

GRADE 9 COMPUTER SCIENCE — STUDY NOTES

Unit 5: Communication and the Internet

CHAPTER 21: NETWORKS

What is a network & why use one?

- **Network:** two or more computers/devices connected together to share resources & data.
- Networks allow multiple users to: read/write files on a central **server** (extra storage + backup), share files/printers, download updates, access the Internet, and communicate (email, video, games).

Types of Network — LAN, WAN, PAN

KEY VOCABULARY

LAN (Local Area Network): Covers a small area (one site) e.g. a home, school, office.

WLAN (Wireless LAN): A LAN where devices connect using radio waves (Wi-Fi) instead of cables.

WAN (Wide Area Network): Connects two or more LANs over a large geographical area. The Internet is the largest WAN.

PAN (Personal Area Network): Short-range network connecting personal devices (phone, laptop, earbuds) — often via Bluetooth (up to ~10m).

Client–Server vs Peer-to-Peer

Client–Server	Peer-to-Peer (P2P)
Has at least one dedicated server providing services	No dedicated server — every computer can be both client and server
Server authenticates users & controls access to files	Each computer shares/requests services directly with others
Used in schools, businesses (centralised control & security)	Used for instant messaging & file sharing (e.g. some Linux distributions); harder to track who is sharing what — can enable piracy

Network Topologies

- The **topology** is the arrangement of connections between devices. Four main types: **Bus, Ring, Star, Mesh**.

Topology	How it works	Key advantage	Key disadvantage
Bus	Single cable (the 'bus') with a terminator at each end; only one message travels at a time (uses CSMA/CD to avoid collisions)	Cheap — needs only one cable; easy to add devices	Whole network fails if the cable breaks; gets slower as more devices/collisions occur; all devices see all data (security risk)
Ring	Devices connected in a closed loop; data travels one direction, device to device, no collisions	Adding devices doesn't slow it down	One broken cable/device can stop the whole network; must shut down network to add/remove a device
Star	Every device connects to a central hub or switch	Damaged cable only affects one device; switch makes it efficient & secure; easy to find faults	If the hub/switch fails, whole network fails; expensive (lots of cabling)
Mesh	Every device connects to one or more others (fully or partially connected); used for Internet & IoT sensors	Very fault-tolerant — messages re-routed if a device fails; high performance	Expensive & complex to install/manage (esp. wired, fully connected)

Remember: A switch/hub is the 'centre' of a Star network. CSMA/CD is the collision-handling method used in Bus networks.

Wired vs Wireless Connectivity

	Advantages	Disadvantages
Wired	Faster; harder to intercept/eavesdrop; less interference	Expensive to install/reconfigure; needs lots of cables
Wireless	No cables needed; lets users bring their own device; wider device compatibility	Can be slower; suffers interference (walls, other devices); data must be encrypted to stop eavesdropping

Network Data Speed & Calculations

- Speed = amount of data sent per second, measured in **bits per second (bps, Mbps, Gbps)** — NOT the same as storage units (bytes)!
- **Bandwidth:** the amount of data that can be carried per unit time. **Latency:** the delay data experiences travelling through a network.

Worked Example — download time for a 50 MB file on a 12 Mbps connection: 1) File size in bits = $50 \times 1024 \times 1024 \times 8 = 419,430,400$ bits 2) Speed in bps = $12 \times 1000 \times 1000 = 12,000,000$ bps 3) Time = $419,430,400 \div 12,000,000 \approx 34.95$ seconds

Protocols — the 'rules' for communication

- **Protocol:** a set of rules that controls how data is formatted, addressed, routed, error-checked and acknowledged between devices.

Protocol	Used for
SMTP	Sending email across the Internet
POP3	Retrieving email — downloads then deletes messages from server
IMAP	Retrieving email — keeps messages on server, syncs across multiple devices
Ethernet	Family of protocols for wired LANs (cabling, connectors, data formatting/error checking)
Wi-Fi	Protocol for wireless LANs
TCP	Ensures reliable delivery — data arrives complete, correct & in order (uses acknowledgements + checksums + flow control)
HTTP	Rules for transferring web pages between browser and web server
HTTPS	Secure (encrypted) version of HTTP — protects data like passwords/bank details
FTP	Transferring files over a network, e.g. uploading a website to a web server

Packets & the TCP/IP 4-Layer Model

- Packet:** a small chunk of data + a header (sender address, recipient address, packet number, total packets). A network that sends data this way is 'packet switched'.

Layer	Role
Application	Interacts with the user; where HTTP, FTP, email protocols operate
Transport	Manages end-to-end communication; TCP sets up communication, splits data into packets, checks arrival
Internet (Network)	Routes packets across networks using IP addresses; adds source/destination IP to packets
Link (Network Access)	Transmits data on the local network (e.g. via Ethernet); handled by the network card & drivers

Mnemonic: "Another Task Is Done" = Application, Transport, Internet, Data-link (top to bottom).

- Benefits of using layers: easier to understand (broken into functional parts), each layer has one job, layers can be swapped/updated independently, easier to find & fix problems, and it gives a universal standard so all hardware/software can work together.

Mobile Communication Standards

Generation	Key feature
2G	First digital standard — text messages & MMS
3G	~2 Mbps — wireless Internet access, video calls, streaming
4G	Much faster & higher capacity — smooth mobile gaming/streaming, uses IP even for calls
5G	Peak speeds up to 100 Gbps, much lower latency — supports driverless cars & IoT

CHAPTER 22: NETWORK SECURITY

Why Network Security Matters — the 3 goals

Goal	Meaning
Confidentiality	Only authorised people can see/access data (encryption + access permissions)
Correctness (Integrity)	Data must not be changed/corrupted without authorisation
Availability	Data/services must be accessible whenever needed (protect against DoS attacks & failures)

- Data may be needed to **run the organisation** (losing it could bankrupt a business), be **private/confidential** (legal duty, risk of being sued), or be **financially valuable** (competitors could exploit leaked data).

Authentication, Validation & Access Control

KEY VOCABULARY

Authentication: Checking the identity of a user, e.g. matching username/password, PIN, or fingerprint against stored records.

Two-factor authentication: An extra check beyond a password, e.g. a code from an SMS or secure token — improves security if a password is stolen.

Access control: Decides what a user can do with a file: read-only, read & write (modify), or full control (delete).

Firewall: Monitors/controls data moving between networks (e.g. Internet ↔ internal network) using a set of rules; can block protocols, addresses, or hacking patterns.

Physical security: Restricting physical access to hardware (locked server rooms, electronic locks, security tags) — vital because physical access can bypass all software security.

Cloud Storage & Security

Advantages	Disadvantages
Provider manages hardware, availability & backups automatically	Reliant on a third-party being trustworthy & reliable
Storage can be scaled up in minutes	Data accessible via Internet = risk of hacking/interception
Off-site storage protects against fire, theft, local hardware failure	Provider could go bankrupt, fail, or be hacked
	Servers might be in another country with different data laws
	Needs a reliable Internet connection to access data

- Risks can be reduced by: choosing providers who replicate data across multiple locations, and by **encrypting** data before/during transfer.
- NAS (Network-Attached Storage):** a storage device connected to a network; risky if the default password isn't changed or software isn't updated. **USB drives:** convenient but easily lost/stolen — use encrypted USB drives for sensitive data.

Cyber Attacks — Two Categories

- 1) Social engineering** (exploiting human behaviour):

Attack	Description
Phishing	Fake message/email pretending to be from a trusted source, tricking the user into entering login/financial details on a fake website
Shoulder surfing	Directly observing someone (e.g. at an ATM) to see their PIN/password
Pharming	Malware redirects a domain name to a fake IP address/website, even if the user typed the correct address

- 2) Technical weaknesses:**

Weakness	Description
Unpatched software	Software without the latest security updates (patches) — attackers exploit known, published weaknesses
USB devices	Can carry malware onto a system or copy data off it
Eavesdropping	Secretly intercepting/reading data travelling across a network without the owner knowing

Prevent pharming by: checking the URL is correct, checking for HTTPS + a valid security certificate, and keeping security updates/antivirus current.

Protecting Systems from Cyber Attacks

- At the design stage:** consider what authentication is needed, different access levels, warnings for risky actions, whether data should be encrypted, and what threats the software will face.
- Code reviews:** either by another (senior) programmer, or using automated analysis software — both check for **code vulnerabilities** and bad programming practice.
- Modular testing:** testing each block of code as it's completed, so small problems (e.g. poor input validation) don't become security holes later.
- Audit trail:** an automatically generated, unchangeable, chronological record of who did what on a system — used to investigate attacks.
- Secure operating systems** and **effective network security provision** (trained staff, up-to-date patching, monitoring) also reduce risk.

Identifying Vulnerabilities

KEY VOCABULARY

Ethical hacking: 'Good' hacking — deliberately looking for weaknesses so they can be fixed, with the organisation's permission.

Penetration testing ('pen testing'): Authorised, simulated attacks on a system to find weaknesses; results reported to management.

Commercial analysis tools: Software that scans a network (internally or externally) for known vulnerabilities — but anyone can buy them, including attackers.

Network & user policies: Written rules covering authorised activities, patching schedules, password rules, security setup and audit trail retention — reviewed regularly and signed by staff.

CHAPTER 23: THE INTERNET AND THE WORLD WIDE WEB

The Internet

- The **Internet** = a global 'network of networks' (the largest WAN) — countries are linked by cables, fibre-optic links & satellites (the 'Internet backbone').
- Domain name:** an easy-to-remember address (e.g. bbc.co.uk) that represents a numeric IP address.
- DNS (Domain Name Service):** a network of servers that translates domain names into IP addresses. If one server doesn't know the address, it asks another until the correct IP is found (this is called 'resolving' the domain name).
- ISP (Internet Service Provider):** a company that provides your connection to the Internet.
- Router:** hardware that forwards data packets between different networks, using a routing table to decide where each packet goes next. A packet may pass through several routers to reach its destination.

IP Addressing — IPv4 vs IPv6

	IPv4	IPv6
Format	Four 8-bit numbers (octets), e.g. 216.27.61.137	Eight groups of hexadecimal numbers separated by colons, e.g. 2001:cdba:0000:....:9652
Size	32 bits	128 bits
Total addresses	~4 billion	$\sim 3.4 \times 10^{38}$ (practically unlimited)
Why needed	Original standard — now running out of addresses	Introduced so many more devices can have a unique address

How a Packet Travels Across the Internet

- 1. Sending computer splits data into packets (each with a header: sender, destination, packet number, total packets). 2. Packets sent to the ISP's router. 3. Each router reads the destination address & forwards the packet toward it (may pass through many routers). 4. Receiving computer collects all packets and reassembles the data in the correct order.

The World Wide Web (WWW)

- The WWW is a **service** that runs on top of the Internet — NOT the same thing as the Internet! It provides web pages linked together by **hyperlinks** (hypertext).

KEY VOCABULARY

URL (uniform resource locator): A web address — points to a web page or an individual file.

Web browser: Software (the 'client') that requests pages from a web server and displays them to the user.

Web server: A powerful computer that stores and serves web pages/files.

HTML (HyperText Markup Language): The text format used to describe a web page's content, formatting, hyperlinks and embedded objects (images/video) so a browser can display it.

- Steps to load a web page: 1) user enters a URL, 2) DNS resolves the domain name to an IP address, 3) browser connects to the web server via HTTP/HTTPS, 4) server sends the page as HTML, 5) browser renders (displays) the page.

Hardware Needed to Access the Internet

Device	Role
Switch	Connects devices within one LAN; reads destination addresses so it sends data only to the intended device (reduces traffic)
Wireless Access Point (WAP)	Lets wireless devices join a wired network using Wi-Fi; transmits to all devices in range (unlike a switch)
Router	Forwards data between different networks (e.g. home network ↔ Internet)
Modem	Converts signals between the LAN and the type of cable used by the ISP (e.g. copper or fibre-optic); often combined with a router as one box

EXAM TIP: Be ready to compare topologies, explain the difference between the Internet and the WWW, describe how DNS resolves a domain name, and know which protocol does what job (SMTP/POP3/IMAP for email; HTTP/HTTPS/FTP for the web).

UNIT 5 PRACTICE QUESTION PAPER

Communication and the Internet

1. A bank wants to share data between its head office and its 400 branches across the country. Explain why the bank would use a WAN rather than a LAN. *[2 marks]*
2. State the purposes of the following TCP/IP layers: (a) Application, (b) Transport, (c) Data link. *[3 marks]*
3. A small business has a network with three computers, one printer and a server, connected using a star topology. Describe how the devices would be connected. *[4 marks]*
4. Describe how an email phishing attack targeting bank customers might work. *[2 marks]*
5. Which of the following protocols would NOT be used when transferring a web page from a web server using the Internet? a) TCP b) IP c) IMAP d) HTTP *[1 mark]*
6. Explain the difference between the Internet and the World Wide Web. *[2 marks]*
7. Ayana's computer has the IP address 213.36.27.127. (a) Explain why a computer requires an IP address to access the Internet. (b) An IP address consists of four numbers, each between 0 and 255. State how many bits are needed to store the IP address. (c) Describe the difference between IPv4 and IPv6 addresses. *[5 marks]*
8. When Ayana accesses a website, she types in a domain name rather than the IP address. Discuss how she is able to access the website using the domain name. *[4 marks]*
9. State the wireless networking device that would allow Anika to connect her laptop to her college network without a cable. *[1 mark]*
10. Explain the role of a router in a home network. *[2 marks]*
11. With the aid of a description, explain the role of a switch in a local area network. *[6 marks]*
12. (a) State what is meant by the acronyms HTML and HTTP. (b) Describe how HTTP is different to HTTPS. *[6 marks]*
13. Explain what is meant by a firewall, and describe two things a firewall's rules can do. *[4 marks]*
14. Describe two advantages and two disadvantages of storing an organisation's data using cloud storage rather than on local servers. *[4 marks]*

Total marks: 46

ANSWERS

1. A bank wants to share data between its head office and its 400 branches across the country. Explain why the bank would use a WAN rather than a LAN. [2 marks]

Answer: A WAN covers a large geographical area and connects multiple LANs together (e.g. one LAN per branch). A LAN only covers a single small site, so it could not connect head office to 400 separate branch locations across the country.

2. State the purposes of the following TCP/IP layers: (a) Application, (b) Transport, (c) Data link. [3 marks]

Answer: (a) Application — interacts with the user and provides access to network services/data (e.g. web browsing, email). (b) Transport — manages end-to-end communication, splitting data into packets and checking they arrive correctly (TCP). (c) Data link — controls transmission/reception of data on the local network (e.g. via Ethernet, using the network card and drivers).

3. A small business has a network with three computers, one printer and a server, connected using a star topology. Describe how the devices would be connected. [4 marks]

Answer: Each device (3 computers, 1 printer, 1 server) is connected by its own individual cable to a central hub or switch. The hub/switch sits at the centre and passes messages between devices; a switch would send data only to the intended recipient rather than to all devices.

4. Describe how an email phishing attack targeting bank customers might work. [2 marks]

Answer: The attacker sends an email pretending to be from the bank, claiming there is a problem (e.g. suspicious activity) and asking the customer to click a link and log in. The link leads to a fake website that looks like the real bank site. When the customer enters their username/password, the details are sent to the attacker, who can then use them to access the real account.

5. Which of the following protocols would NOT be used when transferring a web page from a web server using the Internet? a) TCP b) IP c) IMAP d) HTTP [1 mark]

Answer: c) IMAP — this is an email protocol used to retrieve emails, not for transferring web pages. TCP, IP and HTTP are all involved in delivering a web page.

6. Explain the difference between the Internet and the World Wide Web. [2 marks]

Answer: The Internet is the huge global network of interconnected networks (hardware — cables, routers, servers) that allows data to be exchanged worldwide. The World Wide Web is a service that runs on top of the Internet, providing web pages linked together by hyperlinks, accessed using protocols such as HTTP/HTTPS. The Internet also carries other services besides the Web, such as email.

7. Ayana's computer has the IP address 213.36.27.127. (a) Explain why a computer requires an IP address to access the Internet. (b) An IP address consists of four numbers, each between 0 and 255. State how many bits are needed to store the IP address. (c) Describe the difference between IPv4 and IPv6 addresses. [5 marks]

Answer: (a) Every device on the Internet needs a unique address so that data can be correctly routed to and from it — without an address, other devices would not know where to send data. (b) 32 bits (four 8-bit numbers/octets). (c) IPv4 uses 32 bits (four octets, ~4 billion addresses) and is written in decimal, e.g. 213.36.27.127. IPv6 uses 128 bits (eight groups of hexadecimal numbers separated by colons) giving vastly more addresses ($\sim 3.4 \times 10^{38}$), introduced because IPv4 addresses were running out.

8. When Ayana accesses a website, she types in a domain name rather than the IP address. Discuss how she is able to access the website using the domain name. [4 marks]

Answer: Ayana's browser sends the domain name to a DNS server, which holds a database matching domain names to IP addresses. If that DNS server does not have the address, it asks another DNS server, and so on, until the correct IP address is found (resolved). The IP address is then returned to Ayana's browser, which uses it to connect directly to the correct web server and request the page.

9. State the wireless networking device that would allow Anika to connect her laptop to her college network without a cable. [1 mark]

Answer: A Wireless Access Point (WAP).

10. Explain the role of a router in a home network. [2 marks]

Answer: A router connects the home network (LAN) to the Internet (a WAN), allowing all devices on the home network to share one Internet connection. It reads the destination address of incoming data and forwards it to the correct device on the home network.

11. With the aid of a description, explain the role of a switch in a local area network. [6 marks]

Answer: A switch is the central connection point in a star-topology LAN — every device (computers, printer, server) connects to it with its own cable. When a device sends data, the switch reads the destination address in the data and builds up a table of all device addresses on the network. It then forwards the data only to the intended recipient device, rather than to every device on the network (unlike a hub). This makes the network more efficient (less unnecessary traffic) and more secure (devices don't see data meant for others).

12. (a) State what is meant by the acronyms HTML and HTTP. (b) Describe how HTTP is different to HTTPS. [6 marks]

Answer: (a) HTML = HyperText Markup Language, the language used to describe the content, formatting and hyperlinks of a web page. HTTP = HyperText Transfer Protocol, the protocol used to send/receive data between a web browser and a web server. (b) HTTPS is the secure version of HTTP — data sent between the browser and server is encrypted, preventing a third party from reading it, and it helps confirm the user is communicating with the genuine website rather than a fake one trying to steal data such as passwords or bank details.

13. Explain what is meant by a firewall, and describe two things a firewall's rules can do. [4 marks]

Answer: A firewall is a network security system (hardware or software) that monitors and controls data moving between networks, often between the Internet and an internal network, using a set of rules. Its rules can, for example: block certain protocols (e.g. FTP) to stop data being copied to an external server; block data from/to specific addresses (e.g. particular countries or organisations); or stop hacking attempts by disallowing data matching known attack patterns.

14. Describe two advantages and two disadvantages of storing an organisation's data using cloud storage rather than on local servers. [4 marks]

Answer: Advantages: the provider manages hardware/maintenance and ensures availability; storage capacity can be increased quickly (in minutes) without buying new hardware; data is protected against local disasters (fire, theft, hardware failure) since it's stored off-site; providers often manage automatic backups. Disadvantages: the organisation depends on a third party being trustworthy and reliable; data sent over the Internet could be intercepted or hacked; the provider could fail, be hacked, or go bankrupt; access depends on having a reliable Internet connection.