



KAMALDNP

kamaldnp.com • IT Training, Varanasi

PDF created by Raj Kamal using AI

Short Notes — Advance Computer Networks

BTEUP Diploma in Computer Science & Engineering • 5th 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 notes cover **Advance Computer Networks**, a programme elective in the BTEUP 2026-27 fifth-semester scheme for Computer Science and Engineering — students choose either this subject or Information Security as one elective. In the 2026-27 scheme the subject is a **practicum**, so most marks come from practical work, but a clear theory base is still essential for the viva and for doing the practicals correctly.

Use the notes unit by unit: read the points, revise the one-line summary at the end, and try the likely question for each unit — including the worked subnetting example in Unit 1 — in your own words. Always match your final preparation with the official syllabus PDF and your lab records.

Unit 1 — Review of Networking Basics (10 Periods)

Topics: Advanced topics in IPv4 — subnetting, multicasting, multicast routing protocols (IGMP, PIM, DVMRP); advanced topics in TCP — flow management, congestion avoidance, protocol spoofing; IPv6.

Advanced topics in IPv4 — subnetting

Subnetting divides one IP network into smaller sub-networks by borrowing bits from the host part for the subnet part. It reduces broadcast traffic, improves organisation and security, and uses addresses efficiently.

Worked example: Divide **192.168.1.0/24** into 4 subnets.

Borrowed bits needed: 2, because $2^2 = 4$ subnets. New prefix = $24 + 2 = /26$, so the new mask is **255.255.255.192**. Host bits left = $32 - 26 = 6$, so addresses per subnet = $2^6 = 64$, and usable hosts = $64 - 2 = 62$ (excluding the network and broadcast addresses). Block size = 64, so the four subnets are:

- 192.168.1.0/26 — usable .1 to .62, broadcast .63
- 192.168.1.64/26 — usable .65 to .126, broadcast .127
- 192.168.1.128/26 — usable .129 to .190, broadcast .191
- 192.168.1.192/26 — usable .193 to .254, broadcast .255

Check: 4 subnets $\times$ 64 addresses = 256, exactly the original /24 — the maths balances.

Multicasting and multicast routing protocols — IGMP, PIM, DVMRP

Multicasting sends one stream from a source to a group of interested receivers at once — efficient for live video, online classes and stock tickers. Unlike broadcast, only group members receive it; unlike unicast, the sender does not send separate copies. Multicast uses Class D addresses (224.0.0.0 to 239.255.255.255).

Supporting protocols:

- **IGMP (Internet Group Management Protocol)** — works between hosts and their local router; hosts use it to join and leave multicast groups.
- **DVMRP (Distance Vector Multicast Routing Protocol)** — builds multicast delivery by flooding and then pruning branches with no members (source-based trees).
- **PIM (Protocol Independent Multicast)** — the widely used family; PIM-SM uses a shared rendezvous point, PIM-DM suits dense receiver populations. 'Independent' means it uses whatever unicast routing table already exists.

Exam line: IGMP manages membership at the edge; PIM and DVMRP route the multicast traffic across the network.

Advanced topics in TCP — flow management, congestion avoidance, protocol spoofing

At this advanced level, TCP study focuses on how it protects both the receiver and the network. **Flow management (flow control)** stops a fast sender overwhelming a slow receiver: the receiver advertises a window size saying how much buffer space it has, and the sender must stay within it.

Congestion avoidance protects the network itself. TCP starts cautiously (slow start), increases its sending window gradually while acknowledgements arrive cleanly, and cuts the window sharply when loss signals congestion — then grows again carefully. This add-a-little, cut-a-lot behaviour keeps shared links stable when many flows compete.

Protocol spoofing in this context means a device (commonly on satellite or WAN links) imitating the far endpoint locally — for example, acknowledging data on behalf of the distant receiver — to hide long delays from TCP and improve apparent performance. Note the term's other common meaning (faking addresses) belongs to security; here, be ready to explain the performance meaning asked in this syllabus, and mention the distinction in viva if asked.

IPv6

IPv6 is the successor to IPv4, created mainly because IPv4's 32-bit address space (about 4.3 billion addresses) ran out as devices multiplied. IPv6 uses **128-bit addresses**, giving an effectively unlimited supply, written in hexadecimal groups separated by colons, e.g. 2001:db8::1, where :: compresses consecutive zero groups.

Improvements beyond size:

- Simpler, fixed-format header — routers forward faster; extension headers carry optional features.
- No broadcast — replaced by efficient multicast and anycast.
- Built-in support for auto-configuration, so devices can obtain addresses with less manual setup, and for IPSec-based security.
- Better support for QoS labelling through the flow label field.

IPv4 and IPv6 co-exist during transition using dual stack (devices run both), tunnelling and translation techniques. Viva contrast: IPv4 = 32-bit, dotted decimal, broadcast exists; IPv6 = 128-bit, hexadecimal, no broadcast, vastly larger space.

Likely question: A network 192.168.1.0/24 must be divided into 4 subnets. Find the new subnet mask, the subnets and the usable hosts per subnet. Also explain the need for IPv6.

Unit 2 — Telecom Networks, Switching Techniques (10 Periods)

Topics: Introduction to Frame Relay, ATM, MPLS; VSAT communication — star and mesh architectures, bandwidth reservation; wireless networks — WiFi, WiMax; cellular phone technologies — GSM, CDMA, 3G, 4G.

Frame Relay, ATM and MPLS

These three are WAN technologies for carrying data between sites, in historical order.

- **Frame Relay** — a packet-switched WAN service using virtual circuits over shared carrier networks. It trimmed error checking (relying on modern reliable lines and end systems) to cut cost and delay, and was widely used to connect branch offices at committed data rates.
- **ATM (Asynchronous Transfer Mode)** — divides all traffic into small, fixed-size 53-byte **cells** and switches them at high speed. Fixed cells make hardware switching fast and timing predictable, suiting combined voice, video and data with QoS classes.

- **MPLS (Multi-Protocol Label Switching)** — forwards packets by short **labels** instead of long address lookups. Ingress routers attach a label; core routers switch by label along pre-set paths (LSPs). MPLS enables traffic engineering and fast VPN services and remains widely used in provider networks.

One-line comparison: Frame Relay = variable frames on virtual circuits; ATM = fixed cells; MPLS = label-based fast forwarding.

VSAT communication — star and mesh architectures, bandwidth reservation

VSAT (Very Small Aperture Terminal) communication uses small satellite dish terminals to connect remote sites — banks, petrol pumps, rural offices — where terrestrial lines are unavailable. A large central **hub** station coordinates the network.

- **Star architecture** — every remote communicates only through the hub. Remote-to-remote traffic makes two satellite hops (remote → hub → remote), adding delay, but control and management are simple and centralised. This is the most common VSAT design.
- **Mesh architecture** — remotes communicate **directly** with each other in one hop, halving delay for remote-to-remote voice/data, but terminals and management become more complex and costly.

Bandwidth reservation: in shared satellite systems, bandwidth is a scarce, costly resource. Reservation means guaranteeing an agreed share (a committed rate) to a site or application — for example through assigned time slots or demand-assigned schemes — so critical traffic is not starved when the link is busy.

Wireless networks — WiFi and WiMax

WiFi is wireless LAN technology (IEEE 802.11 family) giving short-range, high-speed access inside homes, offices and campuses through access points. It is designed for local coverage — typically tens of metres — with many generations improving speed and capacity.

WiMax (IEEE 802.16 family) was designed as wireless broadband for a much larger area — a metropolitan scale, covering kilometres from one base station — to deliver internet access to whole localities, including places without wired broadband (the 'last mile' problem).

Exam differentiation:

- Coverage: WiFi = local area; WiMax = metropolitan area.
- Typical use: WiFi connects devices inside a premises; WiMax was meant to connect premises and areas to the provider.
- Licensing/design: WiFi works mainly in unlicensed bands for LANs; WiMax was designed for carrier deployment with scheduled, QoS-managed access.

In practice WiFi became universal indoors while mobile 4G largely took the wide-area role WiMax aimed at.

Cellular phone technologies — GSM, CDMA, 3G and 4G

Cellular systems divide an area into cells, each served by a base station, reusing frequencies across distant cells.

- **GSM** — the dominant 2G digital standard: TDMA-based, SIM-card identity, voice plus basic data (with GPRS/EDGE as data enhancements).
- **CDMA** — the rival 2G family in which all users share the same frequency, separated by unique codes; known for good voice quality and soft handovers between cells.
- **3G** — the generation built for mobile data as well as voice: packet data, video calling and practical mobile internet at megabit-class rates (UMTS/HSPA families).
- **4G** — an all-IP generation (LTE family): much higher data rates, low delay, designed for smartphones, streaming and apps; voice itself is carried as data (VoLTE).

Trend for viva: each generation mainly raises data capability — 2G digitised voice, 3G added real data, 4G made the network all-IP and broadband.

Likely question: Describe briefly Frame Relay, ATM and MPLS. Differentiate between star and mesh architectures in VSAT communication.

Unit 3 — QoS (6 Periods)

Topics: Network redundancy; load balancers; caching; storage networks; QoS; network monitoring — SNMP, RMON.

Network redundancy and load balancers

Network redundancy means providing backup paths, links or devices so the network keeps working when one element fails — duplicate uplinks, a second router, or an alternate route that routing protocols switch to automatically. Redundancy costs extra but converts failures from outages into brief interruptions.

A **load balancer** distributes incoming requests across several servers (or traffic across several links) so no single server is overloaded. Benefits:

- Better response time by using all servers evenly — common methods include round robin and least connections.
- Higher availability: if a health check finds a server down, the balancer stops sending it traffic.
- Easier maintenance: a server can be taken out of rotation, serviced and returned without downtime.

Together: redundancy protects against failure of components, load balancing protects against overload of components — both serve the same goal of continuous, responsive service.

Caching and storage networks

Caching stores copies of frequently requested content close to the user — in a browser, a proxy, or a content-delivery server. The next request is served from the nearby copy, cutting delay, saving WAN bandwidth and reducing load on the origin server. The design problem is freshness: policies must decide how long a copy stays valid and when to fetch a new one.

Storage networks connect servers to shared, centralised storage over a network instead of disks inside each server. The classic form is a **SAN (Storage Area Network)** — a dedicated high-speed network giving block-level storage access — while **NAS (Network Attached Storage)** shares files over the ordinary data network. Central storage simplifies backup, sharing and expansion: many servers can use one managed storage pool, and a failed server can be replaced without losing its data.

Connect the two ideas: caching moves copies of hot data near users for speed; storage networks centralise the master data for control.

QoS — Quality of Service

QoS (Quality of Service) is the set of techniques that manage network resources so important traffic gets the treatment it needs. It matters because not all traffic is equal: a voice call is ruined by delay and jitter (variation in delay), while a file download only cares about total throughput.

QoS parameters to define: **bandwidth, delay (latency), jitter** and **packet loss**.

How QoS is achieved:

- **Classification and marking** — traffic is identified (voice, video, bulk) and marked, e.g. with DSCP values.
- **Queuing and scheduling** — routers give priority queues to delay-sensitive classes when links are congested.
- **Policing and shaping** — limit or smooth traffic that exceeds its agreed rate.
- **Admission/reservation** — reserve resources for critical flows where the design supports it.

Without QoS, one large download can starve a live class or call on the same link; with QoS, the network degrades bulk traffic first and protects real-time communication.

Network monitoring — SNMP and RMON

Network monitoring means continuously observing devices and traffic so faults, overloads and attacks are detected early. Two standard tools are named in the syllabus:

- **SNMP (Simple Network Management Protocol)** — the standard management framework. A manager program polls **agents** running on routers, switches and servers for values stored in a Management Information Base (MIB) — interface traffic, errors, CPU, status — and can also set some values. Devices can send unsolicited **traps** to the manager when important events occur, such as a link going down.

- **RMON (Remote Network Monitoring)** — extends monitoring to whole LAN segments: an RMON probe collects statistics, history, alarms and top-talker information locally and reports summaries, so the manager need not pull raw traffic across the network.

One-line difference: SNMP manages and polls individual devices; RMON watches network segments and their traffic behaviour.

Likely question: What is QoS and why is it needed? Explain the roles of load balancers, caching and SNMP in improving network service.

Unit 4 — Introduction to Network Security (8 Periods)

Topics: VLAN, VPN, firewall, IPS, proxy servers.

VLAN and VPN

A **VLAN (Virtual LAN)** divides one physical LAN into several separate logical networks using switch configuration. Devices in different VLANs cannot communicate directly even on the same switch — traffic must pass through a router or Layer-3 switch, where rules can be applied. Benefits: better security and isolation between departments, smaller broadcast domains, and flexible grouping independent of physical location.

A **VPN (Virtual Private Network)** creates a private, encrypted **tunnel** across a public network such as the internet. Remote users and branch offices connect through the tunnel so their data is protected as if on a private line: encryption gives privacy, and authentication controls who may connect.

Clear difference for the exam: a VLAN segments a network **inside** a site for organisation and isolation; a VPN securely **connects** users or sites across an untrusted network. They often work together — a VPN user may be placed into a specific VLAN on arrival.

Firewall, IPS and proxy servers

A **firewall** enforces a security policy on traffic entering and leaving a network, examining addresses, ports, protocols and connection state, and allowing or blocking packets by its rule set (deny by default). It is the basic boundary guard of a network.

An **IPS (Intrusion Prevention System)** inspects traffic content for known attack patterns and suspicious behaviour and actively **blocks** attacks in real time — dropping packets, resetting connections or blocking the source. Unlike a firewall's rule-based filtering of traffic types, the IPS recognises attacks within traffic that may use allowed ports.

A **proxy server** acts as an intermediary: clients ask the proxy, and the proxy makes requests on their behalf. This hides internal addresses, lets the organisation filter and log web access, enforce policy, and cache popular content for speed (linking back to Unit 3 caching).

Combined defence: firewall decides what may pass, IPS checks what passes for attacks, proxy controls and records application-level access — layered security, or defence in depth.

Likely question: Differentiate between VLAN and VPN. Explain the functions of a firewall, an IPS and a proxy server.

Unit 5 — Network Simulation (8 Periods)

Topics: Network simulation; network design case studies and exercises; IP addressing schema; protocol analysers (Wireshark, etc.).

Network simulation

Network simulation means building a software model of a network — its topology, devices, links, protocols and traffic — and running experiments on the model instead of the real network. Simulators let a designer change one factor at a time (link speed, number of users, routing choice) and measure the effect on delay, throughput and loss.

Why it is used:

- Testing a design before spending on equipment and installation.
- Studying situations that are hard or risky to create live — link failures, overloads, attacks.
- Training and viva-style understanding: students can observe protocol behaviour step by step.
- Comparing alternatives fairly under identical simulated traffic.

Limitation to state honestly: a simulation is only as good as its model and assumptions, so key results are finally confirmed on a test setup or pilot before full deployment.

Network design case studies and exercises — IP addressing schema

Network design case studies and exercises in this unit mean applying the whole subject to realistic briefs — for example, designing the network for a campus, office or multi-branch organisation. A sound exercise follows fixed steps: gather requirements (users, applications, sites), draw the topology, choose devices and technologies, plan redundancy and security, estimate capacity, and document the design.

The **IP addressing schema** is the documented plan of which address blocks each part receives. A good schema:

- Uses private address ranges internally, organised hierarchically (site → department → subnet), applying subnetting as in Unit 1.
- Keeps blocks contiguous so routing tables stay small (route summarisation).
- Reserves space for growth and separates ranges for servers, users, guests and management.

- Is written down in a table — network address, mask, gateway, purpose — so any engineer can understand and maintain it.

A clear addressing schema prevents conflicts, eases troubleshooting and makes later expansion orderly rather than chaotic.

Protocol analysers — Wireshark, etc.

Protocol analysers capture and decode the actual packets travelling on a network so engineers can see exactly what the protocols are doing. **Wireshark** is the best-known example: free, widely used, and able to decode hundreds of protocols.

Typical uses in practical work:

- Capturing traffic on an interface and filtering by protocol, address or port to isolate one conversation.
- Following a TCP stream to check handshakes, retransmissions and window behaviour studied in Unit 1.
- Finding faults — repeated requests with no reply, wrong addresses, excessive broadcasts — and measuring delays between packets.

Working cautions: capture only on networks you are authorised to examine (captured packets can contain private data), and use display filters to manage the huge volume of traffic on a busy link. In viva, summarise: simulation predicts behaviour before building; a protocol analyser reveals behaviour on the real network after building.

Likely question: What is network simulation and why is it used in network design? Describe the use of a protocol analyser such as Wireshark.

Quick Revision — One Line Each

- Subnetting borrows host bits for subnets: /24 borrowed by 2 bits gives /26, 4 subnets, 62 usable hosts each.
- Multicast sends one stream efficiently to a group; IGMP manages group membership on the local network.
- TCP congestion control: slow start, then careful growth; a drop in acknowledgements means slow down.
- IPv6 uses 128-bit addresses, written in hexadecimal groups — no address shortage, simpler header.
- Frame Relay and ATM are older WAN technologies; MPLS forwards by short labels and is still widely used.
- VSAT star: all traffic via the hub; mesh: remotes talk directly, saving a satellite hop.
- WiFi is local-area wireless; WiMax was designed for larger, metropolitan-range wireless access.
- QoS prioritises delay-sensitive traffic (voice/video) over bulk traffic such as downloads.

- SNMP lets a manager poll and configure devices; RMON adds remote traffic statistics and alarms.
- VLAN = logical segmentation; VPN = encrypted tunnel; proxy = intermediary that can filter and cache.
- A load balancer spreads requests across servers; redundancy ensures a backup path or device exists.
- Wireshark captures packets so protocol behaviour, errors and delays can be inspected frame by frame.

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.

