ULTRA NETWORKING

Table Of Contents

A. INTRODUCTION

The purpose of this report is to first and foremost explains the fundamentals of networking, providing the readers with the ability to install, troubleshoot and operare a small network. This also includes IP routing technologies, IP services and the basics in troubleshooting. Readers will develop skills such as communication literacy, critical thinking, analysis, reasoning and interpretation, which are crucial for gaining employment and developing academic competence.

Computer networking has basically become essential for how modern organizations actually function, letting people communicate, share resources, and work together even when they're in different places. As businesses, schools, and other institutions rely more and more on connected systems just to get things done, understanding how networks work and how to design them properly is really important. This report walks through networking fundamentals in a way that should make sense even if you're pretty new to the subject. It starts with basic stuff like what different network types are and how they're arranged physically, then moves into the more technical details about protocols and standards that let computers talk to each other, and finally gets into practical considerations for actually setting up networks in the real world. The main goal is to give readers both the theoretical knowledge they need and practical insights they can actually use when designing, implementing, and maintaining network systems. By looking closely at network hardware components, different types of servers, how networking devices actually operate, and especially how hardware and software depend on each other completely, this report shows how every technical decision you make affects overall network performance, reliability, and how much it costs. Rather than just throwing theory at you, the report examines these concepts through a practical scenario involving an educational institution with 235 users spread across multiple floors, which helps connect abstract networking ideas to real implementation challenges you might actually face. Whether it's figuring out how choosing a particular physical topology affects bandwidth, understanding how protocol layering lets networks scale up, or deciding which servers to buy when you've got budget constraints, this report emphasizes that successful networking really requires understanding how all these different pieces fit together to create infrastructure that actually works, performs well, and stays secure.

B. CONTENT

I – Discuss the benefits and constraints of different network types and standards

1. What is Computer Networking?

a. Networking defintions and its roles in connection between devices

A network is basically just two or more computers connected together so they can exchange information and share resources (Lowe, 2004, p. 9). The basic definition sounds simple enough, but if you think about why networks actually exist, it becomes clearer why they matter so much. Without networks, computers would be isolated, which means no shared resources or teamwork. When organisations connect machines together, they avoid buying the same equipment multiple times and let people actually work on the same projects instead of working separately.

b. Simple diagram to visualize how devices are connected.

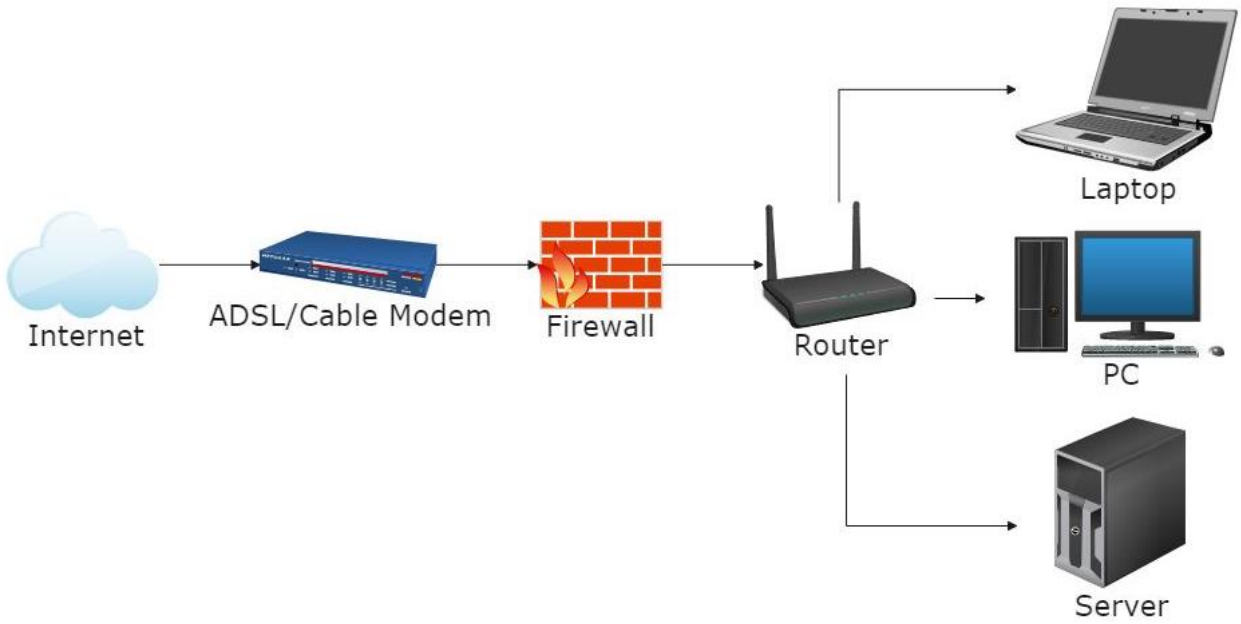

Figure 1. Basic Network Diagram

2. Common Network Types

a. LAN (Local Area Network)

A LAN connects computers within close proximity, such as within the same office or building (Lowe, 2004, p. 14). This definition does not imply small size; LANs can contain hundreds of computers. What matters is geographic proximity, typically within a single building or across nearby buildings on a campus.

+Diagram:

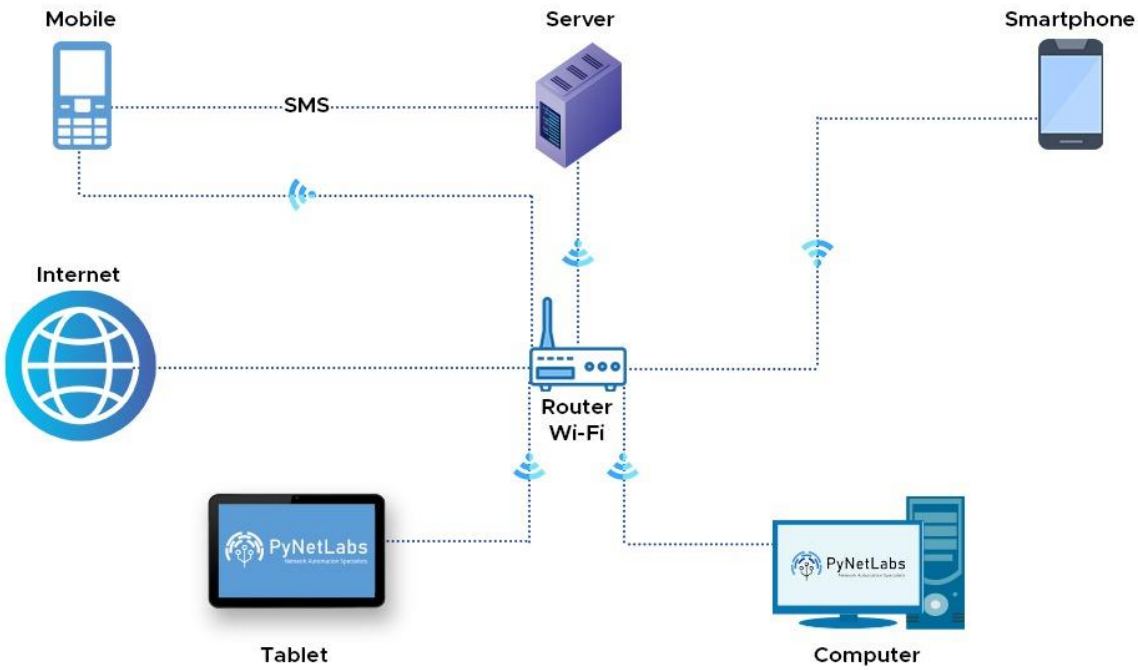

Figure 2. LAN Diagram

+Advantages:

- Reduces unnecessary traffic by limiting communication to machines that need to interact (Burgess, 2004, p. 51).
- Cost-effective compared to WANs because infrastructure remains localised.
- Simplifies administrative responsbility for a defined geographic area.
- Enables efficient resource sharing among nearby devices.

+Disadvantages:

- Limited by physical proximity constraints that cannot be overcome without additional infrastructure.
- Requires careful initial planning of cable routes and connection points.
- Performance can degrade when too many machines share the same cable segment.
- Scalability reaches practical limits beyond approximately 30 computers without segmentation.

b. Wireless LAN (WLAN)

A WLAN functions like a wired LAN but uses radio signals instead of cables, with transmitters and receivers replacing physical connections (Lowe, 2004, p. 10). Computers can be located anywhere within the broadcast range.

+Diagram:

Figure 3. WLAN Diagram

+Advantages:

- Eliminates cable installation requirements, particularly valuable in difficult-to-wire spaces.
- Enables device mobility and flexibility in workspace design.
- Reduce infrastructure installation costs compared to cabled LANs.
- Supports temporary or portable network configurations.

+Disadvantages:

- Inherently less secure than cabled networks because radio signals propagate beyond intended areas (Lowe, 2004, p. 11).
- Signal strength decreases with distance and physical obstacles like walls.
- Performance varies based on environmental interference from other wireless devices.
- Requires stronger security measures to prevent unauthorised network access.

c. WAN (Wide Area Network)

A WAN spans large geographic territories such as entire cities, regions, or countries (Lowe, 2004, p. 14). WANs typically connect two or more LANs that are far apart. Geographic distance, not computer count, defines whether a network is a WAN.

+Diagram:

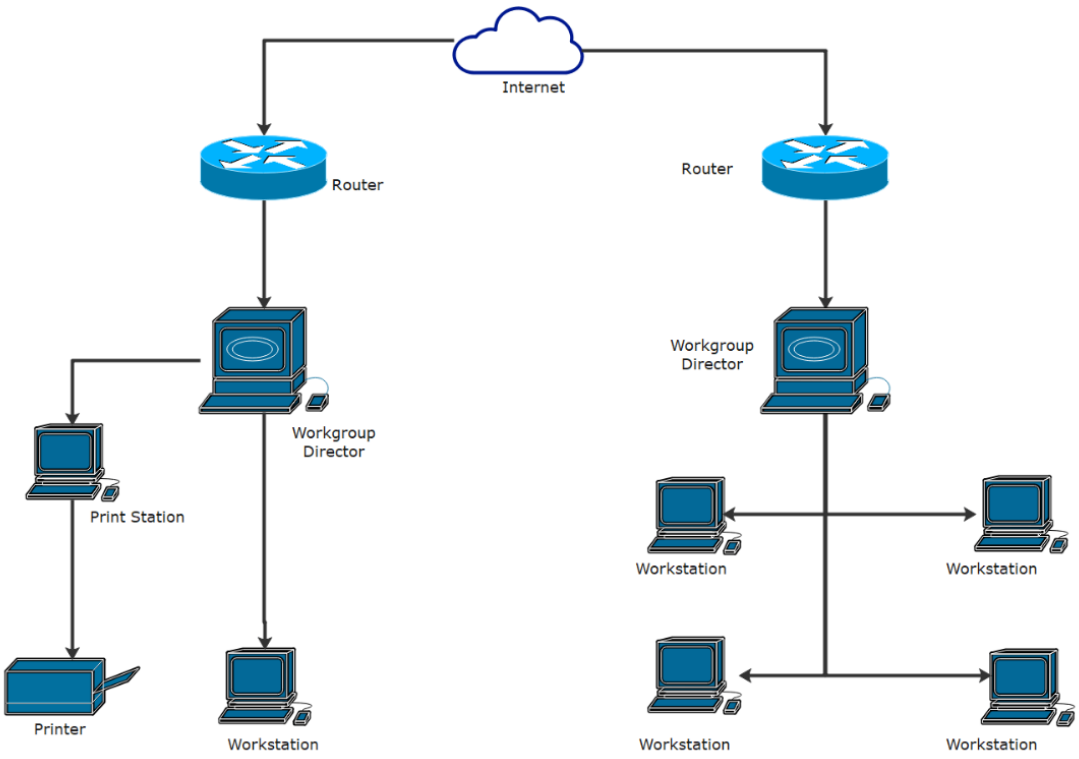

Figure 4. WAN Diagram

+Advantages:

- Eliminates cable installation requirements, particularly valuable in difficult-to-wire spaces.
- Enables device mobility and flexibility in workspace design.
- Reduces infrastructure installation costs compared to cabled LANs.
- Supports temporary or portable network configurations.

+Disadvantages:

- Inherently less secure than cabled networks because radio signals propagate beyond intended areas (Lowe, 2004, p. 11).
- Signal strength decreases with distance and physical obstacles like walls.
- Performance varies based on environmental interference from other wireless devices.
- Requires stronger security measures to prevent unauthorised network access.

3. Networking Standards

Standards are basically industry-wide definitions of how protocols should work, and they're not tied to any single company (Lowe, 2004, p. 21). This is pretty important because before standards existed, each manufacturer would just make their own thing, and then equipment from different companies couldn't work together on the same network. Standards organisations like ANSI, IEEE, ISO, IETF, and W3C set up these definitions.

II - Explain the impact network topologies have on communication and bandwidth requirements

1. Network Topologies

Network topology basically just means the physical shape and arrangement of how computers and network components actually connect to each other (Lowe, 2004, p. 15). Understanding topology matters because it directly changes how well the network works, how reliable it is, and how much it costs. Different topologies are just different ways of solving the same basic problem: how do you connect multiple machines efficiently?

a. Physical Topology vs Logical Topology

Physical topology is basically just the actual physical layout of how the cables and devices are arranged in the real world (Lowe, 2004, p. 15). It's what you'd see if you looked at your network and where the cables actually go, where the switches sit, which computers plug into which ports.

Diagram:

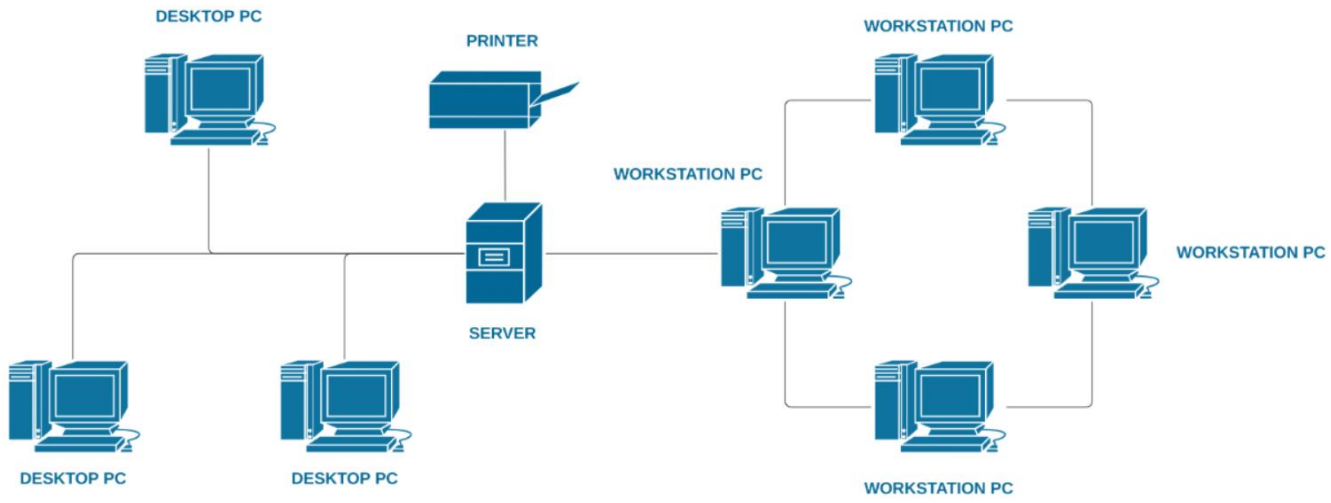

Figure 5. Physical Topology Diagram

On the other hand, logical topology describes how data actually flows between devices, which might be completely different from the physical arrangement (Burgess, 2004, p. 46). So you could have a physical star topology where all cables run to a central hub, but if that hub is a switch that only sends data to specific ports, the logical topology is still star. But if it's an old hub that broadcasts to everything, the logical topology is more like a bus even though physically it looks like a star (Lowe, 2004, p. 16).

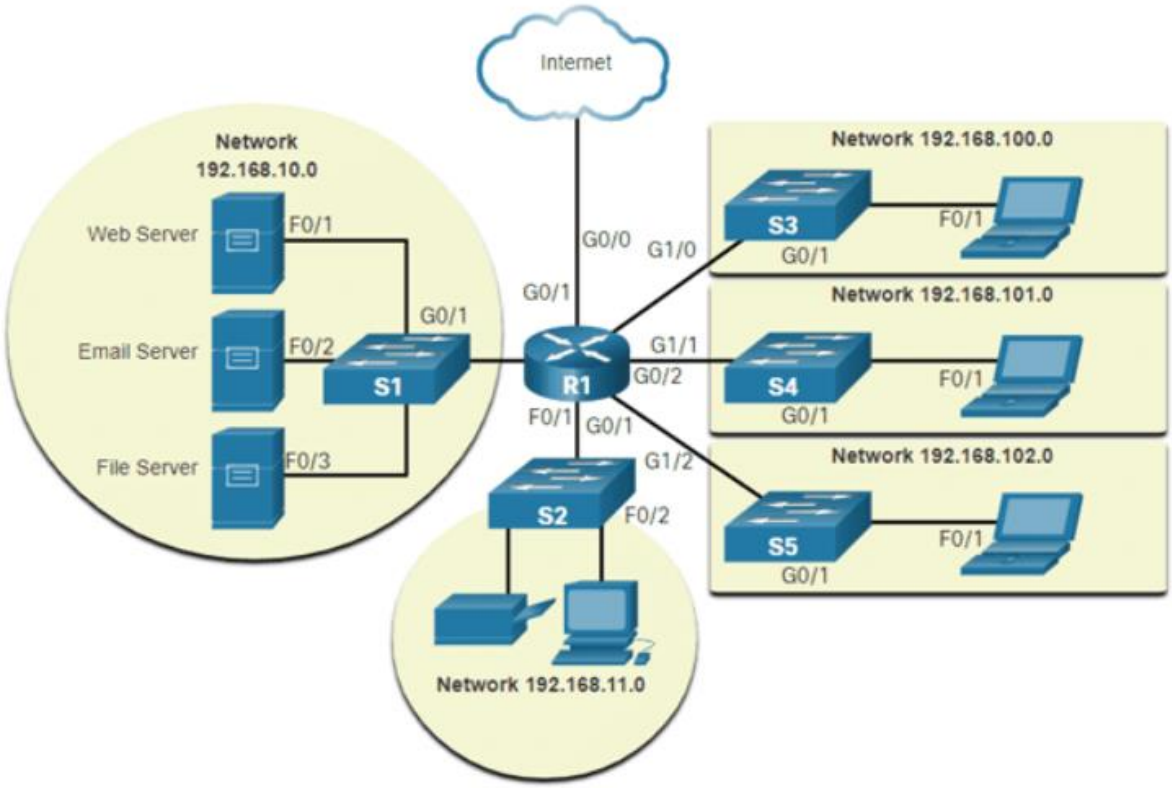

Figure 6. Logical Topology Diagram

This distinction matters because understanding how data actually moves through your network is more important than just knowing what it looks like physically. Two networks could look identical physically but behave completely differently depending on what devices are in the middle.

1.1. LAN Topology:

a. Bus Topology

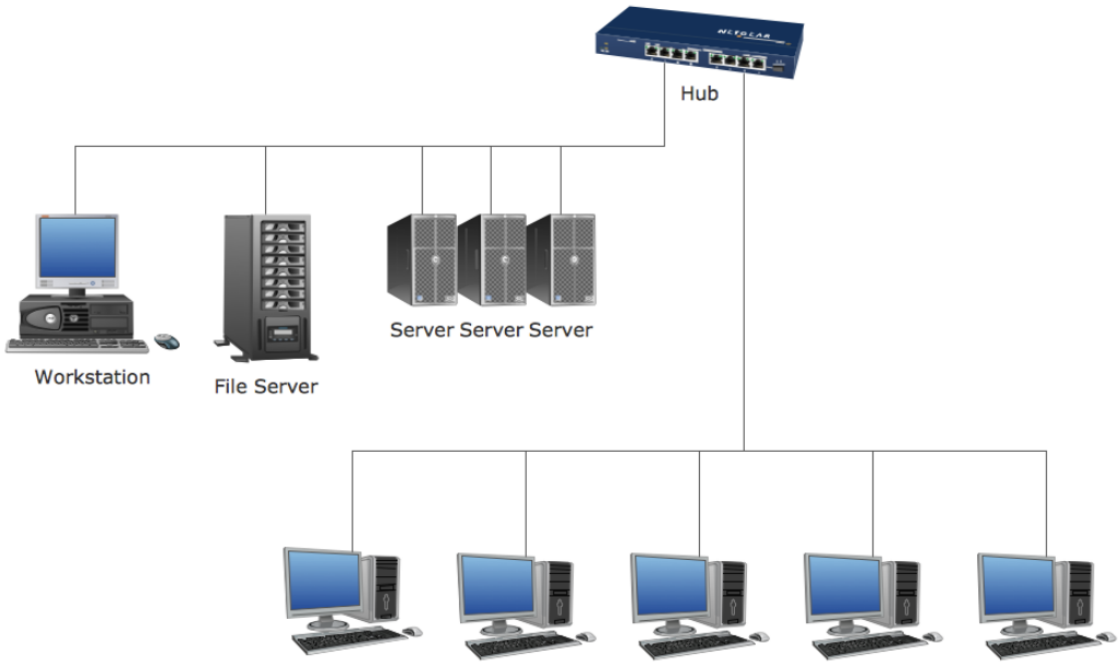

Figure 7. Bus Topology Diagram

Definition: In a bus topology, nodes connect to a single cable with each node basically "tapping into" it (Lowe, 2004, p. 15). Every node sees every packet and has to check each one to see if it's meant for them (Lowe, 2004, p. 15). This approach is simple but has big implications for how well it works and how reliable it is. When a cable breaks, the network splits into two separate sections, so communication can't cross the break (Lowe, 2004, p. 15).

Advantages: Simple to implement; uses less cabling than other topologies; straightforward to understand for small networks.

Disadvantages: Network performance gets worse pretty quickly as more computers try to send data at the same time. After around 30 computers, collisions happen so often that you notice the slowdown. Adding or removing devices causes the network to stop working. If the cable breaks, it cuts the network into separate pieces that can't talk to each other.

b. Star Topology

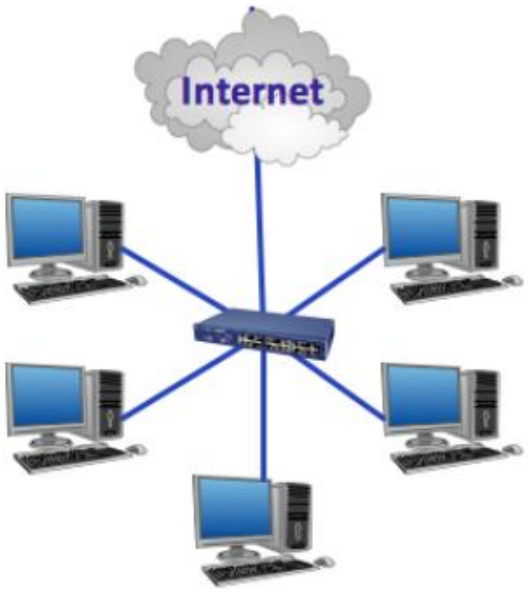

Figure 8. Star Topology Diagram

Definition: Each network node connects to a central device called a hub or switch (Lowe, 2004, p. 16). A hub just broadcasts packets to all ports without really knowing which computer is on which port, while a switch actually knows which computer connects to each port and forwards packets only to the right place (Lowe, 2004, p. 16). If a cable breaks, only that one node gets disconnected, assuming the central device is still working (Lowe, 2004, p. 16).

Advantages: If one cable fails, just that node gets isolated; easy to add or remove nodes; you have a central point to manage; troubleshooting individual connections is straightforward.

Disadvantages: If the central device fails, the entire network goes down; requires more cabling than bus topology; the central device is kind of a weak point that everything depends on.

c. Ring Topology

Figure 9. Ring Topology Diagram

Definition: Packets travel around the circle from computer to computer, and each one checks the packets to figure out if they were meant for them (Lowe, 2004, p. 17). This approach is really different from bus topology because it doesn't rely on computers competing to send data.

Advantages: No random collisions happening; you can use bigger packet sizes; performance is predictable.

Disadvantages: If one computer fails, the whole ring breaks and communication stops; adding or removing computers means you have to stop the network; growing a ring network requires careful planning; ring topologies basically don't exist in modern networks anymore (Lowe, 2004, p. 18).

d. Tree Topology

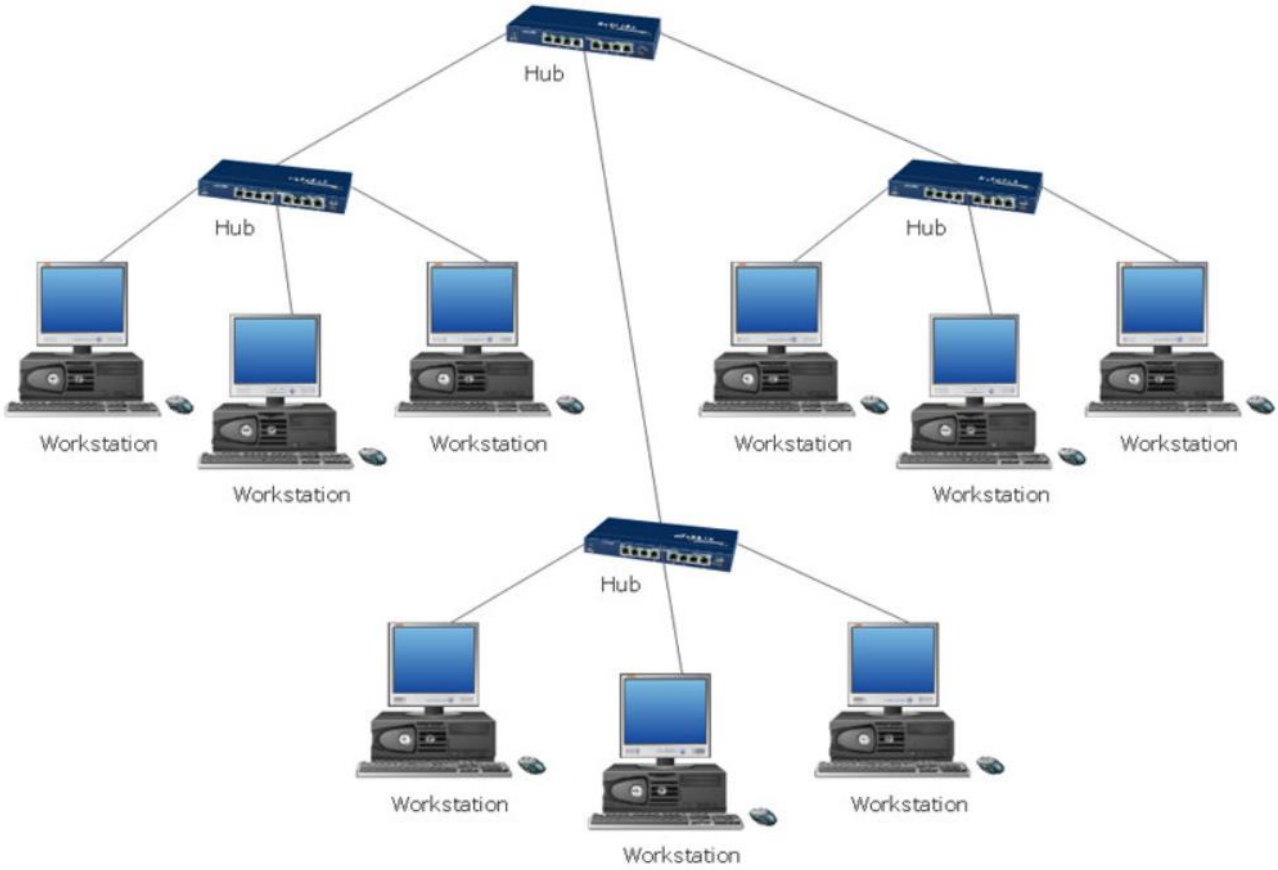

Figure 10. Tree Topology Diagram

Definition: Tree topologies basically combine parts of star and bus topologies, with a main backbone and devices arranged hierarchically in different branches (Lowe, 2004, p. 17). Routers sit at the junction points and control traffic flow between the different branches.

Advantages: Supports large networks spread out in different areas; lets you split things into different administrative zones; you can prioritise traffic between different branches.

Disadvantages: Pretty complicated to design and maintain; if the backbone fails, multiple branches stop working; expensive to set up; requires special tools to manage it properly.

1.2. WAN Topology:

a. Point-to-Point

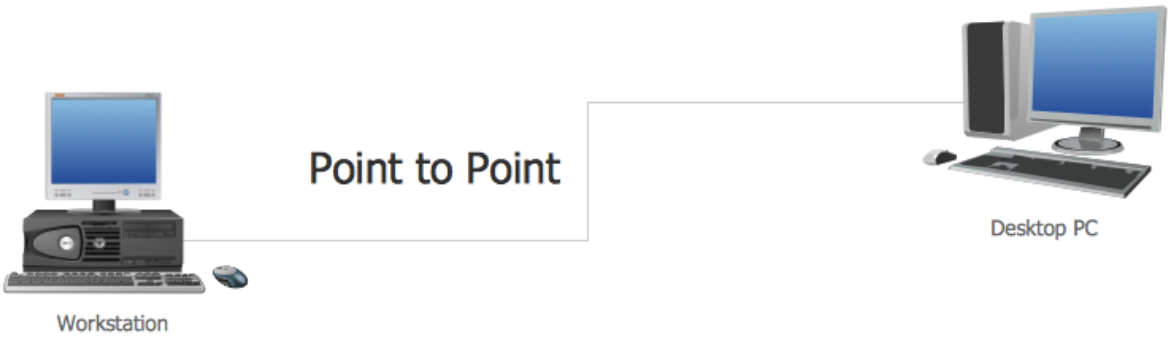

Figure 11. Point-To-Point Topology Diagram

Definition: A direct dedicated connection just links two network sites with all traffic going over that single link.

Advantages: Simple to set up; performance is predictable; you get dedicated bandwidth; routing is straightforward because there's basically only one path.

Disadvantages: Expensive for each connection you add; doesn't scale well for many locations; wasteful if traffic patterns are unbalanced; if the link fails, there's no backup.

b. Star (Hub-and-Spoke)

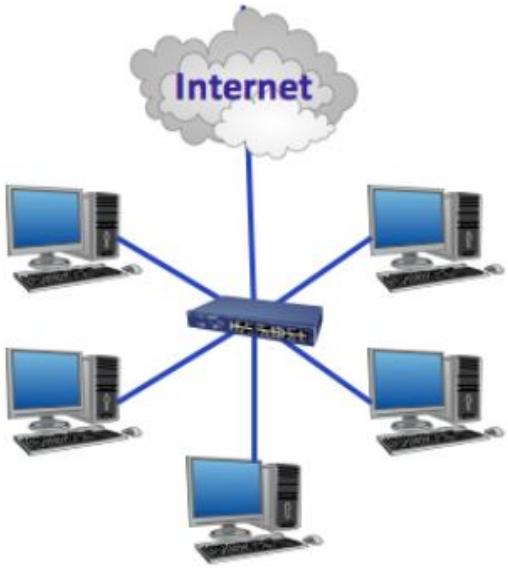

Figure 12. Star Topology Diagram

Definition: A central site (hub) connects to multiple remote locations (spokes), and if branch offices want to talk to each other, traffic has to go through the central location.

Advantages: You can manage everything from headquarters; troubleshooting is straightforward; simple topology that's easy to understand and document.

Disadvantages: The central link becomes a bottleneck limiting all inter-branch communication; if the central site fails, all branches get disconnected; how much you can grow is limited by the central link's capacity.

c. Mesh Topology

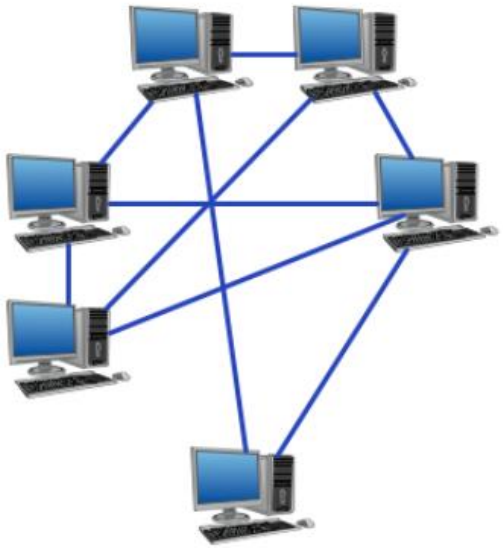

Figure 13. Mesh Topology Diagram

Definition: Mesh networks have multiple connections between nodes, so packets can take a different route if one connection fails (Lowe, 2004, p. 18). In full mesh, every computer connects to every other one; in partial mesh, only the important computers have backup connections.

Advantages: Lots of redundancy with multiple paths between nodes; no single point of failure; traffic can automatically reroute around problems.

Disadvantages: Extremely expensive because each computer needs many network cards and you need cables connecting to lots of computers; managing and configuring it is complicated; doesn't work well for LANs (Lowe, 2004, p. 18).

2. Communication Concepts

Computers communicate by transmitting electrical or optical signals over wires or fibres (Burgess, 2004, p. 46). Each node on the same cable segment perceives all signals passing through it (Burgess, 2004, p. 392). However, messages incorporate MAC addresses, and typically only the host with the matching address processes the message (Burgess, 2004, p. 392). A host listening to all traffic operates in promiscuous mode (Burgess, 2004, p. 392).

3. Bandwidth Requirements

Cable technologies have inherent limitations. Only one host can transmit at any instant on shared media (Burgess, 2004, p. 393). A single contiguous Ethernet segment can span at most 5,000 metres with a minimum packet size of 64 bytes before collision rates cause network performance to collapse (Burgess, 2004, p. 393). As networks grow, broadcast messages create traffic that slows busy networks.

III - Assess common networking principles and how protocols enable the effectiveness of networked systems

1. OSI Model

The OSI (Open Systems Interconnection) model breaks network operations into seven distinct layers (Lowe, 2004, p. 22). The model functions as a framework rather than a strict standard (Lowe, 2004, p. 22). While actual networking protocols don't follow the OSI model perfectly, it provides a useful conceptual picture of how networking works (Lowe, 2004, p. 22).

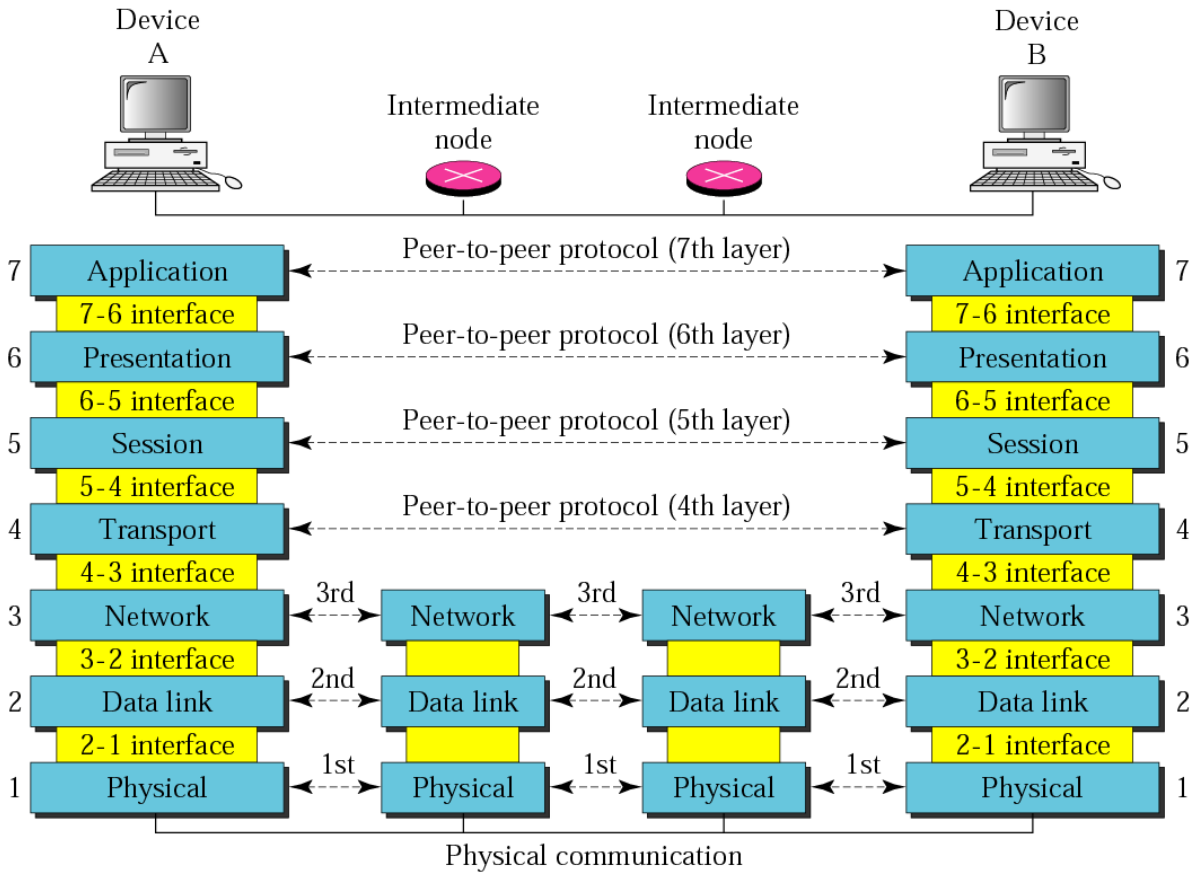

Figure 14. OSI Model Diagram

Layer 1 (Physical) governs the layout of cables and devices such as repeaters and hubs (Lowe, 2004, p. 23). Layer 2 (Data Link) provides MAC addresses to uniquely identify network nodes and enables data transmission as packets (Lowe, 2004, p. 24). Layer 3 (Network) handles routing of data across network segments (Lowe, 2004, p. 26). Layer 4 (Transport) provides reliable packet delivery (Lowe, 2004, p. 28). Layer 5 (Session) establishes sessions between network applications (Lowe, 2004, p. 29). Layer 6 (Presentation) converts data so systems using different formats can exchange information (Lowe, 2004, p. 30). Layer 7 (Application) allows applications to request network services (Lowe, 2004, p. 30).

2. TCP/IP Model

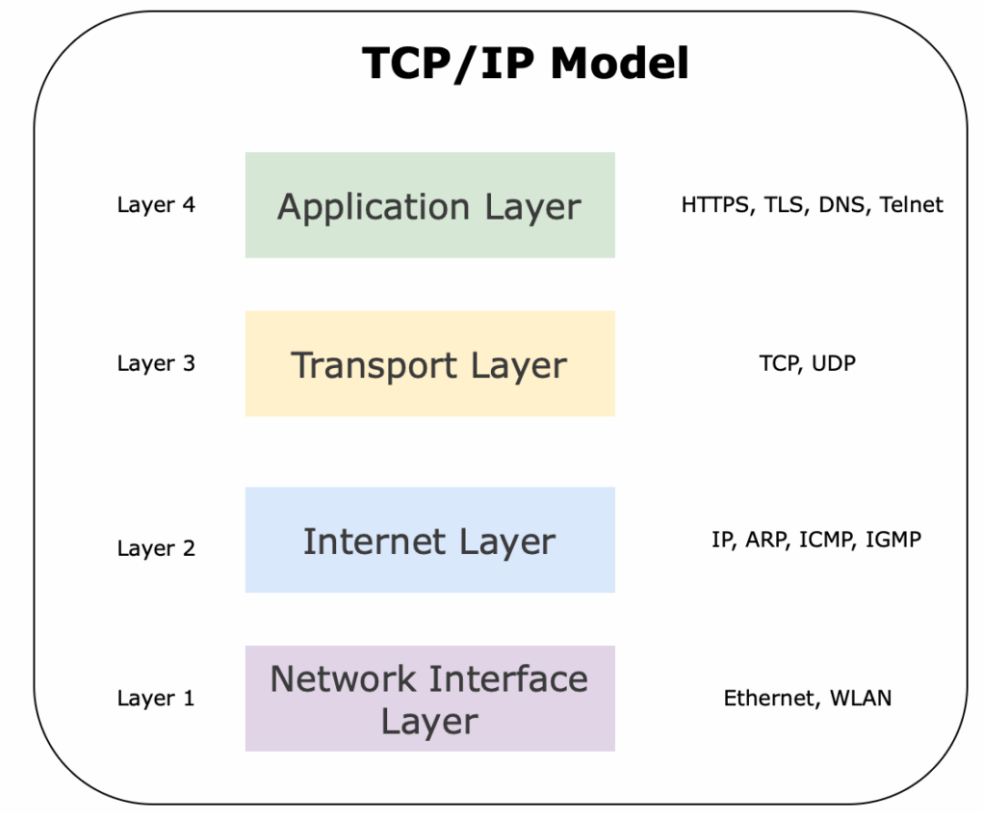

Figure 15. TCP/IP Model Diagram

TCP/IP is actually an entire suite of related protocols, not a single protocol (Lowe, 2004, p. 35). The TCP/IP suite operates on a four-layer model similar to the OSI model. The Network Interface layer corresponds to the OSI Physical and Data Link layers and can run over various protocols including Ethernet, Token Ring, and FDDI (Lowe, 2004, p. 35). The Application layer corresponds to the OSI Session, Presentation, and Application layers, including protocols like HTTP, FTP, Telnet, SMTP, DNS, and SNMP (Lowe, 2004, p. 35).

3. Comparison: OSI vs TCP/IP

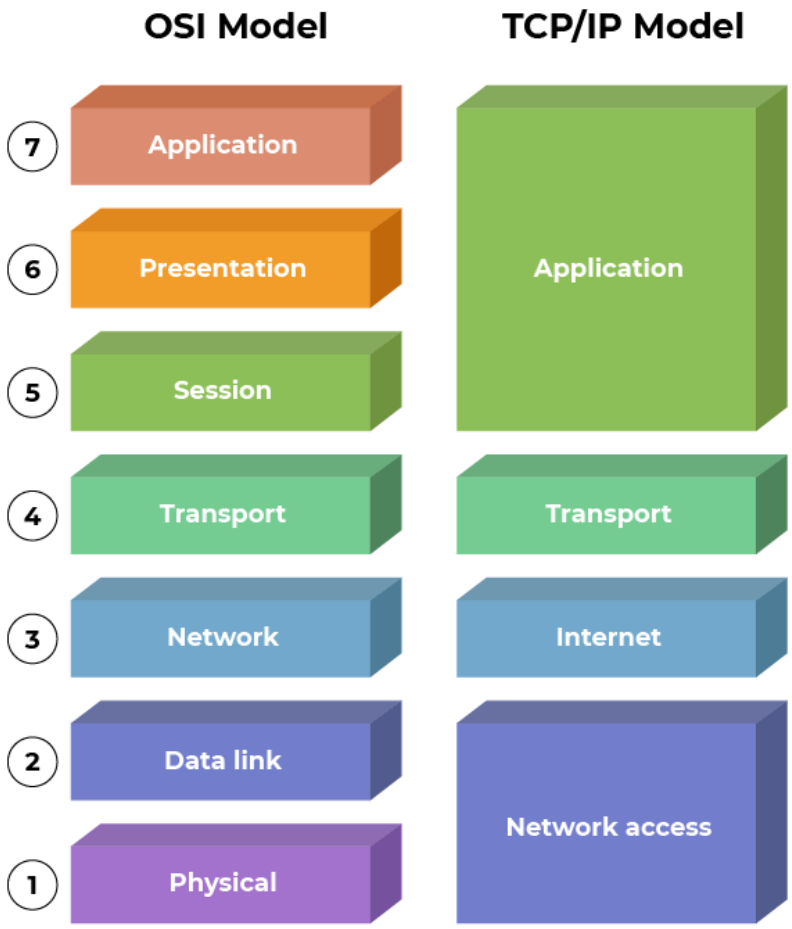

Figure 16. OSI vs TCP/IP Diagram for comparison

The OSI model provides a seven-layer theoretical framework for understanding networking (Lowe, 2004, p. 22), while the TCP/IP model describes how the actual Internet functions (Lowe, 2004, p. 35). In real-world networks, Layer 2 typically corresponds to Ethernet or equivalent technologies, while Layer 3 corresponds to the IP-addressable transport layer. The OSI model is better for learning and conceptualising networking (Lowe, 2004, p. 22), while TCP/IP better explains actual implementations.

a. Key Protocols

IPv4 (Internet Protocol)
Every network interface needs a unique number called an address (Burgess, 2004, p. 55). IP addresses organise hierarchically, enabling router networks to search for hosts efficiently (Burgess, 2004, p. 55). Without such structure, finding hosts outside immediate cable segments would be impossible (Burgess, 2004, p. 55).

IPv4 addresses consist of four bytes (32 bits) (Lowe, 2004, p. 270). The address structure trades between network and host portions: using all 32 bits for hosts prevents routing; using all for networks allows one host per network (Burgess, 2004, p. 55).

Diagram:

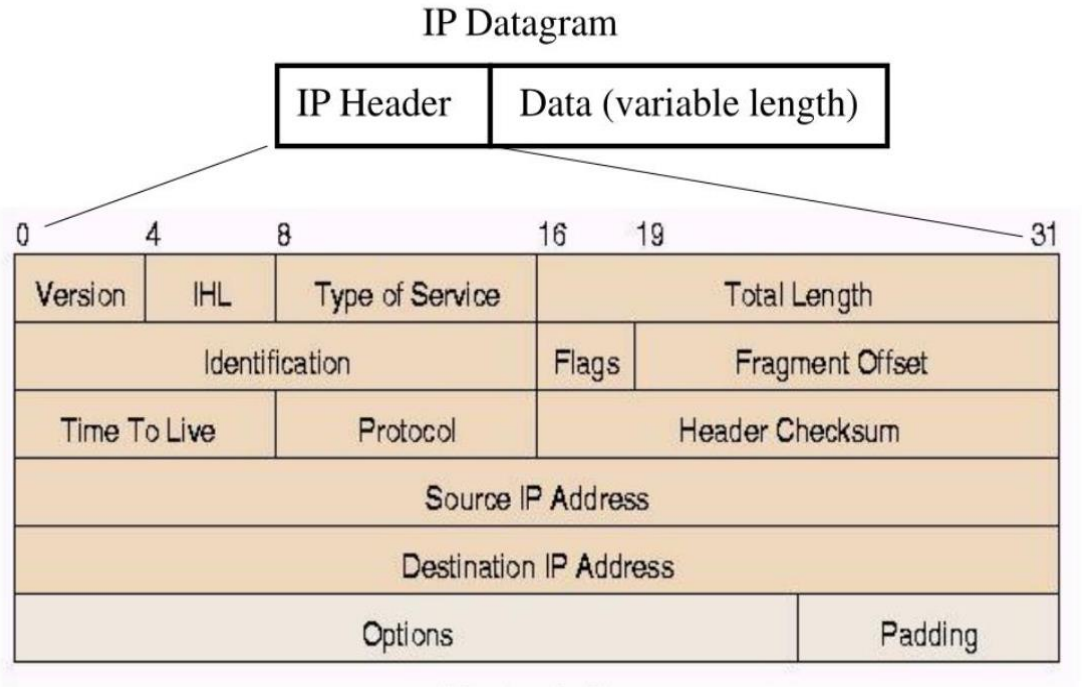

Figure 17. IPv4 Diagram

IPv4 historically divided into classes (Lowe, 2004, p. 272). Class A networks dedicate the first byte to network identification, allowing 126 networks with enormous host counts (Burgess, 2004, p. 56). Class B networks dedicate the first two bytes, providing 16,384 networks with 65,534 hosts each (Burgess, 2004, p. 56). Class C networks dedicate three bytes, creating 2,097,152 networks with 254 hosts each (Burgess, 2004, p. 57). Class D addresses support multicast (one-to-many transmission) (Burgess, 2004, p. 57), while Class E addresses remain experimental (Burgess, 2004, p. 57).

TCP vs UDP

TCP (Transmission Control Protocol) is a connection-oriented Transport layer protocol enabling devices to reliably send packets to other devices on the same or different networks (Lowe, 2004, p. 37). TCP establishes connections, ensures all packets arrive intact in correct order, and resends lost packets (Lowe, 2004, p. 37). Connection closes only after successful delivery or unrecoverable error (Lowe, 2004, p. 37). TCP enables one-to-one communications and is used by HTTP, Telnet, FTP, and SMTP (Lowe, 2004, p. 37).

UDP (User Datagram Protocol) is a connectionless Transport layer protocol used when connection overhead isn't required (Lowe, 2004, p. 37). After UDP places a packet on the network, it forgets about it. UDP doesn't guarantee packet arrival (Lowe, 2004, p. 37). Applications using UDP wait for expected

replies; if replies don't arrive within certain periods, applications resend or give up (Lowe, 2004, p. 37). DNS is the best-known UDP protocol (Lowe, 2004, p. 37).

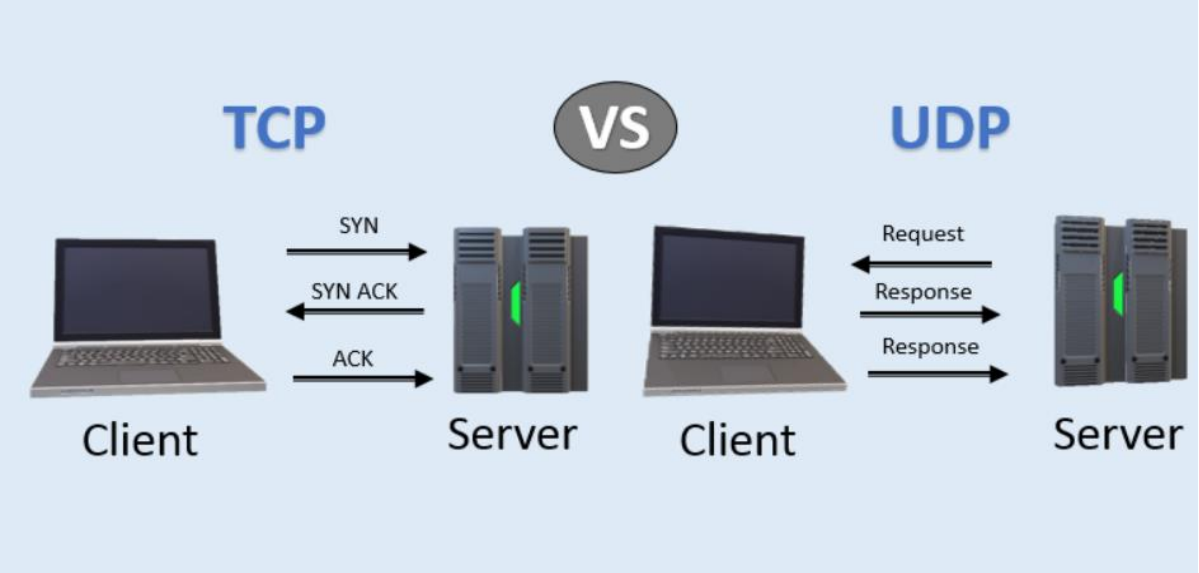

Figure 18. TCP vs UDP Comparison Diagram

HTTP (HyperText Transfer Protocol)

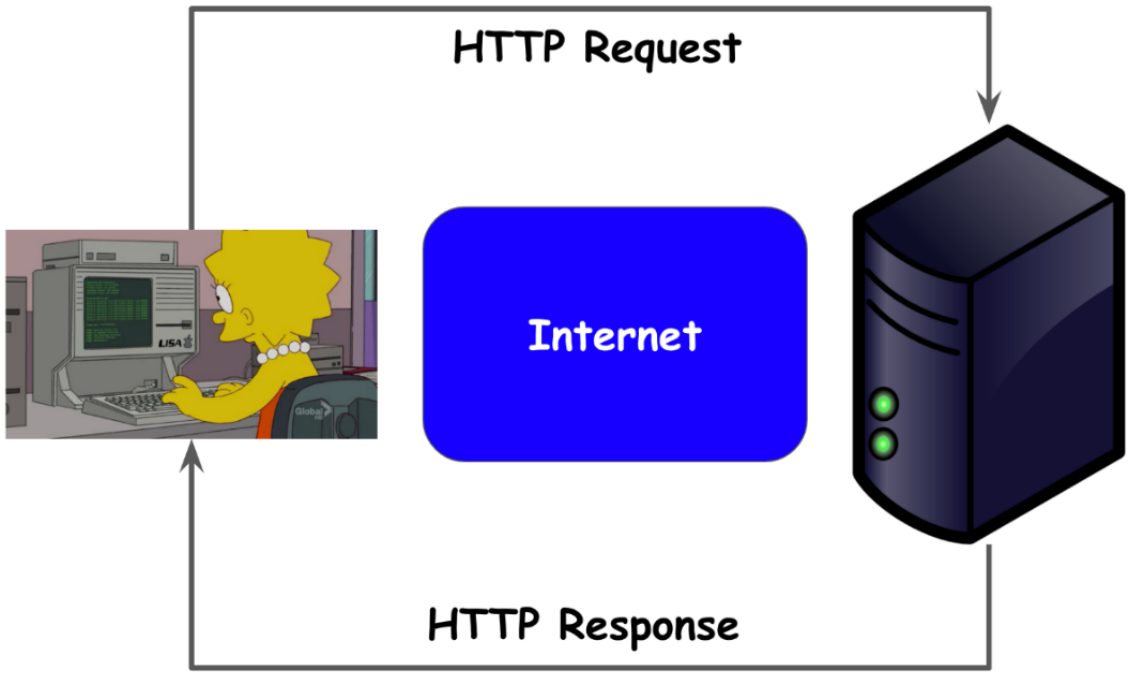

Figure 19. HTTP Diagram

HTTP is the Application layer protocol enabling web communication between browsers and web servers (Lowe, 2004, p. 30). When users request pages, browsers send HTTP requests via TCP to web servers,

which respond with page content including HTML, images, and other files, again via TCP (Lowe, 2004, p. 30). HTTP operates on top of TCP's reliable delivery (Lowe, 2004, p. 30).

a. How Protocols Enable Network Effectiveness:

Protocols are sets of rules enabling effective communications (Lowe, 2004, p. 19). Protocols wrap data in envelope information containing destination addresses, with each transmission layer prefixing header information (Burgess, 2004, p. 53). This encapsulation is essential for network security and administration understanding (Burgess, 2004, p. 53).

IV - Discuss the operating principles of networking devices and server types.

Network devices and servers form the infrastructure that enables communication and resource sharing across networks. Understanding how these components operate is essential for designing, implementing, and maintaining effective network systems.

1. Network Devices

1.1. Network Interface Card (NIC)

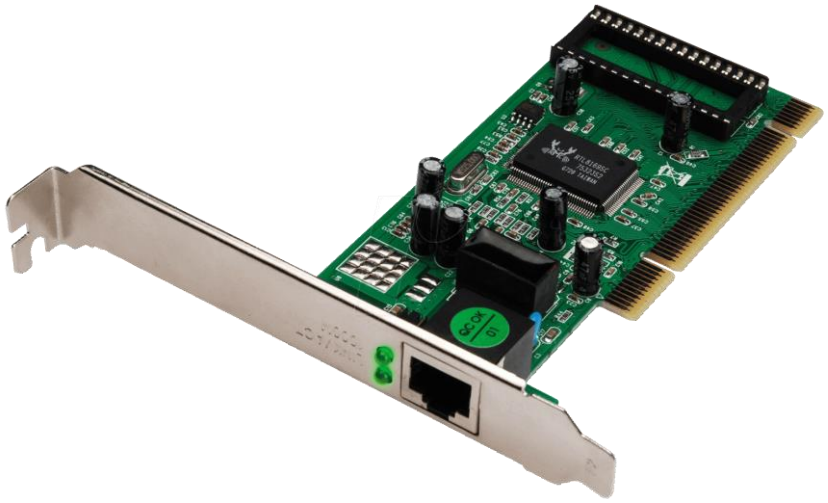

Figure 20. NIC Picture

A NIC is basically the component that lets any computer connect to a network. It's either a separate card you slot into the motherboard or it's already built into the motherboard itself. For regular computers that just one person uses, the cheap built-in NICs work fine. But for servers that have to handle lots of people connecting at once, you really need to invest in better quality cards from companies like Intel, SMC, or 3Com (Lowe, 2004, p. 46).

a. Hub

Figure 21. Hub Picture

Think of a hub as the central meeting point for a network using twisted-pair cables. It lets multiple computers connect together in what's called a star topology. Hubs used to be really expensive, which is why people avoided them and used cheaper coaxial cable instead. But nowadays they're so affordable that the advantages of using twisted-pair cable and hubs completely outweigh any cost concerns. With hubs, you can easily add new computers, move things around, troubleshoot cable problems, and temporarily disconnect computers when you need to service them (Lowe, 2004, p. 50).

b. Switch

Figure 22. Switch Picture

A switch is basically a smarter version of a hub, and because their prices have dropped so much, most new networks use switches instead of hubs. The big difference is that switches can actually look inside the data packets and read the MAC addresses. This means a switch can remember which computer is plugged into which port (Lowe, 2004, p. 52).

c. Repeater

Figure 23. Repeater Picture

Repeaters are devices that boost network signals so they can travel farther. You need them when your cable is longer than the maximum allowed distance, which is about 185 meters for coaxial cable or 100 meters for twisted-pair cable. The repeater basically sits in the middle and divides the cable into two separate segments (Lowe, 2004, pp. 52-53).

d. Bridge

Figure 24. Bridge Picture

A bridge connects two networks so they can act like one network, and it's smarter than a repeater. While repeaters just blindly amplify everything they hear, bridges actually listen to the network and figure out

which computers are on each side. Then they only forward messages across when necessary, specifically when a computer on one side needs to talk to a computer on the other side (Lowe, 2004, pp. 54-55).

e. Router

Figure 25. Router Picture

Routers are like bridges but operate at a higher level of intelligence. While bridges work with MAC addresses at the Data Link layer, routers work with IP addresses at the Network layer. This means routers can actually peek into the message content and see what network the message is coming from and going to (Lowe, 2004, p. 55).

2. Server Types

Servers are specialized computers or processes that provide services to other computers on the network. The client-server model represents an efficient centralization of resources based on the principle that specialists should handle specialized tasks rather than expecting everyone to do everything themselves (Burgess, 2004, p. 78).

a. File Server

File servers provide disk storage that network users can access as if it were part of their own computer's disk space. This is probably the most common reason servers exist on networks. As networks grow and users need more storage, administrators constantly look for ways to add capacity (Lowe, 2004, pp. 41, 57).

b. Print Server

Print servers manage network printers and handle print jobs from multiple users. When several people send documents to the same printer, the print server stores the jobs in a queue and prints them in the order they were received. Although you can connect printers directly to the network, having a server manage them is still a good idea because it handles the queuing and ensures fair access (Lowe, 2004, pp. 58, 84).

c. Web Server

Web servers host websites and handle HTTP requests from browsers. When users request web pages, browsers send HTTP requests via TCP to web servers, which respond with page content including HTML, images, and other files. The web server operates on top of TCP's reliable delivery, ensuring that web pages arrive intact (Lowe, 2004, pp. 30, 84).

d. Mail Server

Mail servers handle sending, receiving, and storing email messages for network users. They use protocols like SMTP for sending mail and POP3 or IMAP for receiving and storing mail. Mail servers need to be at well-known, static network locations so other servers can reliably deliver messages to them (Lowe, 2004, p. 84; Burgess, 2004, p. 81).

e. DNS Server

DNS (Domain Name Service) servers translate human-readable domain names into IP addresses that computers actually use for communication. DNS is the only worldwide naming service in common use and it associates IP addresses with lists of names. Every host in DNS has a canonical or official name and any number of aliases. For example, a host running several services might have the official name "mother.domain.country" with aliases like "www.domain.country" and "ftp.domain.country" (Burgess, 2004, pp. 80-82).

f. DHCP Server

DHCP (Dynamic Host Configuration Protocol) servers automatically assign IP addresses to computers when they connect to the network. Instead of manually configuring each computer with a static IP address, DHCP servers maintain pools of available addresses and hand them out as needed. This is particularly useful for networks with many computers or devices that connect temporarily (Lowe, 2004, p. 84; Burgess, 2004, p. 81).

V - Discuss the interdependence of workstation hardware and relevant networking software

1. Workstation Hardware

a. Central Processing Unit (CPU)

The CPU is essentially the brain of the computer (Lowe, 2004, p. 43). It's the component that actually executes instructions and performs calculations. While people often think of the CPU first when deciding what type of computer to purchase, it's not the only factor affecting overall system performance (Lowe, 2004, p. 43). CPUs are characterized by their clock speed, which refers to how fast the basic clock driving the processor's operation ticks (Lowe, 2004, p. 43). In theory, faster clock speed means faster processing, but clock speed alone is only reliable for comparing processors within the same family. Different processor architectures can accomplish more work per clock cycle, making a processor with a lower clock speed potentially faster than one with a higher clock speed if it has more advanced circuitry (Lowe, 2004, p. 43).

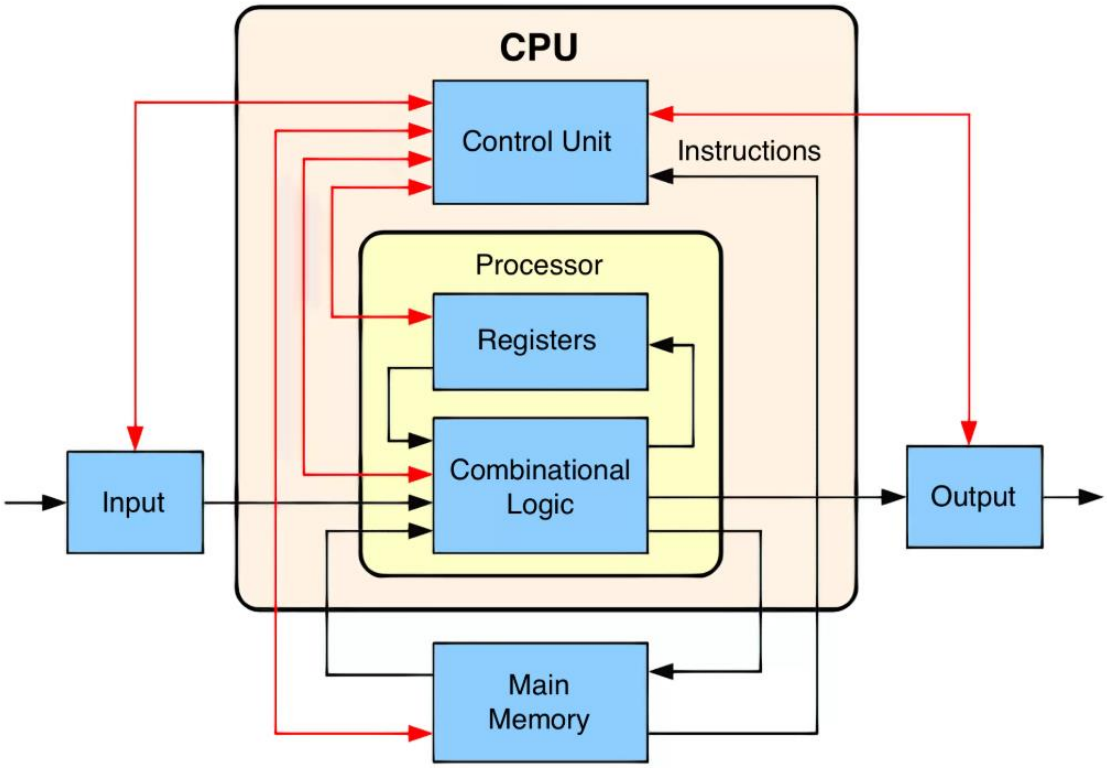

Figure 26. Central Processing Unit Diagram

b. Random Access Memory (RAM)

RAM is the computer's working memory where data and programs are temporarily stored while the computer is running. Modern CMOS chips that make up RAM work at low voltages, typically 5 volts or

lower, making them quite fragile (Burgess, 2004, p. 14). Memory is critical for system performance, and people rarely complain about servers having too much memory (Lowe, 2004, p. 43).

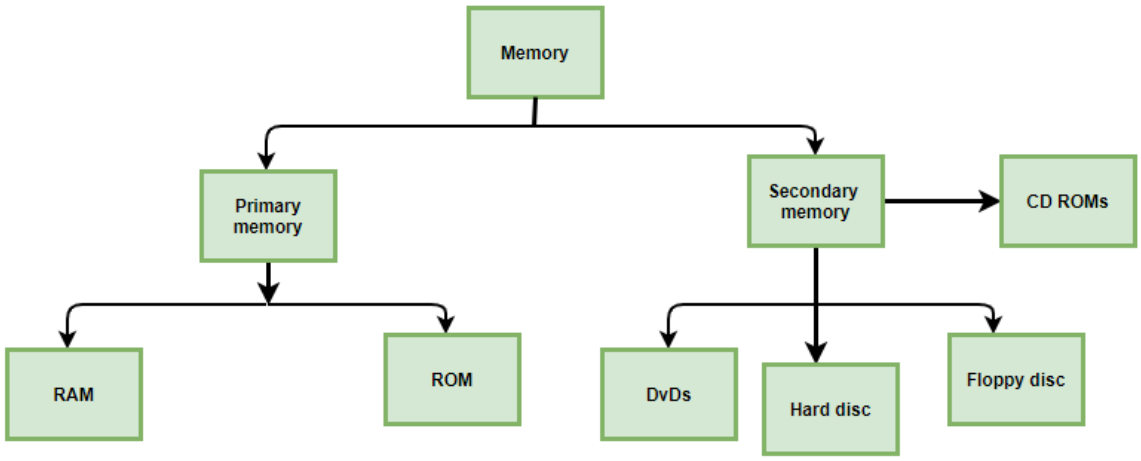

Figure 27. Random Access Memory Diagram

c. Read-Only Memory (ROM)

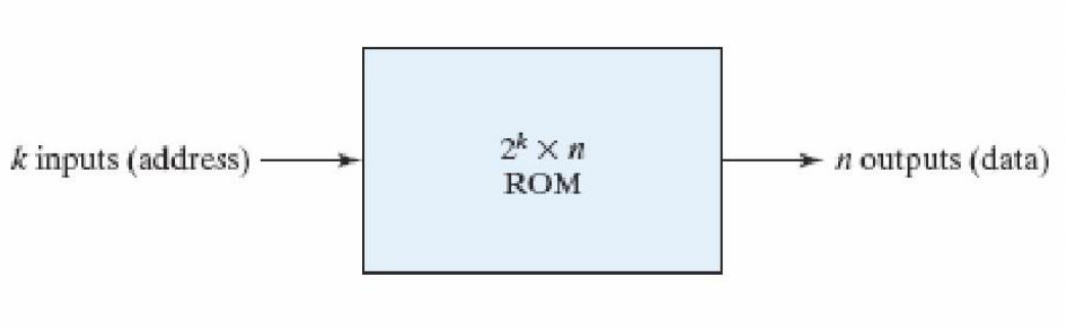

Figure 28 Read-Only Memory Diagram

ROM contains permanent instructions that don't disappear when the computer is turned off. The most important ROM in a computer is the BIOS (Basic Input/Output System), which contains the fundamental instructions needed to start the computer and perform basic operations. Early operating systems like MS-DOS and Windows 3.x built on this ROM-based library of basic input-output functions that could write to the screen, disk, and other devices (Burgess, 2004, p. 17). When you turn on a computer, the BIOS instructions in ROM execute first, initializing hardware and loading the operating system from disk into RAM.

d. Hard Disk Drive (HDD) / Solid State Drive (SSD)

Storage drives hold all the computer's data and programs permanently, even when the power is off. Most desktop computers use inexpensive drives called IDE drives (sometimes also called ATA), which are

adequate for individual users (Lowe, 2004, p. 44). However, because performance is more important for servers, another type of drive known as SCSI is usually used instead. For the best performance, SCSI drives should be used along with a high-performance SCSI controller card (Lowe, 2004, p. 44).

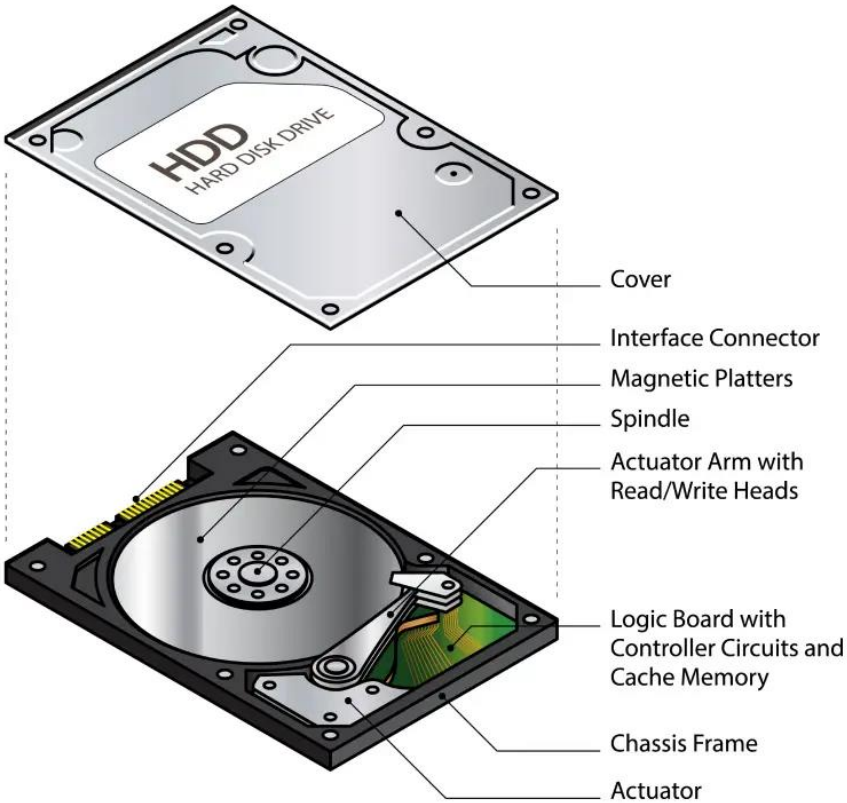

Figure 29. HDD Diagram

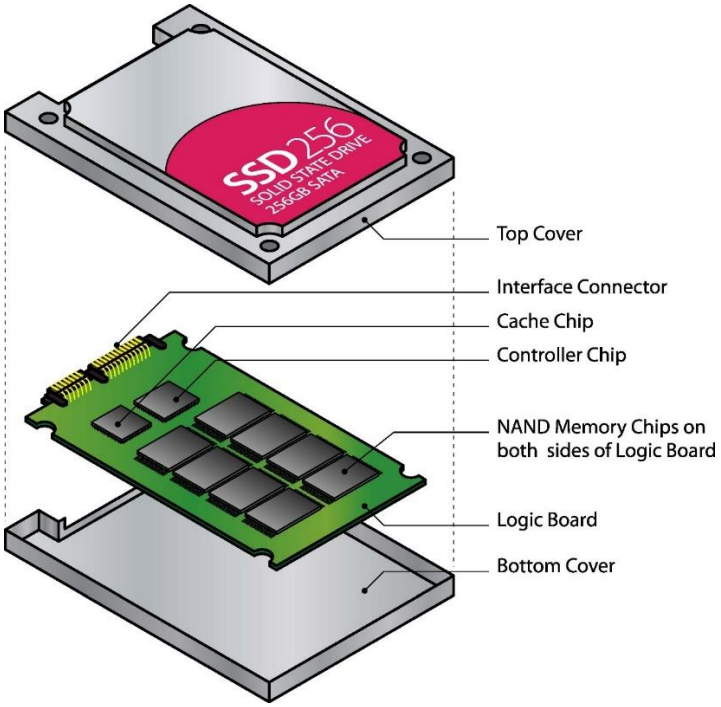

Figure 30. SSD Diagram

Disk technology has been improving steadily for decades. The most common disk types in the workplace fall into two families: ATA (formerly IDE) and SCSI (Burgess, 2004, p. 14). ATA disks are now generally cheaper than SCSI disks due to volume sales and excel at sequential access, but SCSI disks have traditionally been more efficient at handling multiple accesses due to a multitasking bus design, making them better in multitasking systems where random access is important (Burgess, 2004, p. 14). However, filesystem design also plays an important role in determining the perceived performance of each type.

e. Motherboard

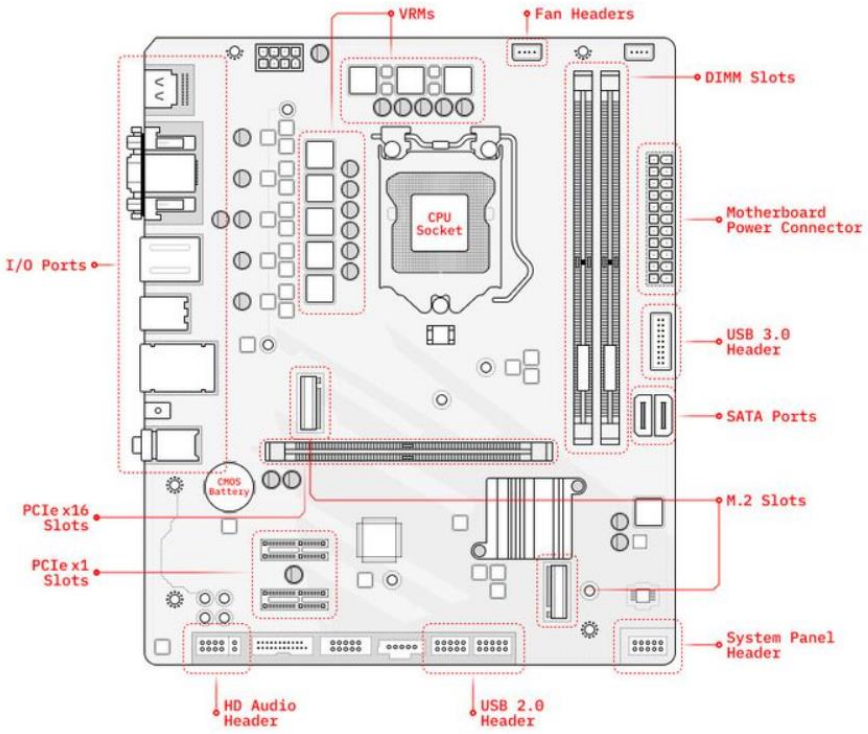

Figure 31. Motherboard Diagram

The motherboard is the computer's main electronic circuit board to which all other components connect (Lowe, 2004, p. 42). More than any other component, the motherboard essentially is the computer, all other components attach to it (Lowe, 2004, p. 43). The major components on the motherboard include the processor or CPU, supporting circuitry called the chipset, memory, expansion slots, a standard IDE hard drive controller, and I/O ports for devices such as keyboards, mice, and printers (Lowe, 2004, p. 43). Some motherboards also include additional built-in features such as a graphic adapter, SCSI disk controller, or a network interface (Lowe, 2004, p. 43).

f. Input/Output Devices

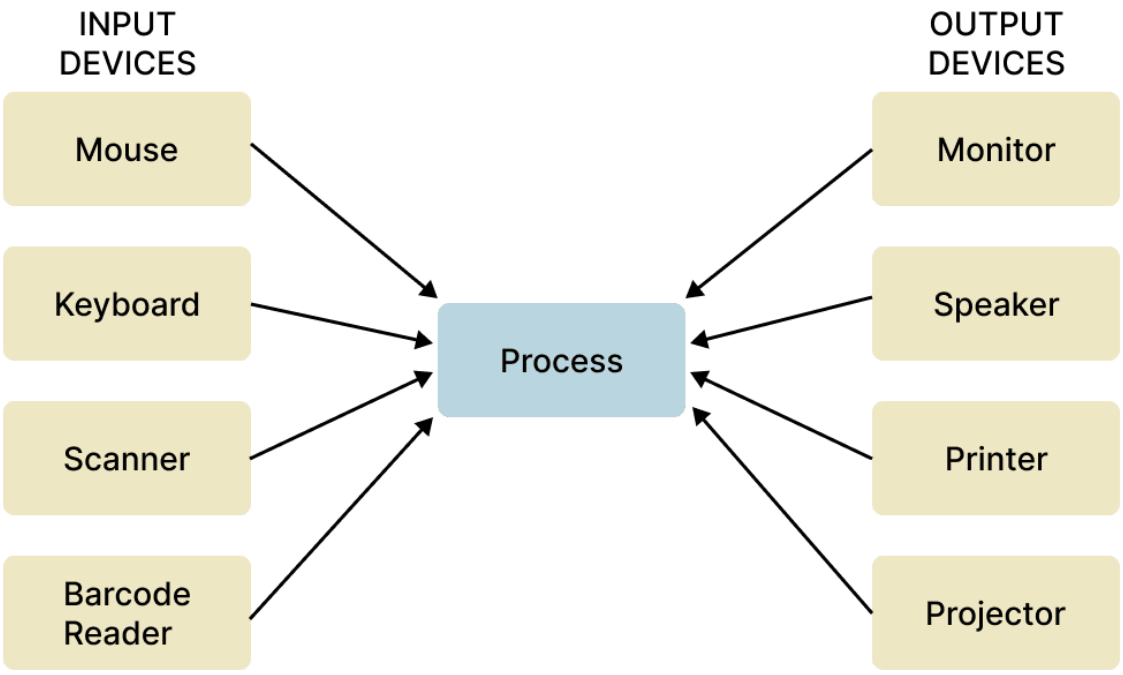

Figure 32. Input/Output Devices Diagram

Input devices like keyboards and mice allow users to interact with the computer, while output devices like monitors and printers display information. These devices connect to the motherboard through various ports and interfaces. The operating system includes a technical layer of software for driving the hardware of the computer, including disk drives, the keyboard, and the screen (Burgess, 2004, p. 16). This layer provides the crucial bridge between physical hardware devices and the software that uses them.

2. Networking Software

a. Definition and Core Functions

Networking software encompasses all the programs and protocols that enable computers to communicate and share resources over a network. An operating system has several key elements: a technical layer of software for driving hardware, a filesystem that provides a way of organizing files logically, and a simple user interface that enables users to run programs and manipulate files (Burgess, 2004, p. 16).

b. Security and Privilege Management

For an operating system to be managed consistently, it must be possible to prevent its destruction by restricting the privileges of its users (Burgess, 2004, p. 16). Different operating systems vary in their provisions for restricting privilege. In operating systems where any user can change any file, there is little

or no possibility of gaining true control over the system, any accident or whim on the part of a user can make uncontrollable changes (Burgess, 2004, p. 16).

c. Hardware and Software Working Together

The relationship between hardware and software in networked systems is one of complete interdependence. Hardware provides the physical capabilities, but without software, it's just inert circuitry. Software provides the intelligence and instructions, but without hardware, it has nothing to execute on.

VI - Explore a range of server types and justify the selection of a server for a given scenario, regarding cost and performance optimisation.

The educational institute scenario presents a moderately-sized network environment requiring careful consideration of server types to balance cost constraints with performance needs. With 235 total users (200 students, 15 teachers, 12 marketing and administration staff, 5 higher managers, and 3 network administrators) spread across three floors, the network requires multiple server types to function efficiently.

1. Analysis of Network Requirements

Before selecting servers, it's essential to understand what the network needs to accomplish. The institute has 50 student lab computers, 35 staff computers, and 3 printers distributed across three floors, with IT labs on the first and second floors while most other equipment resides on the ground floor (Scenario specification). This physical distribution creates specific challenges for network design and server placement.

2. Server Consolidation Strategy

Given budget constraints common in educational institutions, strategic server consolidation makes sense:

Chosen Option: Three-Server Configuration

Server 1 - Core Services Server

- Services: DHCP, DNS, and Authentication/Domain Controller
- Specifications: Mid-range server with 8-16GB RAM, dual network interfaces, reliable components
- Reasoning: These services are critical but not resource-intensive when combined. Authentication requires reliability, so quality hardware is justified.

Server 2 - File Server (Dedicated)

- Services: File storage only

- Specifications: High-end server with 16-32GB RAM, SCSI/SAS RAID storage arrays, multiple gigabit network interfaces
- Reasoning: File service is the most resource-intensive application with 235 users. This server needs dedicated resources for optimal performance.

Server 3 - Application Server

- Services: Print server, web server, and any additional applications
- Specifications: Mid-to-high-range server with 12-16GB RAM, adequate storage, quality network interface
- Reasoning: Print and web services are moderately resource-intensive. Combining them on capable hardware provides good performance at reasonable cost.

Estimated Cost: Approximately $15,000-$25,000 for hardware plus software licensing

VII - Evaluate the topology and protocol suite selected for a given scenario and how it demonstrates the efficient utilisation of a networking system

C. CONCLUSION

This report has explored the fundamental principles and practical applications of computer networking, from basic definitions to complex system implementations. The examination of network types, topologies, and protocols reveals that effective networking is fundamentally about balancing competing priorities: cost versus performance, simplicity versus scalability, and security versus accessibility. The interdependence between hardware components and networking software demonstrates that successful network design requires holistic thinking, as each element from the CPU and RAM to the network interface card must work seamlessly with operating systems and protocols to enable reliable communication. The practical application of these principles to the educational institute scenario illustrates that network planning demands careful analysis of organizational needs, user requirements, and budget constraints. Whether choosing between star and mesh topologies, selecting TCP over UDP for specific applications, or deciding on server consolidation strategies, administrators must understand both the technical capabilities and limitations of networking technologies. Ultimately, this report demonstrates that modern networking is not merely about connecting computers together, but about creating robust, scalable, and secure infrastructure that enables organizations to share resources efficiently, support diverse user needs, and adapt to evolving technological demands while maintaining operational reliability and cost-effectiveness.

D. REFERENCE

- Burgess, M. (2004) *Principles of Network and System Administration*. 2nd Ed. Chichester: John Wiley and Sons.

- Burgess, M. (2004) Chapter 2: System Components, Section 2.6 - Networks. In: *Principles of Network and System Administration*. 2nd Ed. Chichester: John Wiley and Sons, pp. 46-54.

- Burgess, M. (2004) Chapter 2: System Components, Section 2.7 - IPv4 networks. In: *Principles of Network and System Administration*. 2nd Ed. Chichester: John Wiley and Sons, pp. 55-62.

- Burgess, M. (2004) Chapter 10: Network-level Services, Section 10.2 - A recap of networking concepts. In: *Principles of Network and System Administration*. 2nd Ed. Chichester: John Wiley and Sons, pp. 391-393.

- Burgess, M. (2004) Chapter 10: Network-level Services, Section 10.3 - Getting traffic to its destination. In: *Principles of Network and System Administration*. 2nd Ed. Chichester: John Wiley and Sons, pp. 393-397.

- Lowe, D. (2004) *Networking All-in-One Desk Reference For Dummies*. 2nd Ed. Indianapolis: Wiley Publishing.

- Lowe, D. (2004) Chapter 1: Understanding Networks. In: *Networking All-in-One Desk Reference For Dummies*. 2nd Ed. Indianapolis: Wiley Publishing, pp. 9-18.

- Lowe, D. (2004) Chapter 2: Understanding Network Protocols and Standards. In: *Networking All-in-One Desk Reference For Dummies*. 2nd Ed. Indianapolis: Wiley Publishing, pp. 19-39.

- Burgess, M. (2004) Chapter 3: Networked Communities, Section 3.5 - Clients, servers and delegation. In: Principles of Network and System Administration. 2nd Ed. Chichester: John Wiley and Sons, pp. 78-80.

- Burgess, M. (2004) Chapter 3: Networked Communities, Section 3.6 - Host identities and name services. In: Principles of Network and System Administration. 2nd Ed. Chichester: John Wiley and Sons, pp. 80-82.

- Lowe, D. (2004) Book I, Chapter 3: Understanding Network Hardware. In: Networking All-in-One Desk Reference For Dummies. 2nd Ed. Indianapolis: Wiley Publishing, pp. 41-58.

- Lowe, D. (2004) Book I, Chapter 4: Understanding Network Operating Systems. In: Networking All-in-One Desk Reference For Dummies. 2nd Ed. Indianapolis: Wiley Publishing, pp. 59-73.

- Burgess, M. (2004) Chapter 2: System Components, Section 2.2 - Handling hardware. In: Principles of Network and System Administration. 2nd Ed. Chichester: John Wiley and Sons, pp. 13-16.

- Burgess, M. (2004) Chapter 2: System Components, Section 2.3 - Operating systems. In: Principles of Network and System Administration. 2nd Ed. Chichester: John Wiley and Sons, pp. 16-25.

- Lowe, D. (2004) Book I, Chapter 3: Understanding Network Hardware. In: Networking All-in-One Desk Reference For Dummies. 2nd Ed. Indianapolis: Wiley Publishing, pp. 41-58.

- Lowe, D. (2004) Book I, Chapter 4: Understanding Network Operating Systems. In: Networking All-in-One Desk Reference For Dummies. 2nd Ed. Indianapolis: Wiley Publishing, pp. 59-73.

- Lowe, D. (2004) Book II, Chapter 1: Planning a Network. In: Networking All-in-One Desk Reference For Dummies. 2nd Ed. Indianapolis: Wiley Publishing, pp. 77-93.