VIRTUAL PRIVATE NETWORK: ARCHITECTURE AND IMPLEMENTATIONS

A thesis submitted to the graduate school in partial
fulfillment of the requirements for the degree
Master of Science (Information Technology)
Universiti Utara Malaysia

by

KHAIRUL NAJMY HAJI ABDUL RANI

Sekolah Siswazah
(Graduate School)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certification of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

KHAIRUL NAJMY HAJI ABDUL RANI

calon untuk Ijazah
(candidate for the degree of) Sarjana Sains (Teknologi Maklumat)

telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

VIRTUAL PRIVATE NETWORK : ARCHITECTURE AND IMPLEMENTATIONS

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan, dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the field is covered by the project paper).

Nama Penyelia
(Name of Supervisor) : En. Helmi Mohamed Hussain

Tandatangan
(Signature) : Helmi Hussain

Tarikh
(Date) : 22 OKTOBER 2000

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or, in their absence, by the Dean of the Graduate School. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Graduate School
Universiti Utara Malaysia
06010 Sintok
Kedah Darulaman
Malaysia

ABSTRAK

Revolusi ekonomi berasaskan rangkaian telah mengubahkan cara manusia menjalankan aktiviti-aktiviti pemiagaan Di dalam hal ini, keperluan-keperluan komunikasi terkini diperlukan untuk menjadikan pemiagaan lebih berdaya saing. Sebagai contoh, sesetengah staf kini mungkin bekerja di dalam bangunan yang berlainan atau malahan negeri yang berlainan dengan pengurus mereka. Jadi satu jaringan meliputi kawasan luas diperlukan bagi memudahkan kedua-dua pihak pengurus dan staf-staf tersebut untuk berkomunikasi walaupun pada jarak yang berjauhan. Contoh seterusnya, menjalankan kerjasama atau perkongsian pintar di antara syarikat-syarikat adalah merupakan satu strategi perniagaan yang sangat penting, terutamanya dalam menghadapi tekanan saingan pemiagaan. Oleh yang demikian, satu rangkaian komunikasi yang selamat diperlukan bagi menghubungkan syarikat-syarikat yang terlibat di dalam proses kerjasama atau perkongsian pintar pemiagaan itu. Salah satu penyelesai untuk Rangkaian Kawasan Luas (WAN) yang digunakan bagi memenuhi keperluan-keperluan komunikasi yang kompleks tertera di atas, dikenali sebagai **Virtual Private Network** (VPN). VPN adalah satu teknologi terkini yang menggunakan Internet sebagai tulang belakang rangkaian yang **utama.**

Secara amnya, VPN telah dikatakan lebih fleksibel, efektif, dan efisien dalam menjanakan pemiagaan berbanding dengan teknologi-teknologi WAN yang lain. Terdapat dua fungsi utama yang membuatkan VPN menjadi salah satu penyelesai alternatif WAN pada masa kini: Penekanan *privacy* di dalam melakukan pertukaran data yang sensitif melalui cara yang lebih murah berbanding dengan penyelesai-penyelesai WAN tradisional, dan juga perlindungan keselamatan yang sangat baik terhadap aset-aset maklumat yang dihantar melalui infrastruktur Internet.

Adalah menjadi satu kebaikan untuk memahami teknologi VPN secara terperinci sebelum ianya digunakan. Di dalam projek ini, terdapat kajian mengenai VPN dari segi latarbelakang pembangunan, konfigurasi, jenis-jenis aplikasi, ciri-ciri penyelesai (keselamatan), kerangka rekabentuk, kebaikan dan keburukan jika dibandingkan dengan teknologi-teknologi saingan, *Quality of Service* (QoS) dan *Service Level of Agreements* (SLAs), IO-langkah berguna untuk membina infrastruktur VPN, dan penggunaan VPN di dunia nyata. Diharapkan, laporan projek ini dapat menjadi sebagai satu rujukan atau petunjuk yang berguna terutamanya kepada mereka yang berminat di dalam merekabentuk, membangun, dan mengimplementasikan teknologi VPN.

Pada kenyataannya, VPN adalah merupakan satu teknologi baru dan boleh diperkemaskan lagi. Terdapat beberapa kelemahan di dalam senibinanya dan ciri-ciri penyelesainya, di mana ianya perlu dikembangkan lagi. Projek ini memfokuskan teknologi VPN berbanding dengan teknologi-teknologi saingannnya di dalam menyediakan penyelesaian terbaik di dalam rangkaian *Enterprise* sesebuah organisasi.

ABSTRACT

The revolution of the networked-centric economy has transformed the way of people carrying out business activities. ln this case, the business needs new kind of communication requirements in order to be more competitive. For instance, some corporate staffs are no longer work in the same building or even in the same country with their managers. Therefore a wide area link is needed to communicate with these staffs working in the remote branches or in the fields. Another example, alliances and partnerships among enterprises have become as crucial strategies that need to be regulated by many industries to cater the pressures from business competitors. Therefore, a secure communication solution is needed to link all the joined enterprises. One of the latest emerged Wide Area Network (WAN) solutions used to fulfill all the complex communication requirements is **known** as **Virtual Private Network** (VPN), which use the Internet as the main backbone.

In general, VPN has been claimed to be more flexible, effective and efficient compared to other WAN technologies. Two essential functions that make VPN as one of the best alternative WAN solutions currently: Privacy for interchange of sensitive data in a cheaper way compared to traditional WAN solutions, and Remarkable security protection of information assets transmitted over the Internet infrastructure.

It is good to understand the VPN technology in details before starting to implement it. In this thesis, there will be a study on VPN in terms of its progression backgrounds? configurations, application types, solution (security) features, design framework, pros and cons with respect to other competitor technologies, Quality of Service (QoS) and Service Level Agreements (SLAs), useful lo-point plan infrastructure building, real world implementation. Hopefully this thesis can be as a useful reference or guidance for those who are really interested in designing, developing, and implementing the VPN technology.

In reality. VPN is an immature and upgradable technology. There are certain loopholes in its architectures and solution features that can be enhanced. This project will focus on VPN's technology compared to other WAN solutions in providing the best solution for the organization's enterprise network.

ACKNOWLEDGEMENT

Firstly, *Syukur Alhamdulillah* and great thanks to ALLAH TA'ALA for giving me opportunities in terms of healthy mind and body, patience, as well as sufficient time and energy to finish up this project. I would also like to show great appreciation to Mr. Helmi Mohamed Hussain who was my project supervisor. Though he was busy, he still could spend time with me to give a lot of useful guidance and constructive ideas in making this project become so successful and have research values. Not forgotten, I would like to give high gratitude to Mr. Abdul Razak Jusoh, an Information System officer from the UUM Computer Center Department for providing me with some useful information and layouts of the existing UUM Integrated Sintok Local Area Network (ISLAN) and Mrs. Fauzuniah Pangil,a Lecturer from the UUM School of Management for helping me out in preparing this project report.. Finally, I would like to express high gratefulness to my wife Mrs. Alawiyah Hj. Abd. Wahab, my only daughter Nurul Najihah Khairul Najmy, and all of my other family members, relatives and friends for keep supporting me to finish up this project and through it to complete my MSc.IT program course work successfully. All co-operations, supports and guidance that you guys gave me are greatly appreciated and may ALLAH TA'ALA bless all of you.

Thanks and best regards.

Yours sincerely,
KHAIRUL NAJMY HJ. ABDUL RANI (81303)
MSc.IT (UUM)
OCTOBER 2000

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES

CHAPTER 1

Introduction

1.1 Today's Corporate Requirements for High-Performance and Secure Wide Area Network (WAN) Solutions

The emergence of digital communication systems particularly computer networks has changed significantly the way people practice businesses during this information age. Formerly, computer networks were considered merely a convenient method of sharing resources or sending simple messages [38]. Today, computer networks have become a key component of a corporation's strategic assets, and a driving force in transformation of Information Technology (IT) from a back-office tool to a marketplace weapon, where there should be a continuous evaluation of information network's ability to fully support corporate goals and missions [38].

Two important things have to be emphasized simultaneously by businesses in evaluating information network's ability. Firstly, the network should have the capability to support a broader variety of communications among a wider range of sites. This is due to current employees extensive demand to access the resources of their corporate intranets as they take to the road, telecommute, or dial in from customer sites. Furthermore, business partners, outside consultants and vendors sometimes are required to join together in the extranets to share or exchange business information so that a joint project can successfully be done for long-term strategic benefits [40].

Secondly, the infrastructure of the networks should be designed, built and managed at a low cost. In this case, the characteristics demanded by current business environment in the development of "virtual offices" and "virtual project teams" are more typically found in public, rather than private data networks [38]. Thus, it is no doubt to say that the exponential growth of the Internet and the emergence of Web-based intranets have encouraged corporations to evaluate the low cost, ubiquitous and highly scalable Internet as a potential replacement for private networks as the primary medium for corporate data communications [38].

Technically speaking, businesses have found that past solutions to Wide Area Network (WAN) solutions between the main corporate network and branch offices, such as dedicated leased lines or Frame Relay circuits are not really practical enough. This is because both solutions do not provide the flexibility required for quickly creating new partner links or supporting project teams in the field [40].

In addition, many organizations also realized that in order to use the Internet as a private WAN, two main hurdles have to be overcome [3]. The first hurdle is networks often communicate using various protocols, for example Internet Packet Exchange (IPX) and Network Basic Input/Output System Extended User Interface (NetBEUI), however the Internet can only handle Internet Protocol (IP) traffic. The second hurdle is all the data packets traveling in the Internet are routed in clear text resulting confidential business information can easily be read by unauthorized person or hackers who can see Internet traffic.

As a result, a private encapsulated network service known as **Virtual Private Network** (VPN) has been introduced, developed and used in the Internet as a private WAN to overcome many networking problems mentioned earlier. In this case, the VPN applies a strategy called Tunneling via local Internet Service Provider (ISP) as a gateway to build private WAN. It is stated that through VPN, an organization can increase sales, accelerate product development, and strengthen strategic partnerships in a new business direction [24].

1.2 Problem Statements

The problem is how true that VPN is becoming a cost-effective, secure, and efficient technology in order to improve business communications both internally and externally. An analysis and an assessment on its configuration, core components, solution features, conceptual and logical designs and Quality of Service (QoS) should be made carefully in order to find out the answer. Besides, there should also be a study on how to clarify the VPN pros and cons compared to other competitor technologies.

1.3 Objectives of Project

This research project is conducted based on several main objectives enlisted below, which are:

1. To study the general theory or fundamental principle of the VPN components including its architecture or configuration, its application, its security and control features, its core devices including routers and firewalls, and its network performance measures based on VPN QoS building blocks.
2. To study how the VPN technology is being designed and developed by various key players, such as Cisco Systems, Nortel Networks, Enterasys Incorporated, and Nokia Incorporated.
3. To analyze how VPN is implemented successfully by various scale of organizations worldwide as a useful reference.
4. To identify the environment suitable for VPN through the evaluation of its capabilities and constraints especially after being utilized via the Internet that might include the implementation cost and data security issues.
5. To analyze and to compare the VPN technology advantages and disadvantages compared to other WAN solutions such as Dedicated Point-to-Point (Leased Line) and Frame Relay circuits particularly in becoming as a communication solution between a corporate main network and branch offices.
6. To highlight the 10-point plan (useful tip) for building a VPN as a cost-effective and a highly secure data communication solution for corporate.
7. To apply VPN in designing a low cost, a secure, and an efficient communication network between the UUM main campuses located in Sintok, Kedah Darulaman and its branch campuses nationwide as a case study.

1.4 Scopes and Limitations of Project

The project would exclusively cover some detail information regarding the architectures or configurations, the main applications, the solution features and the performance measures (based on QoS building blocks) of VPN, which primarily used as a communication link between organizations' main network and branch offices. In addition, there will be a case study on how to design VPN as a private encapsulated

network service particularly to link the UUM main campus Integrated Sintok Local Area Network (ISLAN) (equipped with the Gigabit Ethernet backbone) and its branch campuses nationwide.

1.5 Significance of Project

In general, this research project is made to highlight the cost effectiveness, flexible solution features and good performance measures (based on QoS building blocks) of VPN, which is one of the latest communication solutions in WAN. It is really hoped that this project report could be as a useful guidance for any network designers or network administrators or network engineers in designing and implementing the VPN technology to link up a corporate main network with branch offices worldwide via the Public Network.

1.6 Methodology

Generally, the project will greatly deal with the approach of studying (analyzing) through literature reviews and proposing (designing) VPN as an organization's main network WAN solution linked with branch offices (in this case, UUM main campus ISLAN with UUM branch campuses nationwide). There are 9 steps used to complete this project. Figure 1.1 shows the diagram of the methodology relationships.

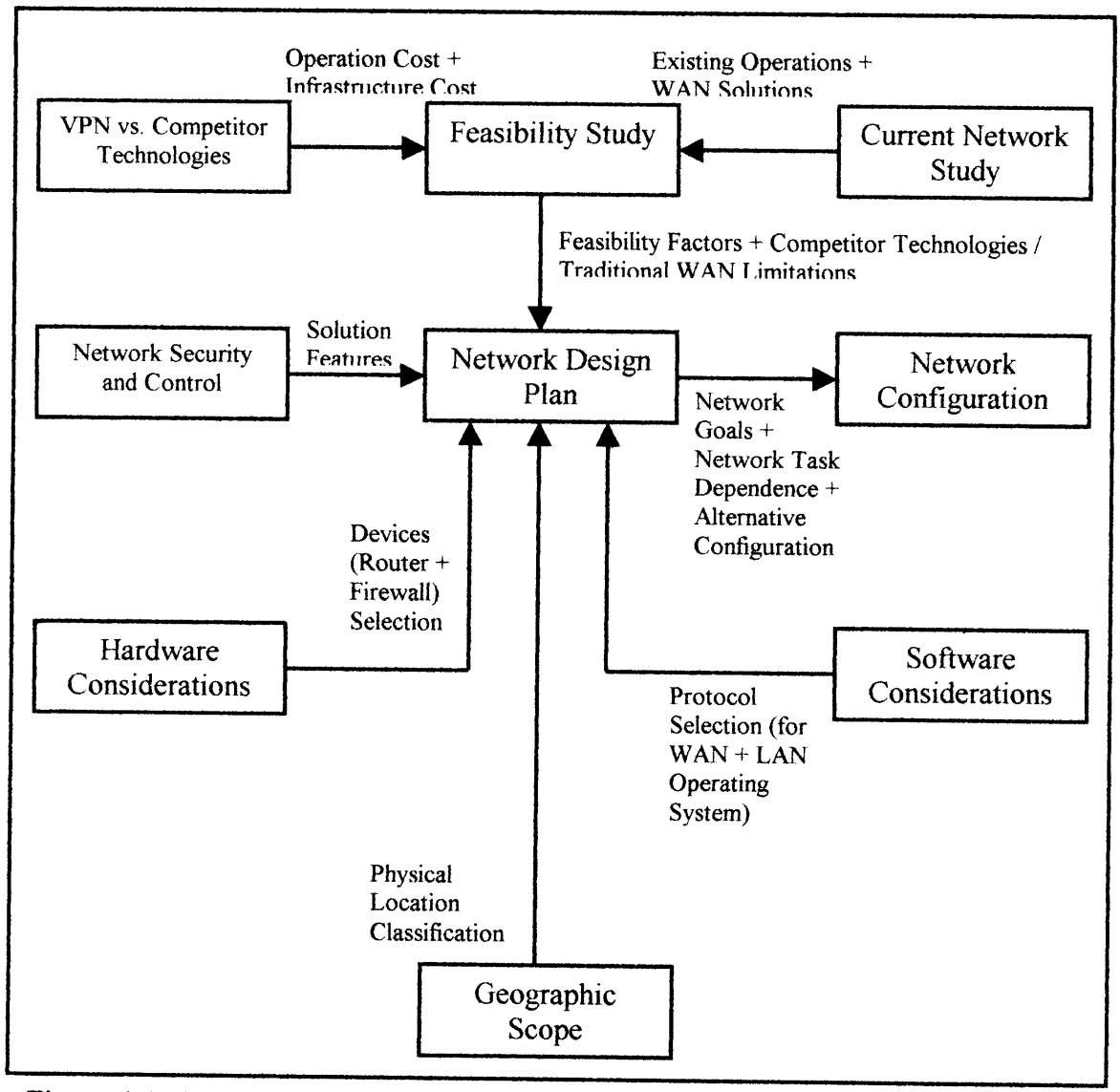


Figure 1.1: Diagram of Methodology Relationships

Below is enlisted some brief information regarding each of 9 steps used as this project methodology:

1. Conduct a feasibility study.
    - The study is made mainly to get some ideas about a new evolved network technology, which is VPN in this project. In this case, doing a lot of literature reviews are the important task to be made. The study requires some assessment factors in identifying the problem definition, such as the limitations of traditional WAN solutions that make VPN as the best alternative solution in near future.

2. Prepare a network design plan.
    - There will be 3 feasibility factors need to be determined, which are the Technical Feasibility that covers the VPN configuration/architecture and core components; the Operational Feasibility that covers the VPN applications, solution features and the QoS building blocks; and the Economic Feasibility that includes the VPN cost-effectiveness compared to other competitor technologies.
3. Understand the current network (implemented WAN solution used by UUM).
    - The main purpose here is to gain a good understanding of the existing network operations or traditional WAN solutions, particularly the one used by the UUM. As a result, it is easier to suggest some information needs and some specific applications to be used in the newly designed data communication network for UUM.
4. Identify the geographic scope.
    - The idea is to know the physical location that will be interconnected by the newly designed VPN. There are 4 basic levels of geographic scope need to be classified in mapping the network that are International, Country, City or District or State, and Local facility.
5. Identify the network security and control.
    - In this case, the main objective is to protect information from errors and omissions, message lost or change, disasters and disruptions, breach of privacy, theft, unreliability, inaccurate recovery and fault restart, poor error handling, and last but not least harmful computer viruses. This can be done through implementing VPN solution features that include firewall, encryption / decryption, authentication / access protocol and encapsulation / tunneling process.
6. Analyze and design network configurations.
    - The configurations or layouts are designed based on the listed network goals. Other related issues include analyzing task dependence in network configurations and evaluating possible alternative network configurations.

7. Evaluate software considerations.
    - The evaluation is made to overcome the limitation of different types of terminals or other hardware that can be utilized through protocol selection procedures. There will be some descriptions of the selected protocols, as well as documentation for both WAN and LAN software.
8. Evaluate hardware considerations.
    - The evaluation is to consider some pieces of hardware selection, which includes the VPN router and firewall. There will be the final configurations showing the appropriate nodes (buildings), and a list of hardware communication protocol requirements/features.

CHAPTER 2

Introducing VPN

2.1 Definition of VPN

Basically, VPN is a private data network that makes use the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures [39]. Precisely, VPN can be defined into two terms in providing network solutions. Firstly, in a nutshell term, a VPN is a private connection between two devices or networks over a shared Public Network. Secondly, in practical terms, VPN lets an organization securely extends its network services over the Internet to remote users, branch offices, and partner companies. According to Airamo (1997), VPN is fundamentally a flexible communication system that gives an image of a large-area computer network in a private use. To make things simpler, VPN turns the Internet into a simulated private WAN (Chae 1998). In this case, VPN applies the Internet as a backbone in a manner that provides the same security and features available in private networks. The basic idea of VPN is shown in Figure 2.1.

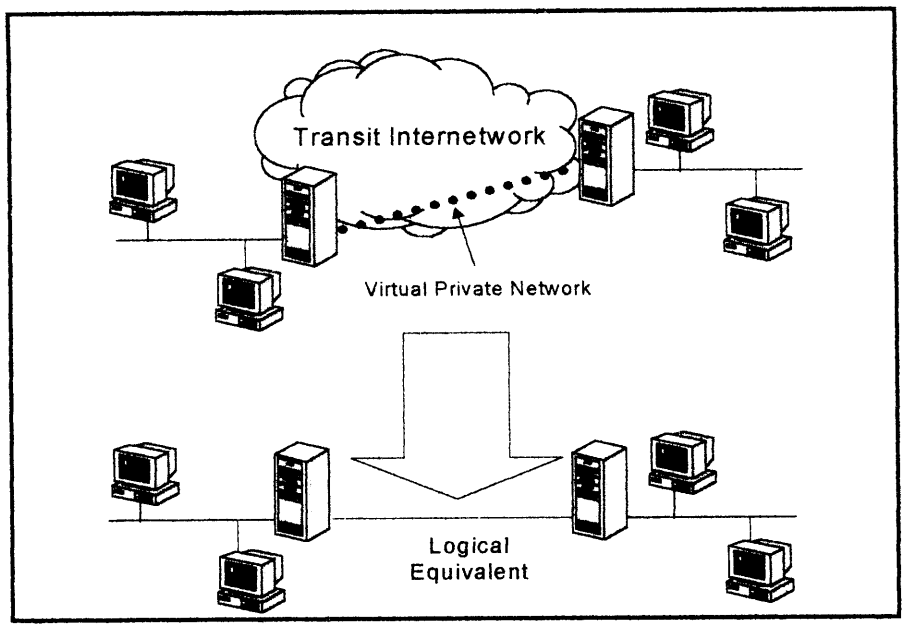


Figure 2.1: Virtual Private Network

2.2 Overview of VPN

As a matter of fact, VPN systems enable distributed private networks to communicate securely among each other over the Internet or shared Public Network (Herscovitz 1998). In this case, the systems will encrypt transmitted information with complicated algorithms to hide sensitive data from WAN intruders or perpetrators. Herscovitz (1998), depicted the overall structure of a secure VPN as shown in Figure 2.2 and clarified general processes of VPN systems as enlisted below:

1. A protected host sends clear traffic to a VPN kit (the source driver) located at the point of connection to the Internet or the shared Public Network.
2. The source device examines the data according to rules specified by the network manager securing the information or allowing it to pass unaffected.
3. When data protection is required, the source device encrypts (encodes) and authenticates (attaches a digital signature to) the whole packet, including the transmitted data as well as the source and the destination host IP addresses.
4. The source device then attaches a new header to the data, including the information that the destination device requires for security functions and process initialization.
5. The source VPN kit then encapsulates the encrypted and authenticated packet with the source and destination IP addresses of the destination device(s). This results in a virtual tunnel through the Internet or shared Public Network.
6. When the encapsulated data reaches the destination device(s), the data is decapsulated, its digital signature is checked and verified, and the packet is decrypted.

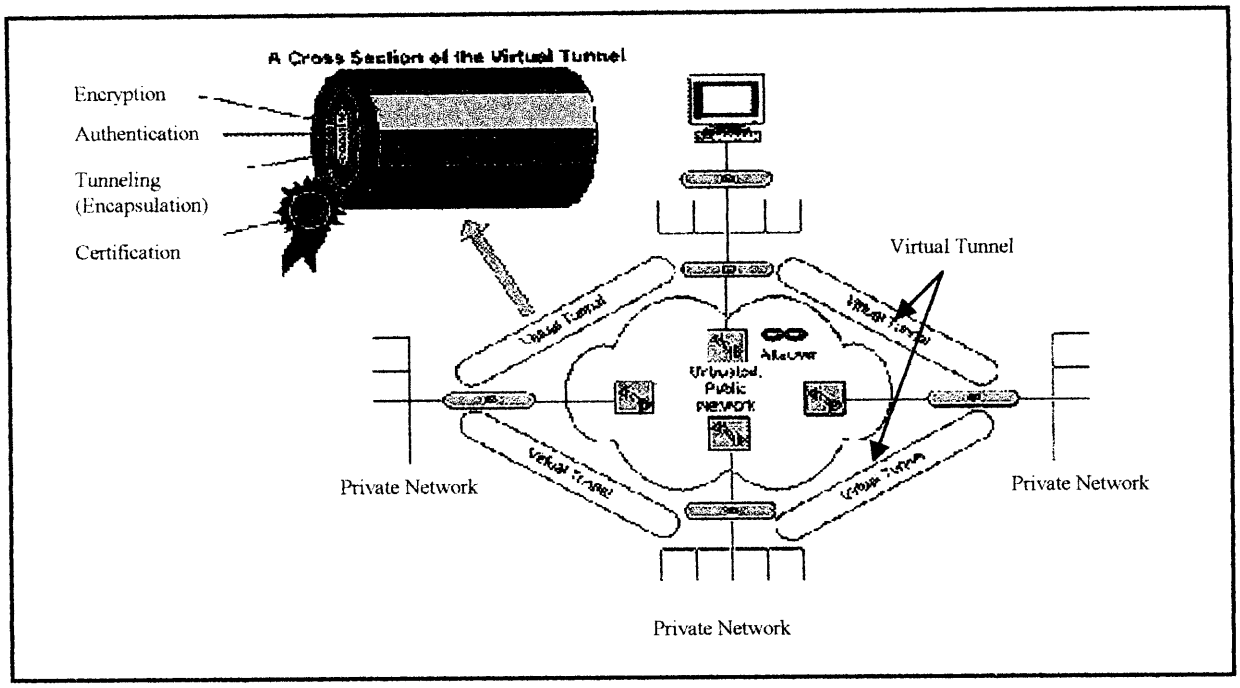


Figure 2.2: Overall Structure of a Secure VPN

In VPN, a process called "tunneling" is important since it allows user to encapsulate a packet within a packet to accommodate incompatible protocols (Scott 2000). As a result, there is no problem for two different Local Area Networks (LANs) with different protocols to communicate via VPN. For instance, LAN with Windows NT servers (using the NetBEUI protocol) can communicate with LAN with Novell servers (using the IPX protocol) through VPN without having any obstacles.

Tunneling is stated to be as a technology that allows a network transport protocol to carry information for other protocols within its own packets. The packets are delivered unmodified to a remote device that has been set up to handle them. The packet may be secured using data encryption, authentication, authorization or integrity functions. Figure 2.3 shows how tunneling process is made via Internetworking infrastructure.

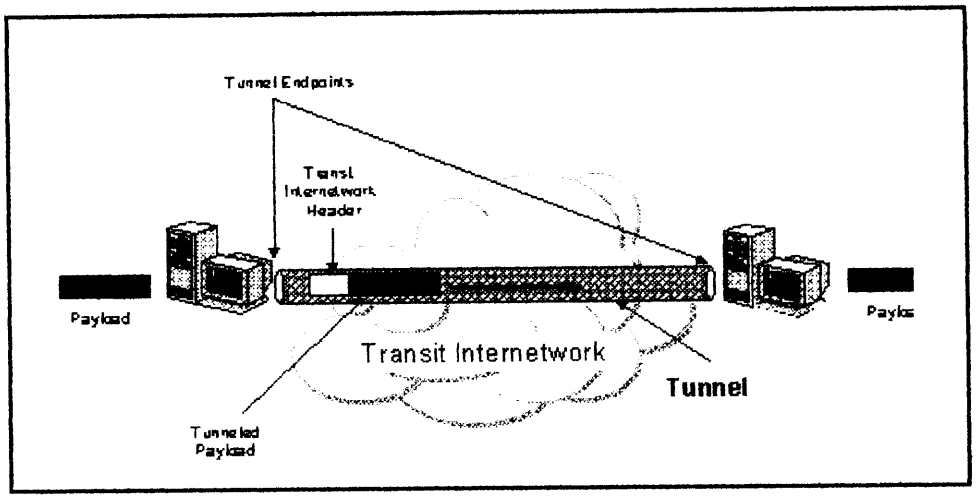


Figure 2.3: Tunneling Process

In general, there are two types of tunneling used in VPN, which are voluntary tunneling and compulsory tunneling. The brief descriptions of both tunneling types are:

1. Voluntary Tunneling
   - A user can issue a VPN request to configure and create a voluntary tunnel. In this case, the user's computer is a tunnel endpoint and acts as the tunnel client. Today, the voluntary tunneling is seen more popular than the compulsory tunneling.
2. Compulsory Tunneling
   - A VPN-capable dial-up access server configures and creates a compulsory tunnel. With a compulsory tunnel, the user's computer is not a tunnel endpoint. Another device, the remote access server located between the user's computer and the tunnel server is the tunnel endpoint and acts as the tunnel client.

2.3 Histories and Timeline (Evolution) of VPN

VPN is only just becoming reality though its technology has been under rapid development for some time. Some of the VPN background issues will be explained in below section.

2.3.1 Introduction of the Internet

The growth of the Internet in recent years has been nothing short of explosive and this trend seems set to continue progressively. The introduction and the development of the

Internet Protocol (IP), and the remarkable and insightful "go anywhere" interface provided by web browsers has made the Internet to be as a very useful and popular information gathering and publishing tool as well as a very cost-effective marketing and sales tool. In addition, web/Internet tools have proved to be very flexible and have been adapted for various applications. As a result, the tools are quite often used by many organizations within their private networks or intranets currently.

As the backbone capacity, sophistication and coverage of the Internet increases, new service offerings are being discovered and developed by ISPs. In this case, IP protocols development has allowed the Internet to support communication services traditionally carried by Telecommunication companies (Telcos), such as fax, voice, remote access and site-to-site, while also introduce new ways of doing business, such as Electronic Commerce (E-Commerce). However, it is found that the main technical problems facing these new Internet-based services are directly related to the provision of QoS and security features. Figure 2.4 shows the configuration of Internet-based services in VPN.

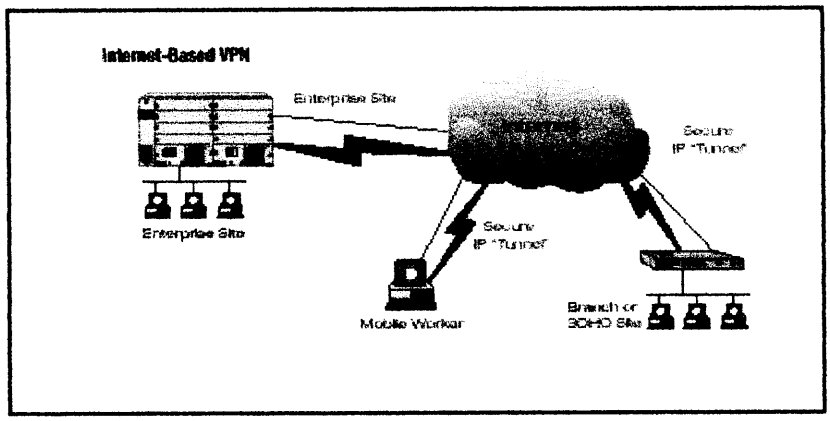


Figure 2.4: Internet-Based VPN

2.3.2 Timeline (Evolution) of VPN

Today, VPN is being adopted as a mean of reducing the cost of providing remote access to the ever-growing number of mobile workers and small branch sites requiring connecting to main corporate LANs. Remote access VPN commonly uses the Internet as the backbone and a Point-to-Point Protocol (PPP)–based tunneling technology to provide easy migration from traditional Remote Access Service (RAS) conducted on direct dial circuits. Recently, VPN carriers or ISPs have explored new service offerings that make

site-to-site and multimedia address QoS over VPN, such as Voice Over IP (VoIP) becomes a reality.

It is crucial for VPN carriers or ISPs to offer guarantees of throughput, reliability and accountability, especially for network managers who are willing to utilize VPN facility as a replacement of the traditional private site-to-site links, such as leased line. Until such time, network managers are likely to apply VPN as a supplement to their private site-to-site links to provide backup and top up. However, new VPN-focused data services are now beginning to emerge. These newly developed network features are expected to provide guaranteed traffic monitoring/reporting and Denial-of-Service (DoS) filtering services that network managers require before they can replace their private site-to-site links facility.

Some VPN carriers offer a VPN routing service where the customer's intranet routers are maintained by the ISPs. Thus, this will reduce the need for complex routing products in the customer's premises and will ease the installation of equipment in remote, unskilled sites. More over, these site-to-site or intranet VPN services can offer resilience, capacity and manageability at a much cheaper price compared to the cost of building and maintaining a traditional private network. Furthermore, these services can also encourage companies to completely outsource their networking requirements over time.

Note that, VPN can help organizations to expand their roles or operations by allowing extranet connections between organizations and their business partners, suppliers, vendors and customers for the purpose of E-Commerce. In this networking environment, aspects such as throughput, reliability, guaranteed services, traffic monitoring/reporting and accounting are vital.

Table 1 below depicts a timeline that outlines four VPN market phases and characteristics between the year 1998 and the year 2000 [8].

Time Frame	Market Phase	Market Characteristics
	Phase 1: Early Adopters	• Service trials • Telecommuters • Ad-hoc deployment
1998		
	Phase 2: Dial Migration	• Home workers • Mobile workers • Traditional dial-up for backup
1999		
	Phase 3: Branch Migration	• Use for top-up and back-up • Few tunnels, many users • Non-critical LAN-to-LAN traffic
2000		
	Phase 4 Extranets	• End-to-end QoS and SLAs • Many tunnels, many users • Mission critical LAN-to-LAN traffic • Secure Extranets

Table 1: VPN Market Phases and Characteristics

2.3.3 The First Remote Access VPN

The early version of VPN is mainly used for remote access relies on authentication and IP filtering offered by the VPN carriers. In addition, it also requires sharing of routing information between the corporation intranet and the VPN carriers. As a matter of fact, users who utilize dial service including modem and Integrated Services Digital Network (ISDN) to connect to ISP's Point Of Presence (POP) are classified as VPN subscribers via PPP authentication. In this case, IP filtering is applied to restrict traffic flow to VPN traffic only letting the subscribers exchange data with the designated corporate remote access concentration devices. Essentially, such VPN comprises of a private IP numbering space. This mechanism can also be used to provide intranet VPN connections, with tunnels used to allow multiprotocol support and private routing information exchange. However, this model has several limitations [8]:

1. When changes are needed to the client authentication database, the carrier needs to be contacted to make the change. This presents scalability and manageability issues. Some providers now offer customer-manageable networking, which allows the customer to share monitoring, and configuration responsibility with the provider.
2. With regard to security, the VPN customer needs to trust the carrier to authenticate the remote user correctly. Developments with IP Security (IPSec) would allow encryption between hosts, once hosts are equipped with this capability.

3. The VPN customer has no automatic mechanism for retrieving the cost information for the remote connection sessions, for example, the costs of dial connection time incurred by the remote users.

Despite those listed limitations, this model offers some useful features. For instance, when used in partnership with tunneling, security issues are under the control of the VPN customer, and multiprotocol support is more achievable.

2.3.4 The First Tunnel Protocols

Tunneling was devised as a mechanism to span a foreign and complex routed network in a single hop. This technology is accepted as the right approach to use the Internet for VPN building where private addressing is kept separate (hidden). When looking to replace a leased line with a VPN link over a shared and routed IP network, there are two main concerns:

1. Security and multiprotocol support issues where PPP is commonly used on leased lines and supports multiprotocol encapsulation and security.
2. Therefore, Layer-2 tunneling should allow a PPP tunnel to be established over a complex network.

2.3.5 The Emergence of Layer-2 Forwarding (L2F)

The Cisco Systems Inc. has developed L2F primarily as a tunneling service resided partly in the carrier's network and partly at the customer central offices. Through L2F, the remote dial clients connect to the carrier with PPP. In this case, the carrier does not allocate an Internet IP address (as for normal Internet account access). Instead, the carrier creates an L2F tunnel connection to the appropriate customer owned tunnel server. The tunnel then enables client-to-server PPP exchange, simulating a direct-dial PPP/RAS session. This approach allows standard dial-up networking to be used on the remote client systems (refer to Chapter 6.4.4 for more details about L2F).

2.3.6 The Emergence of Point-to-Point Tunneling Protocol (PPTP)

The Microsoft Corporation Inc. has introduced and developed the Point-to-Point Tunneling Protocol (PPTP). This is primarily intended as a "client-based" (new tunnel coded needed on client's PC) approach where the dial client obtains one Internet IP address from the carrier and then a second intranet address from the corporate tunnel server, again via client-to-server PPP. PPTP has been developed by third parties to allow legacy PPP implementations to make use of tunneling, such as PPTP in Windows 3.1.

Both L2F and PPTP are sorts of IP tunnels (PPP carried in IP) that carry PPP packets across the Internet mimicking the PPP exchange between a client and server for direct-dial remote access. In this way, the corporate server is in charge of authentication, and is able to negotiate "all things PPP" with the remote client, enabling common remote access features to be re-used for VPN remote access. Unfortunately, both L2F and PPTP approaches do not offer confidentiality, but client-to-server PPP exchange means that PPP encryption can be negotiated if required (refer to Chapter 6.4.2 for details about PPTP).

2.3.7 The Emergence of Layer-2 Tunneling Protocol (L2TP)

Due to the similarities between the L2F and PPTP proposals, the IETF agreed to merge the two protocols into a single standard approach known as L2TP. It is believed that the L2TP protocol will become the next-generation of the VPN technology. The L2TP approach is well supported by router manufacturers and is the subject of a dozen related IETF drafts. However, since L2TP offers little or no advantage over PPTP, it is unclear whether L2TP will be widely adopted by client software vendors. For non-IP intranet VPN links, L2TP is likely to become the tunneling technology of choice.

In recent months, L2TP has been identified as needing increased security to protect L2TP tunnels from certain security attacks. To resolve these problems, the recommendations from the IP Security (IPSec) working group are now required by conforming L2TP implementations (refer to Chapter 6.4.3 for more details about L2TP).

2.3.8 The Emergence of Internet Protocol Security (IPSec)

First-generation tunneling techniques (PPP, or Layer-2 tunneling) have now been joined by Layer-3 tunneling, which offers security at the IP layer between corporate security gateways. IPSec is a working group within the IETF and is likely to become part of all IP communication in the near future. The general goal of this group is to design cryptographic security for IP datagrams, which deliver integrity (protection from tampering), origin authentication (being able to trust the IP source address), data and traffic flow confidentiality (encryption and padding), and protection from "replay" security attacks (refer to Chapter 6.4.1 for more details about IPSec).

To make use of IPSec protocols to connect LANs over a VPN, the edge devices (routers/bridges) need to provide a secure IP tunnels between the sites; that is, the edge devices act as security gateways, as defined in the IPSec architecture. This does not require upgrades to hosts. In time, IPSec will be common on host systems using IPSec in "transport mode" to exchange confidential or authenticated information from host to host.

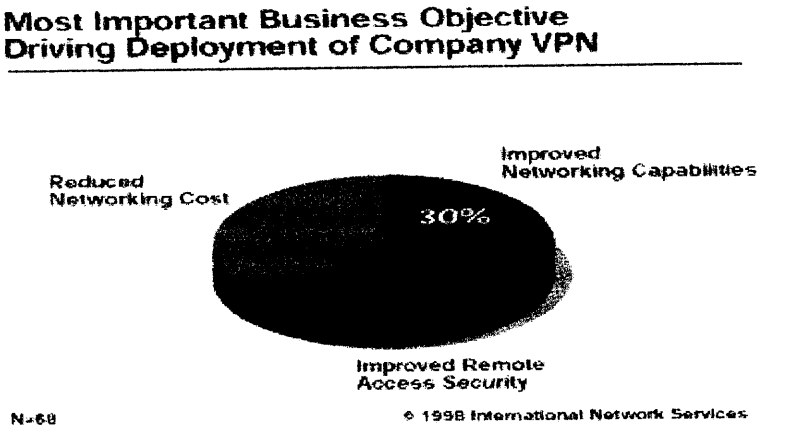
2.4 Market Trends of VPN

It is stated that VPN is already making its mark in the United States (US). A research being conducted by the Infonetics Research Inc. found that the percentage of corporate employees using VPN for the remote LAN access in the US rise from 8% in 1997 to 22% in 1999 (Ferrell). This situation is closely related the highly needs by remote offices to the central network as borderless business markets are constantly expanding.

Besides that, the Infonetics Research Inc. also estimated that by 1999, approximately 99% of all corporate companies in the US would be connected through high-speed Internet connections such as T1 carrier (Ferrell). The Infonetics Research Inc. also estimates that by 2001, VPN products sales alone will represent approximately US$1.19 Billion (Herscovitz 1998). According to Nortel Networks, the market for VPN services is forecasted to rapidly increase from today's US$200+ million to more than US$10 billion by 2001, as enterprise users are seeking to enhance the price and performance of their enterprise networks and leverage networking to their business advantage. In

addition, based on a recent survey (focusing on buyer's perspective) done by the International Computer Security Association (ICSA), VPN systems are becoming as another "big-ticket items" by positioning third on the list of "Top 10 products and services organizations plan to buy in near future". Furthermore, according to Gartner Group, by 2003 nearly 100% of enterprises will supplement their WAN infrastructures with VPNs [25]. To sum up, all these statistical values and customer's perspective findings possibly show a high demand on the utilization of VPN for business purposes.
It is reported by Taylor and Hecht (1999), some of the current market leaders of VPN are Cisco Systems, Nortel Networks, Checkpoint, Lucent Technologies, Nokia Corporation, and many others. More detail discussions will be made regarding the VPN key players in later part. As a matter of fact, it has been identified some of the VPN technology challengers are Frame Relay, Digital Subscriber Line (DSL) and ISDN.

Figure 2.5 shows a study on current market profiles of VPN whereas Figure 2.6 shows type and protocols of VPN, which was carried by International Network Services in 1998.



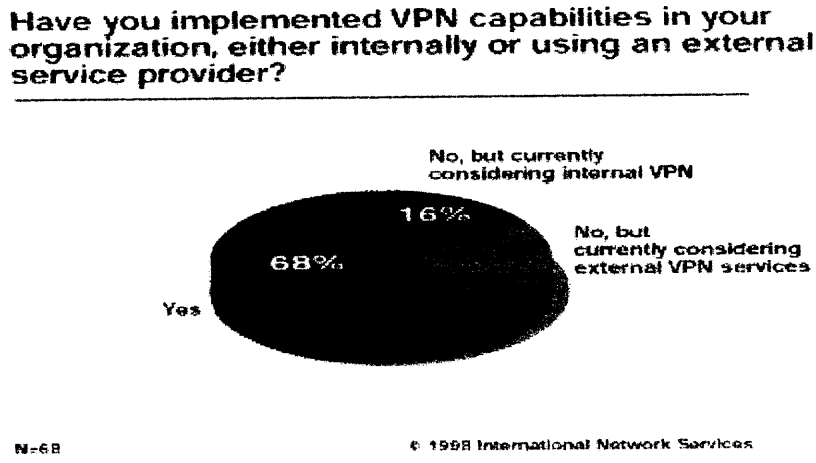
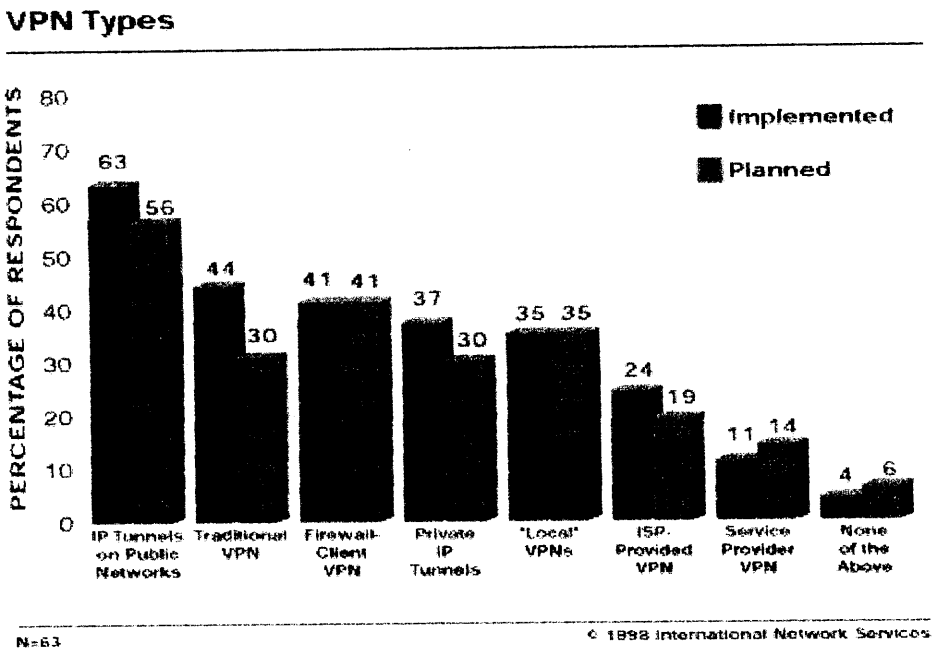


Figure 2.5: Current Market Profiles of VPN



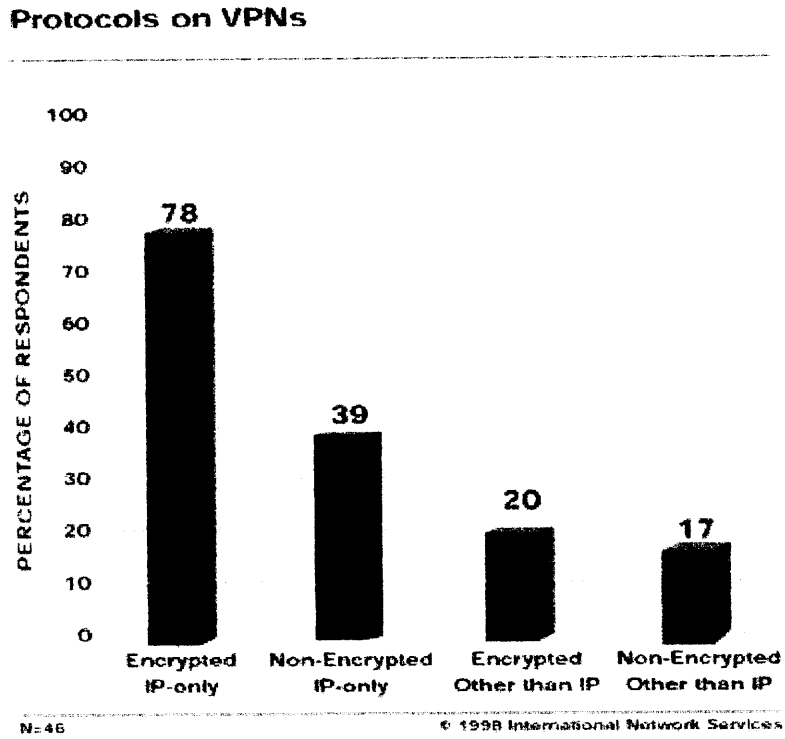


Figure 2.6: Type and Protocol of VPN in Market

2.5 Key Players of VPN

There are so many vendors worldwide involved directly in the VPN technologies development. All the vendors have their own resources and specialties in consulting and supporting technically corporate that implement VPN as their WAN solutions. Let review briefly 6 of VPN key players.

2.5.1 Cisco Systems

Cisco Systems is actually taking the leadership in developing VPN through the use of IPSec protocol. In this case, IPSec protocol has become a standard-based method of providing privacy, integrity, and authenticity to information transmitted via IP-based VPN. Cisco Systems has developed L2F technology as its proprietary tunneling implementation. There are 5 key components of VPN solutions delivered by Cisco Systems that are:

1. Platform scalability for VPN to meet bandwidth changing and connectivity needs.
2. Security through tunneling, encryption, and authentication mechanisms.
3. VPN services including bandwidth management and QoS functions such as queuing network congestion avoidance, traffic shaping, packet classification and routing services.
4. Appliances such as firewalls, intrusion detection and active security auditing.
5. Management through enforcing security and bandwidth management policies and monitoring the VPN circuits.

Cisco Systems also offered a suite of sophisticated VPN-enabled and VPN-optimized routers spanning the range of VPN applications:

1. Telecommuters and Small Offices: Cisco 800, Ubr900 and 1400 Series Routers.
    - The Cisco 800 series, which have four router models, provide secure ISDN access to the Internet and the corporate LAN. By incorporating Cisco Internetwork Operating System (IOS) features including IPSec, L2TP, GRE, and the Cisco IOS Firewall Feature Set, the Cisco 800 extends VPN applications to telecommuters and very small offices. The Cisco Ubr900 and 1400 series, with support for IPSec, L2TP, and the Cisco IOS Firewall feature set, provide integrated VPN

solutions for cable- and DSL-based VPN. The Cisco Ubr900 cable access router is a fully integrated Cisco IOS router and Data-over-Cable Service Interface Specification (DOCSIS) 1.1 standard-based cable modem, thus ensuring interoperability with cable networks and other Cisco IOS devices. The Cisco 1400 series provide high-performance connectivity from Ethernet to ATM cell-based Digital Subscriber Line (DSL) WAN infrastructures with support for multiple DSL standards.

2. Small Branch Offices: Cisco 1700 Series Routers.
   - The Cisco 1700 access router is a modular solution that provides all the necessary components required to build an integrated VPN solution on one platform. Powered by a RISC processor, the Cisco 1700 is optimized to support VPN applications with full Cisco IOS software support for encryption, tunneling, QoS, Cisco IOS Firewall, and an option for compression. The Cisco 1700 series features an auto sensing 10/100 Fast Ethernet port, up to 3 modular voice or WAN interface card slots, and one auxiliary (AUX) port. The Cisco 1700 series is also flexible in supporting any of WAN interface cards for the Cisco 1600, 2600, and 3600 platforms, including ISDN, Serial, and Integrated Data Service Unit / Channel Service Unit (DSU/CSU) cards.
3. Medium-Sized Branches and Small Regional Offices: Cisco 2600 and 3600 Series Routers.
   - Both Cisco 2600 and 3600 are effectively one extended family of products since they share so many of the same Network Modules (NMs) and WAN interface cards. The Cisco 2600 is an ideal platform for VPN because its RISC processor provides the power to run the robust Cisco Internetwork Operating System (IOS) security, tunneling, and QoS features that make the virtual network privates. On the other hand, the Cisco 3600 series offer higher-performance RISC processors and higher density VPN platform for large branch offices and small regional offices. With packetized voice modules, both Cisco 2600 and 3600 series are already enabled for the expansion of VPN from data to multiservice.

4. Regional Offices and Headquarters: Cisco 7100, 7200, and 7500 Series Routers.
   - Cisco 7100, 7200, and 7500 series routers integrate high-speed, industry-leading routing with comprehensive VPN services, such as tunneling, data encryption, security, advanced bandwidth management, and service-level validation. Cisco 7200 and 7500 series routers are able to provide scalable VPN solutions while also accommodating extensive private WAN aggregation requirements. The Cisco 7100 series VPN router supplements VPN solutions offered by both Cisco 7200 and 7500 series, providing scalable. As members of the Cisco 7000 routers family, the Cisco 7100, 7200, and 7500 share interface cards, known as port adapters. Each of these platforms supports IPSec, L2TP, L2F, and Generic Routing Encapsulation (GRE) for tunneling and encryption of data transmitted over the Internet. The Cisco 7100 and 7200 also support Point-to-Point Tunneling Protocol (PPTP) and Microsoft Point-to-Point Encryption (MPPE) as well as the Cisco IOS Firewall feature set to enable stateful packet filtering on the routing infrastructure.

2.5.2 Nortel Networks

Nortel Networks actually deliver a broad range of connectivity solutions, a growing breadth of performance and QoS capabilities, network and application-level security, customer-service and policy capabilities, and billing. The current and future products in Nortel Networks VPN architectures provide [40]:

1. Highly scalable robust platforms.
2. Differentiated and enhanced services to customers.
3. Improved profit margins for IP services.
4. A competitive differentiator for driving away new entrants.
5. A competitive differentiator against new entrants capitalizing on the existing investment in router, Frame Relay, and ATM infrastructures.

Nortel Networks also provides integrated solution for ISP known as Integrated Network Management (INM), which is based on emerging standards Telecommunication Management Network (TMN) and Telecommunication Information Networking

Architecture (TINA) as architectural guidelines, and CORBA and JAVA as standard computing technology components.

2.5.3 IBM Networking Divisions

IBM has been a leader in the deployment of Layer-2 Tunneling Protocol (L2TP) for tunneling process (refer to Chapter 6.4.3 for details about L2TP). The major components of L2TP focused by IBM are:

1. Network Access Server (NAS).
2. L2TP Access Concentrator (LAC).
3. L2TP Network Server (LNS).
4. Remote Access Dial In User Services (RADIUS).
5. Authentication, Accounting, and Authorization (AAA) Functions.
6. Point-to-Point Protocol (PPTP).

2.5.4 Microsoft Corporation

The Microsoft Corp. emphasizes on the use of PPTP to enable a security of the data transfer from a remote client to a private enterprise server by establishing VPN across TCP/IP-based data networks. Basically, there are three computers involved in each PPTP deployment that are PPPTP Client, NAS, and PPTP Server [37]. The company's PPTP with NOS, such as Windows NT Server V4.0 and Windows NT Workstation V4.0 has its unique benefit where it can support VPN by applying Public Switched Telephone Network (PSTN).

2.5.5 Enterasys Incorporated

Enterasys is a company that offers VPN solutions to small businesses and enterprise customers in cost-effectively connecting their own sites (small offices, branch offices, and larger sites) and in building a secure link to business partners across the Internet and other IP networks. In this case, the cost of VPN is streamlined by providing [8]:

1. Flexibility to migrate from private WAN to VPN services based on specific requirements.

2. Lower equipment costs by integrating VPN gateway and routing capability into a single device.
3. Lower network management expenses by offering a single set of SPECTRUM management tools to manage both private WAN and VPN environments.
4. Lower bandwidth costs by allowing customers to select the right combination of private WAN and VPN services.
5. Greater choices of the appropriate access technology at each site depending on telecommunication tariffs, application requirements and backup requirements.

2.5.6 Nokia Incorporated

Nokia is a company that is really serious in providing VPN customer with a high security and availability to insure continuous Internet connectivity. A service known as Nokia IP Network Security Solutions has been introduced by the company to offer an unprecedented level of redundancy in maximizing fault tolerance and in ensuring continuous Internet connectivity.

Besides, the service also is applied to provide fast, seamless recovery of firewall resources. This is done by combining the Virtual Router Redundancy Protocol (VRRP) with standard routing protocols, such as Border Gateway Protocol 4 (BGP4), Open Shortest Path First (OSPF), and RIPv2, and with the Check Point FireWall-1 synchronization feature on Nokia IP Network Application Platforms [45]. As a result, network managers enable to deploy fully redundant and highly available router firewall configurations. Figure 2.7 shows the layout of Nokia IP Network Application Platforms with the VRRP and the firewall synchronization.

Technically speaking, the unique Nokia approach to delivering firewall redundancy has several key benefits, such as firewall redundancy does not require host or server reconfiguration, integrated router firewall platform simplifies redundant configuration and setup, fast "cutover" time in the event of a network failure maximizes network uptime and provides seamless transition, and lastly load-sharing capabilities allow for maximum use of critical network resources and eliminate firewall bottlenecks.

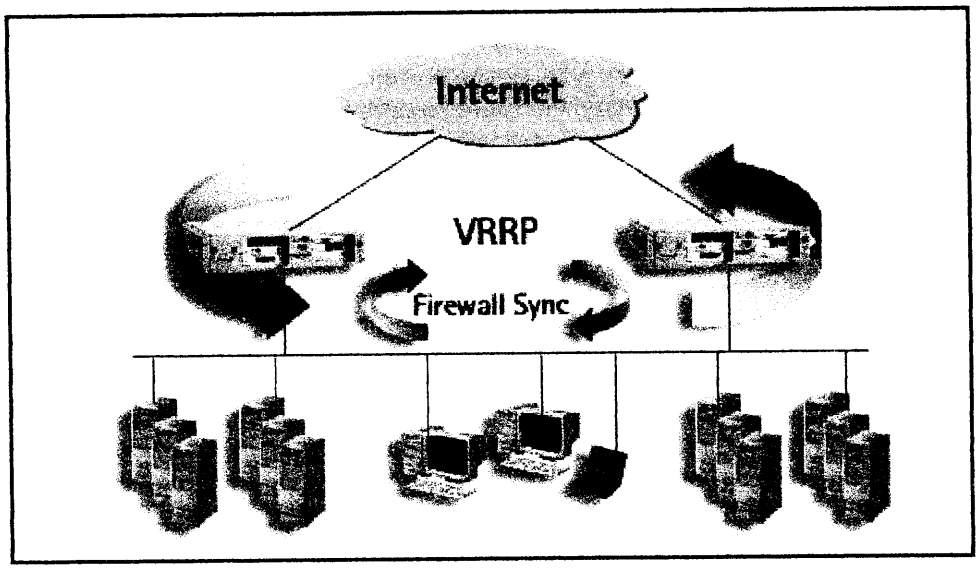


Figure 2.7: Nokia IP Network Application Platform

As a matter of fact, Nokia offered three types of platform or IP network security solutions devices that can support managed firewall services [47]:

1. Nokia IP650
   - Provides carrier-class security and high-bandwidth throughput for corporate clients with large networks; supports a comprehensive suite of IP-routing functions and protocols for both unicast and multicast traffics; and ensures high service availability through features like hot-swappable components.
2. Nokia IP440
   - Reliable, scalable, economical, easy-to-use, flexible and high-speed performance package for delivering Internet access and network security; has the capability to support up to 16 physical interfaces; and permits fully centralized remote management via a Web-based management application that operates with any standard browser.
3. Nokia IP330
   - Ideal, low-cost, and simple-to-install for deployments at small organizations or client sites with fairly simple and secure network-connectivity needs, such as remote offices; supports a comprehensive suite of IP-routing functions and protocols for both unicast and multicast traffics; and includes the remote-management features of Nokia Voyager, making it highly effective for small branch office installations.

2.6 Environment Suitable for VPN

Theoretically, VPN is found most suitable for organizations that really require good WAN solutions that can provide flexibility in terms of quickly creating new partner links, extensively supporting project teams in the field worldwide and well handling large number of telecommuters directly involved in mobile sales force. In this case, many organizations have found that past WAN solutions such as dedicated leased line and Frame Relay architectures have technical limitations in fulfilling extensive networking requirements as mentioned earlier.

According to Nortel Networks (www.webproforum.com), nowadays many organizations tend to use VPN since it can allow network managers to connect remote branch offices and also project teams to the main headquarter economically and efficiently. Besides, VPN is widely chosen since it reduces a lot of cost savings due to less in-house requirements for communication device and technical support.

However, due to certain limitations, VPN is not really suitable for all cases. Since the Internet or shared Public Network being as the main VPN backbone, the network is found not that reliable in guaranteeing the data integrity and confidentiality. The data transmitted via Internet backbone is having high probability to be "hacked" and "modified" by network perpetrators. Besides, ISP might temporarily unable to give maximum services to avoid delays at a critical moment especially when full bandwidth is strongly required to cater heavy traffics. In addition, since the VPN QoS aspect is left to ISP (instead of being integrated into corporate networking policy), many organizations may have limited control and authorization in manageability, scalability and interoperability of their own VPN, which is not really beneficial in the long-term run.

VPN is found not the best WAN solution specifically for organization dealing with highly confidential data at high transfer rates. In this case, federal organizations such as the Ministry of Defense or Bank Negara should stick to the classic WAN solutions such as Frame Relay circuits or perhaps very dedicated leased lines to avoid many threats, such as loss of privacy, loss of data integrity, identity spoofing, and Denial of Service.

CHAPTER 3

CONFIGURATION OF VPN

VPN is generically referred to a Layer-2 (equivalent to the Data Link layer in the Open Systems Interconnected (OSI) model) VPN. The emerging form of VPN is a network constructed across shared IP backbones, referred to as IP VPN. Each kind of VPN has it own challenges, and different ways in which it can be built. This section will provide 8 different configurations of VPN that support today's business:

1. Untrusted Private Network
2. Trusted Private Network
3. Corporate-to-the Internet
4. De-Militarized Zone (DMZ)
5. Behind an Existing Firewall
6. Additional Firewall and Tunnel Functionality
7. Adding a VPN to an Existing Firewall Infrastructure
8. Internal Application

3.1 Untrusted Private Network

Untrusted private network means that users on each LAN require their interconnected communications to be protected and authenticated but at the same time, do not allow to grant unrestricted access to each other's networks. For example, Company A and Company B are both competitors and want to share some common information (such as quality or safety standards, product universal specifications, press release, etc) within themselves, but do not permit each other to access any other information.

This scenario shows a tunnel between the two companies. Both companies have VPN Gateway attached, with firewall functionality enabled on both ends. The tunnel endpoints both terminate on the side of the VPN Gateways. For example, traffic going from Company A to Company B must first exit from Company A's firewall, then

permitted to go through Company B's firewall [18]. Figure 3.1 shows the configuration of untrusted VPN.

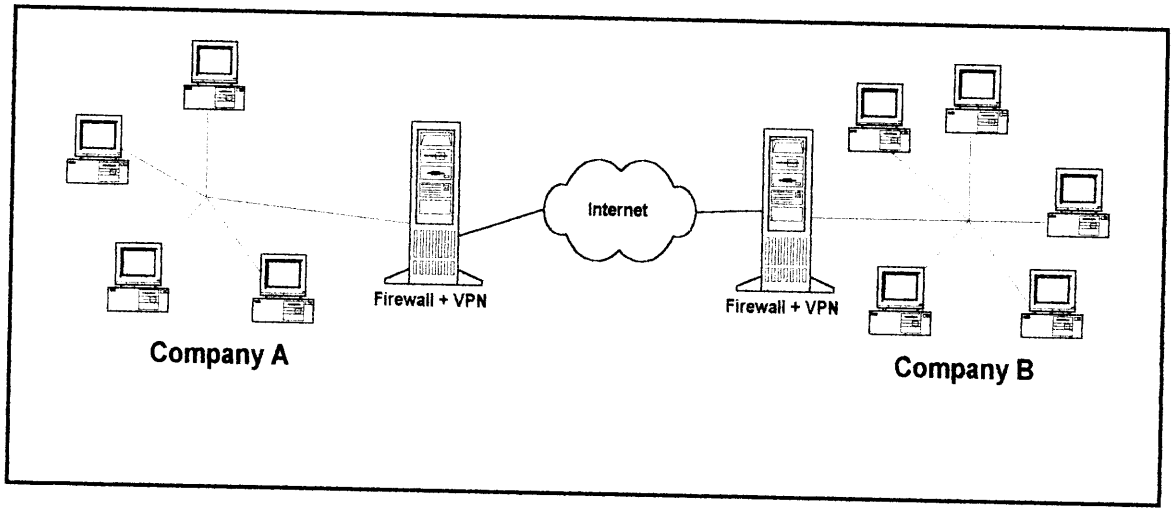


Figure 3.1: LAN-to-LAN Connection for an Untrusted Private Networks

3.2 Trusted Private Network

Trusted private network means that users on one LAN are permitted to access to other connected LAN via the Internet backbone. For instance, connecting a branch office to corporate headquarter. Basically, the configuration of trusted private networks is different from the configuration of untrusted ones. In this case, the trusted private networks configuration allows users on each LAN to access all resources on other LAN. Both interconnected LAN is supposedly secured from external perpetrators or hackers.

Lets review how data is transmitted between the untrusted LAN-to-LAN connections through the Internet. Firstly, the packets coming from corporate headquarter will be encrypted for security reasons. Secondly, the packets will undergo the encapsulation process before being sent through the VPN tunnel. Finally, the encrypted and encapsulated packets will be transmitted to the branch office, by bypassing any firewall functions. At the branch office, the packets will be decapsulated and decrypted so that the receivers can read and understand the sent data correctly. The same processes also happen for packets, which are sent from branch offices to corporate headquarter. Note that, although, there is no firewall functionality applied to the tunnel traffic, the firewall

do still operates to prevent the VPN from be attacked by Internet perpetrators or hackers [18]. Figure 3.2 shows the configuration of untrusted private networks.

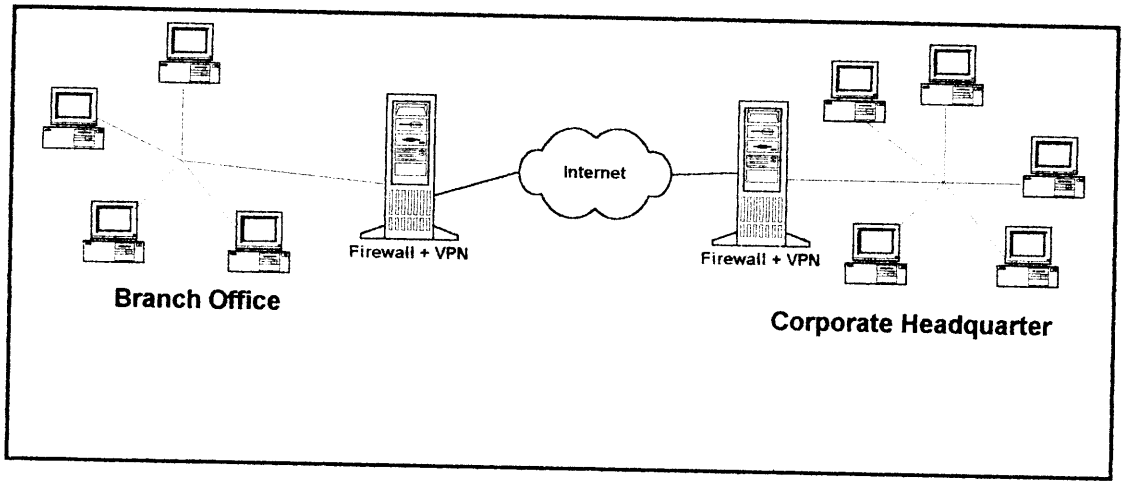


Figure 3.2: LAN-to-LAN Connection for a Trusted Private Networks

3.3 Corporate-to-the Internet

Corporate-to-the Internet model allows user to access to corporate network applications, such as Corporate E-Mail Server, Material Requirement Planning (MRP), and Bills-of-Material (BOM). In this case, a remote employee running the VPN client is able to download and send mail to corporate main network via the Internet.

As a matter of fact, both the Internet user and remote user are actually passing through the Internet. The difference between the two parties is that the Internet user is usually restricted to a specific application (e.g. Corporate E-Mail Box) or a specific server, whereas the remote user is not. All of the Internet users must enter the network through the firewall whereas employees (with the VPN client) have the option to enter the network via the VPN gateway connected into the corporate network [18]. Figure 3.3 shows the difference between the Internet user and the VPN client who are passing through the Internet.

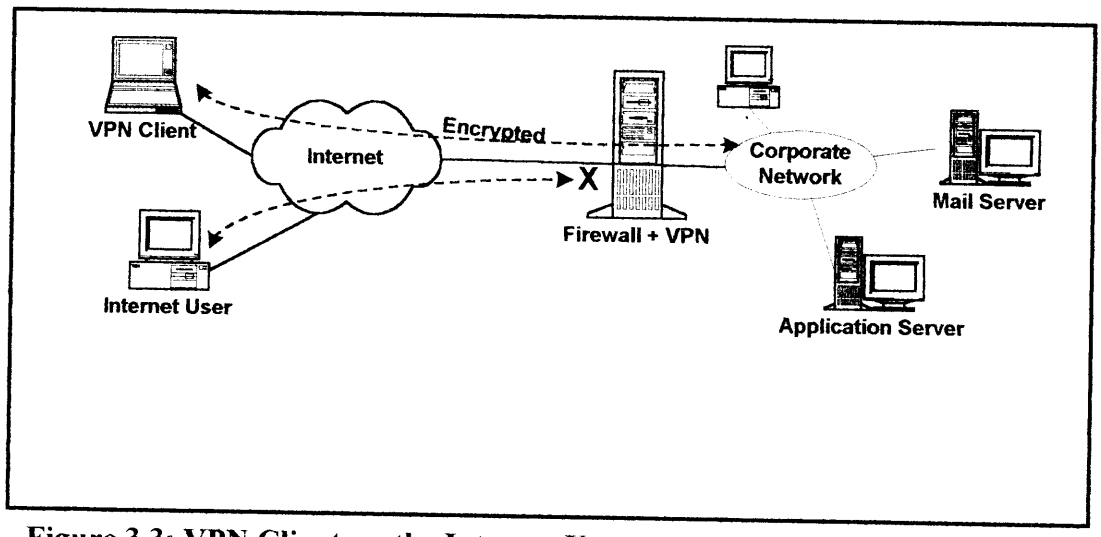


Figure 3.3: VPN Client vs. the Internet User

3.4 De-Militarized Zone (DMZ)

Two VPN Gateways are set up between the corporate network and the Internet. The De-militarized zone (DMZ) is an intermediary zone from which certain services, such as Web are offered. In this case, the VPN Gateway closest to the Internet serves as a pure firewall that protects the DMZ from the Internet. The other VPN Gateway serves as a firewall protecting corporate network from the DMZ and a tunnel for remote users running the VPN client software.

This setup protects the corporate network from a compromising an application running on a device on the DMZ. For example, if a hacker discovers a way to get into a Web server, the only device the hacker can be accessed is that on the DMZ only [18]. Figure 3.4 shows the configuration of corporate network with the DMZ.

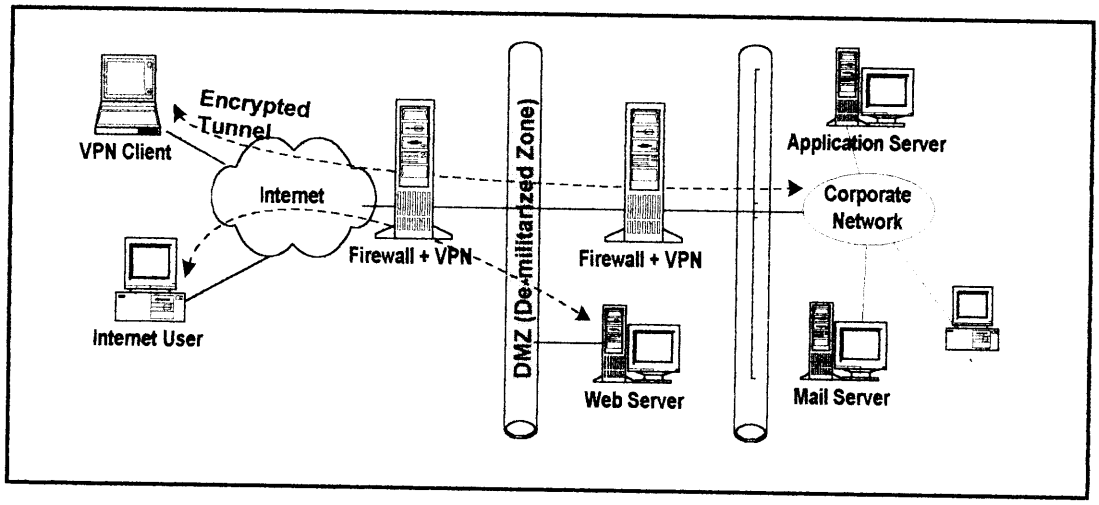


Figure 3.4: Secure Corporate Network and DMZ

3.5 Behind an Existing Firewall

In this case, a Corporation may add a VPN Gateway behind an existing third party firewall because there is a need for extensively communication with its customers and suppliers through this firewall. The VPN Gateway is actually set up to sit behind the existing third-party firewall. This model does not require the VPN Gateway to have any enabled firewall functions. This is due to the VPN Gateway is primarily used to serve the tunnel traffic and to transmit all the traffic to the customers and suppliers' networks through itself. The best thing of having this model is that there is no routing issue to be emphasized [18]. Figure 3.5 shows the configuration of adding VPN Gateway behind an existing firewall.

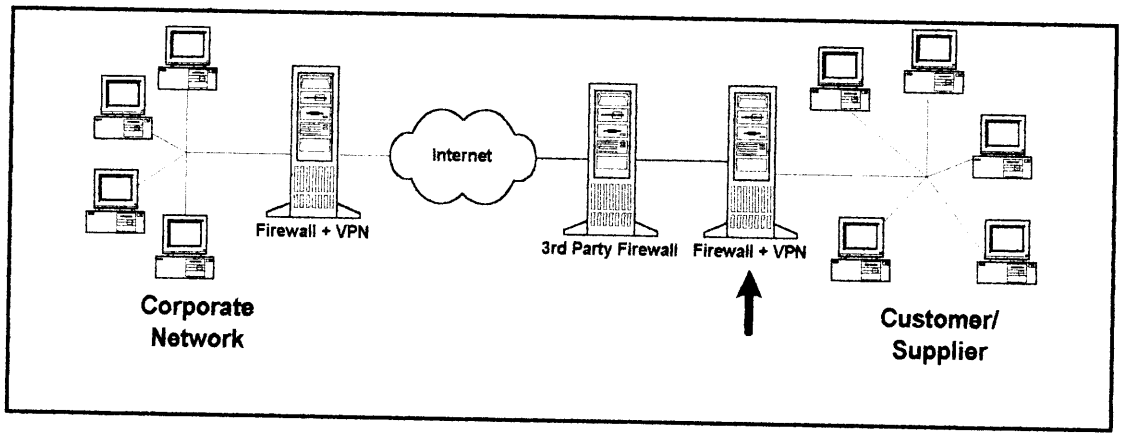


Figure 3.5: VPN Gateway and Existing Third-Party Firewall

3.6 Additional Firewall and Tunnel Functionality

In some cases, a corporation may add a VPN Gateway next to an existing third party firewall because there is a need for extensively communication with customers and suppliers through this firewall. This will allow the customers and suppliers to have two firewalls and two paths out of their network.

The VPN Gateway will handle the traffic between the customers and the suppliers' networks and the corporate network. In addition to that, the VPN Gateway will enable firewall functions as well as will bypass the existing third-party firewall. On the other hand, the existing third-party firewall is fundamentally used for all other kinds of traffic [18]. Figure 3.6 shows the configuration of a VPN Gateway added to the next of an existing third party firewall

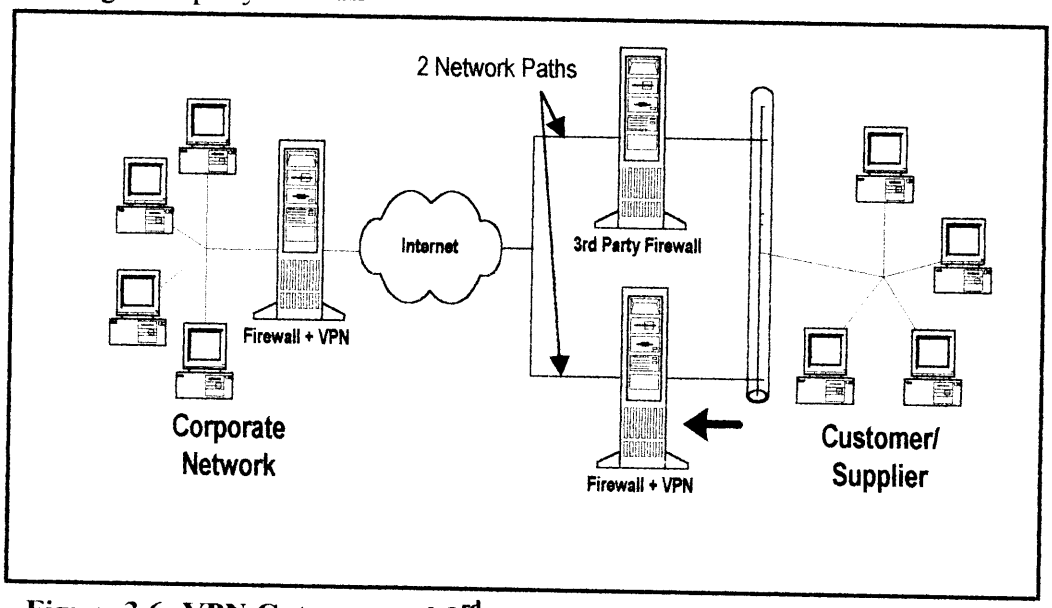


Figure 3.6: VPN Gateway and 3rd Party Firewalls with 2 Network Paths

3.7 Adding a VPN Gateway to an Existing Firewall Infrastructure

In certain situations, customers and suppliers may not want to remove the third-party firewall although the corporation has a VPN gateway in place. In this case, the VPN Gateway is placed on the customers and suppliers' networks to handle the traffic from the corporate network.

In this VPN configuration, there will be no firewall function enabled on the VPN Gateway. Instead, the VPN Gateway will only handle the encryption and decryption of packets transferred through the tunnel between the corporate network and the customers and suppliers' networks. This setup actually provides some advantages, which are [18]:

1. Does not affect the customers and suppliers' existing network infrastructures.
2. Is totally transparent to end-users.
3. Is secure where there is only one path out of the network so all access control is in one place.

Figure 3.7 shows the configuration of a VPN Gateway added to an existing firewall infrastructure in the customers and suppliers' sites.

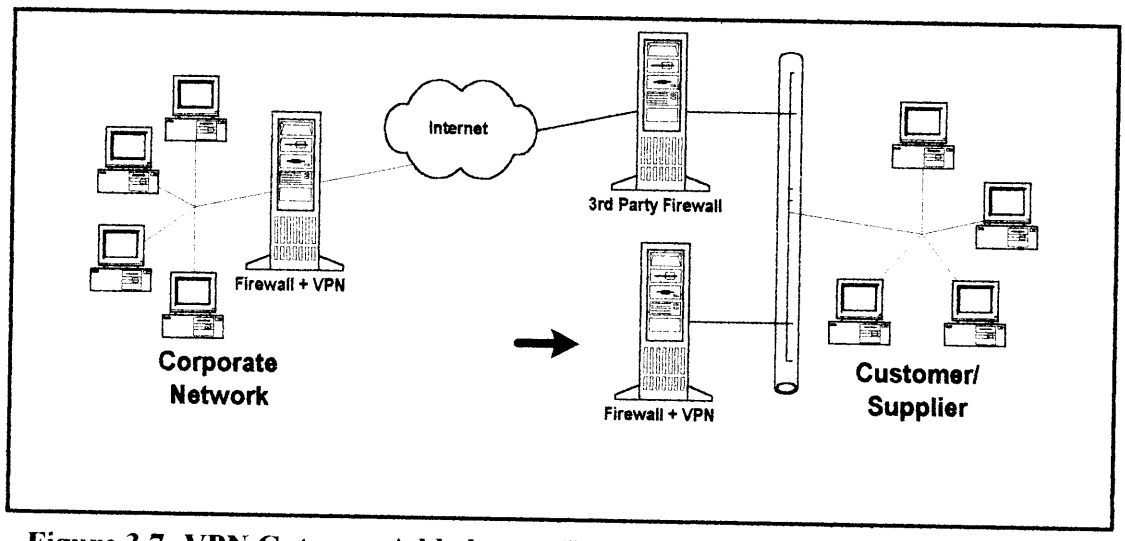


Figure 3.7: VPN Gateway Added to an Existing Firewall Infrastructure

3.8 Internal Applications

Sometimes, a VPN Gateway is installed between the corporate network and a separate and a secure LAN within a company. For example, the secure LAN may consist of the servers used by the Human Resource Department to store highly confidential employees' personal particulars and their payroll records. In this case, the Human Resource Department employees have the authority to access the servers on the secure LAN through the tunnel with the installed client software. Any other unauthorized employees

however cannot get access to it. This configuration setup actually ensures that the sensitive data is secured by undergoing the encryption in the tunnel. The encryption method is more secure than normal application control since the data is not recognizable or unreadable even though a hacker can see it through a Sniffer or any other network analyzer [18]. Figure 3.8 shows configuration setup of VPN Gateway to provide a secure LAN within a company.

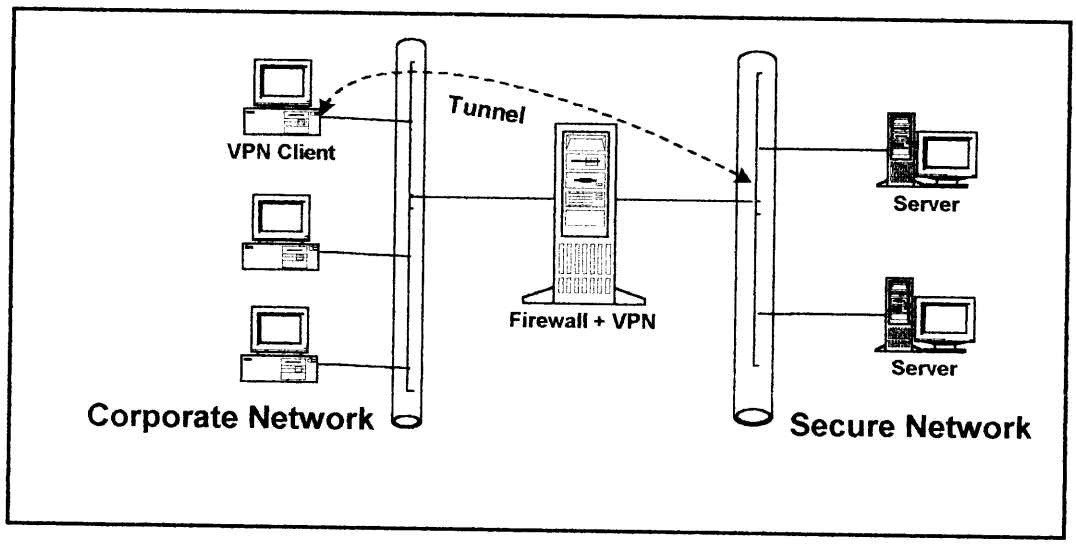


Figure 3.8: VPN Gateway Added to Create a Secure LAN within a Company

SECTION 4

APPLICATIONS OF VPN

4.1 Extranet Application

This type of VPN provides scalable, secure connectivity between an enterprise and its strategic partners, suppliers and customers through standards-based tunneling. In this case, all the connected parties will enjoy the same policies as a private network, including security, QoS, manageability, and reliability. The VPN requires an open, standards-based solution to ensure the interoperability among the various solutions implemented by the business partners [24]. The de facto protocol used for the Internet-based VPN is actually the Internet Protocol Security (IPSec) standard. Figure 4.1 shows graphically the Extranet VPN.

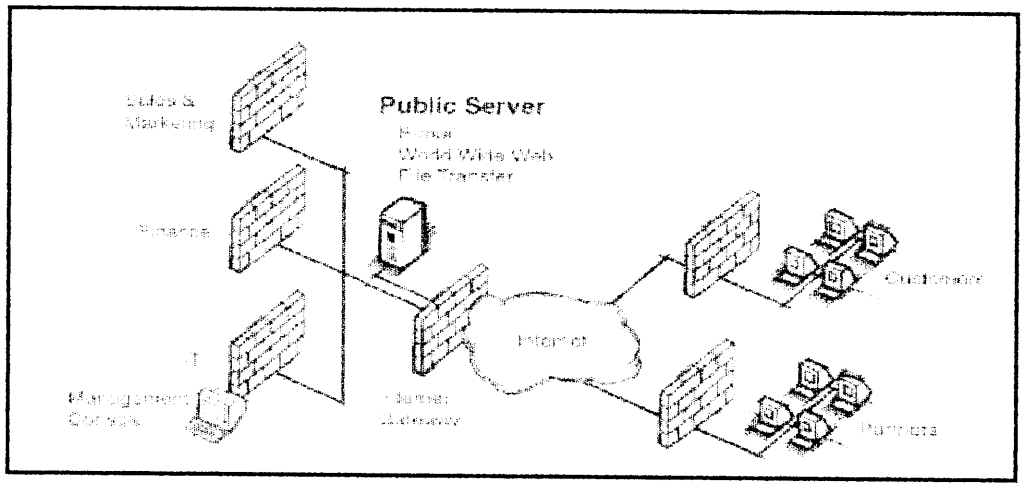


Figure 4.1: Extranet VPN

Network Configurations included in providing the extranet VPN solution are:

1. Untrusted Network (Refer to Section 3.1)
2. De-Militarized Zone or DMZ (Refer to Section 3.4)
3. Additional Firewall and Tunnel Functionality (Refer to Section 3.6)
4. Adding a VPN Gateway to an existing Firewall Infrastructure (Refer to Section 3.7)

4.2 Remote Access Application

This type of VPN provides remote or mobile employees with a reliable access to the corporate intranet (or extranet) over a shared infrastructure with the same policies as a private network. Remote access VPN enables users to access corporate resources whenever and wherever they require via a broad range of access technologies including 56 Kilobits per Second (Kbps) switched-modem, Integrated Services Digital Network (ISDN), cable-modem, and Digital Subscriber Line (DSL) technologies.

The VPN critically requires strong authentication to verify remote or mobile users' identities in the most accurate and efficient manner possible [24]. Besides, the remote access VPN also needs a good centralized management and a high degree of scalability to cater the enormous number of users accessing the network simultaneously. Figure 4.2 shows graphically the Remote Access VPN.

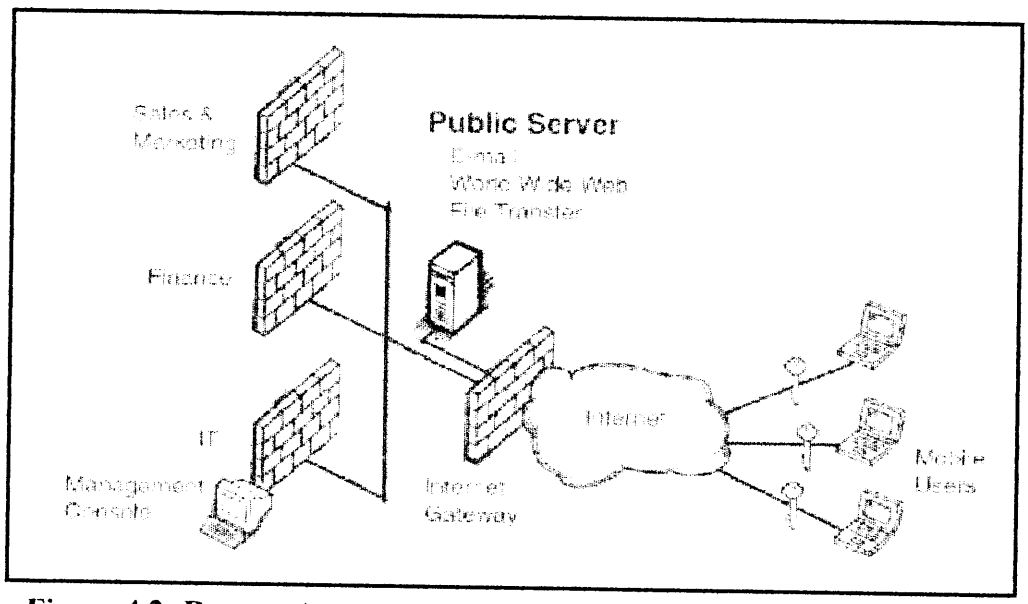


Figure 4.2: Remote Access VPN

The connectivity to support remote access VPN can be made through dialing into any local Point-of-Presences (POPs), tunneling through the Internet, and accessing the corporate network securely without incurring long distance charges associated with direct dialing. Two configurations can be used to support the remote access application are:

1. Corporate-to-the Internet (Refer to Section 3.3)
2. De-Militarized Zone or DMZ (Refer to Section 3.4)

4.3 Intranet (Site-to-Site) Application

This type of VPN application offers scalable, secure IP connectivity among enterprise sites including corporate headquarters, remote offices, and branch offices. The connectivity is made by deploying tunneling over the Internet, Layer-2 (such as, Frame Relay or Asynchronous Transfer Mode (ATM) backbone) connectivity protocols, or a combination of the two depending on the user needs. All the connected sites enjoy the same policies as a private network, including security, quality of service (QoS), manageability, and reliability. The primary technology requirements are [24]:

1. Strong data encryption to protect sensitive information.
2. Reliability to ensure the prioritization of mission-critical applications, such as Manufacturing Resource Planning (MRP-II) systems, sales and customer database management, and document exchange.
3. Scalable management to accommodate the rapidly outgrowth of new users, new offices and new applications.

Figure 4.3 shows graphically the Intranet VPN.

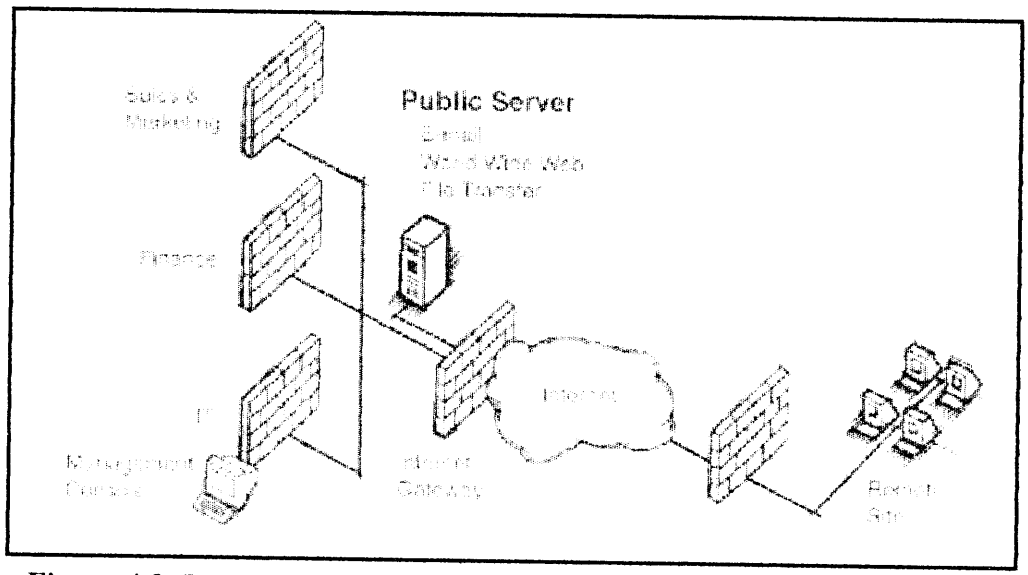


Figure 4.3: Intranet VPN

Two network configurations suitable for the intranet VPN application are:

1. Trusted Network (Refer to Section 3.2)
2. Corporate-to-the Internet (Refer to Section 3.3)

4.4 Enterprise Application (E-VPN)

This type of VPN provides the integration of voice and data applications on a single scalable, reliable, high-bandwidth network. This encourages the enterprise to outsource more than just intersite and remote-access IP networks besides offers ISP the option of managing portions of the enterprise in-building network.

In addition, E-VPN can extend the corporation's network boundary and through it offers new business opportunities and supports for many new-networked applications [42]. This is because E-VPN solutions capable to support all three of the abovementioned applications simultaneously, allowing offices worldwide to access network resources, mobile workers to link up to corporate intranets, customers to place orders and suppliers to check inventory levels, all in a highly secure and cost-effective manner.

Technically speaking, E-VPN demands a greater need of security to protect confidential data passing over the public network infrastructure from being observed and tampered by perpetrators, and to prohibit unauthorized users from gaining access to network resources and proprietary information [42]. There are four key areas of E-VPN security that need to be emphasized, which are authentication, perimeter security, encryption, and intrusion detection. Figure 4.4 shows graphically the layout of E-VPN.

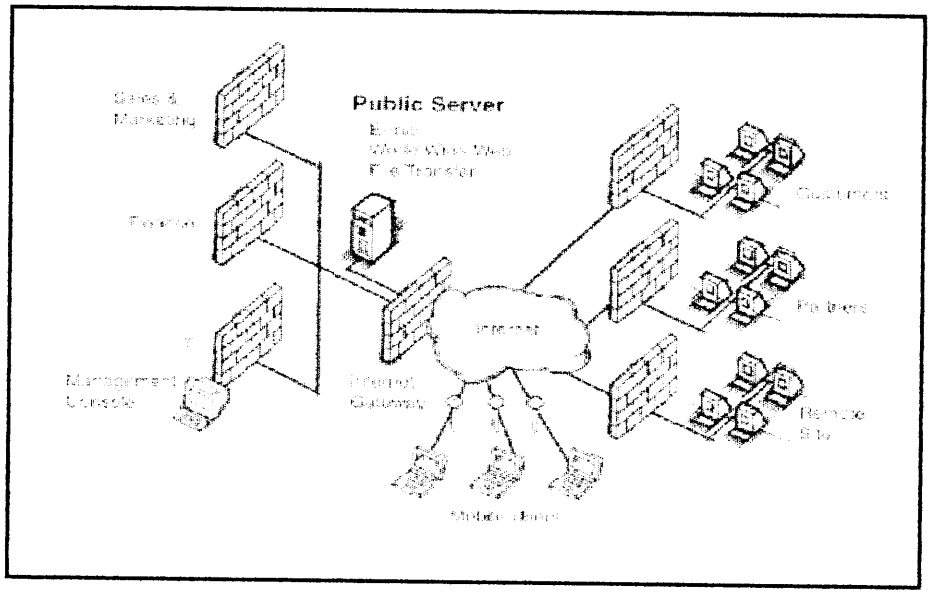


Figure 4.4: Enterprise VPN (E-VPN)

Figure 4.5 shows Cisco's 5-point E-VPN strategy built on the currently offered tool kit of E-VPN platforms, security, services, appliances, and management solutions, as well as offered with greater functionality and performance in an open, standards-based approach [42].

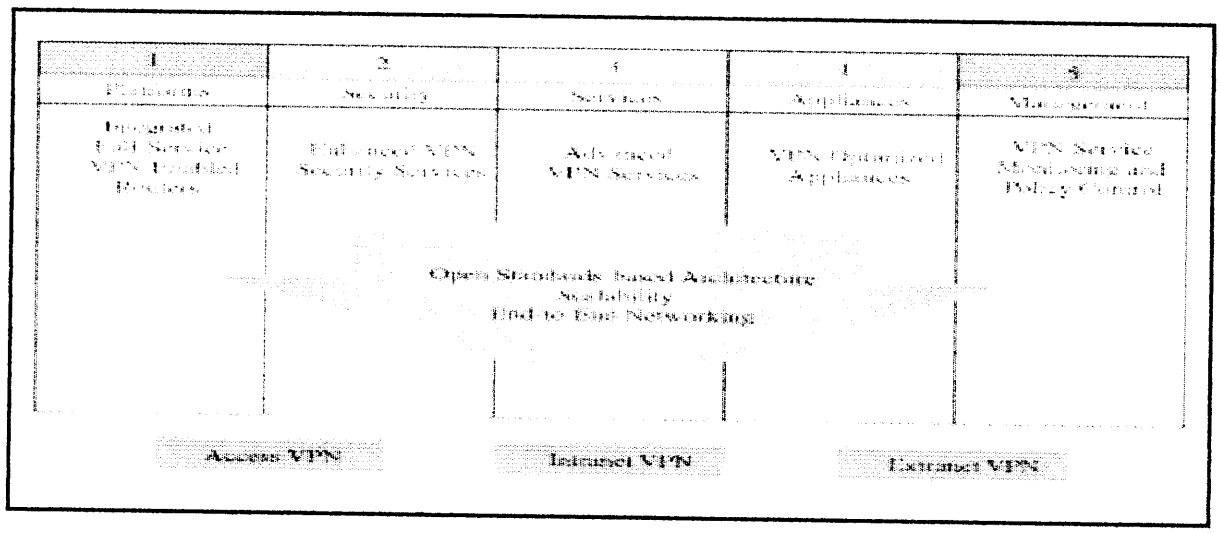


Figure 4.5: Cisco's 5-Point E-VPN Strategy

4.5 Firewall Application

A VPN Gateway can be used to operate as an alternative firewall replacing existing firewall or working in addition to the existing firewall. Depending on the business processes, requirements and environments, network configurations enlisted below can be set as a model to support the firewall VPN application:

1. Untrusted Network (Refer to Section 3.1)
2. Corporate-to-the Internet (Refer to Section 3.3)
3. De-militarized Zone or DMZ (Refer to Section 3.4)
4. Behind an Existing Firewall (Refer to Section 3.5)
5. Additional Firewall and Tunnel Functionality (Refer to Section 3.6)
6. Adding VPN to an Existing Firewall Infrastructure (Refer to Section 3.7)
7. Internal Application (Refer to Section 3.8)

4.6 Internal Application

In this case, a VPN Gateway is used as a firewall to handle applications across LANs or within a LAN. The only network configuration that supports this model is internal application (Refer to Section 3.8 for details).

CHAPTER 5

CORE COMPONENTS OF VPN

The breadth of features offered by VPN defines its solutions. A VPN platform must be secure from intrusion and tampering, deliver mission-critical data in a reliable and timely manner, and be manageable across the enterprise. Unless each of these requirements is addressed, the VPN solution is incomplete. Technically speaking, the essential elements of the VPN solution can be segmented into 5 broad categories [25]:

1. Platform Scalability

   - Each of these elements must be scalable across VPN platforms to enable cost-effective provisioning, and service excellence for an expanding customer base, from the smallest business to the largest global enterprise, including engineering and the ability to provision tens of thousands of VPN. Besides, the platform should have the ability to meet changing bandwidth and connectivity needs, which is crucial in a VPN solution.

2. Security
   - Should include privacy equivalent to what other types of private network offered today. In this case, tunneling, encryption, encapsulation, and packet authentication are necessary for transport security on public networks. Besides, user authentication and access control are also essential in VPN, specifically for assigning network privileges and access (refer to Chapter 6 for more details on VPN security).
3. VPN services
   - Bandwidth management and QoS functions such as queuing network congestion avoidance, traffic shaping, and packet classification are important for VPN implementation (refer to Chapter 9 for more details on QoS for VPN). Furthermore, VPN routing services utilizing Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) are also essential elements to be emphasized in VPN.

4. Appliances

- Tunnels and encryption, packet authentication, firewalls and intrusion detection, user authentication, and active security auditing are essential for comprehensive VPN perimeter security. This is because enterprises need to be assured that their VPNs are always secure from perpetrators and hackers observing or tampering with confidential data passing over the network and from unauthorized users gaining access to network resources and proprietary information. Actually, these appliances or mechanisms complement each other, providing security at different points throughout the network. VPN solutions must offer each of these security features in order to be considered as a viable solution for utilizing a public network infrastructure.

5. Management

- Monitoring the network manageability through security enforcement and bandwidth management policies across the VPN are very important for cost-effective provisioning, management, and billing. With the advanced manageability monitoring and automated flow-through systems, new services can be rolled out so quickly and also end-to-end customer Service Level Agreements (SLAs) can be supported as well. Besides, imposing priority is also vital to ensure proper handling of various traffic types particularly for both mission-critical (for example, Service Access Point or SAP) and time-sensitive (for example, voice and videoconferencing) ones. Another aspect is the reliability management, which is essential for high service uptime that business customers always expect and require.

Those above-listed five key components are actually delivered within the context of open standards, scalability, and provide end-to-end networking capabilities to ensure that the IP-VPN services are fit for robust implementations.

CHAPTER 6

SOLUTION FEATURES OF VPN

6.1 Internet-Firewall

Firewall is actually a very important solution element to be focused in designing and building a secure VPN via the Internet. This is because, a firewall is used significantly to examine Internet addresses on packets or ports requested on incoming connections to decide what traffic is allowed into a network with VPN solutions. Let reviews briefly on a firewall in terms of its definition, functions, architectures and current applications model manufactured by the Cisco Systems Inc.

By definition, a firewall is actually a set of related programs, located at a network gateway server that protects the resources of a private network from other networks' users [39]. Through a firewall, a corporate can prevent outsiders from accessing its own private data resources and can control what outside resources its private network's users have accessed to.

The firewall functions can be thought of as a pair of mechanisms: one that exists to block traffic, and another that exists to permit traffic (Ranum and Curtin 1998). For a firewall to be effective, all traffic to and from the Internet must pass through the firewall, where it can be inspected. The firewall must permit only authorized traffic to pass, and the firewall itself must be immune to penetration. Unfortunately, a firewall system cannot offer any protection once an attacker has gotten through or around the firewall (Semeria 1996).

Note that an Internet firewall (as what is used in VPN) is not just a router, a bastion host, or a combination of devices that provides security for a network. The firewall is actually just a part of an overall security policy that creates a perimeter defense designed to protect the information resources of an organization. This security policy must include published security guidelines to inform users of their responsibilities, corporate policies that define network access, service access, local and remote user authentication, dial-in and dial-out, disk and data encryption, virus protection measures, and lastly employee

training (Semeria 1996). Besides, all network potential attack must be protected with the same level of network security. It can be said that setting up an Internet firewall without a comprehensive security policy is like placing a steel door on a tent.

Firewalls that can be deployed in networks with VPN services are typically implemented based on one of four primary architectures or building blocks enlisted below:

1. Packet Filtering Routers or Screening Routers
   - It has been known that many commercial routers or better known as screening routers provide the capability to screen packets based on criteria such as the type of protocol, the source address and the destination address fields (Cooper 1995). In details, a screening router or sometimes called as packet-filtering router will make a permit or a deny decision for each packet that it receives (Semeria 1996). The router will examine each datagram to determine whether it matches one of the packet-filtering rules. The packet-filtering rules are actually based on the packet header information that is made available to the IP forwarding process. The packet header's information includes the IP source address, the IP destination address, the encapsulated protocol (such as TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), or IP Tunnel), the TCP/UDP source port, the TCP/UDP destination port, the ICMP message type, the incoming interface of the packet, and lastly the outgoing interface of the packet. If there is a match and the packet-filtering rule permits the packet, the packet will be forwarded according to the routing table information. In contrast, if there is a match and the rule denies the packet, the packet will be discarded. However, if there is no matching rule, a user-configurable default parameter determines whether the packet is forwarded or discarded. The enterprise private network's boundary is called the security perimeter. Because malicious hackers abound on the Internet, it is useful to define a zone of risk. The zone of risk is an all TCP/IP-capable network directly accessible through the Internet. TCP/IP-capable means the host supports the TCP/IP protocol its support protocols. "Directly accessible" means that there is no strong security measures between the Internet and hosts on the enterprise network. Figure 6.1 shows how a screening or packet-filtering

router forms a security perimeter. Generally, there are two types of packet-filtering service in making a permit/deny decision for every packet received by the screening routers:

a. *Service-Dependent Filtering*: It deals with the packet-filtering rules that allow a router to permit or deny traffic based on a specific service, since most service listeners reside on well-known TCP/UDP port numbers.

b. *Service-Independent Filtering*: It deals with certain types of attacks that are difficult to identify using basic packet header information because the attacks are service independent.

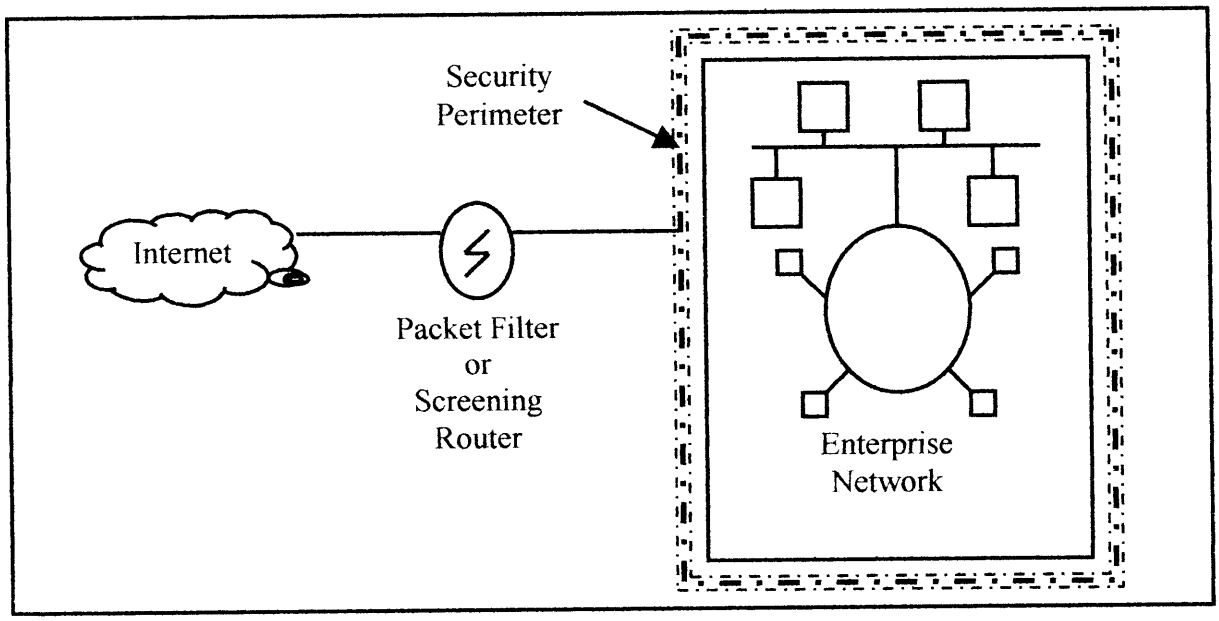


Figure 6.1: Screening Router Forming a Security Perimeter

2. Circuit-Level Gateways

- A circuit-level gateway is actually a specialized function that can be operated via an application-level gateway. A circuit-level gateway simply relays TCP connections without performing any additional packet processing or packet filtering. Telnet connection can also be operated via a circuit-level gateway. In this case, the circuit-level gateway simply transmits the Telnet connection through the Internet firewall without doing additional examination, filtering, or management of the Telnet protocol. In other words, the circuit-level gateway acts like a wire, copying bytes back and forth between the inside connection and the

outside connection. However, since the connection appears originally from the Internet firewall system, the circuit-level gateway conceals or hides information about the protected network. Circuit-level gateways are often implemented for outgoing connections where the system administrator trusts the internal users. Figure 6.2 below shows the diagram of the circuit-level gateway operation.

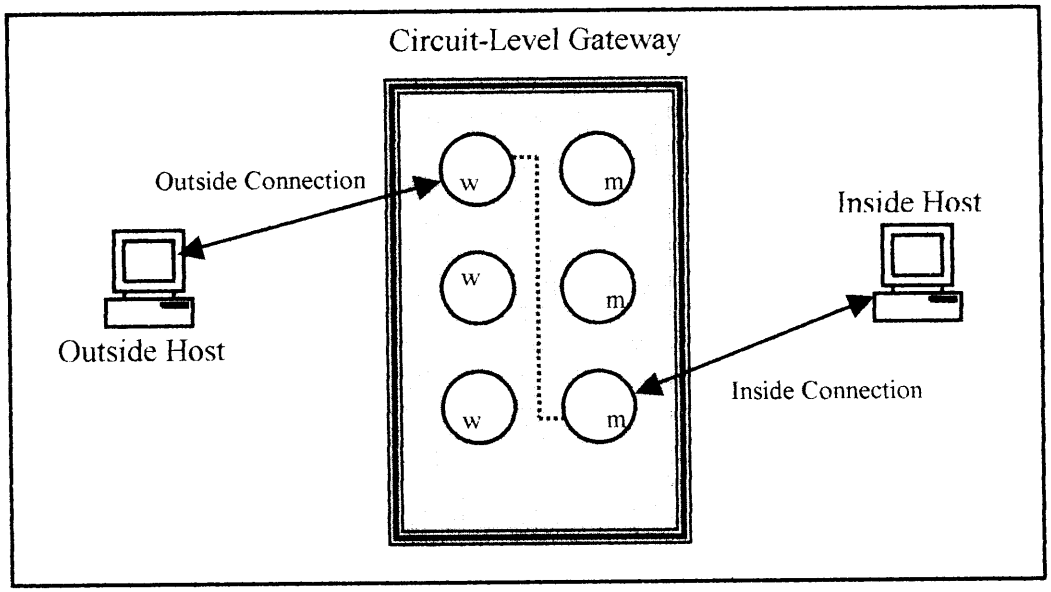


Figure 6.2: Circuit-Level Gateway Operation

3. Application-Level Gateways or Proxy Servers
   - An application-level gateway allows the network administrator a much stricter security policy than with a packet-filtering router (Semeria 1996). Rather than relying on a generic packet-filtering tool to manage the flow of Internet services through the Internet firewall, a special-purpose code is installed on the gateways for each desired application via proxy servers. A proxy server is actually a component of an Internet Firewall that controls how internal users access the outside world (the Internet) and how Internet users access the Internet network (Sheldon 1996). In certain situations, the proxy server will block all outside connections and will only allow internal users to access the Internet. In this case, the only packets that are allowed through the proxy server are those that return responses to requests from inside the Internet firewall. In some other cases, both inbound and outbound traffics are allowed under strictly controlled conditions.

Note that a virtual air gap exists in the Internet firewall between the inside and outside networks. The proxy servers then will bridge this gap by working as agents for internal or external users. An application-level gateway is often referred to as a bastion host because it is a designated system that is specifically armored and protected against attacks (Semeria 1996). The bastion host hardware platform executes a "secure" version of its Operating System (O/S) specifically to protect against O/S vulnerabilities and to ensure the Internet Firewall integrity. Figure 6.3 shows the diagram of the application-level gateway operation.

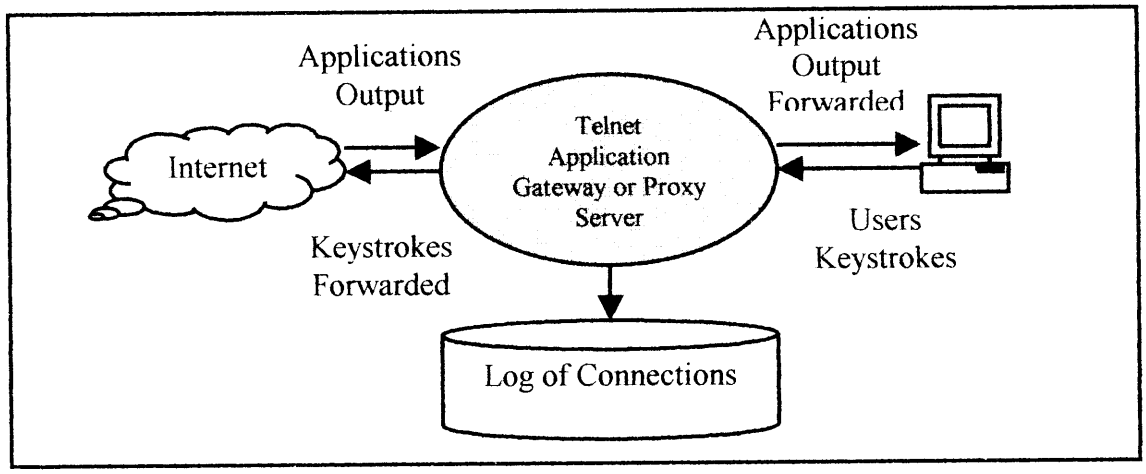


Figure 6.3: Application-Level Gateway Operation

4. Network Address Translation (NAT)

- Firewalls using NAT and/or Port Address Translation (PAT) completely hide the network protected by the firewall by translating the outgoing packets to use different addresses. The Internet firewall is a logical place to deploy NAT that can help to alleviate the address shortage and eliminate the need to renumber when organization changes ISPs (Semeria 1996). In most implementations, there is a single public IP addresses used for the entire network. PAT needs to be added to NAT in order to handle port conflicts. A disadvantage of NAT is that it cannot properly pass protocols containing IP address information in the data portion of the packet.

Cisco Systems Inc. has introduced and developed the Cisco PIX Firewall as a dedicated firewall appliance in Cisco's firewall family. Refer to Figure 6.4 for a configuration of a network with a PIX firewall.

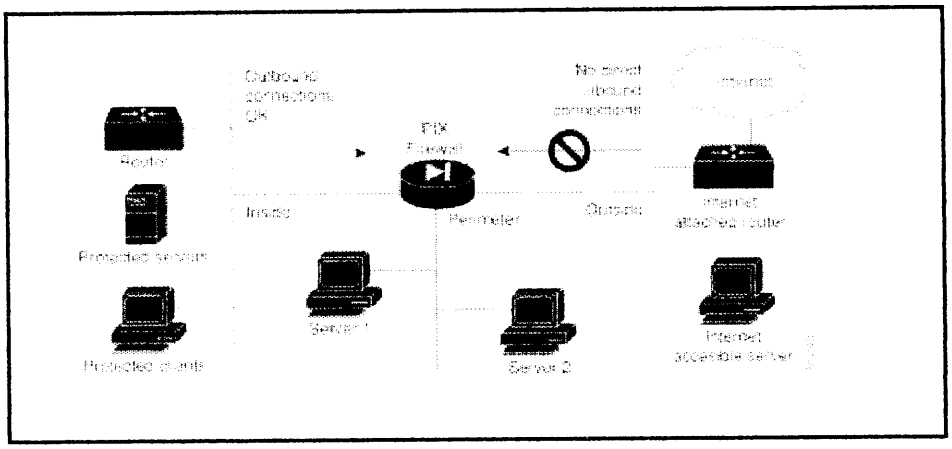


Figure 6.4: Cisco Secure PIX Firewall in a Network

Currently, the Cisco Systems Inc. has scaled up 4 models of PIX firewall to meet a range of customer requirements and network sizes:

1. *Cisco Secure PIX 525:* Is intended for Enterprise and ISP use. Has a throughput of 370 Mbps with the ability to handle as many as 280, 000 simultaneous sessions. Has the 600 MHz CPU that enable to deliver an additional 25% ~ 30% of increased capacity for firewalling services.
2. *Cisco Secure PIX 520:* Intended for large Enterprise organizations and complex high-end traffic environments. Has also a throughput of up to 370 Mbps with the ability to handle 250,000 simultaneous sessions.
3. *Cisco Secure PIX 515:* Intended for Small/Medium Business and remote offices deployments and has throughput measured at 120 Mbps with the ability to handle up to 125,000 simultaneous sessions.
4. *Cisco Secure PIX 506:* Intended for high-end Small Office/Home Office (SOHO) organizations and has throughput measured at 10 Mbps.

All 4 models have IP Security (IPSec) encryption built-in, permitting both site-to-site and remote access VPN deployments, and operate on a hard operating system focused on protecting both the security of the device and the networks.

6.2 Encryption/Decryption

It is essential for VPN to do the encryption methods to ensure the security, integrity, and confidentiality of data transmitting into the wide area link or in the Internet. This is because the encryption methods are capable to prevent snuffers from picking up data transmissions through VPN (Ferrell). Let review briefly the encryption methods in terms of its definition, implementations, algorithms, and VPN applications.

Generally speaking, encryption can be defined as the process of using mathematical formulas to scramble computer data into unreadable code that can be de-ciphered only by authorized persons who hold the key to the code [7]. In other definition, encryption is described as the process of converting some information from an easily understandable format into what appears to be random and useless gibberish (Hughes 1995).

The inversion of encryption is known as "decryption" where only the intended readers can have authority and capability to covert the encrypted information back to its original and intelligible format of data. In this case, the terms "plaintext" is referred to the original message or information before encryption whereas the terms "ciphertext" is referred to the encrypted message or information after undergoing encryption. Figure 6.5 shows one example of message in both plaintext and ciphertext forms.

Plaintext:	**PLEASE FINISH UP ASSIGNMENTS**
Ciphertext:	**SOHDVH IMQMVL XS DVVLJQPHQWV**

Figure 6.5: Plaintext versus Ciphertext

The encryption processes actually can be implemented in a number of steps or simply refers as "algorithms" involving well-defined rules, decisions, and calculations (Hughes 1995). Companion encryption and decryption algorithms are jointly known as "cryptosystem". Some cryptosystems offer more than a standard fare of encryption and decryption. These can produce "digital signatures" for messages that unambiguously identify the messages' senders respectively. Digital signatures actually are methods of

authentication involving encrypting a message in a way only the sender would know (Shay 1999). Besides that, the sender also would send the encrypted message along with an implicating "key", which is a specific set of codes to be used by the algorithm to perform the required encryption (Beyda 1996). There are two kinds of key used for sending the encrypted message (generating by the intended recipient) that are "private key" and "public key".

Let review some common simple cryptosystems invented for manipulating and processing both encryption and decryption algorithms, which are:

1. Caesar cipher.
    - It is one of the earliest and simplest codes replaced each plaintext with another character where the choice of a replacement depends only on the plaintext character (Shay 1999). The method used here is called a "Monoalphabetic cipher" or "Caesar cipher", reputedly dating back to the days of Julius Caesar. Caesar imagined the letters of the alphabet arranged horizontally, and then shifted (or rotated) each to the right three positions. Figure 6.6 shows the Ciphertext after being shifted three positions.

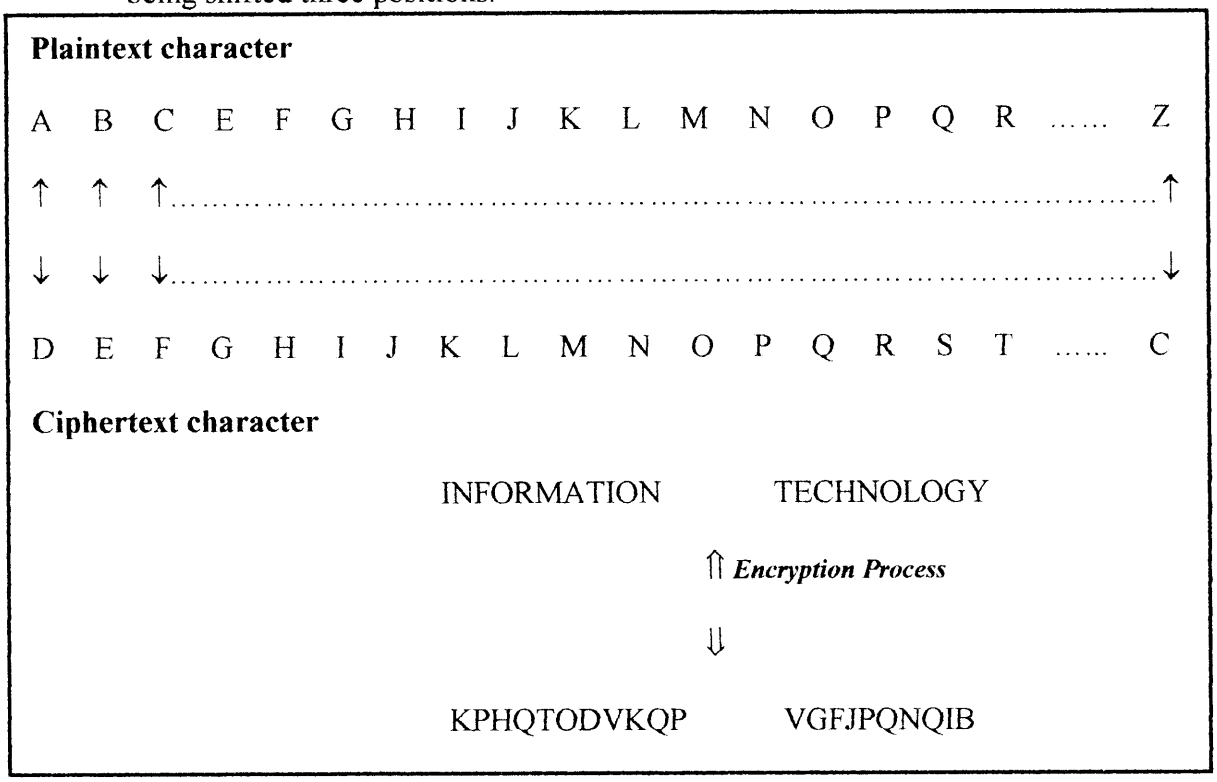


Figure 6.6: The Caesar Cipher

2. Polyalphabetic cipher.

   - One way to change the frequencies and to destroy common sequences is through the utilization of Polyalphabetic cipher (Shay 1999). Similar to the Monoalphabetic cipher, it replaces every character with another. What makes thing difference is a given plaintext character is not always replaced with the same ciphertext one respectively. In this case, a replacement depends on two factors, which are the actual plaintext character and the plaintext character position in the message as well. An example of a Polyalphabetic cipher is a "Vigene're cipher" that applies a 2-Dimensional array of characters (encryption key) in which each row contains the alphabet letters (Shay 1999). Figure 6.7 shows an example this type of cipher.

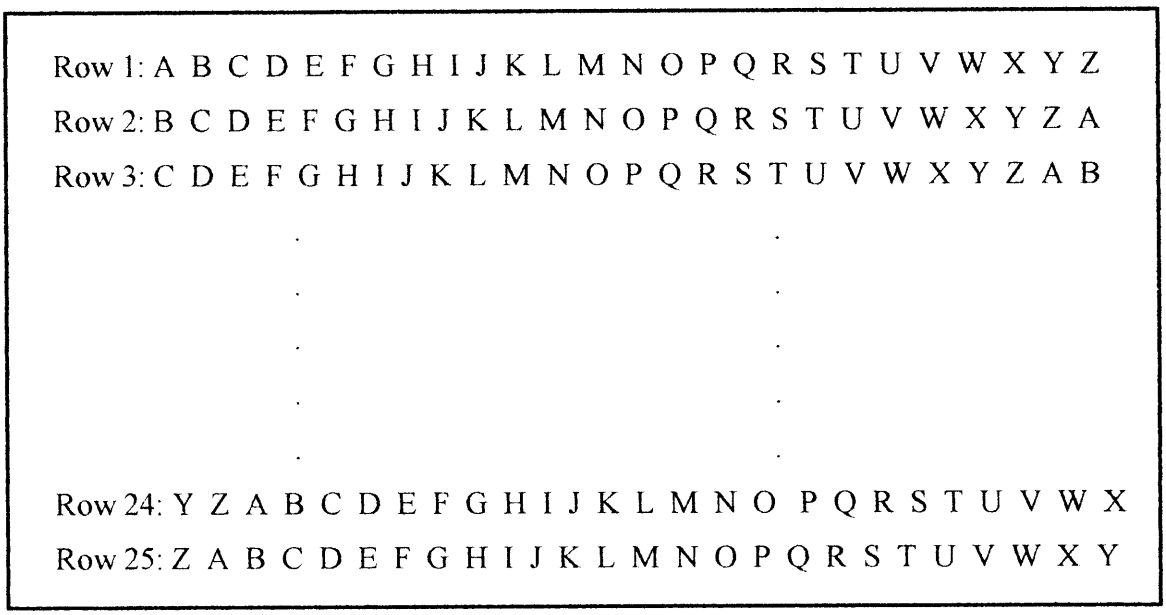


Figure 6.7: Key for Vigene're Cipher

3. Transposition cipher.

   - A Transposition cipher actually rearranges the plaintext letters of a sent message instead of doing ciphertext letters substitution (Shay 1999). One method to do this is by storing the plaintext letters in 2-Dimensional array with *m* columns. The first *m* Plaintext characters are stored in the array's first row, the second *m* characters in the second row, and so on continuously. The next step is to determine a permutation of the numbers 1 through *m*, and write as *p1*, *p2*, *p3*, ...,

pm. The permutation may be assigned randomly or may be determined by some secret method. Either way, the final step is to transmit all the characters in column *p1*, followed by those in column *p2*, and so on. In this case, the last set of characters transmitted are those located in column *pm*. For example, suppose the following message's character are stored in a 2-Dimensional array with 4 columns (refer to Figure 6.8):

UNIVERSITI UTARA MALAYSIA

Lets rearrange column numbers as 3, 2, 1, and 4 where the characters in column 3 are transmitted first, followed by the characters in column 2, 1, and 4 respectively. As a result, the transmitted message would be:

IS RASNRIAMYUETT AA VIUALI

COLUMN NUMBER			
1	***2***	***3***	***4***
U	N	I	V
E	R	S	I
T	I		U
T	A	R	A
	M	A	L
A	Y	S	I
A			

Figure 6.8: Transposition Cipher's Two-Dimensional Array

Some of the primary Encryption Algorithms Standards widely used in computer networking today are (Hughes 1995):

1. Data Encryption Standard (DES)
   - In 1977, the United States of America Government made the DES as the federal standard for the encryption of commercial and sensitive-yet-unclassified government computer data. The DES has its roots in the Lucifer algorithm

invented by IBM in the early 1970's. The logic of this widely used method is built into hardware (such as Very Large-Scale Integrated [VLSI] chips) to make it even faster. The DES divides a message into 64-bit blocks and uses a 56-bit Key (Shay 1999). The DES uses complex combination of transpositions, substitutions, exclusive OR (XOR) operations, and some other processes to produce 64-bits of encrypted data. In general, the 64-bits data should go through 19-succesive steps where the output of each step being inputted to the next step. A far more secure variation on the DES is called Triple DES (3DES).

2. Internal Data Encryption Algorithm (IDEA)
   - The IDEA originally created by noted European cryptologists Xuejia Lai and James L. Massey. Previously, it was known as Improved Proposed Encryption Standard (IPES). The IDEA also divides message into 64-bit blocks and uses a superior 128-bit key. The IDEA was mainly designed for software implementation that has speed faster than the DES with a few special optimizations. The IDEA divides a 64-bit plaintext block into four 16-bit sub-blocks. Each sub-block is subjected to eight computational rounds involving 52 sub-keys derived from the 128-bit key. The calculations in each are quite simple, limited to XOR operation, modular addition, and modular multiplication. Between rounds, the second and third sub-blocks swap positions. After the final round, the four sub-blocks are concatenated to produce a 64-bit block of ciphertext.
3. Ron's Code / Rivest's Code (RC2 and RC4)
   - Both RC2 and RC4 are proprietary block-ciphers and stream-ciphers created by a person named, Ron Rivest. Both algorithms support variable-length keys where longer keys increase the security of the ciphertext, and vice versa. The RC2 was designed mainly to replace the DES economically. In software, the RC2 is usually two or three times faster than the DES. The RC4 is designed to become faster than the DES in terms of the magnitude scale. The RC2 is found can operate in any of the four standard block encryption modes and can also undergo triple encryption similarly to the 3DES. The RC4, however, was apparently reverse-engineered in 1994 due to some uncertainties.

4. Diffie-Hellman
    - Whitfield Diffie and Martin Hellman created the Diffie-Hellman algorithm in 1976. The algorithm is a highly secure mechanism for symmetric key exchange. The Diffie-Hellman algorithm overcomes the key management problem where the sender and the receiver respectively must agree on a common key. In details, enabling both sides to independently derive a key without exchanging any secret information can resolve the problem.
5. Rivest Shamir Adleman (RSA)
    - The RSA algorithm was name after its three creators named Ron Rivest, Adi Shamir, and Leonard Adleman. The algorithm is actually the first public-key cryptosystem offering both encryption and digital signature. The foundation of the RSA security lies in the widely accepted, yet unproved, assumption that is virtually impossible to factor the product of two very large prime numbers (large means in the order of 100 or more digits). Public and private keys are huge numbers that mathematically related, so the RSA algorithm must generate them. The RSA encryption or decryption utilizes roughly 100 times more compute cycle than symmetric block algorithms like the DES. The RSA is actually not considered as a general-purpose cipher since it has worse performance in dedicated hardware implementations. Instead, the RSA is often used to complement secret-key cryptosystems especially when performing bulk encryption. For the creation of digital signatures, the RSA can provide some benefits through enlisting the help of a one-way hash function in making the (hash) value become encrypted in the sender's private key resulting in the "signature".

There are two popular encryption techniques applied in VPN, which are the secret (or private) key encryption and the public key encryption. Examples of these are DES for private key encryption and RSA for public key encryption (Scott 2000). Typically, the choice of encryption technology is not an issue. Most equipment vendors support major choices on the market, including RSA, DES and Triple-DES. Often, the area where a decision must be made is in the selection of key size.

Once encryption is introduced, VPN, like other networks that use encryption must have a mechanism for getting keys to users. The most common key management technologies are the Point-to-Point Protocol's (PPP) Encryption Control Protocol, Microsoft Point-to-Point Encryption (which includes key management), and the Internet Security Association Key Management Protocol/Internet Key Exchange or ISAKMP/IKE (Salamone 1998).

Technically speaking, the Internet Key Exchange (IKE) as described in RFC2409 is used by the IP Security (IPSec) to create shared security parameters and authenticated keys-security associations, between the IPSec cryptographic end points. Two IPSec peers use the IKE to establish a shared and authenticated key. The IKE operates as defined by the Internet Security Association and Key Management Protocol (ISAKMP) and implements parts of two key management protocols known as the OAKLEY and the SKEME. Therefore, the IKE is actually a hybrid protocol use to define the way of deriving authenticated keying material and negotiating shared security policy based on the following components:

1. ISAKMP: The communication language
2. OAKLEY: The modes of operation
3. SKEME: the share and re-keying techniques

On the other hand, the ISAKMP defines packet formats, the retransmission timer and the programming language. The IKE uses the ISAKMP language to express and execute the exchange sequence. A Domain of Interpretation (DOI) – RFC2407 is used to document how the IKE negotiates the IPSec security associations.

In addition, the IKE automates key exchange to deliver keys safely based on a Diffie-Hellman key exchange protocol. The Diffie-Hellman algorithm is a one-way function to securely exchange a shared secret over an untrusted communications channel. It is based on the exponentiation of prime numbers. A public value is exchanged and exponentiated again to create the secret value. It assumes that the identities of the two IPSec end points are known via passwords (pre-shared keys) or digital certificates. Once the end points are

authenticated, the IKE exchanges information to establish a shared key. The hosts share configuration information that specifies the encryption algorithm, authentication algorithm and security keys to use when establishing a security association.

Note that the IKE Security Associations (IKE SA), which certainly different from the IPSec security associations, define algorithms to encrypt the IKE traffic and define how to authenticate the IPSec end points. Under this method, the IKE uses the two phases of the ISAKMP. The first phase establishes the IKE security association and the second phase uses that security association to negotiate security associations for the IPSec.

Unlike the IPSec SA, the IKE SA is actually a bi-directional. The IKE is a request-response protocol where one party is the initiator and the other is a responder. Once the IKE SA is established it may be used to protect both inbound and outbound traffic. The IKE SA has various parameters that are negotiated between two IPSec end points. These parameters are referred to as the Protection Suites that include encryption algorithm, hash algorithm, authentication method, and the Diffie-Hellman group.

6.3 Authentications and Access Protocol

Authentication techniques are essential to VPN, as they ensure the communication parties that they are exchanging data with the correct user or host. In other words, authentication ensures that tunnels will only be established between verified tunnel partners (Ferrell).
For VPN that apply the IPSec standard, each packet that passes through an established tunnel will be authenticated. Under this method, each packet is authenticated using encrypted secrets to prevent session "spoofing", in which an authenticated session is taken over by an outside agency.

In contrast, packets will be authenticated per request in VPN with the Point-to-Point Protocol (PPTP) standard. Under this method, VPN authentication systems are based on a shared key system, such as the Challenge Handshake Authentication Protocol (CHAP) and the Password Authentication Protocol (PAP) routines.

Authentication can also be used to ensure the data integrity. The data itself can be sent through a hashing algorithm to derive a value that is included as a checksum on the message. Any deviation in the checksum sent from one peer to the next means the data was corrupted during transmission, or intercepted and modified along the way. (Scott 2000)

For VPN with the IPSec standard, authentication is done to protect the IP packet from being modified by perpetrators by applying the Authentication Header (AH) and the Encapsulation Security Protocol (ESP) to the IP packet. The AH and ESP are employed in conjunction with industry-standard hashing algorithms, such as Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) to ensure the data integrity of packets transmitted over a shared IP backbone [25]. Please refer to Chapter 6.4.1 for detail information regarding the application of the AH and ESP in the IP packet.

Many VPN vendors offer supporting to the PPP's PAP and CHAP, as well as Microsoft CHAP, which have been used in remote-access scenarios for years. What is emerging now is an increased need to connect outsiders. In many E-Commerce applications, for instance, there is a need to ensure that the person placing an order is authorized to do so and that the person is who say they are. For this level of authentication, digital certificates and Certificate Authorities (CAs) are increasingly become important.

Essentially, the CA is a trusted third party that confirms identity. CAs also holds digital certificates and public encryption keys (Salamone 1998). Note that the CA supports the following authentication standards [36]:

1. X.509v3 certificates
    - The certificates are used with the IKE protocol when authentication requires public keys. In this case, the IPSec-protected network will be allowed to scale by providing the equivalent of a digital ID card to each device. The certificates are obtained from a CA. X.509 that is a part of the X.500 standard.
2. Public-Key Cryptography Standard # 7 (PKCS # 7)
    - This standard developed by the RSA Data Security Inc., mainly used to encrypt and sign certificate enrollment messages.
3. Public-Key Cryptography Standard # 10 (PKCS # 10)

- This standard also developed by the RSA Data Security Inc., specifically used for certificate requests.

4. RSA Keys
   - RSA is actually the public key cryptographic system that comes in pairs: a public key and a private key.

It is important to identify the access privileges after identifying user identity. And that's precisely where authentication servers come into play. Many VPN solutions include their own authentication server known as the Access Control Server (ACS) built around Authentication, Authorization, and Accounting (AAA) capabilities. The AAA capabilities are essential in VPN since they provide the foundation to authenticate users, determine access levels, and archive all the necessary audit and accounting data. For a centralized AAA services, the ACS should support the Remote Access Dial-In User Service (RADIUS) and the Terminal Access Controller Access System Plus (TACAS+) user authentication protocols.

6.4 Encapsulation and Tunneling Protocols

There are currently some tunneling protocols that are used in the majority of VPN solutions, which are the IP Security (IPSec), Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Forwarding (L2F), and Generic Routing Encapsulation (GRE) [25].

Fundamentally, VPN works at Layer-2 and 3 of the OSI model. The PPTP, L2F and L2TP encapsulate PPP into an IP packet for transmission across the Internet between a remote-access server or remote-access client and the terminating gateway on a remote network. Since the IPSec with the 3DES service only handles IP, it is worthless to use the service in the networks that run the IPX or other non-IP protocols. An alternative-transport protocol, such as GRE or one of the Layer-2 protocols (such as L2F, L2TP or PPTP) needs to be applied here.

The most important consideration for remote users is to determine whether non-IP protocols are required or not. Multiprotocol routing from the desktop is handled through

the Layer-2 protocols, and an interoperable multiprotocol VPN support is available with PPTP, L2F and L2TP. The IPSec has been known can provide a very secure VPN across the public IP network. However, it is found that the IPSec services are limited to the IP network only and typically will not cover the NAT (Network Address Translation) or proxy firewalls.

Rule of thumb, the IPSec can be used directly in the IP network with the TCP/IP standard. Other protocols by contrast, such as the L2F, the L2TP, the PPTP, and the IPSec with the GRE are more suitable to be applied for the non-IP network. In this case, the L2F and the L2TP do not provide native support for encryption. However, both PPTP and IPSec protocols offer data encryption with radically different implementations.

6.4.1 Internet Protocol Security (IPSec) protocol

IPSec is a framework of open standards for ensuring secure private communications over IP networks. Based on standards developed by the Internet Engineering Task Force (IETF), IPSec ensures confidentiality, integrity, and authenticity of data communications across a public IP network. IPSec provides a necessary component of a standards-based, flexible solution for deploying a network-wide security policy [16]. Generally, IPSec provides the capability to secure communications across a LAN, across private and public WAN, and across the Internet. Examples of its use include (Stallings 2000):

1. Secure branch office connectivity over the Internet: A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.
2. Secure remote access over the Internet: An end user whose system is equipped with IP security protocols can make a local call to an ISP and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.

3. Establishment of extranet and intranet connectivity with partners: IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

4. Enhancement of electronic commerce security: Most efforts to date to secure electronic commerce on the Internet have relied upon securing Web traffic with Secure Socket Layer (SSL) since that is commonly found in Web browsers and is easy to set up and run. There are new proposals that may utilize IPSec for electronic commerce.

Figure 6.9 shows a typical scenario of IPSec usage. In Figure 6.9, the user workstation can establish an IPSec tunnel with the network devices to protect all the subsequent sessions and accesses performed by users. This is because IPSec protocols can operate in networking devices, such as a router or firewall that connects each network. After this tunnel is established, the workstation can have many different sessions with the devices behind these IPSec gateways. The packets going across the Internet will be protected by IPSec but will be delivered onto each LAN as a normal IP packet.

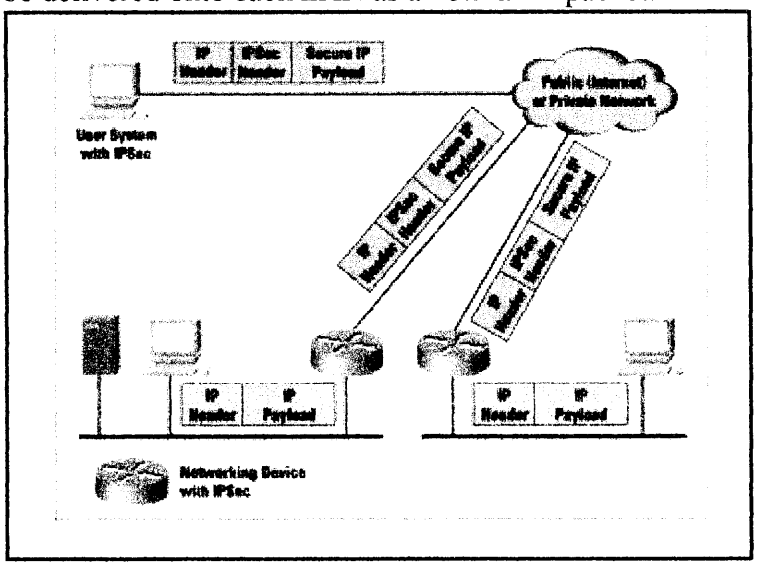


Figure 6.9: An IPSec Scenario

IPSec provides data privacy through IP network-layer encryption and tunneling services. The IPSec standard defines several new packet formats: Authentication Header (AH) and Encapsulating Security Protocol (ESP). Let reviews in details regarding AH first.

The AH provides support for data integrity and authentication of IP packets (Stallings 2000). The data integrity feature ensures that undetected modification to the content of a packet in transit is not possible. In this case, the data integrity feature ensures that undetected modification to the content of a packet in transit is not possible. Besides, it also prevents the address spoofing attacks observed in today's Internet and guards against the replay attack (Stallings 2000). Figure 6.10 shows the IPSec AH.

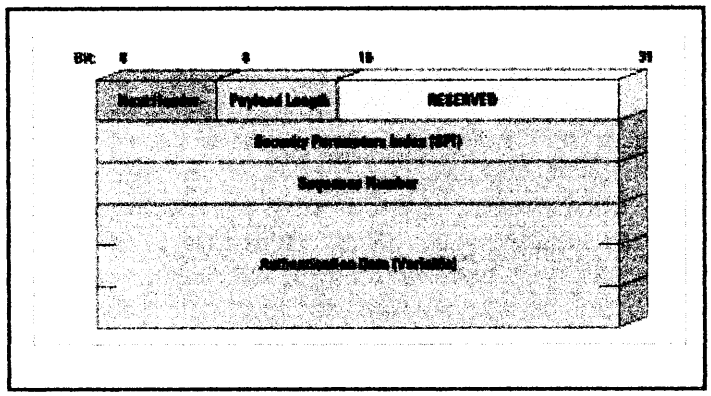


Figure 6.10: An IPSec AH

Based on Figure 6.10, the authentication header consists of following several fields with specific functions relatively:

1. *Next Header* (8 bits): This field identifies the type of header immediately following this header.
2. *Payload Length* (8 bits): This field gives the length of the authentication header in 32-bit words, minus 2. For example, the default length of the authentication data field is 96 bits, or three 32-bit words. With a three-word fixed header, there are a total of six words in the header, and the Payload Length field has a value of 4.
3. *Reserved* (16 bits): This field is reserved for future use.
4. *Security Parameters Index* (32 bits): This field identifies a security association.

5. *Sequence Number* (32 bits): This field contains a monotonically increasing counter value.

6. *Authentication Data* (variable): This variable-length field (must be an integral number of 32-bit words) contains the Integrity Check Value (ICV), or Message Authentication Code (MAC), for this packet.

The Encapsulating Security Protocol (ESP) payload actually provides confidentiality service, including confidentiality of message contents and limited traffic flow confidentiality. As an optional feature, ESP can also provide the same authentication services as AH (Stallings 2000). Figure 6.11 shows the ESP format for IPSec packet.

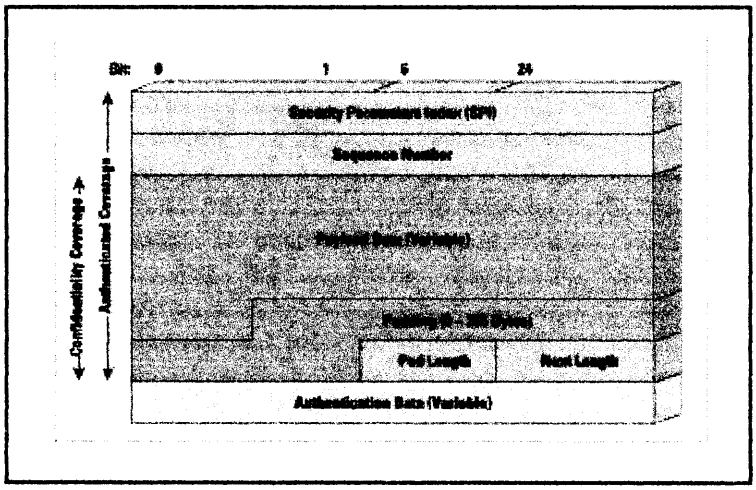


Figure 6.11: An IPSec ESP Format

Figure 6.11 shows the format of an ESP packet. It contains the following fields with specific functions relatively:

1. *Security Parameters Index* (32bits): Identifies a security association

2. *Sequence Number* (32 bits): A monotonically increasing counter value.

3. *Payload Data* (variable): A transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
4. *Padding* (0–255 bytes): Extra bytes that may be required if the encryption algorithm requires the plaintext to be a multiple of some number of octets
5. *Pad Length* (8 bits): Indicates the number of pad bytes immediately preceding this field
6. *Next Header* (8 bits): Identifies the type of data contained in the payload data field by identifying the first header in that payload (for example, an extension header in IPv6, or an upper-layer protocol such as TCP)
7. *Authentication Data* (variable): A variable-length field (must be an integral number of 32-bit words) that contains the integrity check value computed over the ESP packet minus the Authentication Data field

Note that, both AH and ESP support two modes of use that are Transport mode and Tunnel mode. In details, the transport mode is used primarily for upper-layer protocols and for end-to-end communications between two hosts. On the other hand, the tunnel mode is used primarily to encapsulate an entire IP packet within an IP packet to ensure that no part of the original packet is changed as it is moved through a network. Besides, the tunnel mode is also useful in a configuration that includes a firewall or other sort of security gateway (Stallings 2000). Figure 6.12 shows two ways in which the IPSec ESP service can be used where in the lower part tunnel mode operation is used to set up a VPN.

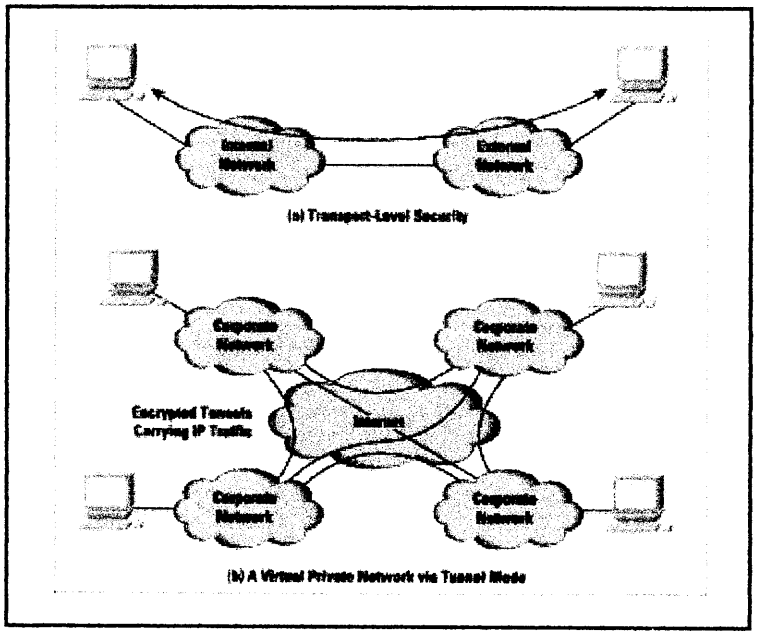


Figure 6.12: Transport Mode vs. Tunnel Mode Encryption

The IPSec parameters between two devices are negotiated with the IKE, formerly known as ISAKMP/Oakley. The IKE can also use digital certificates to authenticate users and devices via a Certificate Authority (CA). Using a CA simplifies the creation of large-scale IPSec VPN. Without digital certificate supports, IPSec solutions must rely on pre-shared keys, which will not scale to accommodate large service provider networks and to the Internet. IPSec provides a necessary component of a standards-based, flexible solution for deploying a network-wide security policy [19].

IPSec provides an excellent remote-user as well as site-to-site solution. Remote user can use an IPSec client on their PC, either alone or in combination with L2TP, to connect

back to the enterprise network. Further more, GRE tunneling combined with IPSec encryption provide multi-protocol support and route resiliency for site-to-site VPN deployments [19].

To sum up, IPSec technologies combine several different security technologies into a complete system to provide confidentiality, integrity and authenticity. In details, IPSec applies:

1. Diffie-Hellman, a public-key method for key exchange between peers on a public network. This feature is used within IKE to establish ephemeral session keys.
2. Public key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties and avoid man-in-the-middle attacks.
3. Bulk encryption algorithms, such as DES and 3DES used to encrypt packet data.
4. Keyed Hash Message Authentication Code (HMAC) combined with traditional Message Digest 5 (MD5) or Secure Hash Algorithms (SHA) used to authenticate packet data.
5. Digital certificates signed by a Certificate Authority (CA) to act as digital ID cards.

6.4.2 Point-to-Point Tunneling Protocol (PPTP)

PPTP is actually a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across TCP/IP-based data networks [37]. As a matter of fact, the PPTP services support on-demand, multiprotocol, virtual private networking over the Internet.

The networking technology of PPTP is an extension of the remote access Point-to-Point Protocol (PPP) defined in the document by the IETF referred to as RFC 1171 [37]. Under this extension, PPTP encapsulates PPP packets into IP datagrams for transmission over the Internet or other public TCP/IP-based networks as well in private LAN-to-LAN networking.

The PPTP protocol is included with the Windows NT Server V4.0 O/S and Windows NT Workstation V4.0 O/S. Thus, computers running these operating systems can use the PPTP protocol to securely connect to a VPN as a remote access client by using the Internet. In other words, PPTP enables on-demand VPN over the Internet and also connects computers to a LAN to create VPN across the LAN. An important feature in the use of PPTP in supporting VPN is it eliminates the need for expensive, leased line or private enterprise-dedicated communication servers because PPTP can be utilized over Public-Switched Telephone Network (PSTN) lines [37].

Generally, there are three computers involved in every PPTP deployment over VPN, which are a PPTP client, a Network Access Server (NAS), and a PPTP server. Both the PPTP client and the PPTP server use tunneling to securely route packets to a computer on VPN by using routers those only know the address of the VPN intermediary server. On the other hand, the NAS uses the TCP/IP protocol for all traffic transmitted to the Internet sent from the PPTP client to the PPTP server and vice versa. Note that also, PPTP encapsulates the encrypted and PPP packets into IP datagrams for a secure transmission over the Internet.

Actually, the PPTP architectures are closely related to the processes involved in creating a secure communication. In this case, the secure communication created using the PPTP protocol typically involves three processes. Each process requires successful completion of the previous process. The processes are [37]:

1. PPP connection and communication
    - A PPTP client uses PPP to connect to an ISP through standard telephone line or ISDN line. This connection applies the PPP protocol to establish the connection and to encrypt data packets. By definition, PPP protocol is a remote access protocol used by PPTP to send multiprotocol data across TCP/IP-based networks. PPP encapsulates IP, IPX, and NetBEUI packets between PPP frames and sends the encapsulated packets by creating a point-to-point link between the sender and the receiver nodes. Most PPTP sessions are actually started by a client dialing up an ISP NAS.

2. PPTP control connection
    - The PPTP protocol creates a control connection from the PPTP client to a PPTP server on the Internet. This connection uses TCP to establish the connection and is called a PPTP "tunnel". In this process, the PPTP protocol specifies a series of control messages between the PPTP-enabled client and the PPTP server. The control messages establish, maintain, and end the PPTP tunnel.
3. PPTP data tunneling
    - Finally, the PPTP protocol establishes IP datagrams containing encrypted PPP packets that are created by Remote Access Server (RAS) and are sent via the PPTP tunnel to the PPTP server. The IP datagrams are established using a modified version of the Internet Generic Routing Encapsulation (GRE) protocol. In this case, the GRE header is used to encapsulate the PPP packet within the IP datagram. The PPTP server disassembles the IP datagrams, decrypts the PPP packets and then routes the decrypted packets to the VPN.

In general, PPTP extends the strict authentication and encryption security available to computers running RAS on the Internet. There are four aspects need to emphasized in understanding PPTP security [37]:

1. Authentication and access control
    - Authentication of remote PPTP clients is done by deploying the same PPP authentication methods used for any RAS client dialing directly to a RAS server. In this case, the RAS used supports the Challenge Handshake Authentication Protocol (CHAP) and the Password Authentication Protocol (PAP) schemes. After authentication, proper permissions are required in order to control users who are accessing the network resources.
2. Data encryption
    - For data encryption, PPTP uses the RAS "shared-secret" encryption process since both ends of the connection share the encryption key. Under the implementation of RAS, the shared-secret is the user password. PPTP uses the PPP encryption and PPP compression schemes. Under this method, PPP negotiates encryption by using the Compression Control Protocol (CCP). The user name and password of

the PPTP client is actually available to the PPTP server and supplied by the PPTP client. An encryption key is derived from the hashed password stored on both the client and server. The RSA RC4 standard is primarily applied to create this 40-bit session key based on the client password. This key then is used to encrypt all data contained in PPP packets that are passed over the Internet, keeping the remote connection private and secure. In this process, all the PPP packets containing a block of encrypted data is then encapsulated into the larger IP datagrams before being routed so that the data would be indecipherable especially for hackers.

3. PPTP packet filtering
   - Enabling PPTP filtering on the PPTP server can enhance network security from malicious activity. As PPTP is enabled, the PPTP server on VPN accepts and routes only PPTP packets from authenticated users. This prevents all other packets from entering the PPTP server and VPN. PPTP filtering is activated on the PPTP server using the protocols tabs in the Network Option of Control Panel.
4. Using 3rd party firewalls
   - PPTP can be used with most firewalls and routers by enabling traffic destined for port 1723 (as assigned by the Internet Assigned Numbers Authority [IANA]) to be routed through the firewall or router. An organization can deploy a PPTP server running Windows NT Server V4.0 behind its firewall. The PPTP server accepts PPTP packets passed to the private network from the firewall and extracts the PPP packet from the IP datagrams, then decrypts and forwards the packet.

6.4.3 Layer-2 Tunneling Protocol (L2TP)

L2TP came out of a mix of the PPTP world and a tunneling protocol known as Layer-2 Forwarding (L2F) developed by the Cisco Systems Inc. The combination is frequently used in node-to-node applications (Salamone 1998). Let reviews briefly L2TP in terms of its general overview, typical topology, protocol used and security features.

In general, L2TP extends the Point-to-Point Protocol (PPP) model by allowing the Layer-2 (L2) and PPP endpoints to reside on different devices interconnected by a packet switched network. With L2TP, a user has an L2 connection to an access concentrator. The concentrator then tunnels individual PPP frames to the Network Access Server

(NAS). This allows the actual processing of PPP packets to be divorced from the termination of the L2 circuit. One obvious benefit of such a separation is that instead of requiring the L2 connection terminate at the NAS (which may require a long-distance toll charge), the connection may terminate at a (local) circuit concentrator, which then extends the logical PPP session over the Internet. Figure 6.13 depicts a typical L2TP scenario.

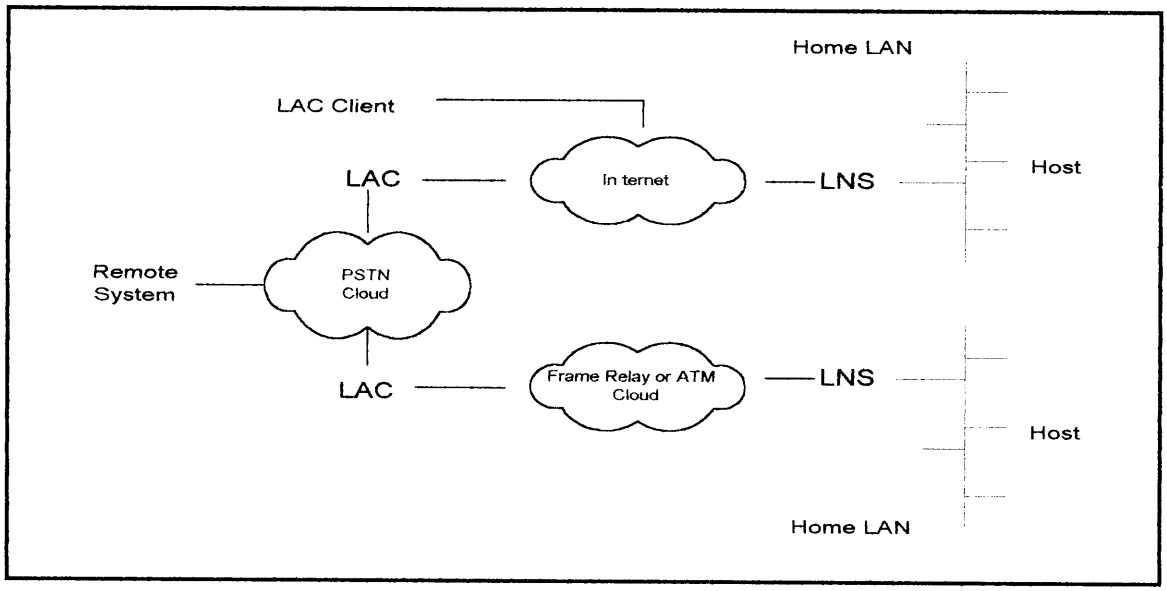


Figure 6.13: Typical L2TP Network Topology

Based on Figure 6.13, the main goal is to tunnel PPP frames between the Remote System or L2TP Access Concentrator (LAC) Client and a L2TP Network Server (LNS) located at a Home LAN. The Remote System initiates a PPP connection across the PSTN Cloud to an LAC. The LAC then tunnels the PPP connection across the Internet to LNS whereby access to a Home LAN is obtained. The Remote System is provided addresses from the HOME LAN via PPP NCP negotiation. The Home LAN's Management Domain may provide Authentication, Authorization and Accounting (AAA) capabilities as if the user were connected to a Network Access Server (NAS) directly.

On the other hand, a LAC Client (a host that runs L2TP natively) may also participate in tunneling to the Home LAN without use of a separate LAC. In this case, the host containing the LAC Client software already has a connection to the public Internet. A

"virtual" PPP connection is then created and the local L2TP LAC Client software creates a tunnel to the LNS. As in the above case, the Home LAN's Management Domain will provide addressing and AAA capabilities.

L2TP utilizes two types of messages that are control messages and data messages. Control messages are used in the establishment, maintenance and clearing of tunnels and calls whereas data messages are used to encapsulate PPP frames being carried over the tunnel. Control messages utilize a reliable Control Channel within L2TP to guarantee delivery. Data messages are not retransmitted when packet loss occurs.

Figure 6.14 shows the L2TP structure that depicts the relationship of PPP frames and Control Messages over the L2TP Control and Data Channels. PPP Frames are passed over an unreliable Data Channel encapsulated first by an L2TP header and then a Packet Transport such as UDP, Frame Relay, and ATM. Control messages are sent over a reliable L2TP Control Channel, which transmits packets in-band over the same Packet Transport.

Sequence numbers are required to be present in all control messages and are used to provide reliable delivery on the Control Channel. Data Messages may use sequence numbers to reorder packets and detect lost packets. All values are placed into their respective fields and sent in network order (high order octets first).

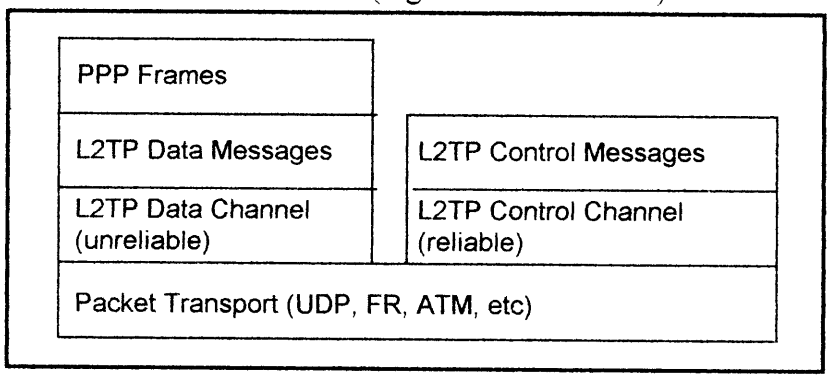


Figure 6.14: L2TP Structure

The necessary setup for tunneling a PPP session with L2TP consists of two steps that are establishing the Control Connection for a Tunnel, and establishing a Session as triggered by an incoming or outgoing call request. The Tunnel and corresponding Control Connection established before an incoming or outgoing call is initiated. An L2TP Session established before L2TP can begin to tunnel PPP frames. Multiple Sessions may exist across a single Tunnel and multiple Tunnels may exist between the same LAC and LNS. Figure 6.15 shows the L2TP operation in setting up for tunneling.

Once tunnel establishment is complete, PPP frames from the remote system are received at the LAC, stripped of CRC, link framing, and transparency bytes, encapsulated in L2TP, and forwarded over the appropriate tunnel. The LNS receives the L2TP packet, and processes the encapsulated PPP frame as if it were received on a local PPP interface.

The sender of a message associated with a particular session and tunnel places the Session ID and Tunnel ID (specified by its peer) in the Session ID and Tunnel ID header for all outgoing messages. In this manner, PPP frames are multiplexed and demultiplexed over a single tunnel between a given LNS-LAC pair. Multiple tunnels may exist between a given LNS-LAC pair, and multiple sessions may exist within a tunnel.

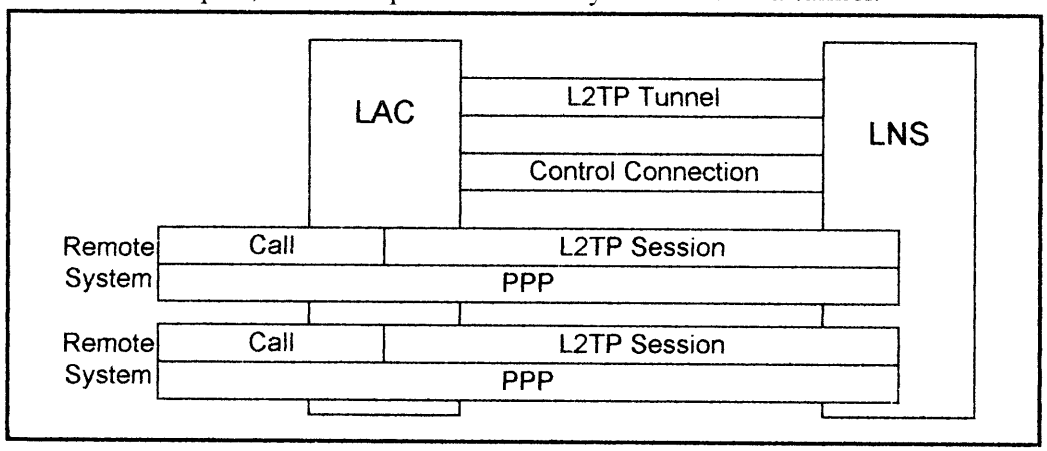


Figure 6.15: Tunneling PPP during the L2TP Session

L2TP offers and delivers a full range of security control and policy management features, including tunnel endpoint security, packet level security, end-to-end security, L2TP and IPSec transport security, and proxy PPP authentication security. Business customers have ultimate control over permitting and denying users, services, or application. Data security

is not compromised when using L2TP to enable user-based VPN services. L2TP supports authentication and authorization features, providing interoperability with TACACS+ and RADIUS servers. It also supports IPSec using DES or 3DES [19].

6.4.4 Layer-2 Forwarding (L2F) Protocol

In general, remote access VPN uses L2F tunnels to tunnel the link layer of high-level protocols (for example, PPP frames or asynchronous High-Level Data Link Control). By using such tunnels, it is possible to detach the location of the ISP's NAS from the location of the enterprise customer's home gateway, where the dial-up protocol connection terminates and access to the enterprise customer's network is provided [21].

In this process, ISPs configure their NASs to receive calls from users and forward the calls to the enterprise customer's home gateway. The ISP only maintains information about the home gateway---the tunnel endpoint. The enterprise customer maintains the home gateway users' IP addresses, routing, and other user database functions. Administration between the ISP and home gateway is reduced to IP connectivity. There will be discussions regarding L2F typical topology and protocol operations including its negotiation sequence and authentication process.

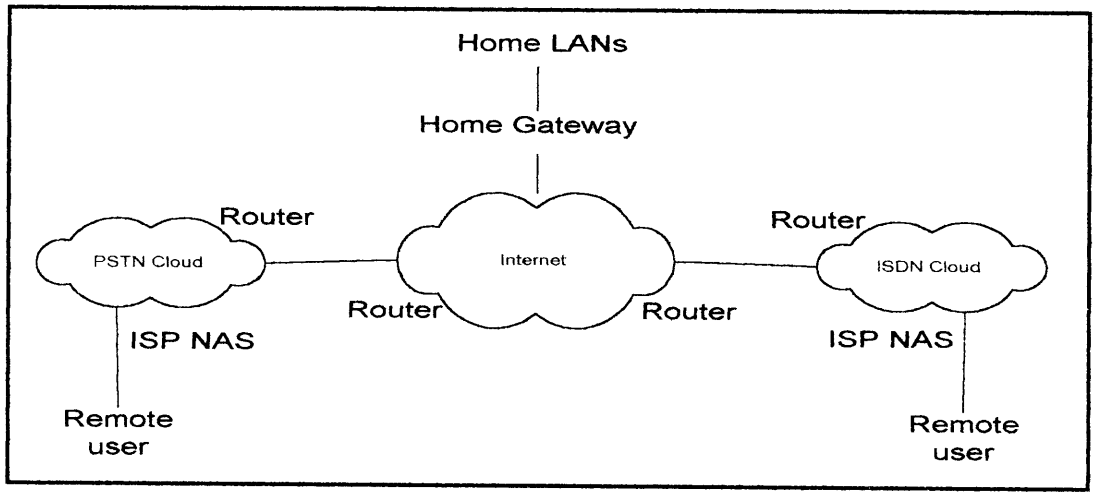


Figure 6.16: Generic Internet with the PSTN and ISDN Accesses

Figure 6.16 shows the typical L2F topology where the PPP link running between a client (the user's hardware and software) and the home gateway. The ISP NAS (with the PSTN

and ISDN accesses) and home gateway establish an L2F tunnel. The ISP NAS then uses the L2F tunnel to forward the PPP link to the home gateway. The access VPN then extends from the client to the home gateway. The L2F tunnel creates a virtual point-to-point connection between the client and the home gateway. Access VPNs connect a variety of users: from a single, mobile employee to an entire branch office. Figure 6.17 illustrates the following methods of logging on to access VPNs [21].

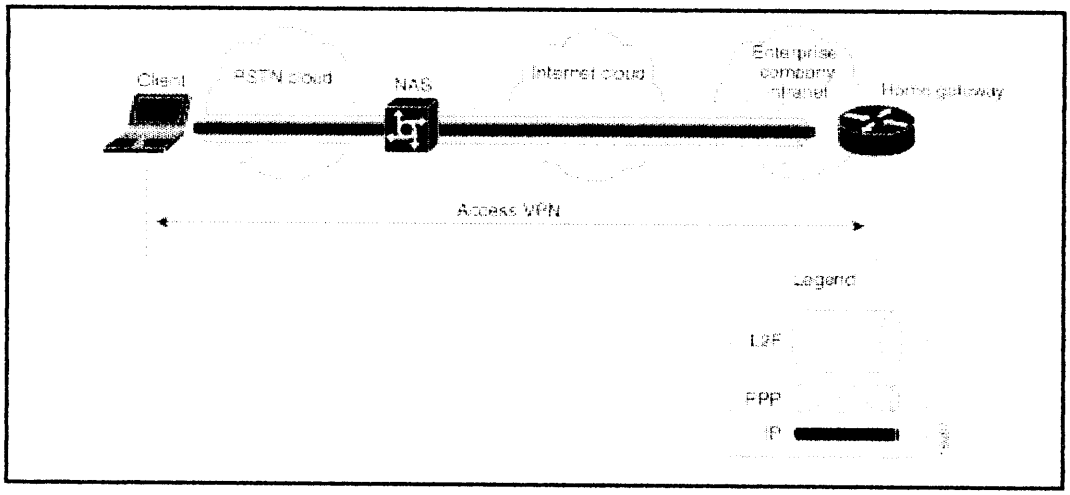


Figure 6.17: Logging on to Access VPNs

When a user wants to connect to the enterprise customer's home gateway, firstly he or she must establish a PPP connection to the ISP's NAS. The NAS then establishes an L2F tunnel with the home gateway. Finally, the home gateway authenticates the client's username and password, and establishes the PPP connection with the client. Figure 6.18 describes the sequence of protocol negotiation events between the ISP's NAS and the enterprise customer's home gateway.

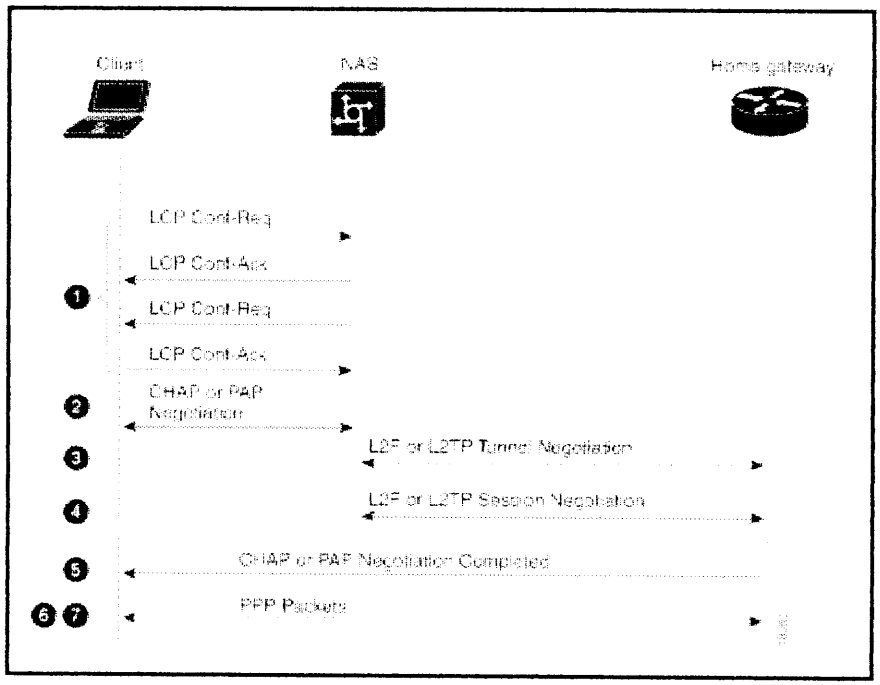


Figure 6.18: Protocol Negotiation Events between Access VPN Devices

When the NAS receives a call from a client that instructs it to create an L2F tunnel with the home gateway, it first sends a challenge to the home gateway. The home gateway then sends a combined challenge and response to the NAS. Finally, the NAS responds to the home gateway's challenge, and the two devices open the L2F tunnel.

Before the NAS and home gateway can authenticate the tunnel, they must have a common "tunnel secret." A tunnel secret is a pair of usernames with the same password that is configured on both the NAS and the home gateway. By combining the tunnel secret with random value algorithms, which are used to encrypt to the tunnel secret, the NAS and home gateway authenticate each other and establish the L2F tunnel. Figure 6.19 describes the tunnel authentication process.

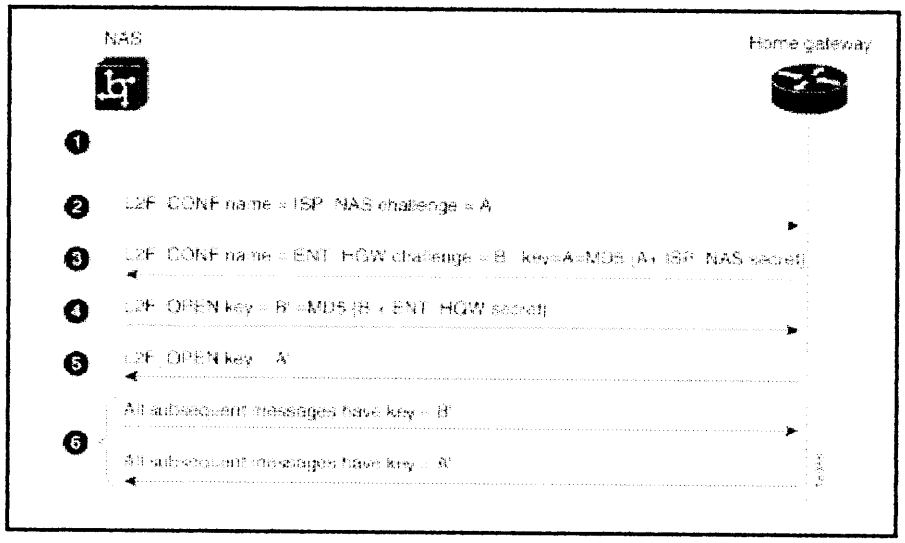


Figure 6.19: L2F Tunnel Authentication Process

The client, NAS, and home gateway use three-way Challenge/Response Authentication Protocol (CHAP) authentication to authenticate the client's username and password when establishing the access VPNs. CHAP is a platform in which the password is sent as a 64-bit signature instead of as plain text. This enables the secure exchange of the user's password between the user's client and the home gateway.

Three processes are involved in this case. Firstly, the NAS challenges the client. Secondly, the client responds. Thirdly, the NAS then forwards this CHAP information to the home gateway, which authenticates the client and sends a third CHAP message (either a success or failure message) to the client. Figure 6.20 describes the three-way CHAP authentication process.

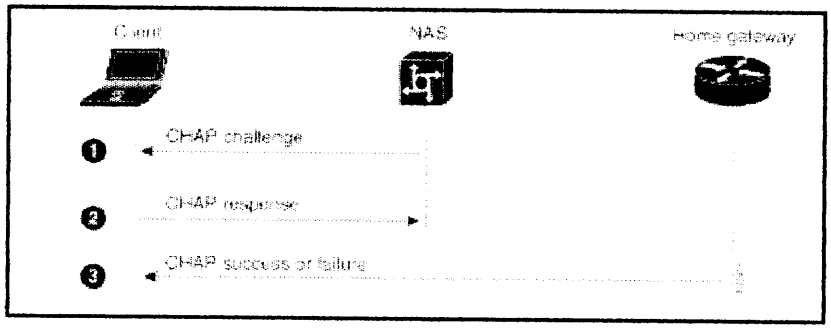


Figure 6.20: Three-Way CHAP Authentication Process

Once the home gateway authenticates the client, the access VPN is established. The L2F tunnel creates a virtual point-to-point connection between the client and the home gateway. The NAS acts as a transparent packet forwarder. When subsequent clients dial in to the NAS to be forwarded to the home gateway, the NAS and home gateway do not need to repeat the L2F session negotiation because the L2F tunnel is already open [21].

6.4.5 Generic Routing Encapsulation (GRE) Protocol

GRE is a standard solution based on RFC 1702 that allows any protocol to be tunneled in an IP packet [22]. In this case, GRE can assist ISPs who want to offer managed IP VPN services across an established IP network.

GRE enables a virtual point-to-point, whereas IPSec supports only IP protocols. IP packets are placed inside a GRE header and encapsulated in an IP datagram. Besides, when configure on the router, the GRE tunnel appears as a point-to-point connection, so this VPN topology uses a point-to-point overlay mesh [19]. In this process also, Type of Service (ToS) bits are copied to the tunnel header as the router encapsulates the IP datagram using GRE. ToS is actually important since it allows routers between GRE-based tunnel end points to adhere to precedence bits thereby improving the routing of premium service packets. A VPN player, Cisco Systems Inc. offers Quality of Service (QoS) technologies, such as Policy Routing, Weighted Fair Queuing (WFQ) and Weighted Random Early Detection (WRED) that can operate on intermediate routers between GRE tunnel endpoints. Refer to Chapter 9 for details on QoS for VPN tunnel exclusively. Figure 6.21 shows the basic configuration of GRE tunnel for the Enterprise VPN (E-VPN) application.

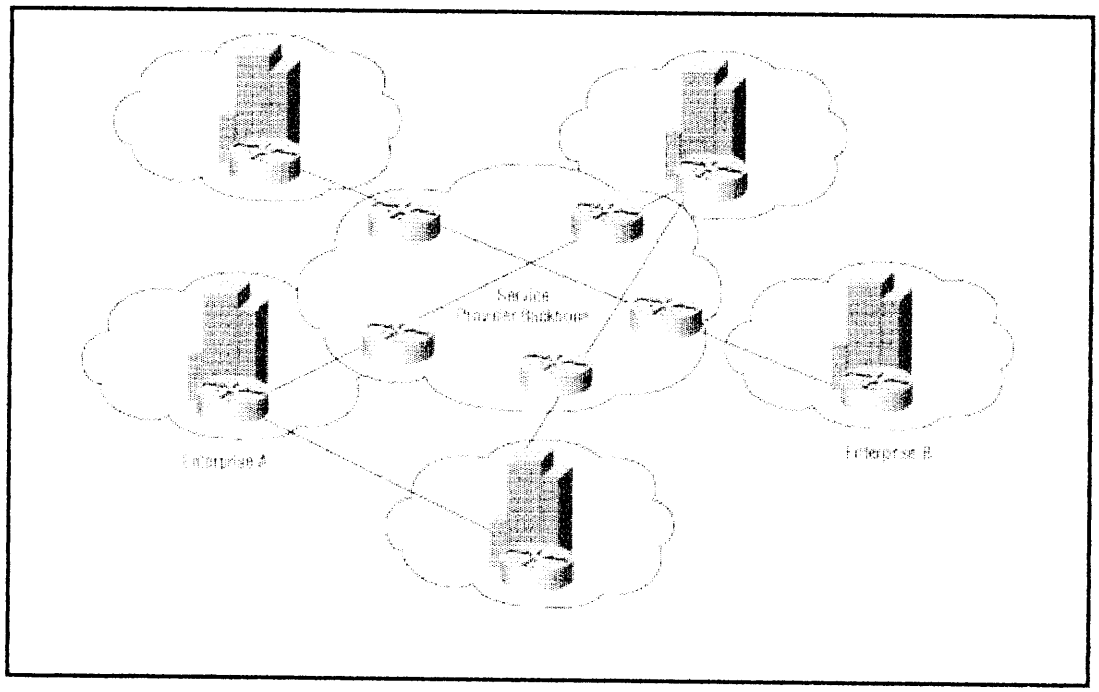


Figure 6.21: GRE Tunnel Architecture for E-VPN

CHAPTER 7

A REFERENCE OF FRAMEWORK DESIGN FOR VPN

7.1 Design Methodology

A general framework based on scenario encompasses the most common environment that implements the complete solution of VPN. The guidelines used in this project are enlisted below:

1. Define the Scope of the Scenario
2. First phase: Build the Conceptual Design
   - To build the conceptual representation of the network design, which includes identification of important entities using the VPN and the virtual links between them is called as the Global Conceptual Model. The global conceptual view is decomposed into more manageable tasks, by examining requirements of each link between two entities, which is called as the Local Conceptual Model. The local conceptual model serves as input for logical design consideration but it is independent of any implementation details such as specific functions or protocols used.
3. Second phase: Build the Logical Design
   - The logical design is used to translate the local conceptual representation to the local logical structure of the network design. This includes specifying required functions in relation to protocols that are used in appropriate location for each decomposed model. After considering each situation for the decomposed-local logical model and review on each link, group duplicate functions together in a relation to a local point to avoid unnecessary duplication of functions. The local logical models are merged back into global logical model to eliminate or at least minimize redundancy of the functions in use. The logical design is a source of information for the physical design phase but independent of hardware, software consideration.
4. Third phase: Build the Physical Design
   - To decide how the logical structure is to be physically implemented on the target network design architecture, which includes detail implementations in terms of allocation of functional components such as software, hardware platform or

integrated solution use in each location. This allows the designer to make decisions on how the network is to be built successfully. Therefore, physical design is tailored to a specific VPN system.

7.2 Scenario Scope

A general environment for complete VPN solution will allow office worldwide to access network resources, mobile workers to link up to corporate intranets, customers to place orders and suppliers to check inventory levels, all in a highly secure and cost-effective manner [24]. By considering the comprehensive solution for present expansion and future growth, the scope covers the integration of the following design [24]: Remote Access VPN between a corporate network and remote or mobile employees.

1. Intranet VPN between internal corporate departments and branch offices
2. Extranet VPN between a corporation and its strategic partners, customers, and suppliers.

7.3 Conceptual Design

7.3.1 Global Conceptual Design

The global conceptual design is primarily used for a complete VPN implementation for intranet, extranet and remote access application (refer to Figure 4.4).

7.3.2 Local Conceptual Design

The global conceptual design can be decomposed into the local conceptual design. In this case, a complete implementation of VPN is decomposed into the remote access VPN (refer to Figure 4.2), the intranet VPN (refer to Figure 4.3), and the extranet VPN (refer to Figure 4.1).

7.4 Logical Design

7.4.1 Local Logical Remote Access VPN Design

It is suitable to use the Corporate-to-the Internet and the DMZ VPN configurations for remote access VPN. The DMZ configuration is neglected in the discussion to reduce the complexity of the VPN configuration and the Internet user access. However, take note that the DMZ zone can be added easily at anytime to the existing VPN configuration.

When implementing a remote access VPN architecture, it is important to consider where to initiate tunneling and encryption, either on the dial-up client PC or on the Network Access Server (NAS).

In the client-initiated model, the encrypted tunnel is established at the client node using the IPSec, L2TP, or PPTP protocols. Thereby making the ISP network solely a mean of transport to the corporate network. An advantage of the client-initiated model is VPN intelligence resides in the Customer Premise Equipment (CPE), enabling VPN functionality to be delivered over the Internet. Besides, clients can make the installment and maintenance of the tunneling/encryption software without restraint.

In the NAS-initiated scenario, the user does not need VPN client software. A remote user dials into a POP using a Point-to-Point Protocol/Serial Line Internet Protocol (PPP/SLIP) connection. The service provider then will authenticate the user. Since the VPN intelligence resides in the service provider's network, there is no end-user client software for the corporation to maintain, thus eliminating client management issues associated with remote access. Note that security/management trade-offs must be balanced in remote access VPN as shown in Figure 7.1 [25].

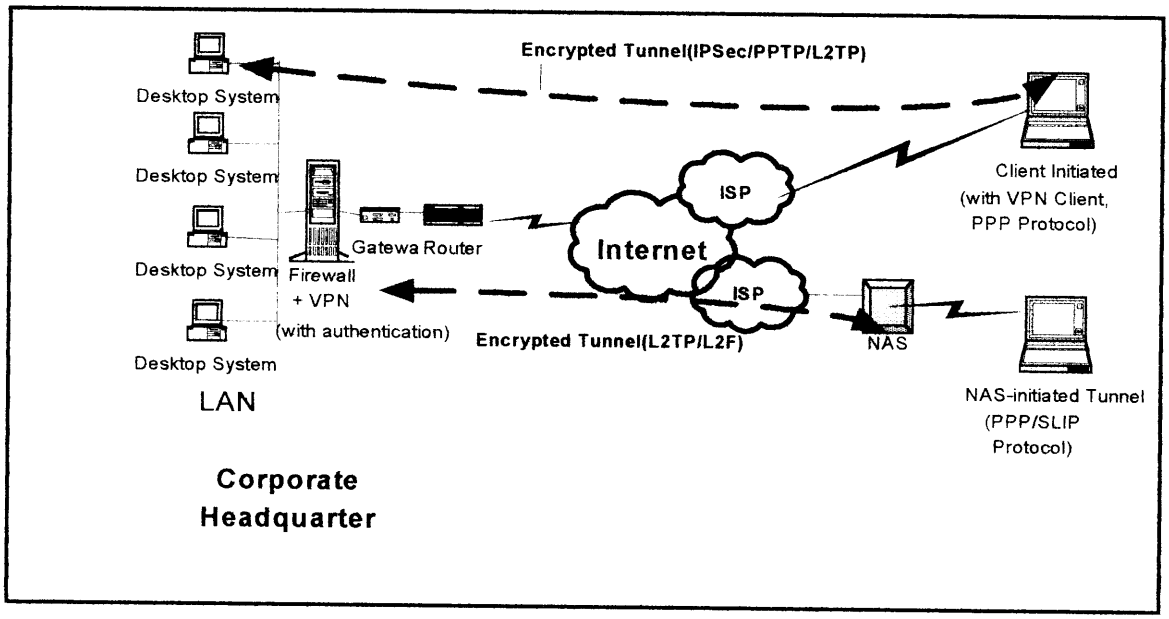


Figure 7.1: Local Logical Remote Access VPN Design

7.4.2 Local Logical Intranet and Local Logical Extranet VPN Design

In Intranet VPNs that facilitate secure communications between a company's internal departments and its branch offices (see Figure 4.3), the primary technology requirements are strong data encryption to protect sensitive information. Intranet VPNs are build on an IP WAN infrastructure utilize IPSec or GRE to create secure tunnels. See Figure 7.2. [25].

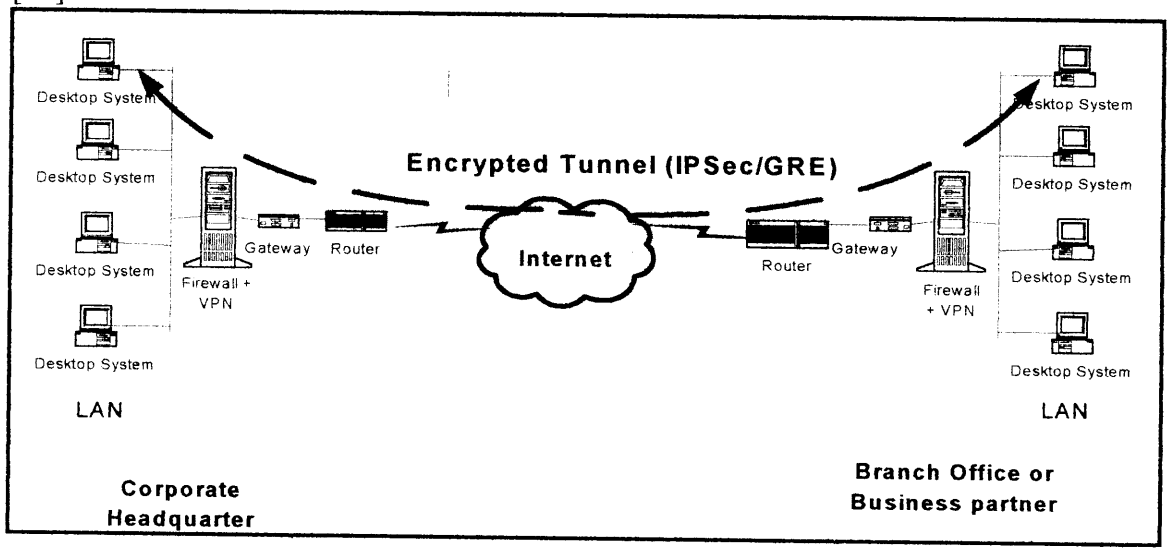


Figure 7.2: Local Logical Intranet and Local Logical Extranet VPN Design

Extranet VPNs between a company and its strategic partners, customers and suppliers (see Figure 4.1) require an open, standards-based solution to ensure interoperability with the various solutions that the business partners might implement. The accepted standard for Internet-based VPNs is the Internet Protocol Security (IPSec) standard. It is vital to eliminate bottlenecks at network access points and guarantee swift delivery of and rapid response times for critical data [24].

Intranet and Extranet VPNs can be provisioned using IP tunnels based on IPSec for data confidentiality and integrity. Alternatively, the GRE protocol can be used to provide privacy through data separation. GRE can also be combined with IPsec to offer multi-protocol and routing update support in an IP environment. GRE is useful for tunneling both IP and non-IP protocols, whereas IPsec supports only IP protocols [19].

7.4.3 Global Logical Design

Figure 7.3 shows the overall global logical design.

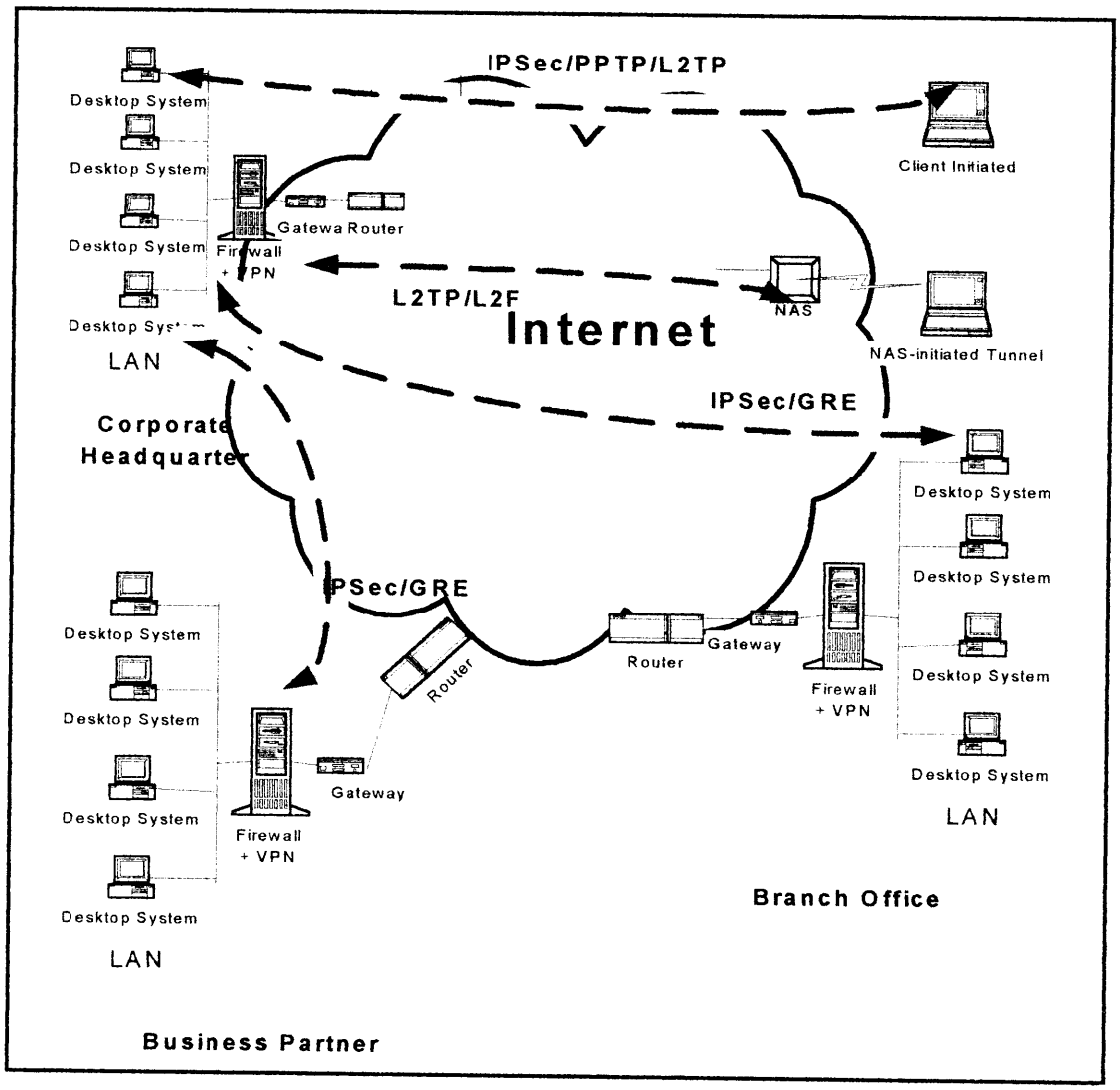


Figure 7.3: Global Logical Design

7.5 Physical Design

Note that, this is not a real physical design as it only provides a reference framework to understand which solution is suit to deploy the VPN solutions. VPN allow users to create a secure, private network over a public network such as the Internet. This is done through encryption, authentication, packet tunneling, and firewalls. They can be created using software, hardware, or a combination of the two that creates a secure link between peers over a public network. The most important concepts are firewalls, authentication, encryption, encapsulation and tunneling (Scott 2000).

VPN solutions come in many types. The best one for you will depend on your application, your budget, and your technical expertise.

7.5.1 Software-Based VPN

There are many ways to deploy virtual private networks. Here we focus on the distinct approaches that use existing networking equipment that are routers, servers and firewalls. Although these devices are radically different, they also have many similarities when deploying VPN. In fact, they share several common benefits such as requiring only a software installation to get started. At the same time, these 3 approaches to VPN also share some comparable concerns when it comes to performance.

The next parts will be discussions on 2 other approaches that are using a dedicated VPN device and turning to an ISP to implement the VPN service. The choice of approach is often based on a company's networking philosophy. Some company networks are router-centric, which means the router is the selected device that an IT manager decides to add for VPN services. Other company networks are LAN-centric, where servers are the primary elements that an IT manager focuses on. For other companies firewall is viewed as the heart of VPN, thus leading to the selection of a firewall-based VPN approach.

First, let review briefly on router-based VPN. Most router vendors have added VPN services to their products. Using VPN-enabled routers, IT managers can send traffic between branch offices over the Internet or an ISP network.

The router-based approach can give several advantages to user. First, adding VPN services to a router are usually made through upgrading the software only. Latest models of routers often come with the VPN services built in the unit software set or even in the router's operating system. Typically, the VPN software add-on for routers includes firewall, encryption and tunneling capabilities. Some vendors link the user authentication to existing authentication services such as the RADIUS. Another advantage is there is no requirement to change the existing network for upgrading purposes. Thus, operating and ownership costs of VPN can be reduced.

However, there are certain limitations of router-based approach that need to be considered by network managers. First, firewall, encryption and tunneling are all done in the software basis, which could cause a problem under heavy traffic loads. In many cases, adding or upgrading software to a router might do some complications.

Software-based VPN services on a router require CPU-intensive usages especially when a high level of encryption, such as 3DES is used at high data-transfer rates. In this case, a hardware add-on dedicated to handling encryption tasks might be necessary. Thus this will add to the cost of deploying the VPN.

Some vendors do not offer add-on encryption hardware devices. This can be a major problem if a large portion of a router processing power is required to cater many users connected simultaneously to VPN at high-access speeds using the IPSec tunneling and high level of encryption. In this case, the VPN tasks would consume so much of the router processing cycles leading to the noticeable performance drop.

Now let analyze on the straight software-based approach. In this case, operating system suppliers and several third-party vendors may offer VPN services, such as encryption, tunneling and authentication required by users over the VPN link. Similarly to the router-based VPN, the software-based VPN also allows users to use existing equipment. This is because the VPN services-software can be installed or downloaded directly on the existing server. This means the network configuration remains intact and the same management skills and tools can be used to administer the VPN.

Another advantage is that the programs frequently tap existing network operating system authentication services. This can greatly simplify VPN administration by linking VPN access rights to existing defined user-access privileges.

However, there are also some constraints of using a straight software-based VPN approach. Similarly to the router-based VPN, performing the VPN encryption and tunneling tasks may take high processing power. To make things worst, the processing load on a server is hard to determine since there is no official standard used for this purpose. The unofficial factors that determine the load include the number of simultaneous VPN sessions that need to be supported, the level of encryption of each session, the type of tunneling used and the rate at which data is being passed over the VPN.

IT managers who opt for the software-based VPN approach typically start using an existing server. In most cases, IT managers along with vendors will perform the pilot run to examine the software-based VPN performance under various conditions. Such experience will help the IT manager to determine if the existing server is capable of supporting a more expensive and high-tech VPN deployment.

Lets review the firewall-based VPN. Many companies centralize their Internet security activities on firewalls to ensure the data integrity and confidentiality. The companies even check for computer viruses and malicious codes at their Internet-firewall. Besides, they also view that adding the VPN security services can be made only on the firewall. As a result, many vendors are now eager to introduce and develop various Internet firewall models with the built-in software of VPN services.

The main advantage of using firewall-based approach is network administrators capable to add new package on the existing firewall without requiring any additional equipment. This is done through paying additional fee to upgrade the VPN services in the existing firewall operating software.

Similarly to the router and straight software-based approaches, IT managers will have to fully determine whether the existing firewall can provide sufficient performance in terms of supporting required number of simultaneous sessions at whatever level of encryption, tunneling and transfer rates.

7.5.2 Hardware-Based VPN

VPN have spawned a new breed of dedicated VPN devices. These devices are designed to perform the tasks required to connect users and sites through VPN links. Specifically, dedicated VPN devices handle encryption and tunneling services for multiple, simultaneous VPN sessions.

The big advantage of using dedicated VPN devices is they can support more sessions under heavier encryption and data traffic loads. Using a dedicated device to perform VPN services means that other devices on the network, such as routers, servers or firewalls do not incur performance problems.

One of the biggest concerns in this hardware-based approach is the network configuration might be changed as a result of adding new dedicated devices. It will also be necessary to purchase warranties and service contracts for the new equipment. Perhaps even more challenging is that the device will have its own administration and management systems, which may not interoperable with the existing network management tools.

7.5.3 Carrier-Based (Service Provider-Based) VPN

It is suitable for a corporate to rely on service provider in a situation where they have no choice or lack of expertise in deploying VPN. In this case, a service provider can simply offer a managed VPN service that includes all of the hardware and VPN software to the corporate (Salamone 1999).

The advantage that the corporate can gain from this approach is there is no end-user client software for the corporation to maintain, thus eliminating client management issues associated with remote access. This is due to all the VPN intelligence facility resides in the service provider network.

CHAPTER 8

COMPARISON BETWEEN COMPETITOR TECHNOLOGIES AND VPN

Lets review the pros and cons of VPN by comparing with other competitor technologies that become as popular WAN solutions today.

8.1 VPN versus Frame Relay

Frame Relay is actually a high performance WAN protocol that operates at the physical and data link layers of the Open System Interconnection (OSI) reference model [10]. Originally, Frame Relay was designed for the purpose of standardization work on ISDN interfaces (DaSilva 1999). Currently, Frame Relay is used over a variety of other network interfaces as well.

As a matter of fact, Frame Relay can be considered as an instance of a packet-switched network where it enables end-stations to dynamically share the network medium and the available bandwidth [10]. In some cases, Frame Relay often is described as a streamlined version of X.25 that technically offers fewer of the robust capabilities, such as windowing and retransmission of lost data as offered in X.25 [10]. Since Frame Relay is strictly a Layer-2 protocol suite, it can provide higher performance and greater efficiency of transmission compared to X.25. As a result, Frame Relay is likely suitable for certain WAN applications, such as LAN-to-LAN interconnection.

A major development for the Frame Relay happened during 1990 when Cisco Systems, Digital Equipment, Nortel and StrataCom extended its basic protocol with additional features and capabilities for sophisticated internetworking environment known as the Local Management Interface (LMI) [10]. The International Union- Telecommunications Sector (ITU-T) is the body that standardizes Frame Relay globally, whereas the American National Standards Institute (ANSI) plays the roles to standardize Frame Relay within the United States alone. Figure 8.1 shows the Frame Relay components.

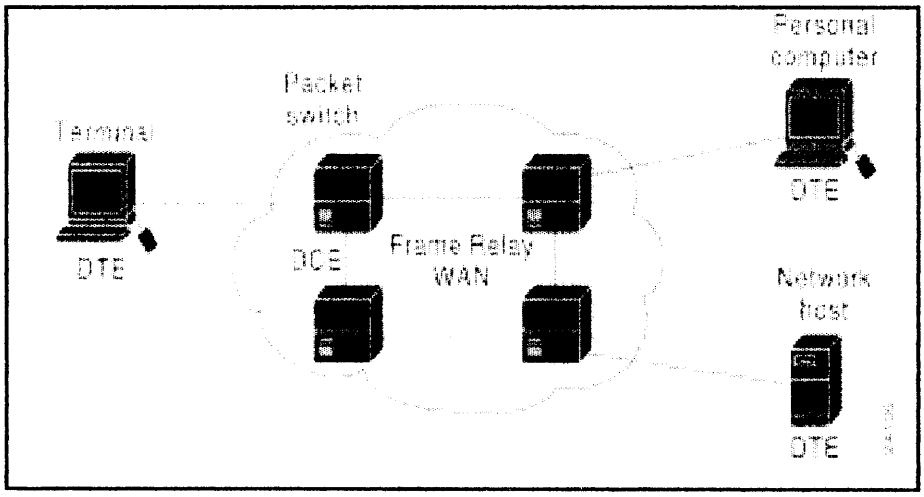


Figure 8.1: Frame Relay Components

Based on Figure 8.1, there are two types of devices attached on Frame Relay circuits that are Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE). DTE is actually a terminating device, such as terminals, PCs, bridges and routers used for a specific network and usually located on customer's premises. On the other hand, DCE is actually a carrier-owned internetworking device used for providing clocking and switching services in a network.

Frame Relay actually offers a service known as Frame Relay Virtual Circuit to establish a logical connection between two DTE devices via its Packet Switched Network or PSN [10]. The service can be classified into two categories that are Switched Virtual Circuit (SVC) and Permanent Virtual Circuit (PVC). In details, SVC is actually a temporary connection used in situations requiring only sporadic data transfer between DTE devices via Frame Relay PSN. There are 4 operational states in SVC that are Call Setup, Data Transfer, Idle, and Call Termination states. On the other hand, PVC is actually an established connection used for frequent and consistent data transfer between DTE devices via Frame Relay PSN. There are only 2 operational states in PVC that are Data Transfer and Idle states.

- Pros

First, VPN is cheaper to be implemented in connecting main network with its remote branch offices located at far distance since its pricing is just based on local WAN service

connection to POP plus Internet Access fee. In contrast, Frame Relay's pricing is much higher respectively since it is based on distance of network connected, bandwidth used, and sometimes data volume transferred.

Second, VPN reduces network management and administration burdens compared to setting up, owning, operating, maintaining, and upgrading Frame Relay infrastructures. In this case, by implementing VPN, a corporate can outsource some or all of WAN functions and operations to a local ISP so that the corporate enable to focus 100% on its core business strategic missions and objectives.

Third, VPN can also reduce WAN setup and maintenance by replacing modem banks and multiple Frame Relay circuits with a single wide area link that carries remote user, LAN-to-LAN, and Internet traffic simultaneously [40].

Lastly, by applying IP backbone in VPN circuits, ISP can eliminate the use of static Permanent Virtual Circuits (PVC) associated with connection-oriented protocols in data link layer communication provided by Frame Relay.

- Cons

First, Frame Relay has the ability to gain lower delay and higher throughput during peak time compared to VPN utilizing shared Public Network as the main backbone, which unable to avoid delays especially when full bandwidth is required to cater heavy traffics.

Second, Frame Relay can accommodate more flexible and use of bandwidth to large number of users compared to VPN. Through packet-switched technology implementation, Frame Relay enable end stations to dynamically share the network medium and the available bandwidth [10]. In this case, variable-length packets are used and switched between various network segments until destination is reached for more ordered data transfers. Besides, Statistical Multiplexing techniques are also applied for more efficient and flexible use of bandwidth.

Third, Frame Relay is more suitable to run time-sensitive applications across WAN, such as audio, video or a real-time database compared to VPN. This is because Frame Relay can provide the guaranteed low-latency connection via mesh network links. On the other hand, VPN that provides higher latency connection is suitable to support time-insensitive applications, such as e-mail and intranet access where short delays in transmission are acceptable [43].

8.2 VPN versus Dedicated Point-to-Point (Leased Line)

A dedicated point-to-point or leased line is essentially a private reserved pathway (or pipeline) through the service provider's network that is rented by the user to carry traffic [50]. In this case, to establish the connection and provide the interface to the service provider's network, some data transmission devices are required, such as router and Channel Service Unit / Data Service Unit (CSU/DSU). Since a leased line can be as a short permanent digital connection to local ISPs, a corporate can have a full or selective global Internet access from anywhere within the corporate network [41]. This dedicated permanent connection guarantees a quick connection to the Internet and costs are reasonable due to short distances [43]. Figure 8.2 below shows graphically the conceptual connection of leased line between sites via WAN.

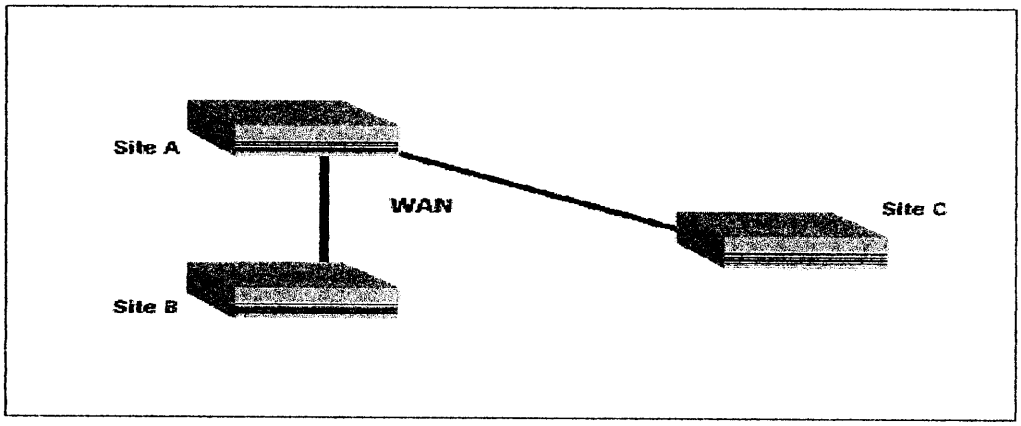


Figure 8.2: Dedicated Point-To-Point (Leased Line) Connection Between Sites

Basically, there are two general types leased line services that are the 56/64 Kbps and the T1/T3 leased line services. The 56/64 Kbps leased line is useful and suitable for networks that have moderate traffic requirements with steady and sustained patterns, such as large file transfers, between a limited numbers of sites [50]. It is stated that the 56

Kbps leased line can support around 10~12 people via the Internet, thus it becomes as a great option for a small office, which needs basic private connectivity, such as e-mail services within the office [11].

On the other hand, the T1/T3 leased line is purposely used for ultra-fast and mission critical connections [11]. In details, the T1/T3 leased line is utilized to link medium to large offices with enough bandwidth to cater several applications, for instances running web servers, hosting e-mail, and massive web surfing for entire offices. As a matter of fact, the transmission rate of the T1 leased line ranging from 384 Kbps to 3 Mbps (Full of dual T1 connection). In addition to that, the transmission rate of the T3 leased line ranging from 6 Mbps to 45 Mbps (Full of T3 connection).

- Pros

First, VPN can offer greater cost savings over dedicated point-to-point or leased line connection. According to Nortel Networks, the corporate that implements VPN can have direct cost savings by not paying leased line T1 (1.5 Mbps) and T3 (45 Mbps) link tariffs that fully covers an installation fee, a monthly fixed cost, and a mileage charge as well as charges offered by ISP that are tiered based on usage [40]. For example, as a public higher educational institution using 2 Mbps leased line, Universiti Utara Malaysia (UUM) has to pay RM 218, 190.00 to Telekom Malaysia Berhad as an annual link tariff (not included the annual payment to Mimos Berhad the Malaysian local ISP for Internet access (Jaring) which is RM 96, 200.00). This tariff actually covers the distance between UUM main campus in Sintok, Kedah and the nearest switching office or POP located in Alor Setar, Kedah that is about 50 Kilometers.

A comparison has been made by Malaysian local ISP, Jaring particularly on monthly operating cost of Internet-based VPN versus leased line (Refer to Table 2). Based on Table 2, the percentage of Internet-based VPN monthly operating cost savings is about 41.1% with respect to 128 Kbps leased line.

Private Line				Internet based VPN			
Item	Qty	Unit Cost (RM)	Ext. Cost (RM)	Item	Qty	Unit Cost (RM)	Ext. Cost (RM)
Capital Cost				Capital Cost			
Router	***3***	***5000***	***15000***	***Router***	***3***	***5000***	***15000***
128K Leased Line Start Up	***3***	***2000***	***6000***	***128K Leased Line Start Up***	***3***	***2000***	***6000***
				Jaring Leased Line Start Up	***3***	***1300***	***3900***
				VPN Gateway Plus Inc. Software	***1***	***42000***	***42000***
				VPN Gateway Express Inc. Software	***2***	***15000***	***30000***
Total Cost			21000	Total Cost			96900
Monthly Operating Cost				Monthly Operating Cost			
128K Leased Line	***3***	***7500***	***22500***	***128K leased line within 10 km to Jaring node (POP)***	***3***	***1714***	***5142***
				ISP Access Charge	***3***	***2700***	***8100***
Total Cost			22500	Total Cost			13242

Table 2: Leased Line and Internet-Based VPN Operating Cost Comparison

Unlike leased line, the pricing of VPN does not primarily depend a mileage connected. Using leased line can be very expensive particularly for networks spanning long transmission distances or requiring extensive connectivity between sites [50]. Besides, leased line customers have also to pay the bandwidth even if it is not being used that is typically about 70 percent of the time [50].

Second, VPN is actually more flexible and greater scalable network architecture than leased line where an organization enables to gain quickly and cost-effectively in

extending connectivity. In contrast, leased line is less flexible in terms of scalability. In this case, adding a new site to the leased line network might be costly since it requires a new circuit to be purchased and provisioned end-to-end for every site with which the new location must communicate.

- Cons

First, the uses of the Internet or shared Public Network as the main backbone in VPN is not that reliable where all the transmitted sensitive data have a high probability to be interfered by hackers. In this case, leased line is more reliable than VPN since it provides a dedicated point-to-point connection between two sites only. Consequently, it is very hard for external intruders to break in the connection built by leased line circuit.

Second, leased line has also higher availability compared to VPN. This is because in its nature, leased line is built up from integration of dedicated lines so that there is no statistical availability issue. On the other hand, VPN that primarily uses Public Network as the backbone has the availability issue especially during the heavy traffics time.

Third, leased line is available on the permanent basis and does not require a connection to be set up before traffic passed [50]. Therefore, the leased line can provide a more reliable, secure and faster service compared to VPN. Thus, the integrity of the transmitted data can be assured more effective through the use of leased line.

8.3 VPN versus X.25

X.25 a standardized protocol was developed by common carriers to increase subscriptions to Public Data Network (PDN) as well as to provide improved WAN equipment compatibility and lower cost [35]. X.25 users are charged based on Packet-Switched Network (PSN) use where the Federal Communications Commission (FCC) regulates all services and charges levied [35].

X.25 and related protocols are administered by an agency known as ITU whose members include the FCC, the European Postal Telephone and Telegraph organizations, common

carriers, and various computer and data communications companies worldwide. As a result, X.25 can be classified as a truly global voice and data communication standard.

The X.25 specification defines a point-to-point interaction between DTE and DCE. In this case, DTEs connect to DCEs, which connect to Packet Switching Exchanges (PSEs) and other DCEs inside a PSN and, ultimately to another DTE [35]. Figure 48 shows the relationship between the entities in the X.25 network. A DTE is connected to a DCE via a translation device known as Packet Assembler / Disassembler (PAD). ITU-T Recommendations X.28, X.3 and X.29 respectively, define the operation of the terminal-to-PAD interface and the interaction between the PAD and the host.

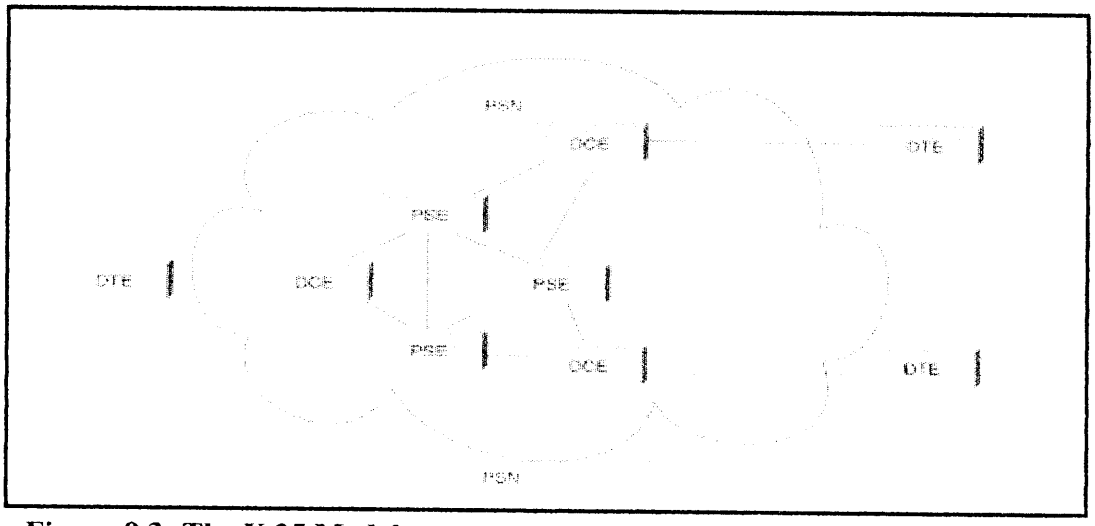


Figure 8.3: The X.25 Model

Technically speaking, the X.25 protocol encompasses the first 3-layers of the OSI 7-layered architecture as enlisted below [48]:

1. Layer-1 (Physical Layer).
    - This layer is concerned with electrical signaling processing and mechanical procedures for activating and deactivating the physical medium connecting both DTE and DCE. This layer includes several standards usage, such as V.35, RS232, and X.21 to identify and synchronize the interchange circuits and electrical characteristics, respectively of a DTE-to-DCE interface. In this case, X.21 standard supports point-to-point connections, speeds up to 19.2 Kbps, and

synchronous full-duplex transmission over 4-wire media [35]. The maximum distance between DTE and DCE is 15 meters.

2. Layer-2 (Data Link Layer).
   - This layer focuses on the implementation of a standard called Link Access Procedure Balanced (LAPB) and provides an error free link between two connected devices. In this case, LAPB defines packet framing for the link connecting both DTE and DCE. There are three-frame format types used by LAPB that are Information (I) frames (carry upper-layer and control information), Supervisory (S) frames (provide control information), and Unnumbered (U) frames (used for control purposes).
3. Layer-3 (Network Layer).
   - This layer describes packet formats and packet exchange procedures between peer Layer-3 entities [35]. This layer is also referred as the X.25 Packet Layer Protocol (PLP) that primarily dealt with the network routing functions and the multiplexing of simultaneous logical connections over a single physical connection. In addition, this layer uses 3-virtual circuit operational procedures that are call setup, data transfer, and call clearing to establish connection on either Switched Virtual Circuit (SVC) or Permanent Virtual Circuit (PVC) logical channel type.

The X.25 frame actually is composed of series of fields as shown in Figure 8.4 [35]. Layer-3 X.25 fields make up an X.25 packet and include a header and user data. Layer-2 X.25 fields include frame-level control and addressing fields, the embedded Layer-3 packet, and a frame check sequence (FCS).

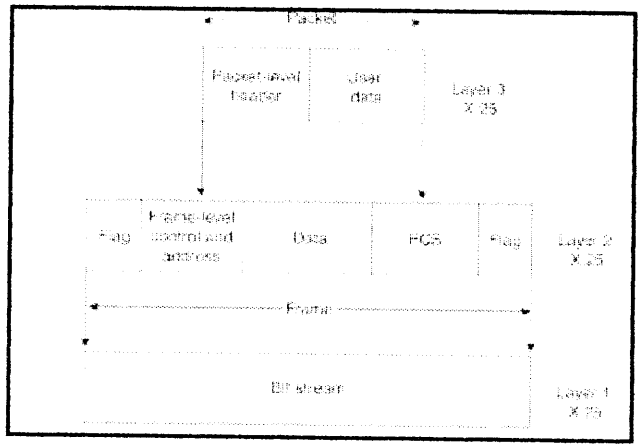


Figure 8.4: The X.25 Frame Format

- Pros

First, VPN is cheaper to be implemented in connecting main network with its remote branch offices located at far distance since it's pricing is just based on local WAN service connection to Point of Presence (POP) plus Internet Access fee. In contrast, X.25's pricing is much higher respectively since it is based on the bandwidth used and also usage per dial-up charge [43].

Second, the connections of Internet-based VPN are flexible since they use the open, distributed infrastructure of the Internet to dynamically transmit data between corporate sites according to organizational needs [40]. On the other hand, the connections of X.25 can occur rigidly within 2 types of logical channels [48]:

1. Switched Virtual Circuit (SVC), where every DTE is given a unique DTE address to ensure that a connection is established, data are transferred and then connection is released completely.
2. Permanent Virtual Circuit (PVC), where the logical connection is established permanently by the PSN administration to ensure that every data is always sent without requiring any call setup.

Third, Internet-based VPN has a larger geographic availability, meaning that it can connect main network with remote branch offices globally since the Internet access is available worldwide. In contrast, X.25 is typically can be implemented as WAN solutions in certain regions only, such as Asia, Latin America and Eastern Europe [43].

Fourth, VPN offers a greater bandwidth range from 56Kb up to 45 Mb depending on what type of backbone (either T1 or E1 or T3) is used between local WAN and POP, whereas X.25 can just accommodate bandwidth at the maximum of 64 Kb only [43].

Fifth, VPN is actually a local independent WAN service since all the packets can be transmitted via the Internet between multiprotocol Data Terminal Equipments (DTEs) through tunneling process. Technically speaking, the VPN Point-to-Point (PPP) encapsulated packet can contain multi-protocol data such as TCP/IP, IPX or NetBEUI

protocols [37]. In contrast, X.25 is local WAN service dependent since all the packets can be transmitted between X.25 switched protocol DTEs only. There might be technical reasons why X.25 network does not transmit multiprotocol data. For instance, although both X.25 and TCP/IP are packet switched protocols but they differ in a number of areas resulting no packet transmission occur between them [48]:

1. TCP/IP has only end-to-end error checking and flow control, whereas X.25 is error checked from node to node.
2. TCP/IP has a much more complicated flow control and window mechanism than X.25, to compensate for the fact that a TCP/IP network is completely passive.
3. The electrical and link levels are tightly specified in X.25 specifications, whereas TCP/IP is designed to travel over many different kinds of media, with many different types of link service, such as Ethernet, Frame Relay, ATM, and FDDI.

- Cons

First, the Internet-based VPN is not good at flow control especially when a full bandwidth is strongly required to cater heavy traffics. However, X.25 is found has an excellent flow control plus a useful speed-matching feature making it suitable for sending data at all time regardless traffic situation.

Second, VPN is still immature and not stable especially in assuring the data integrity since it has just been developed rapidly in the mid 1990's. In contrast, X.25, which has been around since the mid 1970's, is pretty well debugged and stable resulting no data errors especially in the modern X.25 networks [48].

Third, there is no single global standard protocol used for creating VPN currently. In this case, 4 different protocols have been applied depends on corporate requirements where PPTP, L2F and L2TP are largely aimed at the dial-up VPN, while IPSec are focused on LAN-to-LAN solutions [40]. On the other hand, X.25 network just deals with a single global standard protocol known as X.25 Packet Layer Protocol (PLP) regardless corporate requirements. The PLP is primarily administered by an agency of the United Nations called the ITU-T, which is responsible for standardizing voice and data

communications worldwide [48]. In this case, the standard X.25 packet sizes vary from 64 bytes to 4096 bytes (with 128 bytes being a default on most networks) [48].

8.4 VPN versus Integrated Services Digital Network (ISDN)

By definition, ISDN covers 2 "aspects". First, Integrated Services (IS) refers to its ability to sustain numerous applications. Second, Digital Network (DN) relates its end-to-end digital connections [17]. Today, ISDN has become as the natural evolution towards a high-speed digital communications infrastructure. It means that, ISDN becomes as a technology that will eventually enable anyone willing to convert their traditional phone line (copper wiring) to a digital (ISDN) line to make connections more quickly, to communicate at higher speeds, and to pass voice, video and data through this single medium. In other words, ISDN holds tremendous promise in every sphere of communications, from traditional applications, such as high-quality voice service, telecommuting and LAN-to-LAN connectivity to emerging applications such as videoconferencing, multimedia services, and long distance learning [17].

ISDN technology is standardized based on the ITU recommendations, which describes the protocols and architecture used in the worldwide digital communications network [17]. Figure 8.5 shows the traditional phone line (copper wiring) connection versus ISDN connection.

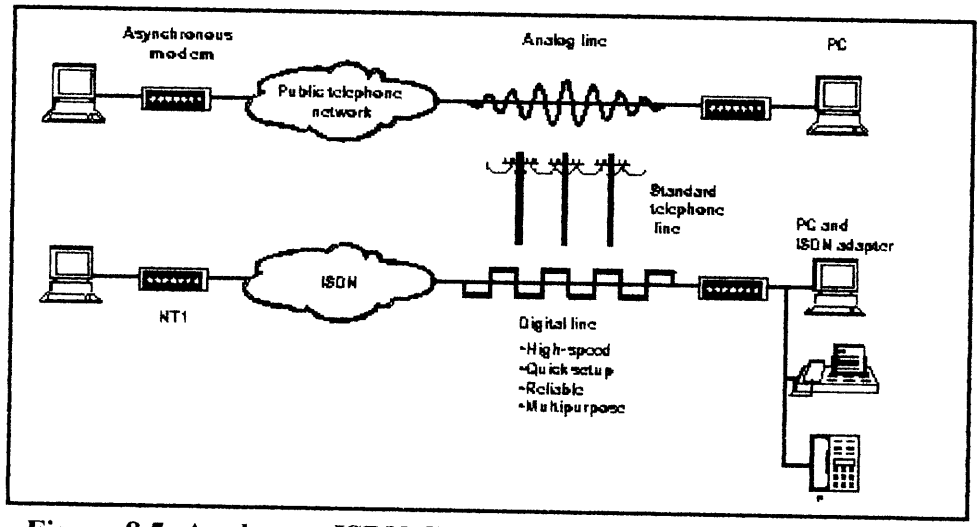


Figure 8.5: Analog vs. ISDN Connections

The process of moving data via ISDN is known as switching. There are two types of switching used, which are Circuit Switching and Packet Switching. Circuit switching ISDN transfers data between 2 points by setting up a physical link or circuit between them. The main advantage of circuit switching ISDN is that the data flow is not subjected to delays, and recipient receives the data exactly as it was sent by source. On the other hand, in packet switching ISDN, data is segmented into certain discrete units or packets. The advantage of packet switching ISDN is short data can be transmitted with little latency due to no end-to-end links establishment.

Technically speaking, there are 2 types of communications channels used in ISDN that are bearer service B-channels (carry data and services at 64 Kbps) and a single D-channel (carries signaling and administrative information to set up and terminate calls) [17]. The ISDN services available in the market can be divided into 2 specifications, which are Basic Rate Interface (BRI) and Primary Rate Interface (PRI). The BRI service is composed by 2 B-channels and a 16 Kbps D-channel (2B + 16D), which is really ideal for a service that can integrate multiple application requirements with the low bandwidth. Please refer to Figure 8.6 for the ISDN BRI service configuration. Meanwhile, the PRI service is composed by 23 B-channels and a 64 Kbps D-channel in the North America and Japan (23B + 1D) or 30 B-channels and a 64 Kbps D-channel in the Europe and most of Asia countries (30B + 1D), which is really ideal for a service that can allocate dynamically multiple application needs with the high bandwidth. Please refer to Figure 8.7 for ISDN PRI service configuration.

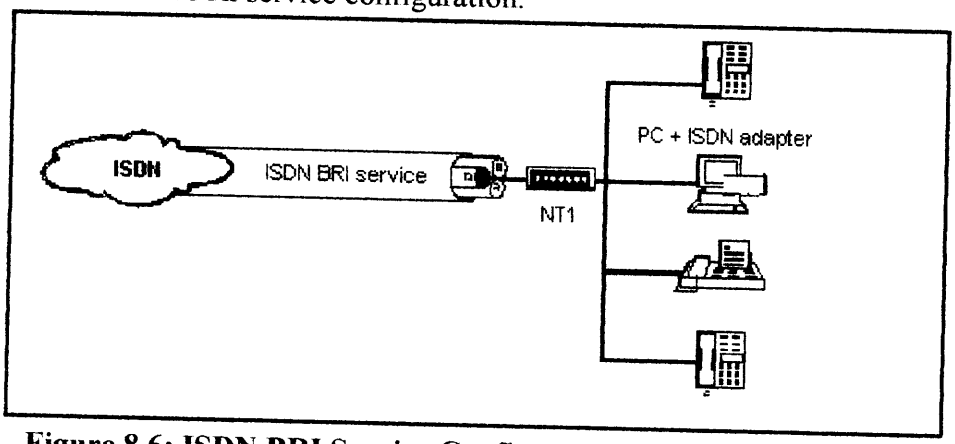


Figure 8.6: ISDN BRI Service Configuration

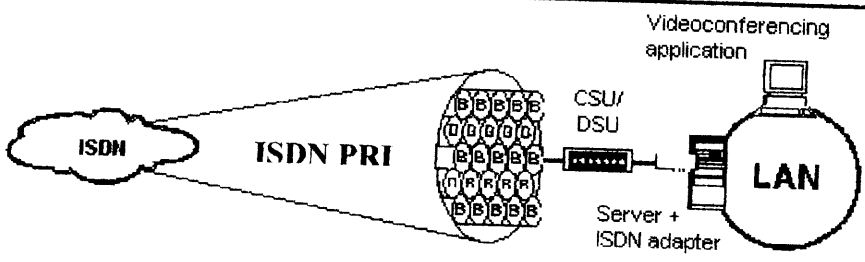


Figure 8.7: ISDN PRI Service Configuration

- Pros

First, VPN is cheaper to be implemented in connecting main network with its remote branch offices located far away since it's pricing is just based on local WAN service connection to POP plus Internet Access fee [43]. In contrast, ISDN that comes in 2 varieties, BRI and PRI are much more expensive where the pricing is primarily depends on the registration/installation fees, the fixed monthly charges and the usage charges [17]. The usage charges basically include both time-metered local and long distance charges, and also the per-dial charge [43]. Currently in the US, the registration/installation fees range from US$50 up to US$500 whereas the monthly charge fees range from US$20 up to US$90 [17]. Thus, the total of ISDN charges are around US$70 to US$590.

Second, the connections of the Internet-based VPN are flexible since they use the open, distributed infrastructure of the Internet to dynamically transmit data between corporate sites according to organizational needs [40]. On the other hand, the services of ISDN can inflexibly occur on 2 varieties only [17]:

1. The BRI service, where ISDN subscribers can access to two 64 Kbps B-channels and one 16 Kbps D-channel, which is really ideal for Small Office and Home Office (SOHO) that getting interest of controlling expenses, requiring a service that can integrate a multiple communication needs.
2. The PRI service, where ISDN subscribers can access to either twenty three 64 Kbps B-channels in North America and Japan or thirty 64 Kbps B-channels in Europe and most Asia region and one 16 Kbps D-channel, which is really ideal corporate that

requires higher bandwidth dynamically allocated among applications such as voice calls and video conference.

Third, the Internet-based VPN has a larger geographic availability, meaning that it can connect main network with remote branch offices unlimitedly since the Internet access is available worldwide. In contrast, both BRI and PRI ISDN services are limitedly implemented as WAN solutions in certain regions only, which are Europe, parts of Asia, North America and parts of Latin America [43].

Fourth, VPN offers a greater bandwidth range that is from 56 Kb up to 45 Mb depending on what type of backbone (either T1 or E1 or T3) is used between local WAN and POP. In contrast, the BRI ISDN service can just accommodate bandwidth at the maximum of 64 Kb per channel plus 128 Kb bonded only, whereas PRI ISDN can support up to 64 Kb per channel only [43].

Fifth, the Internet-based VPN is more flexible especially for remote access service since its traffic exchanged is on the one-to-many (1:M) basis whereas the ISDN traffic exchanged is on the one-to-one (1:1) basis only.

- Cons

First, the Internet-based VPN is not good at flow control especially when a full bandwidth is strongly required to cater heavy traffics. However, both BRI and PRI ISDN have a higher alternative performance with no virtually dial-up time requirements making them suitable for a busy central site [43]

Second, there is no single global standard protocol used for creating VPN currently. In this case, 4 different protocols have been applied depends on corporate requirements where PPTP, L2F and L2TP are largely aimed at the dial-up VPN, while IPSec are focused on LAN-to-LAN solutions [40]. On the other hand, ISDN just deals with the global standard protocols and architectures primarily administered by an agency of the United Nations called the ITU-T. The ITU-T is responsible for standardizing the

implementation of worldwide digital communications network across a telephony infrastructure based on copper wiring through providing the PRI and BRI ISDN services [17].

Third, VPN is still immature and not stable especially in assuring the data integrity and privacy since it has just been developed rapidly in the mid 1990's. In contrast, ISDN, which has been developed during the 1970's, is pretty well debugged and stable specifically in vastly improving the capability of the telephony copper wiring. In this case, ISDN has upgraded the telephony service capacity from originally transmitting the 28 Kbps analog signals to currently transmitting the 128 Kbps digital forms with high throughput, rapid call setup and high level of accuracy [17].

Fourth, the Internet-based VPN is not suitable for running the time-sensitive applications due to its high latency characteristics. In contrast, ISDN is suitable to run the time-sensitive applications via WAN, such as audio, videoconferencing, multimedia services and long-distance learning. This is because ISDN has a low latency characteristic where the flow of data is not subjected to delays in the ISDN circuit [17].

8.5 VPN versus Digital Subscriber Line (DSL)

DSL is a new telecommunications technology that can pump up existing local switched telephone lines (copper wirings) to between 10 and 100 times faster than the speed of the traditional dial-up modems (Gele 1997). DSL actually is a good alternative WAN solution since it has a lower cost than dedicated 1.544 Mbps T1 lines and has a less complicated architecture than ISDN. To end users, DSL simply means [26]:

1. Faster and more reliable connections between networks or to the Internet and it are always on. In this case, DSL offers high-speed data delivery by overcoming the inherent bandwidth limitations of an analog phone line connection (Gele 1997). This can be accomplished by maximizing the available capacity on phone lines to a much greater extent than voice calls.

2. Lower overall communications costs including fixed rate billings and no long distance charges. In other words, subscriber can have a lower installation cost (under

US$ 1000 per installation), a lower monthly cost (between US$ 100~US$300), and a lower cost per seat (between US$ 5~US$15 per person per month) relatively.

3. Access to more services from network providers particularly for both small and medium size businesses, and telecommuters.

Today there are 5 different offerings of DSL or sometimes referred as xDSL designed for various business and individual applications. There are Asymmetric DSL (ADSL); High Data Rate DSL (HDSL); Single-Line DSL (SDSL); ISDN DSL (IDSL) and Very High Data Rate DSL (VDSL). Let review briefly each of the of the xDSL offerings.

The first one is ADSL, which has transfer rate at 1.5 to over 6 Mbps downstream and 64 Kbps to over several hundreds Kbps upstream direction [26]. ADSL transmits digital data coexisted with analog voice traffic on the same wire pair. Currently, ADSL is suited to the last mile of copper wire currently in place between a phone company's central office and a home or smaller office. ADSL is mostly suitable to be used for the Internet/intranet access, interactive multimedia, remote LAN access, and video-on-demand since it applies both upstream and downstream directions of transmission (Gele 1997). In this case, a Web browser typically sends a small amount of data upstream to request content, while the content returned downstream may include large amounts of data in the form of graphics, video, or binary files [26]. Figure 53 shows the structure of an ADSL network.

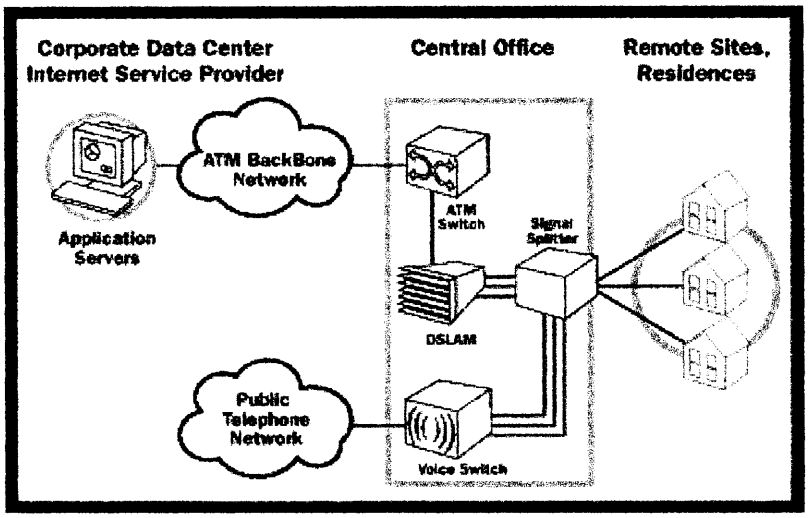


Figure 8.8: ADSL Network Structure

The second offering is known as HDSL, which has transfer rate of 1.5 ~ 2 Mbps in both directions. HDSL is a technology that use transceivers to provide digital service across two pairs of copper lines for up to 12 000 feet, without requiring intermediate amplifiers [26]. HDSL is actually suitable for a corporate to gain broader range of applications and easily to obtain LAN/WAN access leading it becomes as a good alternative to a dedicated T1 line (Gele 1997). It is reported that approximately 50% of all newly installed T1 circuits using HDSL.

The third one is SDSL, a type of DSL that becomes as a close cousin to the 4-wire HDSL. Even though, SDSL uses only one twisted-pair line, it can transfer data at speeds similar to HDSL in both directions. Thus, it is possible for SDSL to be expected gaining popularity particularly for Internet and remote LAN access in the near future (Gele 1997).

The fourth DSL offering is called IDSL. Similarly to SDSL, IDSL applies the more familiar 2B1Q-coding scheme, which is embedded in existing ISDN modems (Gele 1997). IDSL transmits data at the rate of 128 Kbps in both upstream and downstream directions and is mainly used for Internet and remote LAN access.

The fifth and the last one is called VDSL, which is able to deliver communications at impressive speeds between 13 to 52 Mbps downstream and 1.5 to 2.3 Mbps upstream. The VDSL technology uses include Internet access, video-on-demand, High-Definition Television (HDTV), remote LAN access, and interactive multimedia (Gele 1997).

- Pros

First, the Internet-based VPN can be used particularly for remote LAN access or LAN-to-LAN applications without having any restricted limitation of main network-to-branch offices line distance. However, the biggest disadvantage for DSL services in general is that the central office-to-subscriber line distance must be limited at the maximum of 18 000 feet or 3.4 miles or 5.4 Km (Gele 1997). The main reason for the distance limitation is that spreading the DSL signal over more and higher frequencies causes it be more susceptible to noise and interference. Therefore, line distance must be restricted in order

to maintain the reliability and the performance measures. As a result, the distance constraints have made DSL communications become impractical especially for mobile workers (Gele 1997).

Second, VPN actually can reduce network management and administration burdens where a corporate can outsource some or all of WAN operations including connectivity details and managing infrastructures to a local ISP. Thus, the corporate capable to focus 100% on its core business strategic visions and missions. On the other hand, DSL strongly requires businesses for having their own Information Technology (IT) personnel who are really expert at installing DSL premises equipments and maintaining DSL connections and telecommuters (Ybarra 1998). In other words, the businesses cannot outsource some or all of DSL operations to other parties, such as local ISP, vendors or local carriers.

Third, there is no gap or divergence on the ISP sides to deal with the newness of the VPN technology specifically in ensuring that the data is transmitted to the appropriate destinations via Internet. However, there are many gaps on the ISPs' end mainly to the newness and complexities of the DSL technology. In details, there are a lot of disparities or inequalities on the ISP sides particularly on how to put end-to-end DSL service together, how to integrate DSL into existing legacy management systems, how to perform loop qualification cost effectively, how to design an order form for service, how to train customer service reps and how to manage the DSL itself efficiently in general (Gele 1997).

- Cons

First, VPN that uses T1 service, as the main backbone specifically for conditioned local loop might not be so economical compared to DSL. In this case, the installation costs for T1 service is about US$ 6000 plus US$ 1300 per month per line whereas DSL installation costs below US$ 1000 plus US$ 300 per month per line for multiple users. Furthermore, the T1 service operating costs is approximately US$ 800 ~ 1300 monthly whereas DSL operating costs around US$ 100 ~ 300 monthly. Besides, DSL also offers

a lower cost per seat where businesses can use a router to share one DSL line and connect to a 100 or more workstations (persons) simultaneously where for each workstation (person) the cost is just about US$ 5 ~ 15 per month (Ybarra 1998).

Second, VPN can just offer a transmission rate ranging from 56 Kbps up to 45 Mbps depending on what type of backbone (either T1 or E1 or T3) is used between local WAN and ISP POP. On the other hand, the most high-speed DSL version known as Very High Data Rate DSL (VDSL) can deliver various communications applications, such as Internet access, video-on-demand, High-Definition Television (HDTV), remote LAN access, and interactive multimedia at the rate of 13 ~ 52 Mbps downstream and 1.5 ~ 2.3 Mbps upstream (Gele 1997).

CHAPTER 9
QUALITY OF SERVICE (QoS) AND SERVICE LEVEL AGREEMENT (SLA) FOR VPN

9.1 Introducing QoS

In general, users of a widely scattered VPN do not usually care about the network topology or the high level of authentication or encryption or firewalls that handle their traffic. They don't care if the network implementers have incorporated either IPSec tunnels or L2F tunnels or GRE tunnels. What they care about is something more fundamental, such as:

What Quality of Service can you expect from your VPN service provider, and how can you measure what level of service are you getting? [8] OR

Do I get acceptable response times when I access my mission critical applications from a remote office? [22]

As a matter of fact, acceptance levels for delays vary depend on user's perceptions or expectation levels. While a user would be willing to put up with a few additional seconds for a file transfer to complete, the same user would have less tolerance for similar delays when accessing a database or when running voice over an IP data network.

Here comes the need for the QoS in VPN. First, let define what it means by the QoS in VPN perspective. In general, the QoS is actually an end-to-end system architecture that gives network managers the ability to control the mix of bandwidth, delay, jitter and packet loss in the network [6]. In other definition, the QoS is referred to the ability of a network to provide a better service to the selected network traffic over various underlying technologies [15]. In this case, VPN should give better and more predictable network service compared to core WAN competitors, such as Frame Relay and leased line.

Generally, the QoS purpose is to ensure that corporate private network's mission critical traffic has acceptable performance. In the real world where bandwidth is finite and

diverse applications from videoconferencing to Enterprise Resource Planning (ERP) database lookups that vie for scarce resources. Consequently QoS becomes a vital tool to ensure that all applications can coexist and function at acceptable levels of performance.

Another issue to be highlighted here is about the significance of Differentiated Service (DiffServ) in the QoS for VPN. Actually, DiffServ allows certain network traffic to receive premium treatment at the expense of other less-critical traffic on the same WAN link. This idea is similar to what we find in airlines where a first-class passenger may receive better treatment or service than an economy-class passenger while they both physically reside on the same airplane [22].

In this paper, detail discussions will be made regarding the VPN QoS functions including the packet classification; the bandwidth management; the traffic shaping; the congestion avoidance and the enhanced traffic management. There will be also descriptions regarding the Service Level Agreement (SLA) for VPN.

9.2 Packet Classification

The aim of the packet classification function is to group packets based on the predefined criteria so that the resulting groups of packets can then be subjected to the specific packet treatments. The treatments might include faster forwarding by the intermediate routers and switches or lesser probability of the packets being dropped due to lack of buffering resources [22]. A DiffServ model feature, Committed Access Rate (CAR) is primarily used to perform packet classification through IP Precedence and QoS group settings. In general, CAR performs metering and policing of traffic and also providing bandwidth management [15].

It is necessary that traffic be classified before tunneling and encryption since otherwise the tunnel header that is appended to the IP packet would make the QoS markings in the IP header invisible to intermediate routers/switches, which need to read this information and act upon it. Classification brings into question the right match criteria. There are a number of criteria based upon which we may classify traffic before it enters the VPN that

are IP addresses, TCP/UDP port numbers, IP precedence, URL and sub-URL, MAC addresses, and Time of day.

The next step is to "mark" or "color" packets with a unique identification to ensure that this classification is respected end to end. In the near future, the IETF sponsored Differentiated Service Code Points (DSCP) could become the classification criterion of choice. The purpose behind this packet type of marking is to ensure that the downstream QoS features such as scheduling and queuing may accord the right treatment for packets thus marked. Figure 9.1 shows the packet classification process.

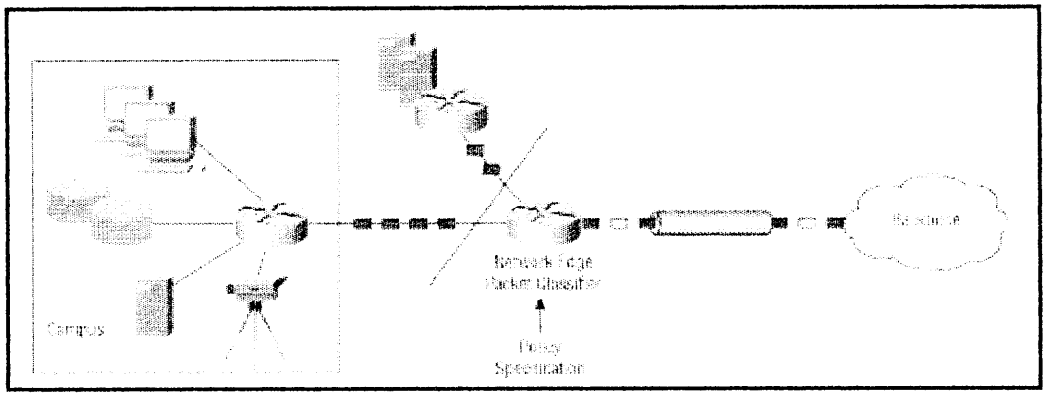


Figure 9.1: Packet Classification at Network Ingress

9.3 Bandwidth Management

Once traffic has been classified, the next step is to ensure that it receives special treatment in the routers. This brings into focus scheduling and queuing. The bandwidth management function is related to a flow process in which a group of packets share common criteria, such as a source/destination IP address, a TCP/UDP port number and a Type of Service (ToS). Figure 9.2 depicts the ToS field in the IP packet header.

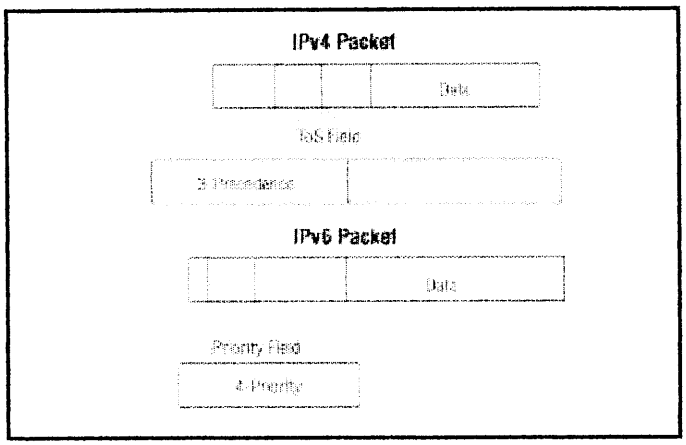


Figure 9.2: ToS Field in the IP Packet Header

There are 2 implementations of weighted fair queuing (WFQ) (used as a DiffServ model feature to allocate bandwidth): the Flow-based WFQ and the Class-based WFQ [22]. In the flow-based WFQ, packets are classified by flow. Each flow corresponds to a separate output queue. When a packet is assigned to a flow, it is placed in the queue for that flow. During periods of congestion, the WFQ allocates a portion of the available bandwidth to each active queue.

On the other hand, the class-based WFQ aims for providing weighted fair queuing functionality among traffic classes defined by the user. A user could create traffic classes using mechanisms like the Access Control Lists (ACLs) and then assign a fraction of the output interface bandwidth to each of these traffic classes. The primary difference between the flow-based WFQ and the class-based WFQ is the fact that in the flow-based WFQ bandwidth allocation is relative to other flows. But in the class-based WFQ, bandwidth allocation is absolute. The class-based WFQ allows the user to assign bandwidth to a class based upon a percentage of the available bandwidth or a fixed kbps value. Figure 9.3 shows the mechanism of the WFQ function.

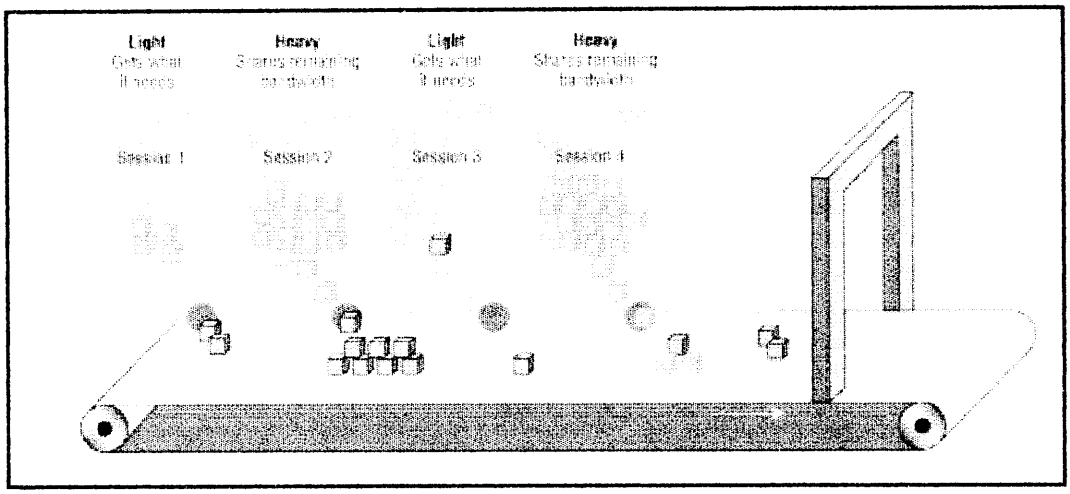


Figure 9.3: Weighted Fair Queuing

9.4 Traffic Shaping

The traffic shaping becomes necessary when Layer-3 traffic mostly be shaped to a desired set of rate parameters to enforce a maximum traffic rate. The outcome will be a smooth traffic stream. Traffic shaping queues and forwards data streams to conform to agreed upon the Service Level Agreements (SLAs). If bursty traffic is queued then TCP senders will identify this and in turn will back off and ensure that subsequent transmissions conform to a desired rate. This type of traffic shaping is commonly referred as adaptive traffic. Figure 9.4 shows the traffic shaping process.

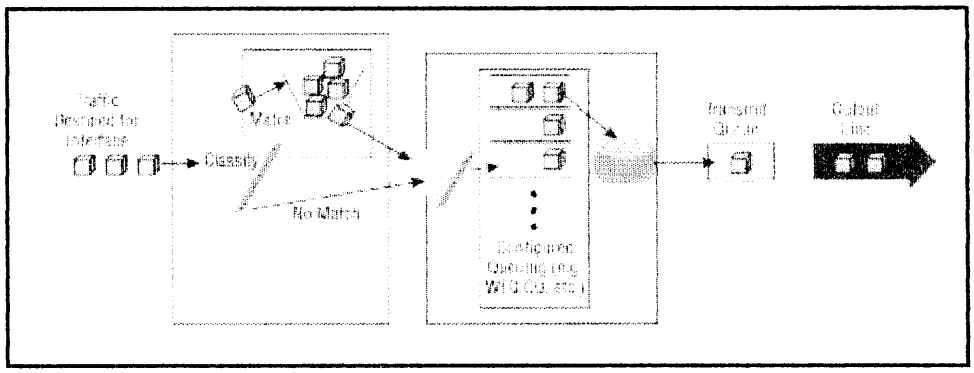


Figure 9.4: Generic Traffic Shaping

9.5 Congestion Avoidance

Congestion avoidance is defined as the ability to recognize and act upon congestion on the output direction of an interface so as to reduce or minimize the effect of that

congestion, which produces adverse effects in VPN [22]. A DiffServ model tool called the Weighted Random Early Detection (WRED) is mainly used for the congestion avoidance function (refer to Figure 9.5). In this process, the WRED will provide differential treatment of traffic by adding per-class queue thresholds that determine when packet drops will occur. The thresholds are user-configurable and set using the Command Line Interface (CLI) in the Internetwork Operating System (IOS) software.

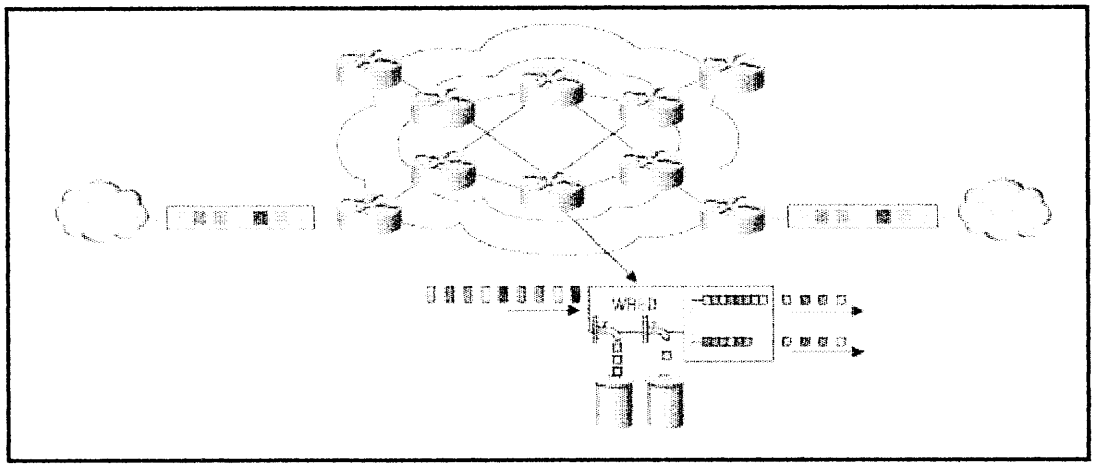


Figure 9.5: Weighted Random Early Detection (WRED)

Packet dropping is based upon the premise that adaptive flows such as the TCP will back off and retransmit if they detect congestion. By monitoring the average output queue depth in the router and by dropping packets from selected flows, the WRED aims to prevent the ramp up of too many TCP sources at once. Unchecked this ramping up could result in problems such as TCP synchronization (refer to Figure 9.6).

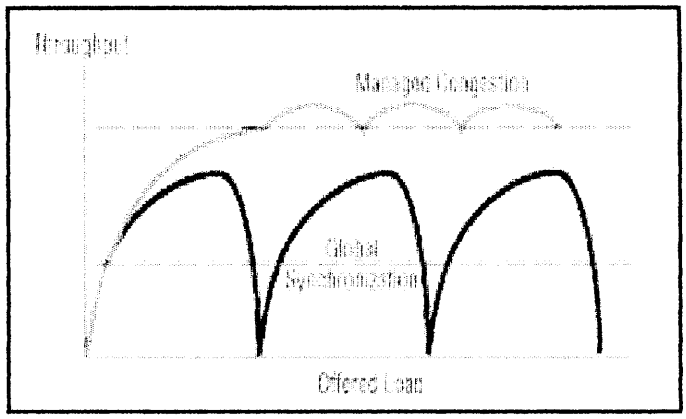


Figure 9.6: Global TCP Synchronization

Under this mechanism, the WRED function will give differential treatment by dropping packets from low priority traffic before it begins to drop packets from high priority traffic. The WRED function allows the user the option to select up to six such traffic classes.

9.6 Enhanced Traffic Management

It is important to have a multivendor internetworking standard that will strengthen VPN service capabilities through enhanced traffic management. In this case, the IETF has introduced an emerging standard known as the Multiprotocol Label Switching (MPLS) [6].

In general, the MPLS uses a label-based forward paradigm in its innovative approach. The label is used to indicate both routes and service attributes. At the ingress edge, incoming packets are processed and labels selected and applied. The core merely reads labels, applies appropriate services, and forwards packets based on the label. Processor-intensive analysis, classification, and filtering happen only once, at the ingress edge. At the egress edge, labels are stripped, and packets forwarded to their final destination.

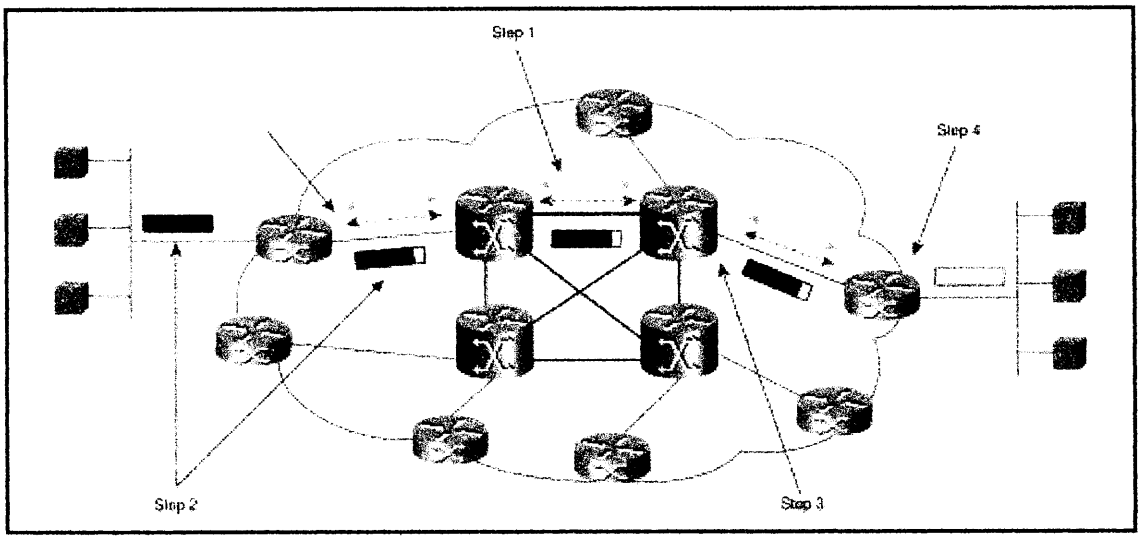


Figure 9.7: MPLS Operations

The easiest way to see how MPLS operates is to follow a packet through an MPLS-enabled service provider network as shown in Figure 9.7. In general, there are 4 steps

consisted in MPLS operations In Step 1, the network will build routing tables automatically. The Label Distribution Protocol (LDP) then will use the routing topology tables to establish label values between adjacent devices. This operation creates the Label Switched Paths (LSPs) or pre-configured maps between destination end points. In Step 2, an ingress packet enters the Edge Label Switch Router (LSR) to determine which L3 services it requires, such as the QoS and the bandwidth management. The Edge LSR then will select and apply a label to the packet header and will forward the packet. In Step 3, the LSR reads the label on each packet, replaces it with a new one as listed in the table, and forwards the packet. Finally, in Step 4, the egress Edge LSR strips the label, reads the packet header, and forwards it to its final destination.

For enabling business IP services, the most significant benefit of the MPLS is the ability to assign labels that have special meanings. Sets of labels distinguish destination address as well as application type or service class. The label is compared to pre-computed switching tables in core devices that contain L3 information allowing each switch to automatically apply the correct IP services in each packet and possibly separate types of traffic (such as best-effort traffic from mission-critical traffic). Since labels have local significance and are used many times in large networks, therefore it is nearly impossible to run out of labels. This characteristic is essential to implementing advanced IP services such as QoS, mega-scale VPNs with enhanced traffic engineering [6].

9.7 SLA Checklists and Future Perspective

It is strongly recommended for an organization (client or user) to clarify a few things with VPN service provider about the SLAs before implementing VPN services [8]:

1. What the QoS scheme is used in the network and what does it cover?
2. What is the level of guarantee of network availability? A typical guarantee is 99.8% network availability.
3. What backup options are offered and at what cost? Check to see whether the service provider offers backup connections such as ISDN or Frame Relay SVCs should the main connection fail.

4. Do customers get a credit when there is an outage and if so, what is the level of credit? Many service providers give service credits based on the duration of outages.
5. Is service availability covered in addition to network availability? Simply having a connection to the network is not enough; the VPN service that runs over the network must also be available.
6. Does the SLA cover temporary disconnection, for example when faced with hacker attacks on a firewall? Elective downtime should be part of the service to protect the integrity of your network.

In the future, the SLAs for VPN services are likely to improve as the various different QoS schemes are deployed more widely. However, until that time, the SLAs may be limited to connections over a single service provider's network. To ensure the end-to-end SLAs in the interim, traffic should stay on the same network. If the connection goes across networks, a service provider has little control over the quality of the other provider's network. This situation is likely to remain until service providers reach agreement on the SLA interworking.

CHAPTER 10

A TEN-POINT PLAN FOR BUILDING A VPN

Building a VPN requires considerable planning. There are 10-point plan outlines steps prepared by the Enterasys Inc. (a VPN vendor), which might help network administrators to successfully build and manage a VPN in their organizations [8].

10.1 Assess Corporate Connectivity Requirements

The first step is to look at the corporate current network and determine which remote access and branch office connections could be replaced with a VPN. Remember that uptime, performance and latency requirements all help determine whether an Internet VPN or a public network VPN is more suitable. Replacing the current remote access connections with a remote access VPN service makes technical and economic sense, but the potential impact on performance and latency does not justify the cost savings of replacing dedicated leased lines between branch offices with the Intranet VPN service.

Then decides what kind of WAN technology is most appropriate. Do remote users reach the corporate network over LAN/WAN or dial-up links? Is remote users part of the same organization? Do branch office connections use dedicated leased lines or switched services such as ISDN or Frame Relay? WAN connections for VPNs fall into two categories: the intranet links and the extranet links.

10.2 Implement or Update the Corporate Security Policy

It is important for management to be concerned about the security implications, especially if the proposed VPN involves the Internet connections or the extranet connections using public network services. Corporate networks are obvious targets for hackers, and management will require assurances that the network is protected against intruders.

An organization's security policy should define what forms of remote access are or are not allowed, and what types of authentication and authorization are used. The security

policy needs to be thoroughly revised when implementing VPNs. In particular, it needs to address whether the Digital Certificates, the Certificate Authorities (CAs) and the Public Key Infrastructures (PKIs) have roles to play in VPN.

Besides, security issues, the policy should address the eligibility for remote access, the executive accountability, the responsibility for connections, and the monitoring of the VPN usage. It also should cover procedures for giving the Internet access to traveling and remote employees. The policy might also cover such technical details as the lengths of encryption keys used in relation to time-sensitivity of the data handled.

For extranets, the policy should specify a procedure for rapid notification of changes in the remote user population. Those who are no longer with the organization must be removed from the authentication database as quickly as possible, and this requires coordination between the external user's organization and the VPN administrator. Human resources departments may already have procedures for managing consultant access and these may be appropriate for VPN users.

10.3 Determine a Backup Plan

VPN users are likely to run more mission-critical applications. Also, as VPN technology is expanded to include business partners, suppliers and customers through extranet connections, the need for a backup plan becomes even more important. Besides having redundant equipment and links, sites with high traffic loads will need to support load balancing across multiple devices and paths. Most VPN service providers support these features as part of their VPN solutions. Determining the backup plan early is key to long-term success and also ensures the right solution is finalized before equipment is purchased or an outsourced service is negotiated.

Having a combination of traditional remote access and remote access VPN especially in one remote access product means that the migration from one technology to the other is less painful. As users move over to remote access VPN, traditional remote access servers can be used to provide backup in the event that the VPN fails and can be used where a traditional remote access solution makes more economical sense. For intranet VPNs,

having a combination of traditional WAN access and VPN capability is essential since most VPN solutions are unable to provide the same level of performance and low latency as dedicated leased lines or Frame Relay services.

10.4 Determine the Best Product or Service Solution

Fortunately, all VPN solutions fall into 1 of 3 categories that are the Firewall-based, the Software-based, and the Hardware-based systems. All of these support remote access and some support intranets as well. For all solutions categories, check thoroughly 5 key areas of the VPN technology that are the protocol support, the encryption support, the authentication methods, the export of encryption technology, and the management of encryption keys.

10.5 Test Proposed Solution

Test the proposed VPN solution by carrying out a pilot project and analyzing the proposed solution extensively. Choose a small group of mobile users or a few remote sites and ask them to participate in the testing. Also, it is essential to include a good cross section of users to assess the problems that real users are likely to encounter. The pilot VPN test should cover assessment criteria, which are configuration; authentication and authorization; key production and distribution; network performance; troubleshooting mechanisms; and usability aspects.

10.6 Size the System

When sizing the system, make sure to estimate the total number of users, the typical number of concurrent sessions, and the time sensitivity of critical data. Also, make sure to take into account the connectivity requirements determined in Section 10.1.

If using a software-based VPN solution, for example a 200-MHz Pentium processor should be able to handle a single T1/E1 network connection assuming there is the 3DES encryption using 128-bit keys, the data compression, and the message authentication. Make sure also that there is as much memory as possible since additional memory allows more simultaneous connections. Lastly, check to see whether any options are available to

provide hardware assistance for the effective encryption or the smooth WAN connectivity.

10.7 Pick the Location for the VPN Equipment

When choosing the site of the VPN equipment, do consider on the number and type of remote users and the proximity of branch offices to each other. Mobile and remote employees will expect to have access to corporate intranet resources as before. In this case, it is recommended to place the VPN equipment and authentication servers on the intranet since most VPN products provide sufficient security to protect an enterprise's internal network from unintended access by users on the Internet.

For a business partner or supplier who are outside of organization, then it makes sense to put the VPN equipment on a firewall DMZ. In this case, separate connections for extranet access and internal VPN access may offer the best protection. Alternatively, if a single connection is used for both, then the VPN server and authentication server should be located on separate firewall DMZs.

10.8 Reconfigure Other Network Devices

Installing a VPN will impact other network devices since it may make use of the Network Address Translation (NAT) that maps private addresses from a block of reserved addresses to one or more public addresses visible on the Internet. Therefore, it is strongly recommended to configure on the Dynamic Host Configuration Protocol (DHCP) parameter that is used to assign IP addresses to client systems automatically; the Firewall if the VPN server is inside the firewall; and the corporate Domain Name System (DNS) server, which is responsible for resolving the host names of private network machines to IP addresses.

10.9 Install and Configure the VPN

For the software-based VPN and those built around firewalls, it is essential to begin with a secure system. Remove all unnecessary services, applications, and user accounts from

the server. Make sure the latest patches and security releases are installed. Only then is it safe to install the VPN software.

When configuring the VPN itself, set parameters for key length; primary and secondary authentication servers (with associated shared secrets); connection and idle timeouts; certificate generation; and key generation and distribution mechanisms. Use digital certificates to verify the identity of VPN users. For remote users, it also will be necessary to set up passwords, prepare connection scripts, and establish authentication procedures. Lastly, sync up authentication and authorization routines for getting secure VPN services.

10.10 Monitor and Manage the VPN

Set up the appropriate procedures to monitor and manage the VPN in terms of its utilization and throughput. This should be done ideally before users start really using the VPN service. Make sure that support staff have been trained to operate the VPN devices, including how to add new users, as well as how to set up and manage authentication and firewall services. Make sure also that network managers/engineers know how the VPN works and capable to do basic troubleshooting if something goes wrong.

Do monitor the performance of the VPN if its services are offered through a service provider to ensure that the agreed QoS metrics are maintained based on the Service Level Agreements (SLAs) specifications. The monitoring can be performed through a service provider web-based application or a management system with the necessary monitoring capability. This may look important if service provider implements a Split Management Horizon (SMH) in their VPN equipment, whereby service provider manages and monitors the equipment WAN side (such as WAN connections, routing, etc.) only to provide the appropriate QoS, while client manages and monitors the security side (such as authorization, firewall, etc.).

CHAPTER 11

CASE STUDY

11.1 VPN Solutions Implemented in the Real World

It has been known that VPN is an effective WAN solution by "converting" the Internet infrastructure to be as a secure private WAN link. Many today's corporate have included VPN as a key strategic component to meet business visions and missions in this information-based or the Internet-centric economy era. In this chapter there will be revelations on how VPN solutions are being implemented in the real world organizations. Besides there will be discussions regarding the VPN solution proposed for connecting the Universiti Utara Malaysia main campus in Sintok, Kedah and its branch campus in Sungai Petani, Kedah.

11.2 VPN Implementation in the Black & Veatch Corporation

First, let discuss briefly on how a big multinational company known as the Black & Veatch Corporation use VPN to meet very urgent and critical business needs. In this case, VPN technology is found works best as a stopgap for this company.

Let review the Black & Veatch Corporation background information briefly. Black & Veatch is actually a US$1.8 billion engineering construction company specializing in the power industry. Currently, the company earns 55% of its revenues overseas primarily in Asia, South America and the Middle East where demands for new power plants is growing rapidly [34]. The corporate headquarters is located in Kansas City, Missouri (MO), USA.

Due to Asian economic turmoil between 1997 and 1998, the corporate found that its business in the region was suffered badly. The corporate tried to formulate good strategies to keep its Asian regional offices operate but at the same time needed to economize wherever possible. As a result, instead of using leased lines, the company has chosen VPN as alternative and thrifty WAN solutions for its smaller regional offices particularly.

In this case, Black & Veatch decided to build Internet-based VPNs (Refer to Figure 2.4 for a basic conceptual diagram) in its small offices located in Indonesia, Singapore, and Thailand connected directly to local ISPs. The company also decided to use PPTP built in the Microsoft Network Operating System (NOS) software for running the encapsulation and tunneling protocols in the VPNs. This was because the company did not want to purchase additional software for running the newly designed VPNs. To reduce VPNs operating cost, Black & Veatch management agreed to give Solutions Group administrators (the company's former IT department, now a subsidiary) a full task to monitor the VPNs remotely from corporate headquarters in Kansas City, MO.

It is stated that today about one hundred Black & Veatch employees worldwide are using the VPNs as primary network for Internet and intranet access, sending e-mail, and also downloading marketing and financial data from headquarters [34]. Besides, the company also has gained a lot of direct cost savings through the VPNs implementation in its regional branches. For instance, for Jakarta office occupied by 25 employees, the company needs to pay only about US$1000 per month for ISP charges (the ISP basic rate: $40 per person per month x 25 person).

In the mean time, the company has clarified that the VPNs is not a platform for offices with users to access Black & Veatch's heavily load proprietary engineering design software. This is because the proprietary engineering design software is developed as a client/server application that can overload VPNs due to high bandwidth and reliability requirements. That is why the company currently is working to develop the heavily load software as a browser-based version so that it can be run feasibly over VPNs someday.

The company has found also that VPN has certain limitation in terms of its accessibility. In this case, VPN is found not suitable for remote access made by the company's employees who are in travel or in field. Alternatively, the employees tend to use IBM's network since IBM's dial-up software is much easier for users compared to finding numbers of the nearest ISP.

11.3 VPN Implementation in the Forum Corporation

Now let review on how VPN is implemented on a big scale by a small American company, the Forum Corporation in order to stay nimble and to win business opportunities in new markets. Forum is actually a global training and consulting firm based in Boston, Massachusetts (MA) [34]. It has 350 staff members working in headquarter located in Boston and in branches worldwide including in Asia and in Europe.

Several years ago, Forum's customers began to demand training programs that would serve their employees anywhere in the world. To do this efficiently and effectively, Forum needed a strategy for its employees to share knowledge. At the time, the company had to rely on the only legacy technologies it could afford, which are facsimile machines and a few carefully located ISDN connections.

In early 1997, the company has made a big move through initiatively implementing VPN as its newly emerging and promising WAN solution. In the year, Forum established an Internet-based VPN linking between its main corporate in Boston and its branch offices in Hong Kong and Toronto (Canada). The company then added its VPN link to its London (England) office in early 1998. Initially, certain groups of workers, such as salespeople, consultants and software developers used the network with VPN technologies for e-mail, intranet and file access, order processing, financial tracking, and also technical support. But then Forum added more features (such as, real-time collaboration, videoconferencing and on-line learning) to its VPN facility to support various mission-critical applications and communications between the US and international sites. The VPN technology infrastructure was also found bringing Forum closer to its customers and suppliers.

According to Enno Becker (Forum's director of technology infrastructure), the company's VPN infrastructure was actually equipped with a sophisticated security

technology from Check Point Software Technologies Ltd., and the Internet access with UUNet [34]. These VPN technologies actually brought good news to the company in terms of cost savings. In this case, the VPN was found could provide the same 128 Kbps bandwidth as the ISDN line in the Hong Kong office, but at approximately US$ 3000 for ISP monthly fees compared with the US$ 9000 for ISDN monthly bill. Besides, Forum was able to quadruple the bandwidth from 56 Kbps up to 256 Kbps (between its office and the ISP) at an added cost of only US$ 1000 per month for its larger and busier office (where speed was more important) located in London. Such cost reductions and speed improvements has helped Forum to be more productive as well as more responsive to its clients.

However, there is one caveat in this VPN implementation where the company can control the bandwidth only from their sites to the ISP on both ends of the connection. In between the data is widely subjected to the perpetrators or whims of the shared Public Network.

More recently, the company has working on to make use the VPN infrastructure as an extranet link with high security capabilities. In this case, the company has allowed several of its customers and software development partners to collaborate in real-time on the development of training software over the implemented VPN. According to Becker, users can test software, access technical documents, run customer demos or download information from Forum's servers [34].

To sum up, VPN has provided the Forum Corporations with a simpler, cheaper, and more accessible WAN solution so that the small growing company can survive in this information age. It is only a matter of time before Forum has standardized all of its VPN applications and configurations, allowing users or clients to connect directly to the Internet and headquarters from wherever the users or they clients may be.

11.4 VPN Solution Proposed for the Universiti Utara Malaysia (UUM) Main Campus and Branch Campuses Nationwide

In this chapter, there will be discussions regarding VPN solution that is exclusively proposed to connect the UUM main campus with its branch nationwide. In this case study, the proposal is made on the basis of linking the UUM main campus in Sintok, Kedah with its branch in Sungai Petani, Kedah through the use of a secure Intranet VPN application specifically. Three main aspects will be emphasized on in the discussions, which are the methodology used by the proposed VPN, design of proposed VPN, the configuration of proposed VPN, and the method (standard) used in the proposed VPN.

11.5 The Design of the Proposed VPN for UUM

First, it is important to enlist down and clarify the steps (used as the systems approach or methodology) in designing the proposed VPN for UUM. The steps are:

1. Conduct a feasibility study
   - Do a lot of literature reviews regarding VPN conceptually. Then try to understand some assessment factors in identifying the problem definition, such as the limitations of traditional WAN solutions (in this case, leased line) that makes VPN as the best alternative solution.
2. Prepare a proposed VPN design plan
   - Try to determine three feasibility factors if possible in preparing the VPN design plan, which are Technical Feasibility that covers the configuration/layout and hardware/software components used; Operational Feasibility that covers the VPN applications (specifically intranet VPN, in this case); and Economic Feasibility that includes the VPN cost-effectiveness compared to other competitor technologies (dedicated leased line, in this case).
3. Understand the existing Integrated Sintok Local Area Network (ISLAN) used in UUM
   - Try to know first the existing configuration, hardware, and WAN technology used in the UUM main network known as the ISLAN (detail explanations will be included in later parts).

4. Identify the geographic scope
    - Try to get some ideas on the physical location that will be interconnected by the newly proposed VPN. In this case, the VPN is used to link the UUM main campus in Sintok (where the nearest POP is in Alor Setar) and the UUM branch campus in Sungai Petani (where the nearest POP is in Sungai Petani).
5. Identify the proposed VPN security and control
    - Try to identify the protocol that is suitable for the proposed VPN in maintaining the integrity, confidentiality and reliability of data or packet transmitted between the UUM main campus and its branch campus. In this case, the IPSec is chosen as the standard security protocol. Besides, the De-Militarized Zone (DMZ) network configuration is identified suitable to protect the UUM ISLAN from being attacked by perpetrators or hackers.
6. Analyze and design the proposed VPN configurations
    - The configurations / layouts made based on the UUM network goal, which is to provide a cost-effective and a secure WAN link between UUM Sintok and UUM Sungai Petani (refer to Chapter 11.6).
7. Evaluate the proposed VPN hardware components
    - Try to find, shortlist and describe the technical specifications of the hardware components, which are VPN-optimized routers and PIX Firewalls recommended for this proposed VPN (detail explanations will be included in later parts).
8. Evaluate the proposed VPN software applications.
    - Try to identify and describe the software applications that is really suitable or match to implement with the proposed hardware components (more explanations in later parts).
9. Compare the operating cost of the proposed VPN with respect to other competitor technologies
    - Try to identify first the cost of operating the traditional WAN solution (leased line, in this case) and the cost of operating the proposed VPN. Make a comparison (detail explanations in later parts).

As mentioned in Step 3, it is important to know first the existing configuration, hardware, and WAN technology used in the UUM main network known as the ISLAN. Figure 11.1 shows the ISLAN Design implemented by UUM (courtesy of UUM Computer Center Department).

The UUM ISLAN basically uses the Gigabit Ethernet (GbE) standard as the main backbone. The ISLAN GbE is used because it can provide dramatic increases in the bandwidth available for all authorized UUM users to access servers and applications. In this case, the GbE provides 1000 Mbps or 1 Gbps bandwidth for LANs of all sizes included in the ISLAN with the natural upgrade path for its implemented Ethernet or Fast Ethernet installations, leveraging existing end stations, management tools and training.

Based on Figure 11.1, the "heart" of the GbE-backbone ISLAN is the switches (Lucent Cajun P880 Switch and Lucent Cajun P550 Switch models). These switches are linked to each other using one pair of 1000BaseLX Single Mode Fiber Optics. Both switches control all the data traffic in the ISLAN by linking with hubs located all over UUM through various cabling standards, such as 100 Base FX, 100 Base TX, 1000 Base SX, and 1000 Base LX. The Lucent P880 Switch is also connected via a Multimode Fiber Optics to the WAN router used for accessing the Internet services known as Jaring provided by Mimos Berhad.

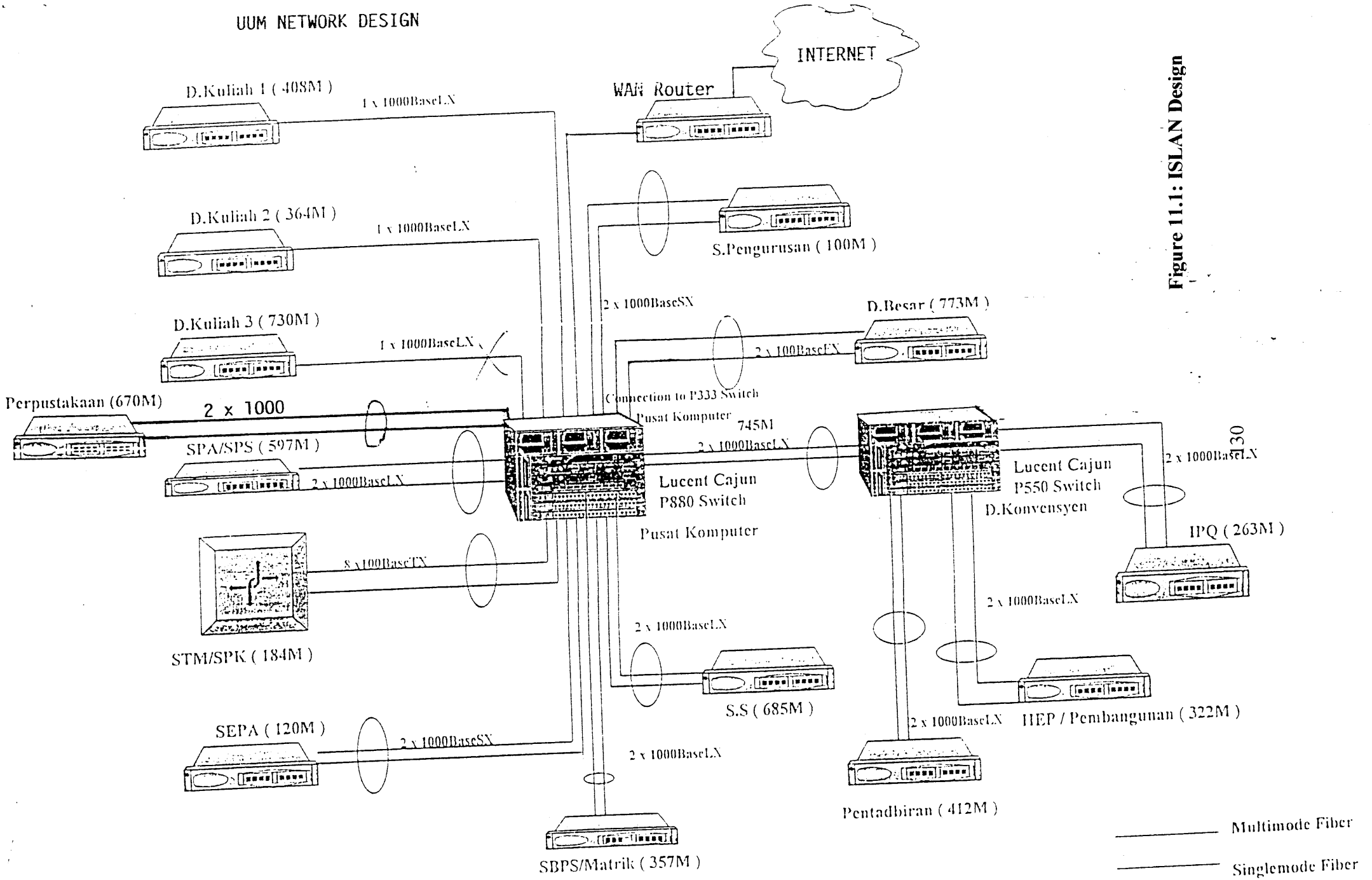


Figure 11.1: ISLAN Design

Following Step 9, let compares the operating cost between the proposed VPN and the leased line if it used as the WAN solution between UUM Sintok and UUM Sungai Petani campuses. Currently, the WAN router (equipped with the Firewall) is directly connected to the nearest Telekom Berhad's Point-of-Presences (POPs) placed in Alor Setar (about 50 km from Sintok) via the 2Mb leased line. According to the UUM Computer Center Department, the annual tariff for this Telekom Berhad's leased line is RM 218,190.00 (thus, estimated rate @ RM 4363.80 per km) whereas the annual fee for the Mimos' s Internet access service is RM 96, 200.00. Thus, the total sum of annual operating cost for the ISLAN facility is RM 324, 390.00.

To compare the operating cost between the proposed VPN and the 2Mb leased line, assumptions and cost estimations are required since the design is still in the conceptual phase. Imagine if the UUM main campus has a dedicated leased line with its Sungai Petani branch campus (assume that the distance is about 125 km). Mathematically, the 2Mb leased line annual tariff is estimated around RM 545, 475.00 (estimated rate @ RM 4363.80 per km). Therefore, summing up with the Internet access service fee (RM 96, 200.00), the annual operating cost will be around **RM 641,675.00**. Relatively, the operating cost sums are quite high especially for an educational institution like UUM. This cost burden logically become worse as if the branch campus located further than Sungai Petani due to a higher operating cost with a greater connected mileage services.

Now imagine if there is an intranet VPN connection between UUM Sintok and UUM Sungai Petani campuses. The 2Mb leased line annual tariff between UUM Sintok and POP in Alor Setar will be stick to RM 218,190.00. On the other hand, the 2Mb leased line annual tariff between UUM Sungai Petani and the nearest POP in Sungai Petani (assume that within 10 km) will be around RM 43, 638.00 (estimated @ RM 4363.80 per km). Therefore, the annual operating cost of the proposed VPN (after both leased line annual tariffs being added with Internet access service fee) is around **RM 358, 028.00**. Thus, a lot of cost savings can be gained through the implementation of extranet VPN, which is around **44.20%** [((RM 641,675 – RM 358,028)/RM 641, 675) * 100%].

Thus, it would be wise to propose UUM to use intranet VPN as an alternative cost-effective and secure WAN solution attached to the existing ISLAN facility.

The next thing is to determine the hardware components that should be included in the proposed VPN design as mentioned in Step 7:

1. Router
    - For the UUM main campus sites, it is recommended to use Cisco 7200 Series Routers. This is because, Cisco 7200 series routers are good VPN solutions for headquarters or organizations, such as main campus in this case, through integration of high-speed, and industry-leading routing with comprehensive VPN services. [25]. These services can provide UUM with scalable VPN platforms for better and more cost-effectively accommodate remote-access, remote-office, and extranet connectivity using the Internet. Besides, the Cisco 7200 series routers also are built with the high port density and robust delivery [25]. This will make the newly designed VPN solutions scalable while also accommodating extensive private WAN aggregation requirements pervasive in classic WAN environments. The most important feature that the Cisco 7200 series routers have is it can deliver tunneling and encryption services suitable for intranet applications required by this proposed VPN. In this case the Cisco 7200 series routers can support many protocols, such as IPSec, L2TP, L2F, GRE, PPTP, and Microsoft Point-to-Point Encryption (MPPE) for securing data over the shared public network or the Internet infrastructure [25]. For perimeter security applications, the Cisco 7200 series also support the Cisco IOS Firewall feature set, enabling stateful packet filtering services.

      On the other hand, it is suggested for the UUM branch campus located in Sungai Petani to use the Cisco 2600 series routers that are claimed a good VPN solution for medium-sized branches by supporting robust extranet VPN services as required by this proposed design. In addition, the Cisco 2600 series can also support for a wide range of serial, channelized, ISDN, and modem interfaces making it become as a flexible VPN platform [25]. For medium-sized branch

offices with a single Network Module (NM) slot, the Cisco 2600 is an ideal platform for VPN because its RISC processor provides the power to run the robust tunneling and QoS features for VPN. In addition, to IPSec, GRE, L2F, and L2TP, the Cisco 2600 series also capable to do a stateful packet filtering along with Cisco IOS Firewall as well as to offer optional encryption hardware modules.

2. Firewall
   - It is recommended to choose the Cisco Secure PIX Firewall allocated on both main and branch campuses since it would be no interoperable or compatibility issue in hooking up with the Cisco routers. In general, the PIX Firewall is claimed delivers strong security, and with market-leading performance creates little to no network performance impact. Besides, the PIX Firewall capable to enforce a secure access in the intranet VPN link as required by this proposed design. Some of the beneficial PIX Firewall features are [46]:
     a. 16 MB Flash Memory Card that permits the PIX Firewall to store larger configurations and additional information.
     b. AAA Service Selection that specifies exceptions to previously defined rules in the AAA command.
     c. AAA Server Groups that defines separate groups of TACACS+ or RADIUS servers for specifying different types of traffic.
     d. Adaptive Security Algorithm (ASA) that allows one-way (inside to outside) connections without an explicit configuration for each internal system and application.
     e. Gigabit Ethernet that provides access to high-speed (1000 Mbps) Ethernet interfaces (suitable for the UUM's GbE-backbone ISLAN application).
     f. Graphical User Interface (GUI) with PIX Firewall Manager that lets user to configure the PIX Firewall via GUI interfaces rather than command line interfaces.
     g. IPSec that provides VPN access via digital certificates or pre-shared or manual keys.

h. Multimedia Support that makes use of applications including Real Audio, Real Video, Xing Stream Works, CU-See-Me, VDOnet VDOLive, and etc.

i. Registration, Admission, and Status (RAS) Version 2 that handles the increased popularity of multimedia applications, such as video conferencing and Voice over IP (VoIP).

j. Routing Information Protocol (RIP) Version 2 that provides Message Digest (MD5) authentication of encryption keys by listening in passive mode and/or broadcasting a default route.

For main campus specifically, the Cisco Secure PIX 520 Firewall model is suitable since it is intended for large enterprise organizations and complex high-end traffic environments. The PIX 520 Firewall also has a throughput of up to 370 Mbps with the ability to support up to 6 Fast Ethernet interfaces and to handle up to 250,000 simultaneous sessions. On the other hand, the Cisco Secure PIX 515 Firewall model is recommended for the UUM branch campus in Sungai Petani. Technically, the PIX 515 Firewall is intended for Small/Medium Branches or Remote Offices deployments and has throughput measured at 120 Mbps with the ability to support up to 6 Ethernet interfaces (2 of which are the 10/100 Ethernet interfaces) and to handle up to 125,000 simultaneous sessions. The PIX 515 actually contains two Ethernet 10/100 interfaces on its motherboard, 16 MB Flash memory, and 32 MB of Random Access Memory (RAM). Besides, the PIX 515 also has two PCI slots for installing additional interfaces or a VPN card.

The next thing is to determine the software that can be used to manage or configure all the hardware components used the proposed VPN (as mentioned in Step 8). It would be appropriate to use the Cisco IOS software since all the VPN-optimized routers proposed are selected from the Cisco series model. The Cisco IOS software has the enhanced security features, such as application-based filtering, defense against network attack, and real-time alert.

In addition, it is recommended to utilize the IPSec software on the PIX Firewalls for the purpose of providing perimeter security by maintaining stateful control of connections between connected network segments. The benefit of implementing the IPSec software is it can support secure VPN between multiple endpoints, and include client-initiated remote access VPN from Windows PC using Cisco Secure VPN Client Software, Cisco routers, other PIX Firewalls, or other standards-compliant IPSec devices. It is suggested to use the intrusion-detection systems software in conjunction with PIX firewalls, known as Cisco NetRanger for the purpose of extending perimeter security to packet payload level and determining the authorization of traffic.

11.6 The Configuration of the Proposed VPN for UUM

In this segment, there will be included the proposed VPN layout in both UUM main campus in Sintok (Figure 11.2) and its branch campus in Sungai Petani (Figure 11.3). There will be brief explanations on how the components are used in connecting both UUM main campus and its branch campus.

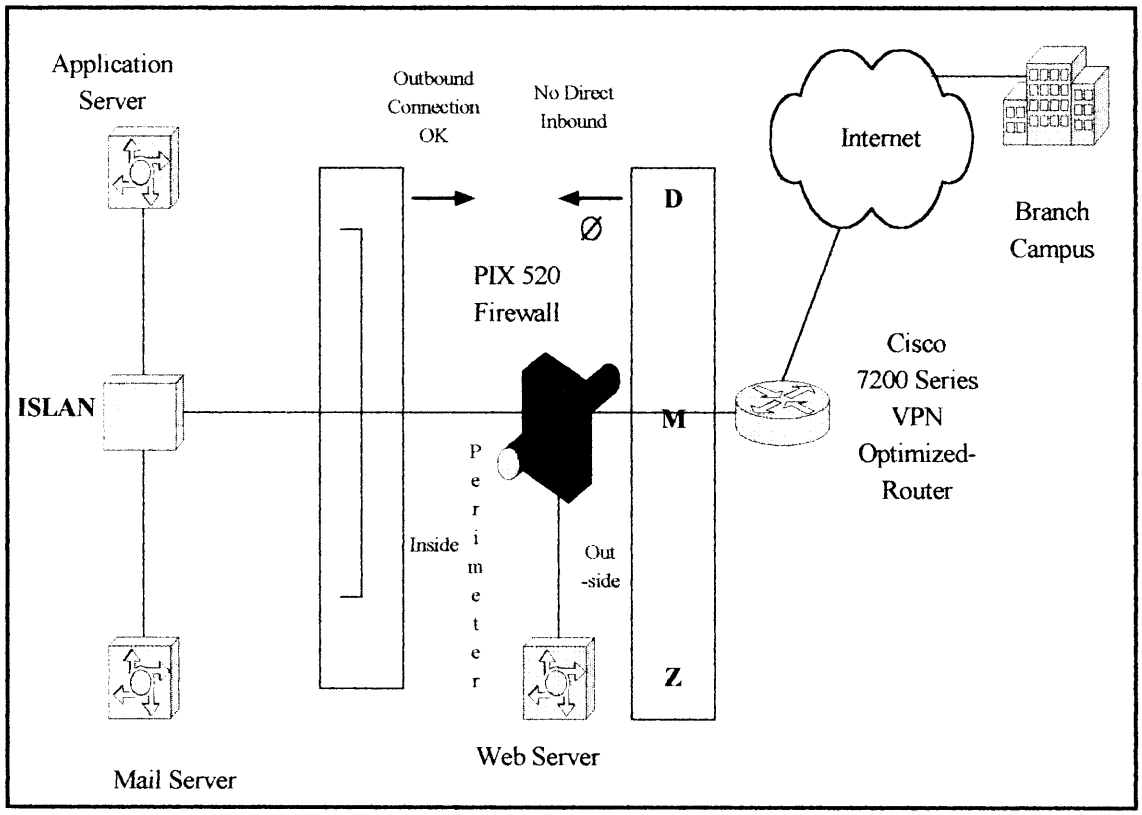


Figure 11.2: UUM Main Campus Proposed VPN Configuration

Based on Figure 11.2, the PIX 520 can optionally support multiple outside or perimeter networks, also known as Demilitarized Zones or DMZs (refer to Chapter 3.4 for details). In this case, connections between the networks (at the main campus side) can be controlled by the PIX Firewall. Attackers or hackers may be able to reach the DMZ where Web server are placed, but they will not be able to damage internal protected segments where ISLAN, Mail server and Application server are located. The PIX 520 also is linked with the 7200 Series VPN-Optimized Router, which is connected directly to the nearest POP in Alor Setar via the 2Mb leased line before entering the Internet infrastructure. Figure 11.3 depicts the proposed VPN configuration for UUM branch campus in Sungai Petani.

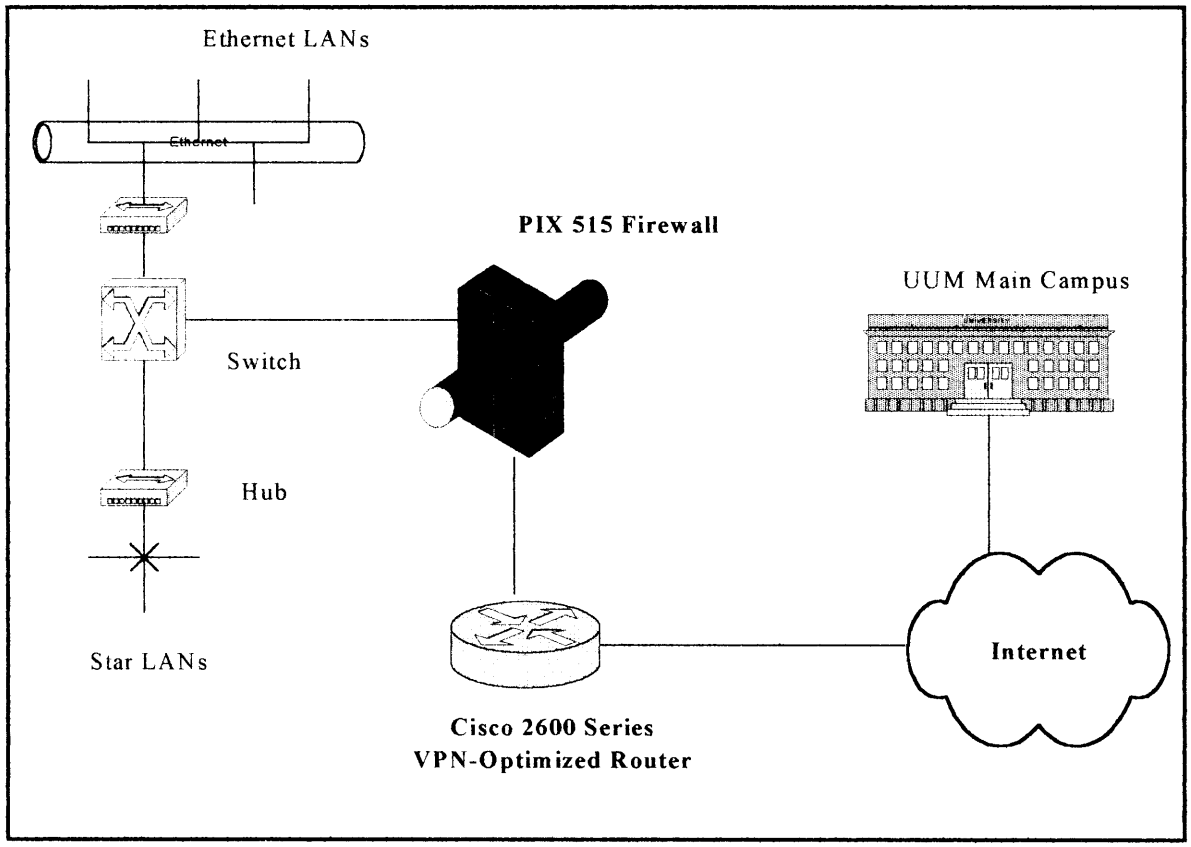


Figure 11.3: UUM Branch Campus Proposed VPN Configuration

Based on Figure 11.3, the PIX 515 is directly connected to switch, which control all the hubs placed within the UUM branch campus. The hubs are actually linked to all possible standard of LANs built in the branch campus building. The PIX 515 is also connected to the 2600 Series VPN-Optimized Router, which is linked directly to the

nearest POP within the Sungai Petani area via the 2Mb leased line before entering the Internet infrastructure.

In the Internet infrastructure, there will be a mechanism used to transmit packet at the highest security level, known as tunneling. Basically, tunneling is the encapsulation and encryption of entire transmitted packets to hide the networking data in addition to the application and payload layers (refer Section 11.8 for the proposed tunneling protocol).

11.7 Alternative Hardware and Software Components for the Proposed VPN

Besides Cisco products (as mentioned earlier), there are also alternative products from other VPN vendors that might suitable for the proposed VPN. Let reviews briefly on the alternative hardware and software components both UUM main and branch campuses:

1. Firewalls
   - First choice is possibly using the Nortel Network's Shasta 5000 Broadband Service Node (BSN) particularly in the UUM main campus. The Shasta 5000 that can do firewalling tasks, can support VPN at 128 000 users per 7 rack (Total of 896 000 users) simultaneously. The Shasta 5000 Firewall actually can support the IPSec AH and IPSec ESP operations through the use of DES56 and 3DES packet compression algorithms. Second choice is applying the Check Point FireWall-1 on both UUM main and branch campuses. The FireWall-1 actually is a fully integrated enterprise security suite that includes access control, user authentication (featuring X.509 digital certificates, RADIUS, and TACACS/TACACS+ protocols), content security, auditing, and NAT.
2. Routers
   - As a matter of fact, the Nortel Network's Shasta 5000 BSN can also be used as a router for the UUM main campus. In this case, the Shasta 5000 router is technically can support multi routing protocols, such as OSPF, RIP, IS-IS, and BGP. Another choice is the Check Point VPN-1 Appliance family products, suitable for the UUM branch campus. The integrated VPN-1 Appliances include a full suite of routing protocols including RIP, OSPF, DVMRP, BGP, Virtual Router Redundancy Protocol (VRRP), and IGRP.

3. Software Appliances
    - It is possible to implement the Check Point VPN-1 SecureRemote (client-side encryption software) particularly in the UUM branch campus in Sungai Petani. The VPN-1 SecureRemote supports IPSec/IKE and X.509 digital certificates, and standard data encryption and user authentication protocols. Besides, it would be recommended to add the VPN-1 SecureClient (to the VPN-1 SecureRemote). The VPN-1 SecureClient adds powerful security features, such as access control and security configuration control.

11.8 Method Used for the Proposed VPN Connectivity

In general, VPN allows the multiprotocol used in different sites to ensure that all the packets can be easily over the Internet through the tunneling method. In this project, the IPSec is chosen as the standard protocol to provide secured communications at the network layer (L3). In this case, through the IPSec tunnel mode, an entire IP packet is encapsulated within an IP packet to ensure that no part of the original packet is changed as it is moved through a network [32]. The entire original, or inner, packet then is transmitted through a "tunnel" from one point of an IP network to another where no router along the way needs to examine the inner IP header (refer Section 6.4.4 for more IPSec information). Technically speaking, there are two main reasons why IPSec is suitable for this proposed VPN.

First, both PIX 515 and PIX 520 Firewalls have IPSec encryption built-in, permitting both site-to-site (intranet) VPN deployments. Thus, there is no logic reason to pay for extra cost for applying other tunneling protocols. Besides, there will be no routing and interoperable issues since both sites used the same tunneling protocol.

Second, the IPSec can provide many reliable security services, such as data resource authentication, data integrity, confidentiality and protection against replay attacks. This security implementation will provide for secured transactions over the Internet, since IP is the language used for communications over the Internet.

CHAPTER 12
CONCLUSIONS

In general, newly evolved VPN is found can provide business with a new paradigm of fulfilling communications requirements through offering various forms of beneficial WAN solutions. The solutions covered the spanning range of business entities from telecommuter to branch / small office and to headquarter / main office. In this case, the solutions are derived from various VPN types of application, which are extranet, remote access, intranet (site-to-site), enterprise, firewall and internal applications.

Compared to other existing competitor technologies, the promising VPN can help business more effective in terms of many aspects. Precisely, some of the aspects are reducing infrastructure complexity; providing more flexible services and greater scalable in extending enterprise network; and offering lower operating and maintenance costs.

Unlike Frame Relay, VPN has the characteristic that can reduce the complexity of WAN setup and maintenance. This is done by replacing modem banks and multiple Frame Relay circuits with a single wide area link that carries remote user, LAN-to-LAN, and the Internet traffic simultaneously. By applying IP backbone in VPN circuits, ISP can eliminate the use of complicated rigid Permanent Virtual Circuits (PVC) associated with connection-oriented protocols in Layer-2 provided by Frame Relay. On the other hand, unlike DSL technology, there is no gap or divergence on the Service Provider sides to deal with the newness of the VPN technology specifically in ensuring that the data is transmitted to the appropriate destinations via the Internet. In this case, VPN technology has feasible solution features and specifications that make the Service Provider sides easily to run essential operations, such as putting VPN end-to-end service together, integrating VPN into existing legacy management systems, designing and updating an order form for service, training customer service reps, and also managing or upgrading or maintaining the VPN facilities in the Internet environment efficiently.

Furthermore, the VPN architecture is actually more greater scalable than leased line where an organization enables to extend connectivity quickly and cost-effectively. In this case, leased line is less flexible and too costly since adding a new site requires a new circuit to be purchased and provisioned end-to-end for every site with which the new location must communicate. Besides that, the connections of the Internet-based VPN are more flexible than ISDN's. This is due to the connections use the open, distributed infrastructure of the Internet to dynamically transmit data between corporate sites based on organizational needs. On the other hand, the services of ISDN can rigidly occur on 2 varieties only, which are the Primary Rate Interface (PRI) and the Basic Rate Interface (BRI) services. In addition, the connections of the Internet-based VPN are more flexible compared to X.25. As mentioned previously, VPN uses the open, distributed infrastructure of the Internet to dynamically transmit data between corporate sites. Contradict to that, the connections of X.25 can occur rigidly within 2 types of logical channels only that are the Switched Virtual Circuit (SVC) and the Permanent Virtual Circuit (PVC).

Unlike Frame Relay, VPN is cheaper to be implemented in connecting main network with its remote branch offices located at far distance since its pricing is just based on the local WAN service connection to the POP plus the Internet access fee. In contrast, Frame Relay's pricing is much higher respectively since it is directly based on the distance of network connected, the bandwidth used, and sometimes the data volume transferred. More over, unlike leased line, the pricing of VPN does not primarily depend a mileage connected. Using leased line can be very expensive particularly for networks spanning long transmission distances or requiring extensive connectivity between sites. Furthermore, leased line customers have also to pay the bandwidth even if it is not being used (statistically 70 percent of the time). VPN is cheaper to be implemented as remote access or site-to-site service compared to X.25. This is because VPN operating cost is just based on local WAN service connection to the Point of Presence (POP) plus the Internet access fee, while X.25's pricing is much higher respectively since it is based on the bandwidth used and also the usage per dial-up charge.

Even though, VPN is not good enough relatively in protecting the integrity, the security and the confidentiality of sensitive data (compared to expensive leased line or Frame Relay), but VPN still can be as a cheaper WAN solution to be implemented in providing a secure link over the Internet or the shared Public Network. This is because not all organizations especially the ones that involved in the small or medium-scale business afford to build such a highly cost leased line or Frame Relay infrastructure. Basically, there are four key components of VPN security that operate at different points throughout the network:

1. Tunnels and Encryption
    - As a matter of fact, VPN offers users with a wide range of tunneling protocols to protect encapsulated data from being intercepted and viewed by unauthorized entities. By using the tunneling protocols, user also can have logical, Point-to-Point (PPP) connections across a connectionless IP network, enabling application of advanced security features. The tunneling protocols employed in VPN currently are IP Security (IPSec), Point-to-Point Tunneling Protocol (PPTP), Layer-2 Tunneling Protocol (L2TP), Layer-2 Forwarding Protocol (L2F), and Generic Routing Encapsulation (GRE). In VPN also, encryption mechanism is applied to the tunneled connection where packets are being scrambled making them become legible only to authorized senders or receivers. Some of the encryption technologies (deployed by VPN) available in the market today are Data Encryption Standard (DES), Triple DES (3DES), and 40/128-bit RC4.
2. Packet Authentication
    - Packet authentication is also included in VPN services because it can protect packets transmitted over the unsecured Public Network from being intercepted and modified their contents before being forwarded to their destination by perpetrators or hackers. In other words, without packet authentication service, the integrity of data cannot be protected. One way to protect the data integrity is by embedding the Authentication Header (AH) and the Encapsulation Security Protocol (ESP) into the IPSec packet. Both AH and ESP should be employed in conjunction with industry-standard hashing algorithms, such as the Message Digest 5 (MD5) and the Secure Hash Algorithm (SHA).

3. Firewalls and Intrusion Detection
    - The Internet-firewall is actually a critical part of an overall security feature of VPN. Firewall is primarily used to monitor traffic crossing network perimeters and to impose restrictions based on corporate security policy. Without firewall, an organization cannot protect its VPN from unauthorized access to computing resources and network attacks, such as the Denial-of-Service (DoS). Besides, it is also essential to include intrusion detection system in conjunction with firewall in VPN since the system can provide extend perimeter security into the packet payload level through examining the content and context of every single packets
4. User Authentication
    - It is important to ensure that authorized users can gain access to enterprise computing resources, while at the same time unauthorized users are locked out of VPN thoroughly. In this case, VPN solutions are built around the Authentication, Authorization, and Accounting (AAA) capabilities to provide the foundation in authenticating users, determining access levels, and archiving all the necessary audit and accounting data. Some of the authentication technologies (deployed by VPN) available in the market are the Remote Access Dial-In User Service (RADIUS) and the Terminal Access Controller Access Control System Plus (TACACS+).

Frankly speaking, it is wise to implement VPN as a secure WAN link in connecting the UUM main campus with its branch campuses (including in Sungai Petani as stated in this project case study) nationwide over the Internet infrastructure. In this case, it is suitable for UUM to implement the intranet VPN type of application (refer Chapter 11 for more details information). VPN is found can offer a lot of benefits to UUM in terms of extra flexibility, greater scalability and higher cost-savings when compared to competitor technologies (as mentioned in earlier parts of this chapter). Another thing is UUM can also gain an effective network protection through 4 key components of security offered by VPN (as mentioned in earlier parts of this chapter).

Generally, VPN have certain constraints in delivering its WAN applications to users. Since the Internet or the shared Public Network being as the backbone, VPN is found not so reliable in guaranteeing the sensitive data security, integrity and confidentiality. The data transmitted via the Internet backbone is having high probability to be "hacked" and "modified" by network perpetrators. Besides, Service Provider might temporary unable to provide optimum bandwidth to avoid delays at a critical moment whenever there are heavy traffics. In addition, since the VPN Quality of Service (QoS) building blocks are left to Service Provider (instead of being integrated into corporate networking policy), corporate managements may have limited control and authorization in their own deployed VPN. Consequently, this is not really beneficial for corporate in the long-term run.

It is hoped that there will be some scientific researches done by telecommunication specialists or networking professionals in the future to overcome or at least to improve the constraints as mentioned above. The researches should be focused on analyzing the VPN architectures or configurations, tunneling protocols, firewall applications, intrusion detection techniques, and authentication mechanisms. It may be necessary to design and to develop new VPN solution features/characteristics that make VPN as the remarkable WAN solution in the next telecommunication era.

In this project report, there are some literature reviews regarding encapsulation / tunneling protocols used in VPN. The reviews basically cover the foundation, characteristic, and application aspects of each tunneling protocol. A continue study can be done to improve this project by making the comparison in terms of pros and cons between these protocols. Besides, it will be essential also to do more study in determining which security key components technologies (including encryption, authentication, and intrusion detection technologies) are really fit to be matched with those protocols in gaining superb WAN solutions. In details, the study should verify which encapsulation / tunneling protocols-security key components technologies combinations are suitable for every application type of VPN and every business entity ranging from telecommuters to small branches and to headquarters. Based on the findings of this continuing study, it is possible for users to implement VPN more effectively and efficiently in the future.

CHAPTER 13

REFERENCES

1. Airamo, Joona. "Virtual Private Networks", 1997.
http://www.tcm/hut.fi/Opinnot/Tik-110.501/1997/virtual_private_networks

2. Beyda, William J. Data Communications: From Basic to Broadband. 2nd ed. Prentice Hall International, 1996.

3. Chae, Lee. "Lesson 123: Virtual Private Networks", 1998.
http://www.networkmagazine.com/magazine/tutorial/9810tut.htm

4. Cooper, Frederic J, Chris Goggans, John K. Halvey, Larry Hughes, Lisa Morgan, Karanjit Siyan, William Stallings and Peter Stephenson. Implementing Internet Security. 1st ed. Indianapolis: New Riders Publishing, 1995.

5. DaSilva, Luiz A. "Frame Relay Presentation", 1999.
http://www.ee.vt.edu/~ee46141d/fr.pdf

6. "Delivering New World Virtual Private Networks with MPLS". A Cisco Systems Incorporated White Paper.
http://www.cisco.com/warp/public/cc/cisco/mkt/servprod/dial/tech/mpls_wi.htm

7. "Encryption". A Novell Corporation White Paper
http://www.novell.com/corp/legal/encrypt.html

8. "Enterasys's Virtual Private Network". An Enterasys Incorporated Handout.
http://www.enterasys.com/vpn/

9. Ferrell, Tom. "Virtual Private Networking Is Real Technology-Now".
http://www.vpdn.com/content/vpnbackground/whitepapers/compatible.html

10. "Frame Relay". A Pulsecom Incorporated White Paper.
http://www.pulsecom.com/framewp.htm

11. "Leased Lines". A Galaxy Internet Services Incorporated White Paper, 1999.
http://www.gis.net/business/leasedlines.html

12. Gele, Brian J. "Digital Subscriber Line (DSL) Services: A New Telecommunications Alternative?", 1997.
http://www.instantweb.com/m/mahesh/4453/DSL.HTML

13. Herscovitz, Eli. "Secure Virtual Private Networks: The Future of Data Communications", 1998.
http://www.vpdn.com/content/vpnbackground/whitepapers/RADGUARD.html

14. Hughes, Larry J. Actually Useful Internet Security Techniques. 1st ed. Indianapolis: New Riders Publishing, 1995.

15. "Introduction: Quality of Service Overview". A Cisco Systems Inc. White Paper. www.cisco.com/univercd/cc/td/doc/product/software/ios/20/12cgcr/qos_c/qcintro.htm

16. "IPSec". A Cisco Systems Incorporated White Paper. http://www.cisco.com/warp/public/cc/cisco/mkt/security/encryp/tech/ipsec_wp.htm

17. "ISDN: The Evolution of Digital Communication". An Eicon Inc. White Paper. http://www.eicon.com/ISDN/whtpap1.htm

18. "LanRover VPN Gateway Site Planning Guide". http://www.shiva.com/pdf/vpnsite.pdf

19. "Managed IPSec VPNs: Building Virtual Private Network". A Cisco Systems Incorporated White Paper. www.cisco.com/warp/public/779/servpro/services/vpn/VPN_Managed_IPSec_TSD.pdf

20. "Networks Go Virtual". A 3Com Corporation White Paper. http://www.3com.com/news/vpn_jp.html

21. "Overview of Access VPNs and Tunneling Technologies". A Cisco Systems Incorporated White Paper. http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/vpn_soln/vpdnover.htm

22. "Quality of Service for Virtual Private Networks". A Cisco Systems Incorporated White Paper. http://www.cisco.com/warp/public/cc/sol/mkt/ent/vpne/tech/qsvpn_wp.htm

23. Ranum, Marcus J. and Matt Curtin. "Internet Firewalls Frequently Asked Questions", 1998. http://www.clark.net/pub/mjr/pubs/fwfaq

24. "Redefining the Virtual Private Network (VPN)". A Checkpoint Inc. White Paper. http://www.checkpoint.com/products/vpn1/vpndef.html

25. "Reference Guide: A Primer for Implementing a Cisco Virtual Private Network". A Cisco Systems Incorporated White Paper. http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21_rg.htm

26. "Remote Network Access Using Digital Subscriber Line Technology". A Flowpoint Corporation White Paper, 1999. http://www.flowpoint.com/tlc/whitepapers/wp-rna/

27. Salamone, S. "VPN White Paper: The Basic VPN Implementation Calls for a Tunnel Trip", 1998.
http://www.internetwk.com/VPN/paper-5.htm

28. Scott, C. "Why Build a Virtual Private Network". A Microsoft Corporation White Paper, 2000.
http://www.microsoft.com/technet/network/vpnch1.asp

29. Semeria, Chuck. "Internet Firewalls and Security: A Technology Overview". A 3Com Corporation White Paper, 1996.
http://www.3com.com/nsc/500619.html

30. Shay, William A. Understanding Data Communications and Networks. 2nd ed. Pacific Grove: Brooks/Cole Publishing, 1999.

31. Sheldon, Tom. "General Firewall White Paper", 1996.
http://www.ntresearch.com/firewall.htm

32. Stallings, William. "IP Security". A Cisco Systems Inc. White Paper, 2000.
http://www.cisco.com/warp/public/759/ipj_3_1_ip.html

33. Taylor, Laura and Bradley Hecht. "VPNs are Hot, but Where are They?", 1999.
http://idm/.internet.com/articles/199911/ft_11_16_99a.html

34. "The Bargain Hunter's Guide to Global Networking – Virtual Private Networks", A CIO Online Article.
http://www.cio.com/archive/040199_vpn.html

35. "Troubleshooting X.25 Connections". A Cisco Systems Inc. White Paper.
http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1919.htm

36. "Understanding PIX Firewall". A Cisco Systems Inc. White Paper, 2000.
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v52/config/intro.htm

37. "Understanding Point-to-Point Tunneling Protocol (PPTP)". Microsoft Corporation White Paper, 1997.
http://msdn.microsoft.com/library/backgrnd/html/Understanding_PPTP.htm

38. "VPLink Technology". A VPNet Corporation White Paper, 1998.
http://www.vpnet.com/products/vplink.html

39. "What Is... a firewall (a definition)", 2000.
http://whatis.com/firewall.htm

40. "Web ProForum Tutorial: VPNs". A Nortel Networks Inc. White Paper, 2000.
http://www.webproforum.com/vpn/index.html

41. "Welcome to Mistral Internet – Services (Leased Line)". A Mistral Incorporated White Paper.
http://www.mistral-uk.net/lline.htm

42. "White Paper: Security Issues for Enterprise VPNs". A Cisco Systems Incorporated White Paper.
http://www.cisco.com/warp/public/cc/sol/mkt/ent/vpne/tech/sevpn_wp.htm

43. "Wide Area Networking: A User's Guide". An Intel Incorporated White Paper.
http://www.intel.com/network/white_papers/wide_area.htm

44. "Virtual Private Network".
http://www.whatis.com/vpn.htm

45. "VPN: High Availability to Insure Continuous Internet Connectivity". A Nokia Incorporated White Paper.
http://www.nokia.com/securitysolutions/network/availability.html

46. "VPN and IPSec Supported Standards". A Cisco Systems Inc. White Paper.
www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v52/ipsec/intro.htm

47. "VPN: Managed Firewall Services with Nokia Security Solutions". A Nokia Incorporated White Paper.
http://www.nokia.com/securitysolutions/network/managedfirewall.html

48. "X.25 Packet Switched Networks". A Sangoma Incorporated White Paper.
http://www.sangoma.com/x25.htm

49. Ybarra, Dano. "DSL White Paper". A Flowpoint Corporation White Paper ,1998.
http://www.flowpoint.com/tlc/whitepapers/flowpoint/wp_dslmk.html

50. "56/64 Kbps Leased Lines".
http://www.mot.com/MIMS/ISG/projects/technology/ll.html.