Computer Science Class 9 Notes

Chapter 6

Introduction to Computer Networks

Punjab Board (RNC 2023) | English Medium

Chapter 6: Introduction to Computer Networks

This chapter introduces computer networks as systems of linked devices that exchange data and work together, ranging from small Local Area Networks (LANs) to the Internet itself. It covers the fundamental components of data communication, the key networking devices (switches, routers, access points), and the four main network topologies (bus, star, ring, mesh) that determine how devices are arranged and connected.

The chapter then explores transmission modes (simplex, half-duplex, full-duplex), the 7-layer OSI networking model, IPv4 and IPv6 addressing, essential protocols and services (TCP/IP, DNS, DHCP), network security methods (firewalls, encryption, antivirus), and the different types of networks classified by size (PAN, LAN, MAN, WAN, CAN), closing with real-world applications across business, education, and healthcare.

Learning Objectives

- Explain computer networks as systems, including their objectives and components
- Identify the five fundamental components of data communication
- Describe the roles of networking devices: switches, routers, and access points
- Differentiate between the four main network topologies: bus, star, ring, and mesh
- Differentiate between simplex, half-duplex, and full-duplex transmission modes
- Describe the 7-layer OSI networking model and the function of each layer
- Differentiate between IPv4 and IPv6, and explain the roles of DNS and DHCP
- Describe network security methods (firewalls, encryption, antivirus) and common security threats

Key Concepts

6.1 Computer Networks as Systems

A computer network is a system of linked devices and computers that exchange data and operate together, ranging from small Local Area Networks (LANs) to large Wide Area Networks (WANs), including the Internet — the largest network, connecting all networks worldwide. Its primary components are nodes (connected devices like computers, smartphones, printers), links (wired or wireless connections between nodes), switches (connect multiple nodes within a network), and routers (connect different networks and direct data between them).

The primary objectives of computer networks are resource sharing (e.g., multiple computers sharing a single printer, reducing costs), data communication (enabling emails, instant messaging, video conferencing), and connectivity and collaboration (enabling remote access and real-time collaboration, e.g., a shared Google Drive document). Data communication itself has five basic components: the sender (the device sending data), the receiver (the device receiving data), the message (the data being communicated), the protocol (rules governing communication, e.g., HTTP), and the medium (the physical or wireless path data travels, e.g., Ethernet cable or Wi-Fi).

6.2 Networking Devices: Switch, Router, and Access Point

A switch connects multiple devices (computers, printers, servers) within a network, operating at the Data Link Layer (Layer 2 of the OSI model). It uses each device's MAC (Media Access Control) address to forward data only to the correct destination device, rather than broadcasting to all devices — the first time, it may broadcast, but once it learns device addresses, it sends data directly to the correct destination, making networks faster and more efficient.

A router interconnects different networks and directs data packets between them, using a routing table to find the best path for each packet to reach its destination. An Access Point (AP) allows wireless devices to connect to a wired network, receiving data from the wired network and transmitting it wirelessly (using radio waves) to devices, and vice versa — modern APs can connect hundreds of devices simultaneously, making them ideal for schools, offices, and stadiums.

6.3 Network Topologies

Network topologies define how devices (nodes) are arranged in a network, affecting reliability and performance. In a Bus topology, all devices share a single communication line (the bus) — easy to set up, but if the main cable fails, the whole network goes down. In a Star topology, each node communicates through a central switch or hub, which acts as a data flow repeater — if one connection fails, only that node is affected.

In a Ring topology, each device is connected in a circular pathway, with data traveling in one direction through each device — it can handle high traffic, but if one connection fails, the whole network is affected (a 2-way ring can help mitigate this). In a Mesh topology, each device is connected to every other device, providing high redundancy and reliability — if one link fails, data can be rerouted through other links, making it the most fault-tolerant topology.

6.4 Transmission Modes

Transmission modes describe how data flows between devices. In Simplex communication, data flows in only one direction — a device can either send or receive, never both (e.g., a keyboard sending data to a computer). In Half-Duplex communication, data can flow in both directions, but not simultaneously — one device must finish transmitting before the other can start (e.g., a walkie-talkie).

In Full-Duplex communication, data can flow in both directions simultaneously — both devices can transmit and receive at the same time (e.g., a telephone conversation, where both people can talk and listen at once). Full-duplex is ideal for modern communication systems like internet browsing and video calls, since it allows for far more efficient data transmission than the older half-duplex systems used by early telephones.

6.5 The OSI 7-Layer Networking Model

The Open Systems Interconnection (OSI) Model is a 7-layer framework for understanding how networking protocols interact. Layer 1 (Physical) handles the actual physical connection between devices — cables, connectors, and voltage levels. Layer 2 (Data Link) handles node-to-node data transport and error detection/correction, like traffic lights managing the flow of data to prevent collisions. Layer 3 (Network) determines the best path for data between different networks using IP addresses, like a GPS finding the best route. Layer 4 (Transport) ensures reliable data transfer between source and destination processes, using protocols like TCP, like a delivery service ensuring a package arrives safely.

Layer 5 (Session) establishes, maintains, and terminates connections between applications, like a phone call being set up, kept connected, and ended. Layer 6 (Presentation) translates, formats, and encrypts data between the application and the network, like a translator converting a book between languages. Layer 7 (Application) is closest to the end user, providing network services directly to applications like email and web browsing, like a waiter taking your order and bringing your food.

6.6 IPv4, IPv6, and Network Services

IP (Internet Protocol) addresses are unique identifiers assigned to devices connected to the Internet. IPv4 uses a 32-bit address scheme, allowing for 2^{32} = 4,294,967,296 (about 4.3 billion) unique addresses, written as four decimal numbers from 0-255 (e.g., 192.168.1.1). IPv6, designed to replace IPv4 due to address depletion, uses a 128-bit scheme, allowing for an almost limitless number of addresses, written in a longer hexadecimal format.

Protocols are sets of rules governing data communication — common examples include TCP/IP, HTTP, FTP, and SMTP. The Domain Name System (DNS) translates human-readable domain names (like www.example.com) into IP addresses that computers use to locate websites. The Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses to devices joining a network, simplifying network management — for example, when a device connects to Wi-Fi, DHCP assigns it an IP address automatically.

6.7 Network Security

Network security protects data and prevents unauthorized access, and matters for data protection (preventing unauthorized access/alteration), preventing attacks, maintaining privacy, and ensuring availability of network resources. Firewalls are security systems that monitor and control incoming/outgoing network traffic based on predetermined rules, acting as a security checkpoint between trusted internal networks and untrusted external networks. Encryption transforms data into a secure format readable only with the correct decryption key — for example, a shift cipher shifting each letter by a fixed number of positions in the alphabet.

Common threats to network security include: Malware (viruses, worms, ransomware that damage or steal data), Phishing (deceptive emails/websites tricking users into revealing sensitive information), Denial of Service (DoS) attacks (overwhelming a network with traffic to disrupt it), and Man-in-the-Middle attacks (intercepting communication to steal or alter information). A combination of firewalls, encryption, and antivirus software provides robust, layered network security.

6.8 Types of Networks and Real-World Applications

Networks are classified by size and range: a Personal Area Network (PAN) connects personal devices over a very short range, like a few meters (e.g., Bluetooth between a phone and headset); a Local Area Network (LAN) connects devices within a limited area like a home, school, or office; a Metropolitan Area Network (MAN) spans a city or large campus, up to around 50 kilometers, connecting multiple LANs; a Wide Area Network (WAN) covers a large geographical area, connecting multiple LANs and MANs (the Internet is the largest WAN); and a Campus Area Network (CAN) connects multiple LANs within a limited area like a university campus.

Computer networks have wide-ranging real-world applications: in business, networks enable efficient communication and resource sharing (e.g., companies using intranets); in education, networks power online learning platforms and Learning Management Systems (LMS) like Blackboard or Moodle; and in healthcare, networks facilitate sharing patient information and telemedicine through Electronic Health Records (EHR) systems.

Important Definitions

What is a computer network?

A system of linked devices and computers that exchange data and operate together, ranging in scale from a small LAN to the entire Internet.

What is a protocol?

A set of rules that governs data communication between devices, such as TCP/IP, HTTP, FTP, or SMTP.

What is a router?

A networking device that interconnects different networks and directs data packets between them, using a routing table to find the best path.

What is a switch?

A networking device that connects multiple devices within a network and forwards data only to the correct destination device using MAC addresses.

What is a network topology?

The arrangement or layout of devices (nodes) and connections in a computer network, such as bus, star, ring, or mesh.

What is the OSI Model?

A 7-layer framework (Physical, Data Link, Network, Transport, Session, Presentation, Application) used to understand how different networking protocols interact.

What is DNS (Domain Name System)?

A network service that translates human-readable domain names, like www.example.com, into the numeric IP addresses computers use to locate websites.

What is encryption?

The process of transforming data into a secure format that can only be read or understood by authorized parties who have the correct decryption key.

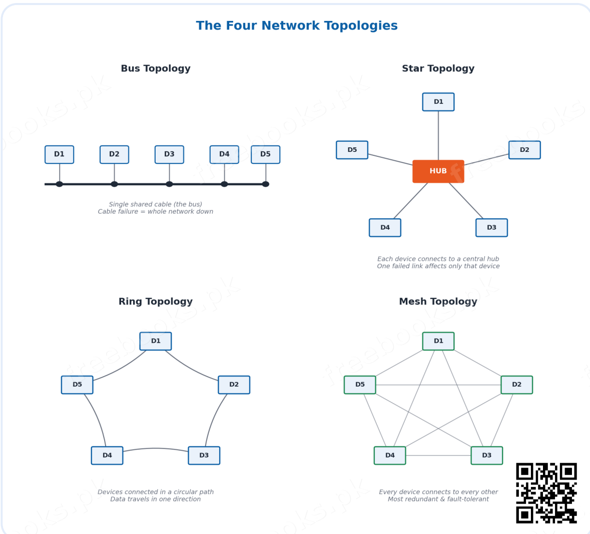
Key Facts and Relations

Topic	Key Fact / Relation

5 components of data communication	Sender + Receiver + Message + Protocol + Medium
4 network topologies	Bus, Star, Ring, Mesh
3 transmission modes	Simplex (one-way), Half-Duplex (both ways, not at once), Full-Duplex (both ways at once)
OSI Model's 7 layers	Physical → Data Link → Network → Transport → Session → Presentation → Application
Total IPv4 addresses	2^{32} = 4,294,967,296 (~4.3 billion)
IPv4 vs IPv6 address length	IPv4 = 32-bit; IPv6 = 128-bit
Key TCP/IP protocols	TCP (reliable transfer), IP (addressing/routing), UDP (faster, less reliable), DNS, DHCP
Networks by size (smallest to largest)	PAN < LAN < CAN < MAN < WAN (Internet)

Diagrams

The Four Network Topologies: A comparison of bus, star, ring, and mesh network topologies, showing how devices are arranged and connected in each

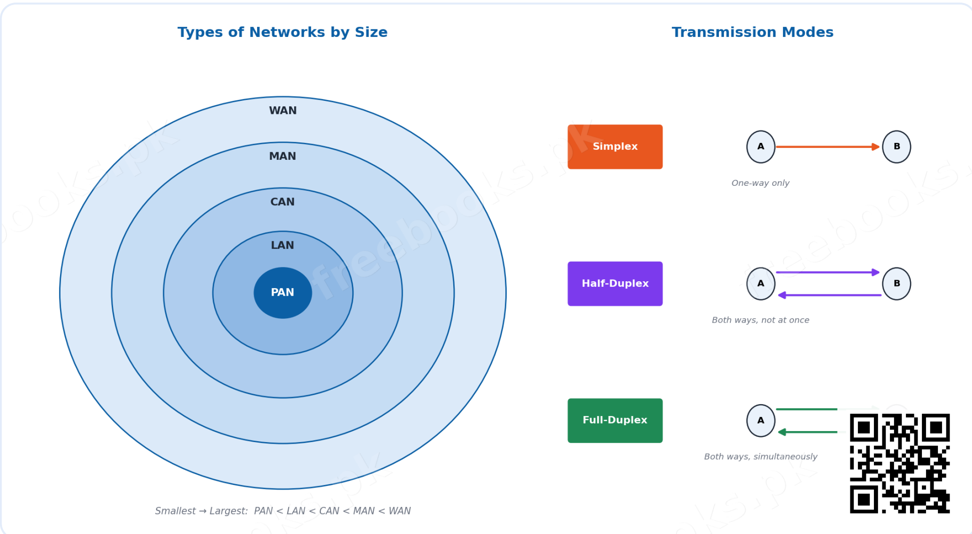


The Four Network Topologies

The 7-Layer OSI Model: A diagram of the seven OSI layers from Physical to Application, with the function of each layer

The 7-Layer OSI Model

Types of Networks by Size: A comparison of PAN, LAN, MAN, and WAN networks by their typical range and scale, alongside the three transmission modes



Types of Networks by Size

Short Questions & Answers

Define data communication and list its key components.

Data communication is the exchange of data between a sender and receiver through a communication medium. Its five key components are the sender, receiver, message, protocol, and medium.

Explain the role of routers in a computer network.

A router interconnects different networks and directs data packets between them, using a routing table to determine the best path for each packet to reach its destination efficiently.

What are the main functions of the Network Layer in the OSI model?

The Network Layer (Layer 3) is responsible for data transfer between different networks, determining the best path for data to travel from source to destination using IP addresses.

What is the purpose of the Dynamic Host Configuration Protocol (DHCP)?

DHCP automatically assigns IP addresses to devices when they join a network, simplifying network management by removing the need for manual IP address configuration.

Differentiate between TCP and UDP in terms of data transfer reliability.

TCP (Transmission Control Protocol) ensures reliable, ordered data transfer with error checking, while UDP (User Datagram Protocol) provides faster but less reliable data transfer without such guarantees.

Explain the importance of encryption in network security.

Encryption transforms data into a secure format that can only be read by parties with the correct decryption key, protecting sensitive information from being intercepted and read by unauthorized parties.

What are the advantages of using a star topology in a network?

In a star topology, if one connection fails, only that single node is affected rather than the whole network, and it is generally easier to manage, troubleshoot, and expand than other topologies.

How do firewalls contribute to network security?

Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules, acting as a checkpoint between trusted internal networks and untrusted external networks.

Long Questions & Answers

Discuss the objectives of computer networks and provide examples of how they facilitate resource sharing and data communication.

Computer networks exist fundamentally to serve three closely interconnected core objectives, each one contributing significantly to the overall practical value and everyday usefulness that networked computing systems consistently provide to both individual users and larger organizations alike, and understanding each of these three objectives in reasonable depth helps to clarify precisely why computer networks have become such an absolutely fundamental and indispensable part of modern life. The first major objective is resource sharing, whereby computer networks allow multiple different devices to share access to valuable hardware and software resources, such as printers, scanners, and shared storage space, thereby meaningfully reducing overall costs and improving general efficiency; a clear, concrete example of this particular objective in action can be seen in a typical office environment, where multiple different employee computers are all connected together to share access to just a single centrally located network printer, rather than each individual employee needing their own separate, dedicated printer, which would clearly be considerably more expensive and also less efficient overall in terms of physical office space and ongoing maintenance costs. The second major objective is data communication, whereby computer networks facilitate the reliable transfer of data between different devices, thereby directly enabling many different forms of modern communication, including email, instant messaging, and real-time video conferencing; a clear, concrete example of this second objective can be seen in a company that has employees working from several different geographic office locations, who are nevertheless able to collaborate together effectively and communicate in real time using popular video conferencing tools such as Zoom or Microsoft Teams, entirely thanks to the underlying computer network connections that make this kind of instantaneous, long-distance communication technically possible in the first place. The third major objective is connectivity and collaboration, whereby computer networks connect together many different individual devices, thereby enabling convenient remote access and genuinely effective real-time collaboration between multiple different users, which in turn significantly improves overall organizational productivity and general day-to-day flexibility; a clear, concrete example of this third objective can be seen in a team of colleagues who are able to work together simultaneously on a single shared document using a cloud-based collaboration service such as Google Drive, with every team member's individual edits and contributions to the document being instantly and automatically visible to every other team member in real time, entirely thanks to the underlying network connectivity that makes this kind of live, simultaneous collaborative editing technically possible. Taken together as a whole, these three core objectives — resource sharing, data communication, and connectivity/collaboration — collectively explain precisely why computer networks have become such an absolutely essential and deeply embedded part of virtually every modern business, every educational institution, and indeed every individual household today.

Compare and contrast the different types of network topologies: star, ring, bus, and mesh.

Network topologies describe the specific physical or logical arrangement of the various different devices, commonly referred to as nodes, that together make up a given computer network, and the four most commonly discussed topology types — bus, star, ring, and mesh — each offer their own genuinely distinct set of characteristic advantages and disadvantages in terms of overall cost, general reliability, and ease of practical setup and ongoing maintenance. In a Bus topology, every single device connected to the network shares one single common communication line, generally referred to as 'the bus,' with each individual device being directly connected to this one shared central cable; this particular topology is generally very simple, inexpensive, and quick to properly set up, but it unfortunately suffers from one very serious potential drawback, since if the single shared central cable itself happens to fail for any reason, the entire network will consequently go down completely, since there exists no meaningful alternative communication pathway that any of the individual connected devices could otherwise use instead. In a Star topology, by contrast, every individual device within the network is instead separately connected to one central, shared hub or switch device, which itself is specifically responsible for centrally managing and correctly directing all of the network's ongoing data flow between the various different connected devices; this particular topology offers the genuine practical advantage that if any single individual connection between one particular device and the central hub happens to fail, only that one specific individual device will actually be affected by the failure, while every other device connected to the network will otherwise continue operating entirely normally and without any interruption whatsoever, although the star topology does still ultimately depend quite heavily on the continued reliability of that one single central hub device itself. In a Ring topology, each individual device is instead connected sequentially to exactly two direct neighbouring devices, together collectively forming one single continuous circular data pathway around which data must travel sequentially, generally flowing in just one single fixed direction around the ring, passing through each individual device in turn before eventually reaching its intended final destination; this particular topology is generally capable of handling relatively high volumes of overall network traffic quite efficiently, but if even just one single individual connection within the overall ring happens to fail, the entire ring network as a whole will typically be seriously affected as a direct result, unless a more resilient two-way (bidirectional) ring configuration is instead specifically used to help meaningfully mitigate this particular structural vulnerability. In a Mesh topology, finally, every single individual device within the network is instead directly connected to every other individual device in the entire network, thereby providing an extremely high overall degree of built-in data redundancy and consequently excellent overall network reliability; this particular topology is widely considered the single most inherently reliable of these four different topology types, since if any one particular individual connection within the overall mesh happens to fail for any reason, the network's data can nevertheless still continue to be successfully and automatically rerouted through any number of the various different alternative available connection paths, although this comes at the cost of the mesh topology generally being considerably more complicated, and also usually significantly more expensive overall, to properly and fully implement across an entire network, when directly compared against the other three, generally simpler topology types discussed above.

Describe how data is transmitted across computer networks using packet switching and circuit switching.

Data transmitted across computer networks is generally sent using one of two fundamentally different, well-established underlying methods, known respectively as packet switching and circuit switching, and each of these two distinct methods approaches the underlying core technical challenge of reliably moving data from one specific point in a network to another in a genuinely quite different way. In packet switching, which is the particular method that is very widely and predominantly used across the modern Internet today, any given piece of data that needs to be transmitted is first broken down and divided into a number of considerably smaller individual units, generally referred to as packets, with each one of these individual data packets separately containing both a specific portion of the overall original data, together with important additional addressing information that specifically indicates that particular packet's intended final destination; these individual packets are then each sent out independently across the network, and, quite significantly, different individual packets belonging to the very same overall original message may sometimes end up actually travelling along several genuinely different specific network paths or routes in order to eventually reach their shared common final destination, entirely depending on which particular network paths happen to be least busy or most readily available to use at that specific moment in time; once every individual packet belonging to a given message has successfully arrived at its intended final destination, these various individual packets are then automatically reassembled together again, in the correct original order, in order to fully reconstruct the complete original message. A genuinely useful analogy that helps to clearly illustrate this particular process is that of air travel: much like individual airline passengers might sometimes be organizationally split up into several smaller separate groups and subsequently assigned to different specific flights, each one of which may potentially take an entirely different specific route through various different intermediate connecting airports, in order to eventually reach one single shared common final destination, individual data packets can quite similarly take several genuinely different specific network paths, each one passing through various different intermediate network routers along the way, before finally arriving together at their own single shared common final destination. Circuit switching, by clear contrast, instead works by first establishing one single dedicated, exclusive communication pathway directly between the sender and the intended receiver, with this one particular dedicated pathway then remaining continuously reserved, exclusively and specifically for that one particular ongoing communication session, throughout the entire remaining duration of that specific communication; this circuit-switching approach was historically used quite extensively by traditional analog telephone networks, where one specific dedicated physical circuit would be temporarily but completely reserved for the sole exclusive use of one single particular telephone call for as long as that particular call continued to remain active and ongoing. Although circuit switching does offer the genuine practical advantage of providing a consistently steady, entirely predictable, and reliably guaranteed data transmission rate throughout an entire ongoing communication session, packet switching is nevertheless generally considered to be a considerably more efficient overall approach for most typical modern computer networking purposes, since it allows the very same underlying shared network infrastructure to be flexibly and dynamically shared simultaneously among many different simultaneous users and communication sessions, rather than requiring one single dedicated pathway to be fully and exclusively reserved for just one single individual communication session at any one given time, as circuit switching would otherwise require.

A network administrator needs to work with IP addressing. (a) Calculate the total number of unique IPv4 addresses possible, given that IPv4 uses a 32-bit addressing scheme. (b) If 10% of the total addresses are reserved for special purposes, how many addresses remain available? Show your working.

IPv4 (Internet Protocol version 4) addresses are constructed using a fixed 32-bit binary addressing scheme, meaning that each individual complete IPv4 address is made up of exactly 32 individual binary digits (bits), with each one of these 32 individual bits being capable of independently holding one of exactly two possible binary values, specifically either a 0 or a 1. Because each one of these 32 individual bits can independently take on either one of these two possible values, the total number of genuinely unique possible combinations that can be formed using all 32 of these individual bits together is calculated mathematically as 2 raised to the power of 32, which is conventionally written using the mathematical notation 2^{32}. Carrying out this specific calculation gives us: $2^{32} = 2 \times 2 = 4{,}294{,}967{,}296$. Therefore, the complete IPv4 addressing scheme is capable of providing a maximum total of exactly 4,294,967,296 (approximately 4.3 billion) genuinely unique individual IP addresses in total. For part (b) of this specific problem, we are additionally told that exactly 10% of this total overall pool of available IPv4 addresses has been specifically set aside and formally reserved for various special administrative purposes (which, in real-world practical IPv4 networking, actually does happen for various legitimate technical reasons, including private internal networks, multicast addressing, and other specific reserved technical uses); in order to correctly calculate the resulting number of addresses that consequently remain available for general everyday public use after this particular 10% reservation has been properly accounted for, we must first calculate exactly what 10% of the total 4,294,967,296 addresses actually amounts to in absolute numerical terms: $4,294,967,296 \times 0.10 = 429,496,729.6$ (which, since we cannot meaningfully have a fractional part of a single individual IP address in any real practical sense, would very typically be rounded in practice to a whole number value of approximately 429,496,730 addresses). Subtracting this specific calculated reserved amount from the original overall total then gives us the final number of addresses that genuinely remain available for regular general use: $4,294,967,296 - 429,496,730 = 3,865,470,566$ (approximately). Therefore, after appropriately setting aside the specified 10% reservation for various special administrative purposes, approximately 3,865,470,566 individual IPv4 addresses would still remain genuinely available for regular, everyday general use — a very large number in absolute terms, yet still one that has nevertheless proven to be entirely insufficient to properly and sustainably meet the enormous, ever-growing global demand created by the sheer number of individual devices that have since become connected to the modern Internet, which is precisely the core underlying reason why the newer IPv6 addressing standard, offering a vastly larger total theoretical address space, was specifically developed in the first place.

Multiple Choice Questions (MCQs)

What is the primary objective of computer networks? (A) Increase computational power (B) Enable resource sharing and data communication (C) Enhance graphic capabilities (D) Improve software development

Correct answer: (B) Enable resource sharing and data communication. The primary objective of computer networks is to enable resource sharing, data communication, and connectivity/collaboration between devices.

Which device is used to connect multiple networks and direct data packets between them? (A) Switch (B) Hub (C) Router (D) Modem

Correct answer: (C) Router. A router connects different networks together and directs data packets between them using a routing table.

Which layer of the OSI model is responsible for node-to-node data transfer and error detection? (A) Physical Layer (B) Data Link Layer (C) Network Layer (D) Transport Layer

Correct answer: (B) Data Link Layer. The Data Link Layer (Layer 2) handles node-to-node data transport along with error detection and correction.

What is the function of the Domain Name System (DNS)? (A) Assign IP addresses dynamically (B) Translate domain names to IP addresses (C) Secure data communication (D) Monitor network traffic

Correct answer: (B) Translate domain names to IP addresses. DNS translates human-readable domain names (like www.example.com) into the numeric IP addresses computers use.

Which method of data transmission uses a dedicated communication path? (A) Packet Switching (B) Circuit Switching (C) Full-Duplex (D) Half-Duplex

Correct answer: (B) Circuit Switching. Circuit switching establishes one dedicated communication pathway that remains reserved for the entire duration of the communication session.

What is encapsulation in the context of network communication? (A) Converting data into a secure format (B) Wrapping data with protocol information (C) Monitoring network traffic (D) Translating domain names to IP addresses

Correct answer: (B) Wrapping data with protocol information. Encapsulation refers to wrapping data with the necessary protocol information (headers) as it passes down through the network layers.

Which protocol is used for reliable data transfer in the TCP/IP model? (A) HTTP (B) FTP (C) TCP (D) UDP

Correct answer: (C) TCP. TCP (Transmission Control Protocol) specifically ensures reliable, ordered, error-checked data transfer.

What is the main purpose of a firewall in network security? (A) Convert data into a secure format (B) Monitor and control network traffic (C) Assign IP addresses (D) Translate domain names

Correct answer: (B) Monitor and control network traffic. A firewall's main purpose is to monitor and control incoming and outgoing network traffic based on predetermined security rules.

Which network topology connects all devices to a central hub? (A) Ring (B) Mesh (C) Bus (D) Star

Correct answer: (D) Star. In a Star topology, every device connects to a central hub or switch, which manages and directs all data flow.

What is a key benefit of using computer networks in businesses? (A) Increase computational power (B) Enable resource sharing and efficient communication (C) Enhance graphic capabilities (D) Improve software development

Correct answer: (B) Enable resource sharing and efficient communication. A key benefit of computer networks in business is enabling resource sharing and efficient communication among employees and departments.

Quick Revision Summary

- 5 data communication components: Sender, Receiver, Message, Protocol, Medium
- Devices: Switch (Layer 2, uses MAC address), Router (connects networks, uses routing table), Access Point (wireless-to-wired bridge)
- 4 topologies: Bus (single shared cable), Star (central hub), Ring (circular, one direction), Mesh (every device connected to every other — most reliable)
- 3 transmission modes: Simplex (one-way), Half-Duplex (both ways, one at a time), Full-Duplex (both ways at once)
- OSI 7 layers: Physical → Data Link → Network → Transport → Session → Presentation → Application
- IPv4 = 32-bit (~4.3 billion addresses); IPv6 = 128-bit (near-limitless); DNS translates names→IPs; DHCP auto-assigns IPs

- Security: Firewalls (monitor/control traffic), Encryption (secures data), Antivirus (removes malware); Threats: Malware, Phishing, DoS, Man-in-the-Middle
- Network sizes (smallest→largest): PAN (few meters) < LAN (building) < CAN (campus) < MAN (city, ~50km) < WAN (Internet)

Exam Tips

- Memorize the OSI model layers in order (Physical, Data Link, Network, Transport, Session, Presentation, Application) — a mnemonic like 'Please Do Not Throw Sausage Pizza Away' can help
- Distinguish Switch (connects devices WITHIN a network, uses MAC) from Router (connects DIFFERENT networks, uses IP)
- Remember mesh topology = most reliable (redundant paths); bus topology = single point of failure (the shared cable)
- Simplex = one-way only; Half-Duplex = both ways but not at once; Full-Duplex = both ways at once (like a phone call) — a very common exam distinction
- For IPv4 total-address questions, always show the 2^{32} calculation explicitly, not just the final number
- Know your network types by size: PAN < LAN < CAN < MAN < WAN — often tested as a matching or ordering question