UNIT 9 CONVERGENCE, INTERNET TELEPHONY AND VPN

Structure

9.1 INTRODUCTION

In this unit we will discuss the concepts of convergence, Internet telephone and VPN. Convergence is a term that has a different meaning for every platform. It covers a wide area of applications. Every field of application is on the way to convergence because of advancement of technology. For example, mechanical convergence is quite different from communication convergence. In simple words, convergence means taking advantage of a unified way to do an operation which is being done through multiple ways, so that effort will be less and the same effect or output is obtained. The VPN market is on the verge of explosive growth. A virtual private network (VPN) broadly defined, is a temporary, secure connection over a public network, usually the Internet. The idea of the VPN is to give the company the same capabilities at a much lower cost by using the shared public infrastructure rather than a private one. Internet telephony is the latest technology to dazzle both the datacom and telecom industries. Many of those outside those sectors are now wondering what exactly this technology is, how it works, and whether it has yet matured into a commercially viable communications tool.

9.2 OBJECTIVES

After studying this unit, you should be able to:

- explain what is Communication Convergence;
- describe what is Virtual Private Network (VPN) its working and Architecture;
- enlist protocols that have emerged for building VPN's; and
- describe what is Internet telephony, and explain the benefits, approval issues and equipments required for Internet telephony.

9.3 WHAT IS CONVERGENCE?

Here a basic concept has been given for digital convergence or Communication Convergence. The concept that all modern information technologies, currently based on very disparate technological paradigms and systems, are becoming digital in nature. At present a person might receive information by telephone, television, radio, newspaper and print. In future these different information delivery systems may be replaced by a unified system based wholly on digital technology, with all its advantages (e.g.: ease of access, flexibility) and disadvantages (e.g.: increased centralize). Communication sector comprises broadcasting, telecom and information technology.

Malaysia is the first country in world to bring the communication convergence through legislation.

9.3.1 The Communication Convergence Bill 2001

The Communication Convergence Bill 2001 was the second in the world. This Bill will replace 5 existing laws .These are The Indian Telegraph Act-1885, Cable TV Networks Act 1995, Indian Wireless Telegraphy Act-1933, The Telegraph Wires (Unlawful Possession) Act 1950 and the Telecom Regulatory Authority of India Act 1997.

The Bill seeks to achieve 4 main purposes-

- The development of national infrastructure for an information based society, and to enable access thereto;
- To provide a choice of services to the people with a view to promoting plurality of news, views and information;
- To establish a regulatory framework for carriage and content of communication;
- To establish a single regulatory and licensing authority with defined powers, procedures and functions and an Appellate Tribunal.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

What are the laws which may be replaced by Convergence Bill if it is passed?

....

....

....

....

....

....

....

9.4 VIRTUAL PRIVATE NETWORK

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

Though the term is relatively new, everyone from telcos to operating system vendors, to firewall suppliers and router companies has rushed to offer some type of VPN capability. Why? This is because VPNs make sense, and as a result, the market is expected to reach at least several billion by the year 2006.

By leveraging the Internet, VPNs offer significant cost savings, greater flexibility, and easier management relative to traditional internetworking methods, such as leased lines and dial-up remote access.

However, choosing an appropriate solution from the recent flood of VPN offerings can be a difficult task for information technology managers who have no spare time. Each solution presents varying levels of security, performance and usability, and each has its benefits and drawbacks.

At minimum, a VPN should encrypt data over a dynamic connection on a public network to protect the information from being revealed if intercepted. Beyond that basic function, VPN features customarily include tools for authentication, and a limited number provide integrated access control and authorization capabilities. In addition to enumerating the possible VPN components, this white paper outlines the predominated VPN technologies and interprets the nuances of different VPN approaches so IS professionals can better decide how to secure their corporate communication.

9.5 DEFINING THE DIFFERENT ASPECTS OF VPNs

Before online business can truly reach its potential, corporations must feel comfortable using the Internet as the backbone for secure communication. VPNs are the first real step towards that end. When implemented correctly, they protect networks from viruses, snoops, corporate spies, and any other known threat that results from mistakes in configuration, poorly implemented access controls, lack of system management, weak authentication, and "back-door" entry points to the network.

The three fundamental features that define virtual private networking are encryption, authentication, and access control. While strong authentication and encryption are critical components of the VPN, they are relatively simple to deploy and verify. Access control, on the other hand, is relatively complex because its deployment is tied intimately to every other security tool. Roughly speaking, the security of a VPN is a function of how tightly authentication, encryption, and access control are connected. If one component is lacking, the VPN will be lacking.

Where a company might use a guarded gate in the physical world to block all unauthorized visitors, a firewall might be used in the analogous VPN world. With emerging VPN technologies and solutions, companies can verify someone's identity with strong authentication technologies like token cards, digital certificates, or even fingerprints. Once identified, users are granted access to resources according to very detailed profiles based on identity and often a user's role within a larger group. VPNs are also beginning to provide tools to monitor a user's activity once inside the corporate network. Prior to even connecting to the Internet, corporations should develop a security policy that clearly identifies who can have access to what resources, leaving room for growth and change. And before implementing a VPN, corporations should evaluate their current security paradigm to determine what equipment can be leveraged for a VPN.

A comprehensive solution might incorporate a firewall, router, proxy server, VPN software or hardware, or all of the above.

Are professionals can effectively use VPNs to address three predominant internetworking scenarios?

1) Between a corporation and its branch offices, which will be referred to as an "intranet VPN"?

2) Between a corporation and its remote or travelling employees, which will be referred to in this paper as a "remote access VPN"?

3) And between a corporation and its business associations, such as partners, customers, suppliers, and investors, which will be referred to as an "extranet VPN".

9.5.1 Intranet VPNs

Intranets are defined here as semi-permanent WAN connections over a public network to a branch office. These types of LAN-to-LAN connections are assumed to carry the least security risk because corporations generally trust their branch offices and view them as extensions of the corporate network.

In this case, the corporation generally controls both the source and destination nodes. IS administrators should ask whether or not this assumption holds true for their company.

General Case

When the two endpoints of a data channel are relatively trusted, a company can comfortably opt for a VPN solution that focuses on performance over security, which is limited to the strength of the encryption and authentication methods between the two routers. High volumes of data are often exchanged between LANs on an intranet VPN, so the premium is wisely placed on speed and smooth interoperability.

The LANs that are connected by centralized corporate databases or other enterprise-wide computing resources should appear to be part of the same corporate network. Many of the firewall, router, and frame relay vendors, as well as some of the ISPs, are offering solutions that adequately secure intranet VPNs while transferring data quickly and reliably.

Highly Secure Case

Security threats often come from within an organization. In fact, according to a study issued jointly by the FBI and the Computer Security Institute, almost half of all computer break-ins occur within a company.

If a company is concerned about proprietary information being leaked by employees, whether intentionally or accidentally, or if a company routinely applies different levels of trust to branch offices or individuals, then it should consider investing in a VPN solution that can control the information flow on an authenticated, user-specific policy level rather than on a trusted subnet basis. IT managers should look closely at solutions that provide reasonable ways to implement and manage these advanced role-based policies.

9.5.2 Remote Access VPNs

Corporations are just now beginning to realise the advantages the Internet offers over traditional direct dial-up remote access. Many corporations, burdened by the effort of maintaining large modem pools and the expense associated with long distance charges, are finding that using the Internet as a backbone for remote access is much more affordable and easier to implement and maintain than traditional solutions.

In any remote access VPN scenario, usability is an important criterion. Most security flaws are attributed to configuration errors, so the easier the system is to manage, the less likely is the chance for oversight. On the client side, simplicity is critical because many travelling employees and telecommuters either lack the technical proficiency or the access to technical resources for troubleshooting. Clients should not have to manually build a VPN tunnel, “manually” meaning having to launch VPN software each time the user wants to establish a secure communication channel. Instead, the VPN software should launch automatically at start-up and run transparently in the background. On the server side, centralized and easy management is essential because monitoring large numbers of users and adding and removing users on a regular basis can quickly become chaotic and can create a security risk.

A directed VPN uses IP to establish directional control of information across a VPN. It also offers capabilities above and beyond typical tunneling solutions, including the ability for IS managers to specify access on the basis of sources, destinations, applications, encryption/authentication and other filtering profiles. Directed VPNs also provide data encryption and user-based authentication. In contrast, VPNs based on tunneling are not as secure or do not offer as many features.

General Case

With most remote access VPNs, it is assumed that a corporation trusts the person at the other end of the link, which is typically a travelling or remote salesperson. Rather than worrying that the employee might do damage to the network or steal proprietary formation, the company is probably more concerned with the unknown element between the two end points. These companies will generally assume a "transparent access" policy, best described as: "The remote employee should have unfettered access to all resources that would be available to them if they were sitting at their desk at corporate headquarters."

The priority, therefore, becomes encrypting the data in transit so that only the intended recipient can decipher it. Most VPNs can meet this basic security requirement, so evaluators should consider additional criteria, such as the strength of the encryption cipher and the authentication method for providing additional security.

Highly Secure Case

The industries that are the most leery of any kind of security risk, such as the financial, health, and government sectors, are paradoxically the earliest adopters of VPN technologies, which have the perception of being less secure than traditional means of networking. In reality, the best VPN technologies are much more secure than most leased lines and dial-up remote access, because highly secure VPNs encrypt all data and generally provide very detailed user profiles for access control. Highly secure remote access solutions are deployed by sophisticated IT shops with a strong understanding of the security risks inherent in any network communication. These shops generally adopt a "controlled access" policy for their remote users. This is best described by the following policy statement: "The remote employee should have tightly controlled access to specific resources on the network according to the requirements of their job function."

These companies deploy policy-driven VPNs to provide highly secure remote access over the public networks. Secure policy-driven VPNs authenticate individual users, not just IP addresses, so that a corporation knows which employee is trying to gain access to the network. This can be accomplished through common passwords digital certificates, token cards, smart cards, or biometrics, such as fingerprint or iris scanning. Once an employee has authenticated to the corporate VPN server, he or she is granted a certain level of access depending on his or her profile, which is usually set up by a network administrator to match the corporate security policy and enforced by a sophisticated system of data stream filters and access control parameters. This three-tier system is essential for companies that allow their employees to access mission-critical information, particularly when those employees are not entirely trusted.

Any time a company wants to provide varying levels of access so that different resources can be made available to different employees when appropriate, or when a company wants to prevent "back-door" holes into the network, which is common in some systems, and then a more robust VPN solution is recommended. In other words, a highly secure VPN should be able to intercept network traffic destined for a particular host, add the required encryption, identify individual users, and apply restrictions and filter content accordingly.

9.5.3 Extranet VPNs

Unlike intranets that are relatively isolated, extranets are intended to reach partners, customers, and suppliers, as well as remote employees. Securing that wide area network requires diligence and the right tools. An extranet VPN needs to be able to provide a hierarchy of security, with access to the most sensitive data being nested under the tightest security control. It should secure all applications, including TCP and UDP applications, such as Real Audio, FTP, etc.; corporate vertical applications, such as SAP, BAAN, People Soft, Oracle, etc.; and "homegrown" applications, such as Java, Active X, Visual Basic, etc. Because most corporate computing environments are heterogeneous with many legacy systems, a sound VPN solution should be extremely versatile and interoperable with multiple platforms, protocols, and authentication and encryption methods.

General vs Highly Secure Case

The main objective of an extranet or business-to-business VPN is to ensure that mission-critical data arrive intact and in the proper hands without ever exposing protected resources to potential threats, so companies should only consider implementing the most secure breed of VPNs.

The security elements of a VPN can be prioritized differently, but with an extranet VPN, all the fundamental pieces 3/4 encryption, authentication, and access control 3/4 should be integrated tightly with some type of perimeter security. Usually this means a company will place a VPN proxy server behind an impenetrable firewall that blocks all unauthenticated traffic. Any traffic that is allowed in is then funneled through a common portal directly to the VPN server, which filters traffic according to company policy. It is essential for the connection between the firewall and the VPN to be strong and reliable, and the client software should be as transparent as possible.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

What is the difference between Intranet and Extranet VPNs?

....

....

....

....

....

9.6 VPN ARCHITECTURE

The most secure VPNs are built around a "directed" architecture, as opposed to a bi-directional "tunneled" method. Directed VPNs transmit encrypted information at a higher level in the networking protocol stack than tunneled VPNs, and security and control increase as functionality moves up the network hierarchy. Directed VPNs act as proxy servers, which means they do not open any direct connections into corporate networks, preventing IP addresses from being "spoofed", or mapped.

Tunneling hides information in IP packets at the packet level, exposing them more easily to attack. Because all data is proxied in directed VPNs, administrators can tell at a glance who has been trying to gain access to the network and how often. Unlike tunneled VPNs, directed VPNs protect connected networks from each other's security flaws. Directed VPNs do not assume a two-way trusted relationship between connecting parties. If security is breached in the directed model, only the attacked network is exposed, not the linked networks. In the tunneled model, when one network is attacked, each successive network is susceptible to the same attacker. In the directed model, each company's IS managers can set their own access privileges and be confident they are not exposing their networks to unknown security problems.

Tunneled VPNs, as the name implies, open tunnels within the Internet and secure information travelling through them with basic packet filtering. This approach gives participating companies weakly secured access to each other's networks, with no way to fine-tune access control. These types of solutions often mistakenly start with the faulty assumption that there should be peer-to-peer trust among companies connected by VPNs. When trading partners or customers are involved, that is rarely the reality.

When companies conduct multi-faceted business transactions over public networks, simple encrypted tunnels will not suffice. Online business, or electronic commerce, is not restricted to credit card transactions. It involves complex negotiations and collaboration on projects. When vital, confidential information is involved, IS professionals cannot risk compromising any portion of the network. An extranet VPN should use the highest encryption available, which is currently 128 bits, except when restricted by exportation laws. In addition, the VPN should support multiple authentication and encryption methods since business partners, suppliers, and customers are likely to have varying network infrastructures and platforms. In a true business-to-business scenario, IS managers should look for a VPN that filters access to resources based on as many parameters as possible, including source, destination, application usage, type of encryption and authentication used, and individual, group, and subnet identity. Administrators should be able to identify individual users, not just IP addresses, either through passwords, token cards, smart cards, or any other method of authentication. Passwords are usually sufficient for casual office use, but they are not considered as secure as token or smart cards. Employees are often careless with their passwords, and they rarely change their codes, whereas token and smart cards change the pass code on a regular basis, often as frequently as every 60 seconds.

Once authenticated, administrators should be able to route authorized traffic to protected resources without jeopardizing network security. The access control is what ultimately distinguishes the level of security among VPN solutions. Without being able to control exactly who has access to each resource on a network, a VPN is virtually useless beyond the network's perimeter. Once authenticated, a user should not have carte blanche to the network. Rather, specific permissions should be granted to each user in order to retain the most control over every resource.

Security should increase, not lessen, as a user moves inward toward the most sensitive data. By utilizing strong encryption, authentication, and access control methods, all working seamlessly within a VPN solution, companies can seal their corporate networks from almost any security breach.

9.7 UNDERSTANDING VPN PROTOCOLS

The VPN security market is young, and standards are still evolving, but a handful of protocols have emerged as the leading choices for building VPNs. An IS manager should not have to base his or her purchasing decision on the technology used, but understanding the benefits of each protocol may help clarify the related strengths and weaknesses of different VPN end products. Although there are many possible security approaches for creating a VPN, the following protocols show the most promise for lasting in the market, whether for the quality of their design or their financial backing.

For secure VPNs, the technologies that VPNC supports are

- IPsec with encryption
- L2TP inside of IPsec
- SSL with encryption

For trusted VPNs, the technologies that VPNC supports are:

- MPLS with constrained distribution of routing information through BGP ("layer 3 VPNs")
- Transport of layer 2 frames over MPLS ("layer 2 VPNs")

IPsec is the most dominant protocol for secure VPNs. SSL gateways for remote-access users are also popular for secure VPNs. L2TP running under IPsec has a much smaller but significant deployment. For trusted VPNs, the market is split on the two MPLS-based protocols. Companies want to do their own routing the to use layer 2 VPNs; companies that want to outsource their routing tend to use layer 3 VPNs.

The various VPN protocols are defined by a large number of standards and recommendations that are codified by the Internet Engineering Task Force (IETF). There are many flavours of IETF standards, recommendations, statements of common practice, and so on. Some of the protocols used in IPsec are full IETF standards; however, the others are often useful and stable enough to be treated as standard by people writing IPsec software. Neither of the trusted VPN technologies are IETF standards yet, although there is a great deal of work being done on them to get them to become standards.

9.7.1 SOCKS v5

SOCKS v5 was originally approved by the IETF as a standard protocol for authenticated firewall traversal, and, when combined with SSL, it provides the foundation for building highly secure VPNs that are compatible with any firewall.

STOCKS 5, which follows a proxy server model and works at the TCP socket level. It requires a SOCKS 5 server and appropriate software in order to work. The SOCKS 5 client intercepts a request for service, and checks it against a security database. If the request is granted, the server establishes an authenticated session with the client, acting as a proxy. This allows network managers to apply specific controls and proxied traffic, and specify which applications can cross the firewall into the Internet.

It is most appropriately applied to VPNs that require the highest degree of security, since its strength is access control. SOCKS v5 was developed in 1990 by David Koblas and championed through the IETF by NEC Systems Laboratory. It is currently the only IETF-approved standard being used to create VPNs. Though it is not as well known as some of the other protocols, it has received widespread support from industry leaders such as Microsoft, Netscape, and IBM. SOCKS v5 is the protocol used in Aventail's policy-based VPN solution.

Advantages

SOCKS v5 controls the flow of data at the session, or circuit, layer, which maps approximately to layer five of the OSI networking model. Because of where it functions in the OSI model, SOCKS v5 provides far more detailed access control than protocols operating at the lower layers, which permit or reject packets based solely on source and destination IP addresses. SOCKS v5 establishes a virtual circuit between a client and a host on a session-by-session basis and provides monitoring and strong access control based on user authentication without the need to reconfigure each new application. Because SOCKS v5 and SSL operate at the session layer, they have the unique ability to interoperate on top of IPv4, IPSec, PPTP, L2TP, or any other lower-layer VPN protocol. In addition, SOCKS v5 and SSL have more information about the applications running above them than do lower-layer protocols, so they can provide very sophisticated methods of securing traffic.

SOCKS v5 stands out as the only VPN approach to use a directed architecture, which essentially protects destination computers by proxying traffic between source and destination computers. When used in conjunction with a firewall, data packets are passed through a single port in the firewall (port 1080 by default) to the proxy server, which then filters what is sent forward to a destination computer. This prevents administrators from having to open multiple holes in their firewall for different applications. For additional security, the VPN proxy server hides the address structure of the network, making it more difficult for confidential data to be cracked. Another design advantage of SOCKS v5 is that the client is non-intrusive. It runs transparently on the user's desktop and does not interfere with networking transport components, as do lower-layer protocols, which often replace the Winsock DLL, TCP/IP stack, and low-level drivers, interfering with desktop applications. SOCKS v5 is also highly flexible. It works easily with multiple security technologies and platforms, which is critical for IS professionals managing heterogeneous computing environments. It offers modular plug-in support for many authentication, encryption, and key management methods, providing IS managers the freedom to adopt the best technologies for their needs. Plug-and-play capabilities include access control tools, protocol filtering, content filtering, traffic monitoring, reporting, and administration applications. SOCKS v5 can filter data streams and applications, including Java applets and ActiveX controls, according to very detailed specifications.

Disadvantages

Because SOCKS v5 adds a layer of security by proxying traffic, its performance generally is slightly slower than that of lower-layer protocols, depending on how the VPN is implemented. Though it is more secure than solutions located at the lower network or transport layers, the extra security requires more sophisticated policy management than at the lower layers. Also, client software is required to build a connection through the firewall to transmit all TCP/IP data through the proxy server.

9.7.2 PPTP/L2TP

One of the most widely known VPN security choices is Point-to-Point Tunneling Protocol (PPTP) from Microsoft. It is embedded in Microsoft's Windows NT v4.0 operating system and is used with Microsoft's Routing and Remote Access Service. It sits at the datalink layer, which maps approximately to layer two of the OSI model. It encapsulates PPP with IP packets and uses simple packet filters and the Microsoft Domain networking controls to provide access control. PPTP and its successor, L2TP, are seen as tools to extend the current PPP dial-up infrastructure supported by Microsoft, most ISPs, and the remote access hardware vendors. Layer Two Transport Protocol (L2TP) has evolved from the combination of Microsoft's PPTP protocol and Cisco Systems' Layer 2 Forwarding (L2F). It supports multiple, simultaneous tunnels for a single client and is targeted at the telco and ISP markets. With L2TP, the end user dials up a local ISP POP without encryption, and the ISP, acting as an agent for the end user, creates an encrypted tunnel back into the secure destination.

Advantages

Are professionals running Microsoft-centric shops will find PPTP and L2TP readymade to work with their systems? Because they use packet-filtering that makes use of existing network routers, they are typically less complicated to implement, and they are transparent to end users.

In typical Microsoft fashion, PPTP is free. Microsoft includes it as a component of its RAS and router software, formerly known as Steelhead. When affordability in a Microsoft-only environment is an issue, PPTP is a viable solution. L2TP will likely follow the same path and be included in upcoming versions of NT servers and Windows 32-bit desktop clients.

Most VPNs secure TCP/IP traffic, but PPTP and L2TP support additional networking protocols such as Novell's IPX, NetBEUI, and AppleTalk. They also support flow control, which keeps traffic from overwhelming clients and servers. They enhance network.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

State whether True or False

1) Tunneled VPN close tunnels within the internet and secure information and secure information in travelling through them with basic packet filtering?

....

2) Socks v5 was developed by David Koblas in 1990 and championed through the IETF by NEC Systems Laboratory.

....

3) PPTP is one of VPN security choices and embedded in Microsoft's window NT v 4.0 operating system.

....

9.8 WHAT IS INTERNET TELEPHONY

The concept behind Internet telephony (also known as Voice over IP (VOIP) or IP telephony) is a simple one: the transfer of voice messages using Internet protocol (IP) networks. This technology enables standard data packets to transmit multimedia information such as voice or video over the Internet or any other IP-based local- or wide-area network. It draws on open standards and recommendations generated by international groups such as the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU). All suppliers of Internet telephony products meet these standards. At present internet telephony has already been legalized in India. It is limited to legalizing PC to PC phone calls to India. Again PC to landline phones is still not permissible in India under the government of India's guidelines.

9.8.1 Benefits of Internet Telephony

Standing to benefit most from Internet telephony, obviously, are companies that make significant numbers of long-distance calls — for example, large organizations with offices around the world. With Internet telephony, the customer pays only for the call to the Internet gateway hosted by its local Internet service provider or its own company intranet. Thus all telephone calls are billed at the local-call rate, dramatically reducing long-distance charges. Moreover, choosing an IP network enables a company to use a single communication medium rather than having to maintain separate systems for voice and data communications — again lowering costs and increasing efficiency.

In effect, then, Internet telephony offers a single method for communications, combining voice, video, and data traffic by adopting IP as a common protocol and merging up to three different network structures in one comprehensive medium.

9.8.2 Bandwidth Growth

One reason for the increasing acceptance of Internet telephony is the continuous expansion of bandwidth within LANs, as Fast-Ethernet and switching are gradually being replaced by the far more efficient asynchronous transfer mode (ATM) and Gigabit Ethernet. The resultant oversupply of bandwidth (especially among local networks) has in turn created a demand for new applications such as Internet telephony. Standards now being developed will guarantee a certain level of service in these IP-based networks, since bodies such as IETF have recognised that few or no standards adequately addressed the transmission of voice or video over the Internet. New technologies such as RSVP (resource reservation protocol) and RTP (real-time transport protocol) have therefore been developed to enable real-time operation on today's existing IP networks. More than anything else, however, it is the sheer improvement in voice quality that has allowed the Internet telephony technology to compete successfully with traditional telephone companies.

9.9 APPROVAL ISSUE AND INTERNET TELEPHONY

On the approval front, there are a number of considerations that must be addressed regarding Internet telephony, including connection scenarios, technical requirements, and country-by-country regulatory differences.

The three basic types of connection in Internet telephony are telephone to telephone, telephone to computer, and computer to computer. At present, no specific country approvals apply specifically to Internet telephony, although formal approval is required for any equipment that connects directly to a public network. Such connections comprise standard telephony connections to the public switched telephone network (PSTN) via either approved telephones or modems; connections via internal or external ISDN adapters (BRI or PRI); connections via "nailed-up" circuits such as G.703s or X.21s; and connections via least-cost routers or PBX systems.

9.10 TYPES OF EQUIPMENT REQUIRED FOR INTERNET TELEPHONY

Exactly what kinds of hardware and software will be required for Internet telephony? For each connection type, several components are necessary within a given telephony network. On one side there are terminals for Internet telephony, much like traditional telephones but with an Ethernet rather than an analog or digital connection to the telephone network; alternatively, there are special PC programs that act as Internet telephones (e.g. Microsoft NetMeeting and Vocal Tec Internet Phone). Gateways are needed at the interface between the traditional telephone network and the IP-based network to map the different signalling and transmission procedures; also necessary are certain central components such as directory services to map and find multiple terminal addresses (both IP and e-mail addresses and telephone numbers), as well as servers for authentication and billing. These devices typify the range of products now being developed for Internet telephony.

9.11 COMMERCIAL VIABILITY

Until very recently, Internet telephony has been widely accused of suffering from poor voice quality and long time delays in transmission. These problems have now been largely eliminated, making Internet telephony's voice quality competitive with that offered by its rival PSTN, and reducing delays to an acceptable 250 milliseconds or less. Unlike traditional PBX telephony, Internet telephony cannot guarantee a 100% connection rate, but its reliability is sufficient to allow companies to save huge sums of money over a relatively short period. Financial controllers of large companies such as PepsiCo have already been persuaded on purely economic grounds to implement IP telephony across their organizations. Industry reports endorse the claims that Internet telephony is here to stay; Forrester Research even predicts that by the year 2004, U.S. telephone companies alone will have lost some $3 billion to Internet telephony. Little wonder, then, that traditional carriers and telcos are beginning to feel the pressure.

9.12 THE H.323 STANDARD: AN INTRODUCTION

H.323 is an umbrella recommendation drafted by the ITU to define multimedia communications in LANs that do not provide a guaranteed level of service quality. Now dominating the world of data processing, such networks include packet-oriented TCP/IP and IPX networks over Ethernet, Fast-Ethernet, or token-ring-network topologies. H.323 and other similar standards promise to be extremely important in the development and provision of new applications that will work together network wide.

Network Components

H.323 contains technical requirements for audio and video transmission within LANs. It covers four main components: terminals, gateways, gatekeepers, and multipoint control units.

Communication

H.323 communication is defined as a combination of audio, video, data, and control information. The standard's mandatory components are transmission of audio, connection control according to Q.931, communication with the gatekeeper over the RAS protocol, and use of the H.245 signaling protocol; the rest of the text, including coverage of the ability to transmit video and data, is optional.

IP Networks and Multimedia

H.323 also covers protected and unprotected connections. Control and data information requires a protected transmission to prevent packets from being lost or not received in the right order. For instance, with video, if a packet arrives late, it loses its meaning and may not be inserted correctly in the clip being played. For this reason, unprotected connections are used only for audio and video transmissions, which are more efficient. In IP-based networks, the connection-oriented TCP protocol, used for protected connections, guarantees an error-free transmission in the right order but causes delays and has a lower throughput. H.323 references TCP connections for the signalling protocol (H.245), for data transmission (T.120), and for connection control (Q.931).

Please answer the following Self Assessment Question.

Self Assessment Question 4 *Spend 1 Min.*

H.323 communication is defined as a combination of audio, video, __________ ______________________________, and ______________________.

Let us now summarize the points covered in this unit.

9.13 SUMMARY

- Convergence is a method of doing many things in a single way. As far as our course is concerned, Communication convergence is most important.
- Communication sector comprises broadcasting, telecom and information technology.
- Malaysia is the first country to introduce Communication Convergence bill.
- A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.
- The three fundamental features that define virtual private networking are encryption, authentication, and access control.
- VPNs can be used by is professionals via Intranet VPN, remote access VPN and extranet VPN.
- Socks v5, PPTP (Point to Point Tunneling Protocol/ L2TPP Layer Two Transport Protocol are VPN protocols.

- A corporation and its branch offices, is referred to as an "intranet VPN".
- The concept behind Internet telephony (also known as Voice over IP or IP telephony) is the transfer of voice messages using Internet protocol (IP) networks.
- At present, Internet telephony is legal in India and fee has been reduced. It is limited to legalizing PC to PC calls in India.
- PC to landlines telephony is still not permissible in India under the Government of India Guidelines.

9.14 TERMINAL QUESTIONS

1) What do you mean by Convergence? Describe Communication convergence with the help of a example?

2) Why are VPNs are still expensive? What types of VPNs are advisable for Extranet Based?

3) Describe VoIP? What techniques are used here? What will be the impact on the economy if PC to land phones telephony? Is allowed?

9.15 ANSWERS AND HINTS

Self Assessment Questions

1) The Communication Convergence Bill would replace 5 existing laws. The Indian Telegraph Act-1885, Cable TV Networks Act 1995, Indian Wireless Telegraphy Act-1933, The Telegraph Wires (Unlawful Possession) Act 1950 and the Telecom Regulatory Authority of India Act 1997.

2) Intranet VPNs are semi-permanent WAN connections over a public network to a branch office and are relatively isolated while extranet VPNs are intended to reach partners, customers, suppliers and also remote employees.

3) (1) False, (2) True, (3) True

4) data and control information

Terminal Questions

1) Refer to section 9.2 of the unit.

2) Refer to section 9.4, 9.5, 9.6 of the unit.

3) Refer to section 9.7, 9.10 of the unit.

Apart from above, please follow other reference books for in depth knowledge.

9.16 REFERENCES AND SUGGESTED READINGS

1. Behrouz A. Forouzan. Data communication & Networking. 2nd ed. TATA McGraw-HILL, 2003.

2. Dr. M. Jain and Satish Jain. Data communication and Networking. 1st ed .BPB, 2004.