



KAMALDNP

kamaldnp.com • IT Training, Varanasi

PDF created by Raj Kamal using AI

Short Notes — Computer Network

BTEUP Diploma in Computer Science & Engineering • 3rd Semester • Short Notes
Session 2026-27

Short Revision Notes — prepared by KAMALDNP Academy from the official BTEUP 2026-27 syllabus. This is NOT a BTEUP board paper or publication.

These **short revision notes** cover all five units of Computer Network from the official BTEUP 2026-27 syllabus for CSE 3rd semester, in syllabus order. Each point gives the definitions, layer functions, comparisons and protocol roles that a short or five-mark answer needs, in plain English.

Please note: Computer Network is a **practicum** subject in the 2026-27 scheme, so these notes target its **theory (lecture) part and viva** — use them together with your practical work, the official syllabus PDF and the matching practice paper. These are revision notes only, not a replacement for your textbook and class notes.

Unit 1 — Introduction (6 Periods, 12%)

Topics: Introduction to computer networks; network models — OSI reference model, TCP/IP model.

Introduction to computer networks

A **computer network** is a group of two or more autonomous computers and devices connected together so that they can communicate and share data and resources. A single isolated computer is not a network; connection plus sharing is the key idea.

Why networks are used:

- **Resource sharing** — many users share one printer, one internet connection and common files.
- **Communication** — email, messaging, video calls and file transfer between distant users.
- **Reliability and saving** — data kept at more than one place survives the failure of one machine, and one powerful server can serve many cheaper clients.

Network types by size: PAN (a few metres, one person), LAN (a building or campus — high speed, privately owned), MAN (a city) and WAN (countries and continents, such as the internet). Basic terms: a **node** is a connected device, a **host** is a computer on the network, bandwidth is the data-carrying capacity, and a **protocol** is the set of rules for communication.

Network models — OSI reference model

The **OSI reference model** (Open Systems Interconnection, by ISO) divides network communication into **seven layers**, each with a fixed job, so that equipment from different makers can work together. Data goes down the layers at the sender (each layer adds its own header — encapsulation) and up the layers at the receiver.

- **7. Application** — services for user programs: email, file transfer, web.
- **6. Presentation** — data format, encryption and compression.
- **5. Session** — starts, manages and ends dialogue sessions between applications.
- **4. Transport** — end-to-end delivery, segmentation, flow and error control (TCP/UDP).
- **3. Network** — logical addressing (IP) and routing across networks.
- **2. Data Link** — framing, physical (MAC) addressing and error detection on one link.
- **1. Physical** — actual bits sent over the medium as signals.

Memory order from top: **A**pplication, **P**resentation, **S**ession, **T**ransport, **N**etwork, **D**ata link, **P**hysical. OSI is mainly a reference/teaching model — it defines the functions, while real networks run the TCP/IP model.

Network models — TCP/IP model

The **TCP/IP model** is the practical model on which the internet works. It has **four layers**:

- **Application layer** — combines the work of OSI's application, presentation and session layers. Protocols: HTTP, SMTP, DNS, FTP.
- **Transport layer** — end-to-end communication between processes using port numbers. Protocols: TCP (reliable) and UDP (fast, unreliable).
- **Internet layer** — logical addressing and routing of packets (called datagrams) across different networks. Main protocol: IP, supported by ICMP and ARP.
- **Network Access (Link) layer** — combines OSI's data link and physical layers; it deals with the actual hardware, cables, WiFi and MAC addresses of the local link.

OSI vs TCP/IP — the comparison examiners want: OSI has 7 layers, was developed as a standard model before wide use, separates session and presentation clearly, and is protocol-independent. TCP/IP has 4 layers, grew from the real ARPANET/internet protocols, merges the top three OSI layers into one application layer, and is the model actually implemented everywhere today.

Likely question: Draw the OSI reference model and write the function of each layer. How does the TCP/IP model differ from the OSI model?

Unit 2 — Data Communication and Communication Methodologies (10 Periods, 25%)

Topics: Transmission media — principles, issues and examples; wired media (coaxial, UTP, STP, fibre optic cables); wireless media (HF, VHF, UHF, microwave, Ku band); network topologies; data link layer — design issues and example protocols (Ethernet, WLAN, Bluetooth); switching techniques (circuit, packet, message).

Transmission media — principles, issues and examples

A **transmission medium** is the physical path through which signals carry data from sender to receiver. In **guided (wired) media** the signal travels inside a solid material such as copper wire or glass fibre; in **unguided (wireless) media** it travels through air or space as radio or microwave waves, guided only by antennas.

Principles to state: the medium fixes the available **bandwidth** (range of frequencies it can carry, hence maximum data rate), and every real medium weakens and distorts the signal.

Main issues:

- **Attenuation** — signal strength falls with distance; repeaters/amplifiers are needed on long paths.
- **Noise and interference** — outside signals mix with data and cause errors; shielding and better cables reduce it.
- **Delay** — signal takes time to travel; more delay means slower interaction.
- **Cost and ease of installation** — fibre is fast but costly to lay; wireless is easy but needs frequency permission for some bands.

Examples: guided — coaxial cable, twisted pair, fibre optic; unguided — radio broadcast, microwave links, satellite and WiFi.

Wired media (coaxial, UTP, STP, fibre optic cables)

- **Coaxial cable** — a central copper conductor, insulation, a braided metal shield and an outer jacket. The shield reduces interference, so it carries signals farther than twisted pair.

Used earlier for cable TV and old Ethernet (Thicknet/Thinnet). Types are named by impedance, such as RG-59 for TV.

- **UTP (Unshielded Twisted Pair)** — pairs of copper wires twisted around each other to cancel interference, with no extra shield. Cheapest and easiest to install and terminate (RJ-45 connector); it is the standard LAN cable today (Cat5e, Cat6). Distance limit is about 100 m per segment.
- **STP (Shielded Twisted Pair)** — twisted pairs with a metal foil/braid shield around them. Better protection against noise than UTP, but costlier, thicker and needs proper earthing of the shield.
- **Fibre optic cable** — carries data as pulses of light through a thin glass/plastic core, using total internal reflection. Highest bandwidth and speed, very low attenuation (runs for kilometres), immune to electrical interference and difficult to tap, but expensive and needs skilled joining. Used for backbones and long-distance links.

Wireless media (HF, VHF, UHF, microwave, Ku band)

Wireless (unguided) media carry data as electromagnetic waves through air. The syllabus names frequency bands and microwave/satellite communication:

- **HF (High Frequency, 3–30 MHz)** — waves reflect off the ionosphere (sky wave), so very long distances are possible; used for international radio broadcast and amateur radio. Quality varies with time and weather.
- **VHF (Very High Frequency, 30–300 MHz)** — travels mainly in straight lines (line of sight); used for FM radio and television broadcast.
- **UHF (Ultra High Frequency, 300 MHz–3 GHz)** — line-of-sight, shorter waves, smaller antennas; used for TV, mobile phones, WiFi and Bluetooth bands nearby, and microwave links.
- **Microwave** — high-frequency line-of-sight transmission between dish antennas on towers; high data rate over long distances, but blocked by hills, buildings and heavy rain, so relay towers are placed at intervals.
- **Ku band (12–18 GHz)** — a microwave band used mainly for **satellite** communication, such as DTH television and VSAT links; needs a clear view of the satellite and suffers rain fade.

Network topologies

Topology is the physical or logical arrangement of nodes and links in a network.

- **Bus** — all nodes connect to one common cable (backbone) with terminators at both ends. Cheap and easy to add nodes, but a break in the main cable stops the whole network and traffic collisions increase with load.
- **Star** — every node connects to a central switch or hub. Easy to install and fault-finding is simple; failure of one cable affects only one node, but failure of the central device stops the network. This is the standard LAN topology today.

- **Ring** — nodes form a closed loop; data travels in one (or both) directions passing through each node. No collisions in token-based working, but one break can disturb the ring.
- **Mesh** — every node connects to many (in full mesh, to every) other node. Very reliable because many alternate paths exist, but cabling cost is high; used for critical backbones, usually as partial mesh.
- **Tree (hybrid)** — star networks joined on a bus backbone, in levels; used in large buildings and campuses.

Data link layer — design issues and example protocols (Ethernet, WLAN, Bluetooth)

The **data link layer** moves frames reliably across a single link between two directly connected nodes. Its **design issues** are:

- **Framing** — dividing the bit stream into frames with clear start and end, so the receiver can separate them.
- **Error control** — detecting (and often correcting or retransmitting) frames damaged by noise, using checks such as CRC and acknowledgements.
- **Flow control** — preventing a fast sender from flooding a slow receiver.
- **Medium access** — when many nodes share one medium, deciding who transmits when; this is the job of methods such as CSMA/CD and CSMA/CA.

Example protocols: Ethernet — the standard wired LAN technology; it uses MAC addresses and frames, and modern Ethernet works through switches in full-duplex mode. **WLAN** — wireless LAN (WiFi, IEEE 802.11 family); stations listen before transmitting and use CSMA/CA with acknowledgements because collisions cannot be detected in radio in the Ethernet way. **Bluetooth** — short-range wireless for personal devices (headphones, keyboards), forming small networks called piconets.

Switching techniques (circuit, packet, message)

Switching is how intermediate nodes forward data across a network from source to destination. Three techniques:

- **Circuit switching** — a dedicated path is set up between sender and receiver before communication and is reserved for the whole session (old telephone network). Phases: circuit establishment, data transfer, circuit release. Guaranteed, steady quality and no delay variation during the call, but the reserved path is wasted when no data flows (for example, during silence).
- **Packet switching** — data is broken into small **packets**, each carrying the destination address and travelling independently, possibly by different routes; packets are reassembled at the destination. Links are shared efficiently and the network is robust, but packets may arrive out of order or with varying delay. The internet works this way (datagram style); a virtual-circuit variant fixes the route for a session.
- **Message switching** — the whole message is sent to an intermediate node, **stored completely**, then forwarded when the next link is free (store-and-forward). No dedicated

path and no size limit, but large storage is needed at each node and delay is high; it is now mostly of historical interest.

Likely question: Compare coaxial, UTP, STP and fibre optic cables. Differentiate between circuit switching, packet switching and message switching with suitable examples.

Unit 3 — Network Layer (10 Periods, 25%)

Topics: Network layer — design issues and example protocols (IPv4); concept of IPv6; routing principles, issues, algorithms (distance-vector, link-state) and protocols (RIP, OSPF).

Network layer — design issues and example protocols (IPv4)

The **network layer** delivers packets from the source host to the destination host, possibly across many different networks. Its main **design issues** are:

- **Routing** — choosing the path each packet takes through the network (studied separately below).
- **Addressing** — giving every host a unique logical address, independent of its hardware.
- **Congestion control** — preventing too many packets from entering the network and collapsing its performance.
- **Internetworking** — joining different types of networks (different sizes, rules, packet sizes — handled by fragmentation) so they appear as one network.
- **Quality of service** — supporting delay/bandwidth needs of real-time traffic as far as possible.

IPv4 is the main example protocol: it gives each interface a **32-bit address** written as four decimal numbers (dotted decimal, for example 192.168.1.10). The IPv4 packet header carries source and destination addresses, a TTL (time to live) field that stops packets looping forever, protocol and fragmentation fields, and a header checksum. IPv4 offers **connectionless, best-effort** delivery — packets may be lost, duplicated or delayed, and reliability is left to TCP above it.

Concept of IPv6

IPv6 is the newer version of the Internet Protocol, designed because IPv4's 32-bit address space (about 4.3 billion addresses) is exhausted by the growth of devices.

Main points of the concept:

- **128-bit addresses** — written as eight groups of four hexadecimal digits separated by colons, for example 2001:0db8:0000:0000:ff00:0042:8329. The address space is so large that every device can have many unique public addresses; NAT workarounds become largely unnecessary.

- **Simpler header** — a fixed 40-byte main header with fewer fields, so routers process packets faster; extra features go into optional extension headers, and there is no header checksum and no router fragmentation.
- **Better support for quality and security** — flow label for real-time flows, and IPsec support built into the design.
- **Auto-configuration** — a device can generate its own address on a network (stateless auto-configuration), making setup easier.

IPv4 and IPv6 do not talk to each other directly; transition methods such as dual stack and tunnelling let both run together while the internet migrates.

Routing principles, issues and algorithms (distance-vector, link-state)

Routing is the process of selecting paths in a network along which packets are forwarded from source to destination. Routers keep a **routing table** that says, for each destination network, the next hop and the cost. Principles: a good route should be correct, simple, robust (survive failures), stable, fair and near-optimal in delay and throughput.

Issues: the topology keeps changing (links and routers fail), traffic creates congestion on popular paths, and routers must decide with only the information they collect — a locally good choice may not be globally best.

- **Distance-vector algorithm** — each router keeps a table of the best known distance (cost) to every destination and the next hop, and periodically exchanges this table with its **neighbours only**. Distances improve gradually by the Bellman-Ford method. Simple, but converges slowly and can suffer the count-to-infinity problem when a link fails.
- **Link-state algorithm** — each router learns the **whole topology**: it measures cost to its neighbours, floods link-state packets to all routers, builds the complete map and runs Dijkstra's shortest-path algorithm to compute the best tree of routes. Converges faster and avoids count-to-infinity, but needs more memory and processing.

Routing protocols (RIP, OSPF)

Routing protocols are the practical rules by which routers exchange information and build their tables. Both examples in the syllabus are **interior gateway protocols** — used inside one organisation's network (autonomous system).

RIP (Routing Information Protocol) — based on the **distance-vector** algorithm.

- Cost metric is **hop count**; the maximum is 15 hops, and 16 means unreachable — so RIP suits only small networks.
- Routers broadcast their full table every 30 seconds to neighbours.
- Very simple to configure, but slow to converge and wastes bandwidth with periodic full updates.

OSPF (Open Shortest Path First) — based on the **link-state** algorithm.

- Each router floods link-state information and computes shortest paths with Dijkstra's algorithm; cost can reflect link bandwidth.
- Updates are sent only when something changes, so convergence is fast and large networks are supported — big networks are divided into areas.
- More complex and needs more CPU and memory than RIP.

One-line summary: small and simple network → RIP; large and fast-changing network → OSPF.

Likely question: What is IPv6 and why was it needed? Differentiate between distance-vector and link-state routing, and write short notes on RIP and OSPF.

Unit 4 — Transport Layer (8 Periods, 25%)

Topics: Transport layer — design issues and example protocols (TCP/UDP); application layer protocols (SMTP, DNS).

Transport layer — design issues and example protocols (TCP/UDP)

The **transport layer** provides communication between **processes** (programs) on different hosts — not just between hosts. It uses **port numbers** to deliver data to the correct application. Its main design issues are:

- **End-to-end delivery** — making data reach the right process reliably, although the network below is unreliable.
- **Error control and sequencing** — detecting lost or damaged segments, retransmitting them and delivering data in order.
- **Flow control** — matching sender speed to receiver capacity (sliding window).
- **Congestion control** — slowing down when the network itself is overloaded.
- **Multiplexing/demultiplexing** — many applications sharing one network connection, separated by ports.

TCP (Transmission Control Protocol): connection-oriented — a connection is set up by a three-way handshake before data flows; it gives reliable, in-order, error-checked delivery with acknowledgements and retransmission. Used for web (HTTP), email and file transfer, where nothing may be lost.

UDP (User Datagram Protocol): connectionless — packets (datagrams) are sent without setup, acknowledgements or retransmission, so overhead and delay are minimal but delivery is not guaranteed. Used for DNS, live streaming, online games and voice calls, where speed matters more than perfection.

Application layer protocols (SMTP, DNS)

The **application layer** is the top layer, where network applications and their protocols work directly for the user.

SMTP (Simple Mail Transfer Protocol) is the standard protocol for **sending** email.

Working: the sender's mail client gives the message to its mail server using SMTP; servers relay it by SMTP to the destination mail server. The receiver then reads mail using a retrieval protocol such as POP3 or IMAP — note that SMTP itself is for sending, not for reading one's mailbox. SMTP works over TCP (well-known port 25). It originally carried plain text; extensions such as MIME allow attachments.

DNS (Domain Name System) translates human-friendly **domain names** (for example `www.example.com`) into the **IP addresses** machines actually use. DNS is a distributed, hierarchical database — no single server holds all names. Working in brief: the resolver asks a local DNS server; if it does not know, it queries step by step from the root, to the top-level domain (.com) server, to the authoritative server of the domain, and caches the answer. DNS normally runs over UDP for speed.

Likely question: Differentiate between TCP and UDP. Explain the working of DNS. What role does SMTP play in sending an email?

Unit 5 — Network Devices (8 Periods, 13%)

Topics: Functioning of network devices — NIC, hub, bridge, switch, router, WiFi devices; network management system and example protocol (SNMP).

Functioning of network devices — NIC, hub, bridge

- **NIC (Network Interface Card)** — the hardware that connects a computer to the network (built-in on modern machines). It converts data between the computer's parallel form and the serial signals of the medium, prepares frames, and carries a unique permanent **MAC address** (48-bit, written in hexadecimal) by which the device is identified on the local network. A wireless NIC does the same job over radio.
- **Hub** — a simple central connecting device of older LANs, working at the physical layer. It simply repeats every incoming signal out of **all** other ports, so all connected devices share the bandwidth and one collision domain; every station receives every frame and must check if it is the destination. Hubs are cheap but wasteful and insecure, and have been replaced by switches.
- **Bridge** — connects two LAN segments at the data link layer and forwards frames between them only when the destination is on the other side, by learning which MAC addresses lie on each side. This divides a network into separate collision domains, reducing unnecessary traffic and letting a larger LAN be built from segments. Bridges are now mostly built into switches, which are effectively multi-port bridges.

Functioning of network devices — switch, router, WiFi devices

- **Switch** — a data-link-layer device with many ports that learns the MAC address connected to each port and forwards a frame **only** to the destination's port. Each port is its own collision domain, connected devices get full bandwidth, and communication can be full-duplex. A switch is the central device of a modern wired LAN.
- **Router** — a network-layer device that connects **different networks** (for example, your LAN to the internet). It reads the destination IP address, consults its routing table and forwards the packet along the best next hop. Routers separate broadcast domains, provide the default gateway for hosts, and in home/SOHO devices also perform functions such as NAT and DHCP.
- **WiFi devices** — include wireless access points, wireless routers and wireless NICs/adapters. An **access point** connects wireless stations to the wired network: devices associate with it using a network name (SSID) and security such as WPA2/WPA3 passwords and encryption. A home **wireless router** combines access point, switch and router in one box. Range is limited by walls and interference, so larger areas use multiple access points.

Layer memory line: hub = Layer 1, bridge/switch and WiFi access point = Layer 2, router = Layer 3.

Network management system and example protocol (SNMP)

A **network management system (NMS)** is the set of tools used to monitor, control and maintain a network from one place. Its main functions are commonly remembered as **FCAPS**: **F**ault management (detect and log failures), **C**onfiguration management (device settings and inventory), **A**ccounting (usage records), **P**erformance management (traffic, delay and utilisation reports) and **S**ecurity management (controlled access to devices). Without management, a large network's faults are found only when users complain.

SNMP (Simple Network Management Protocol) is the standard example protocol. Its parts:

- **Manager** — the NMS software run by the administrator.
- **Agent** — small software running in each router, switch or server, collecting information about that device.
- **MIB (Management Information Base)** — the structured database of managed information in the device, such as traffic counters, interface status and error counts.

The manager asks the agent for values (GET) or changes them (SET), and the agent can itself send an urgent alert called a **trap** when something important happens, for example a link going down. SNMP is an application-layer protocol and normally uses UDP.

Likely question: Write the functions of a switch and a router, and state the layer at which each of hub, bridge, switch and router works. What is SNMP? Name its main components.

Quick Revision — One Line Each

- A network shares resources and data; PAN, LAN, MAN and WAN are classified by size.
- OSI has 7 layers: Application, Presentation, Session, Transport, Network, Data Link, Physical.
- TCP/IP has 4 layers and is the model actually used on the internet; OSI is the reference model.
- Fibre optic is the fastest wired medium and is immune to electrical interference; UTP is the standard LAN cable.
- Star is the standard LAN topology; mesh gives many alternate paths at high cabling cost.
- Circuit switching reserves a path; packet switching sends addressed packets independently — the internet uses packets.
- IPv4 uses 32-bit addresses; IPv6 uses 128-bit addresses, mainly to solve address shortage.
- Distance-vector routers learn from neighbours only; link-state routers build the full map and use Dijkstra's algorithm.
- RIP counts hops (maximum 15); OSPF is link-state and suits large networks.
- TCP is reliable and connection-oriented; UDP is fast and connectionless.
- DNS converts domain names to IP addresses; SMTP is used for sending email.
- Hub works at Layer 1, switch at Layer 2, router at Layer 3; SNMP manages devices through manager, agents and MIB.

KAMALDNP • kamaldnp.com • support@kamaldnp.com • +91 8318013442 • Varanasi, UP

Prepared by KAMALDNP Academy from the official BTEUP 2026-27 syllabus topics. Short explanations are the author's own plain-English summaries, not syllabus text. Please confirm with your own polytechnic for any local changes.