200 Level- BSc. Cybersecurity

Kulugh Victor Emmanuel
Department of Computer Science, Bingham University, Karu, Nigeria

CYB 202 - Systems and Network Administration

Part A: Systems Administration – Definitions

A Systems Administrator (SA) - is an experts who ensures that all software and hardware systems functions properly to achieve organisation’s goals. SAs deal with physical computer servers, other hardware and software infrastructure. They provide support to users that need to access IT resources within the organisation’s ICT infrastructure. The Specific Duties of a System Administrator are outlined thus:

Systems Administration – Duties

i. User Accounts Management: User IDs, emails, group membership, permissions and restrictions, communicating policies and procedures, disabling/removing users

ii. Hardware Management: Capacity planning, inventory, hardware evaluation and purchase, device driver installation, systems configurations and settings, user notifications and documentation.

iii. Data Backups: Disk and backup media planning, disaster recovery (onsite/offsite, periodic testing, multiple copies, user communications/assurance (restore guarantees and procedures, loss tolerance).

iv. Software Installation/Maintenance: Evaluation of software, download and building, installation, maintenance of multiple versions, security, patches and updates, user notification and documentation

v. System Monitoring: hardware and services, capacity (RAM, Disk, CPU, network), security (passwords, break-ins), systems logs.

vi. Troubleshooting: problem discovery, diagnosis and resolution.

vii. Local documentation: administrative policies and procedures (backup media locations, hardware description, configuration, connections and location, software – install location/media, installation and configuration details, patches and update installed); **Acceptable use policies**

viii. Security concerns: systems login and audit, unexpected/unauthorised use detection, monitoring of security advisories.

ix. User assistance: help desks, trouble-ticket systems, systems (hardware/software availability), etc.

Network Administration – definition

Network administrators (NA) is an ICT expert who’s role is to build computer networks and ensure continuous connectivity and availability of the networks. An NA focuses on setting up network equipment and ensuring that their network infrastructure can support user activities within the organisation. They also monitor overall activity and demands on the network, identify vulnerabilities, threats and strange traffic on the network.

Network Administration – Duties

i. Network design – planning the implementation of the network infrastructure.

ii. Research and select and order network hardware – E.g network cables, routers, switches, etc based on requirements with respect to the design

iii. Configuring/installing and testing network equipment – Linking the physical network devices and logically connecting them to be able to communicate.

iv. Troubleshooting and Maintenance of network infrastructure- diagnosing problems, establishing the root cause(s) and resolving them.

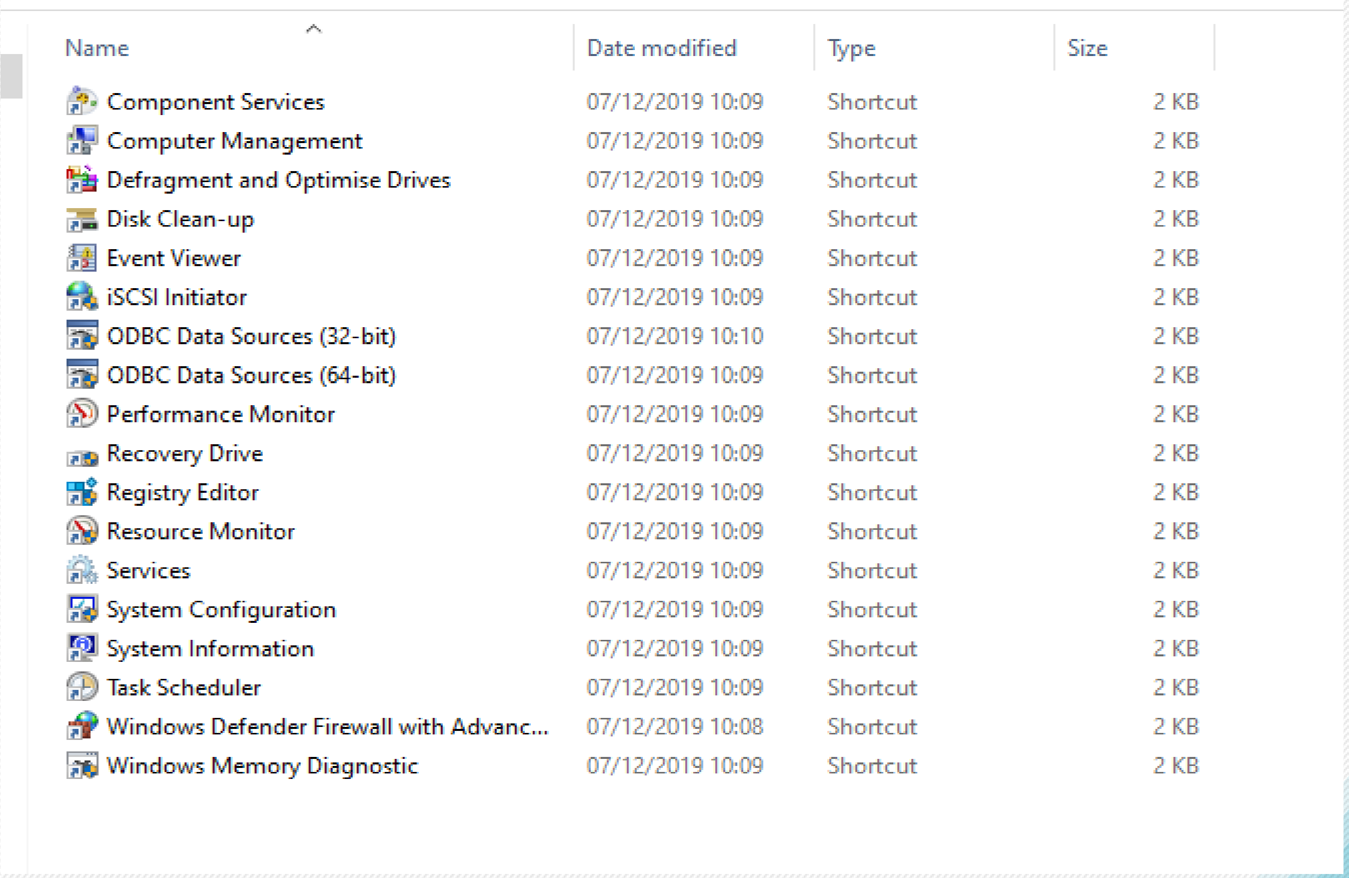
v. Monitoring Network activities – Observing user activities and network loads to proactively identify and resolve potential problems that may result

vi. Setting up firewalls – set up fire walls to secure the network from unauthorised traffic and users.

vii. Respond to and fix network outages- when users report network downtimes, NAs ensure resolution.

System Administration Tools

For systems administrators to perform their functions, they require a set of tools built into the operating system upon which their system run. E.g, Linux/Unix, windows. etc. Here we review some administrative tools for windows.



Name	Date modified	Type	Size
Component Services	07/12/2019 10:09	Shortcut	2 KB
Computer Management	07/12/2019 10:09	Shortcut	2 KB
Defragment and Optimise Drives	07/12/2019 10:09	Shortcut	2 KB
Disk Clean-up	07/12/2019 10:09	Shortcut	2 KB
Event Viewer	07/12/2019 10:09	Shortcut	2 KB
iSCSI Initiator	07/12/2019 10:09	Shortcut	2 KB
ODBC Data Sources (32-bit)	07/12/2019 10:10	Shortcut	2 KB
ODBC Data Sources (64-bit)	07/12/2019 10:09	Shortcut	2 KB
Performance Monitor	07/12/2019 10:09	Shortcut	2 KB
Recovery Drive	07/12/2019 10:09	Shortcut	2 KB
Registry Editor	07/12/2019 10:09	Shortcut	2 KB
Resource Monitor	07/12/2019 10:09	Shortcut	2 KB
Services	07/12/2019 10:09	Shortcut	2 KB
System Configuration	07/12/2019 10:09	Shortcut	2 KB
System Information	07/12/2019 10:09	Shortcut	2 KB
Task Scheduler	07/12/2019 10:09	Shortcut	2 KB
Windows Defender Firewall with Advanc...	07/12/2019 10:08	Shortcut	2 KB
Windows Memory Diagnostic	07/12/2019 10:09	Shortcut	2 KB

Assignment
Access the windows administrative tools for your version of windows from the control panel and explain the application of each of these tools.

To be submitted via email

gwaza.kulugh@gmail.com

Submission is on Monday, 23rd May, 2022

Disk Management and File Types

Disk Management is one of the advanced utilities in different versions of windows that enables SAs to perform different storage management task. The disk management utility can be accessed from the control panel or at the command prompt via the diskmgt.msc command.

i. Initializing new drive – activates a newly inserted disk that the system did not automatically recognise. Disk initialisation erases previously stored data on disk.
ii. Extend a basic volume – extending empty space on the drive that do not have previous volume.
iii. Shrink a basic volume -
iv. Change drive label (letter) – provide labels for
v. Partition drive
vi. Format drive
vii. Mirror drive – creating redundancy that enables the content a drive automatically copied on another
viii. Defragment drive – Opitimize drive by removing empty spaces between file and pushing them to the end.
ix. Create storage pool – combining several drives on a system into a single space to form a storage pool.

Part B: Network Administration – Definitions

Network

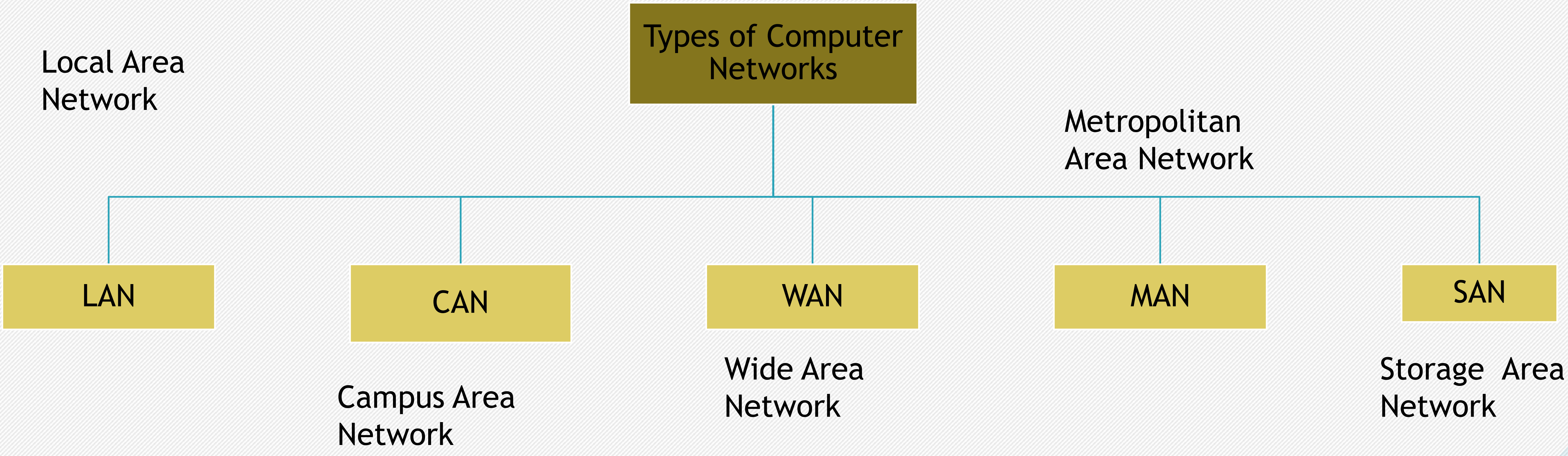
- A network is a connection of two or more computing devices through a media.

- internetwork: Is the interconnection of two or more networks to form a bigger network.

Benefits of a Computer Network:

- Cost-effective resource sharing.
- Improving storage efficiency and volume.
- Access flexibility.
- Cut costs on software.
- Utilize a Centralized Database.
- Securing valuable information.

Types of Networks – cont’d



Types of Computer Networks

LAN

CAN

WAN

MAN

SAN

Local Area Network

Campus Area Network

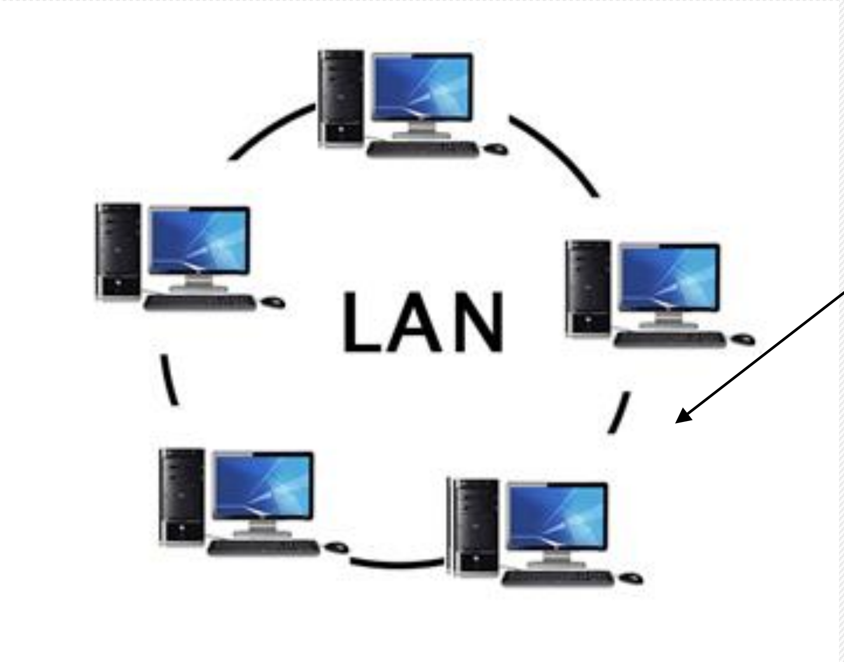
Wide Area Network

Metropolitan Area Network

Storage Area Network

Types of Networks – LAN

LAN is a group of computers connected to each other in a small area such as building or an office. Communication in LAN is through medium such as twisted pair, coaxial cable, etc. it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables. Data transferred rate is extremely fast in LAN and provides higher security.



Local Area Network

Types of Networks – CAN

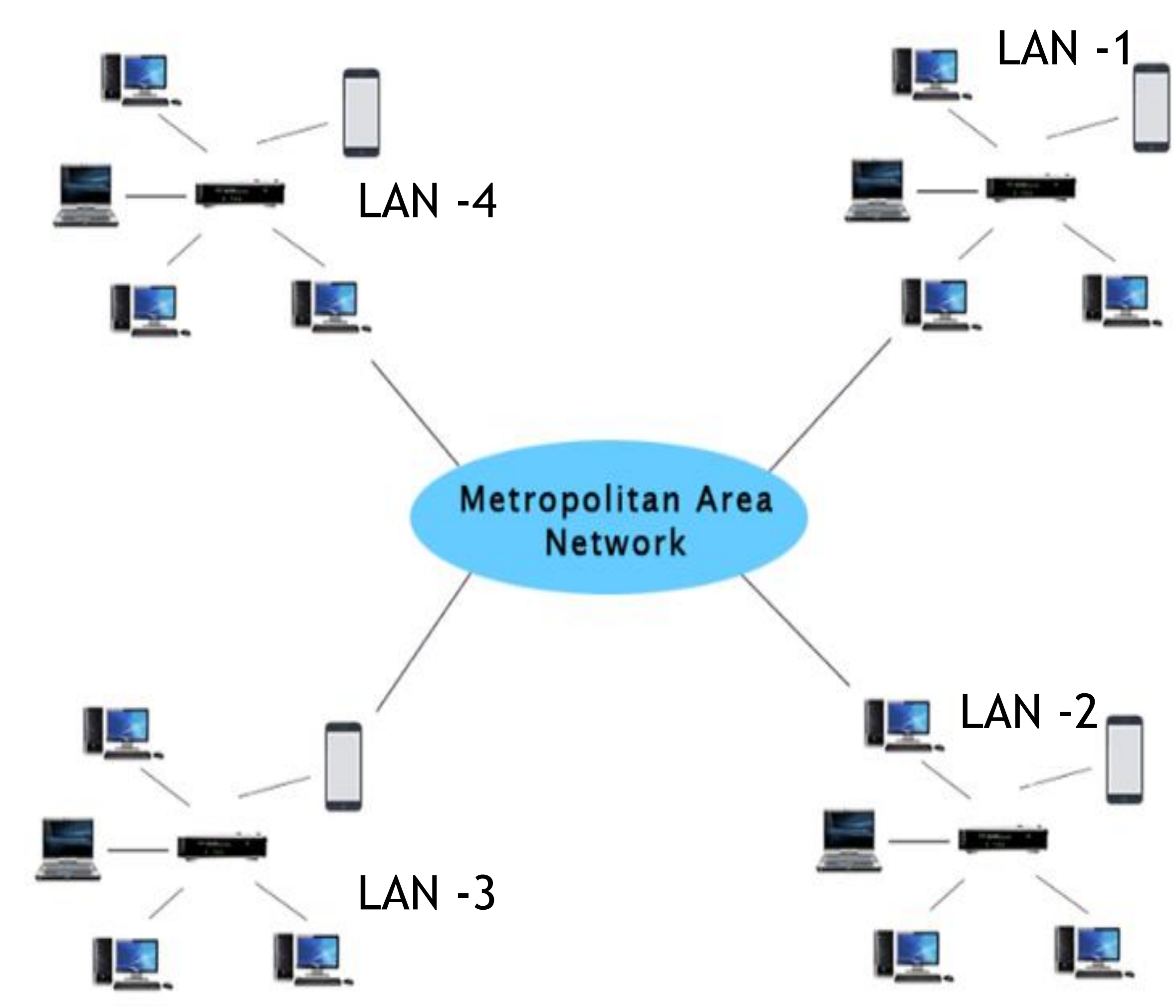
CAN is a network that spans a limited geographic area, usually;

bigger than a LAN but smaller than the WAN and MAN.

- CANs interconnect multiple LANs within an educational or corporate campus.
- Unlike LANs, most CANs connect to the public Internet.
- Typically, the organization that owns the campus also owns and operates all the networking equipment and infrastructure for the CAN.
- In contrast, MANs and WANs may combine infrastructure operated by several different providers.

Types of Networks – MAN

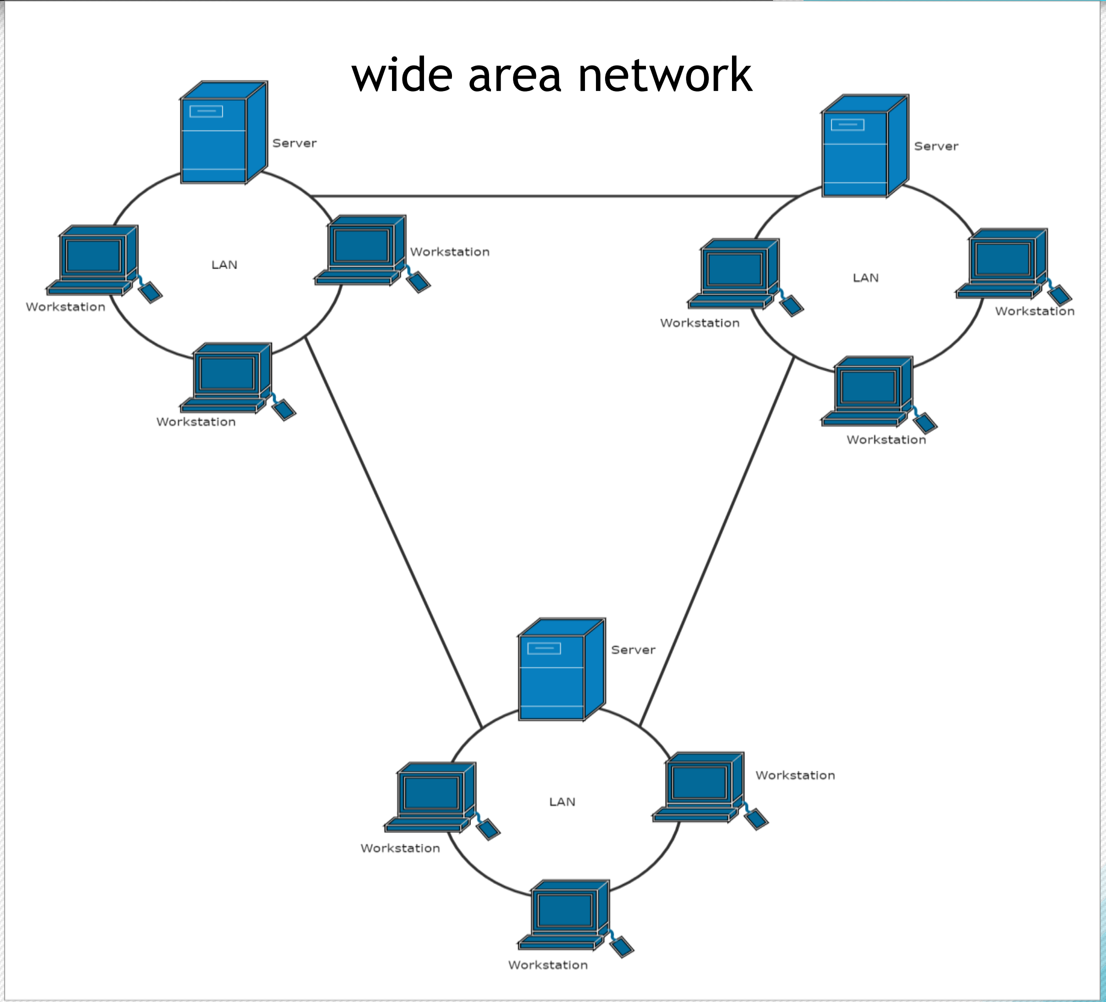
MAN is a network that covers a larger geographic area, like an entire city or metropolis. It is formed by connecting several LANs through telecommunication infrastructure (telephone exchange line). Data transmission rate is not as fast as in LAN and is less secured compared to LAN



Types of Networks – WAN

WAN is a network that extends over a large geographical area such as across cities, states or countries. It is bigger than LAN and MAN and involves the connection of several LANs/MANs via telephone line, fibre optic cable or satellite links, etc. WAN is used in business, government, education, etc.

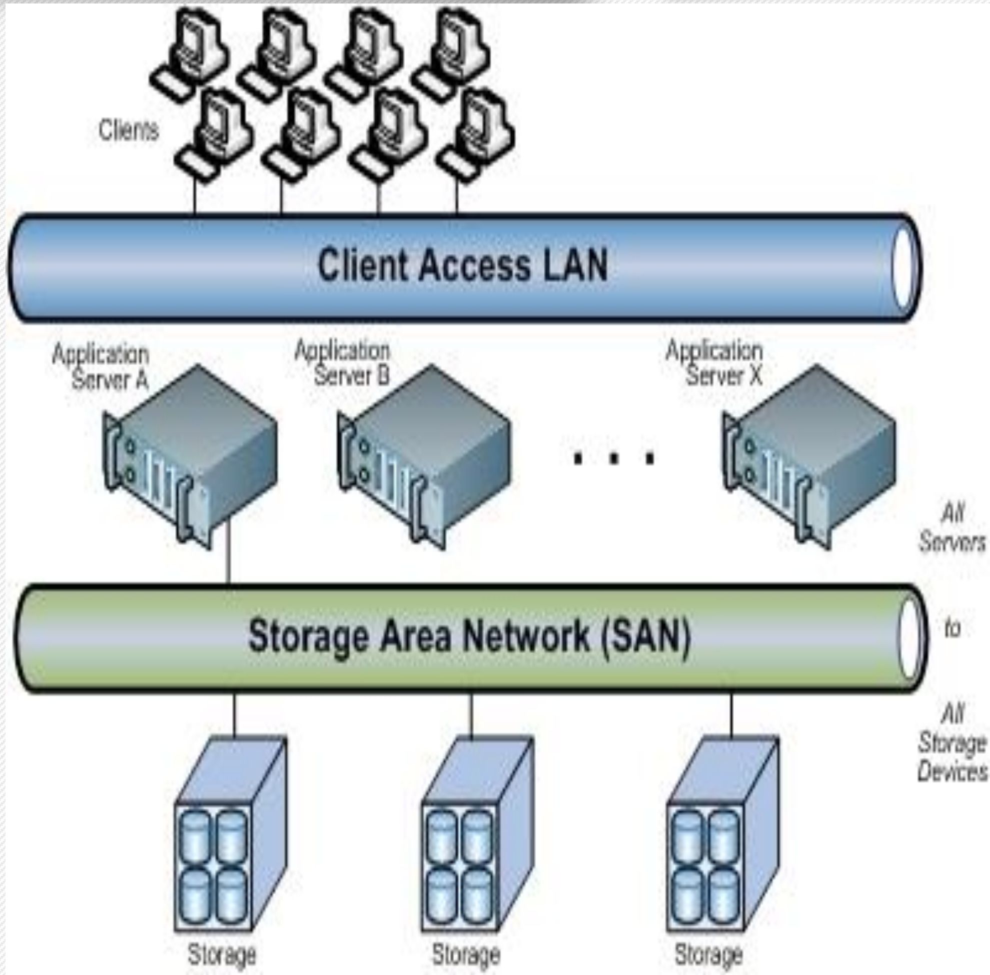
The internet is one of the biggest WAN in the world.



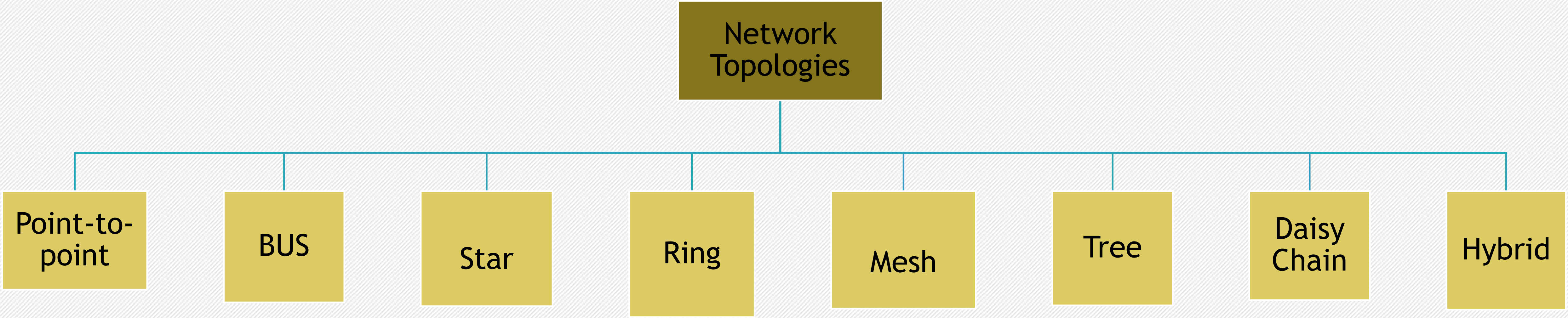
Types of Networks – SAN

SAN is a specialized, high-speed network that provides network access to storage devices. They composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols.

SAN presents storage devices to a host in a manner that the storage appears to reside on the host.



Network Topologies



Network Topologies

Point-to-point

BUS

Star

Ring

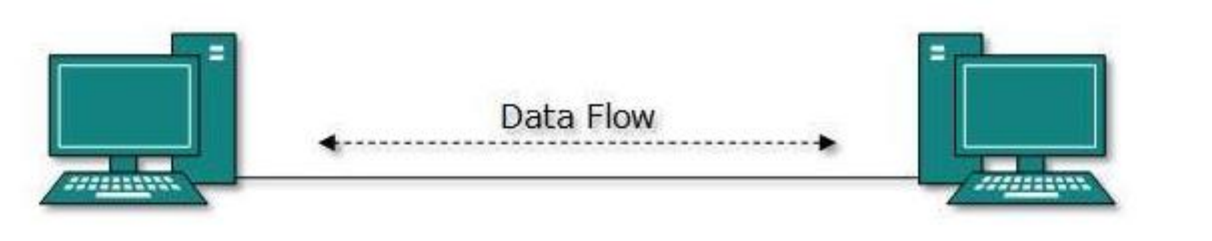
Mesh

Tree

Daisy Chain

Hybrid

Network Topology - point-to-point

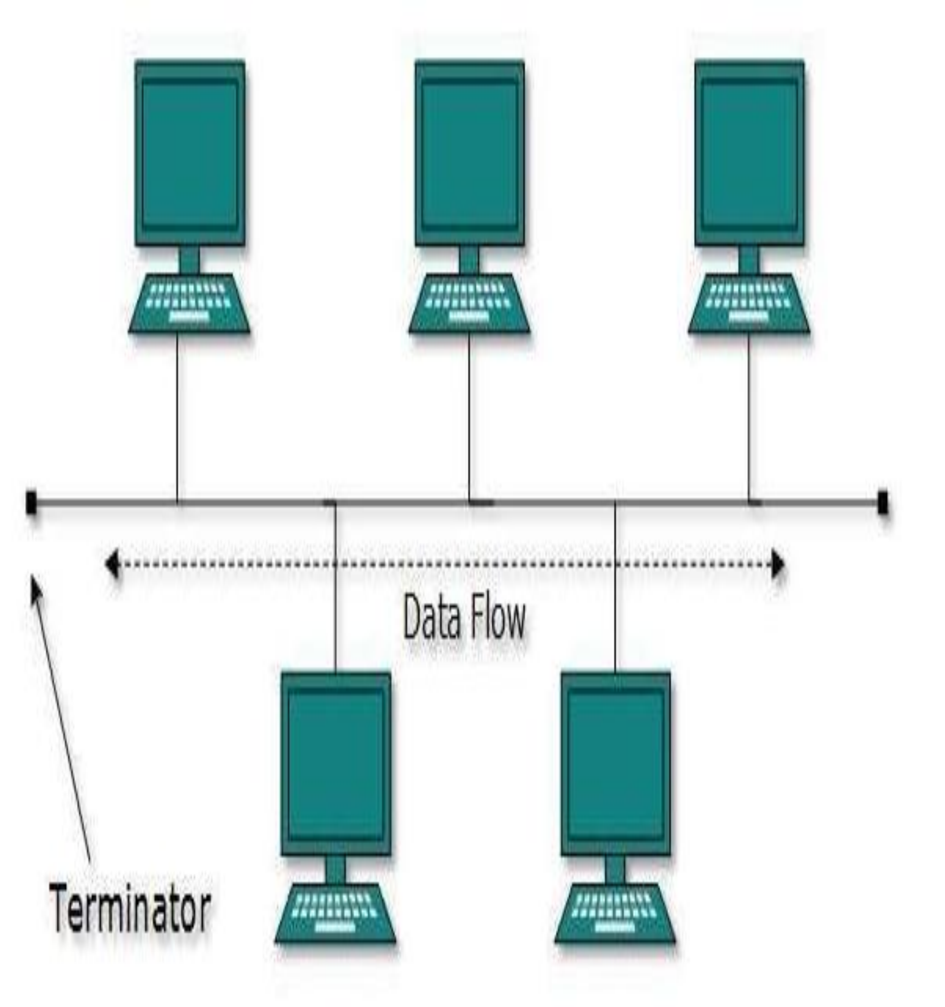


Point-to-point networks contains exactly two hosts such as computer, switches or routers, servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice-versa.

If the hosts are connected point-to-point logically, they may have multiple intermediate devices. But the end hosts are unaware of underlying network and see each other as if they are connected directly.

Network Topology – Bus

- All connected nodes share single communication line.
- There is problem of collision when multiple hosts send data at the same time.
- To resolve this problem, Bus topology uses:
- CSMA/CD technology,
- or recognizes one host as Bus Master.
- Failure of one node does not affect the other devices.
- However, failure of the shared communication line can disrupt the entire network



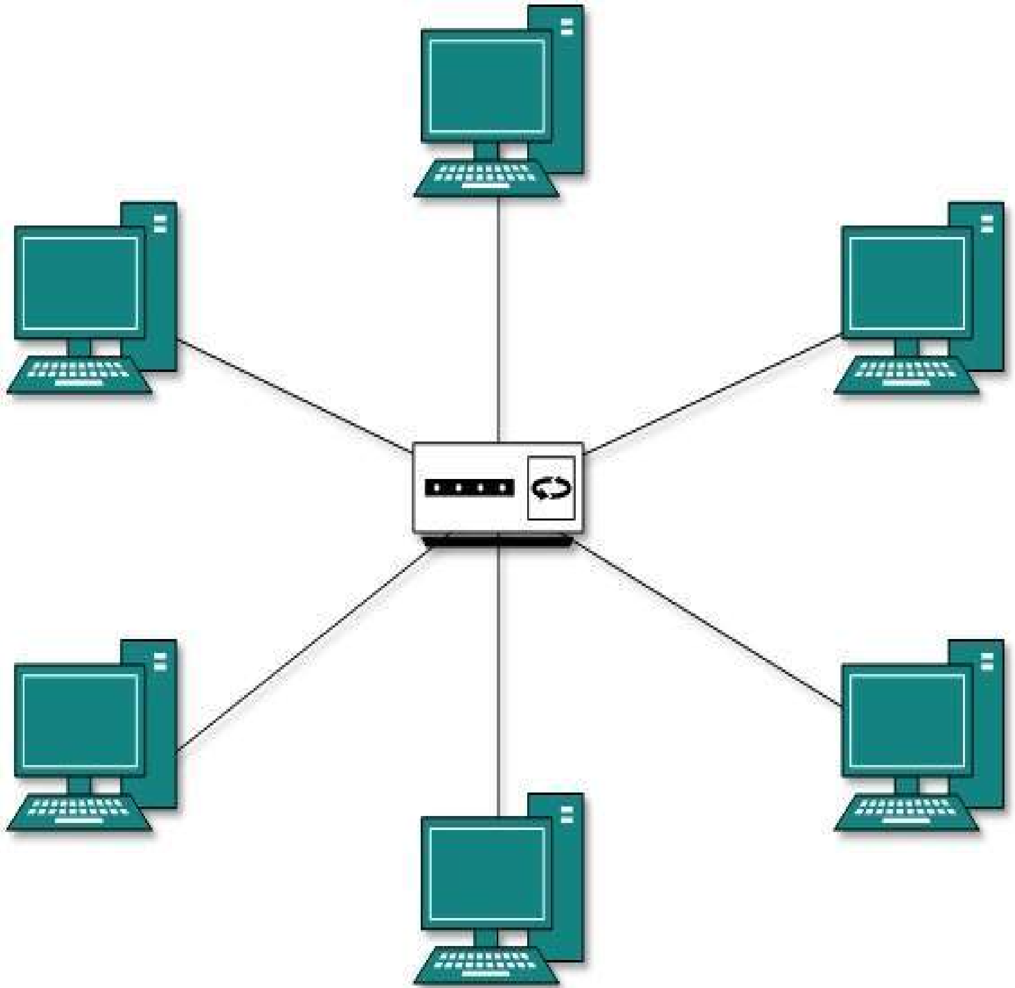
Network Topology – star

All hosts in Star topology are connected to a central device. The hub device can be any of the following: hub or repeater; switch or bridge; router or gateway

As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails.

Communication between hosts takes place through only the hub.

Star topology is inexpensive, to connect one more host, only one cable is required and configuration is simple.

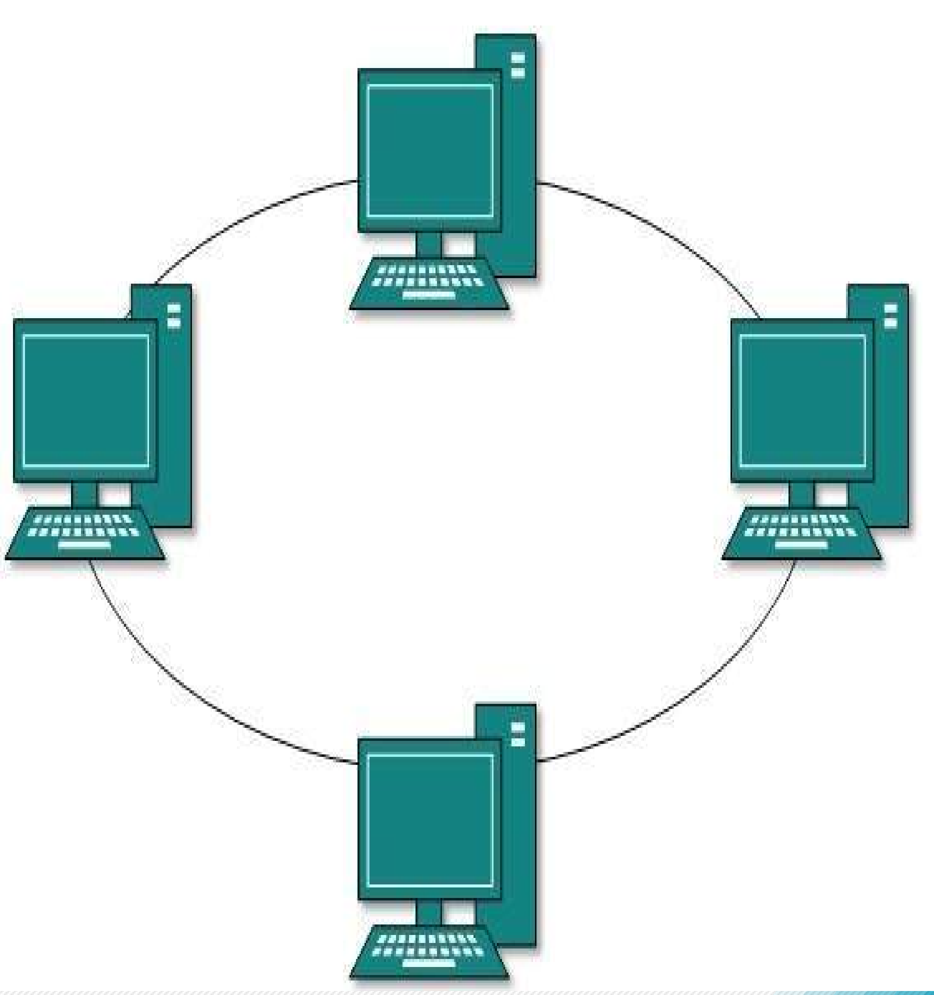


Network Topology - Ring

In ring topology, each node connects to exactly two other nodes, creating a circular network structure.

When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable.

Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure. To resolve this point of failure issue, one more backup ring is used



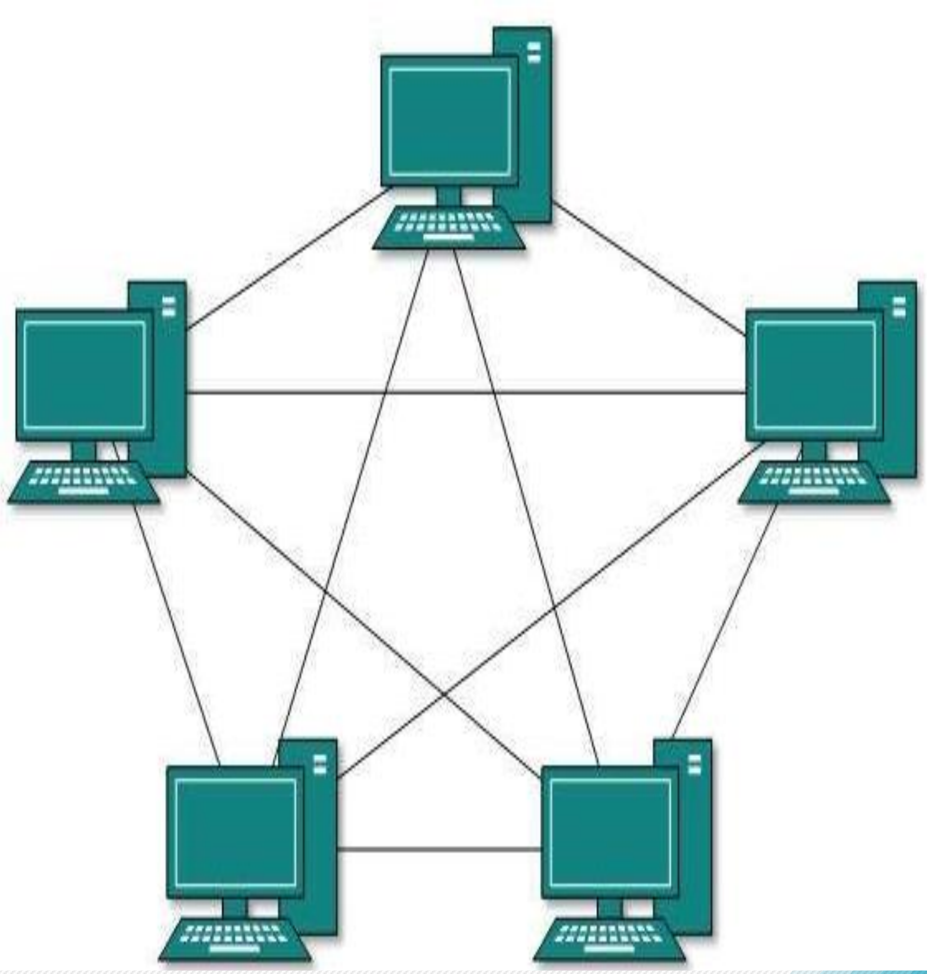
Network Topology – Mesh

This supports the connection one node to one or multiple hosts. This topology has hosts in point-to-point connection with every

other host may also have hosts which are in point-to-point connection to few hosts only. It comes in two variants:

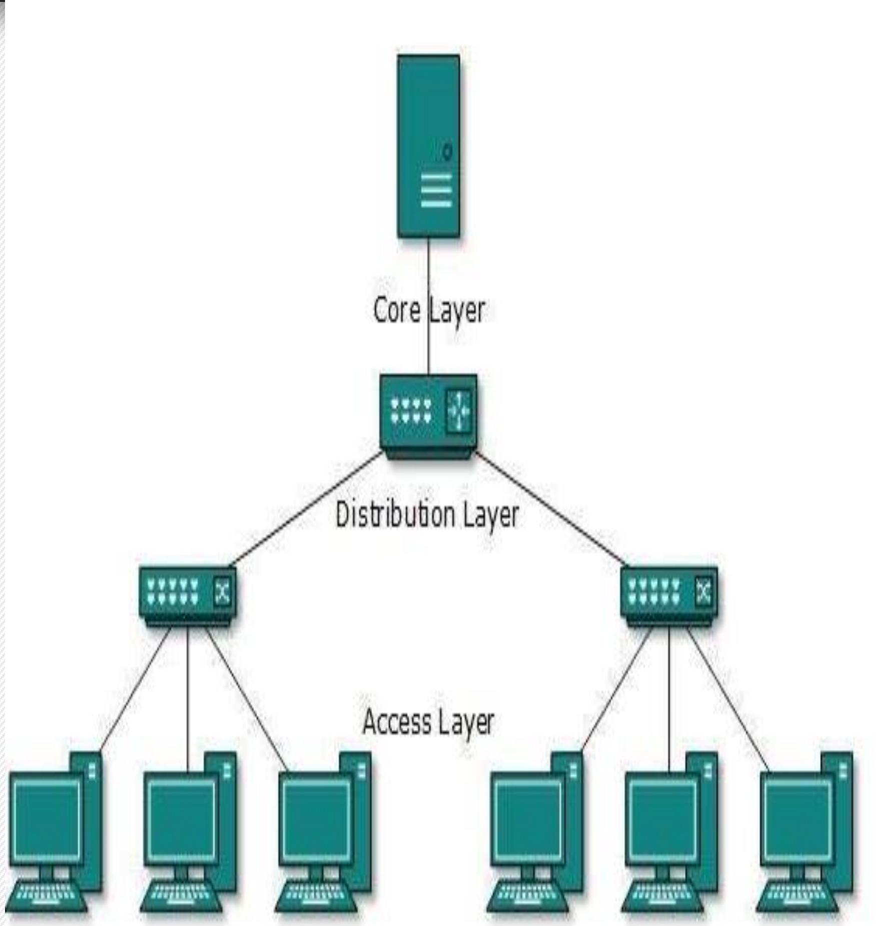
- **Full Mesh**: All hosts have a point-to-point connection to every other host in the network. It provides the most reliable network structure among all network topologies.

- **Partially Mesh**: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.

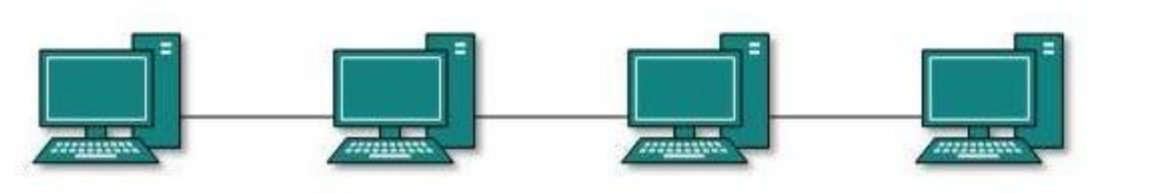


Network Topology - Tree or Hierarchical

This is built as an extended Star topology and inherits some properties of bus topology. It supports the division of a network into multiple layers. Mainly in LANs, a network is bifurcated into three types of network devices. The lowermost is access-layer where computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The highest layer is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork



Network Topology – Daisy Chain

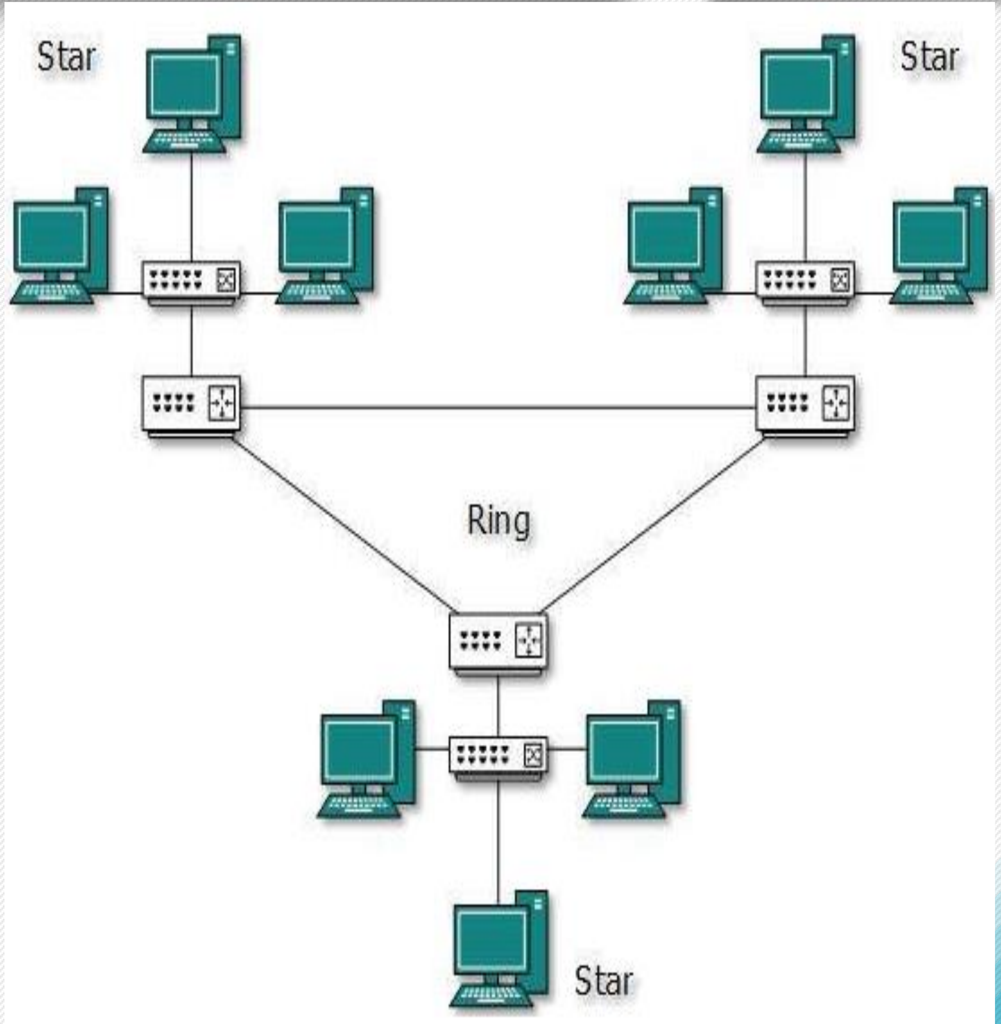


The daisy chain connects nodes in a linear pattern. Similar to Ring topology, each host is connected to two hosts only, except the end hosts. Means, if the end hosts in daisy chain are connected then it forms a Ring topology.

Each link in daisy chain represents single point of failure. Every link failure splits the network into two segments. Every intermediate host works as relay for its immediate hosts.

Network Topology – hybrid

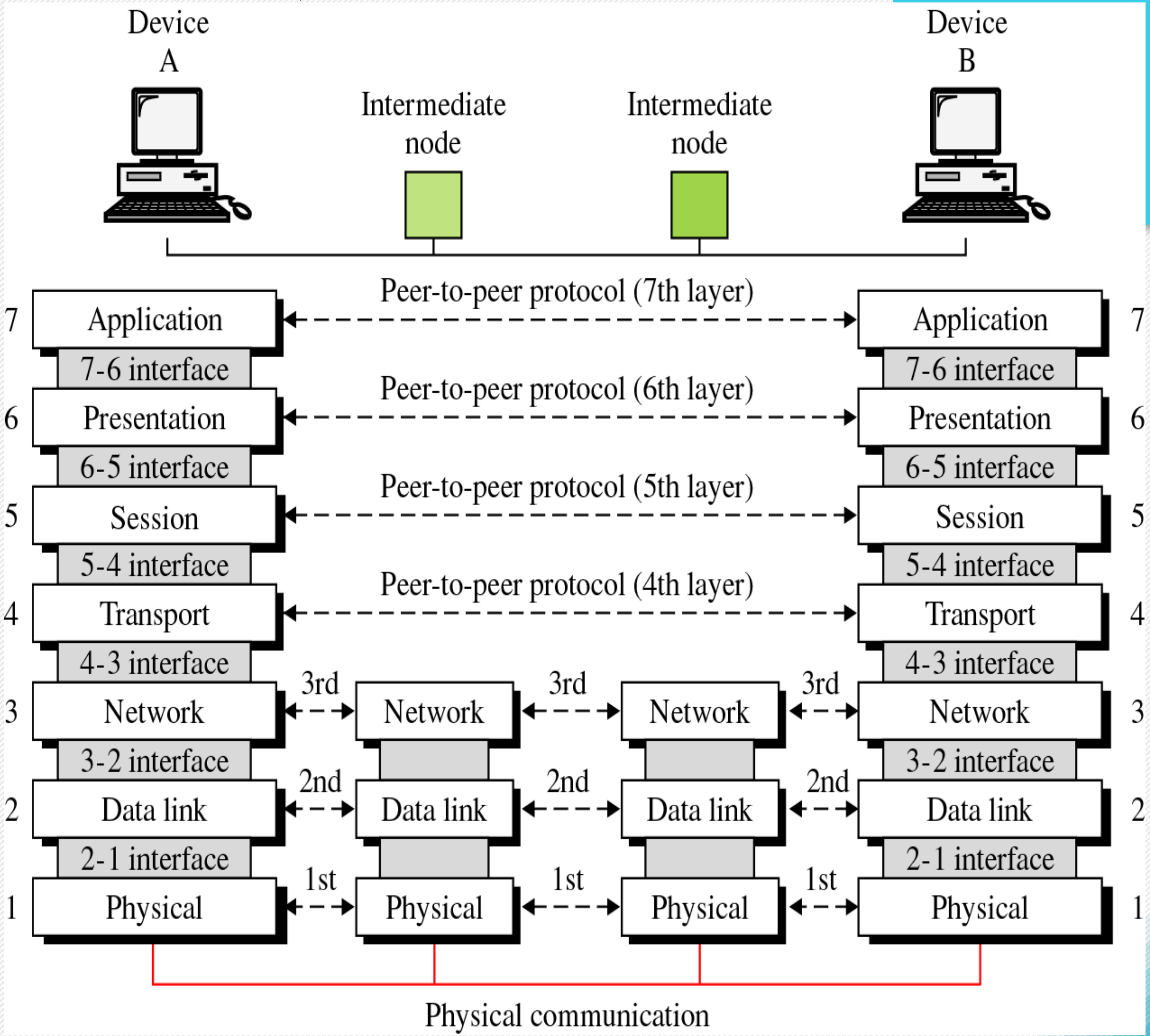
A combination of multiple network topologies to build a single network. It inherits the advantages and disadvantages of the various topologies forming the hybrid topology network. WANs, MANs and the Internet are built on this model.



Open System Interconnection (OSI) Reference Model

The OSI reference model was created by the International organisation for standardization for the following purposes:

i. standardize data networking protocols to allow communication between all networking devices
ii. Provides a model for software/hardware vendors to create products that can interoperate on the network. E.g. IBM products communicate with CISCO equipment
iii. Help network administrators determine easily determine the hardware/software required to build network
iv. Provide a teaching/learning tool that enables the understanding the communication process used between networking components
v. Makes troubleshooting easier for network administrators



OSI Layers

	Data unit	Layer	Function
Host layers	Data	7. Application	Implements the direct interaction between users and application, such as HTTP, FTP and SMTP. ftp, telnet, smptp, http
		6. Presentation	Formats or translate data for the application layer based on the syntax or semantic that the application layer understands. Also performs encryption and decryption. Translation, data compression, encryption,/decryption,
		5. Session	Controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. Start and terminate sessions (session management, authentication, authorization
	Segments	4. Transport	Manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. An example is the TCP. Segmentation, flow control, error control, tcp, udp,
Media layers	Packet	3. Network	Receiving frames from the data link layer and delivering them to their intended destinations based on the addresses contained inside the frame. It uses logical addresses (IP) to determine the destination. Routers are used at this layer. Routers and IP addresses
	Frame	2. Data Link	Directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. Also corrects errors that may occur at the physical layer. It has 2 sub-layers. (1) media access control (MAC), provides flow control and multiplexing for device transmissions over a network. (2) logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols. MAC addresses and switches

Mapping of TCP/IP Model and the OSI Model

OSI	TCP/IP
Application Layer	Application Layer TELNET, FTP, SMTP, POP3, SNMP, NNTP, DNS,NIS, NFS, HTTP, etc.
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer TCP , UDP, etc.
Network Layer	Internet Layer IP , ICMP, ARP, RARP, etc.
Data Link Layer	Link Layer FDDI, Ethernet, ISDN, X.25, etc.
Physical Layer	

Introduction to TCP/IP

TCP (**Transmission Control Protocol**) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

User Datagram Protocol (**UDP**) is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages sometimes known as *datagrams* (using Datagram Sockets) to one another. UDP is sometimes called the **Universal Datagram Protocol** or Unreliable Datagram Protocol.

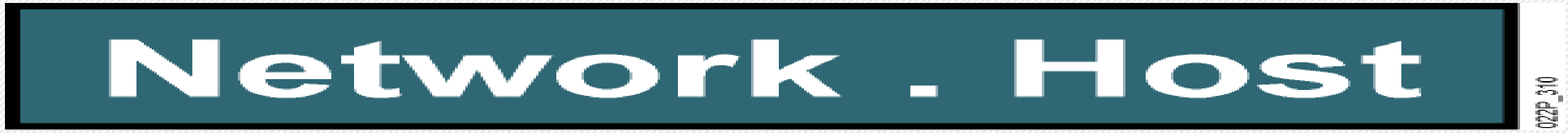
Internet Protocol (IP) Addressing

An IP address uniquely identifies each device on an IP network so that data can be sent correctly to those locations. For example: Address on a letter, Telephone number

Every host (computer, networking device, peripheral) must have a unique address.

Parts of the IP Address

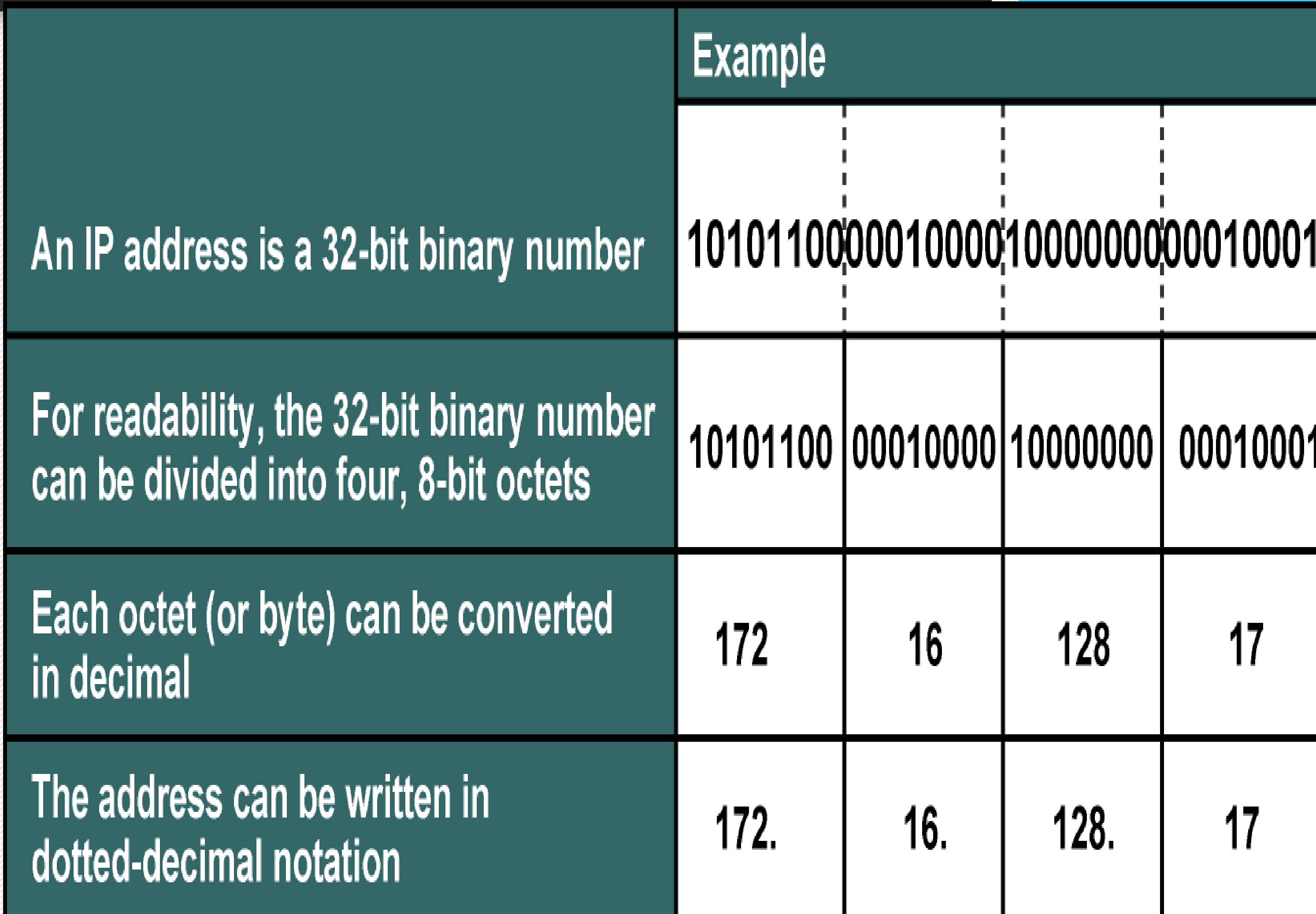
- Each IP address consists of:
    - Network ID
        - Identifies the network to which the host belongs
        - Assigned by registry authority and cannot be changed
    - Host ID
        - Identifies the individual host
        - Assigned by organizations to individual devices



IP Address Format: Dotted Decimal Notation

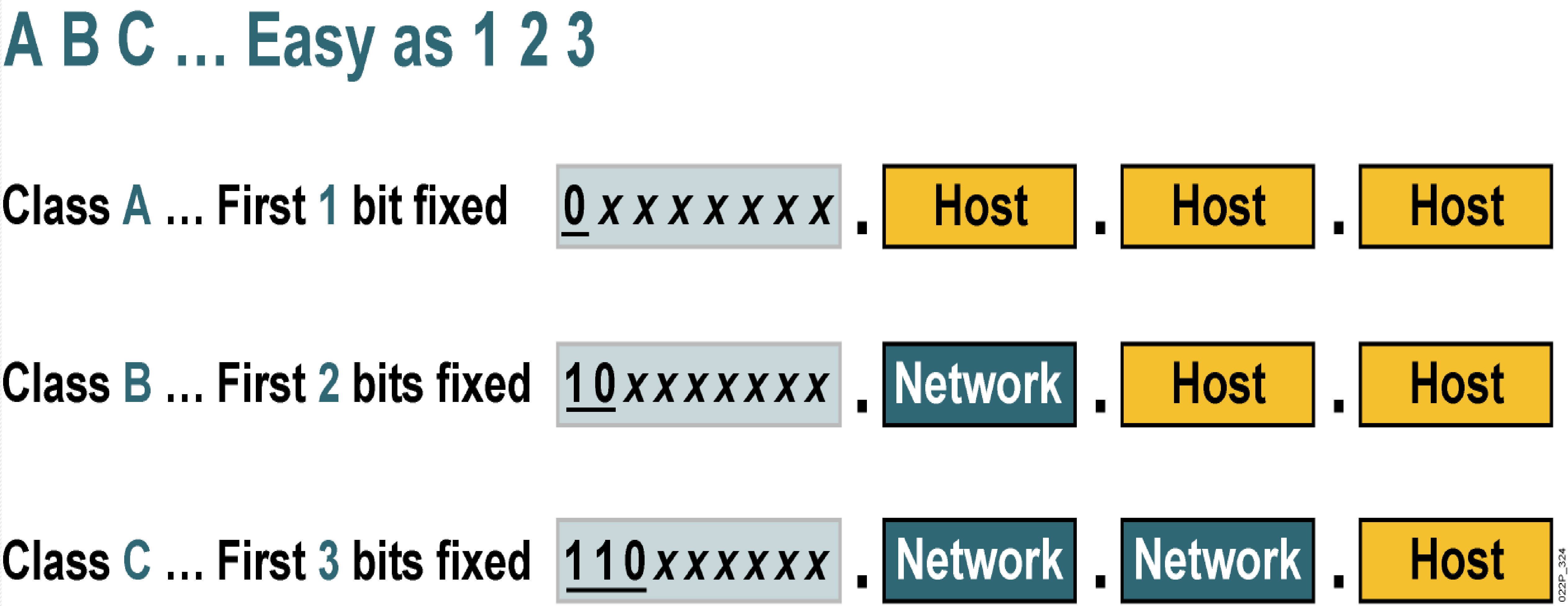
32 bits, with 8 bit groupings

- Example 172.16.128.17
- Each number between the dots can be between 0 and 255
- Allocated in groups called address blocks
- 3 sizes, based on the class of the address
- Class A, Class B, and Class C



	Example			
An IP address is a 32-bit binary number	10101100	00010000	10000000	00010001
For readability, the 32-bit binary number can be divided into four, 8-bit octets	10101100	00010000	10000000	00010001
Each octet (or byte) can be converted in decimal	172	16	128	17
The address can be written in dotted-decimal notation	172.	16.	128.	17

IP Address Classes: The First Octet



A B C ... Easy as 1 2 3

Class A ... First 1 bit fixed	0 x x x x x x x	Host	Host	Host
Class B ... First 2 bits fixed	1 0 x x x x x x	Network	Host	Host
Class C ... First 3 bits fixed	1 1 0 x x x x x	Network	Network	Host

IP Addresses Classes cont’d

Class A:

Owned giant organizations like ISPs, Large Internet companies like Google, CNN, etc
All IP addresses are of the form:
    0 – 126.x.x.x
    x can be between 0 and 255
The first octet is assigned to the owner, the remaining 3 are freely distributable to the nodes. Thus, It Has a 24 bit address space
Uses up to half of the total IP addresses available

Class B:

All Class B Addresses are of the form:
    128 - 191.x.x.x
    Where x can take any number between 0 and 255
The first two octets are assigned to the address block owner, with the last two freely distributable
Has 16-bit address space
¼ of all IP addresses belong to Class B Addresses

IP Addresses Classes cont’d

Class C:

All Class C Addresses have the following format:

192-223.x.x.x

The first three octets are assigned, with the last being freely distributable

Only 253 distributable addresses within a Class C Address

Class D:

Multicast addresses

224 – 247.x.x.x

Class E:

248 – 255.x.x.x

Experimental purposes

IP Address Ranges

Class	Range	Number of Possible Networks	Number of Possible Hosts in One Network	Number of Usable Hosts in One Network
A	1-126	126	16,777,216	16,777,214
B	128 -191	16,382	65,536	65,534
C	192-223	2,097,150	256	254

Number of Possible networks is = $2^{x-y,}$ Where x = number of network bits and y = number of fix bits in the network bits. Note that y depends on the IP address Class

Number of Possible Hosts in one network = 2^{x} where x is the number of hosts bits
Number of usable hosts in one network is = $2^{x} - 2$, where x is the number of host bits

Reserved IP Addresses

Private Networks (no public connections)

- 10.x.x.x – Class A
- 172.16.x.x – Class B
- 192.168.x.x – Class C

Local Network

- 127.x.x.x – local network (loopback)

Multicast

- 255.255.255.255 – broadcast – sends to everyone on the network

IP Address Shortage

IPv4 has potential for 4 billion IP addresses, However, with increased Internet Connectivity, this number is running out.

Applications increasing Demand

Applications in IoTs

Mobile devices

It is projected that by the year 2030, there will be tens of billions of connections

A solution has been created through the 128 bits IPv6 but majority of Internet users are yet to adopt IPv6 due to compatibility issues between IPv4 and IPv6

Thus, leading to shortage in IPv4 addresses and increase in their cost/IP

IP Address Shortage – Solution

Network Address Translation (NAT) - Hides many nodes behind limited set of public addresses

- ❖ Block of addresses are located to ISPs and organisations
- ❖ This is based on classes of IP addresses
- ❖ What if we have a class C allocation that allows for 254 IPs and we have 500 computing devices to connect?

Use a gateway/router to map invalid (reserved) addresses to valid IP addresses

- Translates your local address to a routable address
- Router receives one IP Address
  - Either dynamically assigns addresses to all the nodes behind the router, or it is assigned statically using non-routable addresses
    - If dynamic, uses DHCP (Dynamic Host Configuration Protocol)
  - When someone inside the network wants to access a computer outside the local network (the internet), the request is sent to the router, which uses NAT to send the request to the internet.

NB: This has potentials to increase security as these IPs are not visible outside the network

IPv4 and IPv6

IPv6 was developed by the Internet Engineering Task Force (IETF) to provide a long term solution to the problem of IP exhaustion in IPv4.

It is 128-bits IP addressing Scheme and has address space of 2^{128} bigger than IPv4 with 2^{32}

340,282,366,920,938,463,463,374,607,431,768,211,456 Ips

340 undecillion, approximately 3.4×10^{38}

There are 8 groups separated by colon, each group is represented by 2 bytes (16bits) written in hexadecimal form

IPv4 and IPv6 – cont’d

An IPv6 address is 128 bits in length and consists of eight, 16-bit fields, with each field bounded (separated) by a colon. Each field must contain a hexadecimal number, in contrast to the dotted-decimal notation of IPv4 addresses. In the next figure, the x's represent hexadecimal numbers.

X:X:X:X:X:X:X:X, Note that each X represents a 16-bits field unlike the 4-8bits field in IPv4

2001:0DB8:3C4D:0015:0000:0000:1A2F:1A2B

Most IPv6 addresses do not occupy all of their possible 128 bits. This condition results in fields that are padded with zeros or contain only zeros

IPv4 and IPv6 – Abbreviating IPv6 addresses

Most IPv6 addresses do not occupy all of their possible 128 bits. This condition results in fields that are padded with zeros or contain only zeros

The IPv6 addressing architecture allows one to use the two-colon (::) notation to represent contiguous 16-bit fields of zeros. For example, you might abbreviate the IPv6 address:

2001:0DB8:3C4D:0015:0000:0000:1A2F:1A2B to:

2001:0DB8:3C4D:0015::1A2F:1A2B leading zeros in the fields can also be removed. For example: 0DB8 can become DB8 and 0015 can become 15, the new address becomes: 2001:DB8:3C4D:15::1A2F:1A2B

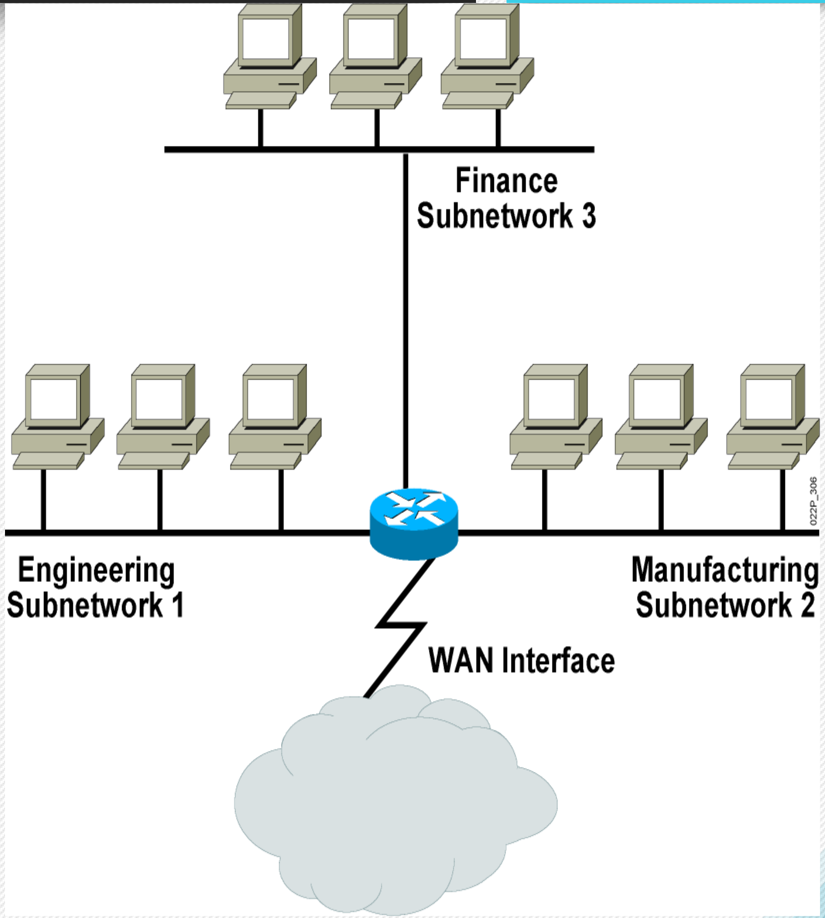
Subnetworks

Subnet – Logical division of IP networks into 2 or more networks

Purpose

- Reduce network congestions
- Improve network performance
- Improve security

Routers are used to communicate between subnets. However, a subnet allows its linked devices to communicate with each other.



Number of Subnets Available

To determine the number of subnets:

✓Borrow bits from the host ID portion of the IP address

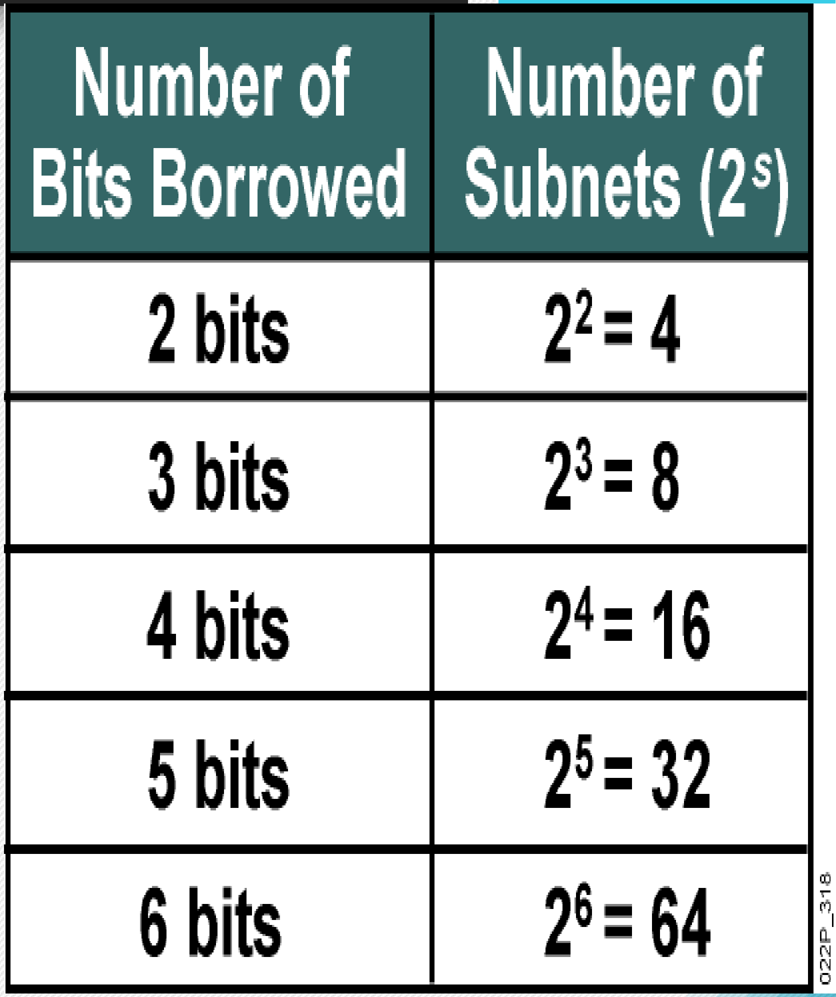
✓Number of subnets available depends on the number of bits borrowed.

✓One address is still reserved as the network address.

✓One address is still reserved as broadcast address.

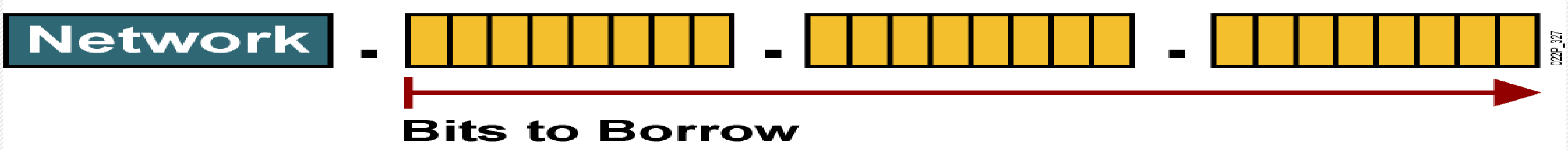
✓Available number of subnets = 2^s where ‘*s*’ is the number of bits borrowed.

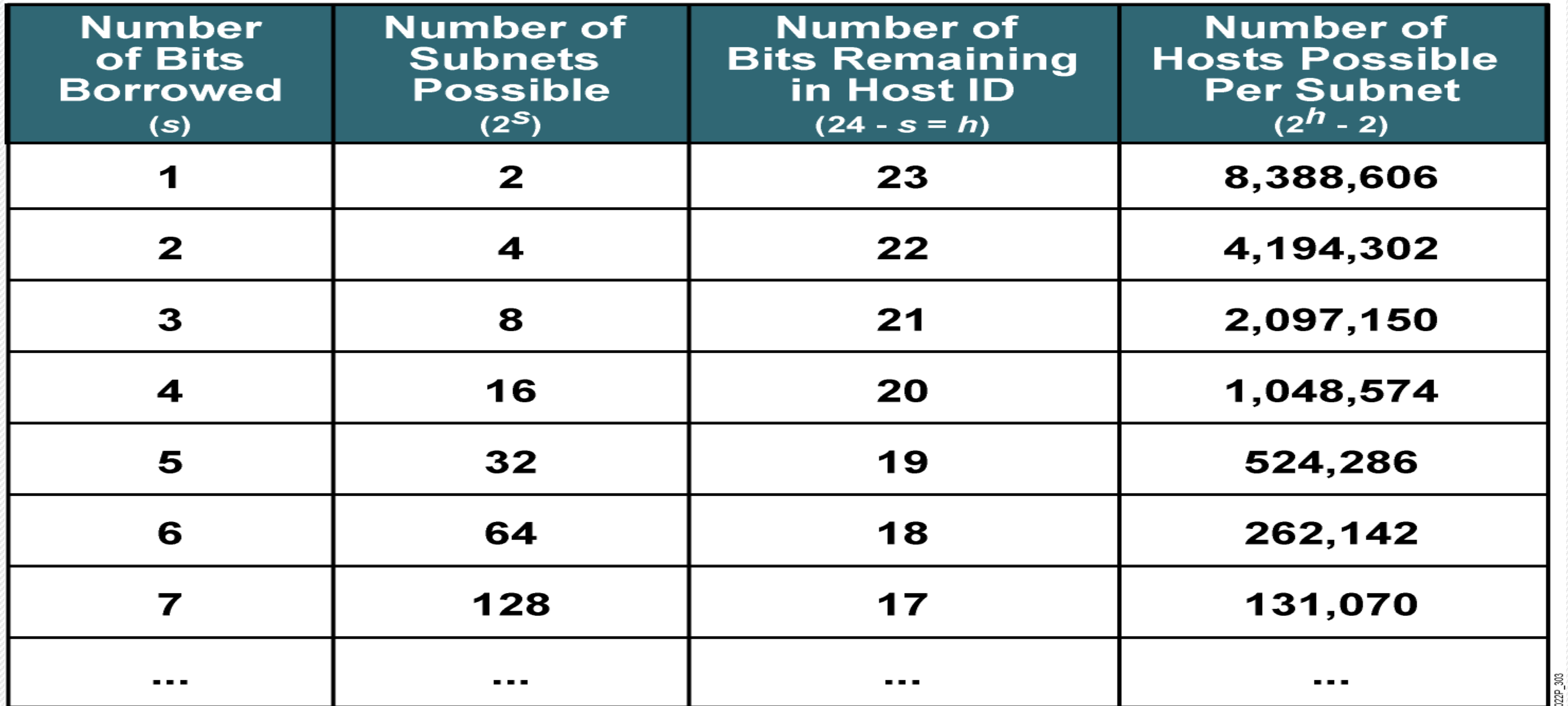
If we have a class C address, the number of possible subnets is as shown in the table.



Number of Bits Borrowed	Number of Subnets (2^s)
2 bits	$2^2 = 4$
3 bits	$2^3 = 8$
4 bits	$2^4 = 16$
5 bits	$2^5 = 32$
6 bits	$2^6 = 64$

Possible Subnets and Hosts for a Class A Network



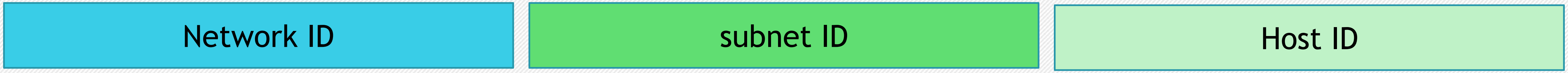


Number of Bits Borrowed (s)	Number of Subnets Possible (2^s)	Number of Bits Remaining in Host ID ($24 - s = h$)	Number of Hosts Possible Per Subnet ($2^h - 2$)
1	2	23	8,388,606
2	4	22	4,194,302
3	8	21	2,097,150
4	16	20	1,048,574
5	32	19	524,286
6	64	18	262,142
7	128	17	131,070
...	...	...	...

Building subnets from a network

You are required to create four networks for faculties of science and tech, agriculture, engineering and medicine with each faculty having 60 systems.

Since we need 60 systems per network, we require a class C IP address: 192.168.4.0



Network ID

subnet ID

Host ID

Although, we have discussed previously that an IP address has two IDs - network and host, as we want to create a subnet, a third ID is introduced between the network and host IDs – i.e subnet ID. The subnet ID is taken from the Host ID, that is, bits are borrowed from the host ID depending on the number of subnets that are to be created. For example we need 4 subnets, therefore, we borrow 2 bits from the host ID. the subnet IDs for the subnets based on borrowed bits will be: 00, 01, 10 and 11. Thus:

Our first network commences from 00000000-01111111 (0 – 63), 2nd subnet 0100000000-01111111 (64-127), 3rd network from 10000000 – 10111111(128-190) and 4th network from 11000000 – 11111111 (192-255)

Note that the number of bits borrowed is a function of the number of subnets required, for example, if we need 8 subnets, we will borrow 3 bits, if we need 16 subnets, we will borrow 4 bits, etc.

Building subnets from a network

Network ID	Host ID range	Number of Usable Host IDs	Broadcast ID
192.168.4.0	192.168.4.1 – 192.168.4.62	62	63
192.168.4.64	192.168.4.65 – 192.168.4.126	62	127
192.168.4.128	192.168.4.129 – 192.168.4.190	62	191
192.168.4.192	192.168.4.193 – 192.168.4.254	62	255

Building subnets from a network - Example

You are given a network 192.168.4.0/24 to create three networks for department of finance, engineering and manufacturing

Step 1: Create a Subnetting Table and identify the column that gives you the number of subnets

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

Here, 4 represents the number of subnets, 64 is the number of possible host (host IDs) and /26 is the new subnet mask.

Building subnets from a network

First host ID is reserved for network ID and last host ID reserved for Broadcast ID

Network ID	Subnet Mask	Host ID range	Number of Usable Host IDs	Broadcast ID
192.168.4.0	/26	192.168.4.1 – 192.168.4.62	62	63
192.168.4.64	/26	192.168.4.65 – 192.168.4.126	62	127
192.168.4.128	/26	192.168.4.129 – 192.168.4.190	62	191
192.168.4.192	/26	192.168.4.193 – 192.168.4.254	62	255

Network Management – NIC and MAC Addresses

- Network Interface (NI) is an interface to a network from a computer, server, printer or any device that connects to a network. All modern computing devices have network interfaces, either wired (ethernet cable) or wireless to connect to a wireless access point (WAP).

- Traditionally, NI came on a separate card thus are referred as network interface cards (NIC). In recent times, NI are built-in on the motherboard

Uses of the NIC

- Provides connection to the network media/Medium (ethernet cables, blue tooth, wi-fi, satellite, etc).
- They have physical addresses referred to as the MAC address
- Enable communication with other devices on the network
- Takes data from the OS, Encapsulates it into frames and makes it suitable for transport on the network.

Differences Between MAC and IP Addresses

- MAC addresses Identifies the device, IP addressed provides the location of the device on the network

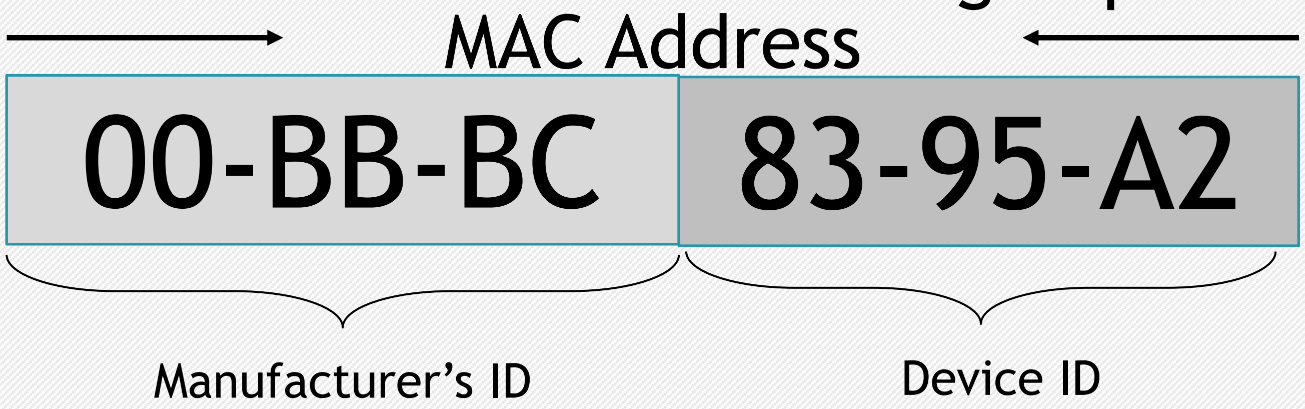
- MAC addresses are permanent identifiers of devices, a device IP address may change.

- Example – IP addresses are like mailing addresses of people living in a house, MAC addresses are the actual names of the individuals living in the house.

All device manufacturers must contact IEEE to give them block of MAC addresses which they burn into the NIC cheap of all devices such that no two devices on earth would have the same MAC addresses

MAC Addresses

A MAC address also referred to as physical or hardware address is a 48-bits number coded in 12 hexadecimal numbers with each hex character representing 4 bits. The hex characters are grouped in twos separated by hyphen.



MAC Address

00-BB-BC

83-95-A2

Manufacturer's ID

Device ID

The first 6 characters represent the device manufacture's ID also referred to as Organisational Unique Identifier (OUI).

The second block of 6 digits is referred to as the device ID

Network Media

Copper Cabling

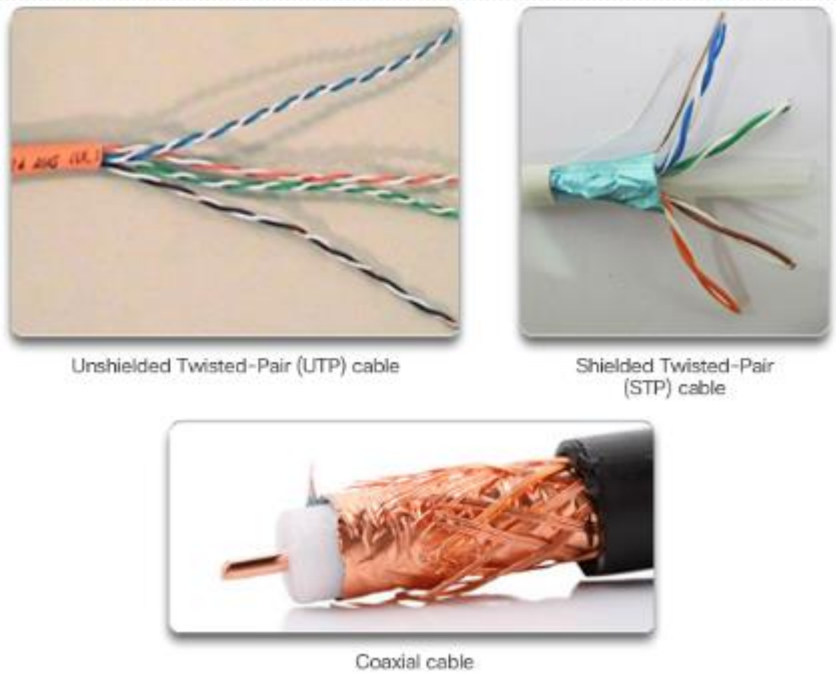
- Characteristics of Copper Cabling

  Inexpensive, easy to install, low resistance to electric current

  Distance and signal interference

- Copper Media
- Unshielded Twisted-Pair Cable
- Shielded Twisted-Pair Cable
- Coaxial Cable
- Copper Media Safety

  Fire and electrical hazards



Unshielded Twisted-Pair (UTP) cable

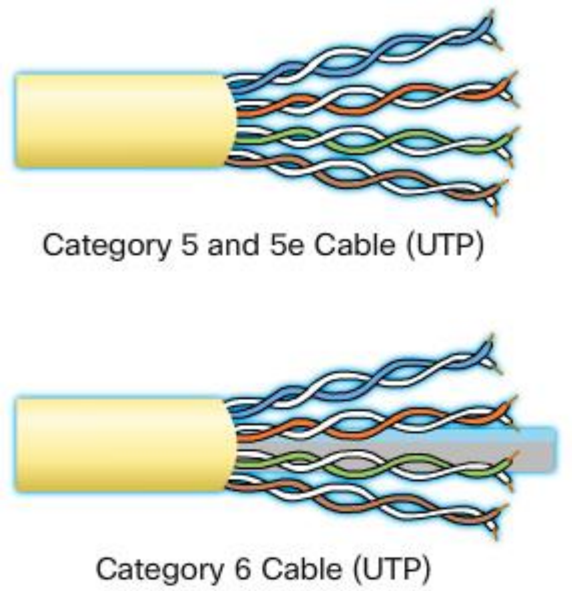
Shielded Twisted-Pair (STP) cable

Coaxial cable

Network Media

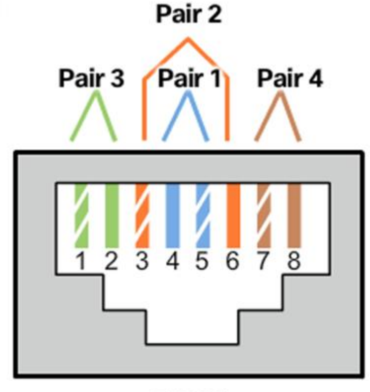
UTP Cabling

- Properties of UTP Cabling
  - Cancellation of EMI and RFI signals with twisted pairs
- UTP Cabling Standards
  - TIA/EIA-568
  - IEEE: Cat5, Cat5e, Cat6, Cat6e
- UTP Connectors
- Types of UTP Cable
  - Rollover
  - Crossover
  - Straight-through
- Testing UTP Cables
- Cable Pinouts

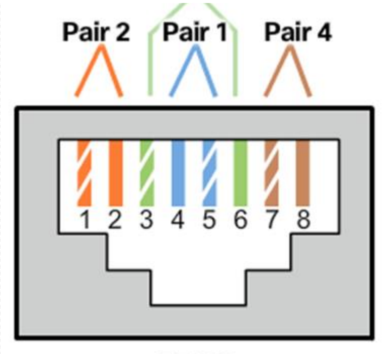


Category 5 and 5e Cable (UTP)

Category 6 Cable (UTP)



T568A

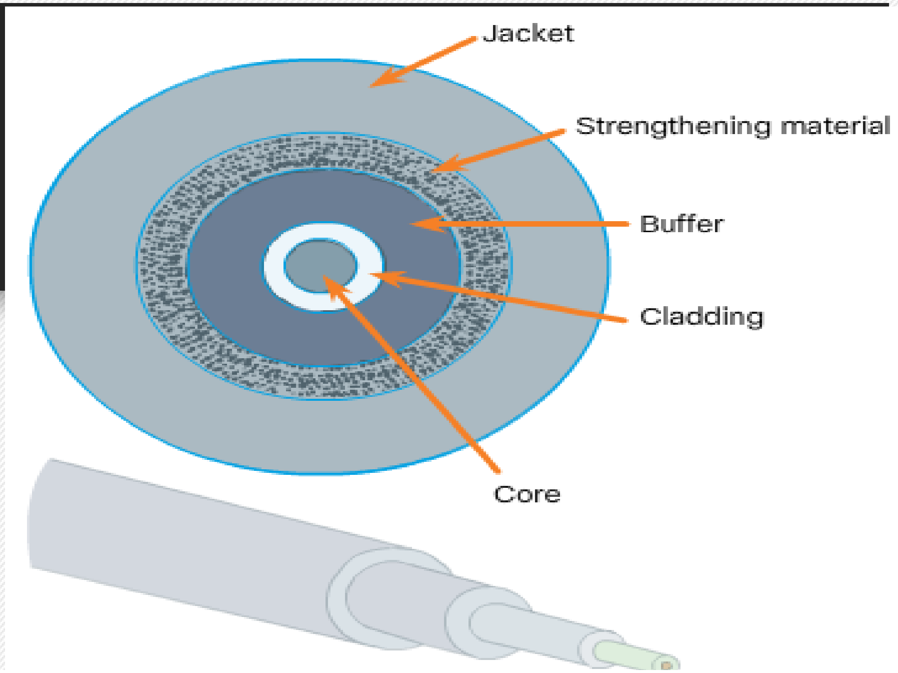


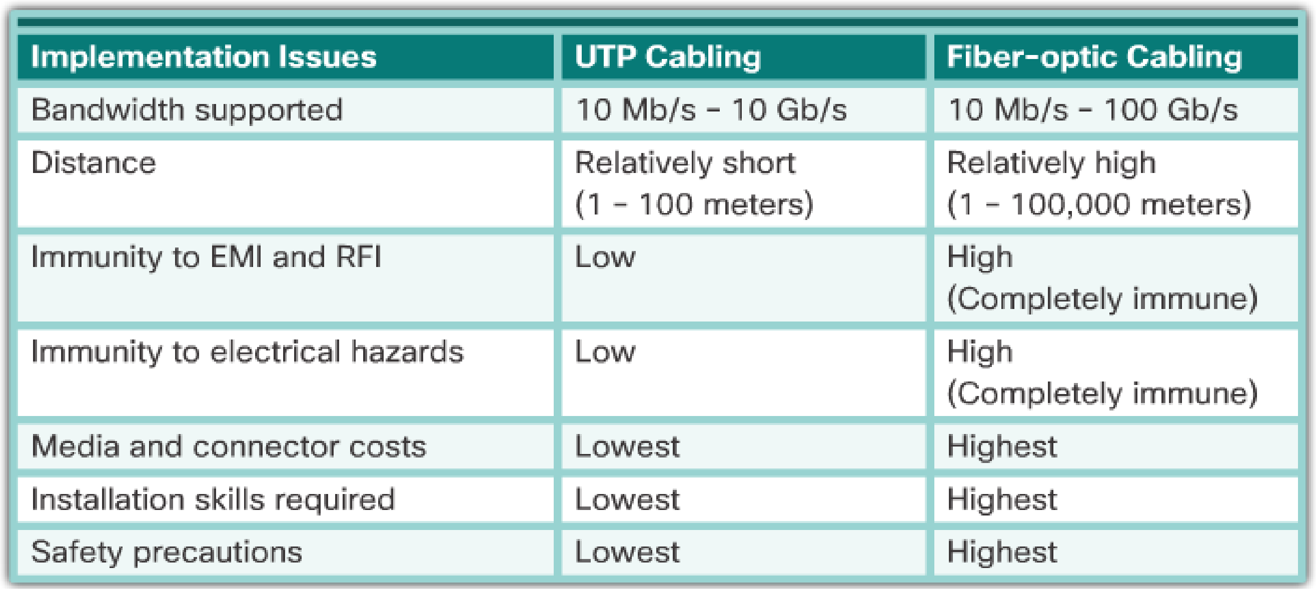
T568B

Network Media

Fiber-Optic Cabling

- Properties of Fiber-Optic Cabling
  - Transmits data over longer distances
  - Flexible, but thin strands of glass
  - Transmits with less attenuation
  - Immune to EMI and RFI
- Fiber Media Cable Design
- Types of Fiber Media
  - Single mode and multimode
- Fiber-Optic Connectors
- Testing Fiber Cables
- Fiber versus Copper



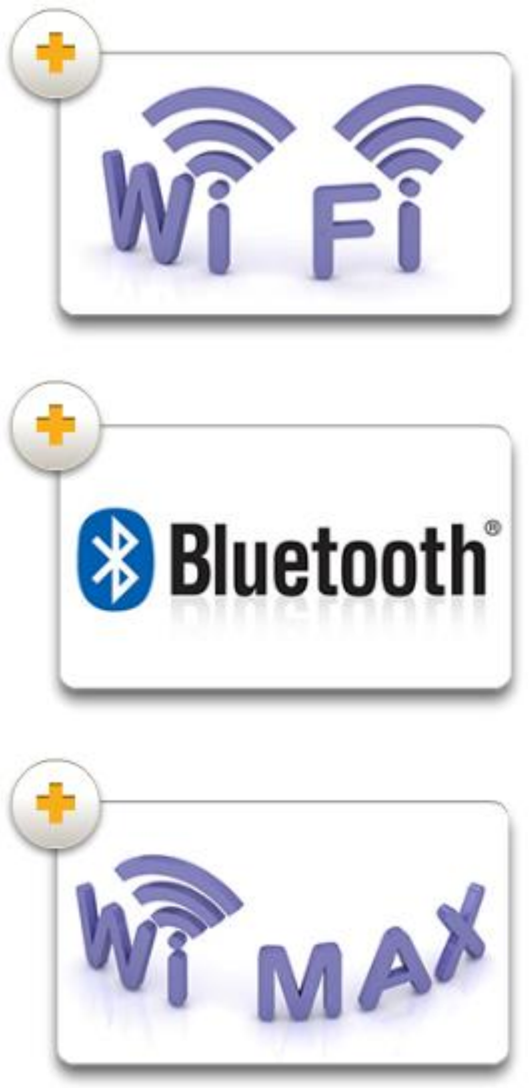


Implementation Issues	UTP Cabling	Fiber-optic Cabling
Bandwidth supported	10 Mb/s – 10 Gb/s	10 Mb/s – 100 Gb/s
Distance	Relatively short (1 – 100 meters)	Relatively high (1 – 100,000 meters)
Immunity to EMI and RFI	Low	High (Completely immune)
Immunity to electrical hazards	Low	High (Completely immune)
Media and connector costs	Lowest	Highest
Installation skills required	Lowest	Highest
Safety precautions	Lowest	Highest

Network Media

Wireless Media

- Properties of Wireless Media
  - Data communications using radio or microwave frequencies
- Types of Wireless Media
  - Wi-Fi, Bluetooth, WiMax
- Wireless LAN
  - Wireless Access Point
  - Wireless NIC adapters



Network Equipment- Hub and Switch

Hub

- Connects network devices together on an internal network
- it has multiple ports for ethernet connections from multiple network devices
- Not intelligent because it does not have capability for filtering data or knowing where the data is to be sent
- When a data packet arrives at one of its ports, it is rebroadcasted to all other devices whose ports are connected to the hub.

Disadvantages

(1) Unnecessarily traffic and (2) security issues

Switch

- Connects network devices together on same network
- Intelligent and capable of learning the MAC addresses of all devices connected to it
- Stores MAC addresses in a table and send data packets only to a particular receiving device
- Operates at data link layer

NB: Hubs and Switches only exchange data within an internal network as they do not have capabilities to read IP addresses

Network Equipment – Router

- Routes or forward data packets from one network to another based on IP addresses
- Inspects a data packet and determine if it were meant for its own network or another
- It receives it if it were meant for it but rejects it if its meant for another network
- It’s a gateway for its network
- Layer 3 device

Essentially, hub and switches are used to create networks while routers are used to connect networks

Routing and Routing Protocols