NETWORKS AND THE EFFECTS OF USING THEM

IGCSE ICT — CHAPTER 4

INSTRUCTOR: TR. WAILINHTET

Visual & Detailed Teaching Presentation

LEARNING OBJECTIVES

- Explain NIC, MAC address, IP address and data packets.
- Compare hubs, switches, bridges and routers.
- Describe Wi-Fi, Bluetooth, cloud storage and network types.
- Explain network security, authentication and anti-malware.
- Compare video, audio and web conferencing.

WHAT IS A NETWORK?

- Two or more connected devices that exchange data or share resources.
- Examples: home Wi-Fi, school computer labs and banking networks.
- Shared resources include printers, software, files and internet access.

NETWORK INTERFACE CARD (NIC)

- A NIC allows a computer or other device to connect to a network.
- Often integrated into the motherboard.
- Wireless NIC (WNIC) uses an antenna and wireless signals.
- Each NIC is associated with a MAC address.

MAC ADDRESS VS IP ADDRESS

MAC ADDRESS

- Identifies a network interface.
- Typically represented as 48 bits in hexadecimal.
- Example: 00-1C-B3-4F-25-FF.
- Associated with the NIC.

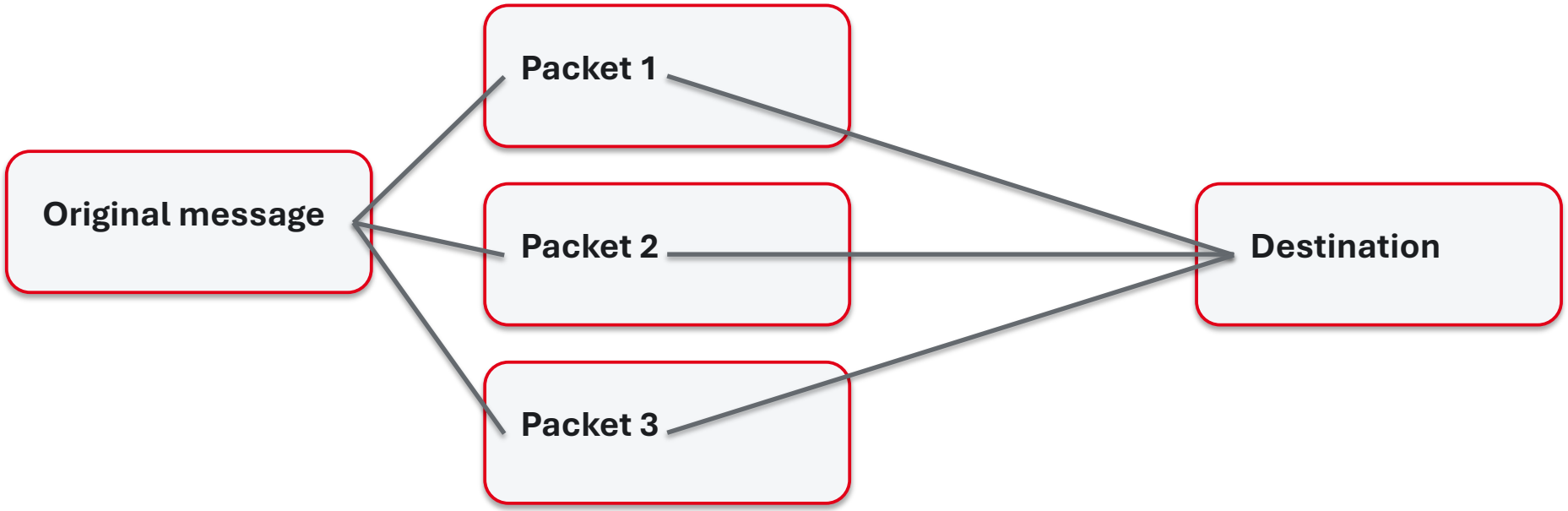
IP ADDRESS

- Identifies a device/interface on an IP network.
- IPv4: 32-bit address, e.g. 254.25.28.77.
- IPv6: 128-bit address in hexadecimal.
- May change when moving between networks.

IPv4 AND IPv6

- IPv4 uses 32 bits in four decimal groups separated by dots.
- IPv6 uses 128 bits in eight groups of hexadecimal digits separated by colons.
- IPv6 provides a much larger address space for connected devices.

DATA PACKETS: HOW MESSAGES TRAVEL



WHAT IS IN A PACKET HEADER?

- Sender IP address and destination IP address.
- Packet sequence or identity number.
- Packet size and information about the complete message.
- The receiver uses sequencing information to reassemble the message.

HUB: BROADCASTS TO ALL

- Connects devices within a LAN.
- Sends incoming data to every connected device.
- Creates unnecessary traffic and uses bandwidth.
- Less secure because other connected devices receive the data.

SWITCH: SENDS TO THE RIGHT DEVICE

- Connects devices within a LAN.
- Uses a MAC-address lookup table associated with ports.
- Forwards a data frame to the intended device/port.
- Generally reduces unnecessary traffic compared with a hub.

HUB VS SWITCH

HUB

- Broadcasts received data to all ports.
- More unnecessary traffic.
- Lower privacy/security.

SWITCH

- Uses MAC address table to forward frames.
- Less unnecessary traffic.
- Better traffic isolation.

TEXTBOOK VISUAL: HUB AND SWITCH

Switches are 'intelligent' versions of hubs. As with hubs, they connect a number of devices together to form a LAN. However, unlike a hub, a switch stores the MAC addresses of all devices on the network. Each port on the switch connected to a device will have a matching MAC address (called a look-up table) as shown in Table 4.1.

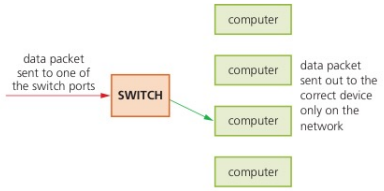


▲ **Figure 4.3** Switch

▼ **Table 4.1** Switch MAC address table

Port number	MAC address
1	a4-00-22-a4-fe-d1
2	00-1c-b3-4f-25-ff
3	33-11-ad-6f-f1-00
4	a4-00-22-b2-24-11
5	00-1c-b3-44-ff-02
6	0d-3e-4f-1a-22-00

Using the look-up table, a switch matches the MAC address of an incoming data packet arriving at one of its ports, and directs it to the correct device. None of the other devices will see this data packet. Thus, if a data packet arrives at port 2, and the MAC address in the data packet is a4-00-22-b2-24-11, then the switch will connect the data packet to port 4 only.



▲ **Figure 4.4** Switch network connections

Consequently, switches are more secure than hubs (because only the intended device is sent the data) and do not waste bandwidth (because network traffic is reduced).

In conclusion, hubs and switches are used to exchange data **within** their own local area networks. They are unable to exchange data with outside networks (such as the internet). To exchange data outside their own LAN, a device needs to be able to read an IP address. Therefore, we need another device to allow communication with external networks.

In summary:

Source: uploaded Chapter 4 PDF, page 4

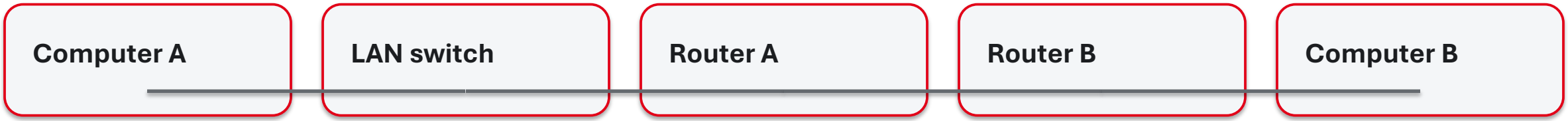
BRIDGES

- Connect LAN segments that use the same communication protocols.
- Can join different parts of a LAN so they function as one LAN.
- Operate using MAC addresses; unlike routers, do not route between external IP networks.

ROUTERS

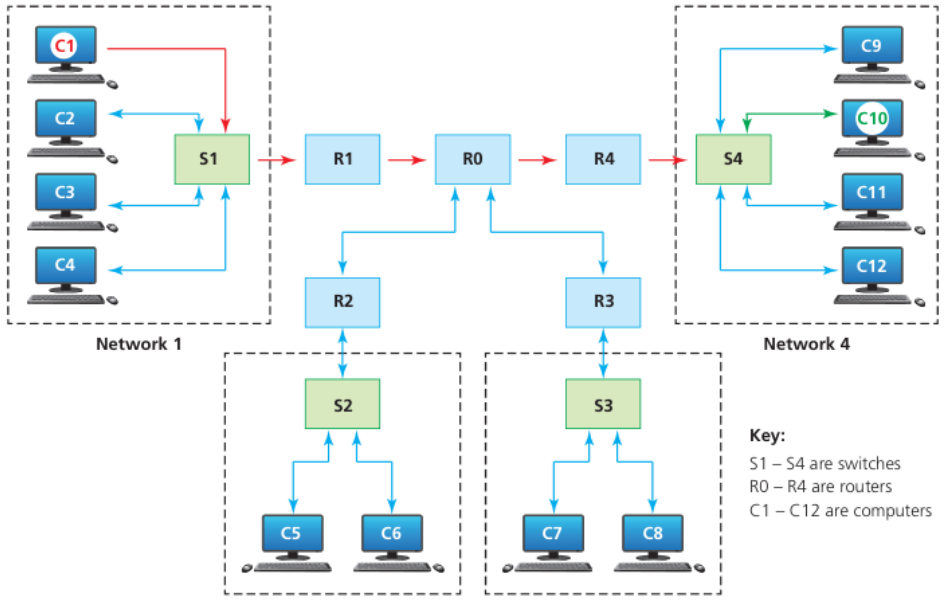
- Route data packets between different networks using IP addresses.
- A router can connect a LAN to the internet.
- Consults a routing table to select the next destination.
- Modern home routers may combine routing, switching and wireless access functions.

ROUTING A PACKET BETWEEN NETWORKS



TEXTBOOK ROUTING EXAMPLE

because the data packet will be sent by the router to the switch on the recipient local network. The switch can then use its look-up table to send the data packet to the correct device.



▲ **Figure 4.9** Routing of data from C1 to C10

Suppose, in Figure 4.9, computer **C1** wishes to send data to computer **C10**:

- Data packets are sent from C1 to R1.
- R1 checks the IP addresses and notes the data packets are not intended for any devices on Network 1.
- The data packets are then forwarded onto the internet (R0).

Source: uploaded Chapter 4 PDF, page 6 — routing diagram

ROUTER VS BRIDGE

ROUTER

- Connects different networks.
- Uses IP addresses.
- Uses routing tables.

BRIDGE

- Connects LAN segments.
- Uses MAC addresses.
- Does not use IP routing tables.

WI-FI VS BLUETOOTH

WI-FI

- Designed for wireless LAN and internet access.
- Commonly uses 2.4 GHz and 5 GHz bands.
- Usually higher throughput and greater range.

BLUETOOTH

- Designed for nearby personal devices.
- Uses the 2.4 GHz band.
- Useful for headphones and low-bandwidth links.

BLUETOOTH: FREQUENCY HOPPING

- Nearby devices pair and communicate over radio.
- Frequency hopping helps reduce interference.
- Typical examples: headsets, keyboards and wireless peripherals.
- Textbook discusses a range of less than 30 metres.

WI-FI ACCESS POINTS

- Access points (APs) connect wireless clients to a network.
- Multiple APs may be needed across a school or large building.
- Signal strength can be affected by distance, walls and interference.

CLOUD COMPUTING / STORAGE

- Data is stored on remote servers managed by a provider.
- Data redundancy means copies can exist across multiple servers.
- Users can access files from different devices over the internet.

TYPES OF CLOUD STORAGE

PUBLIC / PRIVATE

- Public cloud: infrastructure provided by an external service provider.
- Private cloud: dedicated environment for an organisation.

HYBRID

- Hybrid cloud: combines private and public environments.
- Sensitive data can remain private while other workloads use public cloud.

CLOUD STORAGE: EVALUATION

ADVANTAGES

- Remote access and backup.
- Synchronisation between devices.
- Collaboration on shared files.
- Flexible storage capacity.

DISADVANTAGES

- Depends on reliable internet.
- Security and privacy concerns.
- Potential subscription/transfer costs.
- Provider outages and data loss risk.

CLOUD SECURITY RISKS

- Unauthorised access to confidential information.
- Weak controls over provider staff or physical facilities.
- Hacking, data corruption and loss of access.
- Evaluate provider safeguards, backups and disaster recovery.

INTERNET, INTRANET AND EXTRANET

- Internet: global public network of interconnected networks.
- Intranet: private network for authorised members of an organisation.
- Extranet: controlled access for selected external users.
- The uploaded textbook refers to Chapter 10 for deeper coverage.

LOCAL AREA NETWORK (LAN)

- Connects computers within a limited geographical area.
- Typical example: school computer lab or office building.
- Supports resource sharing, communication and central administration.

LAN: BENEFITS AND LIMITATIONS

ADVANTAGES

- Share printers and software.
- Communicate easily within a site.
- Central network administration.

DISADVANTAGES

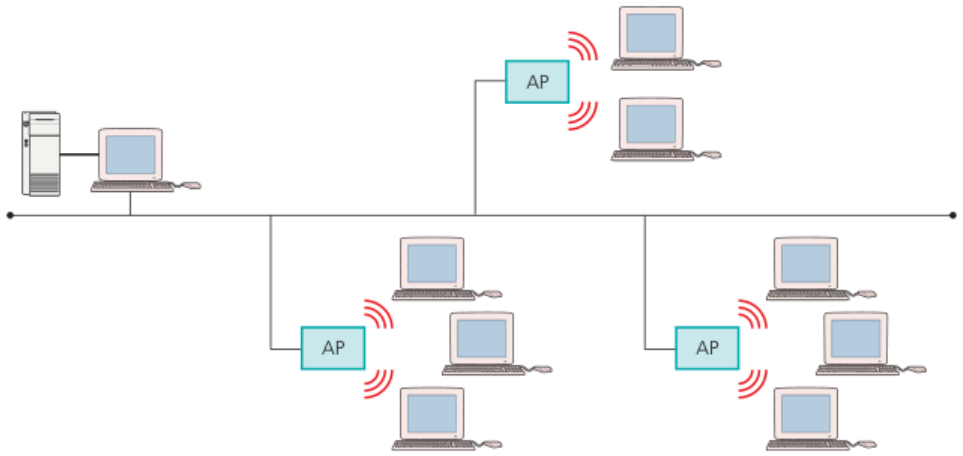
- Malware can spread across devices.
- Shared resources can become congested.
- Server failures may affect users.
- Security requires active management.

WIRELESS LAN (WLAN)

- Uses wireless links rather than cables to connect clients.
- Access points link wireless devices to the wired network.
- Supports mobility but can experience interference and signal dead zones.

TEXTBOOK VISUAL: WLAN SETUP

The AP receives and transmits data between the WLAN and the wired network structure. End-users access the WLAN through wireless LAN adapters which are built into their devices.



▲ **Figure 4.10** Wireless LAN set-up

Wired versus wireless

Table 4.4 compares wired LANs and wireless LANs.

▼ **Table 4.4** Wired versus wired LAN

Wireless networking	Wired networking
It is easier to expand the networks and it is not necessary to connect the devices using cables	Using cables produces a more reliable and stable network; wireless connectivity is often subject to interference

Source: uploaded Chapter 4 PDF, page 11

WIRED VS WIRELESS NETWORKS

WIRED

- More stable, often faster connections.
- Harder to intercept physical cable traffic.
- Cabling restricts mobility and creates clutter.

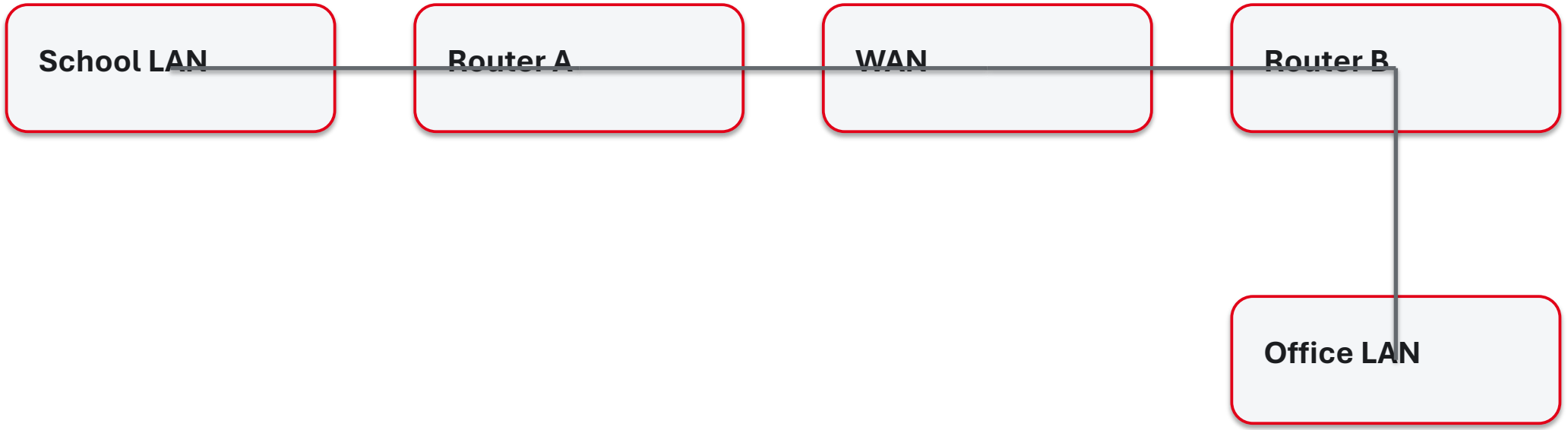
WIRELESS

- Greater mobility and easier expansion.
- Interference and thick walls can reduce performance.
- Wireless traffic requires suitable encryption.

WIDE AREA NETWORK (WAN)

- Connects devices or LANs over large geographic distances.
- Can use public communication systems or leased lines.
- Example: a bank connecting ATM systems across cities.

LANs CONNECTED INTO A WAN



NETWORK SECURITY

- Protect confidentiality, integrity and availability of data.
- Threats include unauthorised access, malicious software and stolen credentials.
- Authentication verifies a user’s claimed identity.

STRONG PASSWORDS

- Avoid predictable words, names and dates.
- The textbook recommends uppercase letters, digits and special characters.
- Use unique passwords and keep them private.
- Combine passwords with another authentication factor where available.

PASSWORD EXERCISE

- Classify these as strong or weak and explain why:
- 25-May-2000 | Pas5word
- ChapTer@15 | AbC*N55! | 12345X
- Discuss why length and predictability matter.

AUTHENTICATION METHODS

- Password or PIN — something you know.
- Physical token or smart card — something you have.
- Fingerprint or face recognition — something you are.
- Using multiple independent factors increases protection.

ZERO LOGIN AND BIOMETRICS

- Uses biometrics and potentially behavioural patterns.
- Examples: fingerprint and face recognition.
- Can make login faster, but raises privacy and monitoring questions.

MAGNETIC STRIPE VS SMART CARD

MAGNETIC STRIPE

- Magnetic stripe is read by swiping.
- Inexpensive and easy to use.
- Can wear out or be copied.

SMART CARD

- Chip and antenna may enable contactless use.
- Can store identification and authentication data.
- May be combined with a PIN.

PHYSICAL AUTHENTICATION TOKENS

- Hardware device generates a one-time password (OTP).
- Disconnected tokens display a code to type manually.
- Connected tokens may transmit the code to a computer.
- OTP codes are valid for a limited period.

ELECTRONIC / SOFTWARE TOKENS

- An app on a phone generates a one-time password.
- The user enters the code during sign-in.
- The server checks the code, often alongside another authentication method.

MULTI-FACTOR AUTHENTICATION



ANTI-VIRUS / ANTI-MALWARE

- Checks files before execution and during downloads.
- Compares files against known malware signatures.
- Heuristic analysis looks for suspicious behaviour.
- Quarantines suspected infections; false positives are possible.
- Update definitions and perform regular scans.

ELECTRONIC CONFERENCING

- Video conferencing: live audio and video.
- Audio conferencing: voice-only group discussion.
- Web conferencing: browser/network-based meetings and content sharing.

VIDEO CONFERENCING: HARDWARE

- Webcam and monitor / display.
- Microphone and speakers.
- Reliable network connection.
- Correct positioning and testing before the meeting.

VIDEO CONFERENCING: SOFTWARE

- Drivers enable webcams and microphones.
- CODEC encodes/decodes or compresses/decompresses media.
- Echo cancellation removes repeated delayed sound.

VIDEO CONFERENCING: EVALUATION

ADVANTAGES

- Reduces travel time and cost.
- Allows remote experts to join.
- Reduces travel-related pollution.
- Meetings can be arranged quickly.

DISADVANTAGES

- Network delays and jerky images.
- Equipment and training costs.
- Time-zone coordination challenges.
- Poor connection can interrupt meetings.

AUDIO CONFERENCING

- Group meetings using sound rather than video.
- May use ordinary telephone networks or VoIP.
- Less visual information than video meetings.
- Useful when video is unnecessary or bandwidth is limited.

WEB CONFERENCING

- Online meetings can include shared documents, screens and presentations.
- Participants can collaborate from different locations.
- Requires suitable software and a reliable network.

EXAM PRACTICE: NETWORKS

- Explain two differences between a hub and a switch. [4]
- Describe how a router forwards a packet to another network. [3]
- Compare the benefits and limitations of a WLAN. [4]
- Explain one advantage and one risk of cloud storage. [4]

EXAM ANSWERS: NETWORKS (1/2)

1. Hub vs switch [4]

- A hub broadcasts packets to every connected port; a switch forwards to the intended port only.
- A switch uses a MAC address look-up table; a hub does not.
- Switches reduce unnecessary traffic and improve privacy.

2. Router and packet forwarding [3]

- Reads the destination IP address in the packet header.
- Consults its routing table to choose the next network / router.
- Forwards the packet towards its destination (and the local switch delivers it).

EXAM ANSWERS: NETWORKS (2/2)

3. WLAN benefits and limitations [4]

- Benefit: mobility within wireless access-point coverage.
- Benefit: easier expansion without installing cables.
- Limitation: interference / walls may weaken or interrupt signals.
- Limitation: wireless transmissions need strong encryption to protect data.

4. Cloud storage advantage and risk [4]

- Advantage: access files from different locations and devices with internet access.
- Explanation: files are stored on remote servers and can synchronise.
- Risk: data may be accessed by unauthorised users or lost.
- Explanation: security breaches or provider failure may compromise stored files.

EXAM PRACTICE: SECURITY

- Explain why a strong password is important. [2]
- Describe two authentication methods other than passwords. [4]
- Explain how antivirus software detects and handles suspicious files. [4]
- Evaluate video conferencing for an international business. [6]

EXAM ANSWERS: SECURITY (1/2)

1. Strong passwords [2]

- Harder for attackers to guess or crack.
- Reduces the chance of unauthorised access to accounts / personal data.

2. Two other authentication methods [4]

- Biometrics: fingerprint or face recognition compares a user's physical feature with stored reference data.
- Electronic token: a phone app generates a short-lived one-time password (OTP) checked during login.
- Other valid examples: smart cards or physical hardware tokens.

EXAM ANSWERS: SECURITY (2/2)

3. Antivirus detection and handling [4]

- Scans files before opening / running and monitors downloads.
- Compares against a database of known virus signatures.
- Uses heuristic checks for suspicious behaviour.
- Quarantines suspected files for deletion or review; updates are needed.

4. Video conferencing evaluation [6]

- Saves travel, accommodation and time costs; reduces pollution.
- Remote colleagues and specialists can attend at short notice.
- Requires suitable webcams, microphones, software and reliable bandwidth.
- Lag, frozen video, time zones and setup/training costs can disrupt meetings.
- Judgement: valuable for regular international meetings if connectivity is reliable.

CHAPTER 4 — FINAL RECAP

- MAC addresses identify network interfaces; IP addresses support routing.
- Switches forward within LANs; routers connect networks.
- Wi-Fi and Bluetooth serve different wireless communication needs.
- Cloud storage and LAN/WAN networking offer benefits and risks.
- Authentication, anti-malware and secure conferencing matter.

THANK YOU

QUESTIONS & DISCUSSION

TR. WAILINHTET | WWW.WAILINHTET.COM