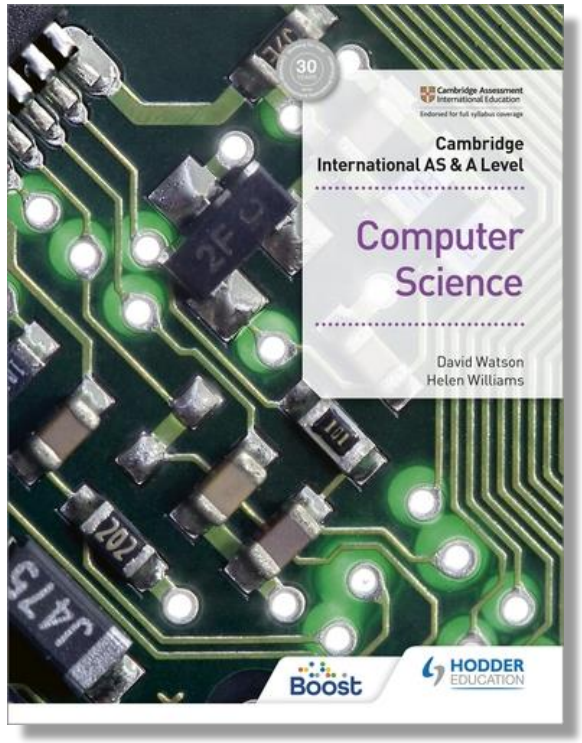
GCE AS LEVEL

In the context of CIE 9618 syllabus

CAMBRIDGE International Examinations

Chapter 2
Communication

2.1 Networking
2.2 The Internet



2 Communication

LEARNING OBJECTIVES:

1. The benefits of networking devices
2. The characteristics of a local area network (LAN) and a wide area network (WAN)
3. Client-server and peer-to-peer models in networking
4. The differences between thin client and thick client
5. Bus, star, mesh and hybrid networking topologies
6. Public and private cloud computing
7. The differences between wired and wireless networks (including types of cable and wireless technologies)
8. The hardware required to support a LAN
9. The function of routers
10. Ethernet and how data collisions are detected and avoided
11. Bit streaming (including differences between real-time and on-demand streaming of data)
12. The differences between the internet and the World Wide Web (WWW)
13. The hardware needed to support the internet
14. IP addresses (including IPv4, IPv6, public IP addresses and private IP addresses)
15. The use of the uniform resource locator (URL) to locate a resource on the world wide web
16. The role of the domain name service (DNS).

2.1 Networking

KEY TERMS: (1/6)

- ARPAnet – Advanced Research Projects Agency Network.
- WAN – wide area network (network covering a very large geographical area).
- LAN – local area network (network covering a small area such as a single building).
- MAN – metropolitan area network (network which is larger than a LAN but smaller than a WAN, which can cover several buildings in a single city, such as a university campus).
- File server – a server on a network where central files and other data are stored. They can be accessed by a user logged onto the network.
- Hub – hardware used to connect together a number of devices to form a LAN that directs incoming data packets to all devices on the network (LAN).
- Switch – hardware used to connect together a number of devices to form a LAN that directs incoming data packets to a specific destination address only.
- Router – device which enables data packets to be routed between different networks (for example, can join LANs to form a WAN).
- Modem – modulator demodulator. A device that converts digital data to analogue data (to be sent down a telephone wire); conversely it also converts analogue data to digital data (which a computer can process).

2.1 Networking

KEY TERMS: (2/6)

- WLAN – wireless LAN.
- (W)AP – (wireless) access point which allows a device to access a LAN without a wired connection.
- PAN – network that is centred around a person or their workspace.
- Client-server – network that uses separate dedicated servers and specific client workstations. All client computers are connected to the dedicated servers.
- Spread spectrum technology – wideband radio frequency with a range of 30 to 50 metres.
- Node – device connected to a network (it can be a computer, storage device or peripheral device).
- Peer-to-peer – network in which each node can share its files with all the other nodes. Each node has its own data and there is no central server.
- Thin client – device that needs access to the internet for it to work and depends on a more powerful computer for processing.
- Thick client – device which can work both off line and on line and is able to do some processing even if not connected to a network/internet.

2.1 Networking

KEY TERMS: (3/6)

- **Bus network topology** – network using single central cable in which all devices are connected to this cable so data can only travel in one direction and only one device is allowed to transmit at a time.
- **Packet** – message/data sent over a network from node to node (packets include the address of the node sending the packet, the address of the packet recipient and the actual.
- **Star network topology** – a network that uses a central hub/switch with all devices connected to this central hub/switch so all data packets are directed through this central hub/switch.
- **Mesh network topology** – interlinked computers/devices, which use routing logic so data packets are sent from sending stations to receiving stations only by the shortest route.
- **Hybrid network** – network made up of a combination of other network topologies.
- **Cloud storage** – method of data storage where data is stored on off-site servers.
- **Data redundancy** – situation in which the same data is stored on several servers in case of maintenance or repair.

2.1 Networking

KEY TERMS: (4/6)

- **Wi-Fi** – wireless connectivity that uses radio waves, microwaves. Implements IEEE 802.11 protocols.
- **Bluetooth** – wireless connectivity that uses radio waves in the 2.45 GHz frequency band.
- **Spread spectrum frequency hopping** – a method of transmitting radio signals in which a device picks one of 79 channels at random. If the chosen channel is already in use, it randomly chooses another channel. It has a range up to 100 metres.
- **WPAN** – wireless personal area network. A local wireless network which connects together devices in very close proximity (such as in a user's house); typical devices would be a laptop, smartphone, tablet and printer.
- **Twisted pair cable** – type of cable in which two wires of a single circuit are twisted together. Several twisted pairs make up a single cable.
- **Coaxial cable** – cable made up of central copper core, insulation, copper mesh and outer insulation.
- **Fibre optic cable** – cable made up of glass fibre wires which use pulses of light (rather than electricity) to transmit data.

2.1 Networking

KEY TERMS: (5/6)

- Gateway – device that connects LANs which use different protocols.
- Repeater – device used to boost a signal on both wired and wireless networks.
- Repeating hubs – network devices which are a hybrid of hub and repeater unit.
- Bridge – device that connects LANs which use the same protocols.
- Softmodem – abbreviation for software modem; a software-based modem that uses minimal hardware.
- NIC – network interface card. These cards allow devices to connect to a network/internet (usually associated with a MAC address set at the factory).
- WNIC – wireless network interface cards/controllers.
- Ethernet – protocol IEEE 802.3 used by many wired LANs.
- Conflict – situation in which two devices have the same IP address.
- Broadcast – communication where pieces of data are sent from sender to receiver.

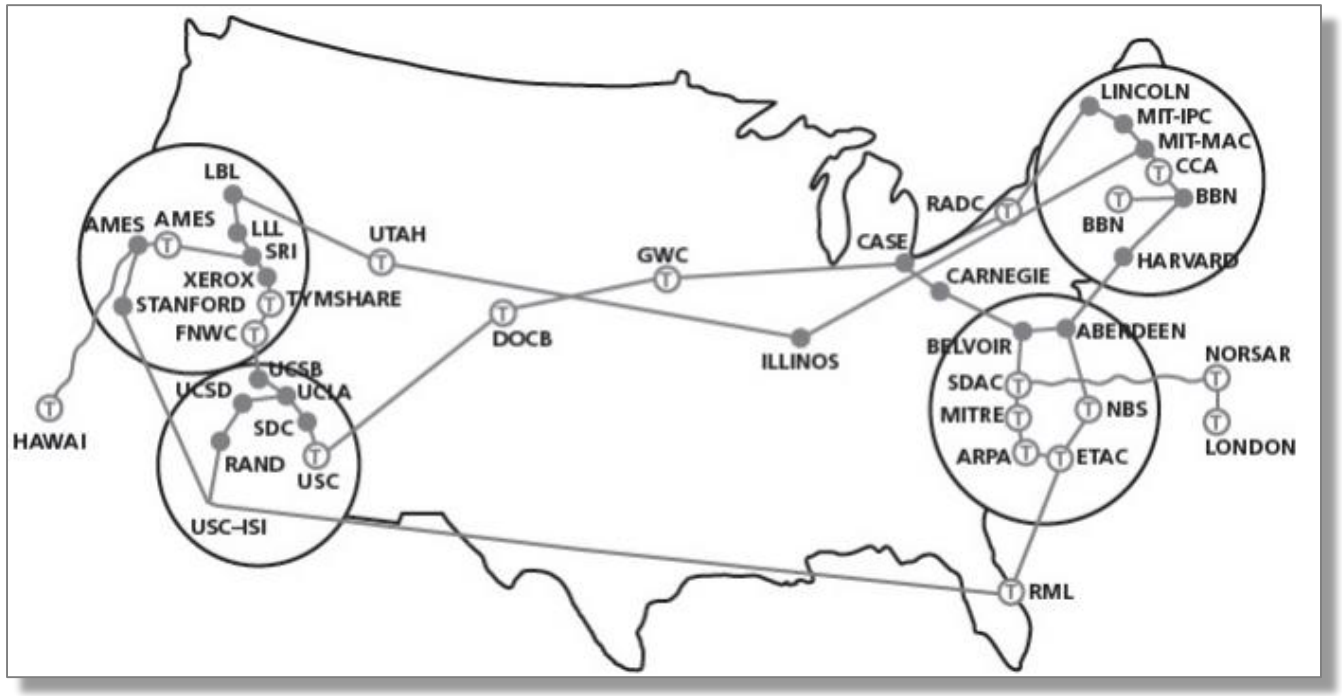
2.1 Networking

KEY TERMS: (6/6)

- Collision – situation in which two messages/data from different sources are trying to transmit along the same data channel.
- CSMA/CD – carrier sense multiple access with collision detection – a method used to detect collisions and resolve the issue.
- Bit streaming – contiguous sequence of digital bits sent over a network/internet.
- Buffering – store which holds data temporarily.
- Bit rate – number of bits per second that can be transmitted over a network. It is a measure of the data transfer rate over a digital telecoms network.
- On demand (bit streaming) – system that allows users to stream video or music files from a central server as and when required without having to save the files on their own computer/tablet/phone.
- Real-time (bit streaming) – system in which an event is captured by camera (and microphone) connected to a computer and sent to a server where the data is encoded. The user can access the data 'as it happens' live.

2.1.1 Networking Devices

- 1970 in the USA: ARPAnet started.
- Advanced Research Projects Agency Network: Early networking form.
- Packet switching WAN: Connected big computers.
- Department of Defense: Initial users.
- Expanded: Included university computers.
- ARPAnet: Developed internet base.



ARPAnet coverage, 1973

2.1.1 Networking Devices

- 1980s: Personal computers developed.
- Local Area Network (LAN): Small network in a building.
- Connect: Computers, shared devices like printers.
- Wide Area Network (WAN): LANs joined, public networks.
- Private network: Needs passwords, user IDs.
- Internet: Decentralized, common access point.
- Vast networks: Anyone with internet can connect.
- Different from WAN.

2.1.1 Networking Devices

- Recent years: New network type - Metropolitan Area Network (MAN).
- MANs: Bigger than LANs, connect city networks.
- Example: University campus in a city.
- Size: Restricted to one city.
- WANs: Larger, cover country or continent.
- Example: Multi-national company connects LANs/MANs for worldwide WAN.

2.1.1 Networking Devices

Main benefits of networking computers and devices (rather than using a number of stand-alone computers):

- Shared Devices: Like printers, save costs.
- Software Licenses: Cheaper on networks than standalone computers.
- File Sharing: Users share files, data.
- Central Data Source: Reliable data from file server.
- Central Backups: Data, files backed up daily.
- Communication: Email, instant messaging.
- Network Manager: Manages network, sets access rights.
- Internet Restrictions: Controls access to external networks.

2.1.1 Networking Devices

Drawbacks of networking computers and devices:

- Expensive Setup: Cabling, servers initial cost.
- Complex Management: Large network challenging to manage.
- Device Breakdown: Like file servers, affects whole network.
- Malware, Hacking Impact: Entire network at risk.

2.1.1 Networking Devices

Network Computers:

- Networked computers form an infrastructure which enables internal and external communications to take place.
- The infrastructure includes the following:

Hardware	Software	Services
• LAN cards • routers • switches • wireless routers • cabling	• operation and management of the network • operation of firewalls • security applications/utilities	• DSL • satellite communication channels • wireless protocols • IP addressing.

2.1.1 Networking Devices

- Networks can be categorised as private or public.

Private Networks:

- Private Networks: Owned by one company/organization.
- Often LANs or Intranets: Restricted access (passwords, user IDs required).
- Responsibility: Companies manage equipment, software, network maintenance.
- Staff Management: Hiring, training personnel.

Public Networks:

- Public Networks: Owned by communications carrier company (telecoms).
- Many Organizations: Use the network.
- No Specific Passwords: Usually no entry password requirements.
- Sub-network Security: Managed for security.

2.1.1 Networking Devices

Local Area Networks (LANs):

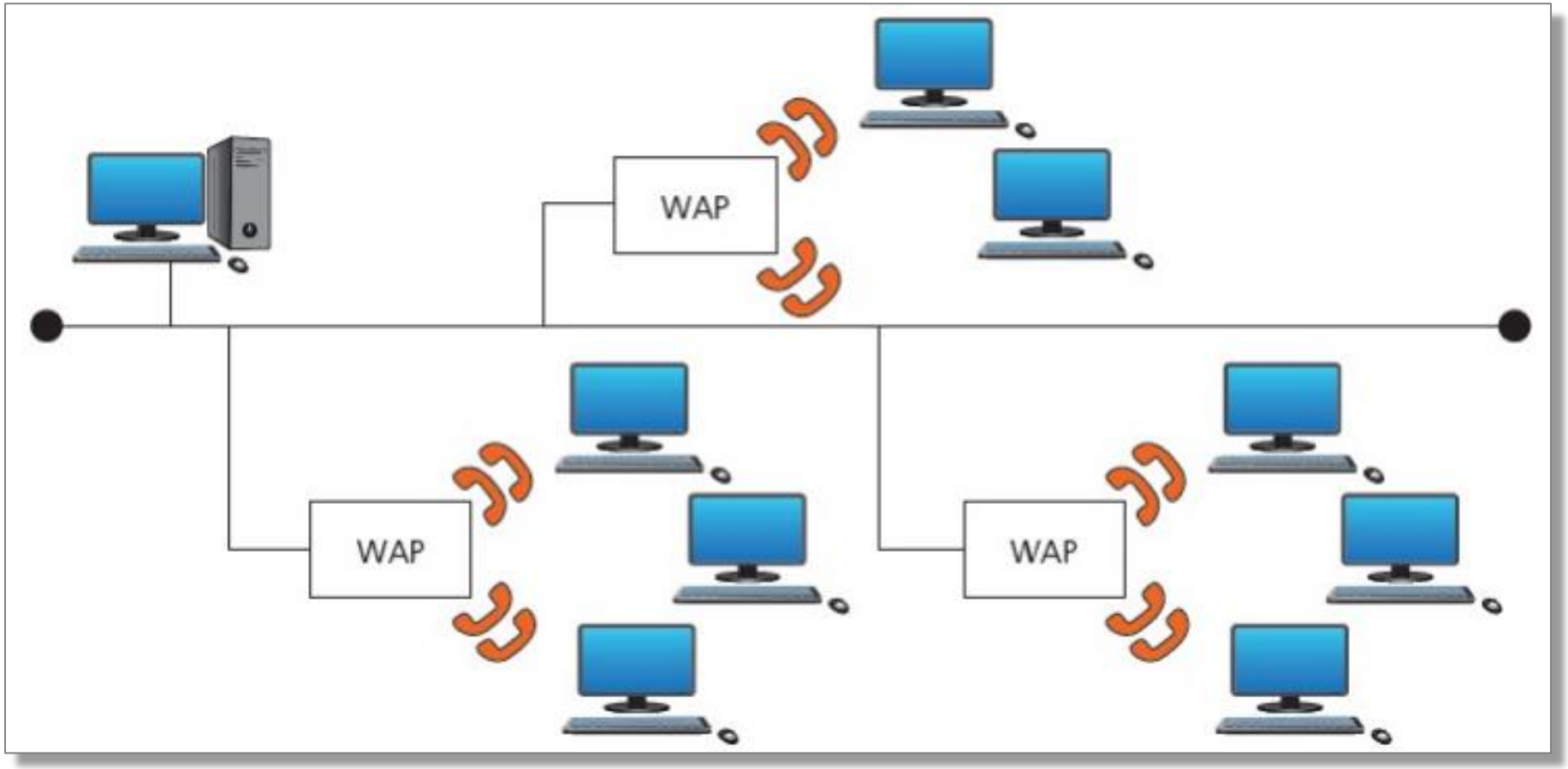
- **LANs**: Often in one building or small area.
- **Typical LAN**: Computers, devices (like printers), connected to hubs/switches.
- **Router/Modem Connection**: Allows LAN to connect to internet/WAN.

Wireless LANs (WLANs):

- **Wireless LANs (WLANs)**: No wires/cables, wireless network.
- **Short Distances**: Radio or infrared signals, up to 100 metres.
- **Wireless Access Points (WAPs)**: Connected in fixed locations.
- **Commercial LANs**: Like college campuses, airports, need multiple WAPs.
- **Spread Spectrum Technology**: Wideband radio, 1-100 metres range.
- **Infrared**: Short range, about 1-2 metres, limited use.

2.1.1 Networking Devices

- The WAP 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 the devices or as a plug in module.



2.1.1 Networking Devices

Wide Area Networks (WANs):

- **Wide Area Networks (WANs)**: Connect distant computers/networks.
- **Example**: Different cities, continents.
- **Multiple LANs**: Joined with router/modem to create WAN.
- ATM **Network**: Common WAN example.
- **Long Distances**: Use public comms network (phone lines, satellites).
- **Dedicated/Leased Lines**: Less costly, more secure than public network.

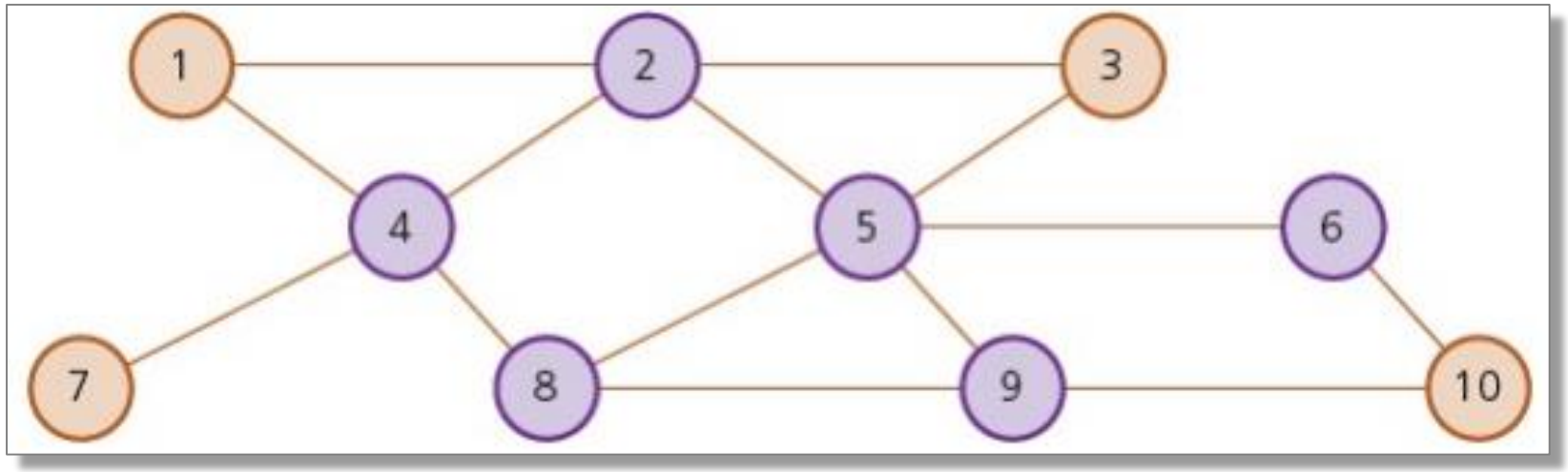
2.1.1 Networking Devices

Wide Area Networks (WANs):

- A typical WAN will consist of end systems and intermediate systems.
- 1, 3, 7 and 10 are known as end systems.
- The remainder are known as intermediate systems.
- The distance between each system can be considerable, especially if the WAN is run by a multinational company.

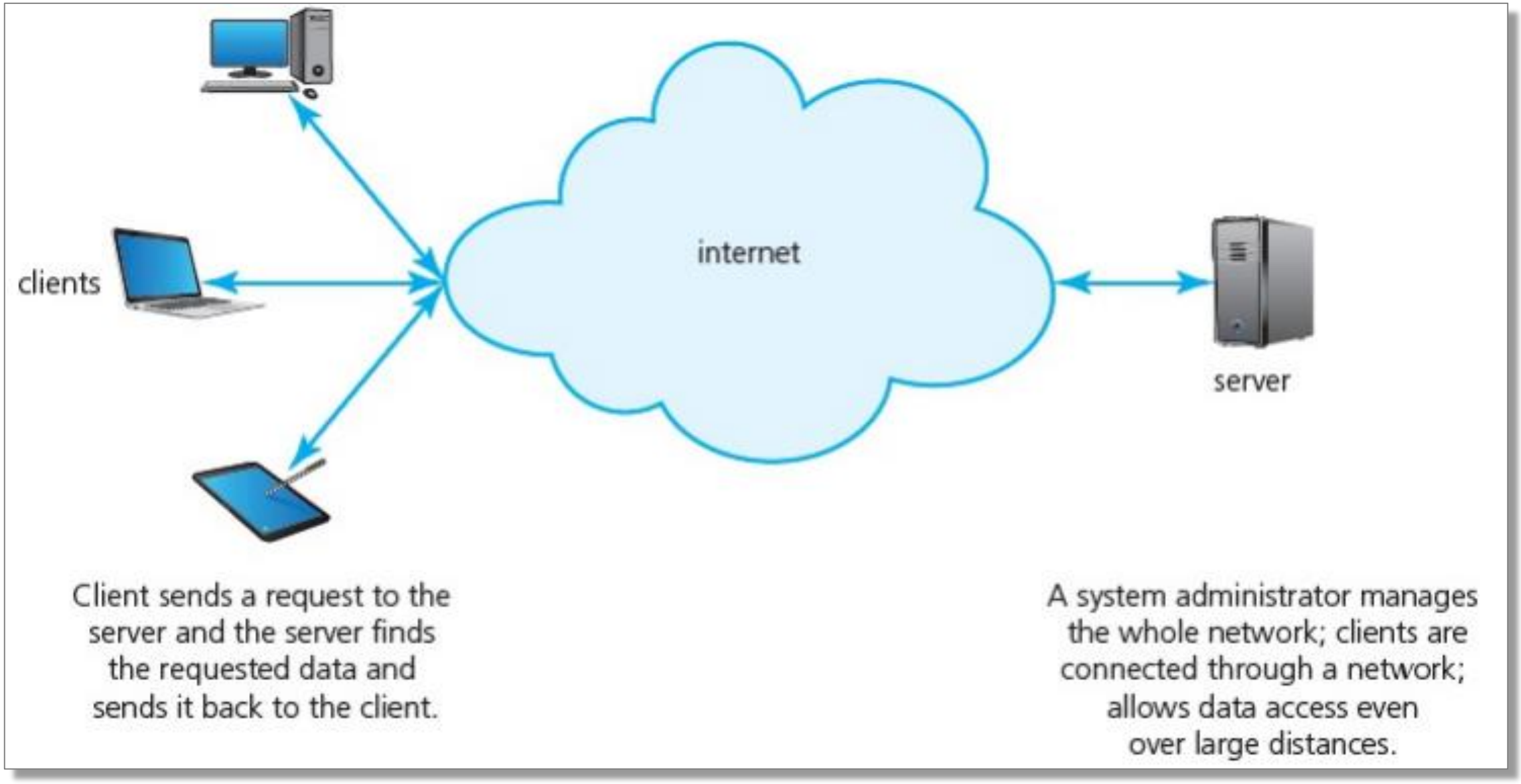
The following is used as a guide for deciding the 'size' of a network:

- WAN: 100 km to over 1000 km
- MAN: 1 km to 100 km
- LAN: 10 m to 1000 m
- PAN: 1 m to 10 m (this is not a commonly used term – it means **personal area network**; in other words, a home system)



2.1.2 Client-server and peer-to-peer networking models

Client-Server Model:



2.1.2 Client-server and peer-to-peer networking models

Client-Server Model:

- **Client-Server Model:**
  - Dedicated servers, specific client workstations.
  - Clients connect to server computer(s).
  - Access files stored on dedicated servers.
  - Server controls user-file access.
  - Allows software installation on client computers.
- **Central Security Databases:**
  - Control shared resource access.
  - Requires passwords, user IDs for login.
  - Users access assigned resources, files.
- **Security:** More secure than peer-to-peer.
  - User access limited by administrator.
- **Scal`ability:**
  - Client-server networks easily scalable.
  - Larger size, simpler scaling compared to peer-to-peer.

2.1.2 Client-server and peer-to-peer networking models

Client-Server Model:

- **Email Management:**
  - Central server handles storing, delivery, sending of emails.
- **Stability:** More stable system.
  - Deleted resource restored through nightly backup.
- **Bottlenecks:**
  - Client-server networks can bottleneck with multiple requests.
- **Client-Server Model:**
  - File Server is used and is responsible for:
    - Manages data storage centrally.
    - Enables user file access.
    - Information sharing without offline devices.
    - Any computer as host/file server.
    - Server can be storage device (SSD/HDD).
    - Acts as remote storage for other computers.

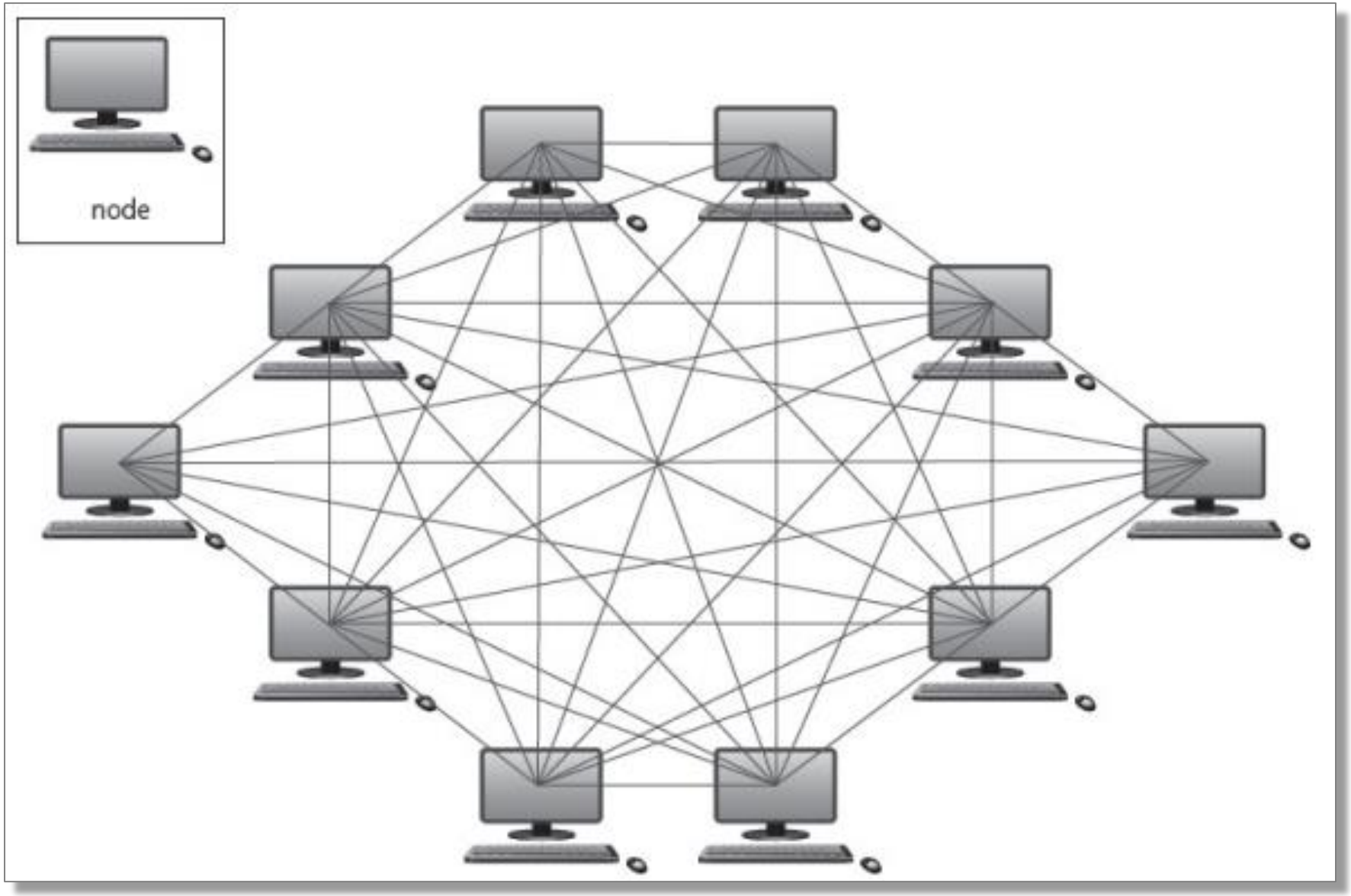
2.1.2 Client-server and peer-to-peer networking models

Examples of use of Client-Server Model:

- Reasons for Choosing Client-Server Model:
  - Large user-base or small groups needing data sharing.
  - Controlled network resource access.
  - Strong network security.
  - Centralized data backup to prevent loss.
- Example: Amazon's Use:
  - Front-end updated upon user login.
  - Large server architecture handles orders, billing, security.
  - Users unaware of each other's presence.
  - Interaction between users and server is separate.

2.1.2 Client-server and peer-to-peer networking models

Peer-to-Peer Model:



2.1.2 Client-server and peer-to-peer networking models

Peer-to-Peer Model:

- Peer-to-Peer Network:
  - Nodes provide services to other users.
  - 'Look up' computer lists available services.
  - Access data from other nodes.
  - Communicate with connected peers.
  - Peers act as suppliers and consumers.
  - Peers equal on network, unlike client-server.
- No Central Server:
  - Nodes share files among themselves.
  - Each node has own data, no central storage.
  - No need for user authentication.
- Use Cases:
  - Up to 10 nodes, like small businesses.
  - Contact among users is frequent.
- Performance and Management:
  - More than 10 nodes can lead to issues.
- Data Security:
  - Limited data security.
  - No central security system.
  - Users control own node share point.
  - Lack of authentication procedures.

2.1.2 Client-server and peer-to-peer networking models

Examples of Peer-to-Peer Network Model:

- **Reasons to Choose Peer-to-Peer Network Model**:
  - **Small Network**: Limited number of users.
  - **Less Security Needed**: Robust security not essential.
  - **Workstation Applications**: Prefer workstation-based over server-based.
- **Example**: **Small Business Use**:
  - Frequent user interaction.
  - No need for client-server features.
  - Builder and workers accessing each other's data.

2.1.2 Client-server and peer-to-peer networking models

Thin client:

- Thin Client Dependency:
  - Relies on server for file access, uninterrupted app running.
- Device or Software:
  - Needs connection to powerful computer/server.
  - Internet or network (LAN/MAN/WAN) connection.
- Constant Connection:
  - Must be connected to computer/server all times.
  - Software example: Web browser, limited functions without server.
  - Mobile phone apps needing continuous server access.
- Hardware Example:
  - POS terminal at supermarket needs constant server access.
  - Prices, customer charges, significant processing.

2.1.2 Client-server and peer-to-peer networking models

Thick client:

- **Thick Client Definition:**
  - Device or software, works offline or online.
  - Some processing possible without server connection.
- **Connectivity Options:**
  - Connects to LAN/MAN/WAN, virtual network, internet, cloud server.
- **Hardware Example:**
  - Normal PC/laptop/tablet, has storage, RAM, OS.
  - Effective operation online/offline.
- **Software Example:**
  - Computer game runs independently on user's computer.
  - Can connect to online server for multiplayer gameplay, communication.

2.1.2 Client-server and peer-to-peer networking models

Advs. and Disadvs. of using thick client hardware:

Advantages	Disadvantages
• More robust (device can carry out processing even when not connected to server) • Clients have more control (they can store their own programs and data/files)	• Less secure (relies on clients to keep their own data secure) • Each client needs to update data and software individually • Data integrity issues, since many clients access the same data which can lead to inconsistencies

2.1.2 Client-server and peer-to-peer networking models

Advs. and Disadvs. of using thin client hardware:

Advantages	Disadvantages
• Less expensive to expand (lowpowered and cheap devices can be used) • All devices are linked to a server (data updates and new software installation done centrally) • Server can offer protection against hacking and malware	• High reliance on the server; if the server goes down or there is a break in the communication link then the devices cannot work • Despite cheaper hardware, the start-up costs are generally higher than for thick clients

2.1.2 Client-server and peer-to-peer networking models

Differences between thick client and thin client hardware:

Thick Client software	Thin Client software
• Can run some of the features of the software even when not connected to a server • Relies heavily on local resources • More tolerant of a slow network connection • Can store data on local resources such as HDD or SSD	• Always relies on a connection to a remote server or computer for it to work • Requires very few local resources (such as SSD, RAM memory or computer processing time) • Relies on a good, stable and fast network connection for it to work • Data is stored on a remote server or computer

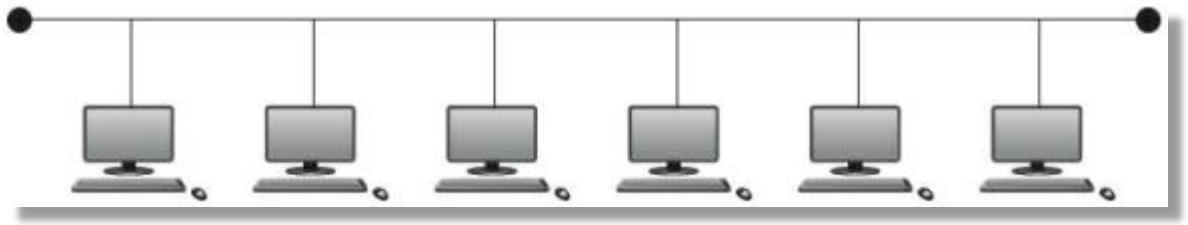
2.1.3 Network Topologies

- There are many ways to connect computers to make complex networks.
  - Bus networks
  - Star networks
  - Mesh networks
  - Hybrid networks

2.1.3 Network Topologies

Bus Networks:

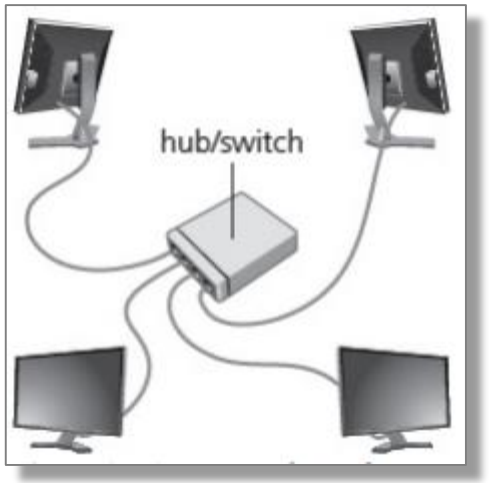
- Bus Network Topology:
  - Single central cable connects all computers/devices.
  - Easy expansion, minimal cabling.
  - Data travels in one direction.
  - Terminators prevent signal reflection.
- Disadvantages:
  - Main cable failure causes network outage.
  - Performance degrades with heavy load.
  - Not secure, packets pass through every node.
- Advantages:
  - Network continues if one node fails.
  - Easily expandable by adding nodes.
- Bus Network Node Behavior:
  - Node checks packet recipient address.
  - Matches: Node accepts packet.
  - Doesn't match: Packet ignored.
- Suitability:
  - Small device number, light traffic.
  - Small company, office environment example.



2.1.3 Network Topologies

Star Networks:

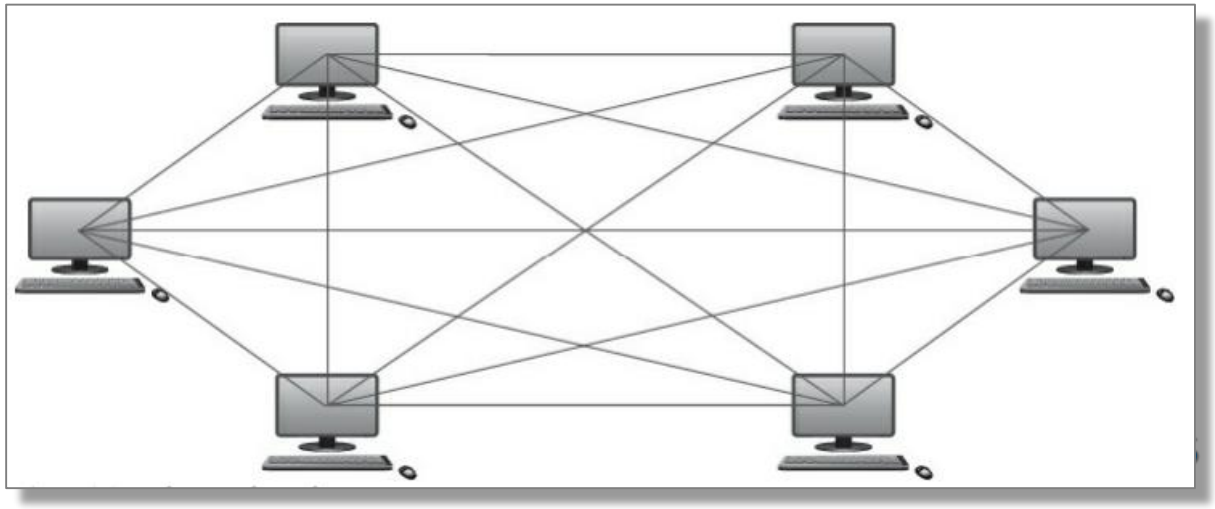
- Star Network Topology:
  - Central hub/switch, computers/devices connect.
  - Data directed through central hub/switch.
  - Each computer/device has dedicated connection.
  - Various cables can be used (wired/wireless).
- Disadvantages:
  - High initial installation costs.
  - Hub/switch failure affects whole network.
- Advantages:
  - Reduced data collisions.
  - More secure, central node security.
  - Easy improvement with upgraded hub.
  - Broken connection affects only one node.
- Packet Handling:
  - Depends on central node (switch/hub).
  - Hub: Packets to every device, accepted if address matches.
  - Switch: Packets to intended nodes only for higher security.
- Usefulness:
  - Evolving networks, frequent device changes.
  - Heavy data traffic applications.



2.1.3 Network Topologies

Mesh Networks:

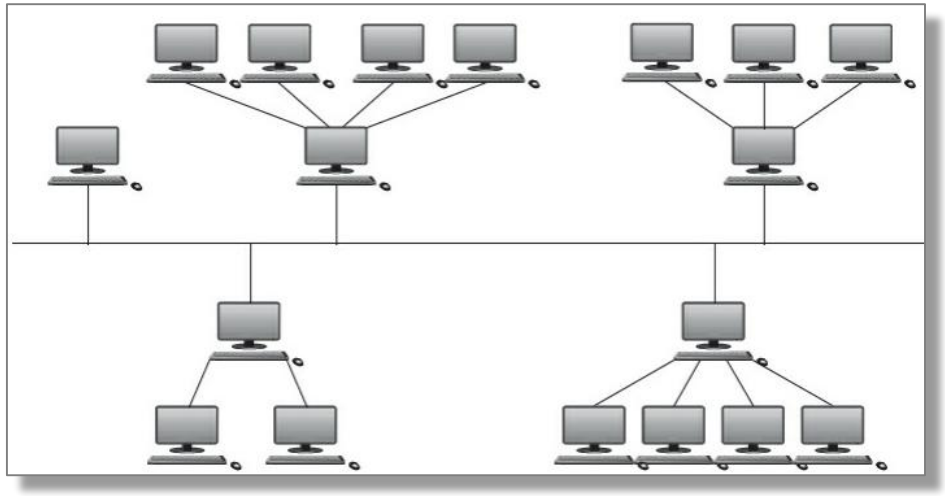
- **Mesh Network Topologies: Two Types:**
  - Routing: Nodes act as routers for shortest data route.
  - Flooding: Data sent to all nodes, no routing logic.
- **Routing Disadvantages:**
  - High cabling requirement, costly and time-consuming.
  - Complex setup and maintenance.
- **Advantages of Mesh Network:**
  - Easy fault identification.
  - Broken links don't affect other nodes.
  - Privacy, security via dedicated routes.
  - Network expansion is relatively simple.
- **Applications:**
  - Internet, WANs/MANs common uses.
  - Industrial monitoring, sensor-based mesh systems.
  - Examples:
    - Medical patient monitoring
    - Electronics connectivity.
    - Modern vehicles using wireless mesh networks.



2.1.3 Network Topologies

Hybrid Networks:

- **Hybrid Network: Mix of Different Topologies**:
  - Bus and star, bus and mesh, etc.
  - Advantages and disadvantages vary based on used topologies.
  - Complex installation, configuration, and maintenance.
- **Additional Advantages**:
  - Handles large traffic volumes.
  - Easy fault identification.
  - Well-suited for larger networks.
- **Packet Handling**:
  - Depends on hybrid structure's topologies
- **Application Example: Hotel Chains**:
  - Chain A: Bus network.
  - Chain B: Star network.
  - Chain C: Mesh network.
  - All chains connected by hybrid network technology.
- **Usage**:
  - Other applications possible.
  - Explore applications for each network topology.



2.1.4 Public and Private Cloud Computing

Cloud Computing:

- Cloud Storage Method:
  - Data stored on offsite servers.
  - Multiple servers for data redundancy.
  - Access data anytime, known as data redundancy.
  - Owned and managed by hosting company.
- Three Common Systems:
  - Public Cloud: Client and provider separate companies.
  - Private Cloud: Dedicated, behind company firewall.
  - Hybrid Cloud: Mix of private and public clouds.
- Cloud Benefits:
  - Data saved remotely, not local storage.

2.1.4 Public and Private Cloud Computing

Advs. and Disadvs. of using Cloud Computing:

Advantages	Disadvantages

• Access files anytime, anywhere with internet.
• No external storage needed, multiple devices usable.
• Remote data backup for data loss recovery.
• Recovers data after hardware failure.
• Offers nearly limitless storage capacity.
	• Internet Connection Issues:
	  • Slow/unstable connection hampers access.
	  • Problems with data/files download.
	• Cost Considerations:
	  • High costs for large storage needs.
	• Data Transfer Limits:
	  • High fees for download/upload limits.
	  • Internet service provider (ISP) charges.
	• Cloud Company Risks:
	  • Company failure risk, potential data loss.

2.1.4 Public and Private Cloud Computing

Data security when using cloud storage:

- Data Transfer to Cloud Providers:
  - Relinquishing data security control.
- Concerns Raised:
  - Physical Security: Data housing building.
  - Disaster/Power Resilience: Cloud provider's capability.
  - Personnel Safeguards: Cloud service company employees.
  - Unauthorized Access: Risk of misuse for monetary gain.

2.1.4 Public and Private Cloud Computing

Potential data loss when using cloud storage:

- Cloud Storage Risks:
  - Important data loss risk.
  - Hacker actions, access or attacks.
  - Safeguards needed against risks.
- Security Breaches Examples:
  - XEN Security Threat:
    - Cloud operators reboot due to XEN hypervisor issue.
  - Permanent Data Loss:
    - Data loss during routine backup by large provider.
  - Celebrity Photos Hack:
    - Leaked private celebrity photos.
    - Hackers accessed cloud accounts, published and sold photos.
  - Mexico Voter Data Breach:
    - National Electoral Institute breach.
    - 93 million voter registrations compromised.
    - Linked to an Amazon cloud server outside Mexico.

2.1.4 Public and Private Cloud Computing

Cloud Software:

- Cloud Computing Aspects:
  - Includes storage, databases, networking, software, analytics via internet.
- Cloud Software:
  - Delivered on demand to user's computer.
  - Hosted, managed by cloud provider.
  - Maintenance, upgrades, security included for fee.
- Accessing Cloud Software:
  - Connect to internet, contact cloud supplier.
  - Cloud supplier connects to required software.
- Advantages:
  - Fully tested software, no need on user's device.
  - Use software even offline, data stored locally.
- Cloud vs. Web-Based Apps:
  - Cloud-based apps work on local device.
  - Different from web-based apps needing constant internet.

2.1.5 Wired and Wireless Networking

Wireless:

- Wi-Fi and Bluetooth: Wireless Communication:
  - Use electromagnetic radiation for data transmission.
- Bluetooth:
  - 79 frequencies (channels) at 2.45 GHz.
  - Devices auto-detect, connect.
  - No interference, different channels per pair.
  - Random channel selection, frequency hopping.
  - Changes channels rapidly for minimal interference.
  - Secure WPAN based on key encryption.
  - Useful for short-range data transfer (within 30m).
  - Low bandwidth applications, non-critical speed.
- Wi-Fi:
  - Spread spectrum technology.
  - Full-scale networks.
  - Faster data rates, better range, security.
  - Access internet wirelessly up to 100m.

	radio waves	microwaves	infrared	visible light	ultra violet	X-rays	gamma rays
Wave length (m)	10^{2}	10^{-1}	10^{-3}	10^{-5}	10^{-7}	10^{-9}	10^{-11}
Frequency (Hz)	3 MHz	3 GHz	300 GHz	30 THz	3 PHz	300 PHz	30 EHz

Frequency and wavelength of magnetic radiation

2.1.5 Wired and Wireless Networking

Wireless:

- **Penetration and Attenuation:**
  - **Penetration:** Radiation passage through media.
  - **Attenuation:** Signal amplitude reduction.
- **Infrared's Characteristics:**
  - Low attenuation, affected by rain, walls.
  - Suitable for indoor use, stopped by walls.
  - Advantage: Prevents interference.
- **Microwaves Advantages:**
  - Good compromise.
  - Reasonable bandwidth, penetration, attenuation.

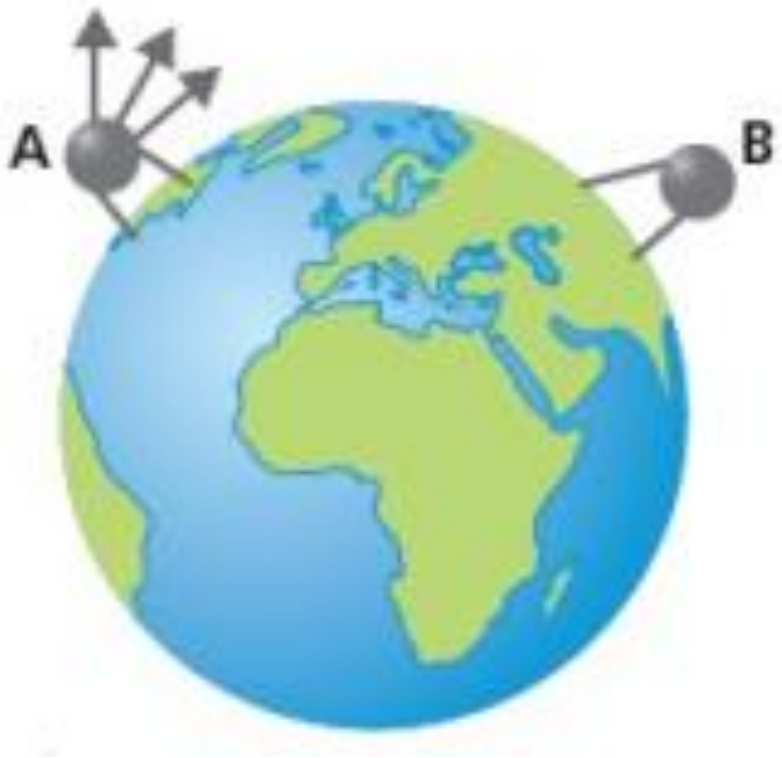
Bandwidth	infrared > microwaves > radio waves (infrared has the largest bandwidth)
Penetration	radio waves > microwaves > infrared (radio waves have the best penetration)
Attenuation	radio waves > microwaves > infrared (radio waves have the best attenuation)

Comparison of radio waves, microwaves and infrared

2.1.5 Wired and Wireless Networking

Additional notes on the use of satellites:

- **Microwaves and Radio Waves for Wi-Fi:**
  - Methods for Wi-Fi connectivity in networks.
  - Suitable for short distances.
  - Electromagnetic waves carry signals.
- **Global Data Transmission Limitation:**
  - Earth's curvature hinders global data transmission.
  - Not feasible for worldwide coverage.



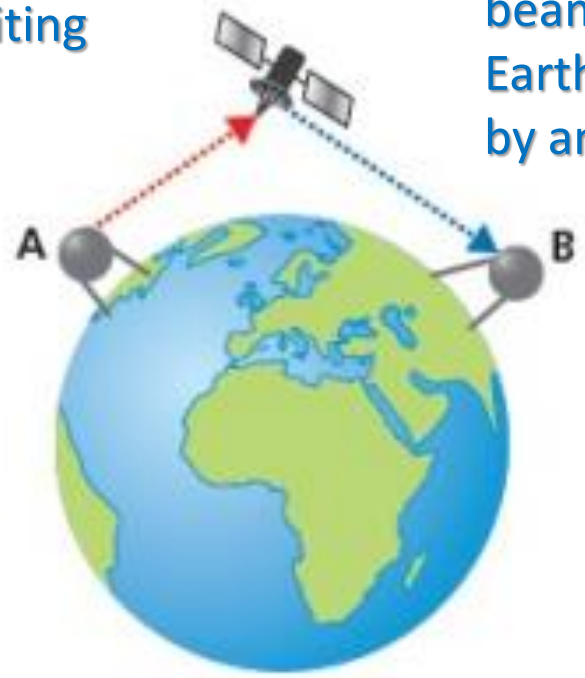
The electromagnetic radiation from antenna.
A is transmitted but is unable to reach antenna
B due to the Earth's curvature.

2.1.5 Wired and Wireless Networking

Additional notes on the use of satellites:

- To overcome this problem, we need to adopt satellite technology:
- Antennae-Satellite Communication:
  - Methods: Radio waves, microwave frequencies.
  - Frequency Bands: Prevent interference.
  - Enable global communication through satellites.
  - Many satellites orbiting Earth.

The signal is beamed from antenna A to a satellite orbiting Earth.

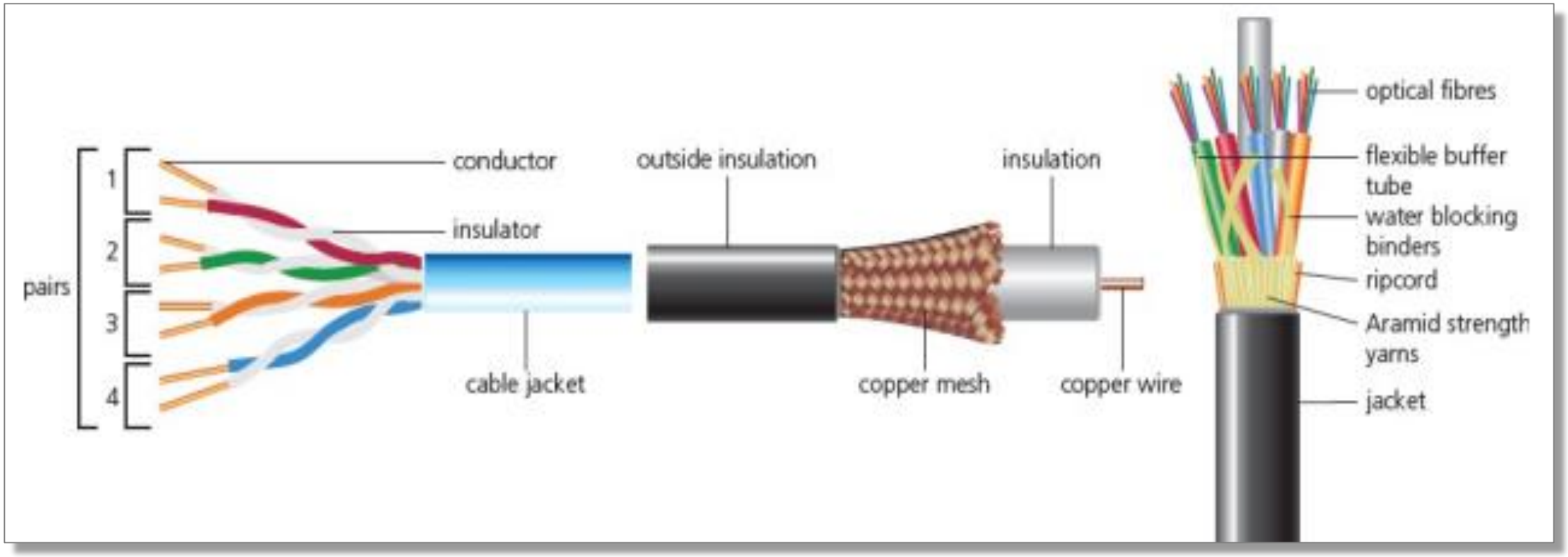


The signal is boosted by the satellite orbiting Earth and is then beamed back to Earth and picked up by antenna B.

2.1.5 Wired and Wireless Networking

Wired:

- There are three main types of cable used in wired networks:



Twisted pair cable, coaxial cable, fibre optic cable

2.1.5 Wired and Wireless Networking

- Twisted Pair Cables:
  - Most common in LANs.
  - Lowest data transfer rate.
  - Affected by interference.
  - Cheapest option.
  - **Types:** Unshielded and shielded.
- Coaxial Cables:
  - Used in MANs, cable TV.
  - Better data transfer than twisted pair.
  - Less external interference.
  - Higher cost than twisted pair.
  - About 80 times transmission capacity.
  - High anti-jamming capabilities.
  - Signal attenuation drawback.
- Fibre Optic Cables:
  - Used for long-distance data transfer.
  - Best data transfer rate.
  - Low signal attenuation, high resistance to interference.
  - High cost.
  - Use light pulses, not electricity.
  - About 26,000 times transmission capacity.
  - Types: Single-mode and multi-core.
  - Single-mode: Faster and further, good for CATV and telecom.
  - Multi-core: Higher reflections, shorter distances (LAN).

2.1.5 Wired and Wireless Networking

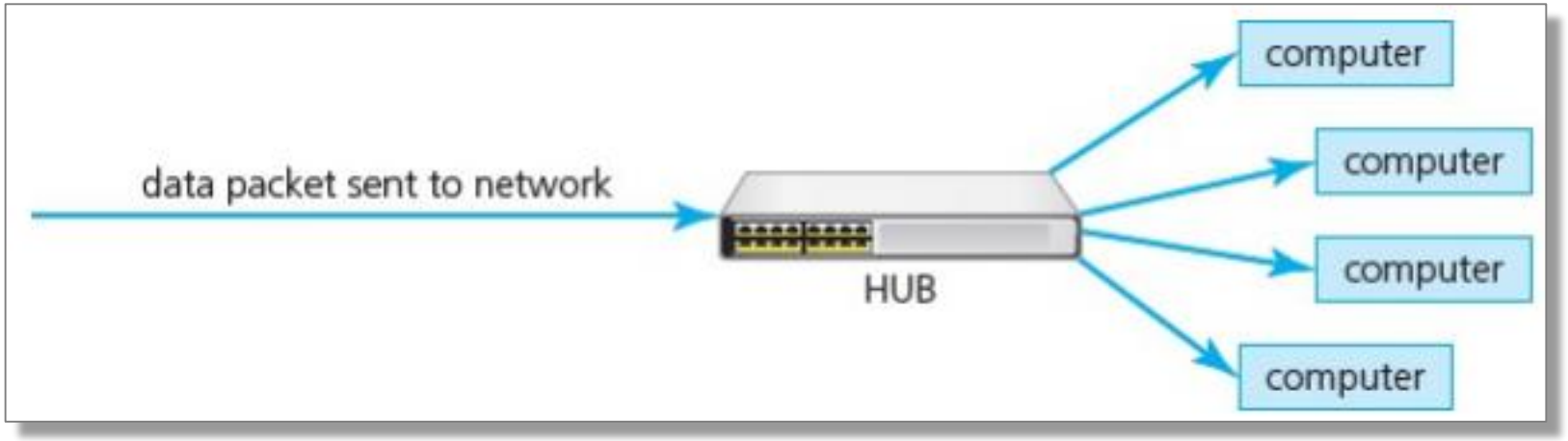
Wired versus wireless:

- **Wireless Networking**:
  - Easier network expansion, no cables needed.
  - Increased device mobility within WAP range.
  - Higher chance of external interference.
  - Less secure data transmission, needs encryption (WEP, WPA2).
  - Slower data transmission than wired.
  - Signals can be blocked by walls, signal strength varies.
- **Wired Networking**:
  - More reliable and stable, less interference.
  - Faster data transfer, no dead spots.
  - Tends to be cheaper overall.
  - Devices not mobile, need cable connections.
  - Tripping hazards, overheating, disconnection risks.
- **Other Considerations**:
  - Mobile devices need Wi-Fi/Bluetooth capability.
  - Legal regulations on wireless frequencies in some countries.
  - Permissions needed for laying underground cables.
  - Competing signals in the air, consider wired/wireless choice.

2.1.6 Hardware requirements of networks

Hardware items needed to form a LAN network and WAN network:

- Hub:
  - Hardware devices connecting multiple devices or computers.
  - Commonly used to create a local area network (LAN), like a star network.
  - Main task is broadcasting received data packet to all computers in the network.
  - Not secure and wastes bandwidth.
  - Available as wired or wireless devices.

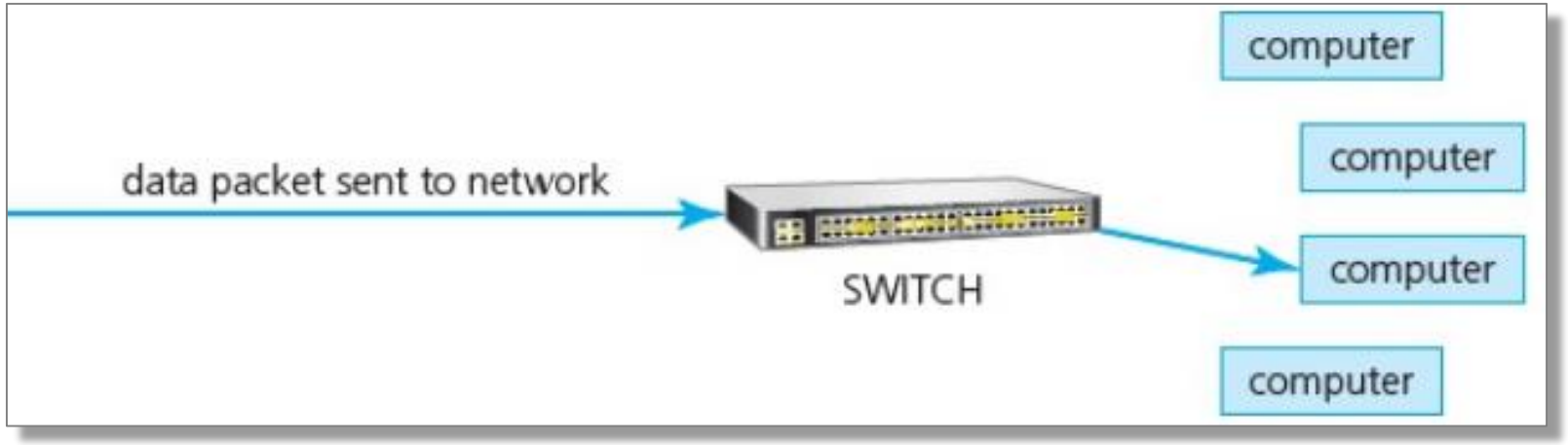


Data sent out to all computers on the network.

2.1.6 Hardware requirements of networks

Hardware items needed to form a LAN network and WAN network:

- Switch:
  - Similar to hubs but more efficient in data distribution.
  - Connects devices to create a LAN, like a star network.
  - Checks received data packet, determines destination address, and sends data to appropriate computer(s).
  - More secure and efficient method of data distribution compared to hubs.
  - Each device has a unique MAC address for identification.
  - Available as wired or wireless devices.



Data sent out only to the appropriate computers on the network.

2.1.6 Hardware requirements of networks

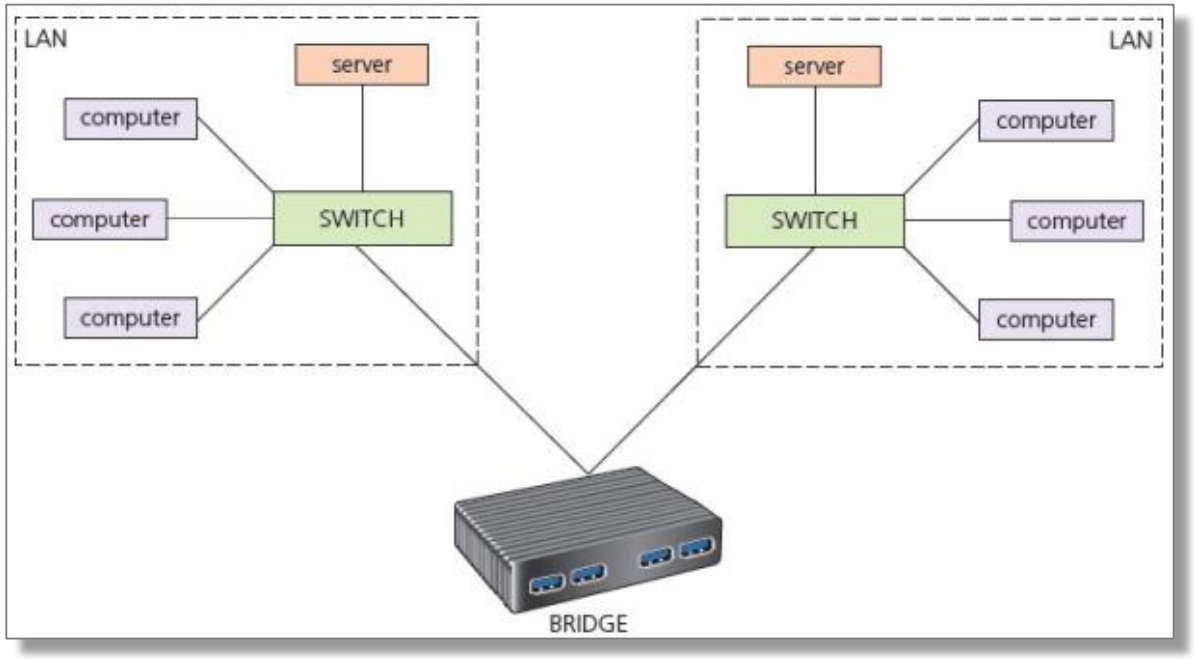
Hardware items needed to form a LAN network and WAN network:

- Repeater:
  - Boosts signals over long distances to counter attenuation.
  - Amplifies both analogue (copper cable) and digital (fibre optic cable) signals.
  - Used in wireless systems to prevent Wi-Fi dead spots.
  - Non-logical devices, amplify all detected signals without selectivity.
  - Hubs with repeaters are called repeating hubs, expanding operational range.
  - Drawbacks of repeating hubs:
    - Single collision domain, collisions not resolved immediately.
    - Unmanaged devices, lack control over delivery paths and network security.

2.1.6 Hardware requirements of networks

Hardware items needed to form a LAN network and WAN network:

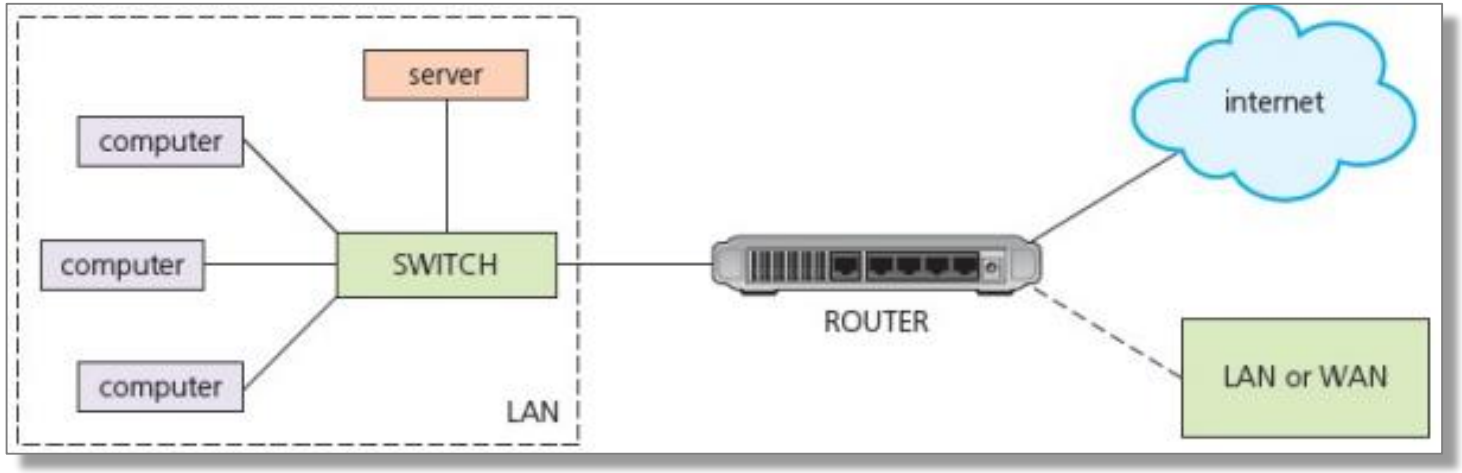
- Bridge:
  - Connects one LAN to another using the same protocol.
  - Often joins LAN parts to function as a single LAN.
  - Interconnects LANs or LAN parts to prevent flooding with excessive traffic.
  - Routers communicate with other networks like the internet.
  - Bridges can be wired or wireless devices.



2.1.6 Hardware requirements of networks

Hardware items needed to form a LAN network and WAN network:

- Router:
  - Routes data packets between different networks (e.g., LAN to WAN).
  - Converts data from one network's format to another's, enabling communication.
  - Restricts broadcasts within a LAN to manage network traffic.
  - Acts as a default gateway for network communication.
  - Performs protocol translation, facilitating communication between different types of networks.
  - Moves data between networks and calculates optimal routes.
  - Broadband routers include firewalls to protect network computers.
  - Inspects data packets, sending to appropriate devices based on IP and MAC addresses.
  - Routers can be wired or wireless devices.



2.1.6 Hardware requirements of networks

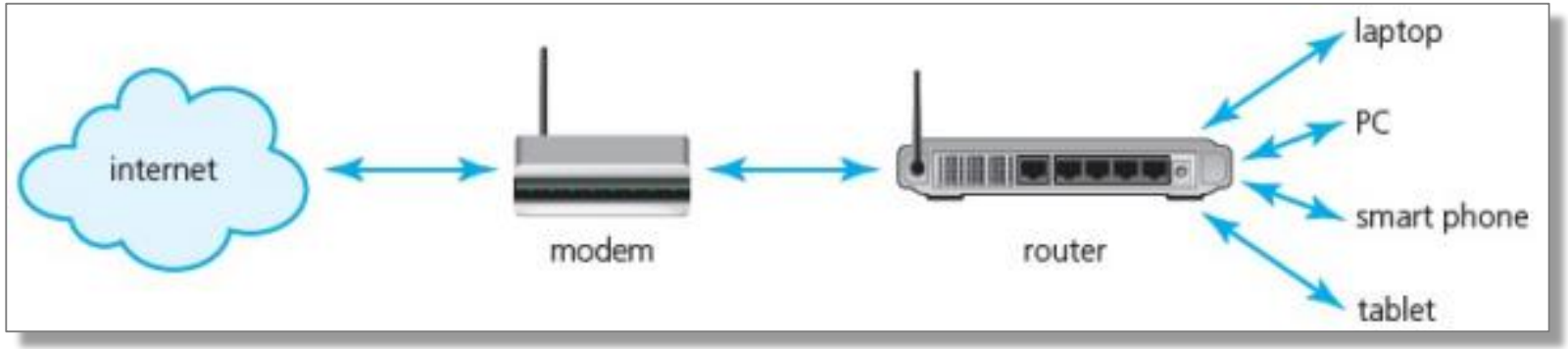
Hardware items needed to form a LAN network and WAN network:

- Gateway:
  - Acts as an entrance between networks, facilitating data exchange.
  - Connects dissimilar LANs using different protocols.
  - Converts data packets from one protocol to another.
  - Can function as a router, firewall, or server allowing traffic flow in and out.
  - Essential for communication outside a network, connecting to other networks.
  - Gateways can be wired or wireless devices.

2.1.6 Hardware requirements of networks

Hardware items needed to form a LAN network and WAN network:

- Modems:
  - Convert digital data to analogue data for transmission over analogue communication channels.
  - Reverse the process, converting analogue data from the network into digital data for computers.
  - Wireless modems enable simultaneous wireless communications without interference.
  - Connect to public infrastructure (cable, telephone, fiber-optics, satellite) and provide a standard Ethernet output for connection to a router.
  - Combine with routers to offer both router and modem functions in one unit.
  - Softmodem (software modem) uses minimal hardware and relies on the host computer's resources for processing and RAM.



2.1.6 Hardware requirements of networks

Hardware items needed to form a LAN network and WAN network:
Differences between routers and gateways.

Routers	Gateways
• Forward packets of data from one network to another; routers read each incoming packet of data and decide where to forward the packet • Can route traffic from one network to another network • Can be used to join LANs together to form a WAN (sometimes called brouters) and also to connect a number of LANs to the internet • Offer additional features such as dynamic routing (ability to forward data by different routes)	• Convert one protocol (or data format) to another protocol (format) used in a different network • Convert data packets from one protocol to another; they act as an entry and exit point to networks • Translate from one protocol to another • Do not support dynamic routing

2.1.6 Hardware requirements of networks

Hardware items needed to form a LAN network and WAN network:

- Network Interface Card (NIC):
  - Essential component for connecting a device to a network, including the internet.
  - Typically integrated into device hardware.
  - Often includes a manufacturing-generated MAC address for unique identification.

2.1.6 Hardware requirements of networks

Hardware items needed to form a LAN network and WAN network:

- Wireless Network Interface Card/Controller (WNIC):
  - Similar to regular NICs for network connection.
  - Utilizes antenna for communication through microwaves.
  - Often plugs into USB port or can be integrated internally.
  - Operates on layers 1 and 2 of OSI model.
  - Works in two modes:
    - Infrastructure mode: Requires Wireless Access Points (WAPs); data transmitted through WAP and hub/switch; devices connect to WAP with shared security.
    - Ad hoc mode: Direct device-to-device communication without WAPs; no need for intermediary WAPs.

Wireless network interface card/controller (WNIC)

2.1.7 Ethernet

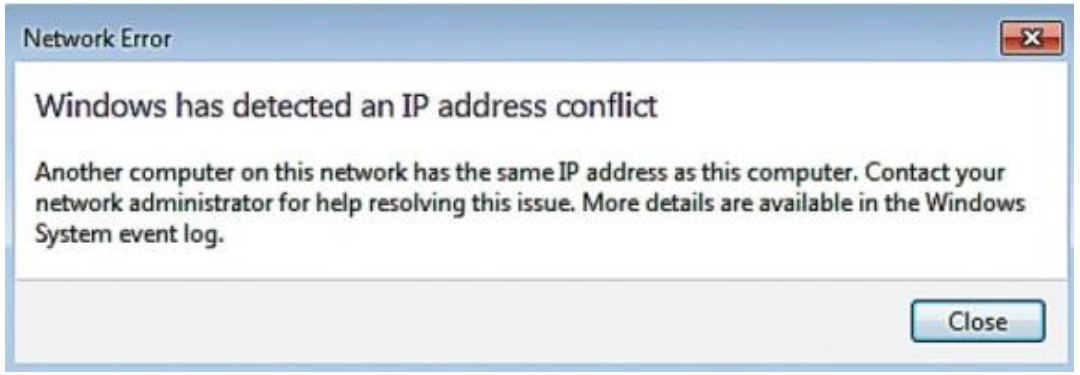
Ethernet:

- Ethernet Protocol:
  - Used in numerous wired LANs.
  - Standardized by IEEE as IEEE 802.3.
  - Ethernet network consists of:
    - Node: Any device within the LAN.
    - Medium: Path used by LAN devices (e.g., Ethernet cable).
    - Frame: Data transmitted in frames containing source and destination addresses (usually MAC addresses).

2.1.7 Ethernet

Conflicts and IP Address Conflicts:

- Ethernet networks can experience IP address conflicts.
- Conflicts might result in warnings.
- Conflict arises when devices share the same IP address on the network.
- Unique IP addresses are essential for network connectivity.
- Common in LANs with dynamic IP addresses.
- Dynamic IP addresses are temporary and can be reused.
- Conflict may occur if a dynamic IP is reassigned and matches a static IP.
- Resolution often involves restarting the router.
- Router restart leads to reassignment of dynamic IP addresses, resolving conflicts.



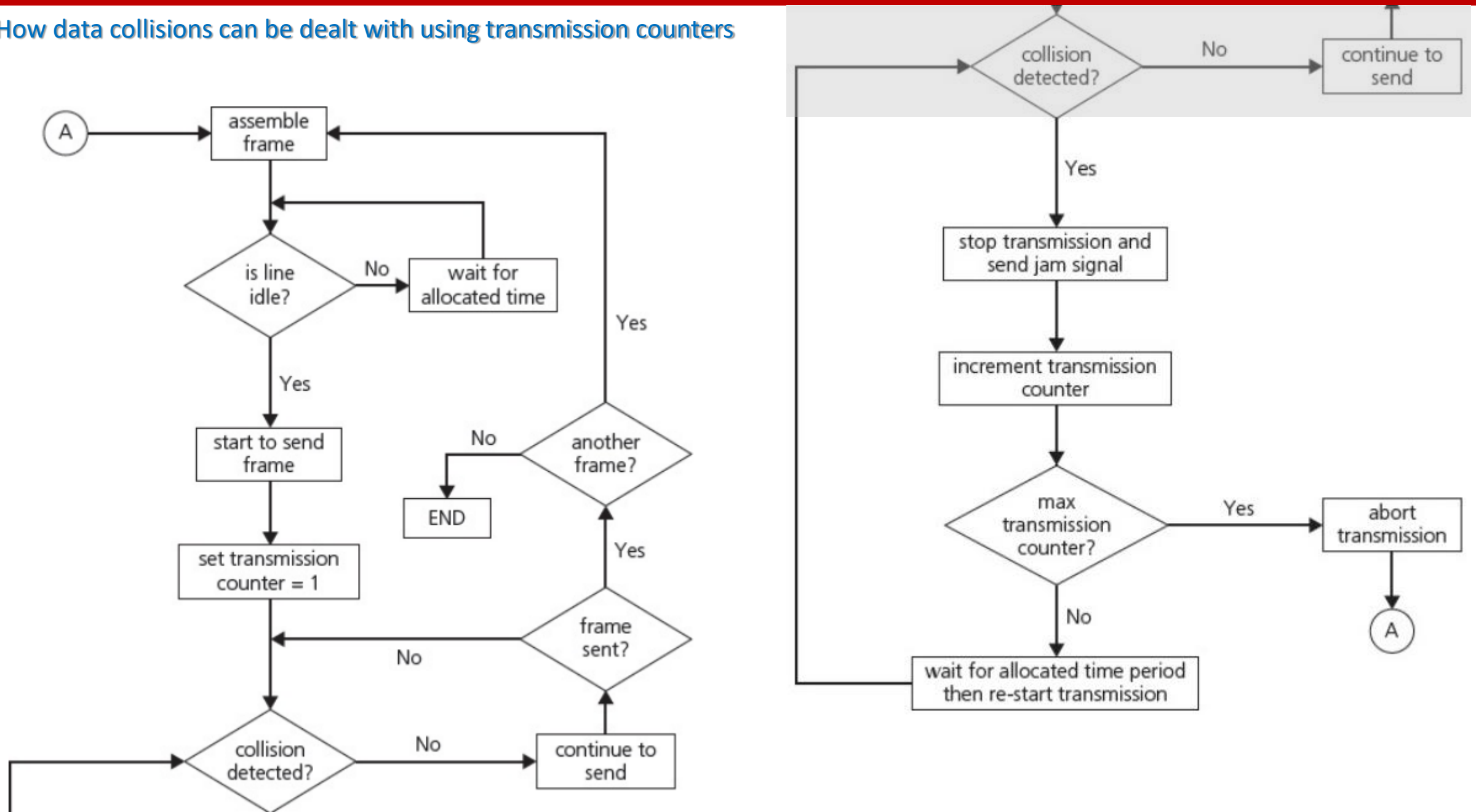
2.1.7 Ethernet

Ethernet Broadcast and Collision Handling:

- Ethernet supports broadcast transmission, sending data from sender to all LAN devices.
- Risk of collision when multiple messages share the same data channel.
- Carrier sense multiple access with collision detection (CSMA/CD) developed to address collisions.
- Collision detection relies on detecting voltage changes on the Ethernet cable.
- Upon collision detection, node halts transmission, sends a 'jam' signal, and waits.
- After a random time interval, device resends the frame.
- CSMA/CD protocol defines the random waiting period before retransmission.

2.1.7 Ethernet

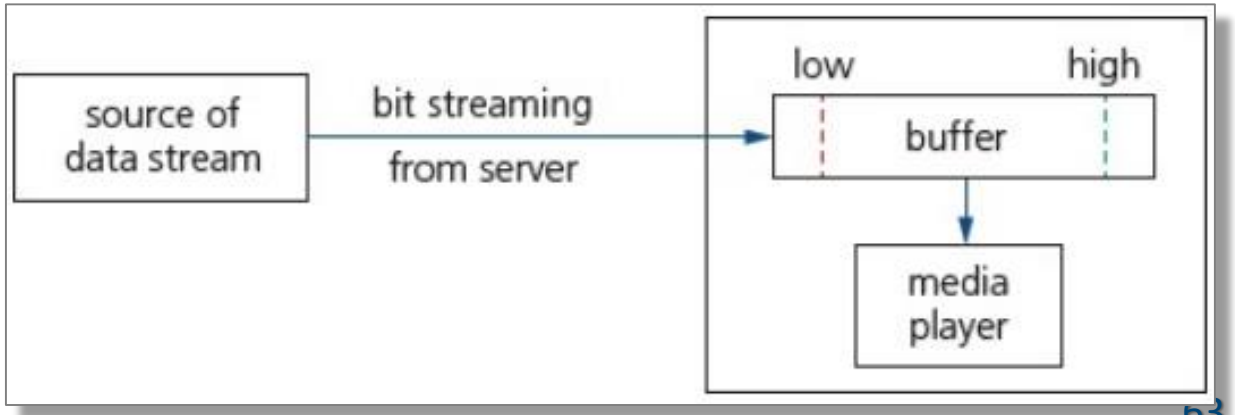
How data collisions can be dealt with using transmission counters



2.1.8 Bit Streaming

Bit Streaming and Buffering:

- Bit streaming involves sending a sequence of digital bits over the internet or a network.
- Requires high-speed data communication link, like fast broadband.
- Data compression often applied to large files (e.g., videos) before transmission.
- Buffering necessary for smooth playback of media files.
- Data transmission rate from file server to buffer must be higher than buffer to media player rate.
- Larger buffer enhances control over bit rate to media player.
- Media player maintains data between minimum (low water mark) and maximum (high water mark) values.
- Difference between values about 80% of total buffer capacity.
- Buffer serves as a temporary storage area on the computer.



2.1.8 Bit Streaming

Advantages and Disadvantages of Bit Streaming:

Advantages	Disadvantages
• No need to wait for complete download of video or music file before playback. • No need to store large files on device. • Enables on-demand playback of video and music files. • No specialized hardware required. • Offers anti-piracy protection, as streaming files are harder to copy compared to stored files on a hard drive.	• Cannot stream video or music files without an active broadband connection. • Video or music files may pause to buffer if insufficient buffer capacity or slow broadband. • Streaming consumes significant bandwidth. • Security risks linked to downloading files from the internet. • Potential copyright issues involved in streaming content.

2.1.8 Bit Streaming

Bit streaming can be either on demand or real time:

On Demand:

- Digital files are encoded and uploaded to a server.
- A download link to the encoded file is placed on the web server.
- Users click on the link to initiate the download of the contiguous bit stream.
- Streamed video/music is broadcast on demand to users.
- Pause, rewind, and fast forward functionalities are available for the streamed content.

Real-Time:

- An event is captured by camera and microphone and sent to a computer.
- The video signal is encoded to create a streaming media file.
- The encoded file is uploaded to a dedicated video streaming server.
- The server sends the live video to the user's device.
- Due to the live nature, pause, rewind, or fast forward options are not available for the video footage.

2.2 The Internet

KEY TERMS: (1/2)

- Internet – massive network of networks, made up of computers and other electronic devices; uses TCP/IP communication protocols.
- World Wide Web (WWW) – collection of multimedia web pages stored on a website, which uses the internet to access information from servers and other computers.
- HyperText Mark-up Language (HTML) – used to design web pages and to write http(s) protocols, for example.
- Uniform resource locator (URL) – specifies location of a web page (for example, www.hoddereducation.co.uk).
- Web browser – software that connects to DNS to locate IP addresses; interprets web pages sent to a user's computer so that documents and multimedia can be read or watched/listened to.
- Internet service provider (ISP) – company which allows a user to connect to the internet. They will usually charge a monthly fee for the service they provide.
- Public switched telephone network (PSTN) – network used by traditional telephones when making calls or when sending faxes.
- Voice over Internet Protocol (VoIP) – converts voice and webcam images into digital packages to be sent over the internet.
- Internet protocol (IP) – uses IPv4 or IPv6 to give addresses to devices connected to the internet.

2.2 The Internet

KEY TERMS: (2/2)

- IPv4 – IP address format which uses 32 bits, such as 200.21.100.6.
- Classless inter-domain routing (CIDR) – increases IPv4 flexibility by adding a suffix to the IP address, such as 200.21.100.6/18.
- IPv6 – newer IP address format which uses 128 bits, such as A8F0:7FFF:F0F1:F000:3DD0:256A:22FF:AA00.
- Zero compression – way of reducing the length of an IPv6 address by replacing groups of zeroes by a double colon (::); this can only be applied once to an address to avoid ambiguity.
- Sub-netting – practice of dividing networks into two or more sub-networks.
- Private IP address – an IP address reserved for internal network use behind a router.
- Public IP address – an IP address allocated by the user's ISP to identify the location of their device on the internet.
- Domain name service (DNS) – (also known as domain name system) gives domain names for internet hosts and is a system for finding IP addresses of a domain name.
- JavaScript® – object-orientated (or scripting) programming language used mainly on the web to enhance HTML pages. PHP – hypertext processor; an HTML-embedded scripting language used to write web pages.

2.2.1 The differences between the Internet and the World Wide Web

Internet:

- The Internet is a massive network of networks (although not a WAN) composed of various computers and electronic devices.
- It stands for interconnected network.
- The internet utilizes transmission control protocol (TCP)/internet protocol (IP).

World Wide Web (WWW):

- The World Wide Web (WWW) is a collection of multimedia web pages and documents stored on websites.
- HTTP(s) protocols are written using HyperText Mark-up Language (HTML).
- Uniform resource locators (URLs) specify the location of web pages.
- Web resources are accessed by web browsers.
- The WWW uses the Internet to access information from servers and other computers.

2.2.2 Hardware and Software needed to support the Internet

Fundamental things you need to connect to the Internet:

- Device: Like a computer, tablet, or phone.
- Connection: Use a phone line or mobile network. Tablets and phones can also connect through a wireless router.
- Router: This can be wired or wireless, and sometimes you need a modem too.
- Internet Service Provider (ISP): They give you the connection using hardware and software.
- Web Browser: Like Chrome or Firefox.

2.2.2 Hardware and Software needed to support the Internet

Fundamental things you need to connect to the Internet:

- Internet connects computers and devices between cities using the public switched telephone network (PSTN). To connect to other countries, we use satellite technology.
- Nowadays, phone lines are becoming fiber optic cables, which allow faster and better data transfer. These are often called "fast broadband". High-speed broadband lets us make WLANs (wireless local area networks) with WAPs (wireless access points).
- With fast connections, you can make phone and video calls using the internet. For phone calls, you can use a phone that connects to a computer or use a microphone and speakers. Video calls need a webcam. When you use the internet to make a call, your voice becomes digital data using VoIP. This data is split into packages and sent through the network's fastest path.

2.2.2 Hardware and Software needed to support the Internet

Comparison between PSTN and internet when making a phone call:

Public Switched Telephone Network (PSTN):

- PSTN uses a regular phone connected to a phone line.
- The phone line is always connected, even if nobody is talking.
- The connection stays until both people hang up.
- Phone lines work even during power outages with their own power.
- Modern phones use digital systems and fiber optic cables (but this can waste a lot of capacity, sending much data for short calls).
- Current phone lines use circuit switching where the connection is held for the whole call, which is how PSTN works.

2.2.2 Hardware and Software needed to support the Internet

Comparison between PSTN and internet when making a phone call:

Phone Calls Over the Internet

- Use an internet phone or microphone and speakers for calls (video needs a webcam).
- Internet only active when sending sound/video.
- Voice over Internet Protocol (VoIP) changes sound into digital parts to send over the internet.
- VoIP uses packet switching, where data is sent as needed with no dedicated line.
- Data split into packages with sender, receiver, and order info.
- VoIP compresses files to send less data.
- Short call may use about 3 MB data (more efficient than PSTN).

2.2.2 Hardware and Software needed to support the Internet

Comparison between PSTN and internet when making a phone call:

Cellular Networks and Satellites

- Mobile phones use cellular network (like groups of connected towers).
- Phone providers act as ISPs (internet providers).
- Phones have software for calls and internet.
- Satellites help with long-distance connections.
- Satellite's orbit height decides its coverage.
- Satellites give full coverage and less signal loss than cables.

2.2.2 Hardware and Software needed to support the Internet

How satellites are classified according to how high they orbit in relation to the Earth's surface:

Geostationary Earth Orbit (GEO) provide long distance telephone and computer network communications; orbital period = 24 hours

Medium Earth Orbit (MEO) used for GPS systems (about 10 MEO satellites are currently orbiting the Earth); orbital period = 2 to 12 hours

Low Earth Orbit (LEO) used by the mobile phone networks (there are currently more than 100 LEO satellites orbiting the Earth); orbital period = 80 mins to 2 hours

2.2.3 IP Addresses

TCP/IP protocols:

- The Internet is based on TCP/IP protocols.
- Protocols define the rules that must be agreed by senders and receivers on the Internet.
- Protocols can be divided into TCP layers.

2.2.3 IP Addresses

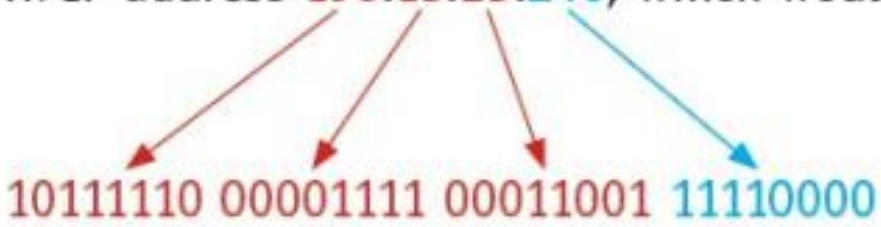
Internet protocols (IP):

- IPv4 Addressing
  - IPv4 is the common internet addressing type.
  - Based on 32 bits, offering 2^32 (4,294,967,296) addresses.
  - 32 bits divided into four 8-bit groups (0-255), like 254.0.128.77.
  - NetID and HostID are defined using these bit groups.
  - Transmission routed based on netID, hostID used by receiver.
  - Networks categorized into 5 classes.

Network class	IPv4 range	Number of netID bits	Number of hostID bits	Types of network
A	0.0.0.0 to 127.255.255.255	8	24	very large
B	128.0.0.0 to 191.255.255.255	16	16	medium size
C	192.0.0.0 to 223.255.255.255	24	8	small networks
D	224.0.0.0 to 239.255.255.255	–	–	multi-cast
E	240.0.0.0 to 255.255.255.255	–	–	experimental

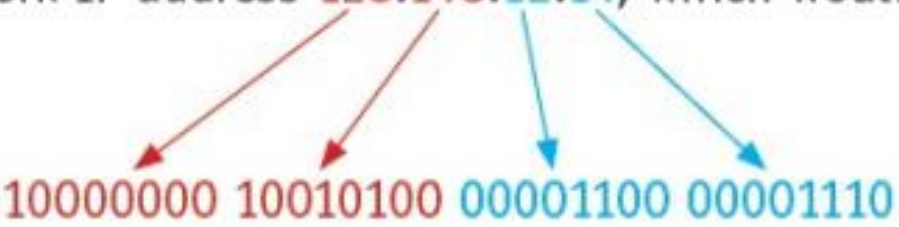
2.2.3 IP Addresses

Consider the class C network IP address 190.15.25.240, which would be written in binary as:



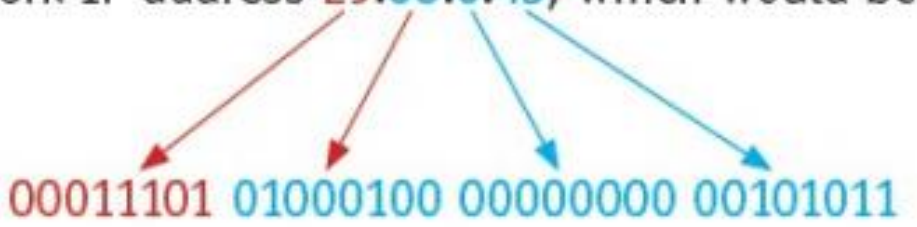
Here the network id is 190.15.25 and the host ID is 240.

Consider the class B network IP address 128.148.12.14, which would be written in binary as:



Here the network ID is 128.148 and the host ID is 12.14 (made up of sub-net ID 12 and host ID of 14).

Consider the class A network IP address 29.68.0.43, which would be written in binary as:



Here the network ID is 29 and the host ID is 68.0.43 (made up of sub-net ID 68.0 and host ID of 43).

Here the network ID is 29 and the host ID is 68.0.43
(made up of sub-net ID 68.0 and host ID of 43).

2.2.3 IP Addresses

Internet protocols (IP):

- IPv6 Addressing
  - Developed to address IPv4 problems.
  - Uses 128-bit addressing, allowing complex structures.
  - Address divided into 16-bit chunks, using hexadecimal notation.
  - For example: A8FB:7A88:FFF0:0FFF:3D21:2085:66FB:F0FA

    Note how a colon (:) rather than a decimal point (.) is used here

  - Facilitates internet growth in hosts and data traffic.
  - IPv6 advantages over IPv4:
    - No need for NATs (network address translation).
    - Eliminates risk of private IP address collisions.
    - Built-in authentication.
    - Enables more efficient routing.

2.2.3 IP Addresses

Internet protocols (IP):

- Zero Compression
  - IPv6 addresses can be quite long; but there is a way to shorten them using zero compression.
  - For example: 900B:3E4A:AE41:0000:0000:AFF7:DD44:F1FF
    can be written as: 900B:3E4A:AE41::AFF7:DD44:F1FF
    With the section 0000:0000 replaced by ::
  - The zero compression can only be applied ONCE to an IPv6 address, otherwise it would be impossible to tell how many zeros were replaced on each occasion where it was applied.
  - For example: 8055:F2F2:0000:0000:FFF1:0000:0000:DD04
    can be written as: 8055:F2F2::FFF1:0000:0000:DD04 *or*
    8055:F2F2:0000:0000:FFF1::DD04

2.2.3 IP Addresses

Internet protocols (IP):

- Zero Compression
  - 8055:F2F2::FFF1::DD04 is not a legal way of compressing the original address.
  - We have no way of knowing whether the original address was

    8055:F2F2:0000:FFF1:0000:0000:0000:DD04 *or*
    8055:F2F2:0000:0000:0000:FFF1:0000:DD04 *or*
    8055:F2F2:0000:0000:FFF1:0000:0000:DD04

  - It would, therefore, be regarded as ambiguous.

2.2.3 IP Addresses

Internet protocols (IP):

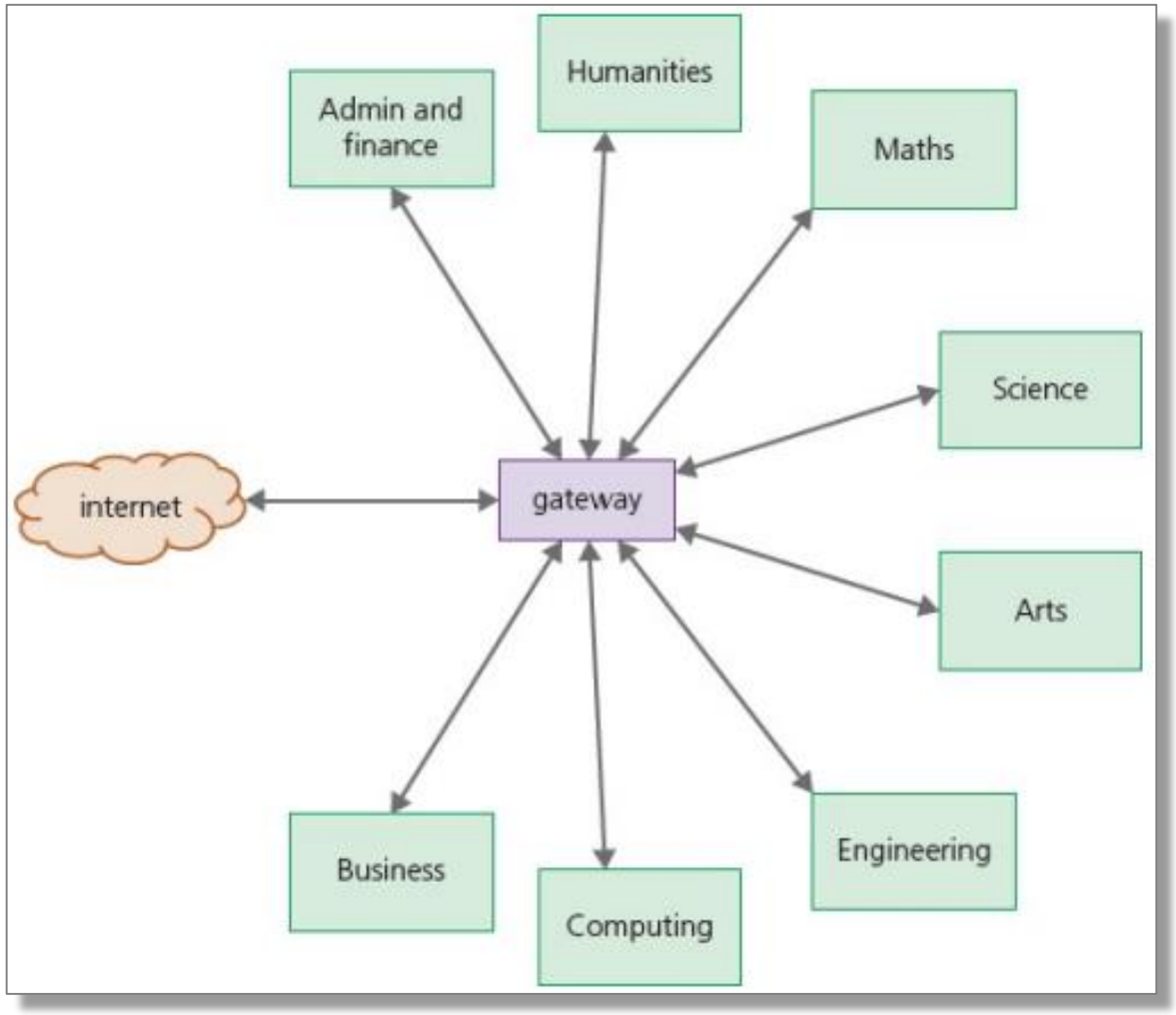
- Sub-netting
  - Sub-netting divides a LAN into two or more smaller networks.
  - This helps reduce network traffic and can also hide the complexity of the overall network.
  - Recall that the IP address (using IPv4) is made up of the netID and hostID.

  - Suppose a university network has eight departments and has a netID of 192.200.20 (11000000.11001000.00010100).
  - All of the devices on the university network will be associated with this netID and can have hostID values from 00000001 to 1111110 (hostIDs containing all 0s or all 1s are forbidden).

2.2.3 IP Addresses

Internet protocols (IP):

- Sub-netting
  - The university network will look something like this:



2.2.3 IP Addresses

Internet protocols (IP):

- Sub-netting
  - So, for example, the devices in the Admin and finance department might have hostIDs of 1, 8, 240, 35, 67, 88, 134, and so on, with similar spreads for the other seven departments.
  - It would be beneficial to organise the netIDs and hostIDs so that the network was a lot less complex in nature.
  - With sub-netting, the hostID is split as follows:
    000 00000
    where the first 3 bits are netID expansion
    the last 5 bits are the hostIDs.

2.2.3 IP Addresses

Internet protocols (IP):

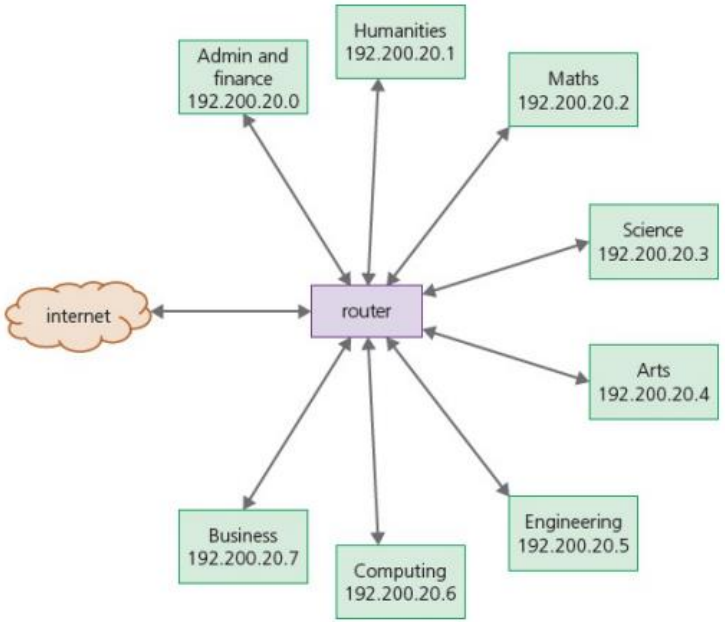
- Sub-netting
  - Thus, we have 8 sub-nets with the same range of hostIDs.

Department	netID	hostID range
Admin and finance	192.200.20.0	00001 to 11110
Humanities	192.200.20.1	00001 to 11110
Maths	192.200.20.2	00001 to 11110
Science	192.200.20.3	00001 to 11110
Arts	192.200.20.4	00001 to 11110
Engineering	192.200.20.5	00001 to 11110
Computing	192.200.20.6	00001 to 11110
Business	192.200.20.7	00001 to 11110

2.2.3 IP Addresses

Internet protocols (IP):

- Sub-netting



The devices in the Admin and finance department will have IP addresses

192.200.20.000 00001 to 192.200.20.000 11110

The Humanities department will have IP addresses

192.200.20.001 00001 to 192.200.20.001 11110

And so on for the other departments.

To obtain the netID from the IP address we can apply the AND mask (recall that 1 AND 1 = 1, 0 AND 0 = 0 or 1 AND 0 = 0). Thus, if a device has an IP address of

11000000.11001000.00010100.011 00011

we can apply the AND mask

11111111.11111111.11111111.111 00000

which results in the netID value

11000000.11001000.00010100.011 00000 (or 192.200.20.03)

This is the Science department. Consequently, the whole network is more efficient (for the reasons stated above) and less complex. Compare this to CIDR 192/200/20/0/27, which extends the size of the netID to 27 bits and has a hostID of only 5 bits, but would not reduce the complexity of the network.

2.2.3 IP Addresses

Private IP addresses and public IP addresses:

- Private IP Addresses:
  - Reserved for internal use behind a router or NAT device.
  - Allow for a separate set of addresses within a network.
  - Do not take up public IP address space.
  - Devices using private IP addresses not reachable by internet users.
- Public IP Addresses:
  - Allocated by ISP to identify device location.
  - Devices using these addresses accessible by internet users.
  - Used by:
    - DNS servers
    - Network routers
    - Directly-controlled computers

The following blocks are reserved for private IP addresses

Class A	10.0.0.0 to 10.255.255.255	16 million possible addresses
Class B	172.16.0.0 to 172.31.255.255	1 million possible addresses
Class C	192.168.0.0 to 192.168.255.255	65 600 possible addresses

2.2.4 Uniform resource service (URLs)

- Web browsers are software that allow users to access and display web pages on their screens.
- They interpret HTML sent from websites and display the results.
- Web browsers use uniform resource locators (URL) to access websites; these are represented by a set of four numbers, such as 109.108.158.1.
- But it is much easier to type this into a browser using the following format:

protocol://website address/path/filename

- Protocol is usually http or https
- Website address is
  - domain host (www)
  - domain name (name of website)
  - domain type (.com, .org, .net, .gov, and so on)
  - country code (.uk, .de, .cy, .br, and so on).
- Path is the web page (if this is omitted then it is the root directory of the website)
- Filename is the item from the web page

http://www.hoddereducation.co.uk/computerscience

2.2.5 Domain name service (DNS)

Domain Name Service (DNS):

- Also known as Domain Name System.
- Provides domain names for internet hosts.
- Finds IP addresses of domain names.
- Eliminates need to memorize IP addresses.
- Involves converting host name (e.g., **https://www.cam.ac.uk**) into an IP address.
- DNS servers often contain a database of URLs with matching IP addresses.

2.2.5 Domain name service (DNS)

Domain Name Service (DNS):

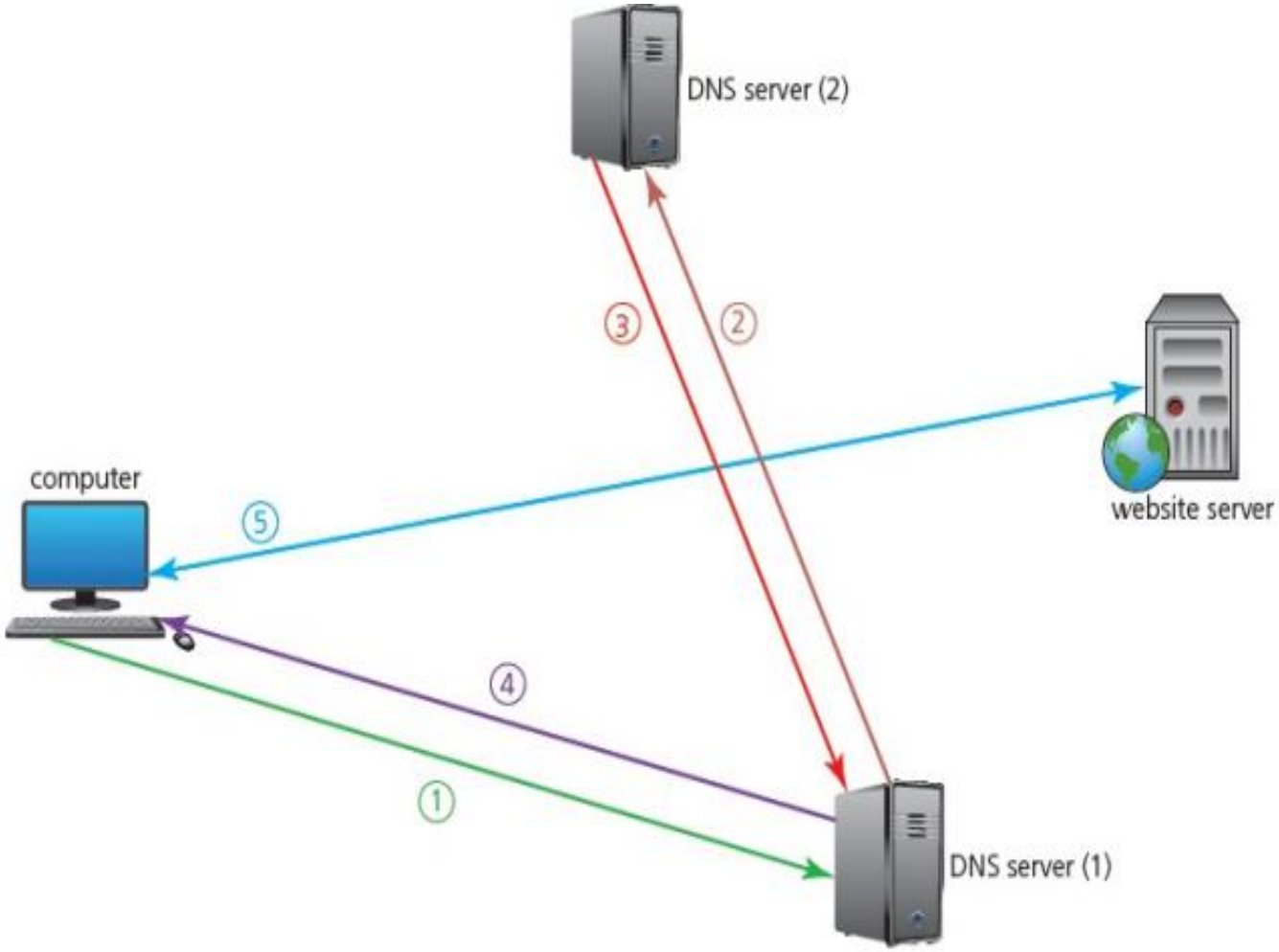
① The user opens their web browser and types in the URL (**https://www.cam.ac.uk**) and the web browser asks the DNS server (1) for the IP address of the website.

② The DNS server can't find **https://www.cam.ac.uk** in its database or its cache and sends out a request to DNS server (2).

③ DNS server (2) finds the URL and can map it to 107.162.140.19; the IP address is sent back to DNS server (1) which now puts the IP address and associated URL into its cache/database.

④ This IP address is then sent back to the user's computer.

⑤ The computer now sets up a communication with the website server and the required pages are downloaded. The web browser interprets the HTML and displays the information on the user's screen.



2.2.6 Scripting in HTML

HTML Scripting with JavaScript and PHP:

- HTML scripting using JavaScript and PHP discussed.
- Extends beyond the syllabus but included to understand website creation and browser-server communication.
- Included for information and understanding.
- To develop a web application (client-server based) on own computer, user needs to:
  - Download necessary server software.
  - Install the application on chosen/allocated server.
  - Use web browser to access and interpret application web pages.
- Each web page created using HTML.
- Domain name purchased from web-hosting company.
- HTML files uploaded to server allocated by web-hosting company.

2.2.6 Scripting in HTML

HTML Scripting with JavaScript and PHP:

- HTML would be used to create a file using tags.
- For example:

```
<html>
<body>
<p> Example <p/>
[program code]
</html>
```

- Between the HTML tags the inclusion of JavaScript or PHP can be used.

2.2.6 Scripting in HTML

HTML Scripting with JavaScript and PHP:

JavaScript:

- JavaScript is a programming language that runs on the client-side.
- Difference between client-side and server-side execution:
  - Client-side: Script runs on the computer making the request, processes web page data received from the server.
  - Server-side: Script runs on the web server, processing results sent to requesting computer.
- The following short program inputs a temperature and outputs 'HIGH' if it is 200 °C or over,
'OK' if it is 100 °C or over and 'LOW' if it is below 100 °C.

```
01  <html>
02  <body>
03  <p>Enter the temperature</p>
04  <input id="Temp" value="0"
05  <button onclick="checkReading()>"Enter</button>
06  <script>
07    function checkReading() {
08      var temp, result;
09      temp = document.getElementById("Temp").value;
10      if (temp >= 200) {
11      result = "HIGH"
12      } else if (temp >= 100) {
13        result = "OK"
14      } else {
15        result = "LOW"
16      }
17      alert("The result is " + result)
18    }
19  </script>
20  </body>
21  </html>
```

2.2.6 Scripting in HTML

HTML Scripting with JavaScript and PHP:

PHP:

- PHP in HTML - Server-side Processing:
- PHP is a language embedded within HTML.
- PHP is processed on the server-side.
- PHP code is placed within HTML and saved as a .php file.
- The following example temperatures are input but this time 'H', 'O' and 'L' are output depending on the result. Note that variables begin with $ and are case-sensitive.

```
01  <?php
02    if(isset($_GET['temp'])) {
03    echo "Result: " . checkReading($_GET['temp']);
04    } else {
05  ?>
06  <form action="#" method="get">
07    Enter Temp: <input type="text" name="temp" /><br />
08    <input type="submit" value="Calculate" />
09    </form>
10
11  <?php
12    }
13      function checkReading($inputTemp) {
14        $resultChar = "L";
15      if($inputTemp >= 200) $resultChar = "H";
16      else if($inputTemp >= 100) $resultChar = "O";
17      return $resultChar;
18    }
19  ?>
```