

OCR Computer Science A Level

1.3.3 Networks

Intermediate Notes



Specification

1.3.3 a)

- Characteristics of a Network
- Importance of Protocols and Standards

1.3.3 b)

- The internet Structure:
 - The TCP/IP stack
 - Protocol Layering
 - LANs and WANs
 - DNS
 - Packet and Circuit Switching

1.3.3 c)

- Network Security and Threats
- Firewalls
- Proxies
- Encryption

1.3.3 d)

- Network Hardware

1.3.3 e)

- Client-server
- Peer-to-peer



Networks and Protocols

Characteristics of a network

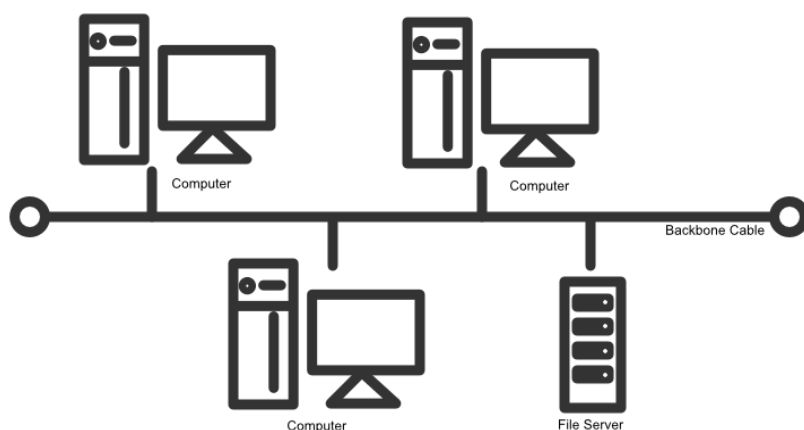
A **network** is the name given to **two or more** computers connected together with the ability to **transmit data** between each other. There are two main types of networks: **Local Area Networks** and **Wide area networks**.

Local area network (or LAN) is the name given to a network which is spread over a **small geographical area** or a **single site**, for example: a school. A wide area network (or WAN) is the name given to a network which is spread over a **large geographical area**.

There are two types of network topology:

- 1) **Physical** topology: the **physical layout** of the wires and components which form the network. Examples include bus, star and mesh.
- 2) **Logical** topology: the layout which shows how **data flows**.

Bus Topology



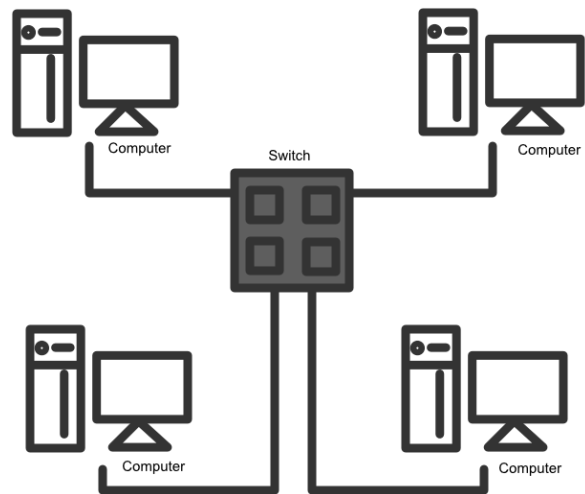
In a bus topology, all the **terminals** (devices) are connected to a **backbone cable**, the ends of which are plugged into a **terminator**.

Advantages of Bus Topology	Disadvantages of Bus Topology
<ul style="list-style-type: none"> • Relatively inexpensive to set up • Doesn't require any additional hardware 	<ul style="list-style-type: none"> • If backbone cable fails, the entire network gets disconnected • As traffic increases, performance decreases • All computers can see the data transmission



Star Topology

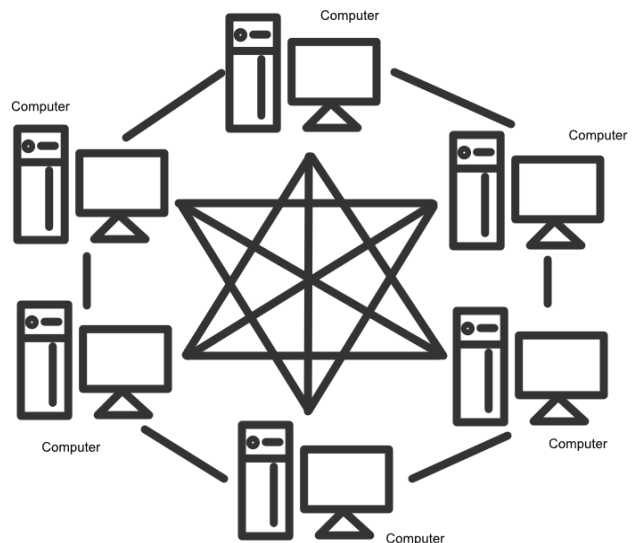
Star topologies use a central node, often a **switch**, to direct data through the network. Every device on the network is connected to the switch.



Advantages of Star Topology	Disadvantages of Star Topology
<ul style="list-style-type: none"> Performance is consistent even with heavy network traffic If one cable fails, only that station is affected Easy to add new stations 	<ul style="list-style-type: none"> Expensive due to switch and cabling If the central switch fails the rest of the network fails

Mesh Topology

In a mesh topology, every node is connected to every other node. Mesh topologies are most commonly found with wireless technology such as **Wi-Fi**.



Advantages of Mesh Topology	Disadvantages of Mesh Topology
<ul style="list-style-type: none"> • If using a wireless network, there is no cabling cost • As the number of nodes increase, the reliability and speed of network becomes better • Nodes are automatically incorporated • Nodes don't go through a central switch, improving speed 	<ul style="list-style-type: none"> • If using a wireless network, devices with wireless capability (which increases cost) must be purchased • If using a wired network, a large quantity of cable is required compared to other network topologies like bus and star • Maintaining the network is difficult

Protocols

A protocol is a **set of rules** defining how two computers **communicate** with each other. Protocols are standard so that all devices have a designated method of communicating with each other, regardless of manufacturer.

Examples of commonly used protocols are:

- **HTTP** – Used for web page rendering
- **TCP/IP** – A networking protocol used in the routing of packets through networks
- **POP3** and **IMAP** – Mailing protocols, used for email access.
- **FTP** – Used for the transmission of files over networks.

The Internet Structure

The Internet is a **network of networks** which allows computers on opposite sides of the globe to communicate with each other. Continents are connected to each other using **large international backbone cables**.

The TCP/IP Stack and protocol layering

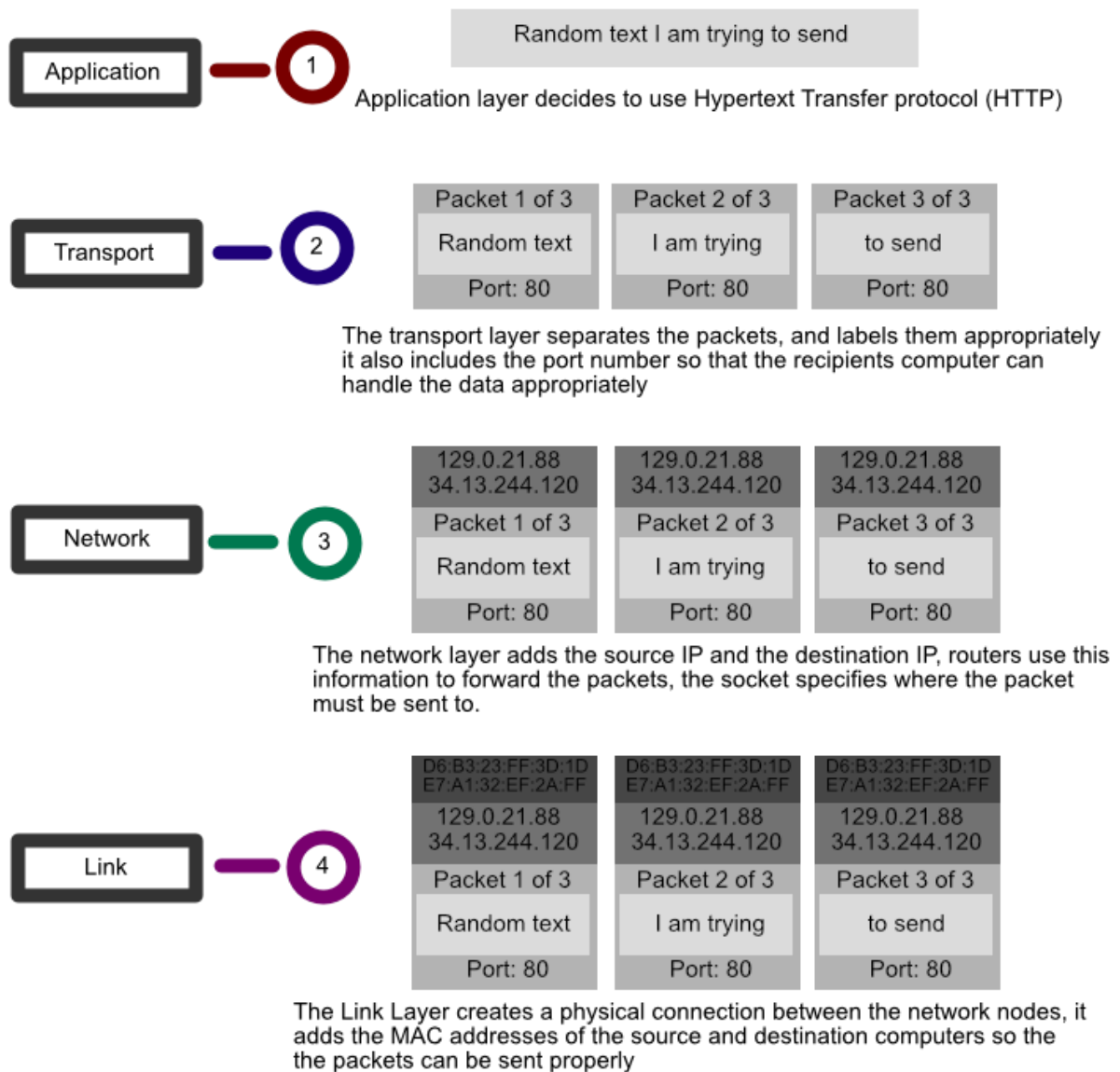
TCP/IP is a **stack of networking protocols** that work together passing packets during communication. They work as follows:

- Application Layer
 - Specifies the **protocol** that needs to be used in order to **relate the application that's being sent**.
 - For example, if the application is a web browser then it would select the appropriate protocol such as HTTP
- Transport Layer
 - Establishes **end-to-end connection** between the source and the recipient computer
 - **Splits up data into packets** and labels these packets with their packet number, the total number of packets original data was split up into and the port number being used for communication



- Network Layer
 - Adds the source and destination **IP addresses**.
 - **Routers** use IP addresses and sockets to forward the packets to the specified destination
- Link Layer
 - Adds the **MAC address** identifying the **Network Interface Cards** of the source and destination computers

Below is a diagram showing exactly what happens in the process of sending a file.



LANs and WANs

As specified earlier, a LAN is a local area network and a WAN is a wide area network. A LAN is a network spread over a **small geographical area** while a WAN is typically spread over a **large geographical area**. Infrastructure used in WANs is owned by third-parties. The largest WAN is the Internet, and is made up of a series of smaller networks.

DNS

The **domain name system** (DNS) is the system used to **name** and **organise internet resources**. It is a hierarchy, in which each smaller domain is separated from the larger domain by a full stop. Domain names are much easier to remember than IP addresses, which is why they are used to link to servers across the world. The role of the domain name system server (DNS server) is to translate these domain names into IP addresses when we wish to access a website.

Network Communication

Data Packets

Packets are **segments of data**. They contain various information:

- Header:
 - Sender and recipient **IP addresses**
Allow the packet to be delivered to the correct destination and enables the recipient device to trace **where the packet came from**.
 - **Protocol** being used
Allows the recipient computer to interpret the packet.
 - **Order** of the packets
Used to reconstruct data from packets
 - **Time To Live** / Hop Limit
Tells the packet **when to expire** so that it does not travel forever.
- Payload
 - Raw **data** to be transmitted
- Trailer
 - **Checksum**, or **cyclic redundancy check**
Code used to detect whether any errors have occurred during transmission.

Circuit Switching and Packet Switching

There are two techniques using which networks exchange data: **circuit switching** and **packet switching**.

Packet switching is a method of communication in which data is communicated using **packets** across a network. Packets are sent across the most efficient route, which can vary for each packet.



Advantages	Disadvantages
Multiple methods to ensure data arrives intact eg. checksums and cyclic redundancy checks	Time is spent deconstructing and reconstructing the data packets
Multiple routes can be used between devices, so if one path breaks, another can be used.	Must wait for all packets to arrive before data can be received.
Packets can be transferred over very large networks to allow communication globally.	

Circuit switching is a method of communication where a [direct link](#) is created between two devices. This direct link is maintained for the duration of the [entire conversation](#) between devices. This requires the two devices to transfer and receive data at the [same rate](#).

Advantages	Disadvantages
Data arrives in a logical order which results in a quicker reconstruction of the data.	Bandwidth is wasted during periods of time in which no data is being sent.
Enables two users to hold a call without delay in speech.	Devices must transfer and receive data at the same rate .
	Using switches means electrical interference may be produced which can corrupt or destroy data.
	Ties up sections of the network which cannot be used by others data until transmission has been completed

Network Security and Threats

Firewalls

A firewall is a device designed to [prevent unauthorised access](#) to a network. A firewall consists of two network interface cards (NICs) between the user and the Internet. The firewall passes the packets between these two NICs and compares them against a set of rules set by the firewall software. The preconfigured rules are called [packet filters](#).

Packet filtering / static filtering [limits network access](#) in accordance with [administrator rules](#) and policies. It works by examining the source IP, destination IP and the protocols being used as well as the ports being requested.

Proxies

A proxy server acts as an intermediary, collecting and sending data on behalf of the user. There are several benefits of using proxies:

- The privacy of the user is protected and they [remain anonymous](#)
- The proxy server can cache frequently used website data making it [faster to load](#)



- Proxies can reduce overall web traffic
- Can be used by administrators to **prevent access** to **sensitive or irrelevant information** at work or at school

Encryption

Encryption is a way of **keeping data secure** when transmitting it over the Internet. Encryption makes data unreadable if it is intercepted. Data is encrypted and decrypted using a set of keys.

Synoptic Link

Encryption is a way of mapping data so it's unreadable if intercepted

Encryption is covered in **1.3.1 Compression, Encryption and Hashing**

Network Hardware

Maintaining a network requires various pieces of hardware, some of which are built into devices, such as a network interface card (NIC) while others, like switches, are not.

Network interface cards (NIC)

A network interface card is the card required to **connect a device to a network**. This is built into the device and assigns a unique media access control (MAC) address to each device. The MAC address is a **48-bit value** coded into the device and is written as a **twelve digit hexadecimal** number.

Synoptic Link

Hexadecimal is a a number base which uses the numbers 0–9 in addition to the letters A–F.

Hexadecimal is covered in **1.4.1 Data Types**

Switch

A switch is a device used to **direct the flow of data** across a network. Switches are most commonly used in networks using a **star topology**.

Wireless Access Point (WAP)

This is a device which allows a device to **connect to a network**. It is more commonly combined with a **router** to enable internet access. These are used in **mesh networks**.

Routers

A router is used to **connect** two or more **networks together**. Routers allow private, home networks to connect to the Internet.

Gateway

A gateway is used when **protocols are not the same** between networks. It **translates** the protocols so that networks can communicate with each other. Gateways work by removing the header from packets before adding the data to packets using the new protocol.



Client-Server and Peer-to-Peer

Client-server

Client-server networks consist of **terminals** known as clients connected to a **server**. The server is a **powerful, central computer**. It holds all of the **important information and resources** and has **greater processing power** than the terminals.

Advantages of Client-server	Disadvantages of Client-server
<ul style="list-style-type: none"> • More secure as data is stored in one location • Central backups are carried out so there is no need for individual backups • Data and resources can be shared between clients 	<ul style="list-style-type: none"> • Relatively expensive to set up • Functionality of terminals depends on the server; if this fails, performance falls • Trained staff are required to maintain the server

Peer-to-Peer

A network in which **computers are connected to each other** so that they can share files. Each device effectively acts as both a server and client, as it can both provide and request resources. Peer-to-peer networks are used in **piracy**, since it's almost **impossible to trace** the origin of files.

Advantages of Peer-to-peer	Disadvantages of Peer-to-peer
<ul style="list-style-type: none"> • Cheaper to set up • Allows users to share resources • Easy to maintain • Not dependent on a central server • Specialist staff are not required 	<ul style="list-style-type: none"> • Impossible to trace the origin of files • Backups must be performed separately • Poorer security • May be difficult to locate resources

