UNIT-5

LAN COMPONENTS AND PROTOCOLS

CHAPTER OUTLINE

5.1 LAN Connectors, wireless network adapter

5.2 Coaxial Cables, Twisted-Pair Cables, Optical Fiber Cables, and Connectors used in Networking

5.3 Ethernet

5.4 LAN Devices

5.5 WLAN (Wireless LAN)

5.6 State the need for Protocols in Computer Networks

5.7 Protocols

5.1 LAN CONNECTORS, WIRELESS NETWORK ADAPTER

When two computers communicate, the source computer sends data to the destination computer. This data is converted into signals at the physical layer. The physical layer is also responsible for sending the signals over a connectivity medium. The most commonly used connectivity medium to connect computers or devices is a cable, a wire capable of transmitting signals from one device to another. When transmitting electric or optical signal from one device to another, following factors must be considered.

- Bandwidth
- Distance

Bandwidth : It is defined as the amount of data that can be transmitted by a cable for fixed period of time.

Distance : The bandwidth offered by a connectivity medium is limited by the distance over which the medium needs to transmit the signal. When the distance between the devices is greater, the bandwidth decreases because the signal needs to travel over a greater distance.

Connector : Connectors act as an interface between NIC of the computer and the cable that transmits the signal. As a result, the type of connector depends on the cable type used to connect computers or devices in the network.

Wireless Network Adapter : A wireless network adapter allows a computing device to join a wireless LAN. Wireless network adapters contain a built-in radio transmitter and receiver. Each adapter supports one or more of the 802.11a, 802.11b, or 802.11g Wi-Fi standards. Wireless network adapters also exist in several different form factors.

5.2 COAXIAL CABLES, TWISTED-PAIR CABLES, OPTICAL FIBER CABLES, AND CONNECTORS USED IN NETWORKING

The transmission media is the physical path between the transmitter and receiver. Transmission media can be classified as guided and unguided. In both cases, communication is in the form electromagnetic waves. With guided media, the waves are guided along a solid medium, such as copper twisted pair, copper coaxial cable and optical fiber. The atmosphere is an example of unguided media that provide a means of transmitting electromagnetic signals but do not guide them, this form of transmission is usually referred to as wireless transmission.

Guided Media :

1. Twisted pair cable.
2. Coaxial cable.
3. Optic fiber cable.

Unguided Media :

1. Radio frequency.
2. Terrestrial microwave.
3. Satellite communication.
4. Cellular telephony.

As listed above, number of transmission media are available, selection of the media depends on the following factors.

1. Transmission rate.
2. Distances.
3. Cost and ease of installation.
4. Resistance to environmental conditions.

5.2.1 *Preparation of Straight and Cross Cable*

UTP cable transfers data between two nodes or end devices.straight and cross cable are UTP wire to establish connection amongst networking devices.

A NIC uses pins 1 and 2 to transmit the data. To receive data, it uses pins 3 and 6. A switch does the opposite of it. It receives data on pins 1 and 2 and transmits data from the pin 3 and 6. Based on the type of end devices, a UTP cable can be made in two ways. The first type of cable, known as the straight-through cable, connects two different types of end devices; such as PC to Switch. The second type of cable, known as the cross-over cable, connects two same type of end devices such as PC to PC or Switch to Switch.

Straight-through Cable : In straight-through cable, wires are placed in the same position at both ends. The wire at pin 1 on one end of the cable connects to pin 1 at the other end of the cable. The wire at pin 2 connects to pin 2 on the other end of the cable; and so on.

The following table lists the wire positions of the straight-through cable on both sides.

Side A	Side B
Green White	Green White
Green	Green
Orange White	Orange White
Blue	Blue

Blue White	Blue White
Orange	Orange
Brown White	Brown White
Brown	Brown

A straight-through cable is used to connect the following devices.

- PC to Switch
- Router to Switch
- Hub to Server
- PC to Hub
- Switch to Server

Ethernet Cross-Over Cable :

- In this cable, transmitting pins of one side connect with the receiving pins of the other side.
- The wire at pin 1 on one end of the cable connects to pin 3 at the other end of the cable. The wire at pin 2 connects to pin 6 on the other end of the cable.
- Remaining wires connect in the same positions at both ends.

The following table lists the wire positions of the cross-over cable on both sides.

Side A	Side B
Green White	Orange White
Green	Orange
Orange White	Green White
BlueBlue	
Blue White	Blue White
Orange	Green
Brown White	Brown White
Brown	Brown

5.3 ETHERNET

Ethernet is a type of communication protocol that is created at Xerox PARC in 1973 by Robert Metcalfe and others, which connects computers on a network over a wired connection. It is a widely used LAN protocol. It connects computers within the Local Area Network and Wide Area Network. Numerous devices like printers and laptops

can be connected by LAN and WAN within buildings, homes, and even small neighbourhoods. It offers a simple user interface that helps to connect various devices easily, such as switches, routers, and computers. A local area network (LAN) can be created with the help of a single router and a few Ethernet cables, which enable communication between all linked devices. This is because an Ethernet port is included in your laptop in which one end of a cable is plugged in and connect the other to a router. Ethernet ports are slightly wider, and they look similar to telephone jacks.

Advantages of Ethernet :

- It is not much costly to form an Ethernet network. As compared to other systems of connecting computers, it is relatively inexpensive.
- Ethernet network provides high security for data as it uses firewalls in terms of data security.
- Also, the Gigabit network allows the users to transmit data at a speed of 1-100Gbps.
- In this network, the quality of the data transfer does maintain.
- In this network, administration and maintenance are easier.
- The latest version of gigabit ethernet and wireless ethernet have the potential to transmit data at the speed of 1-100Gbps.

Disadvantages of Ethernet :

- It needs deterministic service; therefore, it is not considered the best for real-time applications.
- The wired Ethernet network restricts you in terms of distances, and it is best for using in short distances.
- If you create a wired ethernet network that needs cables, hubs, switches, routers, they increase the cost of installation.
- Data needs quick transfer in an interactive application, as well as data is very small.
- In ethernet network, any acknowledge is not sent by receiver after accepting a packet.
- If you are planning to set up a wireless Ethernet network, it can be difficult if you have no experience in the network field.
- Comparing with the wired Ethernet network, wireless network is not more secure.

- The full-duplex data communication mode is not supported by the 100Base-T4 version.
- Additionally, finding a problem is very difficult in an Ethernet network (if has), as it is not easy to determine which node or cable is causing the problem.

5.4 LAN DEVICES

Computer network consist of different devices such as router, hub, switch, and others. Without these network devices data cannot be transmitted from one computer to another in a LAN or WAN network. These devices link up all the local and remote network segments with each other to make data communication from one segment to another. The two important devices of a big network are routers and switches. A computer network with good infrastructure with properly placed and configured network devices such as routers, switches etc. are helpful in reducing the overall operational cost, improve the performance, manageability and reliability.

5.4.1 *Repeaters*

A repeater is a network device that is used to retransmit the weaker signals in a network. A repeater receives the signals on the electromagnetic or optical transmission mediums. Repeater removes the unwanted noise from the incoming signals. A series of the repeaters is used to amplify the signals in the big network. The can also relay the messages between sub networks that use different protocols. Repeaters work at physical layer.

5.4.2 *Hubs*

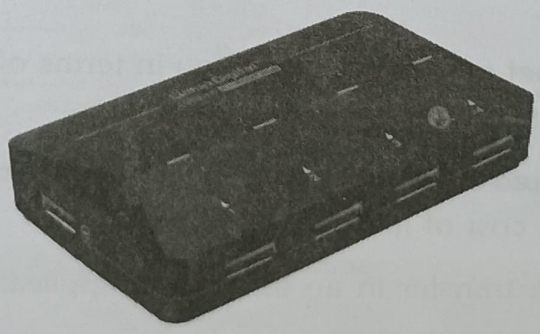


FIG 5.1 : 4 Port Hub

A hub is a networking device, which is used to connect the two segments of a wired network. In star topology, every computer is directly connected with the hub. In case of any fault in the hub, the data communication in the network computers stops. In an Ethernet (bus)-based network a hub is a central device that is used to connect all the computers with each other.

A hub has multiple ports such as 4,6, 8, 16 and 24 etc. When data packets are reached at hub, they are broadcasted to all the computers unlike a switch and only the destined computer receives the data. When you want to connect more than two computers with each other a hub or switch is required in a local area network. Hubs operate at the physical layer.

5.4.3 Switches

A network switch performs the same functionality in a network as a hub except a different that switch does not broadcast the data packets to all the computers in a network like a hub. A network switch has multiple ports like 4, 8, 16 and 24 etc. All the computers in a wired network are directly connected with the switch through Ethernet cable. Switches limit the traffic to and from each port and all the devices connected to the switch has maximum available bandwidth. Switch doesn't provide the built-in firewall capabilities like the routers. In the telecommunication and packet switched infrastructure switches play an important role. They transmit the data towards its destination based on the IP address. Switches work at data link layer.

5.4.4 Bridges

Bridges are used to connect two sub networks that use interchangeable protocols. It combines two LANs to form an extended LAN. The main difference between the bridge and repeater is that the bridge has a penetrating efficiency.

Working of Bridges : A bridge accepts all the packets and amplifies all of them to the other side. The bridges are intelligent devices that allow the passing of only selective packets from them. A bridge only passes those packets addressed from a node in one network to another node in the other network.

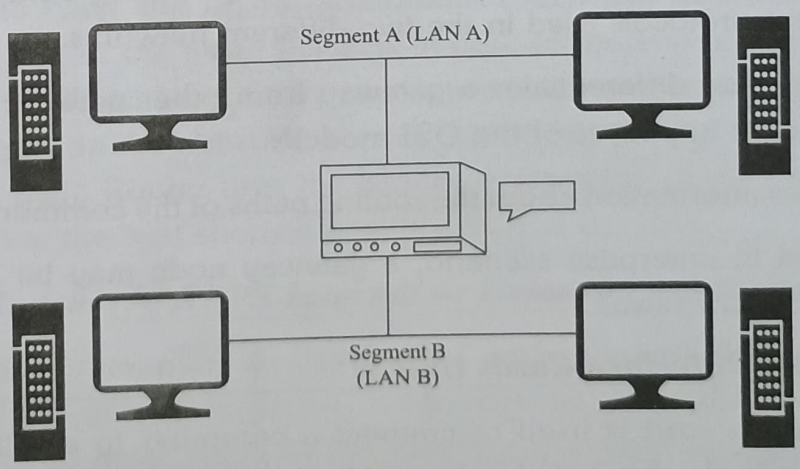


FIG 5.2 : Work of Bridge

A bridge performs in the following aspect :

- A bridge receives all the packets or frame from both LAN (segment) A and B.
- A bridge builds a table of addresses from which it can identify that the packets are sent from which LAN (or segment) to which LAN.
- The bridge reads the send and discards all packets from LAN A sent to a computer on LAN A and that packets from LAN A send to a computer on LAN B are retransmitted to LAN B.
- The packets from LAN B are considered in the same method.

5.4.5 *Gateways*

A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.

Features of Gateways :

- Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.
- It forms a passage between two different networks operating with different transmission protocols.
- A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.
- The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.
- It also stores information about the routing paths of the communicating networks.
- When used in enterprise scenario, a gateway node may be supplemented as proxy server or firewall.

5.4.6 *Network Interface Cards (NICs)*

A network interface card is used to connect a computer to an Ethernet network. The card (shown in the figure below) provides an interface to the media. This may be either using an external transceiver (as shown) or through an internal integrated

transceiver mounted on the network interface card PCB. The card usually also contains the protocol control firmware and Ethernet Controller needed to support the Medium Access Control (MAC) data link protocol used by Ethernet.

There is also a page showing examples of various types of networking equipment, include NICs for Ethernet.

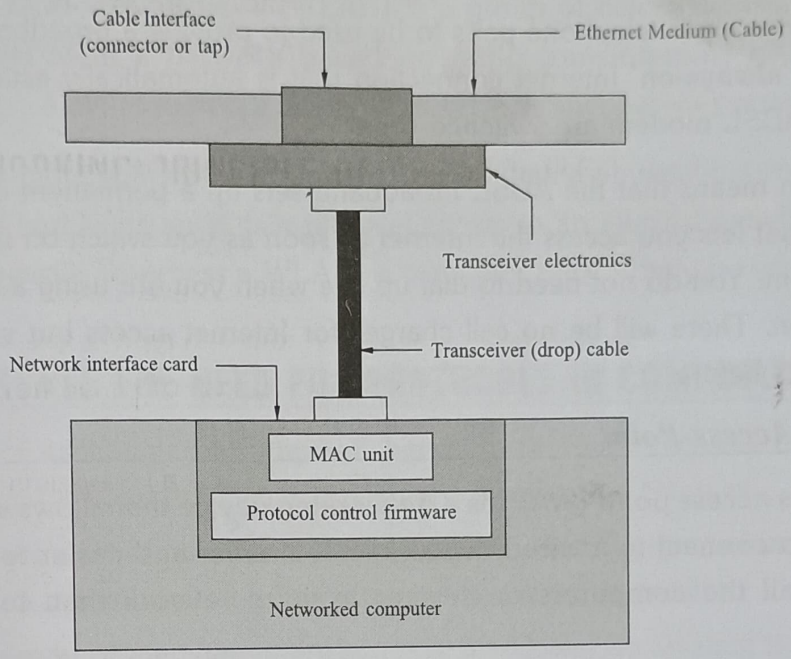


FIG 5.3 : Network Interface Card for Connection of a Computer to an Ethernet Network

5.4.7 *Routers (CISCO, DAX, Etc.)*

A router is a network communication device that is used to connect two or more logically and physically different networks. A router can be used to connect a LAN to LAN, LAN to WAN and LAN to Internet. A router acts as a post office where sorting and distribution of the posts (packets in case of routers) is done. A router works on the basis of an IP address. Every router has built-in operating system known as IOS. A router works on the network layer of the OS model and it routes the data towards the optimal path. Router uses the header information of the packets and forwarding table to define the best shortest possible path of the data.

5.4.8 *Modem (56 KBPS Internal or External, ADSL Modems)*

A modem is communication device that performs two different functions such as modulation and demodulation i.e., it converts the digital data into analog and analog into digital. The faster types of the modems are used by the internet such as DSL modem, cable modem and optical modems.

Internal Modem : A modem that resides on an expansion board that plugs into a computer.

External Modem : An external modem is a box that attaches to a computer's COM port via cables.

ASDL Modem : ADSL stands for Asymmetric Digital Subscriber Line. It is a technology that allows copper telephone pairs to be used to provide a broadband connection. It provides **'always-on'** Internet connection that is automatically established once the PC and ADSL modem are switched on.

Always-on means that the ADSL broadband sets up a permanent connection to the internet that lets you access the internet as soon as you switch on the computer and the modem. You do not need to dial up like when you are using a standard modem connection. There will be no call charges for Internet access but voice calls will be charged as before.

5.4.9 Access Point

A wireless access point (WAP) is a networking device that allows wireless-capable devices to connect to a wired network. It is simpler and easier to install WAPs to connect all the computers or devices in your network than to use wires and cables.

An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a WiFi signal to a designated area. For example, if you want to enable WiFi access in your company's reception area but don't have a router within range, you can install an access point near the front desk and run an Ethernet cable through the ceiling back to the server room.

WAPs are a more convenient, secure, and cost-efficient alternative to using wires and cables to connect every computer or device in your network. And using WAPs to set up a wireless network can provide many advantages and benefits for your small business.

The major difference between Router and Access point is that - The router acts as a hub that sets up a local area network and manages all of the devices and communication in it. An access point, on the other hand, is a sub-device within the local area network that provides another location for devices to connect from and enables more devices to be on the network.

5.5 WLAN (WIRELESS LAN)

A wireless local-area network (WLAN) is a group of colocated computers or other devices that form a network based on radio transmissions rather than wired connections. A Wi-Fi network is a type of WLAN; anyone connected to Wi-Fi network are a part of WLAN.

A wireless local-area network (WLAN) is a group of colocated computers or other devices that form a network based on radio transmissions rather than wired connections. A Wi-Fi network is a type of WLAN; anyone connected to Wi-Fi

A WLAN is more vulnerable to being breached than a physical network. With a wired network, a bad actor must gain physical access to an internal network or breach an external firewall. To access a WLAN, a bad actor must simply be within range of the network.

5.6 STATE THE NEED FOR PROTOCOLS IN COMPUTER NETWORKS

The task of exchanging information between devices - requires a high degree of cooperation between the involved parties can be quite complex

Protocols are a set of rules and conventions. By enforcing that communicating parties fallows to a common protocol, communication is made possible.

The complexity of the communication task is reduced by dividing it into subtasks.

Each subtask is implemented independently. Each subtask provides a service to another subtask.

5.7 PROTOCOLS

5.7.1 *Hyper Text Transfer Protocol (HTTP)*

HTTP is the protocol used to access resources, usually web sites, present on the Internet. HTTP uses TCP for transmission of data between the users computer and the web site. When a user keys in the Uniform Resource Locator of a web site in the browsers address bar, an HTTP request is generated. The browser is an HTTP client, and requests of HTTP clients are handled by the HTTP daemon that reside on the web server. A web server is a computer on which the files pertaining to a web sites are located. Once the HTTP daemon accepts theclient request, the user can view the web page in the browser.

HTTPS : For secure communication across the Internet, the secure HTTP (HTTPS) protocol is used for accessing and posting web server information. HTTPS can use authentication and encryption to secure data as it travels between the client and server. HTTPS specifies additional rules for passing data between the application layer and the transport layer

5.7.2 Hyper Text Transfer Protocol Secure (HTTPS)

- **HTTPS** is an abbreviation of **Hypertext Transfer Protocol Secure**. It is a secure extension or version of HTTP. This protocol is mainly used for providing security to the data sent between a website and the web browser. It is widely used on the internet and used for secure communications. This protocol uses the 443 port number for communicating the data.
- This protocol is also called **HTTP over SSL** because the HTTPS communication protocols are encrypted using the SSL (Secure Socket Layer).
- By default, it is supported by various web browsers.
- Those websites which need login credentials should use the HTTPS protocol for sending the data.

Advantages of HTTPS :

Following are the advantages or benefits of a Hypertext Transfer Protocol Secure (HTTPS) :

- The main advantage of HTTPS is that it provides high security to users.
- Data and information are protected. So, it ensures data protection.
- SSL technology in HTTPS protects the data from third-party or hackers. And this technology builds trust for the users who are using it.
- It helps users by performing banking transactions.

Disadvantages of HTTPS :

Following are the disadvantages or limitations of a Hypertext Transfer Protocol Secure (HTTPS) :

- The big disadvantage of HTTPS is that users need to purchase the SSL certificate.
- The speed of accessing the website is slow because there are various complexities in communication.
- Users need to update all their internal links.

5.7.3 File Transfer Protocol (FTP)

File Transfer Protocol (FTP), a standard Internet protocol, is the simplest way to exchange files between computers on the Internet.

It provides the ability to transfer files between dissimilar networks.

FTP Provides Two Types of Access :

- Public
- Restricted.

Remote login means that someone in New York could connect to a computer in Hyderabad, once connected, the users

computer emulates the remote computer. When the user types in commands, they are executed on the remote computer. The users monitor displays what is taking place on the remote computer during the telnet session.

FTP	Telnet
Stands for file transfer protocol.	Derived from Telecommunication Network.
FTP is entirely different from postage mail.	Telnet is also not related to postage mail.
Using FTP also we can send files.	We cannot sent files using Telnet.
Same as with e-mail.	We can access a remote computer.
Using FTP we can send any size file.	Not applicable.

In public access mode, we can login to the system with anonymous as user name.

In restricted access mode, we have to specify user name and password for accessing the files.

FTP Commands :

- **Ftp [host] :** Open an ftp session with the specified host machine.

  Example : C:\> ftp neserve0 C:\> ftp erols.erols.com

- **Open [host] :** Establish a connection to the specified host when you're already at an ftp prompt.

  Example : ftp> open neserve0

  ftp> open erols.erols.com

- **User [username] :** Log into an ftp server when you're already connected in an ftp session.

  Example : ftp> user dlozinsk ftp> user anonymous

- **Put [local-file] :** Put (upload) local-file to the remote machine. No wildcards!

  Example : ftp> put index.html ftp> put test.txt

- **Get [remote-file] :** Retrieve (download) remote-file and store it on the local machine. No wildcards! Can only get one file at a time.

  Example : ftp> get index.html

  ftp> get /tmp/readme.txt

5.7.4 *Simple Mail Transfer Protocol (SMTP)*

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail.

5.7.5 *Telnet*

The word telnet derived from telecommunications and network and is a protocol that allows a user to log on to a remote computer.

Telnet is also known as remote login, which means connecting one machine to another in such a way that a person may interact with as if it is being used locally.

REVIEW QUESTIONS

Part-A

1. What is an accesspoint?
2. What is Ethernet?
3. What is HTTPS?
4. Why computer network is needed.
5. Classify computer networks.
6. List the layers in TCP/IP reference model.
7. List various LAN components.
8. What are the various connectors used in LAN.
9. What is repeater ?
10. What is a switch ?
11. What are the components of IP addressing ?

Part-B

1. Explain HTTPS and its advantages.
2. What is an Access point?
3. What is a bridge? What is its purpose?
4. What is a repeater? What is its need?
5. Compare LAN and WAN.
6. List hardware & software components in LAN.
7. List the layers in OSI reference model.
8. List the advantages and disadvantages of bus topology.
9. What are the advantages and disadvantages of ring topology ?
10. Compare FTP & Telnet.
11. Compare TCP/IP with OSI.
12. Compare various transmission media.

13. What are the advantages and disadvantages of star topology ?
14. Compare bus topology with ring topology.

Part-C

1. Explain WLAN and its need.
2. Explain Ethernet and its usage.
3. Explain about various types of network.
4. Explain about OSI reference model.
5. Explain about TCP/IP reference model.
6. Explain about different network topologies.
7. Explain about LAN cables.
8. Explain about various LAN devices
9. Explain about transmission media.

UNIT-6

NETWORK ADDRESSING AND MANAGEMENT

CHAPTER OUTLINE

6.1 INTRODUCTION TO NETWORK ADDRESSING

A network address is an identifier for a node or network interface of a telecommunications network. The process or system of assigning network address is called as network addressing. Network addresses are often designed to be unique across the network, although some networks allow for relative or local addresses that may not be unique. More than one type of network address may be used in any one network. In some cases terminal nodes may have more than one network address, for example, each link interface may be uniquely identified. In addition, non terminal nodes are often assigned network addresses.

- **IP Address :** A logical numeric address that is assigned to every single computer, printer, switch, router or any other device that is part of a TCP/IP-based network
- **Subnet :** A separate and identifiable portion of an organization's network, typically arranged on one floor, building or geographical location.
- **Subnet Mask :** A 32-bit number used to differentiate the network component of an IP address by dividing the IP address into a network address and host address
- **Network Interface Card (NIC) :** A computer hardware component that allows a computer to connect to a network.

6.2 TCP/IP ADDRESSING SCHEME

TCP/IP uses a 32 bit addressing scheme to identify the devices on a network. These 32 bits are divided into four octets, of eight bits each. Each of these four octets is represented in a decimal form, and separated by a dot. For example, 198.172.168.10 is an IP address. This format of representing IP address is called the dotted decimal format.

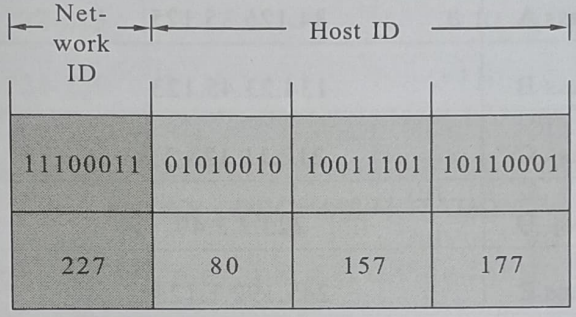
The octets in an IP address can take a decimal value form 9 to 255 because the largest decimal value that can be represented by eight binary bits is 255(11111111 in binary). For example, the 32 bit binary address 11000110.10101100. 1010100.0001010 represents the IP address 198.172.168.10.

The addressing provided by a network layer protocol to a device is called its network address. For example, 198.172.168.10 is the network address of a device. This is different from the MAC address which is the hardware address of the NIC or the device(routers or switch). The network address in a TCP/IP network are also known as IP addresses. Therefore, 198.172.168.10 is also known as the IP address.

6.2.1 Components of IP Address

For continence sake we use IP address dotted-decimal notation, while the computer converts this into binary. However, even though these sets of 32 bits are considered a single *"entity"*, they have an internal structure containing two components :

- **Network Identifier (Network ID) :** A certain number of bits, starting from the left-most bit, is used to identify the network where the host or other network interface is located. This is also sometimes called the network prefix or even just the prefix. This is the address of the network itself, and is used by other networks to identify this network.
- **Host Identifier (Host ID) :** The remainder of the bits are used to identify the host on the network. This is the address of the device with in the network.



IP ADDRESS : 227.82.157.177

SPLIT INTO 8-BIT NETWORK ID AND 24 - BIT HOST ID

FIG 6.1 : Basic IP Address Division: Network ID and Host ID

The fundamental division of the bits of an IP address is into a network ID and host ID. Here, the network ID is 8 bits long and the host ID is 24 bits in length.

6.2.2 IP Address Classes

Internet addresses are allocated by the InterNIC the organization that administers the Internet. These IP addresses are divided into classes. The most common of these are classes A, B, and C. Classes D and E exist, but are not generally used by end users. Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet. Following are the ranges of Class A, B, and C Internet addresses, each with an example address :

- **Class A Networks** use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.
- **Class B Networks** use a default subnet mask of 255.255.0.0 and have 128-191 as their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.

- **Class C networks** use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

- **Class D Network,** binary addresses start with 1110, therefore the decimal number can be anywhere from 224 to 239. Class D networks are used to support multicasting.

- **Class E Network,** binary addresses start with 1111, therefore the decimal number can be anywhere from 240 to 255. Class E networks are used for experimentation. They have never been documented or utilized in a standard way.

First Octet Value	Class	Example IP Address
0-126	Class A	34.126.35.125
128 - 191	Class B	134.23.45.123
192 - 223	Class C	212.11.123.3.
224 - 239	Class D	225.2.3.40
240 - 255	Class E	245.192.1.123

Class	Address Components	Network/Host
Class A	Network.Host.Host.Host	34.126.35.125
Class B	Network.Network.Host.Host	134.23.45.123
Class C	Network.Network.Network.Host	212.11.123.3.
Class D	Not Defined	Not Defined
Class E	Not Defined	Not Defined

6.2.3 *Classify the Internet Protocol Addressing IPv4*

Classful Addressing : IPV4 address, at its inception, used the concept of classes. This architecture is called classful addressing. Although this scheme is obsolete, we briefly discuss it here to show the rationale behind classless addressing.

In classful addressing, the address space is divided unto five classes A, B, C, D and E. We can the class of an address when given the address, in binary notation or dotted-decimal notation. If the address is given in the binary notation, the first few bits can immediately tell us the class of the address. If the address is given in decimal dotted notation, the first byte the class. Both methods are shown in Fig. 6.2, 6.3.

Class	First Byte	Second Byte	Third Byte	Fourth Byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			

FIG 6.2 : BINARY NOTATION

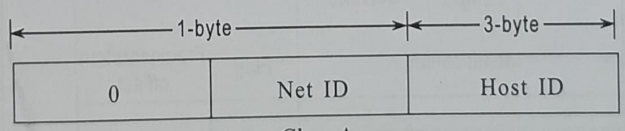
Class	First Byte	Second Byte	Third Byte	Fourth Byte
Class A	0-127			
Class B	127-191			
Class C	192-223			
Class D	224-239			
Class E	240-255			

FIG 6.3 : DECIMAL NOTATION

In classful addressing, the address space is divided unto five classes A, B, C, D and E

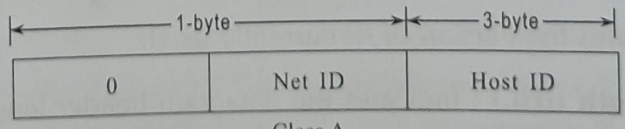
1. Class A.
2. Class B.
3. Class C.
4. Class D.
5. Class E.

1. **Class-A :** In class A, 1 byte is used for network address and 3byte are used for host address. The first always '0' for class A network . Class A addresses were designed for large organization with a large number of attached hosts or routers.



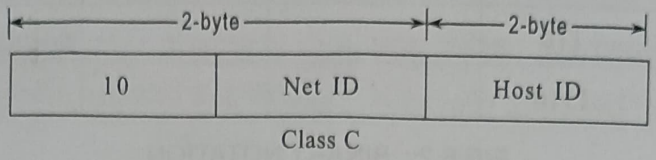
Class A

2. **Class-B :** In class B, 2 bytes reserved for network address and 2 bytes are reserved for a host address. Class B addresses were designed for midsize organization with tens of hounds' of attached hosts or routers.



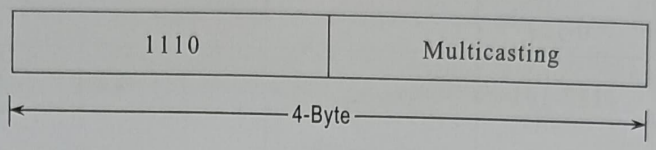
Class A

3. **Class-C :** In class C, 3 bytes are reserved for network address and 1 byte are reserved for a host address. In class C addresses were designed for small organization with small number of attached hosts or routers.



Class C

4. **Class D :**



5. **Class E :** Class E address were reserved future use, only a few were used, resulting in another waste of addresses.

IPV4 Address : An IPV4 address is a 32-bit address that uniquely and universally defines the connection of a device to the internet. IPV4 address are unique. They are unique in the sense that each address defines one and only one connection to the internet. Two devices on the internet can never have the same time.

IPV4 Header Format :

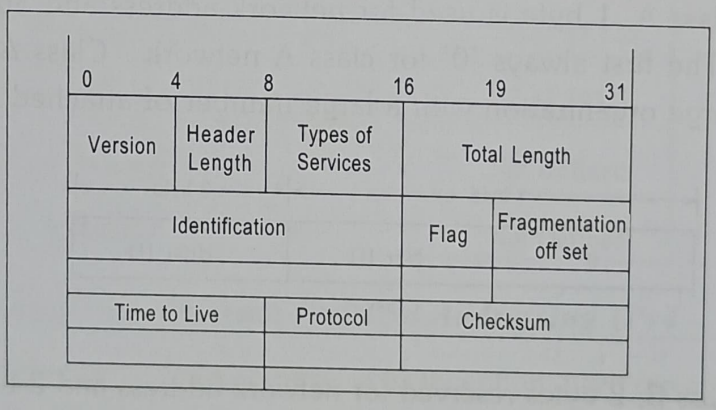


FIG 6.4 :

Source Address Destination Address Options (If any) Padding :

- **Version :** Indicates the version of IP currently used.
- **IP Header Length (IHL) :** Indicates the datagram header lengthin 32-bit words.
- **Type-of-Service :** Assigns data grams various levels ofimportance.

- **Total Length :** Specifies the length, in bytes, of the entire IP packet.
- **Identification :** Contains an integer that identifies the currentdatagram.
- **Flags :** The two low-order (least-significant) bits controlfragmentation. The low-order bit specifies whether the packet can be fragmented. The middle bit specifies whether the packet is the last fragment in a series of fragmented packets. The third or high-order bit is not used.
- **Fragment Offset :** Indicates the position of the fragment's datarelative to the beginning of the data in the original datagram.
- **Time-to-Live :** Maintains a counter that gradually decrementsdown to zero, at which point the datagram is discarded. This keeps packets from looping endlessly.

Classless Addressing : To overcome address depletion and give more organization access to the internet classless addressing was designed and implemented. In this scheme, there are no classes, but the addresses are still granted in blocks.

Address Blocks : In classless addressing, when an entity, small or large, needs to be connected to the internet, it is granted a block (range) of addresses. The size of the block (the number of addresses) varies based on the nature and size of the entity .for example, a household may be given only two address :a large organization may be given thousands of addresses. An ISP (internet services), may be given thousands or hundreds of thousands based on the number of customer it may serve.

Restriction :

1. To simplify the handling of addresses, the internet authorities impose three restriction on classless address block :
2. The address in a block must be contiguous, one after another.
3. The number of address in block must be a power of 2 (1, 2, 4, 8).
4. The first address must be evenly by the number of addresses.

Example : Fig. 6.5 shows a block of addresses, in both binary and dotted-decimal notation ,granted to a small business that needs 16 addresses.

We can see that the restriction are applied to this block. The address are contiguous. the number of addresses is a power of 2(16=24) and the first address is divisible by 16. The first address, when converted to decimal number, is 3, 440, 387, 360, which can be divided by 16 results in 215, 024, 210. In appendix B, we show how to find the decimal value of an IP address.

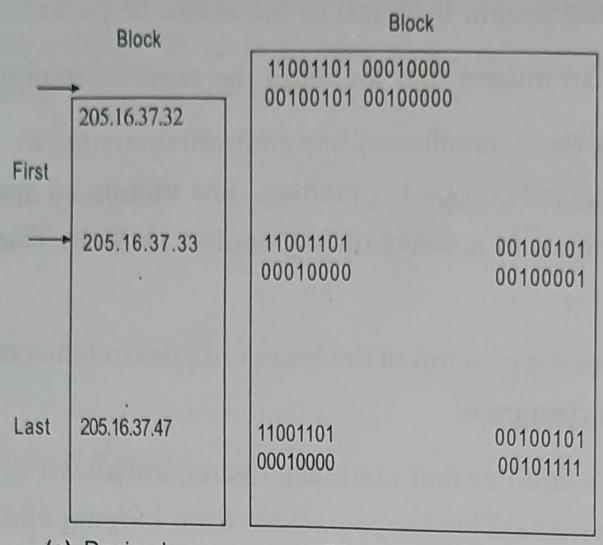


FIG 6.5 :

Classless Inter Domain Routing : CIDR is a way to allocate and specify the internet addresses used in inter domain routing more flexibly then with the original system of internet protocol address classes.

One of the most commonly used classes is class B, which allocate space for up to 65,533 host address. A company who needs more than 254 host machines, but far less than 65,533 host address possible, would essentially be wasting most of the block or address allocated. For this reason, the internet was running out of address space. CIDR effectively solved theproblem by specifying a new way to specify the network addresses in the router.

Using CIDR each IP address has a network prefix that indicate either a combination of network gateway or an individual gateway. The length of a network prefix is also number of bits that are required. Routers are required to use the most specific or longest network prefix in the routing table when forwarding packets.

A CIDR network address looks like this 192-30.250.00/18

The format 192.30.250.00is the network address and 18 specifies that the first 18-bits are the network part of the address. leaving the last 14-bits for specific host address .CIDR lets one routing table entry represent an aggregation of networks that exit in the forward path. this aggregation of networks in a single address is some times referred as a super net.

CIDR is supported by an exterior gateway protocol called as the border gateway protocol. It is also supported by open shortest path first interior gateway protocol.

6.2.4 Classful Addressing and Classless Addressing in IPv4

(6.2.3 and 6.2.4 are the same)

Difference between Classful and Classless Addressing :

- Classful addressing is a technique of allocating IP addresses that divides them into five categories. Classless addressing is a technique of allocating IP addresses that is intended to replace classful addressing in order to reduce IP address depletion.
- The utility of classful and classless addressing is another distinction. Addressing without a class is more practical and helpful than addressing with a class.
- The network ID and host ID change based on the classes in classful addressing. In classless addressing, however, there is no distinction between network ID and host ID. As a result, another distinction between classful and classless addressing may be made.

6.2.5 IP Subnetting

Subnets are an efficient method for logically dividing a network into segments, such that the network performance is optimized. Subnets are defined as the segments of a network that use addrssing schemes different from one another but corresponding to the adressing scheme used by the main network. Therefore, devices in one subnet cannot directly communicate with devices represented by 192.168.30.0, in which 192.168.30 represents the network address, and the value in the fourth octet would represent the host on the network. For example, the address of a particular host in this network would be 192.168.30.4. The fourth octet in a Class C address can take a value between 0 and 255, and therefore, this network can have up to 256 hosts. However, configuring 255 components in a single network would significantly degrade the performance of the network as well as the network router. Therefore, the network, 192.168.30.x can be divided into subjets, with each subnet consisting of, say, 16 computers.

On a network without subnets, a device outside the network can identify a host with the help of the network and host addresses. On a network with subnets, however, an additional piece of information, called the subnet mask, is needed to identify a host. The network address helps determine the network in which the host is located, whereas the subnet mask is responsible for locating the subnet on the network to which the host belongs. The host address identifies the individual host.

However, the addresing scheme used by IP has only four octets that can be used to represent the network address or the host depending on the IP address class. It is not possible to include information on the subnet in the IP address itself, and therefore, the subnet mask is a separate 32 bit address, accompanying the IP address of a device.

The default subnet mask values for Class A, Class B, Class IP addresses are listed in table.

TABLE : Default Subnet Masks of IP Address Classes

IP Address Class	Default Subnet Mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

The default subnet masks are used when a network does not have any subnets. For creating subnets, the defult values are modified to obtain customized subnet masks. When subnet masks are customized, only the octets that denote the host address are modified, and not the octet(s) that represent the netwok address. For example 255.244.0.0 is a valid subnet mask for a Class A network but not 252.124.0.0. In fact, 252.124.0.0 is not a valid subnet mask for a network of any IP address class.

The subnet masks and IP addresses on the network are dependant on one another because of network that belongs to a particular IP address class can accommodate only a particular number of devices irrespective of the number of subnets. For example, a Class B network can have a maximum of only 65,536 devices irrespective of the number of subnets that are created. Therefore, the subnet mask values are derived from the IP address of the network. Fig. 6.6, represents the components of a typical IP address further divided to depict the subnet address.

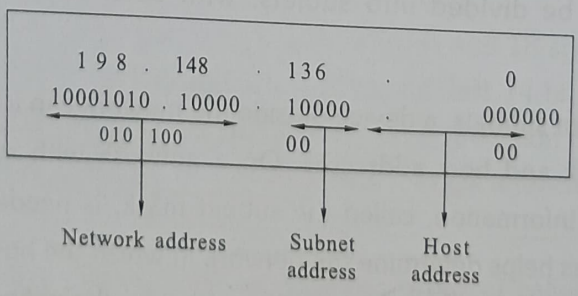


FIG 6.6 : Subnet Address Component of IP Address

As represented in Fig. 6.6, the bits of the octet (s) representing the host address are subdivided to represent the subnet address and the host adress. For example, in a class C IP address, the bits of the last octet represent the subnet address as well as the host address. The number of bits used by the subnet address, and the number of bits used by the host address are determinedby the subnet mask. The following sub-topic explains the steps involved in creating subnets.

6.2.6 State the Need for IPv6

- Header format simplification.
- Expanded routing and addressing capabilities.
- Improved support for extensions and options.
- Flow labeling (for QoS) capability.
- Auto-configuration and Neighbor discovery.
- Authentication and privacy capabilities.
- Simple transition from IPv4.

6.2.7 Internet Protocol Version-6 (IPv6) Addressing

IPV6 is designed to solve the problem of IPV4. It does this by creating new version of protocol which performs the function of IPV4, but without the limitations of IPV4. In this version, the internet uses 128 bit addresses that give much greater flexibility in address allocation. These address referred to as IPV6.

Goals of IPV6 :

- IPV6 reduces the total time which people have to spend configuration and managing systems

IPV6 HEADER FORMAT

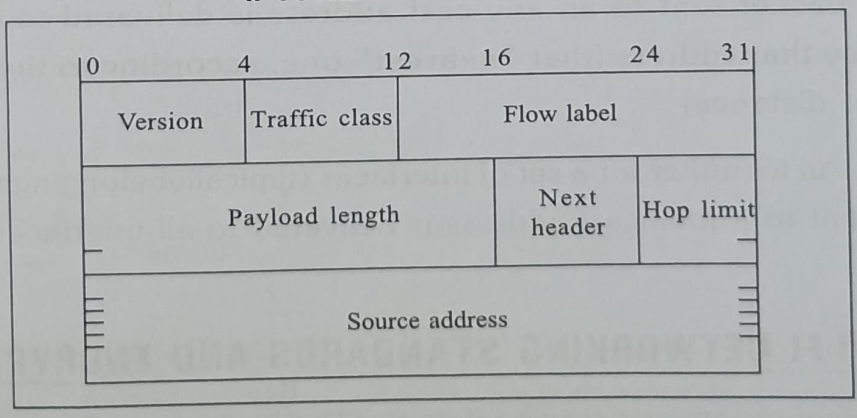


FIG 6.7 :

- IPV6to speed up the network, both from performance and deployment point of view. IPV6 support security protocol, encapsulating protocol and authentication header.

IPV6 address space expansion is to make network address translation, improving total connectivity, reliability and flexibility.

- Version field same size, same location.
- Traffic class to support differentiated services.
- **Flow :** Sequence of packets from particular source toparticular destination for which source requires special handling.
- **Payload Length :** Length of data excluding header, upto 65535 B.
- **Next Header :** Type of extension header that followsbasic header.
- **Hop Limit :** hops packet can travel before beingdropped by a router.

Address Categories : IPv6 addresses are 128-bit identifiers for interfaces and sets of interfaces. There are three types of addresses :

1. Unicast.
2. Anycast.
3. Multicast.

1. **Unicast :** An identifier for a single interface. A packet sent toa unicast address is delivered to the interface identified by that address.
2. **Anycast :** An identifier for a set of interfaces (typically belongingto different nodes). A packet sent to an any cast address is delivered to one the interfaces identified by that address (that **"nearest"** one, according to the routing protocols' measure of distance)
3. **Multicast :** An identifier for a set of interfaces (typicallybelonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.

6.3 WI-FI NETWORKING STANDARDS AND ENCRYPTION TYPES

Wireless Fidelity is generic terms refers to (The institute of Electrical and Electronics Engineers) IEEE 802.11 standards for Wireless Local Area Network.

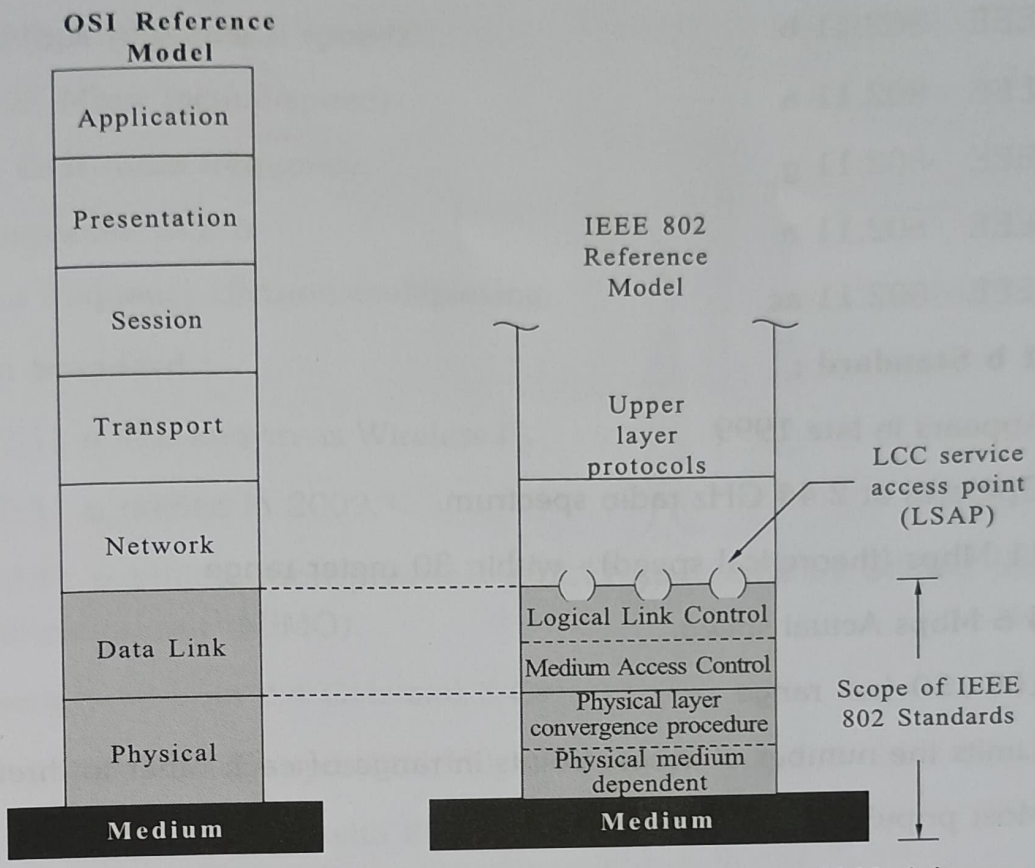


FIG 6.8 : IEEE 802 Protocol Layers Compared to OSI Model

Wi-Fi is a wireless technology that uses radio frequency to transmit data through the air.

Wi-Fi Network Connects Computer to each other, to the internet and to the wired network.

Wi-Fi Works on IEEE 802.11 Standards :

- 802.11 is primarily concerned with the lower layer of the OSI model.
- Data Link Layer
  - (i) Logical Link Control (LLC)
  - (ii) Medium Access Control (MAC)
- Physical Layer
  - (i) Physical Layer Convergence Procedure (PLCP).
  - (ii) Physical Medium Dependent (PMD).

802.11 Standards : IEEE 802.11 is a set of Media Access Control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5 and 60 GHz frequency bands.

- IEEE 802.11 b
- IEEE 802.11 a
- IEEE 802.11 g
- IEEE 802.11 n
- IEEE 802.11 ac

802.11 b Standard :

- Appears in late 1999
- Operates at 2.44 GHz radio spectrum.
- 11 Mbps (theoretical speed) - within 30 meter range
- 4-6 Mbps Actual speed.
- 100-150 feet range.
- Limits the number of access points in range of each other to three.
- Most popular, Least expensive.
- Uses direct sequence spread-spectrum technology.

802.11 a Standard :

- Introduction in 2001
- Operates at 5 GHz
- Less popular and less interfered.
- 54 Mbps (theoretical speed).
- 15-20 Mbps (Actual speed).
- 50-75 feet range.
- More expensive
- Highly obstructed
- Not compatible with 802.11 b
- Uses frequency division multiplexing.

802.11 g Standard :

- Introduce in 2003.
- Combine features of both a and b
- 100-150 feet range.

- 54 Mbps (theoretical speed).
- 20-25 Mbps (actual speed)
- 2.4 GHz radio frequency.
- Compatible with b
- Uses frequency division multiplexing.

802.11 n Standard :

- 802.11 n also known as Wireless N.
- 802.11 n ratified in 2009.
- 802.11 n builds upon previous 802.11 standards by adding multiple-input multiple-output (MIMO).
- Operates on both 2.4 GHz and 5 GHz
- Provide bandwidth upto 300 Mbps.
- Backward-compatible with 802.11 b/g gear
- Increased speed and range.

802.11 ac Standard :

- Builds on 802.11 n, published in 2013
- The addition of multi-user MIMO (MU-MIMO)
- Utilizes dual band wireless technology.
- Support connection both 2.4 GHz and 5 GHz.
- Backward compatibility to 802.11 b/g/n.
- Bandwidth rates upto 1300 Mbps on the 5 GHz.
- Bandwidth rates upto 450 Mbps on the 2.4 GHz.

6.3.1 *Encryption*

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it.

A process that converts original information, also called plain text into a difficult-to-interpret from called **ciphertext.**

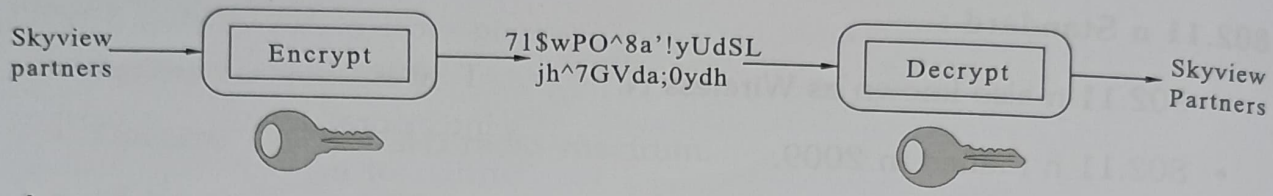
Encryption does not of itself prevent interception, but denies the message content to the interceptor.

Done by using an encryption algorithm, a formula used to turn plain text into ciphertext.

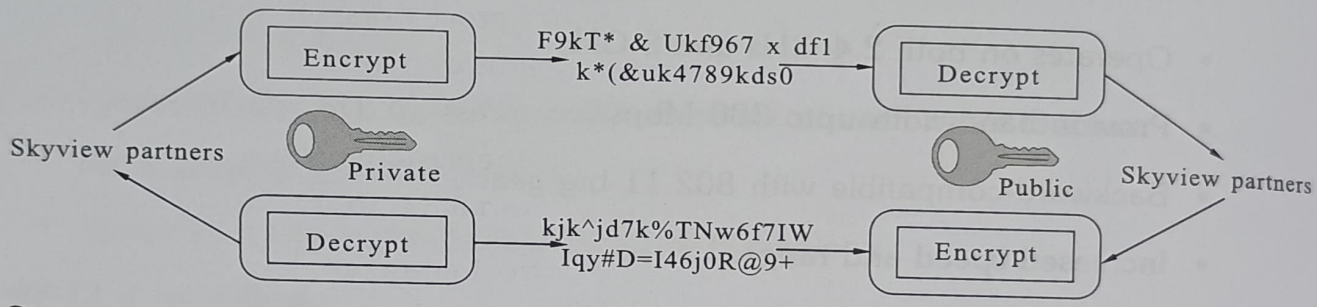
Types of Encryption : There are two types of encryption. They are :

- Symmetric key encryption.
- Asymmetric key encryption.

Symmetric keys : Encryption and decryption use the same key



Asymmetric keys : Encryption and decryption use different keys, a ***public key*** and a ***private key***.



Symmetric Key Encryption :

- A secret key, is applied to the text of a message to change the content in a particular way.
- Uses the same keys for both encryption of plaintext and decryption of ciphertext.
- The keys may be identical or there may be a simple transformation to go between the two keys.
- The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.
- Both parties have access to the secret key which is one of the main drawbacks of symmetric key encryption, in comparison to asymmetric key encryption.

Asymmetric Key Encryption :

- Known as public-private key or public key encryption.
- Uses key pairs for encrypting or decrypting data.
- Public key is used to encrypt the data and private key is used to decrypt the data.

- Any message that is encrypted by using the private key can only be decrypated by using the matching public key.
- It hs ability to share secret data without sharing the same encryption key.

6.4 UNDERSTAND THE OVERVIEW OF NETWORK MANAGEMENT

A network management system is a collection of tools for network monitoring and control that is integrated in the following senses,single operator interface with a powerful but user-friendly set of commands for performing most or all network management tasks,A minimal amount of separate equipment. That is, most of the hardware and software required for network management is incorporated into the existing user equipment. A network management system consists of incremental hardware and software additions implemented among existing network components. The software used in accomplishing the network management tasks resides in the host computers and communications processors (e.g., front-end processors, terminal cluster controllers, bridges, routers).A network management system is designed to view the entire network as a unified architecture, with addresses and labels assigned to each point and the specific attributes of each element and link known to the system. The active elements of the network provide regular feedback of status information to the network control center.

Network management is the process of Controlling a complex data networkIn order to maximise efficiency and productivity.International.

Organisation for Standardisation (ISO) defines five (5) functional areas :

- Fault management.
- Configuration Management.
- Security Management.
- Performance Management.
- Accounting Management.

6.5 UNDERSTAND THE MODEL OF ISO NETWORK MANAGEMENT

The International Organization for Standardization (ISO) deals with five major functional areas of network management model as performance management, accounting management, configuration management, fault management and security management.

Performance Management : Performance management and monitoring,Assessment and review of the available bandwidth and network usage of resources in a network to make more efficient to run. Performance management is a very important part of

the model of network management, especially for business and / or organization that wants to streamline network performance to their's. Solar Winds is a great tool for performance management.

Accounting Management : Management accounting control and evaluate the use of data and / or resources for settlement purposes. This aspect of network management by Internet service providers to bill customers for the resources they use.

Configuration Management : Configuration management of network monitoring-side versions of hardware and software on the network to identify "Their impact on the operation of the network is an example. The Microsoft System Management Server (SMS) capability that hasmanage, monitor and track each piece of software and hardware in a particular network.

Fault Management : Fault management is what most people think that the administration if they think the network. The purpose of this advanced network management is to identify, detect and alert system administrators of problems that may affect system operations.

Security Management : Security management deals with controlling access to resources and alsoNotify the competent authorities if some resources are available. Similarly, a network operator, or may e-mail outsourcing, if a resource fails, management systems can be used to access the network to send messages when certain files or routers, servers. Intrusion Detection Systems, Symantec Intruder Alert, these capabilities of security management.

There are many products, support for the management of some or all of these areas of the network.That most network management systems have in common is the use of protocols such as Simple Network Management Protocol (SNMP), SNMPv3, and Common Management Information Protocol (CMIP). There are a variety of tools for network management software network management for Intuit's Tivoli, Fidelia Helix of AdventNet. Maybe the solution does not include a network management system for heating prices have gone up as the machines increases, but you can certainly find what you need in these instruments and other awards to the market.

6.6 UNDERSTAND THE NETWORK MONITORING AND TROUBLESHOOTING

Network troubleshooting is the collective measures and processes used to identify, diagnose and resolve problems and issues within a computer network. It is a systematic process that aims to resolve problems and restore normal network operations within the network.

Network troubleshooting is primarily done by network engineers or administrators to repair or optimize a network. It is generally done to recover and establish network or

Internet connections on end nodes/devices. Some of the processes within network troubleshooting include but are not limited.

Finding and resolving problems and establishing Internet/network connection of a computer/device/node.

Configuring a router, switch or any network management device.

- Installing cables or Wi-Fi devices.
- Updating firmware devices on router switch.
- Removing viruses.
- Adding, configuring and reinstalling a network printer

Network troubleshooting can be a manual or automated task. When using automated tools, network management can be done using network diagnostic software.

6.7 NETWORKING TROUBLESHOOTING TOOLS

The network troubleshooting tools are classified into two types :

- Hardware tools
- Software Tools

The hardware tools included in the network troubleshooting are

Cable Tester : It is also known as a media tester. It is used to test whether the cable works properly or not. The cable testers will confirm whether a cable works correctly and if there is a problem with the cable. Tools which are used for testing of the cable can be classified as a cable tester.

Protocol Analyser : This tool is used to analyse the network protocols like UDP, TCP, and FTP etc. This acts as a software as well as hardware-based tool. This tool is also used to identify malicious networks traffic.

Multimeter : It is used to check shorts in the coaxial cable; it can measure current, resistance and voltage. The new version of multi meter also allows measuring the temperature.

Software Tools : The software tools included in the network troubleshooting are

Ping : Ping is a famous tool which is used to perform connectivity tests between the requesting host and the destination host. The Internet Control Message Protocol (ICMP) protocol is used to perform this. If the requesting host receives a response

from the destination host the host is reachable otherwise it is not reachable.

Speedtest.net : This is simple software that can be installed in devices or some add-ons in the browsers. This tool allows the user to check the bandwidth available.

Netsat : Netsat means network statistics. It is used for finding problems in the network and also it can determine the traffic on the network.

6.8 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Simple Network Management protocol is frame work for managing devices in an internet using the TCP/IP. simple network management protocol (SNMP) is an application-layer protocol defined by the internet architecture it is a part of transmission control protocol internet protocol (TCP/IP) protocol suite.

SNMP is one of the widely accepted protocols to manage and monitor network elements. most of the professional-grade network elements come with bundled SNMP agent. these agents have to be enabled and configured to communicate with the network management system.

6.9 HOW SNMP WORKS

The model of network management that is used for SNMP includes the following key elements :

- Management Station, or Manager.
- Agent.
- Management information base.

- **Management Station, or Manager :** The management station is typically a standalone device but may be a capability implemented on a shared system. In either case, the management station serves as the interface between the human network manager and the network management system. The management station will have, at minimum, a set of management applications for data analysis, fault recovery, and so on a user interface by which the network manager may monitor and control the network. The capability of translating the network manager's requirements into the actual monitoring and control of remote elements in the network. A database of network management information extracted from the databases of all the managed entities in the network
- **Management Information Base :** Management information base create a set of objects defined for each entity similar to a data base (mostly meta data in a database, names and types with out value).

Managed Devices : A managed device or the network element is a part of the network that requires some form of monitoring and management. (**Eg :** Routers, switches, servers, workstations, printers, UPSs, etc.,

SNMP Agent : The agent is a program that is packaged within the network element. Enabling the agent allows it to collect the management information database from the device locally and makes it available to the SNMP manager, when it is queried for. These agents could be standard (**Eg :** Net-SNMP) or specific to a vendor (**Eg :** HP insight agent).

SNMP Agent's Key Functions :

- Collects management information about its local environment.
- Stores and retrieves management information as defined in the MIB.
- Signals an event to the manager.
- Acts as a proxy for some non-SNMP manageable network node.

6.10 REMOTE MONITORING (RMON)

Remote Monitoring (RMON) is a standard specification that facilitates the monitoring of network operational activities through the use of remote devices known as monitors.RMON assists network administrators (NA) with efficient network infrastructure control and management.

RMON was initially developed to address the issue of remote site and local area network (LAN) segment management from a centralized location. The RMON standard specifies a group of functions and statistics that may be exchanged between RMON compatible network probes and console managers. RMON performs extensive network-fault detection and provides performance-tuning data to NAs.

RMON collects nine information types, including bytes sent, packets sent, packets dropped and statistics by host. NAs use RMON to determine network user traffic or bandwidth levels and website access information. Additionally, issue alerts may be preconfigured.

RMON uses certain network devices, such as servers, and contains network management applications that serve as clients. RMON controls the network by using its servers and applications simultaneously. When a network packet is transmitted, RMON facilitates packet status viewing and provides further information, in the event that a packet is blocked, terminated or lost.

REVIEW QUESTIONS

Part-A

1. What are the components of IP addressing ?
2. What are classes of IP address ?
3. List IP Address Classes ?
4. State the need for protocol in computer network ?
5. List the need for Internet protocol version-6 (IPv6) addressing ?
6. What is network management ?
7. What is sub netting ?

Part-B

1. Compare FTP & Telnet
2. What is Simple Network Management Protocol (SNMP)?
3. Write about Remote Monitoring (RMON) ?
4. What is SMTP and FTP ?
5. What are classes in IP address?
6. What is the need of IPV6?
7. What is the need troubleshooting?

Part-C

1. Explain classful addressing and classless addressing in IPv4.
2. Describe about Internet protocol version-6 (IPv6) addressing.
3. Explain how SNMP works.
4. Explain about the following
   (i) HTTP
   (ii) HTTPS
   (iii) FTP
   (iv) SMTP
   (v) Telnet

5. Explain about IP subnetting.
6. Explain about IP Address Classes.
7. Explain the Model of ISO Network Management.
8. Explain about IPV4 address format.
9. Explain about IPV46address format and state the need.
10. What are the tools for troubleshooting?
11. How does SNMP works?
12. What is the purpose of RMON?

BOARD DIPLOMA EXAMINATION

APRIL-2023

COMPUTER HARDWARE AND NETWORKING

IV Semester

Time : 2 Hours Max. Marks : 40

PART – A 8 × 1 = 8

Note : *Answer the following questions. Each question carries* ***One*** *mark.*

1. List the hard disk interfacing standards.
2. What is a Multi-Function Printer?
3. What is simple mail transfer protocol (SMTP)?
4. What is BIOS?
5. What is Hub?
6. What is access point?
7. What is Network trouble shooting?
8. What is TCP?

PART – B 4 × 3 = 12

Note : *Answer the following questions. Each question carries* ***Three*** *marks.*

9. (a) Write about POST.

   (or)

   (b) What is TELNET?

10. (a) List the different Network Topologies.

    (or)

    (b) Briefly explain about subnetting.

11. (a) What is Ethernet?

    (or)

    (b) Write a short note on HTTPS.

12. (a) Describe the purpose of Class D IP address.

    (or)

    (b) Write IPV6 address format.

PART – C

Note : *Answer the following questions. Each question carries* ***Five*** *marks.* $4 \times 5 = 20$

13. (a) Differentiate between Hardware and Software.

    (or)

    (b) Explain Hyper Text transfer Protocol?

14. (a) Explain the working of webcam.

    (or)

    (b) Explain briefly about network troubleshooting tools.

15. (a) Explain the need for protocols in computer networks.

    (or)

    (b) Differentiate between MODEM and ROUTER.

16. (a) Explain ISO network management model.

    (or)

    (b) Explain briefly about RMON.

K.N.K