* Network Model
* Topologies
* Types of networks
* Modes of transmission
* Ip Address
* Transmission media
* troubleshooting commands
* network troubleshooting
* proxy server
* remote desktop
* wireless
* osi model
* tcp/ip model
* protocols

======================================================

* **Types of network models:**

1. Peer to peer model P2P

2. Server client model

* Basics of Networking :

A networking consist of 2 or more computers connected together, and they can communicate and share the resources(eg. information).

* Advantages of networking:

1. Data sharing
2. Hardware devices sharing
3. Working is faster
4. reduces the time
5. we can book ticket online
6. reduce the cost of organization
7. we can do bank transaction sitting from home
8. voice and video chatting and conference
9. communication is faster
10. online shopping

Disadvantages of networking:

**Network models:**

1. Peer to peer model (Workgroup model)
2. client server model(Domain model)

1.Peer to peer model:

Clients and sever are not distinguished

All the nodes are having same permission

Advantages of peer to peer network:

low cost

simple to configure

user has full accessibility of the computer

disadvantages:

may have duplication in resources

difficult to use security policy

difficult to handle

* **Client server model:**

------------------------

there is a specific server and specific clients

all the clients are connected to the server

all the clients are controlled by server

* Advantages of server client model or server based networks:

1. sharing resources
2. security
3. centralized management (users and computers)
4. centralized administration and control
5. easy to maintain the network
6. facility of system backup
7. fault tolerance

* **servers:**

Servers are typically powerful computers that run the software that controls and maintains the network. There are some of the servers which are user to perform a particular task:

1. file servers
2. print servers
3. iis web servers
4. proxy server: used to manage internet user
5. exchange servers
6. dhcp server
7. dns server
8. wds(World distribution system)

* **Types of network:**

Networks are typically classified by the amount of geographical coverage.

1. Local area network
2. Metropolitan area network
3. wide area network

1.Local area network:

a local area network is a group of systems associated in a relatively small area. It connects devices in a limited geographical area using or more hubs or switches.

Lan can also be interconnected within a building.

2.Metropolitan area network:

MAN is the network which interconnects larger computer networks in which two or more computers are connected across a city. This network use wireless infrastructure or optical fiber connections to link thir sites.

Imp Features :

A man typically covers an area of between 5 to 50 km diameters.

A man often acts as a high speed network to allow sharing of resources.

* Wide area network:

Wide area network provides network connectivity over large geographical areas between countries. WAN consists of multiple LANs and MANs in a network over a large geographical area.

* Campus area network(CAN):

A CAN or corporate area network is a network made up of an interconnection of local area networks within a limited area. A campus area network is larger than a local area network.

* **Some other Networks :**

PAN: the smallest type of network you can currently use and the name comes from Personal area network.

SAN: Storage Area network that connects severs to data storage devices with the use of a specific technology

DAN: Desk area network is an interconnection of computer devices using ATM(Asynchronous Transfer Mode).

* **Topology**

The topology of a network

It is a design of network or structure of an network

There are two basic categories of network topologies:

physical topology-how devices are connected to each other

logical topology

* **Physcial topology:**

defines how the nodes of the network are physically connected

It refers to the layout of cabling, the locations of nodes, and the interconnections between the nodes and the cabling.

* **Logical topology:**

how data is transmitted between nodes

It is the way that the data passes through the network from one device to another.

Different types of topologies:

Bus,ring,star, mesh, tree and hybrid.

* **Bus topology:**

A bus topology is multipoint.

Here one long cable act as a backbone all the devices are connected to the backbone cable.

This allows only one device to transmit at a time.

(TV DISH)

* Advantages:

1. ease of installation.
2. less expensive

* Disadvantages:

1. Difficult to add new features.
2. If any fault in the backbone can stops all transmission.

* **Ring Topology**

Here each device has a dedicated connection with two devices on either side.

The signal is passed in one direction from device to device until it reaches the destination.

When one device received signals its repeater then regenerates the data and passes them along.

* Advantages:

1. Easy to install
2. easy to reconfigure
3. fault identification is easy.

* Disadvantages of ring topology:

1. Unidirectional traffic
2. Break in a ring can break entire network.

* **Star Topology:**

Here each device has a dedicated point-to-point link to the central controller called “Hub”.

There is no direct traffic between devices.

The transmission are occurred only through the central “hub”.

(used in LANs

* Advantages:

1. Less expensive then mesh since each device is connected only to the hub
2. Installation and configuration are easy.
3. Less cabling is need then mesh.
4. Robustness.(if one link fails, only that links is affected. All other links remain active.)
5. Easy to fault identification and to remove parts.

* Disadvantages:

1. Dependency(whole dependent on one single point(). When it goes down. The whole system is dead.)

* **Mesh Topology: (Submarine cables)**

A network setup where each computer and network device is interconnected with each another for fault tolerance, which is used in wireless and WAN networks.

* Advantages:

1. It is robust. If any one link get damaged it cannot affect others.
2. Mesh topology is used for redundancy purpose.

* Disadvantages:

1. The amount of cabling and the number of I/O ports required very large.
2. Hardware required to connected each device is highly expensive.

* **Tree Topology:**

Tree topology is one of the most common network setups.

That connects multiple star networks to other star networks in the form of tree structure.

* **Hybrid Topology:**

A network which contain all types of physical structure and connected under a single backbone channel. Combinations of 2 or more different topologies.

* **NETWORKING DEVICES**

Networking devices are components used to connect computers or other electronic devices together so that they can share files or resources.

* Different networking devices:

1. Networking interface card
2. Hub
3. Repeaters
4. Bridges
5. Switch
6. Routers

* NIC:

NIC hardware devices that connect a computer with the network.

Computer data is translated into electrical signals send to the network via network interface cards.

It allows users to connect to each other either by using cables or wirelessly.

Three types of nic card:

1. Wired nic card
2. Wireless nic card
3. Fibre optic nic card

* HUB:

A HUB IS A COMMON CONNECTION POINT FOR DEVICES IN A NETWORK

WORKS AT PHYSICAL LAYER AND HENCE CONNECT NETWORKING DEVIES PHYSICALLY TOGETHER

CONTAINS MULTIPLE PORTS

IT IS BROADCASTING

* ***REPEATER:***

IT IS AN ELECTRONIC DEVICE THAT RECEIVES A SIGNAL AND RETRANSMITS IT. REPEATERES ARE USED TO EXTEND THE SIGNAL TO COVER LONGER DISTANCES.

* BRIDGES:

BRIDGES BUILDS THE CONNECTION WITH THE SAME BRIDGE NETWORKS WHICH USE THE SAME PROTOCOL.

IT OPERATE AT THE DAT LINK LAYER OF THE OSI MODEL.

* SWITCHES:

A SWITCH IS AN INTELLIGENT DEVICE THAT WORKS IN THE DATA LINK LAYER.

THE TERM INTELLIGENT REFERS TO THE DECISION MAKING CAPACITY OF THE SWITCH.

SWITCH IS MULTICASTING.

* ROUTERS:

ROUTERS ARE USED TO COMMUNICATE BETWEEN 2 DIFFERENET NETWORKS

ROUTERS OPERATE AT THE NETWORK LAER OF THE OSI MODEL.

* **DIFFERNECES BETWEEN HUB AND SWITCH:**

|  |  |
| --- | --- |
| **HUB** | **SWITCH** |
| **BROADCASTING** | **MULTICASTING** |
| **PHYSICAL LAYER** | **DATA LINK LAYER** |
| **SLOWER** | **FASTER** |
| **SEND DATA IN BINARY BITS** | **DATA SEND IN FRAMES** |
| **HALF DUPLES** | **FULL DUPLES** |
| **HUBS ARE HAVING LESS PORTS** | **SWITCHES HAVING MORE PORTS** |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| **SWITCH** | **ROUTER** |
| **SAME NETWORK** | **DIFFERENT NETWORK** |
| **DATA LINK LAYER** | **NETWORK LAYER** |
| **DATA TRANSMITTED IN FRAMES** | **IN PACKETS** |
| **LOW COST** | **HIGH COST** |
| **USED IN LAN NETWORKS** | **WAN** |
| **USES MAC ADDRESS** | **USES IP ADDDRESS** |
| **USED FOR CONNECTING 2 OR MORE NETWORKS** | **USED FOR CONNECTING 2 OR MORE NODES IN SAME NETWORK OR DIFFERENT NETWORK** |

* **IPv4 address**

1. It is 32 bit IP address
2. It is having 4 octets
3. It is separated by dot(.)
4. It is in decimal format
5. It support maximum of 2^32
6. Example: 192.168.1.1

Each and every pc or host are identified by IP address. Without IP address in a network 2 pc are unable to connect it is a unique address. It is also known as logical address.

|  |  |  |
| --- | --- | --- |
| Class A | 1-126 | Larger Network |
| Class B | 128-191 | Medium Size Network |
| Class C | 192-223 | Small Networl |
| Class C | 192-223 | Multicasting |
| Class C | 192-223 | Research Develeopment |

Class A

Network Host Host Host

Class B 128-191

Network Network Host Host

Default subnet mask 255.255.0.0

Eg.129.10.0.1

Class C 192-223

Network Network Network Host

Default SM: 255.255.255.0

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Class** | **1st Octet Decimal Range** | **1st Octet High Order Bits** | **Network/Host ID (N=Network, H=Host)** | **Default Subnet Mask** | **Number of Networks** | **Hosts per Network (Usable Addresses)** |
| A | 1 – 126\* | 0 | N.H.H.H | 255.0.0.0 | 126 (27 – 2) | 16,777,214 (224 – 2) |
| B | 128 – 191 | 10 | N.N.H.H | 255.255.0.0 | 16,382 (214 – 2) | 65,534 (216 – 2) |
| C | 192 – 223 | 110 | N.N.N.H | 255.255.255.0 | 2,097,150 (221 – 2) | 254 (28 – 2) |
| D | 224 – 239 | 1110 | Reserved for Multicasting | | | |
| E | 240 – 254 | 1111 | Experimental; used for research | | | |

**Note:** Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback and diagnostic functions.

## Private IP Addresses

|  |  |  |  |
| --- | --- | --- | --- |
| **Class** | **Private Networks** | **Subnet Mask** | **Address Range** |
| A | 10.0.0.0 | 255.0.0.0 | 10.0.0.0 - 10.255.255.255 |
| B | 172.16.0.0 - 172.31.0.0 | 255.240.0.0 | 172.16.0.0 - 172.31.255.255 |
| C | 192.168.0.0 | 255.255.0.0 | 192.168.0.0 - 192.168.255.255 |

Private IP address are not used anywhere on public internet. Which is reserved for private LANs.

APIPA

Automatic private id address it is also called as link local address

Client machine can automatically self configure an ip address when dhcp is not working.

APIPA range:

169.254.0.1 to 169.254.255.254

|  |  |
| --- | --- |
| HEXADECIMAL | BINARY |
| 0 | 0000 |
| 1 | 0001 |
| 2 | 0010 |
| 3 | 0011 |
| 4 | 0100 |
| 5 | 0101 |
| 6 | 0110 |
| 7 | 0111 |
| 8 | 1000 |
| 9 | 1001 |
| A | 1010 |
| B | 1011 |
| C | 1100 |
| D | 1101 |
| E | 1110 |
| F | 1111 |
|  |  |

**OSI**

|  |
| --- |
| **Application** |
| **Presentation** |
| **Session** |
| **Transport** |
| **Network** |
| **Data Link** |
| **Physical** |

**Application Layer:**

**AP is responsible for providing networking services to the user. It is also known as Desktop Layer. Identification of Services is done using Port Numbers.**

**Ports are entry and exit points to the layer.**

Resources sharing, remote file accessing , remote printer access, directory service, network management

**Total no. ports: 0-65536**

**Reserved Ports: 0-1023**

**Open client ports: 1024-65535**

**Presentation Layer:**

**PL is responsible for converting data into standard format.**

**Examples: ASCII, EBCDIC, JPED, MPEG, BMP, MIDI, WAV, MP3**

**Following tasks are perform at presentation layer:**

* **Encoding – Decoding**
* **Encryption – Decrypting**
* **Compression – Decompression**
* **Data conversion, data compression, data encryption, decryption**

**Session Layer:**

**SL is responsible for establishing, maintaining and terminating session.**

**Session ID works at SL.**

Session Establishment, maintenance, termination, session support, perform security, logging etc.

**Examples:**

**RPC -> remote procedure call**

**SQL -> Structured query language**

**NFS -> Network file system**

**Transport Layer:**

**TL is responsible for end-to-end connectivity. It is also known as the heart of OSI layers.**

**Following tasks are performed at the TL:**

Message segmentation, acknologement and message traffic control

* **Identifying service**
* **Multiplexing and de – mul**
* **Segmentation**
* **Sequencing and reassembling**
* **Error correction**
* **Flow control**

**Network Layer:**

**NL is responsible for providing best path for data to reach the destination. Logical Addressing works on this layer. Router is Network layer device.**

**It is divided into two parts**

* **Routed protocols**

**Eg. IP, IPX, Apple talk**

* **Routing protocols**

**Eg. RIP, IGRP, OSPF, EIGRP**

**Data Link Layer:**

**DLL is divided into two sub layers:**

* **LCC- Logical Link control**

**It talks about wan protocols eg. PPP, HDLC, Frame-relay**

**Frame traffic control, frame sequencing, fram acknowledgement, frame error checking.**

* **MAC- Media Access Control**

**It talks about physical address.**

**It is a 48 bit address i.e. 12 digit hexadecimal number.**

**It is also responsible for error detection.**

**Devices working on data link layer are switch, bridge, NIC**

**Physical Layer:**

**PL is responsible for electrical, mechanical and procedural checks. Data will be converted into binary.**

**Data will be in the form of electrical pulses if it is coaxial or twisted pair cable and in the form of light it it is fiber optic cable.**

**Devices working at physical layer are hubs, repeaters, cables, modems etc**

Data encoding, transmission technique – baseband or broadband, physical medium transmission.

=============================l====================================================

|  |
| --- |
| A |
| P |
| S |
| T |
| N |
| D |
| P |
|  |
|  |

|  |
| --- |
| Data |
| Data |
| Data |
| Segment |
| Packet |
| Frame |
| Bits |

Data flow from layer: PDU-Protocol Data Unit

**TCP**

|  |
| --- |
| **Application** |
| **Presentation** |
| **Session** |
| **Transport** |
| **Network** |
| **Data Link** |
| **Physical** |

|  |
| --- |
| **Application** |
| **Transport** |
| **Internet** |
| **Network**  **Acess** |

**Differences btw OSI and TCP/IP:**

**OSI model has seven layers**

**TCP has 4 layers**

**OSI model provides clear distinction between services, interfaces and protocols.**

**TCP/IP doesn’t provide clearly distinguish between services, interfaces and protocols.**

**In OSI Data link layer and physical layer are separate layers.**

**In TCP/IP DLL and PL are combines as Network Access Layer.**

PROTOCOLS:

Protocols is a set of rules describes how data is transmitted over a network

Protocols are needed for communication between any two devices.

TCP/IP Protocol Suite

* TCP/IP does not have an official layer structure
* Actually tcp/ip reference model has been built on its protocols.
* Transmission control protocol

Connection oriented

Reliable delivery of data

Ordering of delivery

* User datagram protocol

Connectionless service

Delivery is not guaranteed

Protocol Port number

|  |  |
| --- | --- |
| TCP |  |
| FTP | 20,21 |
| SSH | 22 |
| TELNET | 23 |
| SMTP | 25 |
| HTTP | 80 |
| POP3 | 110 |
| NTP | 123 |
| IMAP4 | 143 |
| HTTPS | 443 |

|  |  |
| --- | --- |
| UDP | 53 |
| DHCP | 67 |
| TFTP | 69 |
| SNMP | 161 |
|  |  |

* FILE TRANSFER PROTOCOLS:

WHICH ARE USED TO UPLOAD AND DOWNLOAD THE FILES.

* TELNET

FOR REMOTE LOGGING OR ACCESSING WITHOUT SECURITY

* SSH SECURE SHELL

FOR REMOTE ACCESSIG WITH SECURITY

* SMPT

USED TO SEND THE MAILS

* HTTP

TO ACCESS WEBSITE

* POP3

WHICH USED TO RECEIVE THE MAIL

* NTP

NETWORK TIME PROTOCOL USED TO CENTRALIZED ALL THE DEVICE AT SAME TIME.

OR MANAGED STANDARD TIME IN ORGANIZATION

* IMAP4

INTERNET MESSAGE ACCESS PROTOCOL USED TO MANAGE ALL THE MAILS CENTRALIZED USING MAIL SERVER

* HTTPS

HTTP SECURED USED FOR SECURED ACCESS OF WEBSITE (FOR CONFIGURING FIREWALL)

* DNS

DOMAIN NAMING SERVICES OR SYSTEM USED TO RESOLVE NAME TO IP OR IP TO NAME.

* DHCP

USED TO ASSIGN IP TO CLIENT AUTOMATICALLY.

* TFTP

TRIVAL FILE TRANSFER PROTOCOL IS SECURED FILE TRANSFER PROTOCOL.

* SNMP

SIMPLE NETWORK MANAGEMENT PROTOCOLS

USED TO MANAGE THE NETWORK OR MONITORING THE NETWORK

COMMUNICATION MODES:

THE COMMUNICATION MODES REFER TO THE MANNER IN WHICH THE TWO DEVICES IN A NETWORK COMMUNICATE WITH EACH OTHER

THER ARE THREE DIFFERENET MODES OF COMMUNICATION

1. SIMPLEX COMMUNICATION
2. HALF DUPLEX COMMUNICATION
3. FULL DUPLEX COMMUNICATION

* SIMPLEX

COMMUNICATIN CHANEEL CAN TRANSFER DATA IN ONLY ONE DIRECTION.

* HALF

THE HALF DUPLEX MODE CMMUNICATIN CAN SEND THE DATA IN BOTH DIRECTIONS BUT NOT SIMULTANEOUSLY. IT CAN EITHER USE THE COMMUNICATION CHANNEL TO SEND THE DATA OR THE SAME CHANNEL CAN BE USED TO RECEIVE THE DATA AT A TIME

WALKIE TALKIES ARE THE BEST EXAMPLES.

* FULL

THE FULL DUPLEX COMMUNICATIN PERMITS DATA TO BE SENT AND RECIVED BY THE SAME COMMUNICATION CHANNEL SIMLUTANEOUSLY.

THE FULL DUPLEX COMMUNICATION CAN BE COMPARED TO A TWO WAY BRIDGE ON A TWO LANE HIGHWAY

TELEPHONE IS THE BEST EXAMPLE.

MESSAGING TYPES

THERE ARE DIFFERENT KINDS MESSAGES WHICH HAVE TO BE SENT FROM ONE DEVICE TO ANOTHER NETWORK.

UNICAST

MULTICAST

BROADCAST

ANYCAST- ONE TO NEAREST

**UNICAST: ONE TO ONE**

UNICAST IN THE COMMUNICATION BETWEEN A SINGLE SENDER AND A SINGLE RECIVER THROUGH THE NETWORK

**MULTICAST: ONE TO MANY**

MULTICAST IS THE DELIVERY OF INFORMATION TO A GROUP OF DESTINATION SYSTEM SIMULTANEOUSLY USING THE MOST EFFICIENT STRATEGY TO DELIVER THE MESSAGES OVER EAC LINK OF THE NETWORK.

**BROADCAST : ONE TO ALL**

BROADCAST IS USED TO SEND THE INFORMATION FROM ONE SOURCE TO MULTIPLE SYSTEMS. ONE SENDER SENDS THE INFORMATION TO ALL CONNECTED RECIVERS. BROADCST TRANSMISSION IS SUPPORTED ON MOST LANs AND CAN BE USED TO SEND MESSAGES TO ALL COMPUTERS ON THE LAN.

**TRANSMISSION MEDIA**

THE TRANSIMISSIN MEDIA IS THE PHYSICAL PATH BETWEEN TRANSMITTER AND RECIVER IN A DATA TRANSMINSSION SYSTEM.

TYPES OF TRANSMISSION MEDIA

1. GUIDED MEDIA

* TWISTED PAIR
* CO-AXIAL CABLES
* OPTIC FIBRES

1. UNIGUIDED MEDIA

* INFRARED
* MICROWAVES
* BLUTOOTH

**GUIDED TRANSMISSION MEDIA:**

THE WAVES ARE GUIDED ALONG A SOLID MEDIUM SUCH AS

* TWISTED PAIR
* CO-AXIAL CABLES
* OPTIC FIBRES
* TWISTED PAIR CABLE:

INFORMATION ISTRANSMITTED BY SENDING ELECTRICAL CURRENT THROUGH THE WIRES.

THE TWISTING TENDS TO DECREASE THE CROSS TALK INTRFERENCE BETWEEN ADJACENT PAIRS.

2 TYPES OF TWISTED PAIR CABLE:

UTP(UNSHIELDED TWISTED PAIR) AND STP(SHIELDED TWISTED PAIR)

UTP AND STP ARE DIVIDED INTO CATEGORIES:

CAT 1

2

3

4

FIRST 4 CAT ARE TELEPHONE LINES

5

6

7

8

ABOVE 4 CAT ARE NETWORKING

AGAIN THE ABOVE CAT ARE DIVIDED INTO 2 TYPES

STRAIGHT THROUGH CABLE

CROSS OVER CABLE

COLOR CODE FOR STRAIGHT THROUGH CABLE

WHITEORANGE ORANGE WHITEGREEN BLUE WHIITEBLUE GREEN WHITEBROWN BROWN

SAME ON BOTH SIDES.

CROSSOVER CABLE COLOR CODE:

WG WO

G O

WO WG

B B

WB WB

O G

WBR WBR

BR BR

568A 568B

**SAME DEVICES WE USE CROSS OVER CABLE WHEREAS DIFFERENT DEVICES WE USE STRAIGHT THROUGH CABLE. BUT TO CONNECT PC AND ROUTER WE USE CROSS OVER CABLE AND CONSOLE CABLE OR ROLLOVER CABLE.**

COAXIAL CABLE

COAXIAL CABLE IS USED TO TRANSMIT BOTH ANALOG AND DIGITAL SIGNALS

CARRY HIGHER FREQUENCIS AND MUCH DATA RATES

LESS INTERFERENCE AND CROSS TALK THAN TWISTED PAIR

FOR LONG DISTANCE TRANSMISSION OF ANALOG SIGNALS AMPLIFIERS ARE NEEDED EVER FEW KILOMETERS

2 TYPES:

THINNET CABLE

THICKNET CABLE

COAXIAL CABLE:

WIDELY INSTALLED FOR USE IN BUSINESS AND CORPORATION ETHERNET AND OTHER TYPES OF LANs.

CONISISTS OF INTER COPPER INSULATOR COVERED BY CLADDING MATERIAL, AND THEN COVERED BY AN OUTER JACKET.

PHYSICAL DESCRIPTIONS:

* INNER CONDUCTOR IS SOLID COPPER METAL
* SEPERATED BY INSULATING MATERIAL
* OUTER CONDUCTOR IS BRAIDED SHIELDED(GROUND)
* COVERED BY SHEATH MATERIAL

PLASTIC LIKE MATERIAL, USED TO SEPARATE THE INNER CONDUCTOR FROM THE OUTER THE CONDUCTOR.

THE OUTER CONDUCTOR IS A FINE CYLINDRICAL MESH MADE FROM COPPER.

DIAMETER 0.4 TO ABOUT 1-INCH.

APPLICATIONS:

TV DISTRIBUTION(CABLE TV), LONG DISTANCE TELEPHONE TRANSMISSION

**OPTICAL FIBRE:**

TRANSMIT LIGHT SIGNALS INNER CORE OF GLASS OR PLASTIC THAT

THE OUTER MOST LAYER IS THE JACKET. THIS JACKET IS COMPOSED OF PLASTIC

50 MICRONS IN DIAMETER.

TWO TYPES OF FIBRE OPTIC CABLE:

1. SIGNLE MODE :SINGLE SIGNAL IS TRANSMITTED
2. MULTI MODE

MULTIMODE FIBER IS OPTICAL FIBER THAT IS DESIGNED TO CARRY MULTIPLE LIGHT RAYS OR MODES CONCURRENTLY EACH AT A SLIGHTLY DIFFERENT REFLECTION ANGLE WITHIN THE OPTICAL FIBER CORE USED FOR RELATIVELY SHORT DISTANCES BECAUSE THE MODES TEND TO DISPERSE OVER LONGER LENGHTS (THIS IS CALLED MODAL DISPERSION)

FOR LONGER DISTANCES, SINGLE MODE FIBER (SOMETIMES CALLED MONOMODE) FIBER IS USED. IN SINGLE MODE FIBER A SINGLE RAY OR MODE OF LIGHT ACT AS A CARRIER.

**UNGUIDED TRANSMISSION MEDIA:**

INFRARED LIGHT IS ELECTROMAGNETIC RADIATION WITH A WAVELENGTH LONGER THAN THAT OF VISIBLE LIGHT.

BLUETOOTH:

BLUETOOTH IS WIRELESS PROTOCOL FOR EXCHANGING DATA OVER SHORT DISTANCES FROM FIXED AND MOBILE DEVICES, CREATING PERSONAL AREA NETWORK (PAN).

**NETWORK TROUBLESHOOTING COMMANDS:**

1. PING
2. TRACERT
3. IPCONFIG
4. IPCONFIG /ALL
5. PING IPADDRESS –T
6. NETSTAT
7. NETSH WINSOCK RESET (FOR RESETTING NIC CARD)

WIRELESS SYSTEMS:

* CELLULAR SYSTEM
* WIRELESS LANs
* SATELLITE SYSTEM
* PAGING SYSTEM
* PANs (BLUETOOTH)

THE WIFI TECHONOLOGY

WIFI NETWORKDS USE RADIO TECHNOLOGIES TO TRANSMIT AND RECIVE DATA AT HIGH SPEED.

IEEE 802.11B

11A

11G

**IEEE 802.11b:**

* APEAR IN LATE 1999
* OPERATES AT 2.4GHz RADIO SPECTRUM
* 11 MBPS(THOERETICAL SPEED) WITHIN 30 M RANGE
* 4-6 MBPS (ACTUAL SPEED)
* 100-150 FEET RANGE
* MOST POPULAR, LEAST EXPENSIVE
* INTERFERENCE FROM MOBILE PHONES AND BLUETOOTH DEVICES WHICH CAN REDUCE THE TRANSMISSION SPEED.

**IEEE 802.11a:**

* INTRODUCE IN 2001
* OPERATES AT 5 GHz (LESS POPULAR)
* 54 MBPS(THOERETICAL SPEED)
* 15-20 MBPS (ACTUAL SPEED)
* 50-76 FEET RANGE
* MORE EXPENSIVE
* NOT COMPATIBLE WITH 802.11B

**IEEE 802.11g:**

* INTRODUCE IN 2003
* COMBINE THE FEATURE OR BOTH STANDARDS (a,b)
* 2.4 GHz RADIO FREQUENCIES
* 54 MBPS
* 100-150 FEET RANGE
* COMPATIBLE WITH ,**b** “

**WIFI NETWORK TOPOLOGIES:**

1. PEER-TO-PEER TOPOLOGY ( AD-HOC MODE)
2. AP-BASED TOPOLOGY (INFRASTRUCTURE MODE)

**PEER TO PEER TOPOLOGY:**

AP IS NOT REQUIRED.

CLIENT DEVICES WITHIN A CELL CAN COMMUNICATE WITH EACH OTHER DIRECTLY

IT IS USEFUL FOR SETTING UP A WIRELESS NETWORK QUICKLY AND EASILY.

**INFRASTRUCTURE NETWORK:**

THE CLIENT COMMUNICATE THROUGH ACESS POINT

ANY COMMUNICATION HAS TO GO THROUGHT AP.

IF A MOBILE STATION (ms) LIKE ACOMPUTER, A PDA OR A PHONE WANTS TO COMMUNICATE WITH ANOTHER MS , IT NEEDS TO SEND THE INFORMATION TO AP FIRST, THEN AP SENDS IT TO THE DESTINATION MS.

How a wifi network works:

A wifi hot sopt is created by installing an acesspoint to an internet connection.

An access point acts as a base station

When wifi enabled device encounters a hotspot the device can then connect to that network wirelessly.

Asingle access point can support up to 30 users and can function within a range a 100 – 150 feet indoors and up to 300 feet outdoors.

Many access points can be connected to each other via Ethernet cables to create a single large network.

**SSID**

Service set identifier

32 bit character unique name

Identifier wireless network

Ssid differentiate one WLAN from other

All access points and wifi devices are able to connect to wlan using SSID.

**Wireless Security:**

1. WEP wired equivalent privacy

Used 64 bit or 128 bit encryption

1. WPA wifi protected access

To avoid weakness in WEPWPA is introduced in 2003