2TPv3)
Multi-Protocol Label Switch (MPLS)	Cisco L2F
	The Secure Socket Layer (SSL)

Point to Point Transport Protocol (PPTP) Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP), or Secure Socket Tunneling Protocol (SSTP) rely on Point-to-Point Protocol (PPP). PPP[1] was designed to provide a full-duplex communication between the two peers that is assumed to deliver packets in order. PPP is intended to support a wide variety of connections between routers, bridges, and hosts.

PPP first authenticates the users before the transmission of data. The PPP encapsulation supports multiplexing of different protocols simultaneously over the same link, thus allowing multiple vendor compatibility and supporting multiple applications and protocols.

PPTP protocol describes how a secure PPP link can be established over a TCP/IP connection. PPTP encapsulates the IP protocol packets inside PPP datagrams and transmits them over the Internet. PPTP requires IP connectivity between the server and the client. If there is already a connection between the server and the remote client, then a PPTP tunnel can easily be created and data transmitted over a secured channel across the LAN. If the remote client needs an Internet connection, then a dial-up can be used or any other services to connect to an ISP before establishing the tunnel.

PPTP was developed by the vendor consortium of Accend Communications, Microsoft Corporation, Copper Mountain Networks, 3COM, U.S. Robotics, and several other individuals. It was then submitted to the Internet community as an RFC 2637.[2]

PPTP allows PPP to be tunneled through the IP network as shown in Figure 12-7. It does not change any PPP protocol itself. PPTP uses Generic Routing Encapsulation (GRE) to provide a flow and congestion control datagram services for transporting PPP packets over the Internet connection.

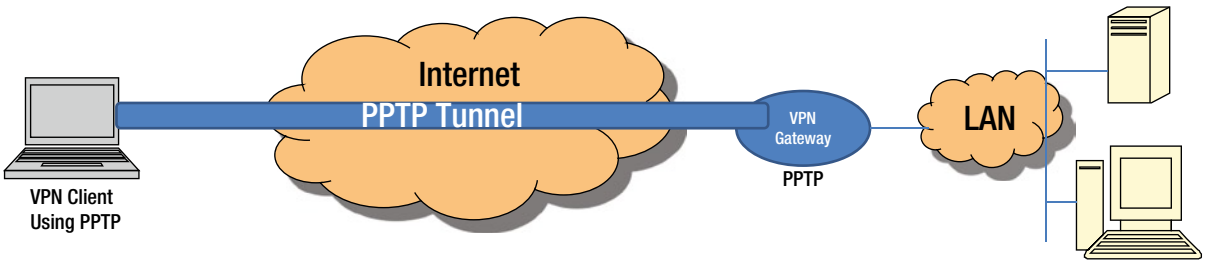

Figure 12-7. *PPTP Tunneling*

PPTP uses an enhanced GRE (Generic Routing Encapsulation) mechanism to provide a flow- and congestion-controlled encapsulated datagram service for carrying PPP packets. The PPTP Network server (NAS) runs on any operating system platform while the client, PPTP Access Controller (AC) operates on a PPP platform.

PPTP supports the Password Authentication Protocol (PAP) and the Challenge Handshake Authentication Protocol (CHAP) authentication methods:

- **PAP** – The Password Authentication Protocol (PAP) provides a simple method for the peer to establish a connection by simple two-way handshake as soon as the link is established.[3]

  PAP is not a strong authentication method. Passwords are sent over the link in a clear text (plain text) format, and there is no protection against playback or repeated packet attacks.

- **CHAP –** This is another protocol for authentication. The Challenge-Handshake Authentication Protocol (CHAP) is used to verify the identity of the remote user by a three-way handshake. After the link is established, the server sends the "challenge" message to the remote user, which becomes the first handshake. The remote user responds to the "challenge" using a one-way hash, which is the second handshake. If the response matches, then the authentication is acknowledged and a connection is established, which is the third handshake. Otherwise the connection is terminated. The CHAP protocol protects the network from playback or repeated packet attacks and controls the frequency and timings of the challenges.[4]

Other protocols include:

- MS-CHAP – Microsoft CHAP
- MS-CHAPv2 – Microsoft CHAP version 2 (and later versions)
- Extensible Authentication Protocol (EAP)

The PPTP protocol implementation is designed to use its own encryption algorithms, with an option to negotiate their own keys. However, DES (Digital Encryption Standard), triple DES, Rivest Cipher (RC)-4, and RC-5 are some of the other common encryption algorithms that are used by PPTP. The 128-key encryption algorithms are considered secure enough for VPN.

Layer Two Tunneling Protocol (L2TPv3)

A Layer Two Tunneling Protocol (L2TP) is an extension of PPTP protocol. It combines the features of PPTP and Cisco's L2F protocols. L2TP provides a transparent communication between the two end-users and applications across the intervening network. L2TP extends the PPP model by allowing Layer 2 protocol and PPP protocol to communicate with each other, interconnected by a packet-switched network. When a user sends the connection request, it first connects to an access device (L2TP Access Concentrator) such as a modem, ADSL, or DSLAM, and then the access device tunnels the PPP frames to the NAS (Network Access Server). [5]

Generic Routing Encapsulation (GRE)

Generic Routing Encapsulation (GRE) tunneling protocol encapsulates one IP datagram within another IP datagram and transports the encapsulated IP datagram. In other words, GRE encapsulates one network layer protocol with any another network layer protocol. The general specification is described in RFC 2890.[6]

A typical GRE datagram is shown in Figure 12-8. A network layer packet, called the "payload" packet is encapsulated in a GRE packet, which may include all the routing information of the network payload packet information. The resulting GRE packet is further encapsulated in some other network layer protocol, called "delivery protocol," and then forwarded to the transmission inside the VPN tunnel.[6]

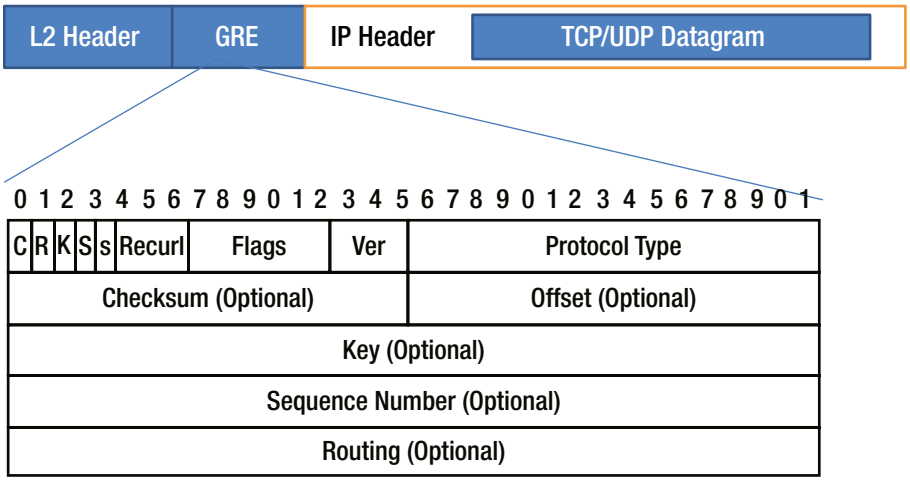

Figure 12-8. *Format of a GRE[6] encapsulated packet*

Internet Protocol Security (IPSec)

The goal of the IPSec is to provide security services for the IP layer, in both IPv4 and IPv6 protocols. *IPsec provides cryptographically designed security services for IPv4 and IPv6 protocol.* [7] IPSec security services cover data confidentiality, data integrity, authenticity, and anti-replay protection for the network traffic.

IPSec is a complex framework consisting of many protocols that provide a flexible set of security features. Toward this end, IPSec uses two main security protocols, the Authentication Header (AH) and the Encapsulating Security Protocol (ESP). The IPSec framework has two modes: the tunnel mode and the transport mode. In tunnel mode, an entire IP packet is encapsulated inside another IP packet. In transport mode, only the IP packet header is modified.

The Authentication Header (AH) supports data integrity, authentication, and optional anti-replay services. The Encapsulation Security Payload (ESP) provides data confidentiality (encryption). Together, AH and ESP provide the full set of security features for IP protocol and these are configured in a data structure called Security Association (SA). To summarize, the main functions of IPsec are Authentication, Encryption, and Key Management.

IPSec RFC 4301, Security Architecture for IP, consists of the following:[8]

- Security Protocols – Authentication Header (AH) and Encapsulating Security Payload (ESP)
- Security Associations – what they are and how they work, how they are managed, and associated processing
- Key Management – manual and automated (The Internet Key Exchange (IKE))
- Cryptographic algorithms for authentication and encryption

IPSec Tunnel and Transport Modes

IPSec is configured in two modes:

- Tunnel mode: is used between two gateways, or between a host and a gateway, with the gateway acting as a proxy for the host behind it.

Transport mode: is used between two end stations or two hosts.

The Authentication Header (AH)

The Authentication Header (AH) protocol provides authentication of the origin and integrity of the datagram transported between two systems. Data integrity in IPv4 is achieved through the CRC check. If a CRC error is detected at the destination, it means that the IP datagram has been changed during the transmission. The same concept is used in AH protocol, except, instead of using a simple algorithm, it uses a special hashing algorithm and a unique key known only to the sender and the receiver. This key is exchanged during the initial phase of connection establishment and Security Association (SA) is established between the two devices to know how to perform the computation of the algorithm using the unique key that has been exchanged during the initial phase, which none of the other systems can perform. On the source device, AH performs the computation and updates the results in the Integrity Check Value (ICV) field of the AH header and the datagram is transmitted. The destination device decrypts the message with the key, if there are no errors in the transmitted datagram.

Some fields of the IP header change during transmission (for example the fragmentation flag), and this change is not predictable during transmission. Hence, such fields are not covered as part of the AH authentication process. AH provides authentication for most of the fields of IP as well as the next level protocol data thus rendering protection provided by AH as partial.

It is important to note that the original data is not changed either by the checksum value or ICV value. Thus, AH performs only integrity check and not privacy (privacy is handled by ESP). The protocol header (IPv4 or IPv6) preceding the AH header SHALL contain the value 51 in its protocol (IPv4) or next header (IPv6) fields. Figure 12-9 illustrates the AH header format.[9]

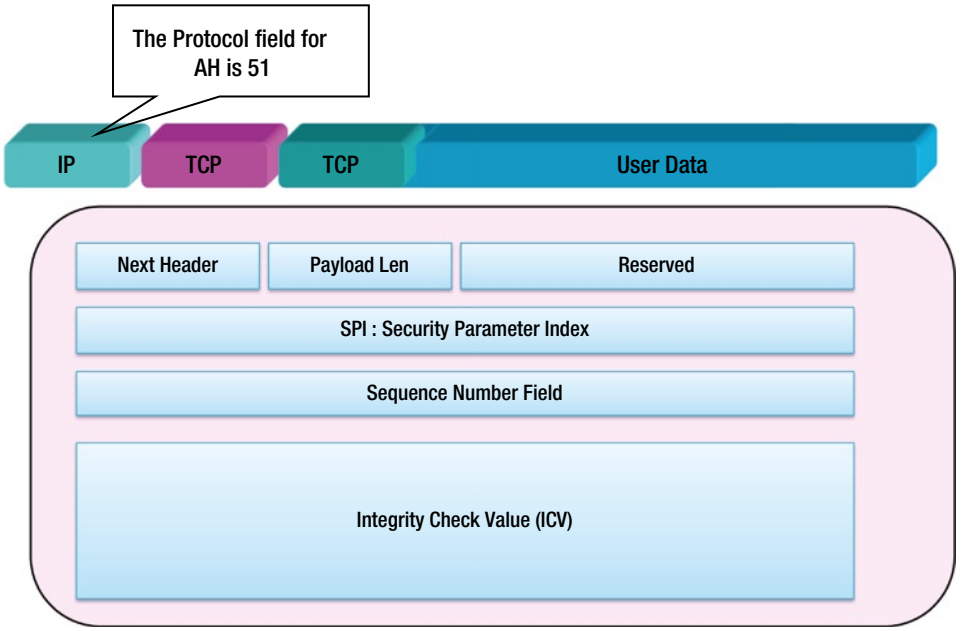

Figure 12-9. *AH Format*

With transport mode, the source IP address fields are not modified as shown in Figure 12-9. The authentication header is added after the original IP header. In tunnel mode, a new IPv4 header is encapsulated in the original IPv4 packet, as shown in the Figure 12-10.

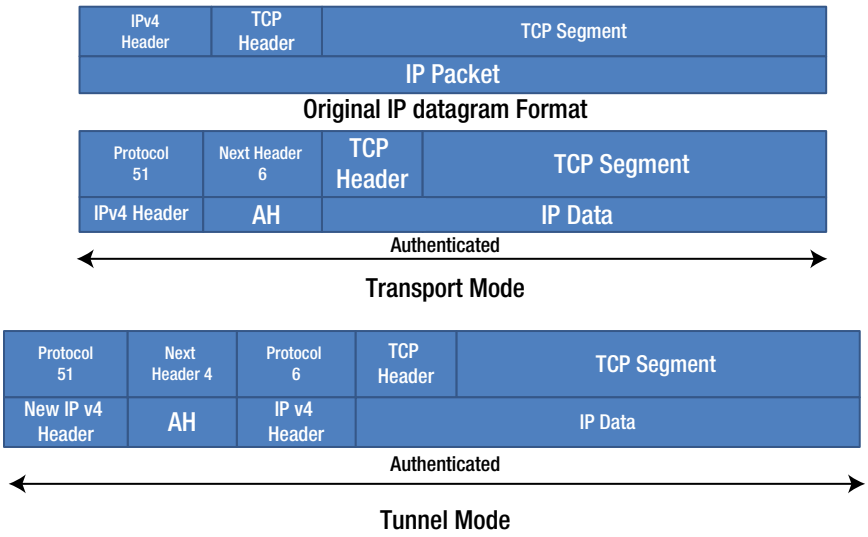

Figure 12-10. *AH Header*

AH uses Hashed Message Authentication Code (HMAC). VPN uses either HMAC-MD5 or HMAC-SHA. But SHA is regarded as more secure because of its large hash length. HMAC-MD5 is defined in RFC 2085, HMAC-SHA is defined in RFC 2404. The details of all the RFCs are given at `http://tools.ietf.org/rfc`.

The Encapsulation Security Protocol (ESP)

IPSec provides data confidentiality services through Encapsulating Security Payload (ESP). ESP may be applied alone or in combination with IP Authentication Header (AH) as described above. Confidentiality is provided by encryption algorithms and confidentiality of the data is between two hosts, two security gateways, or a gateway and a host.[10] The ESP header is illustrated in Figure 12-11.

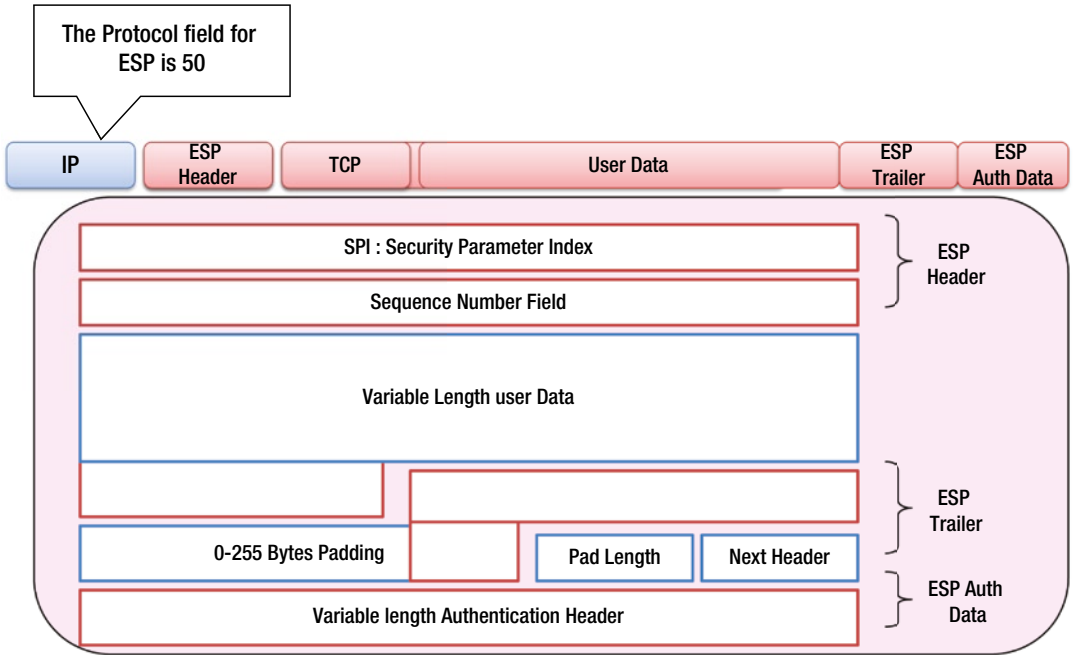

Figure 12-11. *ESP Header*

The encryption algorithms used by ESP are specified by the SA during the negotiation phase. ESP is designed for use with symmetric encryption algorithms. Since IP packets arrive out of order, each packet must have enough information to allow the receiver to establish cryptographic synchronization.[10] ESP uses a shared key for encrypting and decrypting the data, which is exchanged between the two parties.

Figure 12-12 shows the difference between the transport mode and the tunnel mode. In the transport mode, the IP payload is encrypted and the original headers are left intact. In the tunnel mode, the entire original IP datagram is encrypted. However, the new IP header is not included in the authentication mechanism.

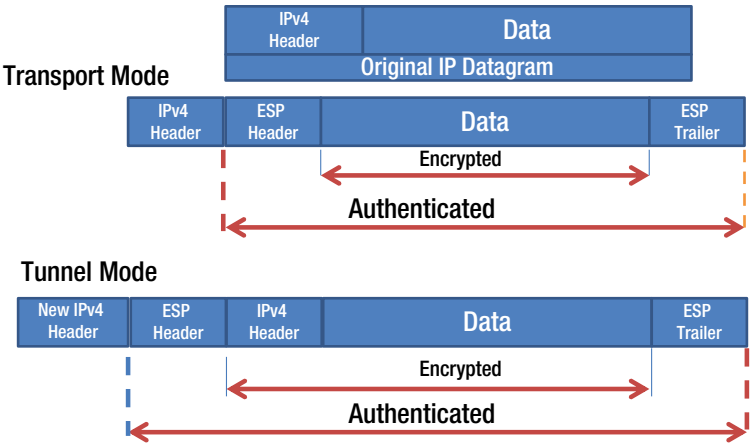

Figure 12-12. *ESP Header – Transport and Tunnel Mode*

ESP uses a symmetric key to encrypt and decrypt the messages. The standard symmetric key algorithm used in IPSec VPN are DES, triple-DES, RC5, RC4, or Advanced Encryption Standard (AES). Whatever the cipher being used, it should be interoperable among IPSec products. RFC 1829 defines DES, RFC 1851 describes 3DES. These RFCs can be downloaded at http://tools.ietf.org/rfc. Other algorithms are MD5 and DES-CBC (Cipher Block Chaining).

Internet Key Management (IKE)

Before a secure transmission can begin, both the sender and the receiver need to negotiate on the keys, which are defined in the Security Association (SA) document. The AH protocol is used for authentication and integrity, the ESP is used for privacy. In both the AH and ESP protocols, both the parties exchange "secret" keys. This exchange of keys happens through a protocol called IPSec Key Exchange (IKE) protocol as defined by RFC2409.

IKE is meant for establishing, negotiating, modifying, and deleting SAs. IKE performs authentication between the two parties and establishes Security Association (SA) by exchanging the secret key that can be used to establish SAs for both AH and ESP protocols and a set of cryptographic algorithm that is used by the SAs to encrypt and decrypt the messages (payload).[11]

MPLS (Multi-Protocol Label Switching)

MPLS is the latest core technology providing the next-generation WAN connectivity, in particular for the optical networks. As a packet travels from one network to another network, each router in that network makes an independent decision on how to forward the packet based on the routing table entries. As the packet enters the router, the router analyzes the packet header and based on its destination address, it looks at the routing table and forwards the packet to the designated interface (network). This process is repeated at each hop. The disadvantage of this process is that every time a packet arrives, the router has to repeat this "table lookup" and if there are more than two packets to the same destination network, the router still has to look up the routing table twice.

The router assigns the packets to the next hop, which can be thought of as a function of two components. The first component could be partitioning an entire set of packets into what is called as "Forward Equivalence Classes (FECs)" and the second is to map each FEC to the next hop. In conventional IP forwarding, each packet header is analyzed and a routing decision is made at each hop, which is time consuming and process intensive.

In case of MPLS[12], the assignment of FEC to a particular packet is done only once, as soon as the packet enters the network. MPLS-Label format is as shown in Figure 12-13. The FEC is given a short, fixed-length value known as a "label" and the label is forwarded along with the packet. When the packet enters the next hop, just the label is analyzed and no further analysis of header is done in subsequent routers. All forwarding is done using "labels." This has a number of advantages over the traditional network layer forwarding apart from faster processing and speed.

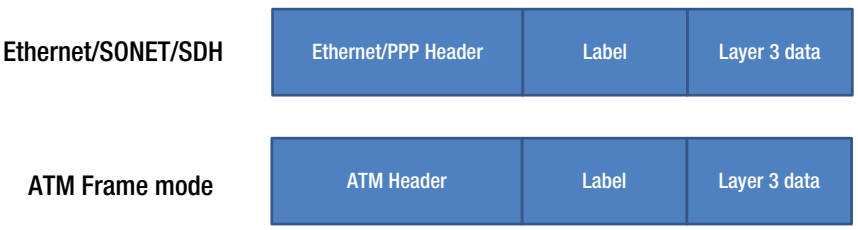

Figure 12-13. *MPLS – Label Format*

The advantages of MPLS networks include:

- MPLS forwarding can be done by L2 layer switches which have capabilities to read MPLS labels but are not capable of analyzing L3 (network) layer headers
- Quality of Service (QoS) - MPLS allows prioritization of traffic, allowing high-priority traffic first on the network then the lower-priority traffic. MPLS networks assign higher priority for latency-sensitive applications like voice and video over less-sensitive applications
- Improved performance, reliability, and efficiency of the network
- MPLS VPNs and VPLS services enable multiple sites to connect seamlessly

MPLS VPN

The main disadvantage of VPN networks is interoperability. The VPN connections are tied to one vendor or one Internet Service Provider (ISP). Many of the IP-based VPN solutions also require encapsulation of IP or double encapsulation of IP. This requires additional processing overhead at the entry and exit of ISP networks.

With MPLS networks, this can be overcome. Intermediate MPLS switches need not process the IP headers, in particular, the destination IP addresses in the packets are not examined, which enables MPLS to offer an efficient mechanism to forward the encapsulated data on the ISP backbone network. MPLS also has greater control over network parameters such as latency, bandwidth, and availability. Hence, MPLS VPN has emerged as a trusted WAN connectivity than the normal IP-based connectivity. One of the major advantages of MPLS VPN is that instead of managing point-to-point connections between multiple branch offices, now MPLS VPN customers need to provide only one connection from their corporate LAN to all other branch offices.

Traditional VPN technology depends on tunneling protocols such as GRE, L2TP, and PPTP whereas MPLS itself is a tunnel over public networks. Therefore, implementation of VPN over MPLS has better advantages. MPLS based VPNs connect geographically spread branch offices of a private network using LSP (Label Switch Path).[12]

Figure 12-14 shows the basic architecture of MPLS-based VPN. There are two components in the architecture, Customer Equipment (CE) and Service Provider Equipment (PE). A CE can be a router, switch, or host. PEs are part of the backbone network. PE is responsible for managing VPN connectivity, VPN users, and establishing MPLS LSP connections (VPN tunnel) between PEs and allocating routes among different branches of the same VPN.

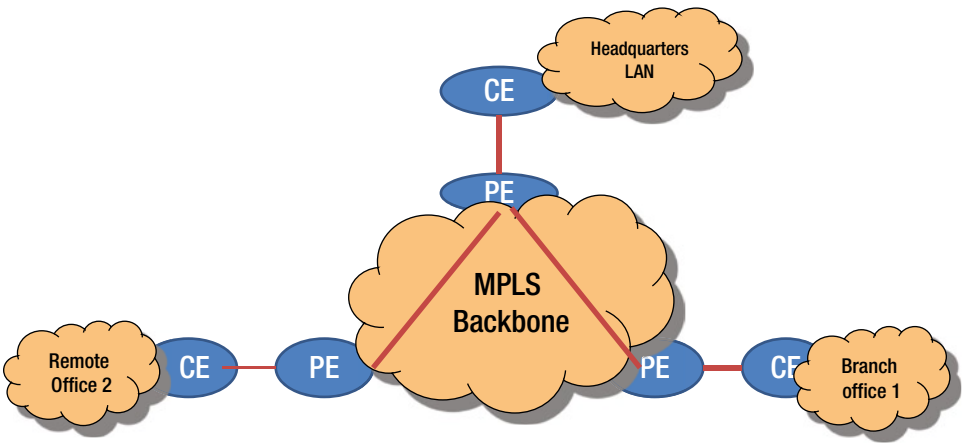

Figure 12-14. *MPLS-based VPN*

MPLS VPN Security

Customers expect their data to be secured across the VPN tunnel. VPN implementation based on ATM and frame relay provides secured VC (virtual connections) by virtue of connection-oriented network. However, IP based VPNs rely on cryptographic means to provide security and authentication. MPLS VPN security[13] is achieved through:

- Ingress SP router assigns a unique VPN ID to each destination thus ensuring private connection between two users
- Any other packet entering the MPLS backbone network without a label or a different label not in the MPLS network will be discarded
- SP routers can use the MD5 or similar technique to encrypt the labels of MPLS thus providing additional security
- If the customer wants to send data that is very sensitive and must be protected, then IPSec or similar protocol can be adopted

Important IETF Standards and RFCs for VPN Implementation

Some of the important Internet Engineering Task Force (IETF) standards and RFCs for VPN implementation are summarized in the Table 12-2. This is not a comprehensive list. For more details, you can refer to VPN consortium home page at http://www.vpnc.org.

Table 12-2. *Important IETF Standards and RFCs for VPN Implementation*

VPN Protocol Category	RFC No.	Description of RFC
Tunneling Protocol	2661	Layer Two Tunneling Protocol (L2TP)
	2637	Point-to-Point Tunneling Protocol (PPTP)
GRE	2890 (Obsolete 2784)	Generic Routing Encapsulation
ESP	4303 (Obsolete 2406)	Encapsulating Security Payload (ESP)
AH	4302 (Obsolete 2402)	IP Authentication Header
IPSec	4301 (updated 6301) (Obsolete 2401)	Security Architecture for the Internet Protocol
	2411	IP Security Roadmap
	2764	A Framework for IP Based Virtual Private Network
	4891	Using IPSec to Secure IPV6-in-IPV4 Tunnels
	5265	Mobile IPV4 Traversal across IPSec-Based Gateways
IPSec Key Exchange	4306	Internet Key Exchange Protocol (IKEv2)
	2408	Internet Security Association and Key Management Protocol (ISAKMP)
	RFC 2409	Internet Key Exchange (IKE)
	RFC 2412	OAKLEY Key Determination Protocol

(*continued*)

Table 12-2. (*continued*)

VPN Protocol Category	RFC No.	Description of RFC
MPLS	4381	Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs)
	4364	BGP/MPLS IP Virtual Private Networks (VPNs)
	4111	Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)
Cryptographic Algorithm	2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
	2104	HMAC: Keyed-Hashing for Message Authentication
	2403	The Use of HMAC-MD5-96 within ESP and AH
	2410	The NULL Encryption Algorithm and Its Use with IPsec
	3173	IP Payload Compression Protocol (IPComp)
	3051	IP Payload Compression Using ITU-T V.44 Packet Method
	3602	The AES-CBC Cipher Algorithm and Its Use with IPSec
	3686	Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)
	4196	The SEED Cipher Algorithm and Its Use with IPsec
	4894	Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec
	4312	The Camella Cipher Algorithm and Its Use with IPsec
	4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
	4615	The Advanced Encryption Standard-Cipher-based Message Authentication Code-Pseudo-Random Function-128 (AES-CMAC-PRF-128) Algorithm for the Internet Key Exchange Protocol (IKE)
	4634	US Secure Hash Algorithms (SHA and HMAC-SHA)
	4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-512 with IPsec.

A Few Final Thoughts about VPN

The Internet is not a safe place. It has every kind of network and every kind of system and every kind of people – good or bad. In order to keep your information safe while transmitting over the Internet, VPN technologies using PPTP, L2TP, IPSec, MPLS, SSL, or other protocols support the following:

- Confidentiality
- Authentication and Data Integrity
- Replay protection

Authentication is used to prevent unauthorized users gaining access to the secured network. Some of the common and traditional algorithms used for the authentication process are PAP (Password Authentication Protocol), CHAP (Challenge-Handshake Authentication Protocol). The newest authentication protocol is EAP, Extensible Authentication Protocol and an extension to EAP is EAP-TLS, EAP-Transaction Level Security. A "Replay" attack is when the attacker taps into the network, hears the conversation, and captures the packets and "replays" those packets to gain access. For example, if the packet is sent for authentication, then the attacker system captures the packet, reads the content, and identifies, say the password field, and the destination address, and then the attacker "replays" the same packet just by changing the source address and tries to gain access. To protect from such attacks, passwords also must be protected.

Encryption is meant to protect the confidentiality of data. A secret key is used to encrypt and decrypt the message. There are two types of encryption key mechanism - symmetric and asymmetric. In symmetric, the same key is used for encrypting and decrypting the messages. In asymmetric encryption, there are two keys – a public key and a private key. Using the public key, data is encrypted and the data is decrypted using the private key. The standard algorithms used for data encryption are the DES and the RSA. RSA is much faster than DES and has become a de-facto standard for high-speed data encryption.

VPNs allow remote sites, small offices, and branch offices to connect to the corporate network over a public network (Internet), while maintaining secure communications. VPN technologies are designed to address the current business needs and trends toward increased telecommuters and mobile and wireless users who are outside of the corporate network but need to connect over cell phones, smartphones, handheld devices, and notebooks distributed globally but at the same time providing a cost-effective solution. However, VPN may not be a good solution where latency and slow performance is not acceptable.

Recent years have seen the growth of several VPN technologies and services. With the advancement in Internet and Internet technologies, these new VPN services work on the same physical infrastructure as much as possible. Traditionally, the remote access services were built on dial-up. However, ADSL, cable modem, and wireless access have become more popular, making dial-up somewhat obsolete. Hence, to support these new access technologies, IPSec and SSL-VPN have evolved.

Service providers typically have a backbone network which is the ATM, Frame relay, or IP network based on MPLS technology. MPLS-based VPN technology has gained popularity because of MPLS's widespread deployment. MPLS-VPN has been deployed as a value-added service by the service providers to provide security services.

Mobile wireless technologies and Wi-Fi technologies are gaining momentum and the Internet can be accessed through your mobile device anytime, anywhere. Most hotels provide Wi-Fi hotspots. So, the corporations need to provide a technology to access their corporate network on these platforms but still need to keep the security in place. Most of the ISPs and the Wi-Fi hotspot routers allow very specific ports such as HTTP, HTTPS, POP3, and SMTP.

SSL-VPN/Web SSL VPN offers a complete, reliable replacement to IPSec remote access with its clientless, web-based architecture. SSL-VPN can offer connections restricted to a specific application by incorporating highly flexible authentication and authorization mechanisms and thus gaining wide acceptance.

While designing VPN technology, it is important to keep the following points in mind:

- VPN accelerator devices should support keys that are sufficiently long enough. A 128-bit key is certainly long enough but not all the devices support it.
- Even with the VPN technologies, it is possible for a hacker to insert bits into the data stream during transmission. IPSec has a mechanism to detect data integrity whereas others may have limitations in this area.
- It is important for the end devices to interoperate. IPSec at both ends should support the same type of AH and ESP algorithms and key length. Otherwise, communication itself may not be able to be established.

Chapter Summary

- The business need for connecting to organizational data centers securely from outside teams, such as sales and marketing and logistics, was explored. As most of the information that's transmitted needs to be secure, we looked into the option of having a dedicated line. We discussed how it is costly to have and maintain a dedicated line. We also discussed the disadvantages of having a dedicated line. Then we discussed a cheaper alternative, Virtual Private Network (VPN), which allows for the privacy, integrity, and authenticity of the data being transmitted by the internal team resources from outside the organization. VPN is a secure tunnel created between outside trusted partners including the internal workers working from outside the organizational boundaries and the internal networks.
- We looked into the benefits of VPNs, including cost savings, smooth and seamless integration, secure remote access, extranet connections, and low maintenance.
- We discussed the two important types of VPNs: Remote Access (Host to Site) and Site to Site. We discussed how Remote Access VPNs help the organizational work force operating from outside the organization to connect securely to the corporate LAN. We also looked into how this is implemented and how a secure tunnel is established to the external workforce and the organizational internal network, after authentication to the VPN gateway. Then we explored how site-to-site VPNs help one branch office to connect to the other branch office or headquarters and how this is established through the handshake between two VPN gateways at two ends. Then we looked into two types of site-to-site VPNs: intranet-based VPNs and extranet-based VPNs. We also looked briefly into how host-to-host VPNs work.
- We also discussed how VPN protocol architecture supports tunneling, data authentication, data integrity, data encryption, and anti-replay services. We then explored each of the protocols like point to point transport protocol (PPTP), layer two tunneling protocol (L2TPv3), generic routing encapsulation (GRE) tunneling protocol, and Internet protocol security (IPSec) in detail. We also looked into the need for Internet key management and how it is ensured.
- Finally, we highlighted some of the points to be kept in mind when designing the VPN technology.