UNIT 2 NETWORK TECHNOLOGY

Structure

2.0 OBJECTIVES

After studying this unit you will be able to:

- understand how communication takes place between two computers;
- know the working of Internet Technology;
- become aware of security related information in networks; and
- get an idea of the latest trends in network technology.

2.1 INTRODUCTION

There are thousands of computer networks operating in the world. The Internet is the biggest of them all. There are millions of computers connected to the Internet the world over. To understand how the computers are connected in a network, it is important to understand the computer communication architecture.

2.2 OSI MODEL

The Open System Interconnection (OSI) model was developed by the International Organisation for Standardisation (ISO) as a model for computer communication architecture. It consists of seven layers as depicted in Figure 1.

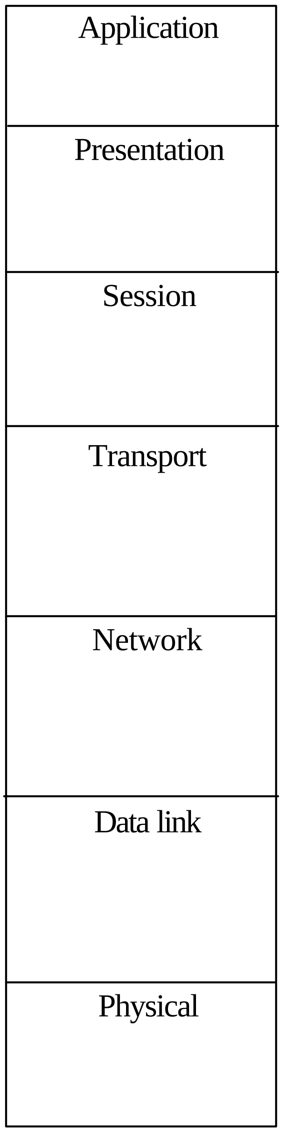


Figure 1: OSI Reference Model

2.2.1 Physical Layer: Bits

The Physical layer provides the mechanical and electrical connections to the network. In other words, it sends bits down a wire. The physical medium can be Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, Repeaters, Hubs FDDI, ATM, SONET/SDH etc.

2.2.1.1 Repeaters

A Repeater is a physical layer device used to interconnect the media segments of an extended network. Repeaters receive signals from one network segment and amplify, retime, and retransmit those signals to another network segment. These actions prevent signal deterioration caused by long cable lengths and large number of connected devices. Repeaters are incapable of performing complex filtering and other traffic processing. In addition, all electrical signals, including electrical disturbances and other errors, are repeated and amplified.

2.2.1.2 Hubs

A Hub is a physical layer device that connects multiple computers each via a dedicated cable. Electrical interconnections are established inside the hub. Hubs are used to create physical star network while maintaining the logical bus or ring configuration of the LAN. In some respects Hub also function like a repeater. Generally 8, 16 and 24 ports hub are available in the market.

2.2.2 Data Link Layer: Frames

The Data Link Layer splits data into frames for sending on the physical layer and receives acknowledgement frames. It performs error checking and retransmits frames not received correctly. It provides an error-free virtual channel to the Network Layer. The Data Link Layer is split into an upper sublayer, Logical Link Control (LLC), and a lower sub-layer, Media Access Control (MAC).

2.2.2.1 Bridges

Bridges connect different types of networks (token ring, Ethernet, etc.), filter network traffic based on MAC address, and remove errors from the network. Use to connect different types of networks.

2.2.2.2 Switches

Switches, also known as Multiport Bridges, transfer data between different ports based on the destination addresses. Each segment or port connection is its own collision domain, but all ports are in the same broadcast domain. Switches can be used to connect multiple ports to the same destination (i.e multiple uplink ports), but only one port can be active at a time. Historically, this is a hardware Layer 2 device and typically operates in one of three modes:

2.2.2.2.1 Store and Forward

This mode copies the entire frame into memory, computes the Cyclic Redundancy Check (CRC) for errors, and then looks up the destination MAC address and forwards the frame. This is slow but offers the best solution for error without affecting the entire backbone in transmission.

2.2.2.2.2 Cut-through

This mode reads the destination address of the frame and forwards to the port connected to that destination MAC address before the entire frame is seen. This is fast but provides very little error correction and will propagate errors from one collision domain to the next.

2.2.2.2.3 Modified Cut-through

This mode reads the first 64 bytes of the frame and then forwards the frame to a port based on the MAC destination address. This is fast and efficient in error correction.

There are two general types of Layer 2 switches.

Workgroup Switches that create dedicated bandwidth by providing private LAN segments for each end device (e.g., workstation or server), effectively replacing shared – media wiring hubs.

Segment switches, on the other hand, are optimised to bridge traffic between multiuser shared-media LAN segments, or between backbone LAN trunks; each port must typically support large numbers of MAC addresses.

2.2.3 Network Layer

The Network layer determines the routing of packets of data from sender to receiver. Routes can be static or dynamic. The Network Layer provides sequencing and flow control of data, selects routes, and provides quality of service through error detection, recovery and notification. It also segments collision and broadcast domains. This is where a MAC or hardware address is translated into Internet Protocol (IP) addresses (or other routable protocol addresses, such as IPX or AppleTalk).

2.2.3.1 Router

A router is a network-layer device (layer 3 under the OSI model) that connect networks and uses matrices to determine the optimal path along which the network traffic should be forwarded. They are occasionally called gateways.

Routers enable the creation of mesh topologies – large, computer systems that feature a number of possible paths between any two points on the network. Operating at the network layer of the OSI model, router joins networks by examining the network layer protocols of each packet individually (using the network address).

Routed protocols are used between routers to direct user traffic such as IP or IPX.

The only job that routing protocols have is to maintain routing tables that are used between routers. Examples of routing protocols are RIP, OSPF, EIGRP, BGP etc.

These protocols provide a way of sharing route information with other routers for the purpose of updating and maintaining tables. These protocols don't send end-user data from network-routing protocols but only pass routing information between routers.

Router use two layers of addressing : data link layer addressing for communications within the LAN and network layer information for communications between LAN segments. The advantage of this type of hierarchical addressing scheme is a reduction in the size of routing tables in large networks.

Router provides network management capabilities such as load balancing, partitioning of the network, use statistics, communication priority, and troubleshooting tools that allow network managers to detect and correct problems even in a computer network.

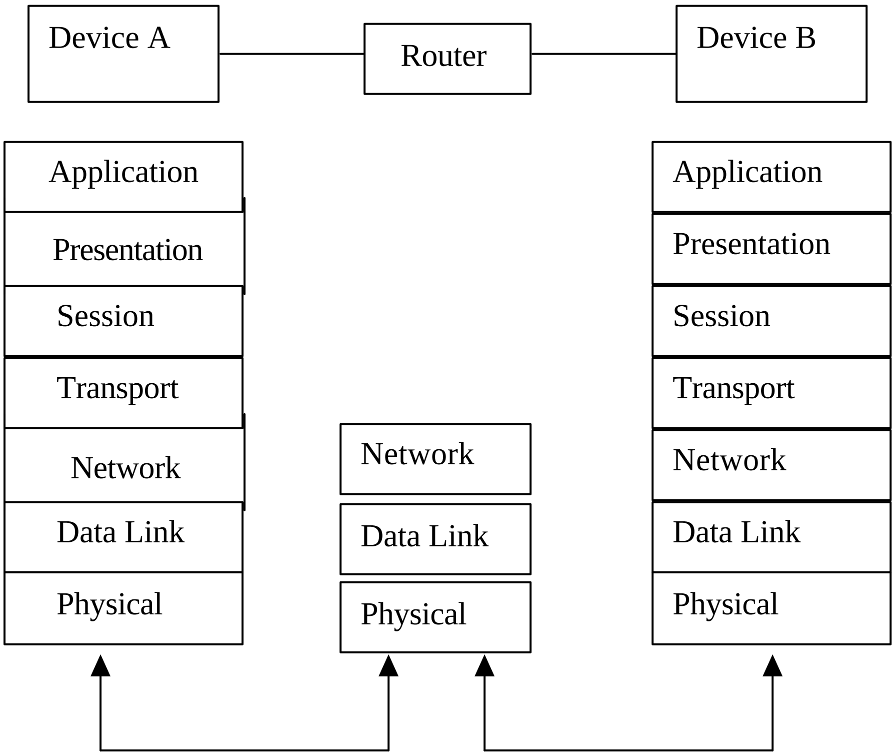


Figure 2

2.2.3.2 Routers Vs. Bridges

Bridges connect similar or identical networks. Bridging functions need to know whether the destination is on the local or a remote network. If it is on the local network, the packet is dropped at the bridge. If it is on a different network , then the bridge passes the packet over to its other network. The bridging functions do not need to know actual path information.

Bridges identify nodes using station addresses, which are usually set by the equipment manufacturer. When a bridge receives a packet, it examines source and destination station address and uses an address table to determine how to process the packet. The address table keeps track of which nodes are on which side (through which port) of the bridge and is kept up-to-date automatically.

Routers route the packet using the network layer addresses of the packets. These are assigned by a network administrator and always configured with a software.

Workgroup Switches create dedicated bandwidth by providing private LAN segments for each end device (e.g., workstation or server), effectively replacing shared – media wiring hubs.

Segment switches, on the other hand, are optimised to bridge traffic between multi-user shared-media LAN segments, or between backbone LAN trunks; each port must typically support large numbers of MAC addresses.

2.2.3.3 Switches (Layer 3)

Switches (Layer 3) are nothing more than wire-spread routers. They come in two basic modes.

2.2.3.3.1 Port Switches decide which physical port network traffic needs to go and direct the traffic appropriately. Each lane is actually a back plane segment on the switch. Because the switching is performed logically via logic circuits and at wire speed, port switches are easier and cheaper to implement than frame switches but give many of the same benefits.

2.2.3.3.2 Frame switches examine each Ethernet packet, determine which segment it came from and where it is going, and send it on its way. These are more expensive than port switches but add a significant performance boost to the network They are also known as Learning Switches.

2.2.4 Transport Layer: Segments

The transport layer is responsible for end-to-end communications, i.e, co-ordinating the communications between the network source and destination systems. This is the layer where TCP and User Data gram Protocol (UDP) reside in the IP protocol stack.

2.2.4.1 Switches (Layer 4)

A simple definition of Layer 4 switching is the ability to make forwarding decisions based not just on the MAC address (Layer 2 bridging) or source/destination IP addresses (Layer 3 routing), but on the TCP/UDP (Layer 4) application port number. This has prompted some of the vendors to describe Layer 4 switching as TCP/UDP switching.

At Layer 4, the TCP and UDP headers include port numbers that uniquely identify which application protocols (e.g., HTTP, SMTP, FTP etc.) are included with each packet. The end system uses the information to interpret the data contained within the packet; in particular the port numbers enable a receiving end computer system to determine the type of IP packet it has received and to hand it off to the appropriate higher layer software. The combination of the port number and a device's IP address is commonly referred to as a "socket".

Known Port Numbers

Application Protocols	**Port Number**
FTP	20 (data)
FTP	21 (control)
TELNET	23
SMTP	25
HTTP	80

Layer 4 Switches make the forwarding decisions based on the session and application – layer information and provide load balancing across multiple servers. Layer 4 switches determine (through different complex and weighted algorithms) the best server of a cluster to process a service request and bind the session to that server's IP address until the session is terminated.

2.2.4.1.1 A load balancer performs the following operations:

2.2.4.1.1.1 Traffic Identification : Traffic identification can be performed by DNS resolution, IP-based load balancing and HTTP redirect.

2.2.4.1.1.2 Application of mathematical algorithms for selecting server site.

Traffic forwarding to the chosen server site.

2.2.4.1.2 Load balancing methods

Round Robin Algorithm: This method treats all servers as equal regardless of the number of connections.

Weighted Round Robin : Each server in the application group is assigned a static weight based on some view of the capacity of each server.

Simple fewest connections: The incoming requests for new connections are directed to the server having minimum active connections.

Hashing: It is a mathematical algorithm, which manipulates IP addresses of client (source) and destination server so that a client's requests are always mapped onto the specified server only.

2.2.4.1.3 Layer 4 traffic forwarding

This is also known as application-aware/client-aware forwarding. Here, the load balance determines the application/content request and directs the traffic to the appropriate server.

2.2.5 Session

The sessions layer is the network dialogue controller. It establishes, maintains, and synchronizes the interaction between communicating devices. It also ensures that each session closes appropriately rather than shutting down abruptly and leaving the user hanging. The responsibilities of sessions layer are Session management, Synchronization, Dialogue control, Graceful close.

2.2.6 Presentation

The presentation layer ensures interoperability among communicating devices. It provides the necessary translation of different control codes, character sets, graphics characters, and so on to allow two devices to understand the same transmission in the same way. The responsibilities of the presentation layer are Translation, Encryption, Compression, Security validating passwords and login-codes, Common formats for representation of data.

2.2.7 Application

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as e-mail, remote file access and transfer, shared database management and other types of distributed information services.

The responsibility of the application layer are Network virtual terminal (A virtual terminal allows you to log on to remote host), File access, transfer and management, Directory services, FTP and SMTP (Electronic Mail)

In OSI terms, higher layer protocols (layer 4 and above) are independent of network architecture and are applicable to LANs and WANs. For LAN protocols, one is principally concerned with lower layers of OSI models.

2.3 INTERNET

The Internet is a network of networks, i.e., the Internet is an interconnection of independent physical networks such as LANs, WANs together by networking devices. A variety of universities, Government agencies and Computer firms are connected to the Internet which follows the TCP/IP protocol.

2.3.1 How Internet Works

An internet under TCP/IP operates like a single network connecting many computers of any size and type.

2.3.1.1 Transmission Control Protocol / Internet Protocol (TCP/IP)

TCP/IP is a set of protocols and programmes used to interconnect computer networks and to route traffic among different types of computers. The suitable shift in terminology reflects the fact that the communication functions are complex and are usually divided into independent layers, also called levels. TCP/IP has four software layers built on an underlying hardware layer. Figure 3 depicts the TCP/IP model. The protocol associated with each layer communicates with only the layers immediately above and below it, and assumes the support of underlying layers. In protocol families, lower layers are closer to the hardware and higher layers are closer to the user.

Layer	Name	Task
4	Application	Accesses the transport layer and sends and receives data.
3	Transport	Provides communication protocols between application programmes and the network layer
2	Network	Takes care of communication between software and hardware
1	Physical	Accepts and transmits data over the physical network

Figure 3 : TCP/IP Model

Transmission Control Protocol (TCP)

The Transmission Control Protocol, TCP works with IP to provide reliable delivery. It provides a means to ensure that various datagrams making up a message are reassembled in the correct order at their final destination and that any missing datagrams are resent until they are correctly received.

The primary purpose of TCP is to avoid loss, damage, duplication, delay or misordering of packets that can occur under IP. Also security provisions such as limiting user access to certain machines can be implemented through TCP.

Internet Protocol (IP)

The Internet Protocol (IP) defines a data delivery system wherein the sending and receiving machines are not necessarily directly connected. IP splits data into packet of a given size, which are then forwarded to the receiving machine via the network. These individual packet data (often called datagrams) are routed through different machines on the Internet to the destination network and ultimately to the receiving machine. Machines on the internet are referred to as hosts or nodes, and are defined by their IP addresses.

The Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed. IP is documented in RFC 791 and is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP has two primary responsibilities: providing connectionless, best-effort delivery of datagrams through an internetwork; and providing fragmentation and reassembly of datagrams to support data links with different maximum-transmission unit (MTU) sizes.

Exploring Addresses, Subnets

Each machine on a TCP/IP Internet has a 32 bit network address. The address scheme is controlled by the IP. The IP address inducts two separate parts. The network ID and the host machine ID. Internet addresses are assigned by Network Information Centre, California, USA.

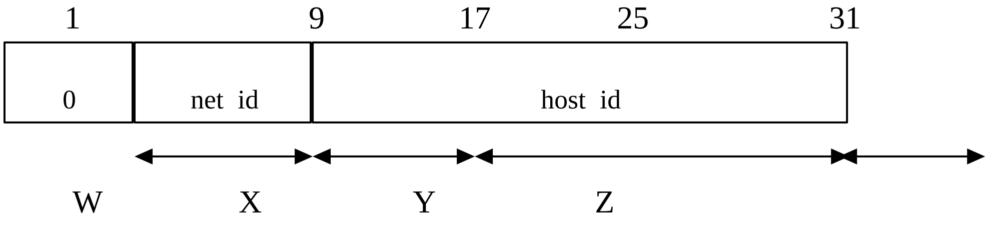
There are three classes of network addresses corresponding to small, medium and large networks identified as A, B, or C.

Class	Network Size Configuration
Class A	Allocates a 7 – bit network id and 24-bit host id
Class B	Allocates a 14 – bit network id and a 16 - bit host id
Class C	Allocates a 21-bit network id and 8 bit host id

Out of the 32 bit network address, the first bit of class A address is 0 (zero) to identify the address as Class A. Class B address begins with the digit 10, and Class C address begins with 11.

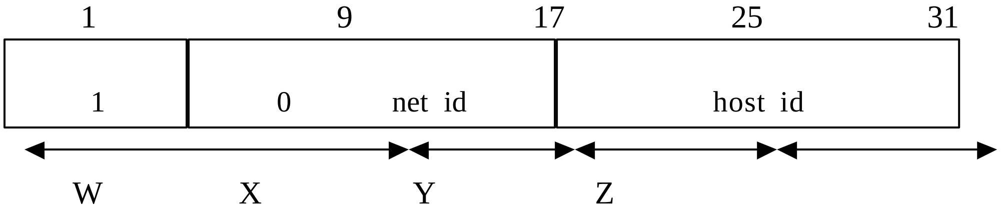
Class A Address Format

Bits

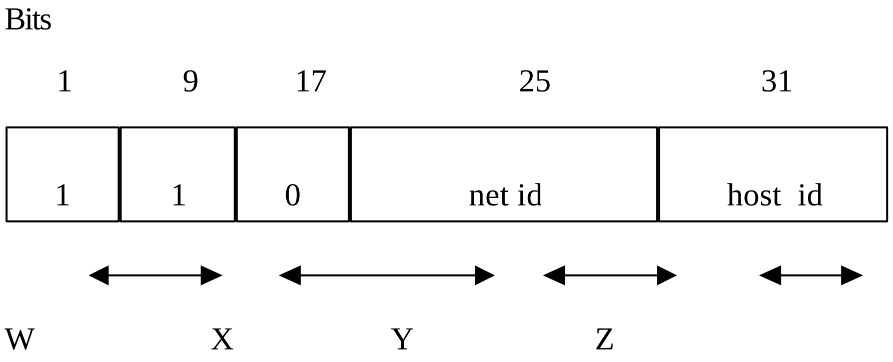


Class B Address Format

Bits



Class C Address Format



IP address can be expressed in several different forms. First is the decimal notation, which shows a decimal number with each byte separated by a dot, as in 202.141.130.66. Figure 4 summarises the relationship between the first octal of a given address and its network id and host id fields. It also identifies the total number of network ids and host ids for each address class that participates in the Internet addressing scheme. This example uses W.X.Y.Z.

Class	W Values*	Network id	Host id	Available Networks	Available Host Per Network
A	1-126	W	X, Y, Z	126	16,777,214
B	128-191	W, X	Y, Z	16,384	65, 534
C	192-223	W, X, Y	Z	2,097,151	254

Figure 4 : IP Addresses Classes

- *Address 127 is reserved for loopback testing and address 224 and above are reserved for special protocols. (Internet Group Management Protocol Multicast and Others) and so ca not be used as host address.*

With the pace at which the Internet is expanding today, the IP addresses are fast getting depleted. One of the reasons for the depletion of the address space is the way in which the different network classes have been designed and allocated. Let us see the problem first.

There are actually 2 billion addresses possible in IPv4 (IP version 4) , but the irony is that the address classes which were designed to optimize the usage of addresses have in turn contributed to its wastage.

No matter how large an organization is , a Class A network with over 16 million addresses is far too big, while a class C Network with just about 256 addresses might prove too small. So, a class B Network with 65,536 addresses might be the best among the three. But in reality, even a Class B address is too big for any organization.

In the early days of the Internet, when there were not too many networks around, even small organizations with about a 100 hosts or so, asked for, and were given Class B addresses leading to an addresses crunch. One of the more practical solutions has been the concept of Classless Inter Domain Routing (CIDR) which advocates the philosophy of grouping class C networks on a need basis and allocating them, rather than generously allocating Class B networks as was done earlier. Accordingly, an organization which might require about 1000 addresses is given a block of four

Class C networks, i.e, 1024 addresses, and not a full Class B address as was being done earlier. The proponents of CIDR also hit upon another idea of dividing the whole world into four zones, and give each of these four zones a chunk of the remaining Class C network. By doing this they were allocating each of the four zones about 32 million addresses each. The allocation of the Class C address is based on Geography.

- Address 194.0.0.0 to 195.255.255.255 for Europe
- Address 198.0.0.0 to 199.255.255.255 for N. America
- Address 200.0.0.0 to 201.255.255.255 for Central and S. America
- Address 202.0.0.0 to 203.255.255.255 for Asia and Pacific

Special Address / Reserved Address

It has been mentioned that there are several different addresses reserved for special purpose.

DOTTED DECIMAL ADDRESS	EXPLANATION
0.0.0.0	All hosts broadcast address for Sun Network.
Num.num.num.0	Identifies the entire network
Num.num.num.255	All hosts on the specified network (Broadcast address)
255.255.255.255	All hosts broadcast for current networks.

Subnet Masks

Subnet masks are 32 bit values that allow the recipient of IP packets to distinguish the network id portion of the IP address from the host id. Subnet mask comes into the picture, because the Router which acts as a gateway between two networks requires distinct IP address. The prime objectives of subnetting are to use scarce IP addresses optimally, to isolate networks and to simplify routing.

Subnet mask are created by assigning 1's to network id bits and 0's to host ID bits. The 32-bit value is then converted to dotted-decimal notation as shown in figure 5.

Address Class	Bits for Subnet Mask	Subnet Mask
Class A	11111111 00000000 00000000 00000000	255.0.0.0
Class B	11111111 11111111 00000000 00000000	255.255.0.0
Class C	11111111 11111111 11111111 00000000	255.255.255.0

Figure 5 : Default Subnet Masks for Standard IP Address Classes

For example INFLIBNET has been allocated 32 IP addresses from ERNET, therefore the Subnet mask is 255.255.255.224

2.3.2 Client/Server Computing

The Internet computing is generally recognised as having its root in " Client/Server computing". The Browser works as a client and communicates with the HTTP server software residing on a separate dedicated computer called Web server. The HTTP server software job is to "listen" for the hyperlinks being transmitted over the Internet and ensure that the link is made to the appropriate information web page or is forwarded to the computer where the information resides. Each Web page, including a Web site's home page, is addressed by typing Uniform Resource Locator (URL) such as http://www.inflibnet.ac.in/ugc.html. URL is nothing but the combination of "http", domain name and the name and path of the requested information from the Web server such as

Protocol	Domain Name	Path to Information
http	www.inflibnet.ac.in	ugc.html
gopher	gopher.college.edu	
ftp	www.inflibnet.ac.in	soft.exe

Once an URL is typed in the open button of browsers, it generates a Get request and connects to the Web server at the designated IP address after a Domain Name System (DNS) lookup and waits for a response. The Web server is a programme that communicates with browsers using the http which runs on TCP/IP. When it receives a request, it locates the html document based on the IP address, sends it back to the browser and closes the connection. This is the basic browser and server interaction. Some of the popular browsers are Internet Explorer from Microsoft, Netscape Communicator from Netscape, etc., and Web servers are Internet Information Server 4.0 from Microsoft, Netscape NSAPI, Apache, etc. Today's browser includes e-mail, conference, Web authoring facilities also.

2.4 VIRTUAL PRIVATE NETWORK (VPN)

The Internet has been successful in its goal of allowing any host to communicate with any other, without setting up virtual circuits, reserving bandwidths, or performing any other actions with high overhead costs. But it falls far short of delivering the kind of security, reliability and performance guarantees that enterprises demand and are accustomed to in their private networks.

A VPN is a network that utilises a public-based infrastructure, such as the Internet, to provide secure, reliable and manageable Business - to – Business (B2B) communications. The followings are three essential elements to make a VPN function in today's complex computing environment.

2.4.1 Security

To provide security to network connections, the authenticity of VPN nodes, and the privacy and integrity of data are important.

2.4.2 Access Control

Access Control dictates the amount of freedom a VPN user has, i.e., control of the access of partners, employees and other outside users to the applications and different portions of the network. A VPN without access control only protects the security of the data in transit, not the network itself.

2.4.3 Authentication

Authentication is the process of verifying that the sender is actually the one who he says he is. A simple password was the first step towards providing identity, but passwords should be changed often to provide a more secure environment. Point – to – Point protocol (PPP) authentication mechanisms are used in many dial-in environments and include the Password Authentication Protocol (PAP) , the Challenge Handshake Protocol (CHAP), and the Extensible Authentication Protocol (EAP).

2.4.3.1 Password Authentication Protocol (PAP)

PAP, is the most basic form of authentication. It transmits a user's name and password over a network and computes it to a table of name-password pairs. The passwords stored in the table usually are encrypted. PAP's weakness, however, is that both username and password are transmitted " in the clear" – that' s, in an unencrypted form.

2.4.3.2 Challenge Handshake Protocol (CHAP)

CHAP features stronger security measures. In CHAP, one router sends a key to the other router to be used to encrypt the username and password. This enables the username and password to be transmitted in an encrypted form to protect them against hacking.

2.4.3.3 Terminal Access Controller Access Control System Plus (TACACS+) and Remote Access Dial-In User Service (RADIUS)

These are protocols that enable scalable identity implementations. The Kerberos protocol is used in limited areas to provide for a single login facility.

2.4.3.4 TACACS+

The TACACS + protocol is the latest generation of TACACS. TACACS is a simple User Datagram Protocol (UDP) –based access control protocol. TACACS+ is a client/server protocol and uses TCP for its transport. Transactions between the TACACS+ client typically a Network Access Server (NAS), and the TACACS+ server are authenticated through the use of a shared secret, which is never sent over the network. NAS (the authenticator) refers to the network point of access for remote dial-in users. The TACACS+ server performs user authentication, and the TACACS+ user profile defines the user's permissions.

2.4.3.5 RADIUS

RADIUS is a client/server protocol. A NAS such as a Cisco AS5200 access server operates as a client of RADIUS. The RADIUS server is usually a daemon process running on some UNIX or Windows NT machine. The client is responsible for passing user information to designated servers, and then acting on the response that is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. The RADIUS server can support a variety of methods to authenticate a user. When it is provided a username and original password given by the user, it can support PAP or CHAP, UNIX login and other authentication mechanisms. RADIUS also allows centralized logging of accounting information.

2.4.3.5.1 Encapsulation

Encapsulation is simply bundling of one protocol into another. VPN uses tunnelling technology also called encapsulation to carry the data from one end to another through the public network. VPN is defined between the tunnel initiator and the tunnel terminator. The tunnel initiator encapsulates packets inside a new packet, which contains a new source and destination headers, as well as the original packet. While all tunnel packets are IP packets, the encapsulated packets can be of any type of protocol, including those formed with non-routable protocol such as NETBUI. The tunnel terminator reverses that encapsulation process, stripping off the new headers and passing the original packet to a local protocol stack or a local network at the destination.

2.4.3.5.2 Encrypted Encapsulation

Encapsulation, in itself, does nothing to enhance the confidentiality or integrity of tunnelled data. Confidentiality is provided by Encryption. Encryption scrambles the data so that only those who have the key to read the information are able to decode the message. Encryption algorithms ensure that it is mathematically impossible to decode the data without the possession of the proper encryption key. Generally speaking, the security of the encrypted communication grows as the key becomes longer. Once the encryption key length is selected and implemented, the next step is to ensure that the keys are protected through a key management system. Key management is the process of distributing the keys, refreshing them at specific intervals and revoking them when necessary. Public–Key Infrastructure (PKIs), such as digital certificates, prescribe how keys will be created, delivered and revoked securely for every participation.

2.4.3.6 Digital Certificate

A digital certificate is an attachment to an electronic message used for security purposes. Companies conducting business over the Net use digital certificates for secure Internet transactions. Certificates are used in a number of techniques and by various applications.

One of the techniques, called the Public Key Infrastructures (PKI), uses public/ private key algorithms and digital certificates to verify the authenticity of all the parties involved in an Internet transactions.

A public/private key algorithm generates a unique set of keys-a public and a private key – for the user. The individual distributes his public key to all those, he wants to send messages to and keeps his private key with him.

While engaging in a digital transaction , the sender encrypts a message with his private key. The recipient uses the sender’s public key to decrypt it.

The above-mentioned digitally signed and transmitted documents provide a new legal standard that goes beyond traditional signed documents. A determined criminal can, after adequate practice , easily forge a signature.

But forgery of a digital signature is possible only if the forger gets hold of the private key of a person.

Alternatively, the forger has to use " Brute Force Attack" to check all possible combinations of the key. Breaking a 56-bit key using a single Computer is estimated to require about 5274 years at a speed of 50 microseconds per test. If the user uses a 128 – bit key and keeps changing it at periodical intervals , breaking of the key by Brute Force becomes almost impossible.

There are a number of **tunneling standards**.

- **PPTP (Point-to-Point Tunneling Protocol):** This works at layer 2 of the OSI model. It was designed for client/server operation and, thus, allows only a single point-to-point connection. PPTP is already present in Microsoft Windows 95/ 98 /NT operating systems but offer no solution for the unit operating system.
- **L2TP (Layer 2 Tunneling Protocol):** This works at layer 2 of the OSI model and was designed for a single point-to-point client/server connection. Multiple protocols can be encapsulated with in the tunnel. L2TP eliminates the PPTP's dependence on IP by abstracting the underlying transport protocol to any packetised protocol, such as IP, X.25 or Frame Relay. The specific network protocol is left up to the vendor implementation. L2TP also helps in reducing network traffic and enables servers to handle congestion by implementing flow control between the network access system (NAS) and the home gateway.

Comparing the two competing dial-up protocols

	PPTP	**L2TP**
Network	IP	Packet – oriented point-to- point (IP , Frame Relay , X.25 , ATM)
Supports	Single tunnel	Multiple tunnels (Different tunnels for different QoS)
Head Compression	N(6-byte overload)	Y (4-byte overload)
Tunnel Authentication	N	Y
Authentication Method	PAP, CHAP, NDS	PAP, CHAP, EAP, RADIUS

- **IPSec (IP Security) :** IPSec, a suite of authentication and encryption protocols from the IETF(Internet Engineering Task Force), is an encapsulation technology. IPSec was designed to provide security between multiple firewalls and routers. IPSec defines security on top of standard IP networking. IPSec, for all practical intents , requires a PKI . IPSec defines two types of key management.

2.5 EMERGING NETWORK TECHNOLOGIES

In the present era, data have become very crucial to any enterprise. Internet browsing, on-line transaction processing, data warehousing, data mining, text mining, etc., call for huge data storage capacities. The emphasis and significance of storage is such that the next decade is hailed as the "Age of Storage". The importance of having a sound and robust methodology to make the information available across the enterprise is the biggest challenge of the times. Just as LAN and WAN were developed to offer solutions to resource sharing, distributed applications and file transfer across the organisations, new technologies are emerging to accommodate storage applications. These are:

- Network Attached Storage (NAS) (Client Centric)
- Storage Area Network (SAN) (Server Centric)

2.5.1 Network Attached Storage (NAS)

NAS is an attempt to tackle data availability even while a server crashes by connecting a storage device directly on to the user network. NAS is just a specialised server (thin server) optimised for file sharing such who CD-ROM servers, DVD-ROM towers etc. NAS devices are connected directly on the LAN using traditional LAN technologies (such as Ethernet) and are accessed by clients using Network File System protocols running on top of IP protocols. NAS allows access to same physical data space from multiple operating systems at the same time. NAS is optimised for serving files to clients and is therefore said to be "Client-Centric". In this environment, the server does not add any significant application value.

2.5.2 Storage Area Network (SAN)

SAN, on the other hand takes off where NAS ends. Unlike NAS, which builds on an existing network, SAN explores the possibility of establishing an exclusive network for storage. Speed, sharing, storage consolidation and inter-operability are some of the objectives of SAN. Storage Area Network can be defined as a dedicated high speed network of directly connected storage elements designed to move large amount of data between host independent storage devices. The ownership of the "storage resource" is "decoupled " from the servers. SANs are optimised for delivering data to the servers and therefore can be thought as being " Server Centric". SAN utilises fibre channel technology to connect servers and high performance storage devices such as disk arrays which can carry data up to 100 Mbps for distances over 10 kms. compared to SCSI (Small Computer System Interface) technology which carries data upto 60 metres at the rate of 40 Mbps. SANs are particularly important in an environment where servers add significant application value such as database application.

2.6 FUTURE OF NETWORKING

As networking technology becomes pervasive, opportunities arise for using it in newer and more creative ways. One example is of using data networks rather than circuit switched networks to carry voice and video traffic. The generic term for this kind of use is converged networking.

Converged networking offers many benefits including integrated multimedia applications. The converged networking is the emerging trend like:

Payload convergence is that aspect of converged networking wherein different data types are carried in the same communications format. For example, while in the past audio and video traffic was carried over circuit switched networks as Layer 1 bit streams, while bursty data traffic was carried over packet switched networks in Layer 3 datagrams, payload convergence describes the trend to carry both audio/video and bursty data traffic in Layer 3 datagrams. Note, however, that payload convergence does not prohibit the network from handling packets differently, according to their service requirements.

Application convergence represents the appearance of applications that integrate formerly separate functions. For example, Web browsers allow the incorporation of plug-in applications that allow Web pages to carry multimedia content such as audio, video, high-resolution graphics, virtual reality graphics, and interactive voice.

Technology convergence signifies the move towards common networking technologies that satisfy both LAN and WAN requirements. For example, ATM can be used to provide both LAN and WAN services.

Self-Check Exercise

1) What is an OSI Model?

2) Explain briefly how the Internet works?

3) State the concept of Virtual Private Network (VPN).

....

....

....

....

....

....

....

2.7 SUMMARY

Constant developments are taking place in the field of Networking Technology. Efforts are underway to improve the capabilities of networks to carry data at higher speeds and over longer distances. Fiber Optic Cables and ATM switches are pointers in these directions. In this Unit, we have presented the current network technologies and also touched upon some emerging trends.

2.8 ANSWERS TO SELF CHECK EXERCISES

1) Short for *Open System Interconnection*, an **ISO standard** for worldwide communications that defines a networking framework is for implementing **protocols** in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the **channel** to the next station and back up the hierarchy.

2) It is a global **network** connecting millions of **computers**. More than 100 countries are linked into exchanges of **data,** news and opinions. Unlike **online services,** which are centrally controlled, the Internet is decentralized by design. Each Internet computer, called a ***host,*** is independent. Its operators can choose which Internet services to use and which **local** services to make available to the global Internet community.

   Remarkably, this anarchy by design works exceedingly well. There are a variety of ways to access the Internet. Most online services, such as **America Online,** offer access to some Internet services. It is also possible to gain access through a commercial **Internet Service Provider (ISP).**

3) VPN is short for *virtual private network,* a ***network*** that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the **Internet** as the medium for transporting data. These systems use **encryption** and other **security** mechanisms to ensure that only **authorized** users can access the network and that the data cannot be intercepted.

2.9 KEYWORDS

Convergence : The coming together of two or more disparate disciplines or technologies. For example, the so-called **fax** revolution was produced by a convergence of **telecommunications** technology, optical scanning technology, and printing technology.

Datagrams : A piece of a message transmitted over a packet-switching network. See under ***packet switching.*** One of the key features of a packet is that it contains the destination address in addition to the data. In **IP** networks, packets are often called *datagrams*.

Domain : A group of **computers** and **devices** on a **network** that are administered as a unit with common rules and procedures. Within the **Internet,** domains are defined by the ***IP address***. All devices sharing a common part of the IP address are said to be in the same domain.

Packet Switching : Refers to **protocols** in which messages are divided into **packets** before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message

2.10 REFERENCES AND FURTHER READING

Addison Wesley(1994) *TCP/IP Illustrated, Volume 1: The Protocols* W. Richard Stevens.

Black, U. (1992). TCP/IP and Related Protocols. New York: NY: McGraw-Hill, Inc.

William Stallings(1997) “Data and Computer Communications”, New Delhi: Prentice Hall of India,

Ramdas. S, Layer 3 Switching, LAN Magazine, November, 1998.

Implement Considerations, Networking Supplement, Microsoft Windows NT Server Address for private Intranet, Express Computer, October 26, 1998.

Miller, M. A. (1991). Internetworking: A Guide to Network Communications LAN to LAN; LAN to WAN. New York: M&T Books.

Perlman, and Mike Speciner (1995).New Delhi: Prentice Hall.

Stevens, W. R. (1994). TCP/IP Illustrated, Volume 1: The Protocols. New York: Addison-Wesley Publishing (Last Modified: July 24, 1996)

Mitesh Tolia ,The Basics of VPNs, LAN Magazine, February,1999 .

Akila Subramanian, The Decade Of Storage, Data Quest, December 15, 1999

Erric Hammond , Designing Storage Network with Fiber Channel Switches, Express Computer, October 25, 1999

The “Soft” future of networking, Express Computer, December 13, 1999.