Technical report, IDE09, March 2009

Security in Private Branch IP-Telephony Network with QoS Demands.

Master's Thesis in Electrical Engineering

Imran Akbar, Khurram Shahzad

School of Information Science, Computer and Electrical Engineering

Halmstad University

Security in Private Branch IP-Telephony Network with QoS Demands.

Master's thesis in Electrical Engineering

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

March 2009

Abstract

At the moment the demand for IP Telephony is increasing because of its scalability and efficient use of bandwidth. The main issues are security and quality of voice in IP Telephony .The study comprises previous research papers and, on the bases of those papers, comparison is made between two security techniques, IPSec VPN and MPLS VPN. The goal behind this study is to build an IP Telephony setup, with security for private branch network, which is an ISP. IP Telephony networks are currently facing issues regarding security and competent packet switching.

The comparison further describes that MPLS VPN technique is more scalable and efficient than IPSec VPN, which has been approved in implementation. In the implementation, one centralized call manager is configured to establish calls between different sites. To secure traffic over the internet which travels from one site to another other site, MPLS VPN is configured in MPLS domain. In order to increase the performance of IP Telephony, quality of service (QoS) is implemented. QoS provides thriving outcomes and it is also practically implemented in the lab. QoS enhances the flow of data by prioritizing the voice packets. At the end, it is concluded that MPLS VPN is more efficient and scalable than IPSec VPN, and shows better results, while completely supporting QoS.

Table of Contents

Tables and Figures.

Chapter 1

1.1 Introduction

Voice over packet switched network is the example of IP Telephony or Voip transmission that has become the emerging trend in modern telecommunication. IP telephony transfers voice traffic over the Internet protocol (IP). Convergence creates many new sets of security problems. Convergence means to combine voice and data to work as a single network. This view is supported by Winn Schwartau "The communications world is moving toward VoIP but does not have the security expertise it needs in-house to meet the real-world stress it will encounter" [1].

The deployment of IP Telephony, and its usage as a practical solution for cost effective communication choice, is challenged via management and security requirements. There are different attacks upon IP Telephony networks such as spam over Internet Telephony (SPIT), call hijacking, denial of service, and fraudulent usage. The current defense systems are inappropriate to block these attacks. IP based solutions and converged networks are also vulnerable to different threats, which need to be understood and managed. Therefore new theoretical and practical solutions for securing and managing IP Telephony are required from the research community.

In this thesis, different security techniques are discussed, but mainly two techniques, IPSec VPN and MPLS VPN, are comparatively studied. In the end the best scalable technique MPLS VPN is implemented with QoS. QoS is used to provide different services to various applications. Voice traffic is a real time data; it can be affected by different parameters, i.e. delay, jitter, and packet loss. A high-

quality IP telephony solution must be properly designed, configured, and managed with QoS [1][2][3].

1.2 Motivation

The most important task in this research is to provide security, scalability and efficient flow of data in IP Telephony network. There are different kinds of user personal information, and business cooperation details in the users accounts. So it is very important to secure it from different attacks. The idea for this thesis came from an organization, Gujranwala Online (GOL), working as internet service provider (ISP). The company is planning to add a new service in the running setup namely IP-Telephony. GOL provides different services such as dial up, DSL, dedicated bandwidth for organizations, web domain and hosting. The work has been divided in two parts. Firstly it is to deploy IP Telephony service for their own offices located on different locations. Secondly, it is to provide IP-Telephone service to different customers. Both tasks have to be completed with security.

The following research provides a solution about the first part, which is to provide IP Telephony service in the current setup. IP Telephony is going to be added as a separate service for voice communication. Therefore it is necessary to come up with a security solution over the wide area network which supports IP Telephony. The task is to select a security technique, which offers maximum-security features and efficient flow of data in the network. Hence, these are the factors in motivating the following thesis.

1.3 Goal

The main goal for the project is to find the number of attacks in IP Telephony network and compare IPSec VPN and MPLS VPN. When security is implemented, the packet size will be increased and, because of this, there will be more packet loss

and less efficient data transmission. To overcome this problem, QoS is implemented. It is also a part of the project to understand how IP Telephony works and which equipment is used to setup IP Telephony network.

Main goals are:

- To build a secure and scalable converge network.
- To optimizing network bandwidth by deploying both voice and data communication on the same network to save network resources.
- Test and compare IPSec VPN and MPLS VPN.
- To accomplish an efficient network.
- To reduce packet loss and increase the productivity of the network while using QoS.

1.4 Description of the Implementation:

The picture below demonstrates about the implementation. It contains two parts, namely user control part and ISP control part. In user control part, the users are controlled locally through local routers known as CE-1 and CE-2. One call manager is configured to establish and tear down calls. The other part is called ISP domain, in which the user cannot control anything. ISP domain contains different routers, known as provider edge routers (PE-1, PE-2) and P routers. In ISP domain, only edge routers take part in routing decisions and P router just take packets from edge router swap lable of the next router and forward it. One monitoring server is used to calculate the interval of the call and quality of the call. There are also different IP phones are used to make calls. The detail of the implementation is given in the eighth chapter.

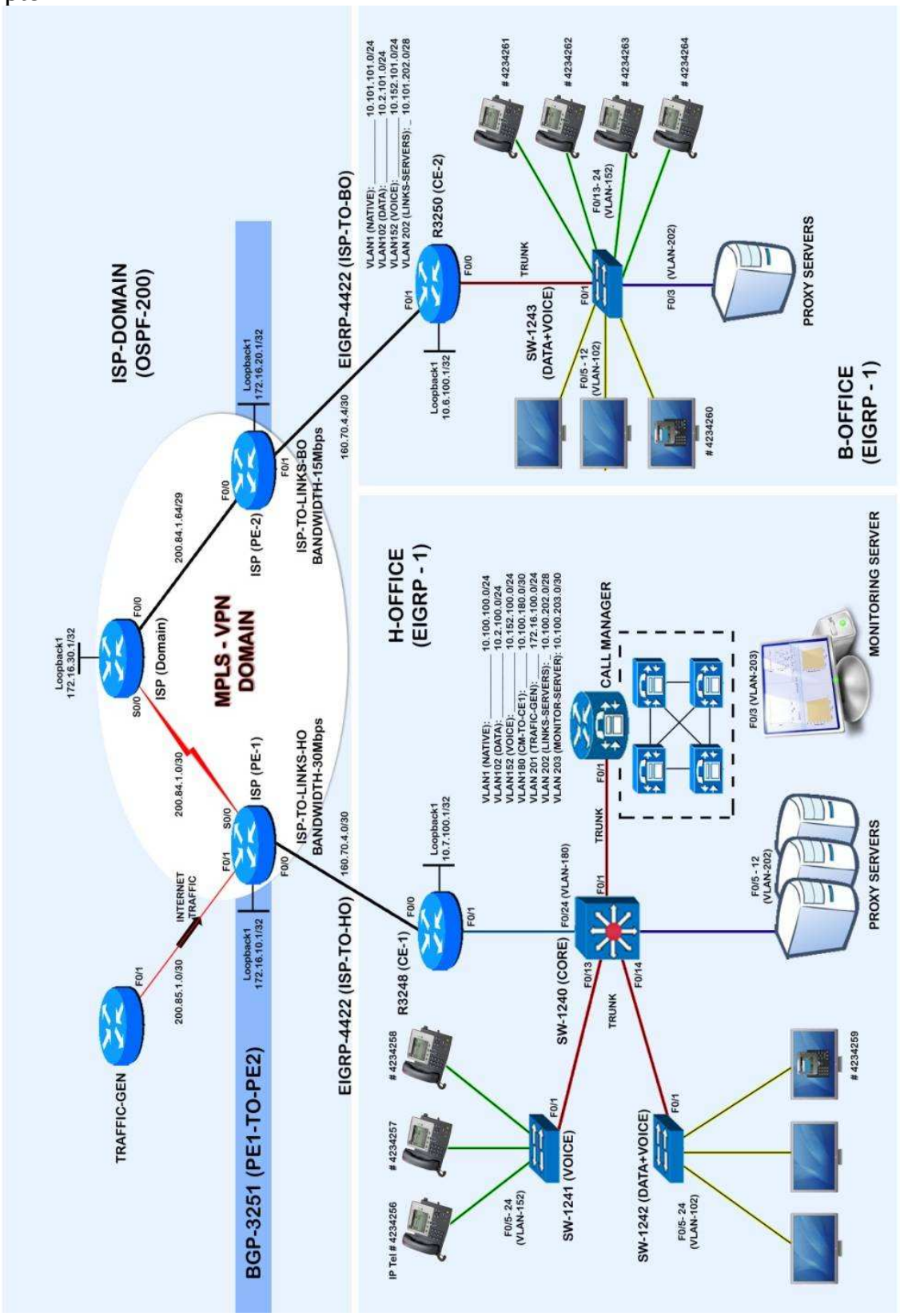

Figure 1.4: Implementation of IP Telephony, MPLS VPN with QoS.

1.5 Description of the Project

The Plan is to provide an efficient and secure IP Telephony solution for organizations. The core theme of the project is to deploy IP Telephony in the already functioning ISP. Many enterprises, whether large or small, are now considering implementing IP Telephony systems and services in their networks. After the implementation of IP Telephony the question arises as to whether it is secured or not. It is also important to check the quality of voice which is affected by delay, jitter and packet loss. Telecommunication requires security for sensitive voice data. The Internet on the other hand is an unsafe and insecure media. Therefore methods for securing IPT are necessary to ensure user acceptance of this new service. Since IP telephony uses the existing IP network as its foundation, attacks on this data network can also adversely affect voice services.

1.6 Methodology

The methodology of this research is mixed; it involves both theoretical comparison and practical implementation. The concept of the research is taken from an ISP known as GOL. To execute this concept, the whole material is obtained from research papers. The comparison is being made after extracting the useful information from previous research papers. The comparison provides the foundation for implementation. Implementation is done with available equipment, detail is given in the chapter eight and configurations are presented in the appendix.

1.7 Background

After the innovation of IP Telephony, the organizations wish to implement IP telephony in their network because it is a scalable and efficient way to transmit data. Before implementing IP Telephony, there was a perception that voice and data cannot be converged together for this reason they have worked separately for a long

time. But after the implementation of IP Telephony, voice and data are working together.

The major concern is security in the IP Telephony setup. There are many threats, such as DoS, DDoS, Spoofing and man in the middle attack which are continuously affecting IP Telephony network. So it is very important to tackle the security problems. There are two kinds of security domains, one is the local area network and the other domain is wide area network. To secure a local area network, different security techniques can be deployed to survive various attacks e.g. port security, firewall, NAT, PAT etc. There are also techniques to secure wide area networks like IPSec VPN, MPLS VPN etc. The main theme is to secure wide area network traffic. Through these security techniques, it is possible to restrict unauthorized users to use the services of IP Telephony setup [4,5].

Chapter 2

2.1 IP Telephony/VOIP Overview

Voice over IP is also called VOIP. VOIP is also referred to as IP Telephony. Both networks send data or voice while using IP network. The main difference between these two is around the end points in use. In VOIP, network traditional digital or analog circuits are used to connect with an IP network while using a gateway. In IP telephony networks the endpoints communicate using IP. IP Telephony sends voice packets with the use of IP network including internet. IP Telephony has made it possible to combine both data and voice network to work together saving money.

VOIP services convert voice into digital form that can be transmitted over an IP network. When dialing a traditional phone number it is then converted into traditional telephone signals first and transmitted to destination. To make a call, VOIP facilitates the use of a computer, using VOIP phone or traditional phone but IP telephony restricts the users to use IP phones to make the calls.

2.2 VOIP/IP Telephony Components

- IP Phones
- Gatekeeper
- Gateway
- Multipoint Control Unit (MCU)
- Call agent
- Application servers

2.3 VOIP Function

The elements used to make a call in the traditional network are transparent to the end user. When migrating to IP Telephony/VOIP an awareness of the needs of protocols and also components that provide the similar functionality in IP network.

2.3.1 Signalling

Signalling is the process of generating and exchanging control information that will be used to set up and monitor the connections between the end points. Voice signalling needs address and alerting function between the end devices. Traditional network (PSTN) uses signalling system 7 (SS7) to transmit control messages. SS7 uses out-of-band signalling, the out-of-band signalling is to exchange control information in a separated dedicated channel [23].

There are different protocols used for signalling. These are Skinny Client Control Protocol (SCCP), Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), and H.323 protocols. The VOIP/IP Telephony gateways are also able to initiate the signals to PSTN network. There are two classifications of signalling protocols: peer-to-peer and client/server protocols.

Both SIP and H.323 are peer-to-peer signalling protocols. In these protocols, the gateways initiate and terminate the calls. MGCP, SCCP, and H.248 are client/server signalling protocols. Here gateways or end devices, are unable to control the call information but send information to a server known as the call agent to do this task. When an MGCP gateway detects a phone which is off hook, it cannot provide a dial-tone. The gateway sends information to the call agent that the phone is off hook. Then call agent instructs the gateway to provide a dial tone.

2.3.2 Database services

Toll free numbers, or caller ID services, require the capability to query a database request. That determines whether the call can be positioned, or information can be completed and made available. Database perform different services

- Billing Access.
- Caller ID delivery.
- Toll free information's.
- Calling card services.

VoIP service providers can differentiate their services by providing access to many unique database services. For example, to simplify fax access to mobile users, a provider can build a service that converts fax to e-mail. Another example is providing a call notification service that places outbound calls with pre-recorded messages at specific times to notify users of such events as school closures, wake-up calls, or appointments.

2.3.3 Bearer Control

This is a voice call carry channel. It is based on call connection and call disconnection signals passed between end devices. The correct signalling guarantees that a channel is allocated to the running voice call and that the channel is de-allocated when either side terminates the call. In PSTN network, connect and disconnect messages are carried through SS7. Within IP network, connect and disconnect messages are carried through H.323, H.248, Sip, or MGCP.

2.3.4 Codecs

Codecs are required for the translation of analog signals into digital signals. There are different types of codecs which defines methods for voice streaming, and also compression techniques which are used to convert voice stream. Time division

multiplexing (TDM) is used to carry PSTN voice calls. In PSTN network, every channel reserves 64-bit bandwidth and uses G.711 codec to convert analog signals into digital stream. In VOIP network, codecs compress voice stream to make it a more efficient use of network bandwidth. In VOIP network G.729 codec is used that compresses voice stream to 8 kbps.

2.4 VOIP Signalling Protocols:

2.4.1 SIP

SIP protocol is used to set up calls and tear down calls. SIP also provides other features like proxy, security and TCP or UDP services. SIP, along with its partner protocols session announcement protocol (SAP), and session description protocols (SDP), provides information to multicast sessions of users in the network. The function of SIP is to provide end-to-end call signalling between the devices. SIP is a type of text-based protocol and borrows many features of HTTP; it uses similar header and response codecs. It also adopts a URL addressing scheme which is used in email, that is based on simple mail transfer protocol (SMTP). There are many applications which use SIP protocol for call setup and tear down. SIP is a more flexible protocol and is used for large networks [23].

Its applications are:

- Skype
- Voipwise
- Globe 7
- Internet calls
- Voip Cheap

2.4.2 Skype Features

Skype establishes peer-to-peer connection while using SIP protocol. It uses AES and RSA encryption techniques to encrypt the data. Skype is also able to call from skype to traditional telephony line, make skype to skype calls, use sms and text chat facility anywhere in the world.

- Voice mail facility.
- Call Forwarding
- Buddy List
- Conference call
- Video calling from Skype to Skype
- Online chat

In other applications like Voipwise it just provides the facility to call from Voipwise to traditional line. It also uses AES encryption to encrypt the data [24].

2.4.3 H.323

H.323 is a standard which includes protocols, components and procedures that provide multimedia communication services. It supports video, audio and data communications in packet switched network. H.323 is a part of international telecommunication union standardization (ITU-T) known as H.32X which provides communication services over different networks. H.32x is a collection of standards which define synchronization of voice, video and data transmission. It supports end-to-end call signalling between the devices.

2.4.4 Skinny Client Control Protocol

Skinny client control protocol (SCCP) is used for the communication of call manager and end devices, like IP phones. SCCP is a type of client server protocol. It means that any event, like on-hook or off-hook is causes to be sent to call

manager. As a response the call manager instructs the device what to do when this condition occurs. Therefore even a button is pressed, the data transmission starts between the end device and call manager. SCCP is mainly used with IP phones. The main benefit in SCCP is that it supports quick changes in the protocol and can also add different required functions. SCCP is the simplest protocol which is used in VOIP/IP Telephony networks. IP Phones which are using SCCP can work with H.323 together. SCCP is the preferred protocol for the IP telephony network and, in our setup, we are also using SCCP protocol for signalling.

2.4.5 MGCP

MGCP is a protocol to control the PSTN gateway. MGCP defines a method to control VOIP gateways which are connected to external devices known as call agents. This protocol provides signalling services even to less expensive edge devices like gateways. It works with the combination of H.323. When off hook occurs on the voice port of the gateway, the voice port sends information of the event to the call agent. The call agent signals the voice port while providing dial tone signalling. MGCP is a light protocol which is used for signalling with the combination of H.323 [23].

Chapter 3

3.1 Threats

This chapter attempts to outline the prospective of security issues faced during the transformation of traditional phone system into IP Telephony systems. The current analysis is provided to identify the impact of security problems in the converged network.

3.2 Man-in-the-Middle Attack

This is a form of active eavesdropping, in which the attacker makes independent connections with the different users. These users are communicating with each other, making them believe that they are talking directly to each other over a private connection but in fact the entire conversation is controlled by the attacker.

There are many issues created by man-in-the-middle attack.

- The rogue proxy can lead the user to deceive both the source and end user while using the IP Telephony services.
- It can collect extremely secret information, e.g. password of OS (Operating System), pin numbers of credit cards, and other types of personal information.
- This attack can be eliminated through secure socket layer (SSL) authentication [6].

3.3 Denial of Service and Distributed Denial of Service

The availability is significant for crucial services. In the conventional converged network, IP Telephony calls must be guaranteed with a high success rate for

providing prompt first-response services. DoS and DDoS are the main attacks for losing the availability. The main way to protect from DoS attack is to find the source of the attack and block that traffic. In the real scenario, DDoS attacks are more malicious than DoS in the network. IP Telephony allows these intruders to launch easily in many real-time networks. Therefore, the converged network has to face many challenges and has to find different kinds of tools to save it from these attacks. These kinds of attacks can be blocked through authentication, authorization, and accounting server (AAA) [6].

3.4 Application Attacks

During the deployment of IP Telephony, there are certain applications used in the converged network e.g. Web servers, Java applets and many more. These applications perform different functions. Java applets are run on IP Phones to provide some additional functions. Web services are used to manage security and the deployment of large networks. To secure the network from these application attacks, these applications must be analyzed for vulnerabilities before deployment in the critical infrastructure [6].

3.5 Conversation Sniffing

The confidentiality of conversation is necessary for several important applications. IP Telephony can be sniffed if both signaling traffic and media traffic are not properly secured. The confidentiality and integrity are the key requirements to provide IP Telephony services. The confidentiality refers to ensure the privacy of information which is exchanged among different users. The integrity ensures that the information exchanged is not tampered during the transmission. Different techniques exists which can be used to guarantee the integrity and confidentiality of IP Telephony phone calls. IPSec can be utilized, either in tunnel mode or transport

mode, for an overall authentication, integrity and confidentiality in the IP Telephony network. The real time protocol (RTP) can also be used for compression of media streams [6].

3.6 Introduction of Unauthorized Component

Components used in IP Telephony network must be secured through any security method. When deploying the components, it is necessary to define the rules related to the users. Rules for every user must be defined like authentication and authorization to use the different equipment. Not all users have the same rights to use the same equipment. During the installation of new components, authentication must also be set to make it more secure. Only valid users can use a particular device. In this way, components can be made more secure [6].

3.7 Rogue Sets

This type of attack is used by an attacker to get the access to other people's resources. After getting the access of resources the intruders simply add any VoIP application to make long distance calls. To overcome this problem, the network administrators use a technique known as a lock down mechanism. Only network administrators can add any VoIP application in the network. When any application is added, the logs are sent to the administrator. The VoIP application will be rejected when any user gaines illegal access of network and tries to add any application to make the calls. When more than three attempts are made then that user authentication is blocked [7].

3.8 Toll Fraud

Toll fraud attack is to establish unauthorized calls while using company's resources. This type is related to rogue sets gaining illegal access of resources and then making long distance calls. The user can utilize different services of IP

Telephony, like return calls from voice mail and call forwarding and trunk to trunk transfers to make calls on external numbers. To overcome this problem, an authorization mechanism is used. It means rogue devices will require authorization to gain access of the devices and to make calls. The administrator defines a group of users and policies and these policies are applied to certain users to establish calls [7].

3.9 Dynamic Host Configuration Protocol

Dynamic host configuration protocol (DHCP) attack is used to send many requests to DHCP server. It forces the server to issue all the addresses. The main purpose of this attack is to spoof DHCP replies. Then the attackers have more points to attack and the DHCP server will not able to respond against the requests. IP Telephony devices will respond and provide correct information to the user. This creates attacks like the DoS and the man in the middle attack. To protect from this attack it is suggested that static IP addressing must be used in the network [7].

3.10 Spam Attack

Like spam emails, the spam messages create problems in the IP telephony network while consuming the bandwidth. Because of spam in the telephony network, delay is increased. In spam, messages are flooded over the entire network like traditional email. It consumes bandwidth, which is not scalable for the running real-time communication network. To block spam messages, it is recommended to utilize anti-spam software [7].

3.11 Reconnaissance Attacks

This is the unauthorized detection and mapping of systems, services or vulnerabilities of a network. This attack is utilized to gather information and provides base for DoS attacks. In the beginning, ping sweep is used to determine

the addresses which are live. Then the intruder gets information about the active ports on the live addresses. Commencing this information, the attacker sends the query to establish the operating system and applications running on the desired node. The reconnaissance attack consists on the following:

- Ping Sweep
- Port Scan
- Packet Sniffer
- Internet Information Queries

The ping sweep is a basic network scanning procedure that determines the range of IP addresses assigned to live nodes. The ping sweep consists of echo requests that are sent to multiple nodes. If any address is live, then it will respond back. This technique is old and slow to scan a network. Many requests are sent to a range of addresses to discover which hosts can be probed for vulnerabilities.

The port scanning is a collection of messages that are sent by intruders while attempting to break into the system to ascertain which services are running in the network. Every service is linked with a distinct port number. It can be an automated scan of a range of UDP or TCP ports on a computer to acquire listening services. Port scanning is a preferred technique to attack on a network which provides the weak points of a network. Basically, a port scan consists of sending a message to every port, but one port at a time. The sort of reply that the sender receives shows whether the port is active and can be probed as a weak spot.

The packet sniffer is a software-bases application, which uses a network adapter card in the promiscuous mode to get network packets that are sent across the network. The packet sniffer does work in the same domain area as the network being attacked. The promiscuous mode is a kind of mode in which network adapter

card forwards all voice and data packets that are received on the physical network wire to a software application for processing. The plaintext data is not encrypted although few network applications distribute packets in plaintext. As the network packets are not in the encrypted form, these can be processed and can be understood by any application that picks them off the network and processes them. To reveal information, domain name server (DNS) queries are used, such as who owns a particular domain and which addresses have been allocated to that domain.

The ping sweeps of addresses discovered by DNS queries can present a picture of the live computers in a particular atmosphere. After generating such a list, the port scanning tools can cycle through all known ports to present a complete catalog of all services that are running on the hosts that the ping sweep discovered. The intruders can check the properties of the applications which are running on the computers. It can be directed to precise information that is constructive when the hacker attempts to compromise that service. To block reconnaissance attack, intrusion detection system (IDS), and intrusion prevention systems (IPS), are used.

Chapter 4

4.1 Virtual Private Network (VPN)

Security and privacy have become the essential requirements for IP Telephony communications. It needs security services like authentication, integrity and confidentiality. The solution for security in IP Telephony is to utilize security methods which are deployed in data networks, e.g. encryption, firewall etc. IPSec VPN is considered a more suitable security solution for communications amongst the users and consequent node over the internet in unsecure IP networks. The IPSec VPN consists of two primary components; one tunnel is for carrying private traffic and second tunnel is for security services.

IPSec employ encryption mechanisms to secure the interception and analysis of packets of data and voice while they are in the public network. At the moment, different connectivity models of VPN exist. The purpose of the remote-access VPN is to connect a remote user with a network. The site-to-site intranet VPN interconnects different remote site offices to the headquarters. The extranet VPN is utilized to connect companies with their business partners and vendors. The deployment of security mechanism, such as IPSec VPN directly affects speech quality and also channels capacity of the network. While supporting real-time traffic over IPSec, VPN reduces the performance and also quality of service [9][10].

4.2 VPN Protocols

The virtual private networks are usually built at the network layer, session layer or at data link layer. In this chapter, different types of VPNs are described.

4.2.1 Data Link layer protocols

Data link layers VPN are considered to expand remote access services over the internet. These protocols can provide flow control and as a result optimizing transmission by cutting down dropped packets. The major disadvantage is that these are targeted at the Microsoft client space, but not at other operating systems. The general link layer protocols are PPTP and L2TP [9] [10].

4.2.2 PPTP

The Point-to-Point Tunneling Protocol (PPTP) encapsulates PPP data traffic inside the IP packets while using a customized version the generic routing encapsulation (GRE). PPTP uses the similar types of validation as PPP. Although these protocols are dependent on password strength which is one means to achieve authentication and security.

Advantages:

- It has lower overhead.
- There is no need for public key infrastructure (PKI).
- Support of more PPTP connections in VPN server.
- It completely supports NAT.

Disadvantage:

- PPTP contains security and firewall problems.
- It can only support one tunnel at a time for each user.
- No additional authentication.
- PPTP access control is based upon packet filtering.

4.2.3 L2TP

The Layer 2 Tunneling Protocol (L2TP) joins results of PPTP with layer 2 forwarding (L2F) protocol. The tunnel which uses L2TP is accomplished with the mixture of multiple levels of encapsulation e.g. L2TP, IPSec, UDP, IP etc. On the other hand, IPSec is used for encryption of layer L2TP tunnels, [9][10].

Advantages:

- It can be used on IP and non-IP networks.
- It supports multiple protocols.
- Additional authentication facilities (e.g. RADIUS).
- Several simultaneous tunnels can be created for each user.
- It also compatible with NAT in case of supporting IPSec NAT traversal [9].

Disadvantages:

- The performance of L2TP is slow.
- It also supports L2TP connections in VPN server.

4.3 Network layer

The network layer protocol used in VPNs are IPSec and GRE.

4.4 IP Sec

IPSec VPN is intended to offer security between two firewalls, gateways and routers. IPSec works with two different modes, transport mode, and tunnel mode. The transport mode is applicable only for host-to-host security, and it provides protection for the payloads of IP packets. The tunnel mode secures the entire IP packet between two networks. Tunnel mode can be enabled in intranet and extranet VPNs. IPSec consists of two security protocols. First, authentication header (AH) protects the source and destination addresses of the IP header while using a hash function with a secret key. The second protocol is encapsulated security payload

(ESP), which provides validation and confidentiality. It also allows for encryption of the data payload, guaranteeing data confidentiality and integrity [9][10][11].

IPSec parameters and exchanging encryption keys are set up by internet key exchange (IKE) protocols in order to create a new security association. IKE validates the users by using either public key cryptography or shared secret keys. To maintain asymmetric user authentication mechanisms, many enhancements are utilized e.g. Hybrid authentication and Extended Authentication (XAUTH). XAUTH put login/password verification after main mode and before the IPSec parameter to negotiate securely to verify the remote user. XAUTH is protected by IKE main mode, which requires a certificate or pre-shared key. Hybrid authentication validates only the server with a public key or certificate, and the client is protected by the legacy methods known as ISAKMP [9][10][11].

Advantages:

- IPSec is a flexible protocol.
- No need for changes to individual user computers.
- It provides secured key exchange and strong data protection.
- IPSec supports a variety of encryption algorithms and checks the integrity of the transmitted data.
- It is an optimal solution for gate-to-gate VPNs.
- IPSec is suited for long-lived connections.
- NATs compatibility and NAT-Traversal support.

Disadvantages

- IPSec is the complex protocol to use.
- It identifies the device, not the end user.
- IPSec has no routing capability built-in.
- It just supports IP protocol.

- It reduces the global performances.
- IPSec does not offer any mechanism to support QoS.

4.5 Session layer

VPN-created, on-session layer has more detailed control of data flow than lower layer VPNs. Session layer protocols work with a variety of authentication and encryption mechanisms and set up a virtual circuit between client and host on a session. It allows monitoring and access control based on user validation. The key drawback is that session layer VPNs proxy all traffic; as a consequence they are slower than lower-layer VPNs. The access control of these protocols is more complicated to set-up, handle and maintain than address-based access control mechanism. The common session layer protocol is SSL/TLS [9][10].

4.6 SSL / TLS

SSL/TLS VPN is based on the Secure Sockets Layer (SSL) Protocol which provides data authentication and encryption for http traffic. SSL can also be utilized for securing real time protocol (RTP) traffic. SSL uses the main secure transport method, SSL/HTTPS, built in to create secure connections from web browsers to web servers. Most of the web browsers' discussion of the certificates lists is not activated by default; consequently a serious problem is aggravated by the security of SSL that is based on these certificates [9][10].

Advantages:

- In SSL there is no need of VPN client software.
- It provides secured key exchange and strong data protection.
- SSL allows access to specific resources inside networks.

Disadvantages:

- SSL secures the application payload only and leaves out the transport and network layer headers as clear text.
- It only works with web applications.
- SSL requires more firewall configuration than IPSec.
- More trouble deflecting denial-of service attacks

4.7 IP Sec with QoS

When using IPSec tunnels with QoS in IP Telephony, network is affected with two parameters, latency and packet loss. The encryption process and the traffic load are the main two reasons of this behaviour. Excessive amount of CPU capacity and memory is required for encryption. For this reason the router's manufacturers suggest the setting up of VPN accelerator cards, which are dedicated entirely to data encryption/decryption. Therefore the router is not involved in any responsibilities other than routing information, consequently increasing the router performance. [12]

The router buffers the multimedia traffic, until the serial link is no longer used. Because of this the latency increments depends on the traffic load. In order to reduce the latency, special treatment must be given set to this sort of traffic over the remaining traffic.

IPSec VPN can be deployed over medium traffic loads. Further careful considerations must be taken when applying it to larger networks such as an (ISP). Behavior is different in peak times and higher amounts of traffic flow. As a result we propose a non-optimum solution. If, without QoS mechanisms, the video conference was set in peak times, the quality might be affected seriously. With the implementation of QoS the priorities are set for different traffic type through different queues [12].

Chapter 5

5.1 MPLS (Multi-Protocol Label Switching)

Multi-protocol label switching (MPLS) is an innovative technology that will be utilized by many prospective core networks; including voice and data. MPLS will work along with the existing and potential routing technologies. It offers very high-speed data forwarding among label-switched routers, known as (LSRs). It reserves the bandwidth for traffic flows with different QoS requirements. IP network services can be enhanced through MPLS which that offers scope for guaranteed QoS, traffic engineering, and VPNs [14].

5.2 MPLS Architecture

MPLS supports multiple protocols in the domain so it has different components that control this process. Mainly, it has two components.

- A Control Plane and
- A Data Plane

It controls the flow of routing as well as labeling the information flowing through the network. It requires different protocols to perform this task: enhanced interior gateway protocol (EIGPR), open shortest path first (OSPF), border gateway protocol (BGP) and label distribution protocol (LDP). It is independent from routing protocols; their main function is to forward packets on the basis of labels. It contains a table, known as label forward information base (LFIB), which contains labels of the next router In MPLS, different kinds of routers are used: label switch router (LSR), and edge label switch router (Edge LSR). LSR routers do not participate in the routing lookup or routing decision. Their main function is to swap

the packet with another label, which is the label of next router to which this router is sending data [13] [14].

The edge LSR takes part in the routing decisions and selects the best path on the basis of any routing protocols. It receives packets from the customer,s router puts a label on it and forward to LSR router. When packets arrive at the destination edge LSR, it removes the MPLS label and forwards the packet to the client router [13][14].

5.3 MPLS Label Distribution

There are two methods used in MPLS label distribution; one method is hard programming and is very similar to how routers are programmed for static routing. With static routing no need to get dynamic routing routes to forward data. MPLS uses a second method known as ‘dynamic’, which decides dynamically to forward labels and data on a particular route. There are two methods to control the distribution of labels within the MPLS namely domain.

- Independent Control and
- Dependent Control

Although using independent control there is no designated router to make decisions about the traffic flow path. No router responsible for forwarding the labels, each router decides independently. In the case of the control method, edge routers are defined as designated routers and these routers are responsible for deciding where and how labels and data are to be delivered.

Two additional triggering methods are used:

- Downstream on unsolicited
- Downstream on demand

In downstream unsolicited, push is based on the decisions of the router, which is labeled as label manager. When labels are forwarded unsolicited by local manager, it is called ‘unsolicited downstream’. These labels are not demanded labels. In downstream demand, the labels are demanded and forwarded to the requested nodes it is called downstream demand or on demand downstream.

5.4 MPLS VPN

MPLS VPN is the combination of peer-to-peer and overlay VPN. Edge routers always uses separate virtual routing table like VRF for every customer. Provider edge routers contribute in the customer routing and giving Provider.

MPLS VPN is a guarantee of maximum speed of routing between the different customers sites. While using MPLS VPN, the customers can even use overlapping addresses as well. As far as understanding of MPLS VPN is concerned, there are two parts of a network. One is customer controlled known as C network while the second is provider controlled known as P network. In the C network, all the nodes are connected with CE routers and then it is connected to PE routers. In the case of PE routers, these are connected to P network which forwards information among MPLS enabled routers [14]. The main routers in MPLS VPN domain are provider edge routers (PE) and provider routers (P). The PE routers terminate the connection with customers and they just forward data to P routers. The P routers forward data towards the destination; edge routers do not participate in the forwarding process. P routers have no connection with customers’ routers. All P and PE routers run with label information to make a network of MPLS path, which is known as label switch path, from each PE to PE network [13][14].

The customer edge routers (CE) are not the part of service provider’s main MPLS VPN domain network. The CE router acts as a peer with the PE router, but not for

other CE routers. Every PE router runs more than one routing protocol, and containing multiple routing and forwarding table is known as Virtual Route Forwarding (VRF). The VRF can have addresses obtained from CE routers which can overlap with other address in the other VRF table [13][14].

In MPLS VPN VRF provides separation between different customers. Therefore, there is need of a routing protocol that will carry routes over the provider network while keeping the separation between the customer address spaces. The ideal solution for customer route propagation is to run one routing protocol between the provider edge routers. This will exchange information between PE routers with the involvement of P routers. It is recommended to use BGP for this purpose. Networks are always expected to increase with customers so there must be a protocol which is scalable and can handle large number of customers' routes from the clients [15].

Figure 5.4: MPLS VPN

The overlapping of addresses is allowed in MPLS VPN because of RD (Route Distinguisher) implemented in BGP. The solution for this problem is to expand the customer IP prefixes while using a unique prefix, making the address distinctive even the addresses are overlapping. The MPLS VPN provides facility to use 64-bit

prefix, known as RD, to convert non-unique 32-bit IPv4 addresses into 96-bit unique addresses that can be carried between provider edge routers. The function of RD is to convert 32-bit IPv4 address into 96-bit unique address; this address is also known as VPN IPv4 address. VPN IPv4 address is exchanged between PE routers, but not between CE routers. [14] In MPLS VPN, route targets (RT) are used, to check the VPN membership how man many VPNs a site is connected. The other benefit of MPLS is the capability to understand a big network and that makes it simple so that easy to manage and control. MPLS makes it possible for every user to manage, monitor and operate it easily. The users can control and manage the flow of data and can also manage the congestion while using traffic engineering in MPLS network [12].

All the members in the MPLS VPN must be connected to ISP network, and these members must know which members are the parts of this VPN network. The members of MPLS can leave the network any time, and this information must be propagated over the VPN network. The members of one VPN must not have information about the other VPN members. Information about other VPNs are kept separate in the same network. All those members who belong to same VPN connection must exchange information of network layer addresses.

While using this mechanism, data is carried amongst the different users in the VPN domain. Data about different VPNs is kept separate. The discovery mechanism includes different protocols LDP, OSPF, BGP. The reach ability information is exchanged also through these protocols. The reach ability and control traffic is exchanged over LSP which are members of the same VPNs. The data traffic is carried over LSPs, which are created to make a connection of all members of the same VPN [12].

5.6 MPLS VPN Deployment in a Backbone Network

The technologies like MPLS provide efficient ways to send data across the MPLS domain. It also enables users to monitor and manage traffic more easily at the backbone network. MPLS also provides the QoS within the MPLS header. It uses layer three information to establish connection. It forwards data while using layer 2 protocols like ATM and attaches a label of next router. Nowadays, it is recommended to use MPLS at the backbone network [12].

While using MPLS, it is possible to provide guaranteed QoS in ISP networks. MPLS always adds a label at layer 2 traffic which describes the path of this data that it has to follow while traveling through the network. While using MPLS and QoS, the ISPs can provide guaranteed performance to VPN users [12].

Chapter 6

6.1 Quality of Service

QoS is a guarantee or optimization or (both) of the users' perceived usefulness of service beneath the constraints of the occupied or available resources. It provides services at different levels. It makes it possible for the network administrator to set priorities on different types of traffic. While prioritizing the classes of traffic, the QoS is able to provide delay sensitive applications to work appropriately in the congested network.There are certain reasons to deploy QoS [16].

- It provides enhanced performance for delay sensitive applications like video and voice.
- It provides priority to critical applications in the network.
- To maximize the current network investment in the running infrastructure.
- To be able respond quickly if any changes occur in the network.

QoS can be categorized in different levels, known as service models. The end-to-end QoS provides a specific level of service to network traffic from one end of the network to the other. There are three service levels, namely best effort service, integrated service, and differentiated service [16].

6.2 Best effort model

The best-effort service makes every feasible attempt to transmit packets across the destination. With the deployment of best-effort technique, there is no guarantee that packet will deliver to the desired destination.

Advantages:

- The best effort model has nearly unlimited scalability. The only way to achieve scalability limits is to reach bandwidth limits; in this case whole network traffic will be affected.
- While using best-effort model there is no need to employ special QoS mechanisms.
- Best-effort is the quickest and easiest model to implement.

Disadvantages:

- In best effort model there are no guarantees of delivery of packets. Packets can arrive at any time and in any order.
- There is no preferential treatment of different packets: all the packets are treated in the same way. Even the crucial data is treated like the ordinary e-mail is treated.

6.3 Integrated service model

The integrated model provides guaranteed flow of data while negotiating different parameters end-to-end. The application requires the level of service which is necessary to operate appropriately. It also requires reserving the resources for this application before it starts transmission of data. The application will not transmit data until it receives the acknowledgment from the network, that the network handles the load providing end-to-end QoS [16].

Advantages:

- The IntServ supports admission control, which permit networks to deny or downgrade new RSVP sessions if any one of the interfaces in the transmission path has reached the boundary limit. The purpose of RSVP is to signal QoS requests for each individual flow.
- RSVP informs all the network devices' flow parameters (port numbers and IP addresses). Few applications utilize dynamic port numbers, such as H.323-based applications, that are difficult for network devices to recognize.

Disadvantages:

- Because of stateful RSVP architecture, there is continuous signaling that adds to the bandwidth overhead. For the entire duration RSVP continues to signal. The network may no longer be able to support the reservation if the network changes, or links fail, and routing convergence occurs.
- For large implementation, such as the public internet, the flow-based approach is not scalable. The reason is because RSVP has to keep a record of each individual flow. This activity makes end-to-end signaling difficult. The best solution is to combine IntServ with DiffServ models to offer the required scalability.

6.4 Differentiated service model

The differentiated service model includes classification tools and queuing mechanisms. The differentiated services depend on the edge routers to classify the different types of traffic which are traversing in the network. The network traffic can be classified through ports, network address, protocols, and it is accomplished by extended access list. The congestion management is a common term which includes different queuing techniques to manage the situations where bandwidth demands exceeds the total bandwidth the network can provide. The congestion

management does not control congestion prior it occurring. Through these queuing techniques, priorities for different types of traffic is set. There are different queuing techniques that exist like first-in-first-out, weighted fair queuing, custom queuing, priority queuing [16].

Advantages:

- The diffserv is highly scalable solution for large networks.
- It offers many different levels of quality for different traffic types.

Disadvantages

- Still there is no guarantee of service quality.
- It needs many complicated mechanisms to work in the running network.
- Packet classification is used to separate different types of classes. Then packet classifier sets each class to behave as an individual flow of data and then QoS is applied on it. There are different reasons to use QoS.

6.5 Marking

Marking is associated with classification. Marking makes it possible for network devices to mark or classify a data packet while using any traffic descriptor. There are different descriptors existence like frame relay, MPLS experimental bits and IP Precedence etc. With the help of marking classification information can be put into layer 2 or layer 3 packet headers. The benefit of marking is that subsequent network devices can easily differentiate the marked packet which belongs to a particular class. When packets are indentified as belonging to a particular class, then QoS mechanisms are applied to ensure compliance using QoS policies.

6.6 Classification

Classification makes different categories of traffic. Traffic descriptor is used to categorize a packet inside a group. When the packet is classified, then it is accessible for handling QoS on the network. Classification makes it possible for network administrator to partition traffic into multiple class of service (CoS). The traffic descriptor is used to classify the traffic, the source agrees to stick to contracted conditions and the network promises QoS. Classification must take place at network end points.

6.7 Delay

It is the time taken by a voice packet to deliver from one point of the network to the other which is its destination. It can be measured in one-way, or round-trip, in the network. Delay is the key factor to check the quality of voice in IP Telephony network.

6.8 Jitter

The variation in delay is called jitter. Jitter can be seen in the characteristics such as the variation interval between successive pulses or amplitude or frequency. Jitter is an important factor in the IP Telephony network.

6.9 Packet Loss

This represents the loss of packets along the flow of packets, if more packets are lost then it severely affects the quality of voice.

6.10 MOS

This is known as (mean opinion score) and is used to check which factor affecting the quality of voice. The MOS is an overall value which represents the quality of

voice. Its values are 1 to 5, the lowest value shows lowest quality of voice and highest value shows best quality of voice.

6.11 R-Factor

This is also a standard used to check the quality of voice. Its values start from 1 and end with 100. Lower values indicate poor quality of voice and higher values indicate better quality of voice [17].

Chapter 7

7.1 Comparative Study between IPSec VPN and MPLS VPN

The IP-based VPN technology is quickly becoming the base for the transmission of prospective internet services, and several service providers are deploying this service. In chapter, 7th IPSec VPN and MPLS VPN comparative study is discussed. These are the differences between the architectures of these two which are described in the below [table 6.1].

IP VPN forwarding tables are used to separate the traffic of different VPN. In MPLS VPN traffic of different customers is separated through virtual route forwarding (VRF). IPSec works at network layer and it is also transparent to all the applications. MPLS VPN works at IP or in both IP and ATM environment and MPLS VPN is totally transparent to the applications. There is no need of network level provisioning for managed CPE based services. When IPSec VPN is deployed, then centralized provisioning and management support is provided. In MPLS, VPN activation of services is required one time on the customer edge router and provider edge router to enable the site to establish the membership with MPLS VPN group [18].

Features	IPSec VPN	MPLS VPN
Traffic Separation	Tables separate different VPN traffic.	VRF separates different customer's traffic.
Transparency	It is transparent and works at network layer.	Totally transparent and one time activation required.
Provisioning	Centralized provisioning required.	One time service activation required.
Service Level deployment	It can be deployed in small or medium existing IP networks.	The edge and core routers to be MPLS capable.
Session Authentication	Pre-shared keys and digital certificates are used.	Route descriptor and logical ports are used.
Confidentiality	Tunneling and encryption mechanisms used.	Provides similar security like ATM or Frame Relay.
Quality of Service, service Level agreement	It is deployed to preserve packet classification for QoS in the IPSec tunnel.	It provides robust QoS mechanism and traffic engineering.
Client Support	It needs VPN Client software.	No need any client software.
Scalability	It requires proper planning and coordination.	No need of site-to-site peering.
Implementing in the network	This can be deployed in the local loop and at the edge.	Implemented at the core and edge routers.
User interaction	Need client software interaction.	No need of client software interaction.
IPv6	IPSec support IPv6.	It also Supports IPv6.

Table 7.1: Theoretical comparison

IPSec VPN can be deployed in a small or medium existing IP network. When upgrading or setting up new MPLS VPN network, it is required to have network elements at the edge and core routers to be MPLS capable. In IPSec VPN, every session has to be authenticated through pre-shared keys or digital certificates, those packets are dropped which do not follow the security rules. In MPLS VPN, the membership is known through service providers which use route descriptor and logical ports to check the membership. The unauthorized access is blocked through the devices which are configured for this purpose. IPSec VPN works at network layer and it provides data confidentiality through tunneling and encryption mechanisms. In MPLS environment, it separates the traffic of different users while providing security similar to the trusted ATM or frame relay environment. IPSec VPN does not provide any reliability or QoS mechanisms. IPSec VPN can be deployed to preserve packet classification for QoS in the IPSec tunnel. MPLS VPN provides robust QoS mechanism and traffic engineering and also other services with guaranteed service level agreements. It also provides scalability in the network [18] [19].

To deploy IPSec VPN at large scale it requires proper planning and coordination, with key distribution peering configuration and key management. In MPLS VPN, there is no need of site-to-site peering and it can support thousands of VPN groups over the same network. It can be deployed in the local loop and at the edge; through IPSec security it can be applied through encryption and tunneling. MPLS VPN is the best deployed at the core of the MPLS network. QoS and bandwidth can be controlled when service level guarantee (SLG) is to be offered as it is the part of MPLS VPN service. In IPSec VPN, users are required to interact with client software. In MPLS VPN, there is no need for user interaction. IPSec VPN and MPLS VPN both support IPv6.

MPLS VPN is a more scalable and reliable solution for the organization. It also supports both IPv4 and IPv6. It can control the QoS and provide guaranteed flow of data. From the above discussion, it is concluded that MPLS VPN is a scalable and cost-effective solution for large networks [18] [19] [20] [21] [22].

7.2 Discussion

IPSec VPN services can be used as a base for a value added service in service provider networks. There are different choices of VPN to use: MPLS base, or IPSec VPN. MPLS VPN is better because it supports QoS completely, which is important for an IP telephony network. IPSec VPN works on the basis of IP addresses, but MPLS works with labels. To intercept the data which is transmitted on the basis of labels is not easy. MPLS VPN can be deployed in the core large network and it can also be used to establish intranets or extranets for subscribers with security.

Chapter 8

8.1 Overview of Implementation

This chapter describes about the implementation of MPLS VPN networks in which different sites are built. It also explains the implementation of QoS to prioritize the IP Telephony traffic in the converged network to reduce jitter and packet loss.

The comparison between MPLS VPN and IPSec VPN provides the basis for this implementation. This implementation is based on local area network (LAN) and wide area network (WAN). LAN has two sites a head office (H-O) and a branch office (B-O). The ISP-domain is WAN site. H-O is the main site for serving IP Telephony services to local users and B-O users. MPLS VPN connection is used between H-O to B-O over the WAN.

8.2 Equipment

The entire implementation is constrained by the lab limitations. Three routers are connected to build a WAN area (ISP-Domain, ISP-PE1 and ISP-PE2) and one router is used to act as dummy internet traffic generator. The LAN sites have two parts, H-O and B-O. H-O has one IP-Telephony service enabled router, known as call manager. The rest of the equipment is given in the appendix A and [table 8.2].

8.3 Distribution of VLAN

In the figure (Fig: 1.1), the IP-Telephony enabled router is known as call manager and router {R3250 (CE-2)} is responsible for inter-VLAN routing. Both sites are having different VLANs and they can access to each other. The connection between catalyst switch and router is a trunk link. Inter-VLAN routing means sub-interfaces

are configured on the router for different VLANs. Complete VLANs details is given in Appendix A and [table 8.3].

8.4 IP Addressing

In this implementation, different IP pools are used for IP addressing. In the WAN area (ISP DOMAIN), public addresses are used and in the LAN area (H-O and B-O) private addresses are used.

In this scenario the ISP is using four IP address pools. Firstly the public IP pool 200.84.1.0/24 for addressing of internal ISP communication links between router and internal LANs (that is not visible in this implementation). Secondly the public IP pool 160.70.4.0/24 for the communication links between ISP and clients. Thirdly is the public IP pool 200.85.1.0/24 is used for Traffic generator. Fourthly private IP pool 172.16.0.0/16 is used for ISP internal loopbacks. LAN areas H-O and B-O both use private IP pool 10.0.0.0/8 for inside communication. H-O uses public IP pool 160.70.4.0/30 and B-O uses 160.70.4.4/30. Each IP address pool is divided into different parts with VLSM. All IP Addressing details are shown in Appendix A and [table 8.4].

8.5 Explanation

The lab experiment scenario is in two main parts LAN and WAN. H-O works as WAN and B-O office works as a LAN. H-O is inside the IP telephony service provider area. A telephony service enabled router is configured as a call manager. It provides IP telephony services to local users as well as remote sites. In this experiment, a call manager is configured for 20 telephony users only, and is configured as dual line for hardware and software based IP phones. Two types of DHCP pools are configured for data and voice. DHCP data pool is for workstations and voice pool is configured for IP Phones address allocation. Configurations of

DHCP pools are shown in Appendix A. The call manager (CM) is configured for inter-VLAN routing, which provides multiple sub-interfaces to communicate between VLANs (Table 8.3). To provide best quality of voice, QoS is configured for data alignments and priority bases differentiate service.

There are two kinds of domains which are used in this scenario. One is customer domain and the other is MPLS domain. In customer domain, two routers are used known as CE-1 and CE-2 and they are not the part of MPLS domain. The local users will interact with these routers and then CE-1 and CE-2 will coordinate with MPLS domain, which is ISP. In MPLS domain, three kinds of routers are used and these are known as PE-1, PE-2 and P routers. PE-1 and PE-2 work as edge routers and are responsible for routing decisions and also for label allocation and de-allocation. PE-1 and PE-2 are also connected with customer routers. The P router, which is also known as provider router, does not take part in routing decisions; it just takes packets and forwards them to next edge router.

CE-1 and CE-2 routers work as customer edge routers which are connected to PE-1 and PE-2 respectively. Both CE-1 and CE-2 routers work as gateways and are also configured as firewalls to block attacks from the Internet. For the security of these two edge routers, AAA models are configured for telnet security.

Routers PE-1 and PE-2 work as provider edge routers which are directly connected with CE-1 and CE-2 respectively. These are also directly connected to P (provider router), known as ISP Domain. QoS (Differentiated Service) is implemented to prioritize the traffic which passes through the MPLS domain and the priority of voice is set to 70 percent of the total bandwidth. For the security purposes in MPLS domain, separate routing tables are created for every customer which is called VRF. It takes packets of IPv4 address from CE-1 and CE-2; converts this IPv4 packet

into VPNv4 packet, puts a label on it and forwards to next P router which is the ISP-Domain in this scenario.

The ISP (domain) router works as middle-man between PE-1 and PE-2. It takes packets from both routers, replaces the label from the packet and forwards it to the next edge router, which is also a part of MPLS domain. This router does not take part in the routing decisions but it just passes information on the basis of labels only.

To monitor ingoing and outgoing traffic, a monitoring server is used. Its function is to create databases that it builds on the bases of source and destination numbers, call duration and as well as quality of call. It also calculates the delay, jitter, losses, Mos and R-factor during each call. In this implementation, voice quality manager (VQ Manager) software is used to monitor voice traffic.

8.6 Results of Implementation

Before implementing QoS, a delay in the voice packets was observed and though, quality of voice was improved when QoS is implemented within MPLS VPN network. It reduces different parameters which affect the quality of voice.

There are three factors in quality of voice which are given below:

- Delay
- MOS
- R-Factor

Figure 8.8-1: Voice Traffic Before QoS

The implementation involves different calls, each consisting of 10 minutes duration and data is counted after every 30 seconds. Due to the software limitations, only three parameters have been shown in the graphs. The graph (8.8-1) was made before implementing QoS. It shows that average data loss for voice packets is 5% which does not look good. Because of this data loss there was distortion in the voice. However, the MOS value is 3.7%, which is certainly not appreciatable. The maximum MOS Value is 5; if the value in the running network is below 4 then it is not considered good for voice. The R-factor indicates an average value of 63%,

which does not offer high sound quality for IP Telephony. The highest value of R-factor is 100 if value is below 70, then it is not acceptable.

Figure 8.8-2: Voice Traffic with QoS

After implementing QoS comparatively, higher results are achieved. As shown in figure 8.8-2, the data loss for voice packets is 1% which is good compared to the non-QoS implementation results. The MOS value obtained is 4.4%, which is also effective in terms of voice quality. The R-factor value (93%), obtained from the QoS enabled implementation, also proves its beneficial results as compared to

previous implementation results. However, it is concluded that the implementation of QoS in our implementation has shown quite high performance aspects.

Figure 8.8-3: Voice Traffic with IPSec

This graph is taken after IPSec implantation which does not show good results. The graph (8.8-3) is taken before the implementation of QoS. It indicates that average packet loss is 10% which does not look good. The MOS value is 3.7% which is also not good and the R-factor value is 75% which is acceptable.

Figure 8.8-4: Voice Traffic with IPSec and QoS

This graph is taken after implementing QoS in IP telephony setup. The demonstration indicates that average packet loss is 7% which is good as compared to packet loss in graph (8.8-3). The average MoS value is 3.8 which is .1% improved. The R-factor value is 76% which is also improved as compared to graph (8.8-3).

The above results shows that MPLS VPN deployment is better than IPSec in IP telephony network because of good results in real time communication. The implementation of MPLS VPN in this scenario shows that MPLS VPN is a secure technique which provides complete address and traffic separation. It also hides the address structure of VPN core network. It is not possible to intercept core network of MPLS from an outside MPLS domain because the information travels on the

basis of labels which conceal the IP header. Even when MPLS VPN is miss-configured it is not possible for one customer to get access of other customer, s VPN which means it is more reliable compared to IPSec VPN. In the end, it is concluded that MPLS VPN is a secure, reliable and scalable technique to use in small or large network.

Conclusion

The implementation analysis showed that IP Telephony networks can be made scalable and efficient through the implementation of MPLS VPN over the internet. Having reviewed the relevant literature, it was decided to make a comparison between IPSec VPN and MPLS VPN. It is concluded that MPLS VPN is more scalable than IPSec VPN for large networks, which was later confirmed by the test results. The results showed that the implementation of QoS over MPLS VPN domains dramatically improved the voice quality for IP Telephony.

However, IPSec VPN is more secure technique to use but with more overheads like delay and packet loss which is shown in the graphs. It also does not support QoS effectively as compared to MPLS VPN domains. IPSec VPN could be a solution for small, remote sites where proper planning and coordination is required. However MPLS VPN provides enough security in IP telephony equal to layer 2 VPN. While implementing MPLS VPN, there was not much coordination and planning required due to its non-complex installation. Therefore, the final results demonstrate that MPLS VPN is a secure, efficient, reliable and scalable technique to use.

References

[1] L. Chaffin; J. Kanclirz, T. Porter, C. Shim, and A. Zmolek, Practical, *Voip Security. Syngress Publishing*, March 2006.

[2] William J. Rippon “Threat Assessment of IP Based Voice Systems” Research I/S Networking Organization: IBM Research I/S. Yorktown Heights, NY, April 2006

[3] D. Richard, Thomas J. Walsh, and S. Fries, “Security Considerations for Voice Over IP Systems”, National Institute of Standards and Technology. Special Publication 800-58. January, 2005.

[4] Miguel V. Martin, Patrick C.K Hung, “Security Policy for Voip”, University of Ontario Institute of Technology and Hung University of Ontario Institute of Technology. May 2005.

[5] N. Ekekwe, A. Maduka, “Security and Risk Challenges of Voice over IP Telephony,” Hopkins University Housing Preservation and Development Baltimore, MD, USA. 2007.

[6] F. Cao, S. Malik, “Security Analysis and Solutions for Deploying IP Telephony in the Critical Infrastructure”, Critical Infrastructure Assurance Group Cisco Systems, Inc. 2005.

[7] Patrick C.K, M. Vargas, “Security Issues in VOIP Applications” Hung University of Ontario Institute of Technology Oshawa, Canada. May 2006.

References

[8] Kotfila, David; Moorhouse, *Implementing Secured Converged WANs*, Cisco Press, July, 2007.

[9] W.B. Diab, S. Tohme, and C. Bassil, “VPN Analysis and New Perspective for Securing Voice over VPN Networks” Université de Versailles Saint-Quentin en Yvelines, France 2008.

[10] S. Frankel, K. Kent, R. Lewkowski, D. Orebaugh, W. Ritchey, and R. Sharma, “Guide to IPSec VPN” National Institute of Standards and Technology. December, 2005.

[11] Carlton R. Davis, “IPSec Securing VPN” McGraw-Hill Companies, April 2001

[12] J. Arturo, Pérez, V. Zárate, Á. Montes, and C. García, “Quality of Service Analysis of IPSec VPNs for Voice and Video Traffic,” Proceedings of the Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services. AICT/ICIW 2006.

[13] G. Armitage, “MPLS the Magic behind the Myths,” Bell Labs research Silicon Valley lucent technologies 2000.

[14] D. Minoli, “Voice over MPLS Planning and Designing Networks”, McGraw-Hill Telecom 1st edition. May, 2002.

[15] Cisco Systems Inc, ‘’Introduction to Virtual Private Network,” (MPLS VPN Technology) Cisco systems, inc. 2002.

References

[16] B. Durand, J. Sommerville, M. Buchmann, R. Fuller, and Technical Editor Michael E. Flannagan, *Administering Cisco QoS for IP Networks*, Syng Press November, 2001.

[17] Cisco Systems Inc, “Best Practices for Monitoring Cisco Systems IP Telephony Networks with AppManager”, White Paper, Cisco Press March, 2006.

[18] Cisco Systems Inc, “Comparing MPLS-Based VPNs, IPSec-Based VPNs, and a Combined Approach from Cisco Systems.’’ White Paper Cisco Press January, 2004.

[19] Cisco Systems Inc, “A Comparison between IPsec and Multiprotocol Label Switching Virtual private Networks” White Paper November, 2000.

[20] J. Pultz, N. Richard, “Analysis of MPLS-based IP VPN Security comparison to traditional L2VPNS such as ATM and FRAME RELAY, and deployment guidelines” Cisco Systems, inc. White Paper. 2004.

[21] Yao C. Chang, Han C. Chao , K.M. Liu and T.G. Tsuei, “MPLS VPN in cellular mobile IPV6 architectures’’ Department of Electrical Engineering, National Dong Hwa University and Ta Hwa Institute of Technology. 2002.

[22] F. Palmieri, “VPN Scalability Over High Performance Backbones Evaluating MPLS VPN Against Traditional Approaches” Università degli Studi di Napoli Federico II - Centro Servizi Didattico Scientifico. Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC’03). 2003.

[23] Kevin Wallace, July 2008, *Cisco Voice over IP (CVOICE)*, Cisco Press, third edition, 800 East 96th Street Indianapolis, IN 46240 USA.

[24] Salman A. Baset and Henning Schulzrinne, "An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol", Department of Computer Science Columbia University, New York NY 10027 September 15, 2004.