H2 Computing Summarised Notes (Part 5)

Networking (in a Nutshell)

Networking Fundamentals

Part 1: Networks and Nodes

1.1 Network

A **network** is a group of devices that are connected together and can communicate and share files and peripheral devices (like printers) between each other.

1.2 Node

A **node** is a device or computer that is able to connect to a network and generate, process and transfer data.

Each node has **addressing information** (MAC address) in order to allow other devices to communicate with it.

1.2.1 Endpoint

An **endpoint** is a node that acts as a source or destination for data transfer.

1.2.2 Redistribution Point

A **redistribution** point is a node that transfers data between other nodes.

(examples: network switches, router)

Part 2: Local Area Network (LAN)

2.1 What is a LAN?

A LAN is a computer network that covers a small geographical area.
(examples: home, office, school, a group of buildings)

2.2 Characteristics of LAN

A LAN is usually…

- Based in **one** or **more than one** building
- The organisation operating the LAN controls its **speed**
- The organisation operating the LAN is responsible for its **management** and **maintenance**
- There is a **choice of technology**.
- There is **no outside involvement** from telecommunications providers, unlike many WANs.

2.3 Network Configurations

A **network configuration** is a design specification for how the nodes of a network are constructed to interact and communicate, by determining the degree by which communications and processing are centralised and distributed.

2.3.1 Centralised Network

A **centralised network** consists of a central mainframe computer, which handles all the communications and data processing in behalf of clients.

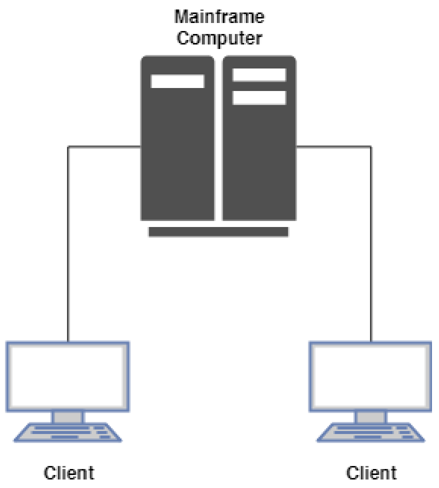
These 'clients' connect to the mainframe computer via **dedicated terminals/terminal emulators**.

Advantages

- ✓ These central mainframe computers are high performance.
- ✓ It allows for management in the LAN to be centralised.

Disadvantage

- ✗ It is generally very expensive to implement, not optimal for smaller businesses.

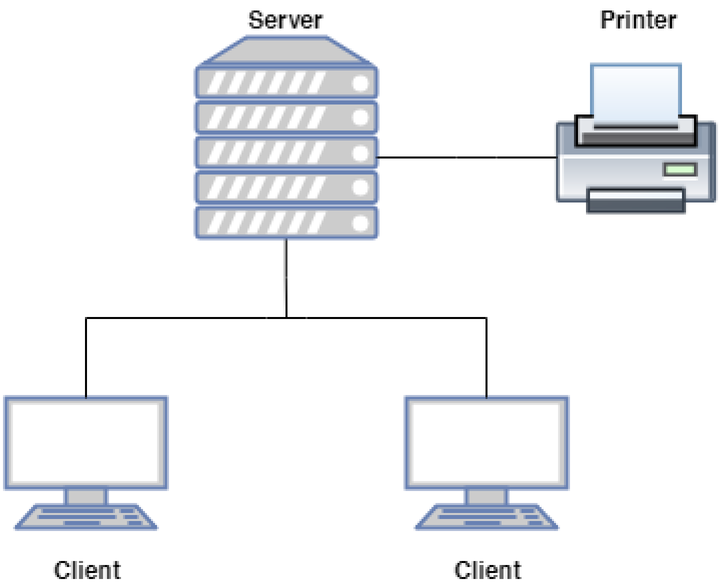


2.3.2 Client/Server Network

A client/server network is one in which servers provide resources to clients.

Usually, there is at least one server that provides central authentication services. Servers also provide access to shared files, printers, hardware storage and applications.

In client/server networks, processing power, management services, and administrative functions can be concentrated, while clients can still perform many basic end-user tasks on their own.



2.3.3 Peer-to-Peer Networks

A peer-to-peer network is a network in which resource sharing, processing, and communications control are completely decentralised. There are (at least) two communication parties with equivalent roles and responsibilities in a peer-to-peer network.

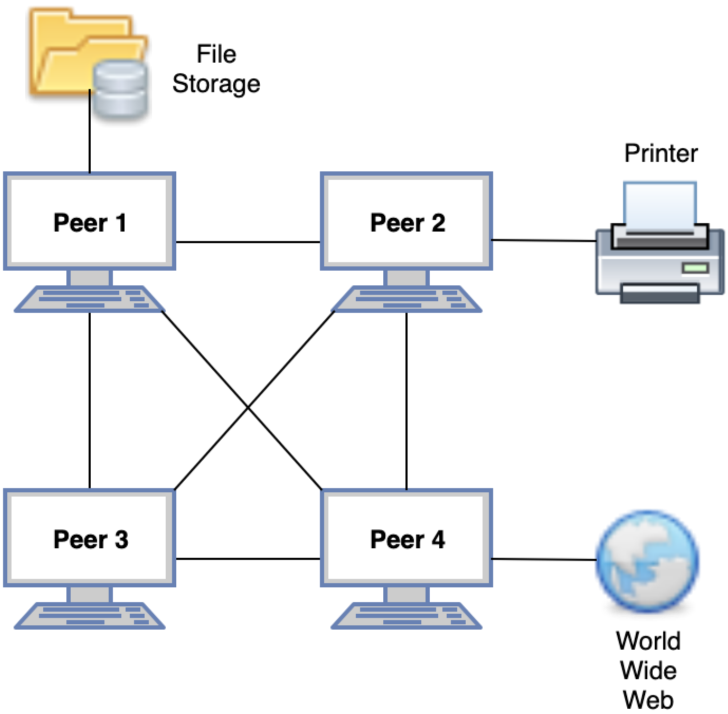
Services and resources are distributed on each computer for other computers to access. All clients on the network are equal in terms of providing and using resources, and each individual device authenticates its users.

Advantages

- ✓ Easy and inexpensive to implement

Disadvantages

- ✗ Data storage and authentication is not centralised, hence it is only practical in very small organisations.
- ✗ User accounts must be duplicated on every device from which a user accesses resources. This distribution of user information makes maintaining a peer-to-peer network difficult, especially as the network grows.



2.4 Network Topologies?

These are not required in the A level syllabus.

Network topologies are the physical shape of the network. There are three types: bus, star, and ring topologies.

2.5 Types of Connections

Simplex Connections

A simplex connection is a connection that allows communication in only one direction, from the transmitter to the receiver.

Half-duplex Connections (HDX)

A half-duplex connection allows communication to take place in both directions, but only at one direction at a time (not simultaneously).

How half-duplex connections work

Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting before replying. Antennas are of trans-receiver type in these devices (transmitter and receiver) so as to transmit and receive the signal.

Full-duplex Connections (FDX)

A full-duplex connection allows communication to take place in both directions simultaneously.

How full-duplex connections work

These connections work by making simultaneous use of two physical pairs of twisted cable, where one pair is used for receiving packets (of data) and one pair is used for sending packets, to a directly connected device.

This effectively makes the cable a collision-free environment and doubles the maximum data capacity for a connection, as compared to a half-duplex connection.

Benefits of using full-duplex over half-duplex

1. Time is not wasted

   No frames need to be re-transmitted using a full-duplex connection as compared to a half-duplex connection, as there are no collisions.

   (In a half-duplex connection, if two or more stations/nodes transmit at the same time, signals will collide and become garbled.)

2. Full data capacity available in both directions

   The send and receive functions in a full-duplex connection are separated, unlike a half-duplex connections where the same antennae send and receive data.

3. Nodes do not have to wait until others complete their transmission

   This is because there is only one transmitter for each twisted pair in cables used in a full-duplex connection.

2.6 Interconnection of LANs

LANs need to be interconnected for various reasons:

- Structure an organisation's network:
  Organisations are generally structured into divisions.
  Each one is likely to have its own LAN.
  To **enable communication** among the divisions, LANs need to be interconnected.

- Extend maximum distance between stations/nodes:
  A division may be spread over several floors in a building.
  Each floor is likely to have its own LAN.
  Hence, there is a need to **interconnect these LANs.**

2.6.1 Ways to interconnect LANs

Ethernet LANs:	Ethernet Hub
	Ethernet Switch
	Bridge
Different types of LANs:	Bridge

2.6.2 Interconnection using Hub

It is a networking device used to connect the nodes in a network to share files, data, and resources.

A hub is a 'non-intelligent' device and does not manage any data flowing through it, hence it broadcasts data that it receives to all nodes in the network – even if the nodes do not request for it.

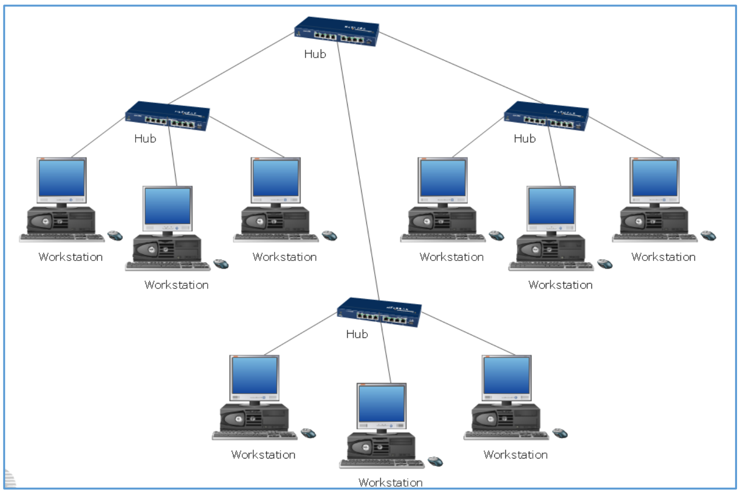
A hub can be connected in a multi-tier design with a backbone hub at its top, hence allowing interconnection of entire LANs.

Advantage:

- ✓ If one hub is down, the remaining network continues to operate.

Disadvantages:

- ✗ Only one station/node can transmit at a time in the entire network, otherwise, there would be collisions. (i.e. lack of traffic isolation in the network)
- ✗ Not too many stations can be connected in the network.



2.6.3 Interconnection using Switch

A switch is a network device that acts as a common connecting point for various nodes or segments. It breaks the network into LAN segments.

However, switches are more 'intelligent' devices as it transmits data around the network more efficiently. This is because it manages network data by examining the Media Access Control (MAC) address of the destination node found in the data and forwards messages only to the receiving device.

Switches filter frames, isolating traffic in the network. The frames on the same LAN segment are not usually forwarded onto other segments.

Like hubs, switches can be connected in a multi-tier design with a backbone switch as its top. This leads to further performance improvement.

2.6.4 Ethernet Switch

It contains two layers, the physical and MAC layer.
It is capable of buffering frames.
It examines frame headers and selectively forwards the frame based on the MAC destination address.
Other links can be used to switch other frames simultaneously.
Stations are unaware of the presence of the switch.

2.6.5 Interconnection using Bridge

A bridge has the same basic functionality of a switch, but it has fewer ports and is software-based.
It passes messages between two segments of a (bus) LAN.
It can be used to segment a bus networks into two segments.
Bridge also has two layers, just like the switch.

Bridges can interconnect different LANs together such that they act as one single LAN and allows two LANs to communicate with each other. This is done by converting the frame header according to the LAN on which a frame is being forwarded.

2.7 Network Architecture

2.7.1 Client/Server Architecture

Roles

Client/Server: The client and server are two communications parties with different roles and responsibilities. Services and resources are placed on the server for the client to access.

Server: It hosts resources (e.g. files) or offers services (e.g. Internet banking).
It is always on to wait for connections to come in. However, servers may be turned off during periods of maintenance/fault.
It is usually given permanent addresses so that it can be accessed easily.

Client: It communicates with servers to access services and/or resources.
A client usually does not communicate with other clients directly. However, this is possible via a server.

What is a client/server architecture?

There is at least one serving computer (the server) which provides all the client machines with all the facilities they need, which is usually file and printer sharing.

Disadvantages

- ✗ Cost
  With client/server computing, there is a need to purchase a central serving machine that should be fast and have huge storage capacity.
- ✗ Reliance on one central system for provision of services
  If this central system (the server) fails, access to all information and to the services on this machine would likely be lost.

2.7.2 Peer-to-Peer Architecture

In a peer-to-peer architecture:

- All nodes are peer-to-peer
- No server required
- A P2P node may offer contents to others. It makes this information available in the network.
- Other P2P nodes may access these contents via direct communication.

2.8 Intranet

An **intranet** is a private network that uses Internet protocols and services to share an organisation's information with its members/staff.

Just like the Internet, these members/staff can access an intranet via a regular web browser and navigate an organisation's web pages. An intranet usually contains information that is segregated from the Internet due to privacy and confidentiality reasons.

Therefore, an **intranet** provides all the features of the World Wide Web, but access is usually given to a closed group only, normally controlled by a password.

2.8.1 Benefits of an Intranet

Over the Internet

- ✓ Access is controlled
- ✓ More secure than the Internet due to only authorised people having access
- ✓ Faster than the Internet as it usually covers a small area.
- ✓ Less likely to crash the websites due to less hits

Tangible Benefits

- ✓ Inexpensive to implement
- ✓ Easy to use, just point and click
- ✓ Saves time and money
- ✓ Better information, faster too
- ✓ Based on open Internet standards
- ✓ Scalable and flexible
- ✓ Puts users in control of their data

Intangible Benefits

- ✓ Improved decision making
- ✓ Improved quality of life
- ✓ Improved productivity
- ✓ Builds a culture of sharing and collaboration
- ✓ Facilitates organisational learning

2.9 Enterprise Networks

It is a network that includes elements of both LANs and WANs. It is owned and operated by a single organisation to interlink its devices and resources so that users have access whether they are on or off premise (i.e. allows for remote access).

They are designed for **fast data access**, **email exchange**, and **collaboration**. They are scalable and include **high-end equipment**, **strong security systems**, and **mission-critical applications**.

Part 3: Wide Area Network (WAN)

3.1 What is a WAN?

Definition: a network that covers a large area, often across multiple geographical locations (e.g. all of an organisation's offices in a country/among different countries).

Part 4: Data Transmission

4.1 What is Data Transmission?

Definition: the physical transfer of data (a digital bit stream) over a point-to-point or point-to-multipoint communication channel.

4.2 Physical Media

Guided media:	signals propagate in solid media	(e.g. copper, fiber, coaxial)
Unguided media:	signals propagate freely	(e.g. radio)

4.3 Digital Signals

Digital signals can have combinations of only two values: **zero** and **one**. These signals can be translated into a **digital waveform**. A waveform can switch between two voltage levels: 0 for zero/ground voltage level and 1 at a +ve/-ve voltage level.

4.4 Digital Data Transmission

Definition: a form of data transmission that makes use of voltage differences to represent the '1's and '0's in data.

4.5 Unicast & Broadcast Transmission

Unicast Transmission

Definition: a method of data transfer from a source address to a destination address.

In unicast transmission, network nodes not involved in the data transfer ignore the transmission.

Broadcast Transmission

Definition: a method of data transfer from a source node to all other nodes in a network.

4.6 Rate & Speed of Data Transmission

Rate of Data Transmission

- Megabits per second (Mb/s – 1 million bits/s)
- Megabytes per second (MB/s – 1 million bytes/s)

Speed of Data Transmission

There are two types of measurements for data measurement speeds: bit rate and baud rate.

Bit rate: Number of bits that are transmitted per unit of time

Baud rate: Number of symbols that are transmitted per unit of time

4.7 Transmission Modes

A given transmission on a communications channel between two machines can occur in several different ways. The transmission is characterised by:

- the direction of the exchanges
- the transmission mode: the number of bits sent simultaneously
- synchronisation between the transmitter and the receiver

4.7.1 Simplex, half-duplex, full-duplex connections

Simplex Connection

Definition: A connection in which data flows in only one direction, from the transmitter to the receiver.

Bandwidth: Full bandwidth, as the transmission operates in one direction

Examples: Radio, television broadcasts

Half-duplex Connection

Definition: A connection in which data flows in one direction and the other, but not both at the same time.

Bandwidth: Full bandwidth, as the transmission operates in one direction at a time

Full-duplex Connection

Definition: A connection in which data flows in both directions at the same time.

Bandwidth: Half bandwidth, as the transmission can operate in both directions simultaneously.

4.7.2 Serial and Parallel Transmission

The transmission mode refers to the number of elementary units of information (bits) that can be simultaneously translated by the communications channel.

Serial Transmission

Definition: A form of data transmission where data are sent one bit at a time over the transmission channel, as one per clock cycle.

Used in: Ethernet, keyboards, mice, etc.

However, as most processors process data in parallel, the transmitter has to transform parallel data to serial data and vice versa for the receiver.

Parallel Transmission

Definition: A form of data transmission where multiple bits are simultaneously transmitted over multiple transmission channels/lines.

These bits are sent simultaneously over multiple different lines, which either consists of:

- Multiple physical lines (such as several wires in a ribbon cable), or
- One physical line split up into multiple sub-channels by dividing up the bandwidth. Each bit is sent along the sub-channel at a different frequency.

Limitation: For parallel transmission, since conductive wires are close to each other in the ribbon cable (*N* physical lines), interference may occur especially at high speeds that may degrade the signal quality.

4.7.3 Synchronous and Asynchronous Transmission

Given the problems that arise with a parallel-type connection, serial connections are normally used. However, since a single wire transports the information, the problem is how to synchronise the transmitter and the receiver – the receiver may not necessarily distinguish the characters because the bits are sent one after the other. To address this problem, there are 2 types of transmission that can be used:

Asynchronous Transmission

The sender inserts special start and stop patterns between each byte of data. By watching for these bit patterns, it allows the receiver to distinguish between bits in the data stream.

- ✓ Each individual character is complete in itself – corruption of a character during asynchronous data transmission does not affect the preceding and succeeding character.
- ✓ Suited for applications where characters are generated at irregular intervals (e.g. data entry from the keyboard)
- ✗ Successful transmission depends on recognition of start bits – they can be easily missed
- ✗ A high proportion of the transmitted bits are used for control (start, stop bits) and carry no useful information (3/11 for ASCII code)
- ✗ These distortion effects limit transmission speeds.

As a result, this is normally only used for speeds up to 3000 bits/second, with only simple, single character error detection.

Synchronous Transmission

A byte is sent after a standardised time interval. The receiver assumes that one byte is transmitted every interval. Two devices must start and stop their reckoning of these intervals at exactly the same time.

Synchronous devices include a clock chip. A special bit pattern is inserted at specific intervals in the data stream, enabling the receiving device to synchronise its clock with the sender.

- ✓ The amount of central information that has to be transmitted is restricted to only a few characters at the start of each block.
- ✓ The system is not that prone to distortion as asynchronous communication and can thus be used at high speeds.
- ✗ If an error occurs during transmission, the whole block of data is lost instead of just a single character (can consist of >100 characters).
- ✗ The sender cannot transmit characters simply as they occur and consequently has to store them until it has built up a block – unsuitable for applications where characters are generated at irregular intervals.

As a result, this is normally used for high-speed communication between computers.

Asynchronous Transmission vs Synchronous Transmission

- Serial transmission can be either asynchronous or synchronous.
- In synchronous transmission a receiver and transmitter is synchronised and a block of characters is transmitted along with the synchronisation transmission while asynchronous transmission is character-oriented meaning each character carries start and stop bits
- Synchronous transmission is used for high speed transmission while asynchronous transmission is used for low speed transmission.

4.8 Circuit Switching and Packet Switching

4.8.1 Router

Definition: A router is a networking device that connects multiple networks. It forwards packets from one network to another. It allows a LAN and a WAN to be connected.

Components:

Routing table:	maps output ports for different network addresses.
Routing protocol:	exchange routing information, construct routing table.
Buffer at o/p port:	stores packets before they are transmitted out.

4.8.2 Circuit Switching

Definition: Circuit switching provides a dedicated communications channel for two nodes to communicate with each other. This communications channel is set up before the nodes communicate. The circuit guarantees the full bandwidth of the channel until the communication session ends.

4.8.3 Packet Switching

Process:

At the sender

1. The data to be sent is split up into multiple packets of a certain size.
2. A header containing the destination MAC address, the length of the data, and the packet sequence number (determines the order to reassemble the packet at the receiver) is added to each packet.
3. The packets get routed independently to its destination, following different paths along its way.

At the router

4. The packet is received and temporarily stored (buffered) in the router
5. The packet is then passed on to the next router. The next router the packet goes to depends on the destination MAC address.
6. Steps 4 and 5 are repeated until the packet reaches the destination node.

At the destination

7. Once all the packets arrive at the destination, the packets are reassembled into the original data in the correct order using the packet sequence number.