OCR Computer Science GCSE

1.3 – Computer networks, connections and protocols

Advanced Notes

1.3.1 Networks and topologies

What is a computer network?

A computer network is a group of connected devices, such as computers, printers, and smartphones, that share data and resources like files or internet access.

Types of networks

LAN (Local Area Network)

- Covers a relatively small geographical area (e.g., a school, home, office)
- Often owned and managed by a single person or organisation
- Only connected to a small number of devices and users

WAN (Wide Area Network)

- Covers a wide geographical area (e.g., the internet, a global company)
- Usually made up of several LANs connected together
- Often under collective ownership
- Usually slower than LANs
- Cost per byte for transmission is much higher on WANs than on LANs

Factors that affect the performance of networks

Network performance refers to how well a network functions, specifically in terms of its speed and reliability. There are several factors that affect how well a network performs.

Bandwidth

Bandwidth refers to the maximum amount of data that can be transmitted over a network within a given time; it's often measured in bits per second (bps).

A higher bandwidth allows for faster data transfer and better overall performance, especially when handling large files or many users simultaneously. Insufficient bandwidth can lead to slow loading times.

Number of devices connected

The number of devices on a network significantly impacts performance, especially if bandwidth is limited. As more users connect and access the network, the available bandwidth must be shared, potentially slowing down everyone's connection.

Roles of computers in different types of networks

Depending on the network model, computers can play different roles within a network.

Client-server

In a client-server model, computers are separated into two roles: clients and servers.

Servers are powerful computers which control the network, and provide services and resources to clients, often carrying out the majority of the processing. They wait for requests from clients and then respond to them.

Clients are the computers that humans use on a network, such as phones and laptops. They send requests to servers and then wait for responses.

Peer-to-peer

In a peer-to-peer model, all computers (peers) on the network have equal status and responsibilities. Each peer can act as both a client and a server - they can request resources from other peers and also provide resources in return.

There is no central server controlling the network, so files and services are shared directly between devices.

Local Area Network (LAN) hardware

There are several hardware components required to connect stand-alone computers into a Local Area Network (LAN).

Wireless access points

Wireless access points use radio transceivers to allow devices to connect wirelessly to a network.

Routers

A router is used to connect two or more networks together. Routers allow LANs such as private home networks to connect to the Internet.

Switches

A switch connects each device on a network. It receives data packets for all of the clients connected to it and is responsible for sending them only to the correct device.

NIC (Network Interface Controller/Card)

NICs are hardware components inside devices that enable them to connect to networks. They convert data that needs to be sent across a network into signals that can be transferred: in a wired network, these signals will be voltages or pulses, and in wireless networks they'll be radio waves.

Transmission media

Transmission media are the physical or wireless methods used to carry data around the network. This includes copper Ethernet cables, fibre-optic cables, or wireless signals like radio waves.

The internet

The internet is a network of smaller computer networks. It allows devices around the world to communicate and share data.

DNS (Domain Name System)

The Domain Name System (DNS) is a system made up of multiple Domain Name Servers that convert URLs (like www.example.com) into IP addresses that computers use to find and communicate with each other. To convert the URL, the DNS server is checked for the URL entered. If it is found, the corresponding IP address is returned. If not, it queries another server, this process is then repeated until it is found.

Hosting

Hosting is the process of storing a website's files on a server and making it accessible to users over the internet. Websites must be hosted on a web server to be available online.

Web servers and clients

A web server stores and provides access to web pages. A client (like a web browser on a laptop or phone) sends a request to the server, and the server responds by sending the data (e.g. a web page). This is an example of a client-server model, where servers provide services and clients use them.

Another example of the client-server model is file servers, which allow clients to store their files and retrieve them.

The cloud

The cloud refers to using remote servers over the internet to store files or run software and services. This means data and programs can be accessed from anywhere with an internet connection.

Advantages of the cloud:

- Accessible from anywhere
- No need to manage or upgrade hardware

Disadvantages of the cloud:

- Requires an internet connection
- Data may be less secure (stored on third-party servers)
- Ongoing subscription costs
- Less control over data and software

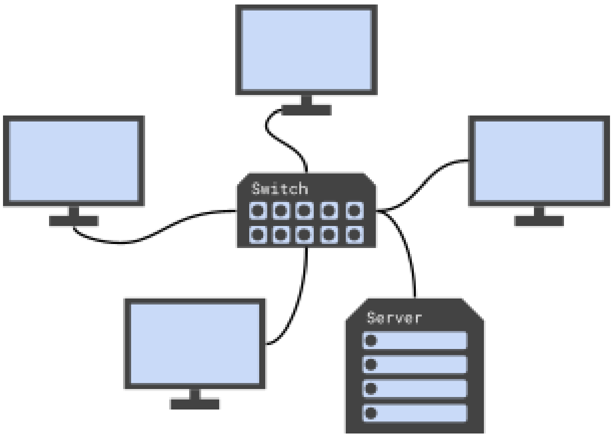
Network topologies

The topology of a network is the way that the devices are connected. Two common network topologies are the star topology and mesh topology.

Star topology

Each client has its own direct connection to the central switch. The switch receives data packets for all of the clients connected to it and is responsible for delivering them to the correct recipient.

A server or shared device such as a printer can be added to the network in the same way that clients are connected to the central switch.



Advantages	Disadvantages
Packets are sent directly to their recipient, over a cable that is connected only to the recipient. Other clients on the network cannot see packets that aren't intended for them.	Should the central switch fail, all communication over the network is stopped.
It is easy to add and remove clients to and from the network.	Expensive to install due to the amount of cable required.
Each cable has just one device communicating over it, eliminating the possibility of collisions.	
The failure of one cable does not affect the performance of the rest of the network.	

Mesh topology

Each device is connected directly to multiple other devices in the network. Data is sent across the network by taking the most efficient path from sender to recipient, and can be passed through other devices to reach its destination. Devices can be added to the network by creating new connections with one or more existing devices.

Advantages	Disadvantages
Data can always take an alternative route if one device or connection fails, making the network very reliable.	Requires a lot of cabling and network ports, especially in a fully connected mesh (every device is connected to every other device).
Data can be transferred quickly and efficiently using the shortest path available.	

1.3.2 Wired and wireless networks, protocols and layers

Modes of connection

Wired

- **Ethernet** is a common method for connecting devices in a local area network (LAN) using wired connections. It allows computers, printers, and other devices to communicate and share data quickly and reliably over physical cables.

Advantages	Disadvantages
Faster and more reliable connection with higher data transfer speeds.	Less convenient, as devices must be physically connected by cables.
More secure, as data travels through physical cables and is harder to intercept.	Harder to set up and expand, especially over long distances or in large buildings.

Wireless

- **Wi-Fi** is a wireless technology that allows devices to connect to a local area network (LAN) and access the internet without using cables. It uses radio waves to transmit data between devices and a router.
- **Bluetooth** is a wireless technology that enables short-range communication between devices, typically within a range of about 10 meters. It allows devices to connect and exchange data without the need for cables or wires, using radio waves to establish a connection.

Advantages	Disadvantages
More convenient and flexible - users can move freely without being tied to cables.	Slower and less reliable than wired connections - signal can be affected by walls or interference.
Easier and cheaper to install. Also easier to add new users to the network.	Less secure, as signals can be intercepted more easily - however, if encrypted then these won't be intelligible.

Encryption

Encryption is a method of converting data into a coded format so that only authorised users with the correct decryption key can understand it. For example, when you shop online, your payment details are encrypted so that, if the data is intercepted, it cannot be read by hackers.

IP addressing and MAC addressing

IP addressing

IP addressing is a system for uniquely identifying devices connected to a network. There are two main versions: IPv4 and IPv6. IPv4 addresses are 32-bit numbers, typically written as four decimal numbers separated by dots (e.g., 192.168.1.1). IPv6 addresses are 128-bit numbers, expressed as eight groups of four hexadecimal digits, separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

A MAC (Media Access Control) address is a unique identifier, permanently assigned to a device's Network Interface Controller (NIC) during its manufacture. It's a 12-digit hexadecimal number, typically displayed in pairs separated by colons or hyphens, like 00:1A:2B:3C:4D:5E. MAC addresses are crucial for identifying devices on a local network and ensuring data is delivered to the correct device, even when IP addresses change.

Standards

Standards are agreed guidelines that provide rules for areas of computing. Standards allow hardware/software to interact across different manufacturers/producers.

Communication protocols

A communication protocol is a set of rules for transferring data. Different types of protocols are used for different purposes. Common protocols are explained in the table below.

Protocol	Purpose
TCP/IP (Transmission Control Protocol / Internet Protocol)	TCP ensures that data sent over a network arrives completely and in the correct order. It breaks data into packets and checks that all packets are received properly, requesting any missing ones to be resent. IP is responsible for addressing and routing data packets across networks. It ensures that data packets can find their way from the sender to the correct destination computer using IP addresses.
HTTP (Hypertext Transfer Protocol)	HTTP is the protocol used for transferring web pages and other content between web servers and browsers. It defines how web browsers request pages and how web servers respond with the requested content.
HTTPS (Hypertext Transfer Protocol Secure)	HTTPS is the secure version of HTTP that encrypts data being transferred between web browsers and servers. It protects sensitive information like passwords and credit card details from being understood if it is intercepted by hackers.
FTP (File Transfer Protocol)	FTP is used to transfer files between computers over a network, such as the internet. It allows users to upload or download files to and from a remote server, often used for managing files on websites.

POP (Post Office Protocol)	POP allows users to access their emails stored on a remote email server. It downloads emails to the client and typically removes them from the server, allowing access to messages offline.
IMAP (Internet Message Access Protocol)	IMAP allows users to access and manage their emails stored on a remote email server. It enables emails to be read and organised from multiple devices whilst keeping them synchronised on the server. It does not remove or locally download emails from the server like POP.
SMTP (Simple Mail Transfer Protocol)	SMTP is used for sending emails from one email server to another across the internet. It handles the delivery of outgoing emails from your email client to the recipient's email server.

Layers

Network communication is often organised into layers, with different protocols operating at each layer. Each layer handles a different part of the communication process and only interacts with the layers directly above and below it. The TCP/IP model includes four layers, however you aren't required to know the details of these layers.

Benefits of using layers

- Each layer is self-contained, so it can be developed and updated independently.
- It makes troubleshooting easier, since problems can be identified in a specific layer.