



KAMALDNP

kamaldnp.com • IT Training, Varanasi

PDF created by Raj Kamal using AI

Practice Question Paper (Theory Part) — Computer Network

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

Practice Questions / Model Paper — NOT a BTEUP board paper

Time: 2.30 Hours (suggested practice time) Practice Score: 50 (self-check only)

General Instructions:

- All questions are compulsory. Each question has three parts (a), (b) and (c) — **answer any two** of the three parts in every question.
- Each part carries 5 marks; each question carries 10 marks.
- Draw neat, labelled diagrams wherever they are asked or wherever they support your answer.
- Write your answers in your own words, in the same order as the questions.

About this paper: In the verified BTEUP 2026-27 scheme this subject is a PRACTICUM (100 marks — lecture and practical work together); it has no separate board theory paper. This practice paper is KAMALDNP Academy's own question set for the theory (lecture) part of the practicum, written from the official syllabus topics, so you can test your concepts for the practicum assessment and viva. The marks shown (10 per question, 50 in all) are a practice weighting for self-checking only — they are NOT board marks. This is NOT a BTEUP board paper, and no question in it is promised to appear anywhere.

Q1. (From: Unit 1 — Introduction) — Answer any two of the following:

(a) Define a computer network and state its main uses. Differentiate between LAN, MAN and WAN with one example of each.

(5)

- (b) Explain the OSI reference model with a neat diagram. State the function of each layer in one line. (5)
- (c) Describe the TCP/IP model in brief. Differentiate between the OSI model and the TCP/IP model. (5)

Q2. (From: Unit 2 — Data Communication and Communication Methodologies) — Answer any two of the following:

- (a) Differentiate between coaxial cable, UTP, STP and fibre optic cable on the basis of construction, interference and use. (5)
- (b) Describe the wireless transmission media HF, VHF, UHF, microwave and Ku band in brief. Also explain bus and star topologies with diagrams, stating one advantage and one disadvantage of each. (5)
- (c) Differentiate between circuit switching, packet switching and message switching. (5)

Q3. (From: Unit 3 — Network Layer) — Answer any two of the following:

- (a) State the design issues of the network layer. Explain the working of IPv4 in brief. (5)
- (b) Explain the concept of IPv6. Differentiate between IPv4 and IPv6. (5)
- (c) Differentiate between distance-vector routing and link-state routing. Name the protocol based on each approach and state where it is used. (5)

Q4. (From: Unit 4 — Transport Layer) — Answer any two of the following:

- (a) State the design issues of the transport layer and explain any three of them in brief. (5)
- (b) Differentiate between TCP and UDP. State the use for which each one is preferred. (5)
- (c) Explain the working of the application layer protocols SMTP and DNS in brief. (5)

Q5. (From: Unit 5 — Network Devices) — Answer any two of the following:

- (a) Explain the functioning of a NIC, a hub and a bridge. (5)
- (b) Explain the functioning of a switch, a router and a WiFi device. How does a switch differ from a router? (5)
- (c) What is a network management system? Explain SNMP, its components and its working in brief. (5)

Model Answer Outline — Computer Network

The key points a full-marks answer contains, question by question.

Practice Questions / Model Paper — NOT a BTEUP board paper

Q1(a)

- A computer network is a group of two or more computers and devices connected so that they can communicate and share resources.
- Purpose: sharing data and files, sharing hardware such as printers, sharing an internet connection, and direct communication between users.
- LAN (Local Area Network): one building or campus, high speed, owned by one organisation; example: a college computer lab network.
- MAN (Metropolitan Area Network): covers a city, often joining several LANs; example: a city cable network. WAN (Wide Area Network): covers a large region or country and uses public lines; the internet is the largest WAN.
- Scope, ownership and speed separate the three types: LAN is smallest and fastest under one owner, WAN is largest, slowest per link and uses outside carriers.

Q1(b)

- List the seven layers top to bottom: Application, Presentation, Session, Transport, Network, Data Link, Physical.
- Application, Presentation and Session (top group): services to the user program, data format and encryption, and starting/ending a dialogue between machines.
- Transport and Network (middle group): end-to-end delivery between processes, and routing packets across networks by logical addressing.
- Data Link and Physical (bottom group): error-free transfer between direct neighbours using frames and physical addresses, and sending raw bits over the medium as signals.
- A neat diagram with data names helps: data, segment, packet, frame, bits as the unit moves down the layers.

Q1(c)

- TCP/IP model layers: Application, Transport, Internet and Network Access (link) — four layers in the form taught here.
- The TCP/IP Application layer covers the work of the OSI Application, Presentation and Session layers, and its Network Access layer covers OSI Data Link and Physical.
- OSI is a general reference model with seven layers, developed as a framework; TCP/IP is the model on which the actual internet protocols run.
- Named protocols: TCP/IP is built around TCP and IP; OSI names layers and services rather than one working protocol set.

- Exam line: OSI explains and separates functions clearly, TCP/IP is the practical, implemented model.

Q2(a)

- Coaxial cable: a central copper conductor with insulation, a metal shield and an outer cover; used earlier for bus networks and cable TV, moderate cost and bandwidth.
- UTP (Unshielded Twisted Pair): pairs of twisted copper wires without extra shielding; cheapest and most common LAN cable, but more open to interference.
- STP (Shielded Twisted Pair): twisted pairs with shielding, so less interference than UTP, but costlier and harder to install.
- Fibre optic cable: carries light through a glass/plastic core; highest bandwidth and distance, immune to electrical interference, but costly and needs skilled joining.
- Twisting and shielding both exist to reduce noise; fibre removes electrical noise completely by using light.

Q2(b)

- Wireless media carry signals through air rather than a cable. HF, VHF and UHF are radio bands used for radio/TV and communication links, with range and bandwidth rising with frequency band in general use.
- Microwave: high-frequency line-of-sight links between towers, used for long-distance and backhaul links; obstacles and rain weaken it. Ku band is used mainly for satellite communication, for example VSAT and DTH services.
- Bus topology: all nodes on one backbone cable; simple and cheap, but a backbone break stops the network and collisions grow with load.
- Star topology: all nodes connect to a central switch/hub; easy to add nodes and one cable fault affects one node, but the central device is a single point of failure.
- Ring and mesh in one line each: ring passes data around a circle of nodes; mesh gives many alternative paths and the best fault tolerance at the highest cabling cost.

Q2(c)

- Circuit switching: a complete path is set up before data flows and stays reserved till the end, as in the traditional telephone network; setup delay exists but the path then has steady delay and no sharing.
- Packet switching: data is broken into packets, each packet travels independently and may take a different route and is reassembled at the destination; links are shared, so use is efficient, but delay can vary.
- Message switching: the whole message is stored at each intermediate node and forwarded when the next link is free (store-and-forward); no path is reserved, but large messages cause long delays and need storage.
- Comparison points to write: path setup, unit of data, link sharing, delay behaviour and one example of each.
- Packet switching is the technique used in computer networks and the internet.

Q3(a)

- Design issues of the network layer: choosing services for the transport layer, routing, congestion control, and connecting different types of networks (internetworking).
- Its main job is delivering packets from source to destination across possibly many networks, choosing a route at each step.
- IPv4 is the example protocol: it gives logical IP addresses to hosts and routers and carries packets in datagrams with a header holding source and destination addresses and control fields.
- IPv4 works on a best-effort basis: it does not by itself guarantee delivery, order or freedom from duplication — higher layers handle that.
- Addressing point: IPv4 uses 32-bit addresses written as four decimal numbers separated by dots.

Q3(b)

- IPv6 is the newer version of IP, introduced mainly because the 32-bit IPv4 address space is too small for the growing number of devices.
- IPv6 uses 128-bit addresses, written in hexadecimal groups separated by colons, giving a vastly larger address space.
- Other improvements to name: a simpler main header for faster processing by routers, and better built-in support for options and security features at the IP level.
- Differences table should cover: address size, address notation, header size/complexity, and address availability.
- IPv4 and IPv6 are not directly compatible; both may run side by side (dual stack) during the changeover.

Q3(c)

- Routing is the process of choosing the best path for packets, judged by cost measures such as hop count, delay or bandwidth.
- Distance-vector routing: each router tells its neighbours what it knows about distances to all destinations, as in a table exchanged periodically; simple, but slow to react to changes and can form loops.
- Link-state routing: each router learns the full map (topology) of the network by flooding link information, then computes shortest paths itself; faster to settle and loop-free, but needs more processing and memory.
- RIP is a distance-vector protocol using hop count as its metric, suitable for small networks. OSPF is a link-state protocol used inside large organisational networks.
- One-line contrast: RIP routers know only what neighbours tell them; OSPF routers each hold the whole network map.

Q4(a)

- Transport layer design issues include: addressing of processes (ports), connection establishment and release, flow control, error control and multiplexing several connections on one network connection.

- It provides end-to-end communication between processes on two machines, while the network layer only reaches the destination machine.
- Reliability work sits here: lost or damaged data is detected and resent where the protocol offers a reliable service.
- Flow control stops a fast sender from flooding a slow receiver, using buffers and acknowledgements.
- Port numbers in the answer show how data reaches the correct program, for example a browser or a mail client, on the host.

Q4(b)

- TCP is connection-oriented: a connection is set up first, data is delivered reliably and in order, lost segments are retransmitted, and flow and congestion control are provided. Used where correctness matters, for example web pages and file transfer.
- UDP is connectionless: no connection setup, no retransmission and no ordering guarantee, so overhead and delay are low. Used where speed matters more than a lost packet, for example live streaming and voice.
- Header and cost: TCP carries a larger header and more control traffic; UDP has a small header and is lighter.
- Reliability line: with UDP, if the application needs reliability it must provide it itself.
- Both run on top of IP and use port numbers to reach the right application process.

Q4(c)

- SMTP (Simple Mail Transfer Protocol) is the application layer protocol used to send and transfer outgoing email between mail servers and from a client to its server.
- Working outline for SMTP: the client connects to the mail server, gives sender and receiver addresses, sends the message, and the server forwards it towards the receiver's mail server for delivery.
- DNS (Domain Name System) translates human-friendly names, such as a website name, into the IP address that machines use for routing.
- Working outline for DNS: the browser asks a DNS server for the address of the name; if that server does not know, it asks other DNS servers step by step and returns the address, which is then used to open the connection.
- Both are needed in a normal email/web action: DNS finds where to go, SMTP carries the mail.

Q5(a)

- NIC (Network Interface Card): the hardware that connects a computer to the network medium; it converts data into signals, has a unique physical (MAC) address, and works at the physical/data link level.
- Hub: a simple central device that repeats every incoming signal to all its ports; all connected devices share one collision domain and the bandwidth, so it is used only in very small, old networks.

- Bridge: joins two network segments and forwards frames using physical addresses, sending a frame only to the segment where the destination lies; this splits a network into separate collision domains.
- Difference line: a hub blindly repeats to everyone, a bridge forwards selectively by address.
- Both bridge and NIC work with physical addresses, unlike a router which uses logical IP addresses.

Q5(b)

- Switch: like a smart bridge with many ports; it learns which physical address is on which port and forwards each frame only to the destination port, giving each port its own collision domain and better use of bandwidth.
- Router: joins different networks and forwards packets by logical (IP) address using a routing table, choosing the best next path; it is the device that connects a LAN to the internet.
- WiFi devices (wireless access point/router): give wireless stations access to the wired network by sending and receiving radio signals; stations connect through it as through a bridge to the LAN.
- Comparison: switch works within one network by MAC address, router works between networks by IP address, WiFi device provides wireless access to the network.
- A home WiFi router usually combines router, switch and wireless access point in one box.

Q5(c)

- A network management system is the set of tools and stations used to monitor, control and maintain a network: checking which devices are up, watching traffic and faults, and changing device settings from one place.
- SNMP (Simple Network Management Protocol) is the example protocol used for this work at the application layer.
- Components: a manager (the management station software), agents (small software in each device such as a router or switch), and the managed information the agents keep about their device.
- Working: the manager asks (polls) agents for values such as interface status or traffic counters, and agents can also send an alert (trap) to the manager when a fault event occurs.
- Without such a system, an administrator would have to visit or log into every device separately to find a fault.

KAMALDNP • kamaldnp.com • support@kamaldnp.com • +91 8318013442 • Varanasi, UP
 Prepared by KAMALDNP Academy from the official BTEUP 2026-27 syllabus. This is a practice/model paper only.