OCR A Level Computer Science

Your notes

3.3 Networks

Contents

Your notes

Networks

What is a Network?

- A network is a set of interconnected devices (such as computers, printers, and servers) designed to share resources, exchange data and communicate with each other
- The main purposes of a network are to enable data sharing, resource sharing, communication, and collaboration

Purpose & importance of protocols

- **Network protocols** define the rules and formats that devices must follow to communicate with each other over the network
- They ensure successful and secure data transmission, and help maintain order and efficiency in communications
- Examples of protocols include HTTP, FTP, TCP/IP, and SMTP, among others

Understanding the term "standard"

- A standard in a network or any data transfer situation refers to a set of guidelines or frameworks that govern how a task should be performed or how a product should function
- Standards ensure compatibility, interoperability, and consistency across different devices and software

Purpose & need for standards in a network

- Standards enable different network devices, regardless of their manufacturer or model, to work together seamlessly
- They ensure that data can be correctly interpreted and processed by the receiving device, regardless of where or how it was sent
- Standards support network expansion and the integration of new technologies without disrupting existing operations
- They foster innovation and competition by providing a common ground for all manufacturers and developers

Common Internet Protocols

Protocol	Notes
HTTP (HyperText Transfer Protocol)	Primary protocol for transferring web content (text, images, video) Works as a request-response protocol in a client-server computing model
HTTPS (HTTP Secure)	A version of HTTP, but with **encryption** for security Used for secure transactions like online banking and shopping
SMTP (Simple Mail Transfer Protocol)	The standard for sending email messages between servers It is also used to send emails from a client to a server for further forwarding
FTP (File Transfer Protocol)	Used for transferring files from one host to another over a network Provides authentication (username and password) and can manage file directories
ARP (Address Resolution Protocol)	Translates IP addresses into MAC (Media Access Control) addresses This ensures that data packets reach the correct device on a network
TCP (Transmission Control Protocol)	Part of the main suite of protocols used in the Internet Protocol Suite Provides reliable, ordered, and error-checked delivery of a stream of packets
UDP (User Datagram Protocol)	A simpler message-based connectionless protocol UDP does not guarantee delivery by disregarding order and error-checking, making it faster
IP (Internet Protocol)	Functions mainly by addressing and routing packets of data from the source to the target device

Your notes

WORKED EXAMPLE

The internet can be considered an example of a WAN.
The internet uses a set of protocols referred to as the TCP/IP stack. The TCP/IP stack consists of four different layers, each with its own set of protocols.

Explain why protocols are important on a network

2 marks


Your notes

How to answer this question:

- You need to know what network protocols are and why they are important for network communication:
  - They allow us to communicate over a network by ensuring that all communicating parties use the same rules and standards
  - Whatever data or signals are sent need to be understood commonly by both the sender and the receiver

Answer:

Example answer that would get full marks:

Protocols are rules that must be followed to allow communication over a network. They ensure that all devices follow the same rules and standards so that they interpret data and signals in the same way.


Your notes

TCP/IP

What is Protocol layering & the TCP/IP stack?

- Protocol layering is the way network **protocols** are divided into layers, each of which performs specific functions
- This allows for modular design, simplifies troubleshooting, and promotes interoperability
- This means that protocols that operate at the network layer can be altered independently of application layer protocols
- TCP/IP stack is the suite of protocols that the internet is based on
- Network protocols are organised into layers to handle different aspects of communication tasks

Why use Layering?

- Modularity: By breaking the complex process of networking into more manageable layers, it's easier to design, implement, and troubleshoot networks
- **Interoperability**: Layering allows different technologies to work together seamlessly. E.g. an application can send data to another application on a different device without knowing the details of how the network structure in between works
- Ease of Updates: With a layered model, changes can be made to one layer without affecting others. This makes updates and improvements easier to implement
- Specialisation: Each layer can be specialised to perform its functions without worrying about the specifics of other layers. This allows for more effective and efficient design

The 4 layer TCP/IP model

- TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet
- This model splits the various protocols into four layers:
  - Application
  - Transport
  - Internet
  - Link

Application layer

- This is the layer where the communication process begins
- The application layer interacts directly with software applications, such as web browsers and email clients
- The application layer prepares data for transmission over the network by converting it into a format that can be sent and received over the network (known as encapsulation)

Transport layer

- The transport layer receives data from the application layer
- The transport layer is responsible for end-to-end communication between the source and destination
- The transport layer breaks the data it receives down into smaller units called packets
- Each packet is assigned a port number (so the data can be reassembled in the correct order at the destination)
- Each packet is also labelled with a header containing information (e.g. the packet number)

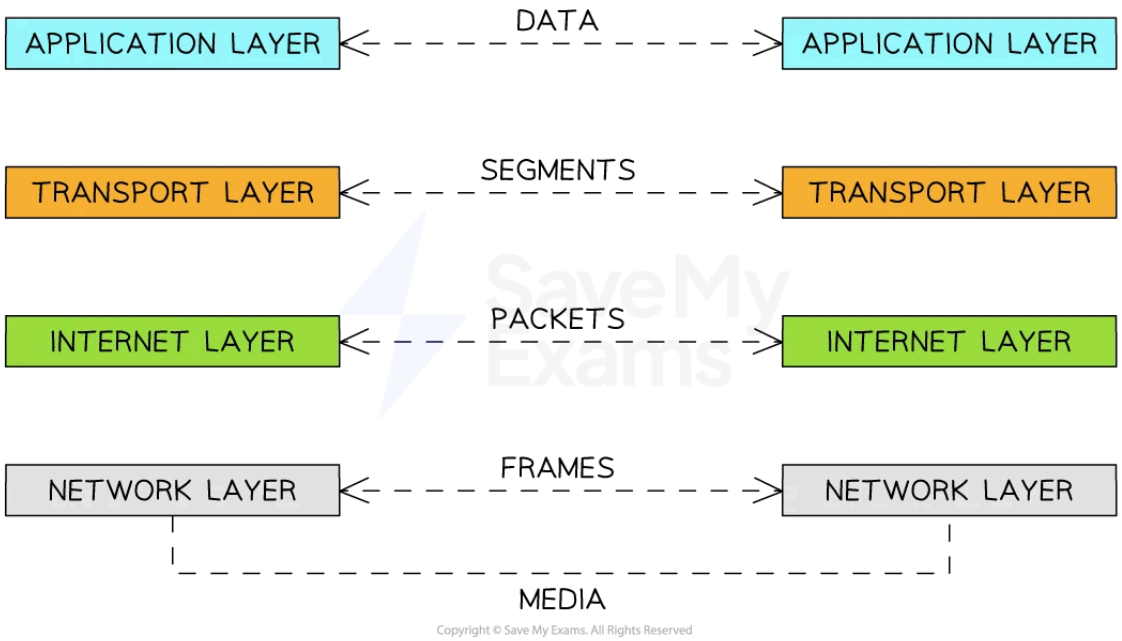
Internet layer

- The internet layer receives packets from the transport layer
- It adds a header to each packet, including the sender's **IP address** and the receiver's IP address
- The internet layer is responsible for routing each packet across the network using the IP addresses in the headers

Link layer

- Also known as the network interface layer
- The link layer receives packets from the Internet layer and prepares them for transmission over the physical network
- The link layer translates the digital packets into an electrical, optical, or wireless signal that can be sent over the network
- Once the signal reaches the receiving end, the network layer translates it back into digital packets


Your notes



TCP/IP stack layers

Your notes

Key points

- At each layer of the TCP/IP model, specific tasks are performed to prepare data for transmission over the network
- The process is reversed at the receiving end, with each layer removing its specific header and performing its specific tasks to get the data back into a format that the receiving application can use

Data transmission over the Internet

- The Internet relies on packet-switched networks, where data is broken down into packets, each of which can take its own route to the destination
- Packets are units of data. They are small and easier to manage
- Each packet contains:
  - The payload (the data)
  - A header (with metadata like source and destination IP addresses)
  - A footer (to signify the end of the packet)

IP addresses

- An IP address is a unique identifier for a device on a network
- IP addresses are used to deliver packets to the correct destination
- Two versions are in use: IPv4 (e.g. 104.22.74.202) and IPv6 (e.g. 0000:0000:0000:0000:0000:ffff:6816:4aca)

Your notes

WORKED EXAMPLE

A company releases an Internet connected fridge. Users can email messages to the fridge and it puts them on its display.

The fridge uses the TCP/IP stack.
Explain what is meant by the term 'TCP/IP stack'.

3 marks

How to answer this question:

- You need to expand the acronym 'TCP/IP' to show the examiner you know what it stands for
- You need to explain what network protocols are and that they are organised into various layers
- You need to describe what happens to the data as it is passed from one layer to the next

Answer:

Example answer that gets full marks:

The TCP/IP stack stands for Transmission Control Protocol / Internet Protocol and refers to a set of layered protocols (rules) used for communicating across the Internet. Each protocol belongs to one of four different layers: the application layer, the transport layer, the internet layer and the network layer. Each layer, starting at the application layer, takes data and encapsulates it before passing it to the next layer.

Your notes

Domain Name System (DNS)

What is the Domain Name System?

- The Domain Name System (DNS for short) can be thought of as the Internet's equivalent to a phone book
- It is essentially a directory of domain names and is used to translate human-readable **domain names** to the numeric IP addresses that computers use
- When you type a **URL** into your browser, the DNS translates the domain name into its associated IP address so your computer can connect to the server hosting the website
- Without DNS, we would have to remember the IP address of every site we want to visit
- When a domain is newly registered, or a server changes its IP address, the DNS record for that domain needs to be updated in what's known as DNS propagation

Components of DNS

DNS resolver

- The first stop in the DNS lookup process, usually provided by your internet service provider (ISP) or a third-party service like Google DNS or OpenDNS

Root servers

- The resolver asks a DNS root server to find the top-level domain (like .com, .org, .edu)

TLD (Top-Level Domain) servers

- The root server directs the resolver to a TLD server, which stores the information of the domain

Authoritative DNS servers

- The TLD server then responds with the IP address of the domain's authoritative DNS server, which the resolver asks for the IP of the domain

Benefits of DNS

- DNS allows us to use easily remembered domain names instead of hard-to-remember IP addresses
- DNS servers handle the mapping between domain names and IP addresses, relieving end users and system administrators from the task

What happens when you type a URL into a web browser?


Your notes

1. **URL Entry:** The user enters the URL of a website into the web browser
2. The **computer checks its local cache** to see if it contains the IP address of the URL from a previous request
3. **DNS Query:** The web browser sends a query to a DNS server (usually hosted by your ISP) to translate the URL (domain name) into an IP address
4. **DNS Resolver:** The DNS resolver checks its cache to see if it has the IP address for the requested domain. If not, it sends the request to the DNS root servers
5. **Root Server Query:** The root server directs the resolver to a Top-Level Domain (TLD) server (like .com, .org) based on the extension of the URL
6. **TLD Server Query:** The TLD server then provides the resolver with the IP address of the domain's authoritative DNS server
7. **Authoritative Server Query:** The resolver queries the authoritative DNS server for the IP address of the domain
8. **Retrieve IP Address:** The authoritative DNS server responds with the IP address for the requested domain
9. **Request the Web Page:** The web browser sends an HTTP or HTTPS request to the IP address it received
10. **Server Response:** The server at the given IP address processes the request and sends back the data for the web page (HTML, CSS, JavaScript, etc.)
11. **Render the Web Page:** The web browser renders the received data into the web page that you see

- DNS (Domain Name System) translates human-friendly URLs into computer-friendly IP addresses
- HTTP/HTTPS are protocols defining how messages are formatted and transmitted on the World Wide Web
- The entire process happens in a matter of milliseconds, making the web user-friendly and efficient

WORKED EXAMPLE

Shreya is a web developer who creates web pages for a variety of different companies.

In order to view a website, a user enters a website address into their web browser such as http://www.ocr.org.uk. The website will then be displayed onto the user's screen.
Explain how the Domain Name System (DNS) plays a role in websites being loaded.

4 marks

How to answer this question:

- Since this question is worth 4 marks you need to explain how the DNS system works rather than just state what it does

Answer:

Example answer that would get full marks:

The DNS is a distributed system that finds the IP address of a particular URL.
The first thing that happens is that the URL is sent to a computer called a DNS resolver.
This checks its cache to see if it has already looked up this URL. If it hasn't it will then ask a top-level domain name server (TLD), which again checks its cache to see if it has done this lookup before.
If not it will then continue on and ask the authoritative name server for that domain.


Your notes

Your notes

LAN & WAN

What is a Local Area Network (LAN)?

- LANs are networks that are contained within a **small geographical location**
- Typically, **all the hardware used to make a LAN is owned by a single entity**
  - This makes them more secure than WANs, which have connections owned by third-party companies
- A LAN is a network that is built using hubs and/or switches that connect several devices
- It is common for one hub or switch to be connected to a router, which will allow the LAN to connect to other networks, such as the Internet
- A LAN can offer many advantages, such as:
  - **Centralised management** - A LAN allows centralised management of updates, backups and software installations
  - **Security** - A LAN can secure its devices with the use of firewalls, antivirus software and other security features to prevent unauthorised access
  - **File Sharing** and collaboration - A LAN allows users on the network to share resources such as printers and other peripherals. Users of the network can also collaborate and share files and folders
- Disadvantages of a LAN include:
  - If **hardware fails, the network may not function** properly or even at all
  - Networks are more **prone to attacks** than standalone computers
  - **Access to data and peripherals can be slow** depending on network traffic when compared to locally stored data and locally connected peripherals
  - **Maintenance** - LAN networks require maintenance to ensure that software is up to date. Upgrades and backups can be costly

What is a Wide Area Network (WAN)?

- WANs are collections of LANs spread over a large geographical area
  - E.g. a company may connect two LANs between two cities to create a WAN

- The individual LANs are usually connected via third-party connections
- e.g. leased lines from ISPs or Telecommunications companies

Your notes

WORKED EXAMPLE

The internet can be considered an example of a WAN.

Describe what is meant by the term 'WAN'.

2 marks

How to answer this question:

- For 2 marks, you need to make 2 points about what a WAN is
- Since the question uses WAN as an acronym, it is a good idea to show you know what WAN stands for

Answer:

Example answer that would get full marks:

A WAN (short for Wide Area Network) is a network spread over a large geographical area such as a country.

WORKED EXAMPLE

A coffee company has coffee shops located across the country. Each shop has its own Local Area Network (LAN)

The company wants to connect the shops in a Wide Area Network (WAN).

Describe two characteristics of a LAN.

2 marks

How to answer this question:

- You need to make 2 points about how a LAN is different from a WAN:
  - LANs cover a small geographical area
  - The hardware that makes up the LAN is typically owned by one company
  - For this reason, a LAN is considered to be more secure than a WAN

Answer:

Example answer that would get full marks:

LANs are considered more secure than WANs since the LAN's connections are owned by the organisation that owns the LAN.

Next topic

Your notes

Your notes

Packet & Circuit Switching

What is Packetising?

- Packetising is a process where a large message is divided into smaller, manageable units called packets
- Each packet can then be sent individually over the network

Packet formation

- When a message is too large to be sent as a single unit, it's divided into smaller packets
- Each packet is typically composed of a header, payload (actual data), and a footer (or trailer)

Use of headers

- Headers are important because they contain information necessary for the packet's delivery
- Typical information in a header includes:
  - Source **IP address**: identifies the sender of the packet
  - Destination IP address: identifies the intended recipient of the packet
  - Sequence Number: helps in reassembling the packets back into the original message at the receiving end
  - **Protocol**: identifies the transport protocol (TCP, UDP, etc.)
  - Packet Length: indicates the size of the packet
  - Checksum: a value used for error-checking

Packet transmission

- After being packetised and **encapsulated** with headers (and trailers), packets are transmitted individually across the network
- Packets might take different routes to reach their destination

Packet reassembly

- When the packets reach their destination, they are reassembled back into the original message using information in the headers

Your notes

Packet switching

- Packet switching is a networking communication method that breaks down data (large files, emails) into smaller packets, sends these packets separately along different routes, and then reassembles them at their destination

Benefits	Drawbacks
Efficient use of network resources as packets can follow different paths to the destination, using more of the available bandwidth	Not ideal for real-time services like video calling or VoIP, which require a steady stream of data without delays
More reliable, as if a single packet fails to reach its destination, only that packet needs to be resent, not the entire data stream	Packets can arrive out of order, requiring reassembly and error-checking
Lower cost due to shared network resources	Potential for congestion in the network

Circuit switching

- Circuit switching is a communication method where a dedicated communication path is established between two devices for the duration of their conversation (like a phone call), and all packets are sent along the same route

Benefits	Drawbacks
Ideal for real-time services, with a constant and steady data transmission rate	Less efficient, as resources remain allocated during the whole conversation, even when no data is being sent
No delays as a dedicated path is established	It is more costly due to the dedicated line requirement
Data arrives in order as it follows the same path	Less flexible and scalable, as adding new devices can be complexx

Packet switching vs Circuit switching comparison table

Packet Switching	Circuit Switching

Benefits	
Efficient use of network resources as packets can follow different paths to the destination, using more of the available bandwidth	Ideal for real-time services, with a constant and steady data transmission rate
More reliable, as if a single packet fails to reach its destination, only that packet needs to be resent, not the entire data stream	No delays as a dedicated path is established
	Data arrives in order as it follows the same path
Drawbacks	
Not ideal for real-time services like video calling or VoIP, which require a steady stream of data without delays	Less efficient, as resources remain allocated during the whole conversation, even when no data is being sent
Packets can arrive out of order, requiring reassembly and error-checking	More costly due to the dedicated line requirement
Network congestion can lead to packet loss	Less flexible and scalable as adding new devices can be complex


Your notes

Summary table for Circuit and Packet Switching

	Packet Switching	Circuit Switching
Definition	A mode of data transmission in which a message is broken into several parts sent independently, over whatever route is optimum for each packet, and reassembled at the destination.	A mode of data transmission in which a dedicated communication path is established between two devices through a network for the duration of their conversation.
Data Transmission	Data is broken into packets and transmitted independently.	Data is transmitted in a continuous stream.

Efficiency	High efficiency as network resources are shared and used as needed.	Lower efficiency as a dedicated path is maintained even when no data is being transmitted.
Reliability	More robust against network failures as packets can be rerouted.	Less flexible in handling network failures as the dedicated path, once broken, needs to be re-established.
Scalability	It is highly scalable as it can accommodate large amounts of data and many users.	Less scalable due to the need for dedicated paths for each communication.
Use Cases	Best for data that can tolerate some delay, such as emails and web pages.	Ideal for real-time services, like voice calls or video conferencing, that require low latency.

Your notes

EXAMINER TIP

- Avoid talking about the speed of data transmission in an answer to a question on packet or circuit switching. This will not get you a mark in the exam and, in some questions, is explicitly stated as not worthy of a mark. It is better to talk about higher bit rates or **bandwidth** (the number of bits sent per second) or the efficiency of the transmission

Your notes

Network Security & Threats

What are Common Network Threats?

Hackers

- Individuals or groups who exploit system vulnerabilities to gain **unauthorised access** to data
  Hacking involves gaining unauthorised access to a system or network to steal or manipulate data, disrupt services, or cause damage
  The aim of hacking can vary from personal gain to activism or cyber espionage

Viruses

- Malicious software programs designed to spread from one computer to another and interfere with normal operations
- A virus attaches itself to a legitimate program or file and then replicates itself to spread to other programs or files on the computer. It can cause damage to the system, including deleting data or damaging hardware

Malware

- Malware is malicious software designed to harm or gain unauthorised access to a system or network. Types of malware include:
  - A worm is similar to a virus but is a standalone program that can spread and replicate itself over computer networks. It can take up storage space or bandwidth
  - A Trojan horse is a program that disguises itself as a legitimate program or file, but when installed, it can delete data or damage hardware
  - Spyware is software that records all key presses and transmits these to a third-party
  - Adware is software that displays unwanted advertisements on the computer without the user's consent. Some of these may contain spyware, and some may link to viruses when clicked
  - Ransomware is malware that encrypts the user's files and demands a ransom payment to decrypt them. It can cause data loss and financial damage and disrupt business operations
- The aim of malware attacks can range from data theft to extortion or disruption of services

Denial of Service (DoS)

- A DoS attack is where a computer floods a server with lots of requests at the same time, which the server can't respond to, causing it to crash or become unavailable to users

- A DoS attack aims to disrupt the normal functioning of a system or network by denying users access

Distributed Denial of Service (DDoS) Attack

- A DDoS attack is where similar to a DoS attack but instead multiple computers are used as bots which send the requests to the server

SQL Injection

- An attack technique used to exploit security vulnerabilities in a website, where malicious SQL statements are inserted into an entry field for execution
- This can potentially expose a company's database to hackers

Phishing

- Attempting to acquire sensitive information by masquerading as a trustworthy entity in an electronic communication
- Phishing involves the user being sent an email that looks legitimate
- This email contains a link to a fake website where the user is encouraged to enter their details
- Phishing aims to steal sensitive information for personal gain or to use it for further cyber attacks

Pharming

- This is a cyber attack intended to redirect a website's traffic to another bogus site
- Pharming involves malware being downloaded without the user's knowledge
- This redirects the user to a fake website where they're encouraged to enter their personal details
- Pharming aims to steal sensitive information for personal gain or to use it for further cyber attacks

Social Engineering

- Social engineering involves manipulating individuals to gain access to confidential information or to perform an action that benefits the attacker
- This can include techniques such as:
  - Posing as someone else to gain trust or access to sensitive information - attackers might pretend to be a co-worker, IT support personnel, or a law enforcement officer to get people to divulge sensitive information or perform an action they wouldn't otherwise do
  - Enticing a victim with the promise of a desirable item to extract sensitive information or gain access to a system
  - Leaving a USB drive with a tempting label, like "salary information," in a public place and waiting for someone to pick it up and plug it into a computer - once the drive is connected to the computer,


Your notes

the attacker can access sensitive information or install malware
- Posing as a bank representative and asking for personal information to "verify your account"


Your notes

Network security

There are many different methods and techniques that have been developed to make networks more secure. Some of these include:

- **Firewalls**: Network security systems that monitor and control incoming and outgoing network traffic based on predetermined security rules
- **Secure Passwords**: Using strong, complex, and unique passwords helps to protect against unauthorised access
- **Anti-virus Software**: Programs designed to detect and neutralise or remove malicious software like viruses, worms, and Trojans
- **Anti-spyware Software**: Tools to detect and remove spyware and other kinds of malware
- **Two-factor Authentication (2FA)**: Adds an additional layer of security by requiring users to provide two forms of identification - usually a code sent to their phone or email as well as their password
- **Regular Software Updates**: Keeping all systems and software up-to-date ensures you have the latest security patches
- **Employee training** can be essential to instil a culture of security consciousness within the company
- **A strong security policy** (e.g. insisting on regular password changes) can further help in maintaining a secure network environment

Your notes

Network Hardware

What Hardware is Needed in a Network?

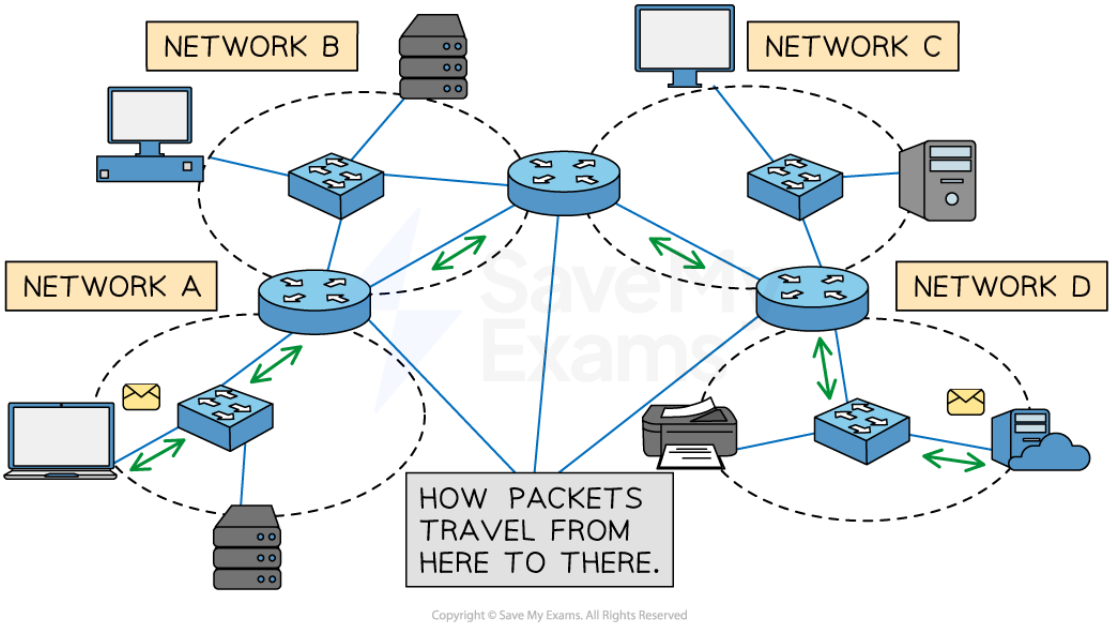
Modem

- A modem (**mod**ulator-**dem**odulator) is a device that modulates an analogue carrier signal to **encode digital information** and also demodulates a carrier signal to decode the transmitted information
- It **enables a computer to transmit data over telephone or cable lines** by converting digital signals into analogue and vice versa for receiving data
- It can be used for **DSL**, cable, or dial-up internet connections

Router

- A router is a network hardware device that routes data from a local area network (LAN) to another network connection - **it joins two networks together**
- Routers analyse data packets and determine the best path for the packet to reach its destination
- The router can **often feature additional functionalities** such as wireless networking, built-in firewalls for enhanced security, and network switch capabilities
- A router being used to connect a LAN to a WAN will have a public **IP address**, which has been assigned to it by an Internet Service Provider
- It is this public IP address that other routers use to identify and direct packets to the network
- An important role of the router is to analyse data packets and direct them to their destination
  - The **header** contains information about the packet
  - The **payload** is the actual data being sent
  - The IP address of both the sender and intended recipient is stored in the header of the data packet

Your notes



Multiple networks connected by routers, represented by the blue circular objects

- If the **data packet** is coming into the LAN, the router will send the data packet to the specific device within its LAN that the packet is meant for
- If the packet is being sent from a device within the LAN, it will read the header of the packet to determine the intended destination IP address
  - It might have to travel through several routers before it gets to its destination
  - Each pass from router to router is called a hop
  - It will then forward the packet to its destination
- The network access device or 'home hub' used in your home network will have a router built into it

Step	Description
1	A router receives incoming data packets from one network and analyses the packet header to determine the destination IP address
2	It then looks up the IP address in a routing table (routing table of known networks) to determine the next network where the packet should be sent

3	The router then forwards the packet to the appropriate network or device


Your notes

- Every router repeats this process the data packet passes through until it reaches its destination
- In addition to routing data between networks, routers can also perform other functions such as:
  - Assigning IP addresses to devices within the LAN
  - Filtering incoming traffic based on certain criteria, such as IP address, port number, or protocol type

Cables

- Cables are the physical paths for data to travel between devices in a network
- **Ethernet** cables, like Cat5, Cat5e, and Cat6, are common types of network cables used for wired networks. They can transfer data at various speeds (10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps)
- Fibre-optic cables use light to transmit data, offering much higher speed and larger data capacity

NIC (Network Interface Card)

- A network interface card (NIC) is a hardware component, historically a card inserted into a slot on the motherboard but now more likely to be built into the motherboard, that enables a device to connect to a network
- NICs have a built-in ethernet port and can be connected to a network via an ethernet cable
- It provides a dedicated, full-time connection to a network, converting the computer's data into a network-friendly format
- Every NIC has a unique identifier called a **MAC address**, used to identify the device on the network
- The primary function of a NIC is to send and receive data packets between the computer or device and the network
- Each network interface card has a unique identifier, which is known as a MAC address, which is created during the manufacturing process

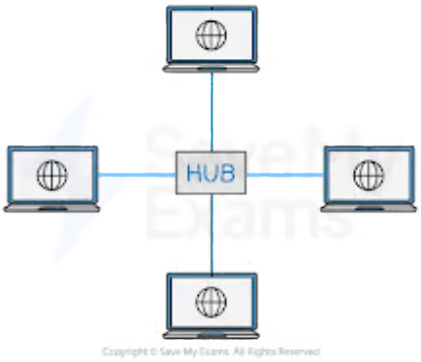
Wireless Access Point (WAP)

- Wireless access points (WAPs) act as a central transmitter and receiver of Wi-Fi signals
- WAPs connect to the wired network from a fixed location using Ethernet or Fibre optic cable and project a Wi-Fi signal to a designated area
- In a large network, multiple access points are used to provide extensive coverage and handle many connections

Hub

Your notes

- A hub is a networking device which is used to connect multiple devices in a network
- Hubs are "dumb" devices that pass on anything received on one connection to all other connections
- Because all data is sent to all devices, it can lead to network inefficiencies and security issues
- Hubs allow multiple other devices to be connected to them

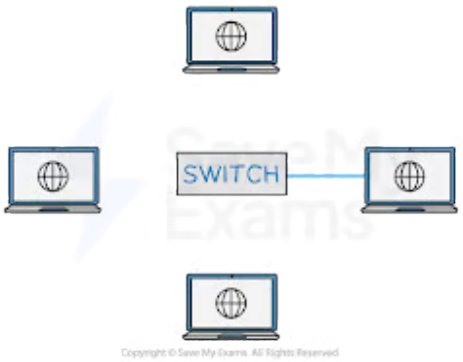


- Hubs are generally much cheaper than switches, but:
  - When a hub receives a data packet, it will broadcast it to every device on the network
- This creates two potential issues:
  - As the information is being broadcast to every device, it will make unnecessary traffic, especially if there are a large number of devices
  - As every device will receive the data packet, security may be a concern

Switch

- A network switch is a networking device that connects devices on a computer network and uses packet switching to receive, process and forward data to the destination device
- Unlike a hub, a switch only sends data to the device it was intended for, which improves network efficiency
- Switches are also used to connect several devices just like a hub; however, rather than sending data packets to all devices on the network, the switch will only send the data to its intended device

Your notes



- This is done by each switch having a lookup table

Port	Mac address
1	DF-42-B2-11-4D-E3
2	11-14-F2-1D-C3-C6
3	00-4B-17-7C-A2-C9

- When a switch receives a data packet, it examines the destination MAC address and looks up that address in its lookup table
- Once it has found the matching MAC address, it will then forward the data packet to the corresponding port

Client Server & Peer to Peer


Your notes

Client-Server

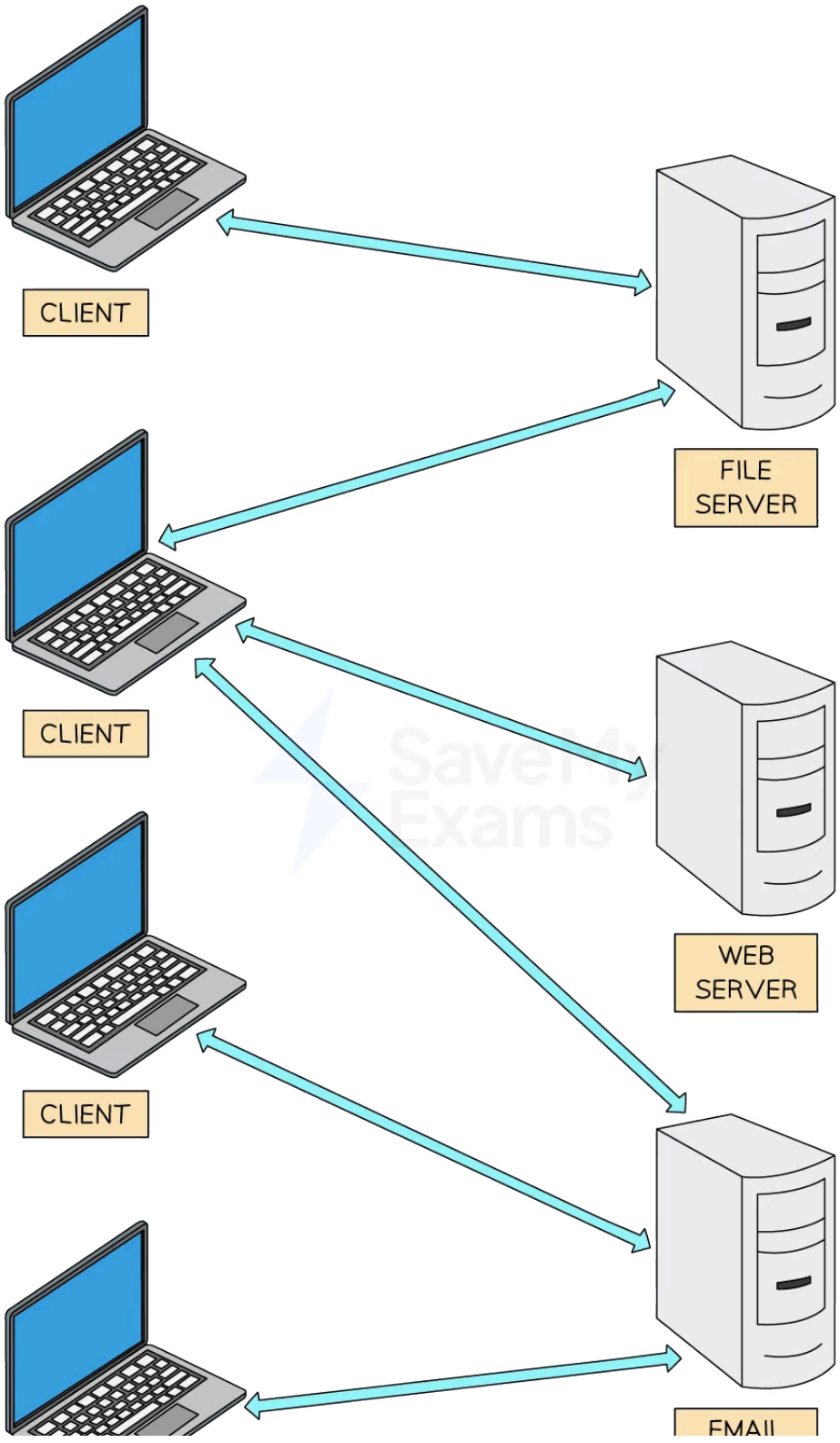
What is a Client-Server Network?

- Powerful and reliable 'server' computers control the network and 'serve' the clients with services such as files, email, web access, etc.
- Clients connect to the servers to access network services
- In this setup, the server hosts, delivers and manages most of the resources and services to be consumed by the clients

Benefits	Drawbacks
Easier central management	Single point of failure - if the server goes down, services could be unavailable
Scalability: new clients can be added easily	It can be expensive to set up and maintain - often need dedicated teams of people to maintain them
Higher reliability as resources are managed centrally	

- Use case: larger organisations where centralised control is needed, and reliability and security are paramount

Your notes



Client computers connected to different servers

Your notes

When to use a client-server network

- The choice between client-server and peer-to-peer depends on the specific needs and resources of the network in question
- Security, cost, ease of setup, and maintenance requirements should be considered

Peer-to-Peer

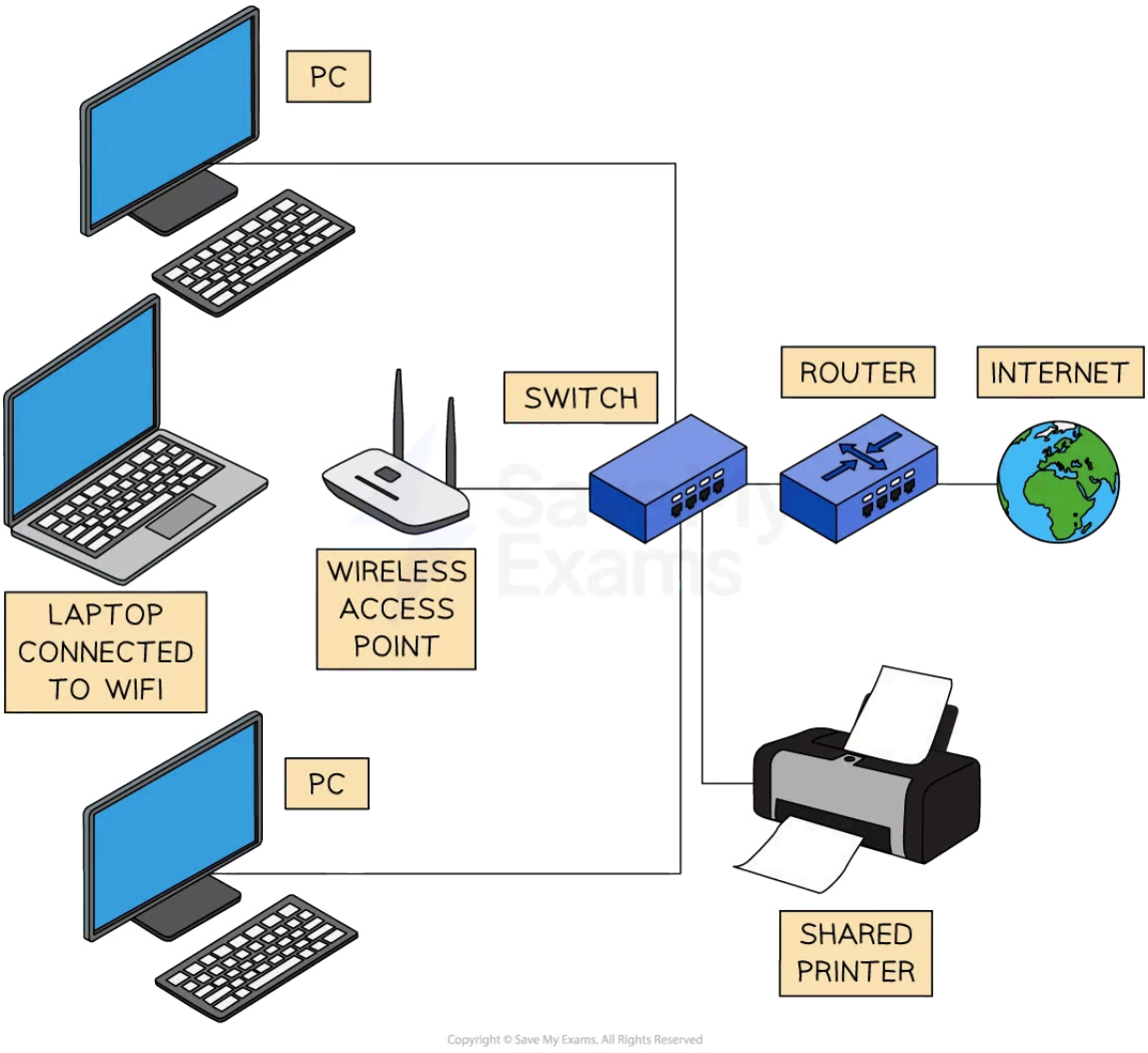
What is a Peer-to-Peer Network?

- This is the simplest type of network
- In this setup, all **computers in the network share equal responsibility,** and there is no central server
- All **machines have equal status**
- Each machine is the responsibility of that machine's user in terms of security, backup, etc.
- **Data is often spread around the network,** with each user being responsible for their data

Benefits	Drawbacks
Easy to set up and less expensive than client-server as no administrative staff are needed	Lack of central control can lead to security issues and vulnerabilities
No dependency on a central server	Not suitable for large networks as it can have performance issues
Data can be shared directly between systems without the need for a central server	

- Use cases: home networks, small businesses, or for specific applications like file sharing

Your notes



Peer to peer network example setup