All unit 19 class notes

Explain - Learners' work shows clear details and gives reasons and/or evidence to support an opinion, view or argument. It could show how conclusions are drawn.

Analyse - Learners present the outcome of methodical and detailed examination either:
• breaking down a theme, topic or situation in order to interpret and study the interrelationships between the parts and/or
• of information or data to interpret and study key trends and interrelationships.

Evaluate - Learners draw on varied information, themes or concepts to consider aspects such as:
• strengths or weaknesses
• advantages or disadvantages
• alternative actions
• relevance or significance.
Learners' enquiries should lead to a supported judgement showing relationship to its context. This will often be in a conclusion.

Further information for teachers and assessors

Resource requirements

For this unit, learners must have access to:
• a physical or virtualised networking environment that provides the necessary hardware and software required to build and test computer networks safely
• computer systems, switches, routers, wireless access points, cabling, and operating systems for clients and servers
• online resources for research and development.

Essential information for assessment decisions

Learning aim A

The evidence should cover network hardware and software, including protocols and how they are used to construct a variety of networks types and models.
For distinction standard, learners will provide a clear and balanced evaluation of the different network models, including peer-to-peer, client/server and thin client. They must consider a wide range of aspects, including ease of use, ease of set-up, performance and suitability for different types of applications. The evidence will provide reasoned examples of the suitability of the different models to different networking applications, and clearly explain each model's benefits and drawbacks. The evidence will demonstrate high-quality written or oral communication through use of accurate and fluent technical vocabulary to support a well-structured and considered response that clearly connects chains of reasoning.
For merit standard, learners will provide a thorough analysis of the key functions of networking hardware and software components, including those used in LAN, WAN and wireless networks. Learners will demonstrate accurate understanding of the importance of the use of protocols and standards to connect various types of computer networks as outlined in the content. They will provide appropriate examples and illustrations to demonstrate their understanding of the complex issue of how data gets transferred within and between computer networks. The evidence will be technically accurate and demonstrate good-quality written or oral communication.
For pass standard, learners will provide detailed explanations of why different types and models of computer networks are needed and how that impacts on the choice of the network type and model used. They will explain how networks are continually evolving and taking different shapes and forms, from LAN, WAN, intranet, extranet and internet to cloud computing. Learners must also explain the general characteristics and functions of the network hardware and software components used to build and connect computer networks as covered in the unit content. The evidence may have some inaccuracies and make limited use of examples as illustrations.

Networking – the interconnection of computing devices that can exchange data and share resources with one another.
Summary of a network:

- 2 or more devices are connected.
- Devices share data.
- Can be large or small.
- Most organisations rely on network to do business.
- Fast-growing industry, a lot of businesses rely on networkin. Switches look at the data traffic and distribute them 5 differences between access point and routers are:

Functionality since a router is a multi-functional device that creates a network and manages traffic between networks which has features like wireless wifi, firewall and other security whereas access point is a single-functional device that acts a bridge to allow wireless network to connect to wired. Network role since a router acts as a gateway of a small home or office connecting it to internet and manage all connected devices whereas an access point is to extend the wireless coverage of a router's network which connects to the router via broadcast wifi signals or ethernet cables via a power line adapter or directly etc. Ip address management
Security features
Use case and coverage since as router can provide sufficient wireless coverage for a small house or office whereas access points can be used for larger houses or business etc to extend wireless coverage to a single router with low connectivity to ensure its connectivity to be consistent therefore result in no deadzones. PAN (personal area network) is a small network connects personal electronic devices within a person's immediate workspace.
LAN (Local area network) connects computers and other devices within a limited geographical area like home, office etc.
MAN (metropolitan area network) is a computer network that spans across a city or metropolitan area WAN (wide area network)
CAN (Campus Area Network) – connects multiple LANs with a limited geographical area
ADDS
DNS
DHCP – Ip addresses blocked DC – Domain Controller Server to switch to client Network models:
Client-server
Peer-to-peer
Thin client

Network topologies:
Physical topology
Logical topology

Network topology types:
1. Point-to-point
2. Bus
3. Ring
4. Star
5. Tree
6. Mesh

7. Hybrid

Task

Design a hybrid topology for a college classroom on draw.io

1. Network Types and Models

Networking – interconnection

1.1 Network Types:

Network types define the scale, structure, and purpose of a network. Common types include:

• LAN (Local Area Network):

◇ Covers a small geographic area like a home, office, building or campus.

◇ Used for: Sharing resources (printers, files) within one location.

🌍 Example: Uxbridge College's campus network.

• WAN (Wide Area Network):

◇ Covers a large geographic area, often connecting multiple LANs.

◇ Used for: Linking multiple branch offices or international operations.

🌍 Example: Amazon connecting warehouses across countries.

• PAN (Personal Area Network):

◇ Very small network, typically for a single person.

◇ Used for: Connecting personal devices like phones, laptops, or smartwatches.

🌍 Example: Bluetooth connection between a phone and headphones.

☑ Quick Summary: LAN = small/local, WAN = large/global, PAN = personal devices.

1.2 Network Models:

Network models describe how devices communicate and share data. Common models include:

• Client-Server Model:

◇ Central server provides resources and services to multiple clients.

◇ Used for: Centralised control and resource management.

🌍 Example: Uxbridge College ID system or email servers.

• Peer-to-Peer (P2P) Model:

◇ All devices are equal and can act as both client and server.

◇ Used for: Small networks where sharing between users is simple.

🌍 Example: Small office file sharing or home networks.

• Hybrid Model:

◇ Combines Client-Server and P2P, using servers for core services but allowing direct sharing between devices.

🌍 Example: Medium-sized companies that need file sharing and central control.

☑ Quick Summary: Client-server = centralised, P2P = decentralised, Hybrid = combination.

1.3 Difference Between Network Types and Models:
• Network Type: Physical/structural classification (LAN, WAN, PAN).
• Network Model: Logical/communication behaviour (Client-Server, P2P, Hybrid).
🔑 Key idea: Type = size & layout; Model = how devices interact.

2. Purpose of a Network:
A network allows an organisation to:
1. Share files and data efficiently.
2. Access centralised resources (printers, servers).
3. Enable communication via email, messaging, or video calls.
4. Support authentication systems (e.g., ID card swipes).
5. Access cloud-based applications and remote services.

🌍 Example: Uxbridge College uses a LAN to control ID swipes, manage student databases, and connect staff computers.

3. Choosing Network Types and Models for Real-World Applications:
3.1 Example – Uxbridge College ID System
• Suitable Network Type: LAN (local coverage, fast communication).
• Suitable Network Model: Client-Server (central server stores ID data; clients are swipe terminals).

☑ Why this combination works:
• Central control ensures accurate authentication.
• LAN ensures low latency and high reliability within campus.
• Client-server model allows scalability if more swipe points are added.

🌍 Other supported functions:
• Email & internal communication.
• Library and learning management systems.
• Shared printers and resources.

❌ Limitations:
• Does not cover remote operations outside campus (would need WAN or VPN).

4. Network Applications in Organisations of Different Sizes

4.1 Similarities Between Large and Small Organisations
• Network Type: Both may use LAN internally.
• Reason: Local resource sharing is essential for any organisation.
• Benefit: Fast, secure, and reliable internal communication.
• Network Model: Client-server often used in both.
• Reason: Central control simplifies management of accounts, access, and files.

4.2 Differences Due to Scale
• Large Organisation (Amazon): WAN connecting multiple warehouses globally. • Small Organisation (MagicMadhouse): May only use LAN and P2P due to smaller scale.

☑ Reason: Larger scale requires networks that can support remote branches, data replication, and disaster recovery.

❌ Not always the case: Small global teams could use cloud services instead of WAN.

5. Applying Knowledge: Key Takeaways
• Focus on where and why a network type/model is used.
• Real-world decisions depend on scale, purpose, security, and cost.
• Networks are tools to support organisational activities, not just theoretical structures.

6. Possible Exam-Style Questions
1. Explain the difference between a network type and a network model.
2. Recommend a network type and model for a university library and justify your choice.
3. Compare the network requirements of a large e-commerce company vs a small online shop.
4. Identify 5 functions that a network allows an organisation to perform, giving examples.
5. Discuss the advantages of using a Client-Server model over a Peer-to-Peer model in medium-sized organisations.

30-Minute Research Task: A2 Network Components Objective:
To research and understand the various hardware and software components that make up a computer network, including end-user devices, connectivity devices, connection media, and key software used in networking systems.

Task Instructions:

Part 1: Hardware Components (20 minutes)

Research and provide a brief summary on the following hardware components. For each, include what it is, its function within a network, and an example.

1. **End-User Devices**
    - Definition: What are end-user devices in a network? End-user devices are the hardware tools that individuals use to connect to and interact with a network. They act as the interface between the user and the network, enabling access to network services, communication, and data exchange.
    - Examples: Include both **mobile** and traditional devices (e.g. smartphones, laptops, desktops). **Mobile Devices:** Smartphones, tablets, and wearable devices like smartwatches. **Traditional Devices:** Laptops, desktop computers, and thin clients.
    - Their role in accessing the network. End-user devices serve as endpoints that send and receive data over the network. They allow users to browse the internet, access cloud services, communicate via email or messaging apps, and use various network-based applications.
    - Differences between mobile and traditional end-user devices.

- **Portability:** Mobile devices are lightweight and portable, designed for use anywhere, while traditional devices are usually stationary or semi-portable.
- **Input Methods:** Mobile devices mainly use touchscreens and virtual keyboards; traditional devices use physical keyboards and mice.
- **Screen Size:** Mobile devices have smaller screens optimised for portability; traditional devices have larger displays for extensive work or multitasking.
- **Power Sources:** Mobile devices rely on batteries and require periodic charging, whereas traditional devices typically depend on constant power supply through cables.

1. **Connectivity Devices**
    - Definition: What are connectivity devices? Connectivity devices are hardware components that enable devices to connect to a network and facilitate the transmission of data between them. They help manage, direct, and control network traffic to ensure effective communication.
    - Examples: **Switches, routers, access points**.

- **Cable:** Ethernet cables (twisted pair), coaxial cables.
- **Wireless:** Wi-Fi, Bluetooth, cellular networks.
- **Fibre:** Fibre optic cables.
    - Functions of each device.
- **Switches:** Connect multiple devices within the same local area network (LAN), allowing them to communicate directly by forwarding data packets to the correct device.
- **Routers:** Connect different networks together, such as linking a home or office network to the internet. They route data between networks and manage traffic efficiently to prevent congestion.

- **Access Points:** Create wireless signals that allow wireless devices like smartphones and laptops to connect to a wired network without physical cables.
    - How these devices interact with end-user devices and each-other.
- **Switches** connect wired devices (desktops, printers) within the local network, enabling data exchange among them.
- **Routers** connect the local network (via switches or APs) to external networks like the internet, managing data flow between internal devices and outside sources.
- **Access Points** broadcast wireless signals, enabling mobile devices to access the network and, through the router, access external resources.

1. **Connection Media**
    - Definition: What is connection media? Connection media refers to the physical or wireless pathways that carry data signals between devices in a network. They provide the channels through which information travels from one device to another.
    - Examples: **Cable, wireless, fibre**.
    - The pros and cons of each type of media.
- **Cable (Ethernet):**
- *Pros:* Stable and reliable connection, high speed, low latency, secure from interference.
- *Cons:* Requires physical installation and cabling, less flexible in terms of mobility.
- **Wireless (Wi-Fi):**
- *Pros:* Convenient and flexible, supports mobility, easy to set up without physical wires.
- *Cons:* Susceptible to interference, limited range, generally slower speeds compared to wired connections, potential security risks.
- **Fibre Optic:**
- *Pros:* Extremely fast data transmission, can cover long distances without signal loss, highly secure, supports large bandwidths.
- *Cons:* Expensive to install and maintain, requires specialised equipment and skilled technicians.
    - Use cases for cable vs wireless vs fibre in different network environments.
- **Cable:** Ideal for office environments, data centres, or places where stable, fast, and secure connections are necessary. It is preferred for devices that don't require mobility.
- **Wireless:** Best suited for homes, cafes, public places, and mobile environments where users need easy and flexible access without cables.

- **Fibre:** Commonly used by ISPs to provide high-speed internet over long distances and in data-intensive environments like enterprise networks and data centres.

Part 2: Software Components (20 minutes)

Research and summarise the role of the following software components in network management and operation: 1. **Networking Systems Software**

  - Definition: What are networking systems software? Networking systems software refers to specialised operating systems and software applications designed to manage and control network resources, traffic, and devices. This software enables communication between devices, ensures security, and facilitates the smooth operation of networks.
  - Examples: Common operating systems or software that support networking (e.g., Cisco IOS, Windows Server).

- **Cisco IOS:** The operating system used in Cisco routers and switches to manage network functions such as routing, switching, and security.
- **Windows Server:** A network operating system that provides services like user management, file sharing, and network security in enterprise environments.
- **Linux-based Network OS:** Used in many servers and network devices for flexibility and customisation.
  - The importance of networking systems software in managing network traffic and devices. Networking systems software is critical for managing network traffic efficiently, ensuring data packets reach their correct destinations, and maintaining the stability and security of the network. It controls device configurations, monitors network health, and enforces policies that prevent unauthorised access. Without such software, networks would lack coordination, resulting in data loss, slow performance, and security vulnerabilities.

1. **Network Monitoring, Management, and Troubleshooting Tools**
  - Examples: **Performance monitors, events and logs viewer, packet sniffers**.

- **Performance Monitors:** Tools like SolarWinds or PRTG that track network metrics such as bandwidth usage, latency, and uptime.
- **Events and Logs Viewer:** Software that records network events, errors, and activities, helping administrators identify issues (e.g., Windows Event Viewer).
- **Packet Sniffers:** Tools like Wireshark that capture and analyse network data packets to diagnose problems or detect suspicious activity.
  - What these tools are used for. These tools monitor the health and performance of a network, detect and diagnose issues, and analyse data traffic. They provide insights into network behaviour, identify bottlenecks or failures, and help trace security breaches or unusual activity.
  - How they help ensure network performance and security.

- **Performance Monitors** allow administrators to proactively detect slowdowns or overloads and optimise network resources.
- **Events and Logs Viewers** provide detailed records that help in troubleshooting problems and understanding network events after incidents.
- **Packet Sniffers** enable deep analysis of data flows to detect malicious traffic, unauthorised access, or configuration errors.

1. **Network Applications**
    - Examples: **Database management systems, document management systems**.
- **Database Management Systems (DBMS):** Such as MySQL, Oracle, and Microsoft SQL Server, which store, manage, and retrieve data for multiple users across a network.
- **Document Management Systems:** Like Microsoft SharePoint or Google Drive, which allow users to store, organise, and collaboratively edit documents.
    - The role of network applications in supporting business operations. Network applications are essential for enabling businesses to efficiently manage data, streamline workflows, and facilitate collaboration among employees. They support tasks like data storage, information retrieval, project management, and communication, which are critical for daily business functions.
    - How these applications use the network to share data and resources. These applications rely on the network to allow multiple users and devices to access shared resources and data simultaneously. They send and receive data over the network to update databases, synchronise documents, and enable real-time collaboration, ensuring that information is accessible from different locations and devices securely and efficiently.

Deliverable:
Prepare a concise 300-400 word written summary of your findings. Include specific examples and highlight key components that are essential for building and managing a network.
Time Breakdown:
- **15 minutes** for hardware research
- **15 minutes** for software research
- 5 extra minutes (optional) to review and summarise findings.

Unit 19 – Computer Networking
Learning Aim A3: Network Communication Standards and Protocols

1 Understanding the OSI and TCP/IP Models
1.1 The OSI Model

The **Open Systems Interconnection (OSI)** model is a **7-layer framework** used to understand how data is transmitted across networks.
Each layer performs specific tasks that allow communication between devices.

🌍 **Example:**
When you send a file online, data passes from the **Application layer (your browser)** down to the **Physical layer (Ethernet/Wi-Fi)** for transmission.

☑ **Quick Summary:**
- OSI = 7 layers (conceptual model).
- Each layer depends on the one below to deliver data successfully.

1.2 The TCP/IP Model
The **Transmission Control Protocol/Internet Protocol (TCP/IP)** model is a **4layer practical model** used by the Internet.

🔑 **Key Facts:**
- OSI has **7 layers**; TCP/IP has **4 layers**.
- TCP/IP's **Network Access** ≈ OSI's **Data Link + Physical layers**.
- Transport layer ensures **error checking**, **sequencing**, and **flow control**.

☑ **Quick Summary:**
- OSI = Theoretical model for understanding.
- TCP/IP = Real-world model used for Internet communication.

2 Protocols and Their Functions
2.1 Common TCP/IP Protocols

🌍 **Example:**
When you visit a website, your browser uses **HTTP** or **HTTPS** to communicate with a web server through **port 80 or 443**.

☑ **Quick Summary:**
- Different protocols serve different communication tasks.
- Port numbers help direct data to the correct service.

2.2 TCP vs UDP

🌍 **Example:**
- **TCP:** Used when accuracy matters (e.g., online banking).

- **UDP:** Used when speed matters (e.g., live video).

☑ **Quick Summary:**
TCP = reliable but slower.
UDP = fast but no guarantee of delivery.

3 Ports, Packets, and Encapsulation

3.1 Key Terms

- **Socket:** A combination of an **IP address and port number** used to identify network connections.
- **Packet:** A small unit of data transmitted across a network containing source, destination, and payload.
- **Frame:** A packet plus the **data link header and trailer** used for transmission at Layer 2.
- **Encapsulation:** The process of **wrapping data with headers** as it moves down the OSI layers.

🌍 **Example:**
When sending an email, the message (Application) becomes a **segment (Transport)**, then a **packet (Network)**, then a **frame (Data Link)**.

☑ **Quick Summary:**
Encapsulation = wrapping;
De-encapsulation = unwrapping during reception.

4 IEEE 802 Standards

☑ **Quick Summary:**
IEEE standards ensure **interoperability and compatibility** between devices and manufacturers.

5 Applied Task Example

Scenario: Designing a Small Business Network Wired Connections:
Use **Ethernet (IEEE 802.3)** for reliability and high speed.
Wireless Access:
Use **Wi-Fi (IEEE 802.11ac or 802.11ax)** to provide mobility and guest access.
IP Addressing and Name Resolution:
Implement **DHCP** to assign IPs automatically and **DNS** to resolve names into IP addresses.

Secure Transmission:
Use **HTTPS** and **SSH** for encryption, **WPA3** for wireless security, and **VPN** for remote access.

🌍 **Example:**
A cafe network uses **Ethernet** for cash register systems, **Wi-Fi** for customers, **DHCP/DNS** for device configuration, and **HTTPS** for secure online payments.

☑ **Quick Summary:**
A good network balances **speed, security, and scalability** using standard protocols.

6 Extension: Encapsulation in Email Transmission

When an email is sent:

1. **Application Layer (SMTP):** Message created and formatted.
2. **Transport Layer (TCP):** Divides message into **segments**, adds sequence numbers.
3. **Internet Layer (IP):** Adds **source and destination IP addresses**.
4. **Network Access Layer (Ethernet/Wi-Fi):** Converts to **frames and signals**.
   At the receiving computer, the process **reverses (de-encapsulation)** — each layer removes its header until the **email application** displays the message.

🌍 **Example:**
Sending from Gmail to Outlook involves **SMTP (sending)** and **POP3/IMAP (receiving)** using **TCP/IP** protocols.

☑ **Quick Summary:**
Encapsulation adds headers for delivery; de-encapsulation removes them for reading.

7 Advantages & Disadvantages of Communication Protocols

8 Possible Exam-Style Questions

5. **Explain the purpose of the OSI model** and describe two of its layers.
6. **Compare TCP and UDP** in terms of reliability and use cases.
7. **Identify the IEEE standards** used for Ethernet and Wi-Fi.
8. **Describe how encapsulation works** when sending an email over the Internet.
9. **Discuss why protocols like DHCP and DNS** are important for modern networks.

10. **Design a small business network** using both wired and wireless standards and justify your choices.

Kerberos (for ticket-based authentication in enterprise environments), RADIUS (a centralised system for managing network access), LDAP (for verifying credentials against a directory service), and TACACS+ (for authenticating access to network devices). These protocols verify user or device identities to protect network resources from unauthorised access by using methods like shared secrets, public keys, or centralised databases.

Key authentication services and protocols

Kerberos

- What it is: A network authentication protocol that uses secret-key cryptography.
- What it does: Issues "tickets" to users to grant them access to various network services without requiring them to re-enter their password for each service.
- Used with: Enterprise environments, Windows and Unix-based systems, and other services that need to provide secure, single-sign-on access. RADIUS (Remote Authentication Dial-In User Service) • What it is: A centralised authentication service.
- What it does: Manages network access by forwarding user credentials to a central server for verification against a database and then granting or denying access based on predefined policies.
- Used with: Centralised authentication for network access, such as Wi-Fi or dial-up, and for controlling access to network devices.

LDAP (Lightweight Directory Access Protocol)

- What it is: A protocol used for accessing and maintaining distributed directory information services.
- What it does: Verifies user credentials by checking them against a user data store, such as a user database.
- Used with: Verifying credentials in applications that use a central directory service for user authentication.

TACACS+

- What it is: A protocol used for network access control.
- What it does: Authenticates and authorises users when they try to access network devices like routers and switches.
- Used with: Network devices that need a centralised authentication and authorisation process for user access.