

Advance Computer Network (315321)

Model Question Paper — Set B · Model Answers

Q.1

a) Subnet mask; default masks

2 M

Subnet mask: a 32-bit number that has 1s in the network (and subnet) part and 0s in the host part of an IP address. ANDing an IP address with the mask gives the network / subnet address.

Class	Default mask	Prefix
A	255.0.0.0	/8
B	255.255.0.0	/16
C	255.255.255.0	/24

(Definition 1 M, default masks 1 M)

b) Purpose of queuing in routers

2 M

1. Packets may arrive faster than the switching fabric or the output link can handle; **queues (buffers)** at input and output ports hold them temporarily instead of dropping them.
2. They absorb short bursts of traffic and smooth the flow.
3. Queue scheduling (FIFO, priority, weighted fair queuing) gives better service (QoS) to important traffic such as voice.
4. When a queue becomes full, packets are dropped — this signals congestion to TCP.

(Any two points, 1 M each)

c) Well-known UDP ports

2 M

Port	Protocol
7	Echo
13	Daytime
53	DNS (Domain Name System)
67 / 68	BOOTP / DHCP server / client
69	TFTP
123	NTP
161 / 162	SNMP / SNMP trap
520	RIP

(Any four, ½ M each)

d) Role of SMTP

2 M

- SMTP (Simple Mail Transfer Protocol) is the **message transfer agent (MTA)** protocol of the Internet: it **pushes** mail from the sender's user agent to the sender's mail server and from that

server to the receiver's mail server.

- It uses TCP port 25 and works in three phases — connection establishment, mail transfer (MAIL FROM, RCPT TO, DATA) and connection termination (QUIT).
- SMTP is used only for sending/relaying; the receiver pulls mail with POP3 or IMAP4.

(Role 2 M)

e) TTL and Protocol fields of IPv4

2 M

TTL (Time to live, 8 bits): limits the number of hops a datagram can travel. Each router decrements it by 1; when it reaches 0 the datagram is discarded (and an ICMP time-exceeded message is sent). It prevents datagrams from looping forever.

Protocol (8 bits): identifies the higher-level protocol whose data is carried, so the destination can hand the data to it: 1 = ICMP, 2 = IGMP, 6 = TCP, 17 = UDP, 89 = OSPF.

(Each field 1 M)

f) Applications of SDN

2 M

1. Data-centre and cloud networks (fast provisioning of virtual networks).
2. Traffic engineering and load balancing.
3. Network security — central firewall policies, DDoS detection and mitigation.
4. SD-WAN connecting branch offices.
5. Network slicing in 5G mobile networks.
6. Campus / enterprise network management and monitoring.

(Any four, ½ M each)

g) Transmission modes of FTP

2 M

1. **Stream mode** (default): data delivered as a continuous stream of bytes; end of file shown by closing the data connection.
2. **Block mode:** data sent in blocks, each preceded by a 3-byte header (descriptor + block size).
3. **Compressed mode:** repeated data is compressed (run-length encoding) before sending.

(Three modes; 2 M)

Q.2

a) Working of TLS

4 M

TLS (Transport Layer Security), the successor of SSL, works between the application layer (e.g. HTTP) and TCP and provides **confidentiality** (symmetric encryption), **integrity** (MAC) and **server authentication** (certificates).

1. **Handshake protocol:** client and server agree on the TLS version and cipher suite, the server sends its certificate, the client verifies it and both derive the same session keys (see figure).
2. **ChangeCipherSpec:** both sides switch to the negotiated keys and algorithms.
3. **Record protocol:** application data is fragmented, optionally compressed, a MAC is added and it is encrypted before giving it to TCP.
4. **Alert protocol:** reports errors and closes the connection safely.

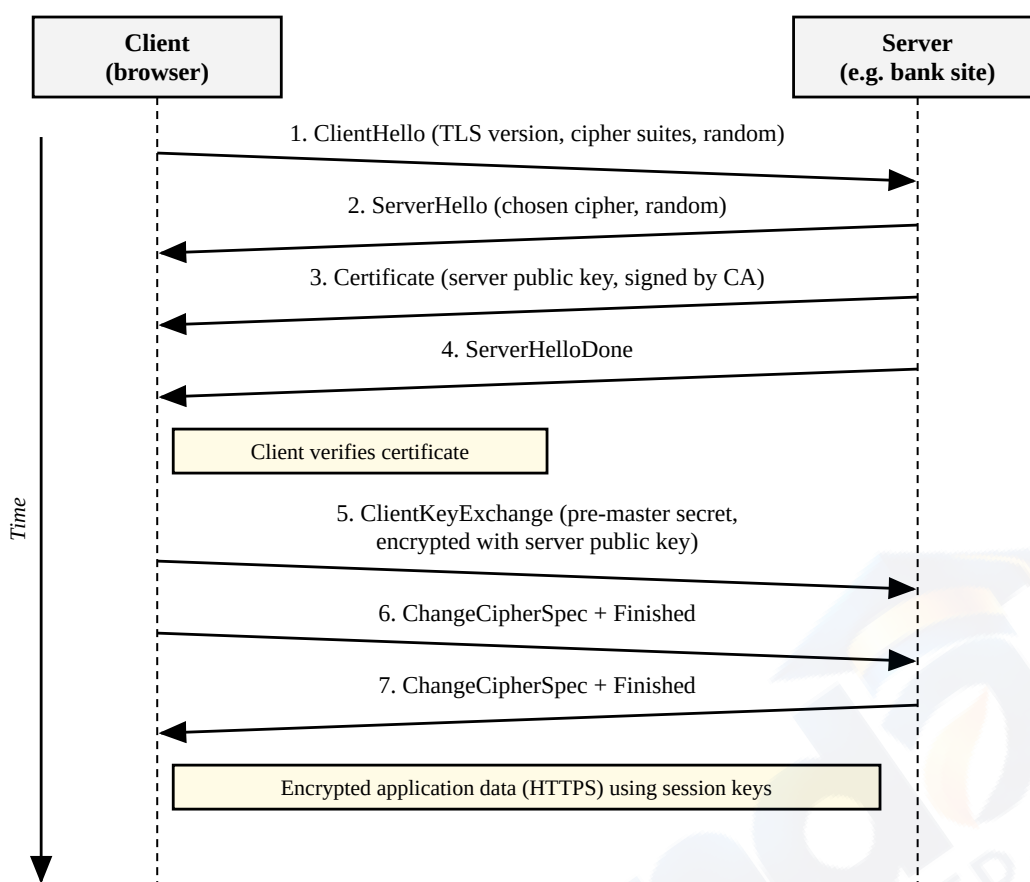


Fig.: TLS handshake (simplified)

Applications: HTTPS (secure web, online banking, e-commerce), secure e-mail (SMTPS, IMAPS, POP3S), SSL/TLS VPNs, secure VoIP signalling (SIP over TLS).

(Working with diagram 3 M, applications 1 M)

b) Inter-domain routing; path vector routing; BGP functions

4 M

Inter-domain routing is routing **between autonomous systems (ASes)**, i.e. between networks under different administrations (ISPs). (Routing inside one AS is intra-domain routing — RIP, OSPF.)

Path vector routing: each AS has a speaker node that advertises to neighbouring ASes the **complete path (list of AS numbers)** to each destination, not just a cost. A router rejects a path that already contains its own AS number (loop prevention) and selects a path according to its own **policy**.

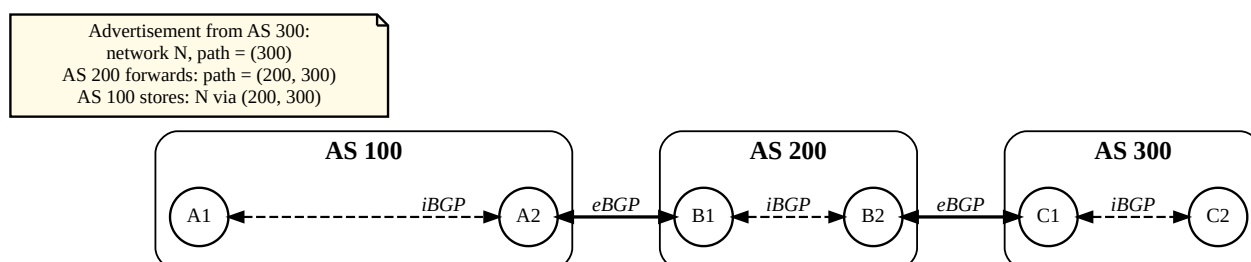


Fig.: Path vector routing with BGP between autonomous systems

Functions of BGP (BGPv4):

1. Exchanges network reachability information between ASes (eBGP) and distributes it inside the AS (iBGP).
2. Uses path vector routing — loop-free, policy-based route selection using attributes such as AS-PATH, NEXT-HOP, LOCAL-PREF.
3. Uses reliable TCP sessions (port 179) with OPEN, UPDATE, KEEPALIVE and NOTIFICATION messages; sends only incremental updates.
4. Supports CIDR and route aggregation, keeping Internet routing tables small.

(Definition 1 M, path vector 1 M, functions 2 M)

c) ARP packet format; ARP vs RARP

4 M

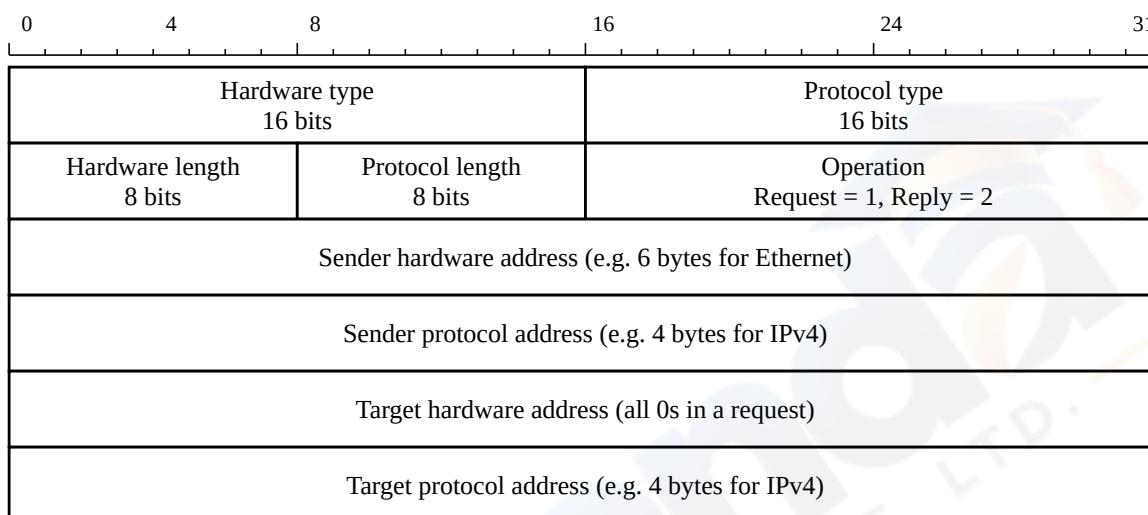


Fig.: ARP packet format

- **Hardware type (16):** type of network, 1 = Ethernet. **Protocol type (16):** 0x0800 for IPv4.
- **Hardware length (8):** length of physical address, 6 for Ethernet. **Protocol length (8):** 4 for IPv4.
- **Operation (16):** 1 = ARP request, 2 = ARP reply.
- **Sender / target hardware and protocol addresses:** physical and logical addresses of sender and target; target hardware address is all 0s in a request.

Sr.	Parameter	ARP	RARP
1	Mapping	Logical (IP) → physical (MAC).	Physical (MAC) → logical (IP).
2	Used by	Any host / router that knows the IP of the next hop.	Diskless machine at boot time that knows only its MAC.
3	Reply sent by	The target host itself.	A RARP server on the network.
4	Status	In use today.	Obsolete; replaced by BOOTP / DHCP.

(Format 2 M, two differences 2 M)

d) TCP segment structure

4 M

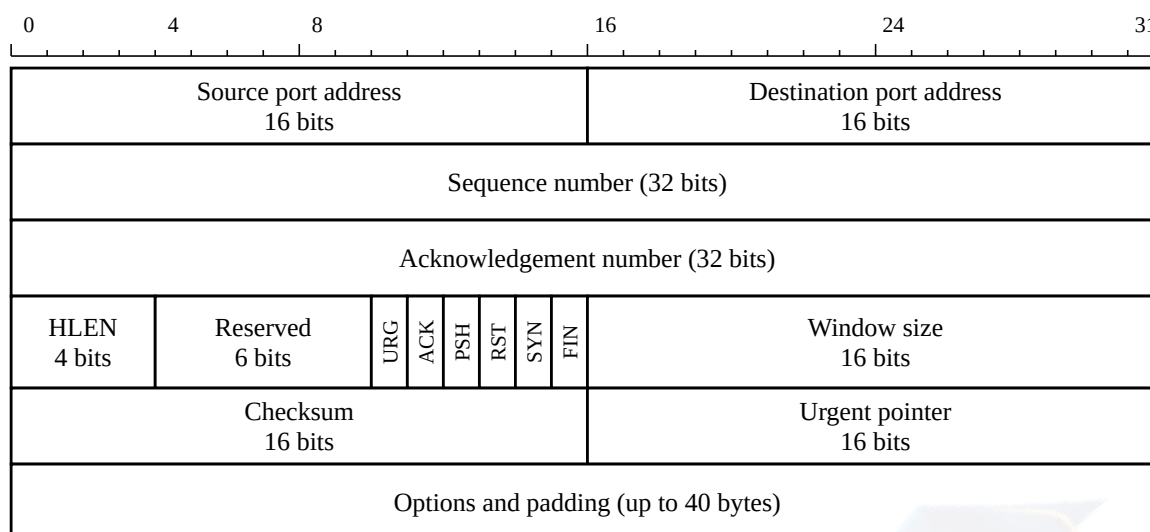


Fig.: TCP segment header format (20 – 60 bytes)

- **Source / destination port (16 bits each):** identify sending and receiving processes.
- **Sequence number (32):** number of the first byte of data in this segment. **Acknowledgement number (32):** next byte expected from the other side.
- **HLEN (4):** header length in 4-byte words (5 – 15, i.e. 20 – 60 bytes). **Reserved (6)** for future use.
- **Control flags:** URG (urgent pointer valid), ACK (ack number valid), PSH (push data), RST (reset connection), SYN (synchronize sequence numbers), FIN (terminate connection).
- **Window size (16):** receiver window (rwnd) in bytes for flow control (max 65,535).
- **Checksum (16):** mandatory error check over pseudo-header, header and data. **Urgent pointer (16):** end of urgent data when URG = 1.
- **Options:** up to 40 bytes, e.g. MSS, window scale, timestamp, SACK.

(Diagram 2 M, fields 2 M)

Q.3

a) Static vs dynamic routing

4 M

Sr.	Parameter	Static routing	Dynamic routing
1	Configuration	Routes are entered manually by the administrator (e.g. <i>ip route</i> command).	Routes are learnt and updated automatically by routing protocols.
2	Security	More secure — no routing updates are advertised.	Less secure — updates can be spoofed; needs authentication.
3	Cost	No extra CPU, memory or bandwidth, but high administrative effort in large networks.	Uses router CPU, memory and link bandwidth for updates; low administrative effort.
4	Routing protocols	None used.	RIP, OSPF, EIGRP, BGP.

5	Adaptability / use	Does not adapt to link failure; suitable for small, stable networks.	Adapts to topology changes; suitable for large networks.
---	--------------------	--	--

(Four points, 1 M each)

b) TCP congestion control

4 M

TCP keeps a **congestion window (cwnd)**; actual window = $\min(\text{rwnd}, \text{cwnd})$. The policy has three phases:

1. **Slow start (exponential increase)**: cwnd starts at 1 MSS and increases by 1 MSS for every ACK, so it **doubles every RTT**, until it reaches the threshold **ssthresh**.
2. **Congestion avoidance (additive increase)**: after ssthresh, cwnd increases by only 1 MSS per RTT.
3. **Congestion detection (multiplicative decrease)**: on a **time-out**, $\text{ssthresh} = \text{cwnd} / 2$, $\text{cwnd} = 1$ and slow start begins again; on **3 duplicate ACKs**, $\text{ssthresh} = \text{cwnd} / 2$ and $\text{cwnd} = \text{ssthresh}$ (fast recovery).

Example (ssthresh = 16, time-out in round 10 when cwnd = 22 → new ssthresh = 11):

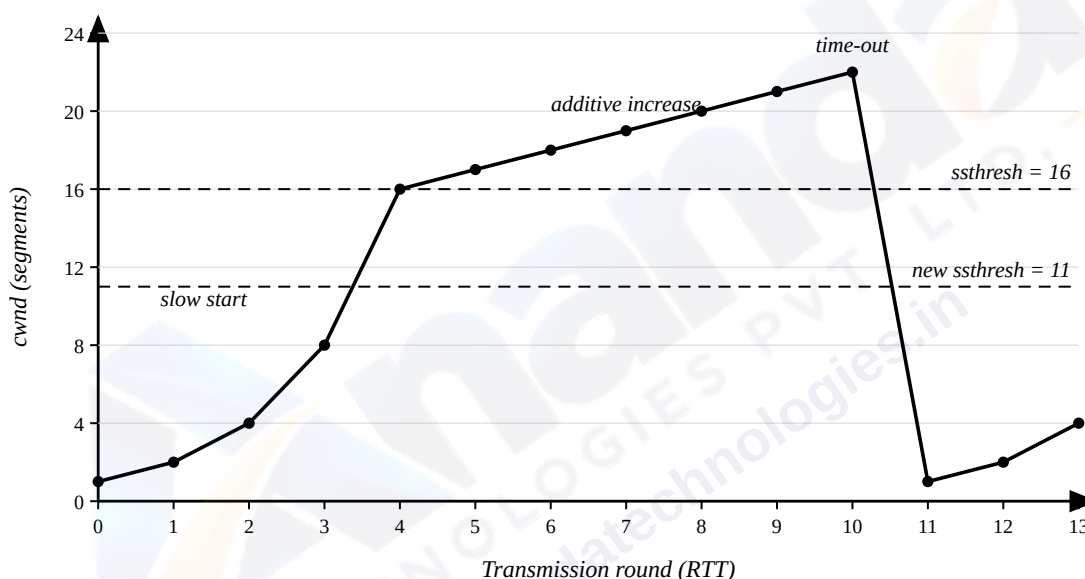


Fig.: Congestion window — slow start, congestion avoidance, time-out

Round	0	1	2	3	4	5	6	7	8	9	10	11	12	13
cwnd	1	2	4	8	16	17	18	19	20	21	22	1	2	4

(Three phases 3 M, graph 1 M)

c) IMAP4 and comparison with POP3

4 M

IMAP4 (Internet Mail Access Protocol version 4) is a message-access protocol (TCP port 143) that lets a user manage mail **on the mail server**. It is more powerful than POP3: a user can check e-mail headers before downloading, search mail on the server, download part of a mail (e.g. skip large attachments), and create, delete or rename mailboxes / folders on the server.

Sr.	Parameter	POP3	IMAP4
1	Port	TCP 110 (995 with TLS).	TCP 143 (993 with TLS).

2	Where mail stays	Usually downloaded and deleted from server (delete mode).	Kept on the server; client works on server copy.
3	Multiple devices	Not suitable — mail ends up on one device.	Synchronized view on all devices.
4	Folders / search	No server-side folders or search.	Folders, search and partial download on server.
5	Complexity	Simple, needs less server storage.	More complex, needs more server storage.

(IMAP explanation 2 M, any four differences 2 M)

d) Role of RTSP in streaming

4 M

RTSP (Real-Time Streaming Protocol) is an application-layer **control protocol** — a "network remote control" for multimedia servers. It does not carry the media itself (that is done by RTP over UDP); it carries control commands **out-of-band** (TCP port 554).

1. Browser gets a **metafile** (address and type of the audio/video) from the web server with HTTP GET.
2. Browser passes the metafile to the **media player**.
3. Media player sends **SETUP** to the media server; server replies with session information.
4. **PLAY** starts the stream; media flows as RTP packets.
5. **PAUSE** stops temporarily; **TEARDOWN** ends the session.

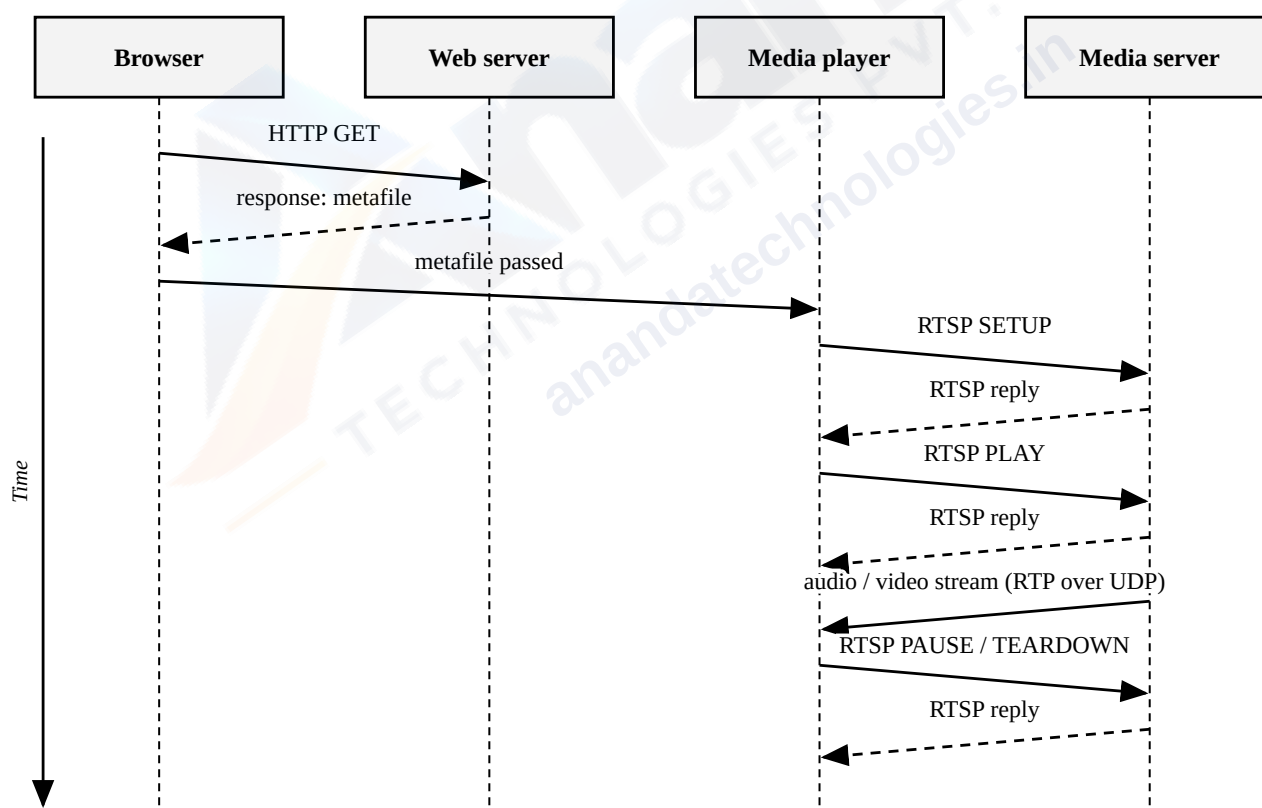


Fig.: Streaming with RTSP — web server, media player and media server

Role: gives VCR-like control (play, pause, seek, stop) over streamed audio/video and manages streaming sessions.

Q.4

a) Supernetting with example

4 M

Supernetting is combining several contiguous smaller networks (e.g. class C blocks) into one larger block by **shortening the mask** (moving bits from the network part to the host part). It reduces routing-table entries (route aggregation) and is the basis of CIDR.

Conditions: number of blocks must be a power of 2; blocks must be contiguous; the third octet of the first block must be divisible by the number of blocks.

Example: 4 blocks = $2^2 \rightarrow$ 2 bits removed from the /24 mask $\rightarrow$ /22. Third octet 16 is divisible by 4 ✓.

Network	3rd octet (binary)
200.10.16.0	00010000
200.10.17.0	00010001
200.10.18.0	00010010
200.10.19.0	00010011

The first 6 bits of the third octet (000100) are common, so prefix = 16 + 6 = 22.

Supernet: 200.10.16.0/22 · Supernet mask: 255.255.252.0 · Range: 200.10.16.0 to 200.10.19.255 (1024 addresses). The router advertises one entry instead of four.

(Definition 1 M, conditions 1 M, example 2 M)

b) Components of a router

4 M

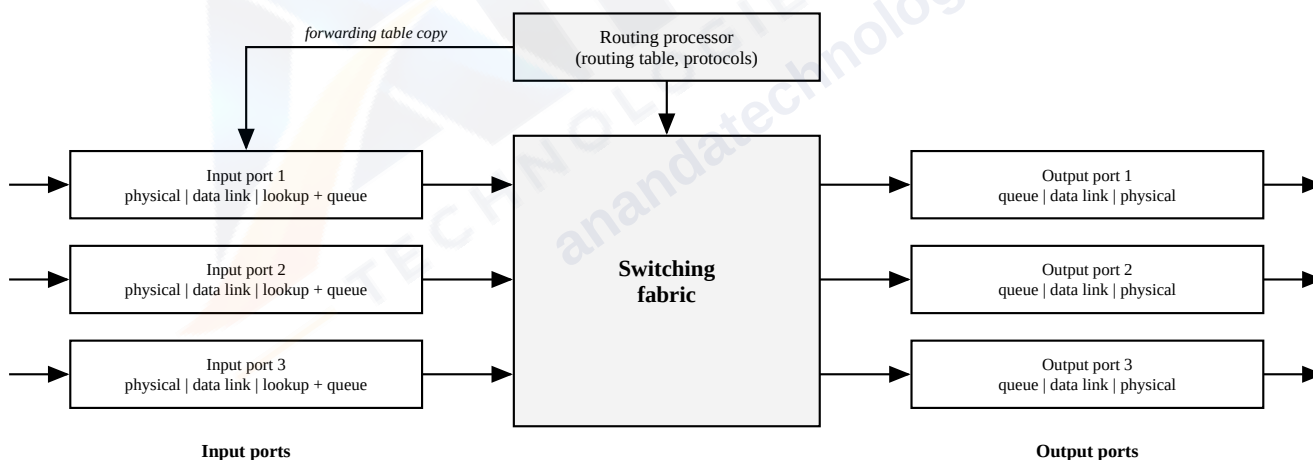


Fig.: Components of a router

- 1. Input ports:** perform physical and data-link layer functions (receive bits, decapsulate frame), look up the destination in the forwarding table and queue the packet until the fabric can accept it.
- 2. Switching fabric:** moves packets from input queue to the proper output queue — crossbar, banyan / Batcher-banyan, memory or bus type. Its speed decides router throughput.

3. **Output ports:** queue outgoing packets, encapsulate them in frames and transmit on the link; scheduling decides which packet goes first.
4. **Routing processor:** runs routing protocols (RIP, OSPF, BGP), builds the routing table and copies the forwarding table to input ports.

(Diagram 2 M, explanation 2 M)

c) HTTP request and response formats

4 M

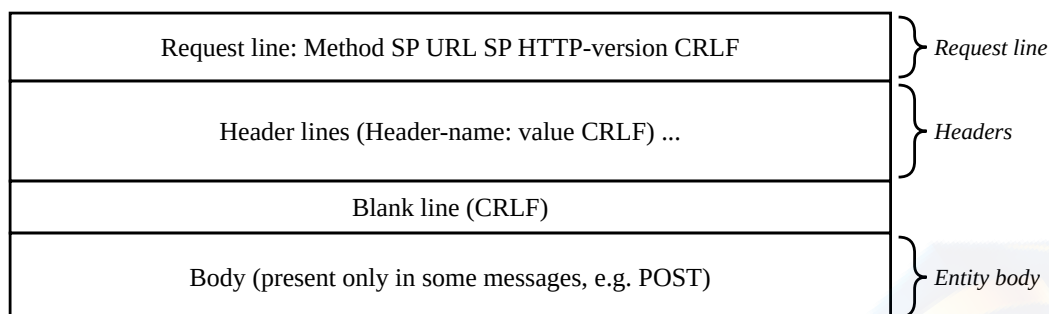


Fig.: HTTP request message format

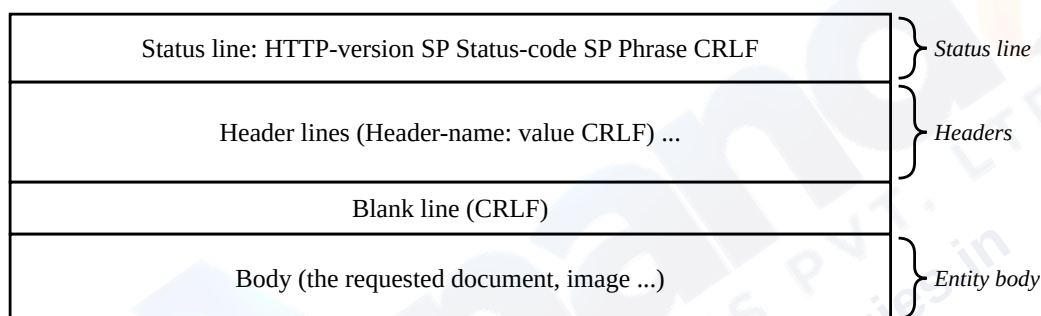


Fig.: HTTP response message format

- **Request line:** method (GET, POST, HEAD, PUT, DELETE), URL and HTTP version.
- **Status line:** HTTP version, status code and phrase — 1xx informational, 2xx success (200 OK), 3xx redirection (301), 4xx client error (404 Not Found), 5xx server error (500).
- **Header lines:** name: value pairs — request: Host, User-Agent, Accept; response: Date, Server, Content-Type, Content-Length.
- A **blank line** ends the headers, followed by the optional **body**.

<pre>GET /index.html HTTP/1.1 Host: www.abc.com Accept: text/html</pre>	<pre>HTTP/1.1 200 OK Content-Type: text/html Content-Length: 1532 <html> ... </html></pre>
---	---

(Request format 2 M, response format 2 M)

d) Edge computing — components and challenges

4 M

Edge computing processes data **near its source** (at the network edge) instead of sending everything to a distant cloud, giving low latency, less bandwidth use and better privacy.

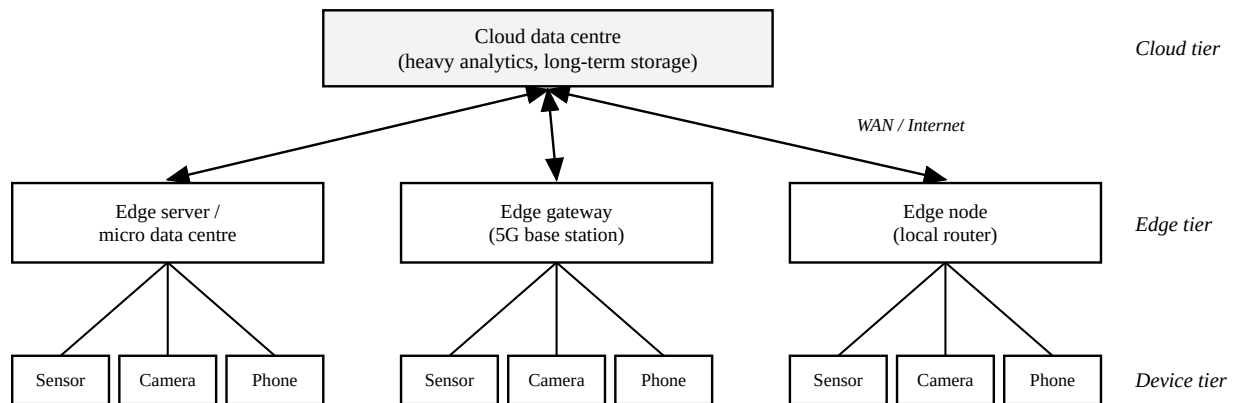


Fig.: Edge computing — cloud tier, edge tier and device tier (processing near the data source gives low latency)

Components: edge devices (IoT sensors, cameras, phones), edge nodes / gateways, edge servers or micro data centres, the network (5G, Wi-Fi, LAN), the central cloud, and management/orchestration software.

Challenges:

1. **Security and privacy** — many distributed nodes in exposed locations are easier to attack.
2. **Limited resources** — edge nodes have less computing power, storage and energy than cloud servers.
3. **Management and orchestration** of thousands of heterogeneous nodes; software updates and monitoring.
4. **Interoperability and standards**, connectivity / reliability and keeping data consistent with the cloud.

(Components 1 M, three challenges 3 M)

e) Flow control and error control in SCTP

4 M

Flow control: SCTP uses a window-based scheme similar to TCP, but data is carried in DATA chunks numbered by TSN.

- The receiver keeps a receive buffer and advertises its free space as **rwnd** (a_rwnd) in every SACK chunk.
- The sender keeps *rwnd* and *inTransit* (bytes sent but not acknowledged); it can send a chunk only if its size $\leq$ *rwnd* – *inTransit*.
- As SACKs arrive, *inTransit* decreases and the window opens again.

Error control:

- Every DATA chunk has a **TSN**; the receiver sends **SACK** chunks containing the cumulative TSN acknowledged, **gap blocks** (out-of-order chunks received) and duplicate TSNs.
- The sender retransmits a chunk when its **retransmission timer expires** or when SACKs repeatedly report it missing (fast retransmission).
- Checksum (CRC-32c) detects corrupted packets, which are discarded.

(Flow control 2 M, error control 2 M)

Q.5

a) IPv6 base header

6 M

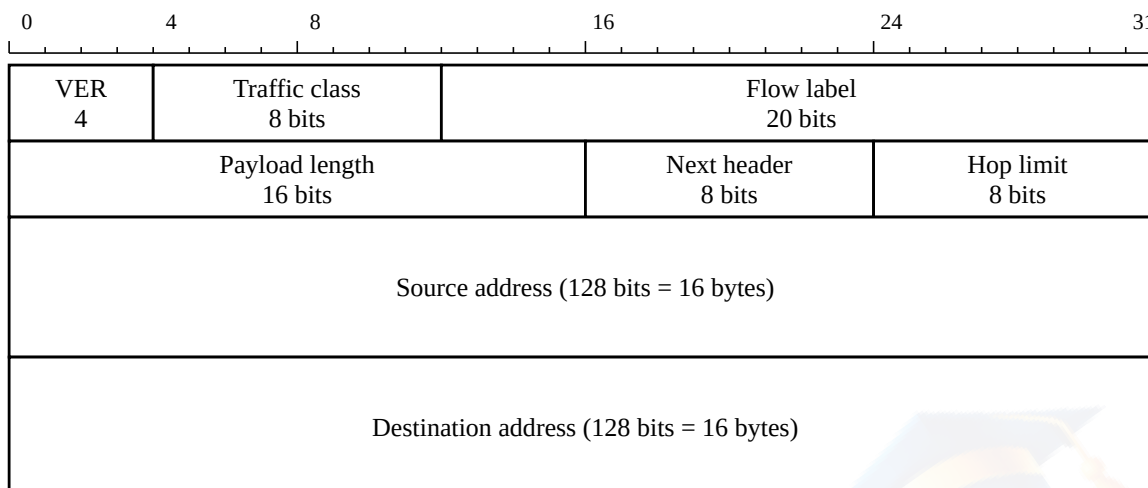


Fig.: IPv6 base header (40 bytes)

- Version (4 bits):** 6 for IPv6.
- Traffic class (8 bits):** priority / class of service of the packet (like DSCP in IPv4).
- Flow label (20 bits):** identifies a flow (sequence of packets) needing special handling, e.g. real-time audio/video.
- Payload length (16 bits):** length of data after the 40-byte base header (extension headers + upper-layer data).
- Next header (8 bits):** type of the header that follows — an extension header or upper-layer protocol (6 = TCP, 17 = UDP, 58 = ICMPv6).
- Hop limit (8 bits):** same purpose as TTL in IPv4; decremented at each router, packet discarded at 0.
- Source address and destination address (128 bits each).**

Extension headers: Hop-by-hop options, Routing, Fragment, Authentication (AH), Encapsulating Security Payload (ESP), Destination options.

(Diagram 2 M, fields 3 M, extension headers 1 M)

b) Wireless networks — types, working, benefits

6 M

A **wireless network** connects devices using radio (or infrared) waves instead of cables.

i) Types:

Type	Range	Standard / example
WPAN — wireless personal area network	about 10 m	Bluetooth, Zigbee
WLAN — wireless LAN	about 100 m	Wi-Fi (IEEE 802.11)
WMAN — wireless metropolitan area network	a city	WiMAX (IEEE 802.16)
WWAN — wireless wide area network	country / world	Cellular 3G / 4G / 5G, satellite

WLANs work in **infrastructure mode** (stations talk through an access point) or **ad-hoc mode** (stations talk directly).

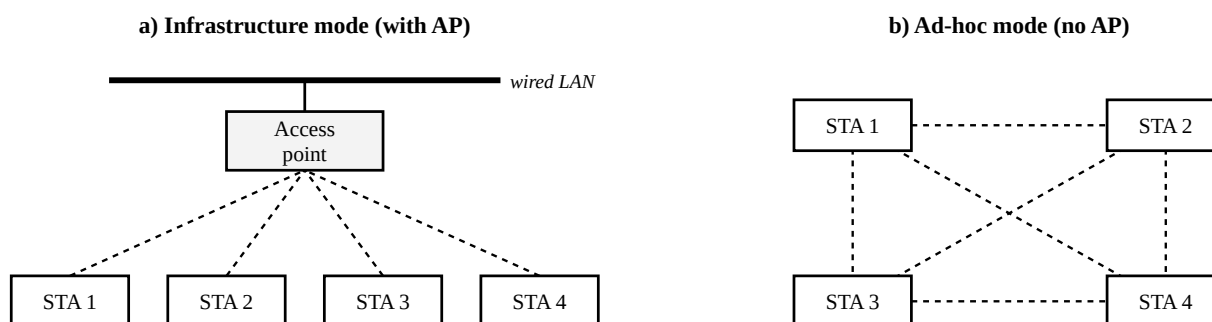


Fig.: Wireless LAN — infrastructure mode (BSS) and ad-hoc mode (IBSS)

ii) Working:

1. The wireless NIC converts data into radio signals and transmits them through its antenna.
2. An access point (or base station) broadcasts its SSID; a station associates with it after authentication (WPA2 / WPA3).
3. Stations share the channel using CSMA/CA (Wi-Fi) or scheduled access (cellular).
4. The AP / base station forwards frames to the wired network or Internet and back.

iii) Benefits: mobility, easy and fast installation without cabling, scalability (add users easily), lower installation cost, access in places where cabling is difficult, flexibility for IoT and mobile devices.

(Types 2 M, working 2 M, benefits 2 M)

c) DNS — name space, domains, name resolution

6 M

DNS (Domain Name System) maps human-friendly host names to IP addresses using a distributed, hierarchical database (UDP / TCP port 53).

i) Domain name space: an inverted tree with the unnamed root at the top and at most 128 levels; each node has a label of up to 63 characters; a fully qualified domain name (FQDN) ends with a dot, e.g. *www.google.com.*

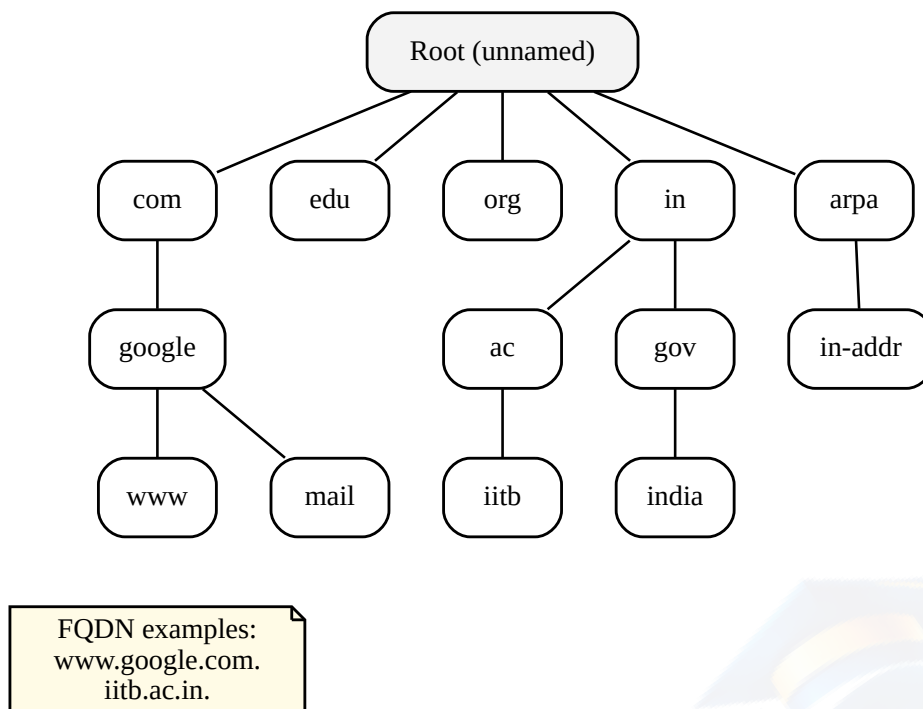


Fig.: DNS domain name space (inverted tree) — generic (com, edu, org), country (in) and inverse (arpa) domains

ii) Types of domains: **Generic domains** — classify hosts by behaviour (com, edu, gov, int, mil, net, org and newer ones). **Country domains** — two-letter country codes (in, us, uk). **Inverse domain** (in-addr.arpa) — maps an address to a name.

iii) Name resolution: the resolver (client) sends a query to the local DNS server. **Recursive resolution:** the server finds the complete answer on behalf of the client by asking other servers. **Iterative resolution:** a server that does not know the answer returns the address of the next server (root → TLD → authoritative), and the local server asks it. Answers are **cached** for the TTL period.

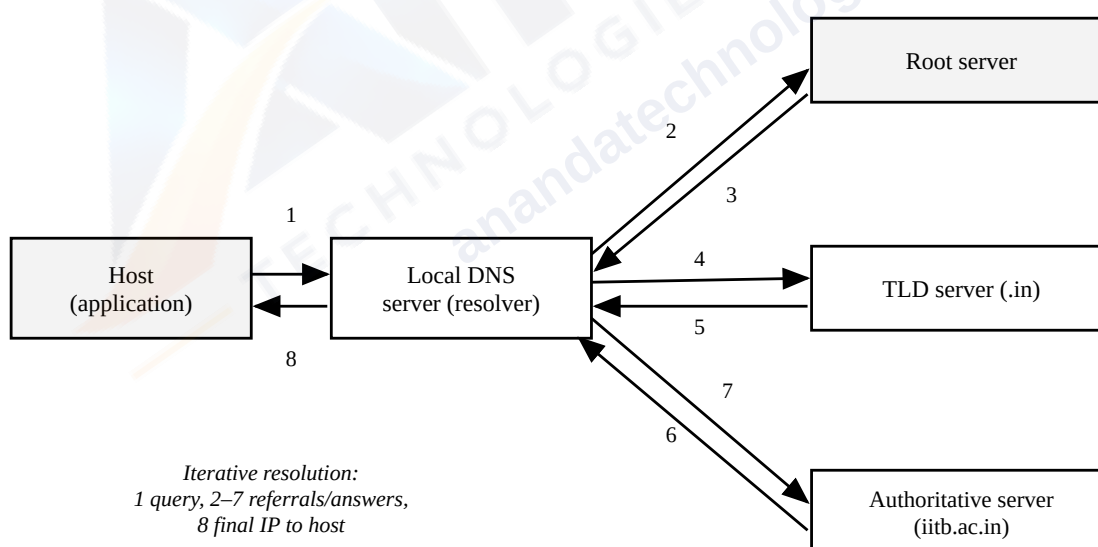


Fig.: DNS architecture — resolver and hierarchy of name servers

(Name space 2 M, domain types 1 M, resolution with diagram 3 M)

Q.6

a) IP address 150.80.200.45 — class, addresses, subnet

6 M

i) **Class:** first octet 150 = 10010110_2 (starts with 10; range 128 – 191) → **Class B**.

ii) **Default mask:** 255.255.0.0 (/16).

iii) **Network address** (IP AND mask) = **150.80.0.0**; network id = 150.80, **host id** = 200.45.

iv) **First usable host:** 150.80.0.1 · **Last usable host:** 150.80.255.254 (usable hosts = $2^{16} - 2 = 65534$).

v) **Broadcast address:** 150.80.255.255.

vi) **8 subnets:** $2^3 = 8$ → borrow 3 bits → /19; **subnet mask** = **255.255.224.0**; block size in third octet = $256 - 224 = 32$; hosts per subnet = 8190.

Subnet	Network address	First host	Last host	Broadcast
1	150.80.0.0/19	150.80.0.1	150.80.31.254	150.80.31.255
2	150.80.32.0/19	150.80.32.1	150.80.63.254	150.80.63.255
3	150.80.64.0/19	150.80.64.1	150.80.95.254	150.80.95.255
4	150.80.96.0/19	150.80.96.1	150.80.127.254	150.80.127.255
5	150.80.128.0/19	150.80.128.1	150.80.159.254	150.80.159.255
6	150.80.160.0/19	150.80.160.1	150.80.191.254	150.80.191.255
7	150.80.192.0/19	150.80.192.1	150.80.223.254	150.80.223.255
8	150.80.224.0/19	150.80.224.1	150.80.255.254	150.80.255.255

Third octet 200 lies in 192 – 223, so 150.80.200.45 belongs to subnet **150.80.192.0/19** (hosts 150.80.192.1 – 150.80.223.254, broadcast 150.80.223.255).

(i–v 3 M, subnet mask and subnet 3 M)

b) **OSPF vs RIP; why OSPF for large networks**

6 M

Sr.	Parameter	RIP	OSPF
1	Type	Distance vector protocol.	Link state protocol.
2	Algorithm	Bellman-Ford.	Dijkstra's shortest path first.
3	Metric	Hop count; maximum 15 (16 = infinity).	Cost (based on bandwidth); no hop limit.
4	Updates	Whole routing table to neighbours every 30 s.	LSAs flooded only when a change occurs (refresh every 30 min).
5	Convergence	Slow; count-to-infinity problem.	Fast; loop-free.
6	Hierarchy / size	Flat; small networks.	Areas with backbone area 0; large networks.
7	Transport	UDP port 520.	Directly over IP (protocol 89).
8	Resources	Low CPU and memory, but more bandwidth for periodic updates.	More CPU and memory, less bandwidth.

Why OSPF is preferred in large networks:

1. No 15-hop limit, so it can cover very large networks.
2. Areas limit LSA flooding and the size of the link-state database; summarization at area borders reduces routing tables.
3. Fast, loop-free convergence after link failures; every router has the complete topology.
4. Cost metric chooses high-bandwidth paths; supports equal-cost load balancing, VLSM/CIDR and authentication.

(Six points 3 M, justification 3 M)

c) Working of PGP at sender and receiver

6 M

PGP (Pretty Good Privacy) provides authentication, integrity, confidentiality, compression and e-mail compatibility for e-mail. Alice (sender) uses her private key and Bob's public key; Bob uses his private key and Alice's public key.

At the sender (Alice):

1. A **message digest** of mail M is created with a hash function (SHA-1 / MD5).
2. The digest is encrypted with **Alice's private key** (RSA) — this is the digital signature.
3. Signature and message are concatenated and **compressed** (ZIP).
4. The result is encrypted with a **one-time session key** using a symmetric algorithm (IDEA / 3DES / CAST).
5. The session key is encrypted with **Bob's public key** and attached.
6. The whole is converted to **Radix-64** (ASCII) so it can travel through e-mail systems.

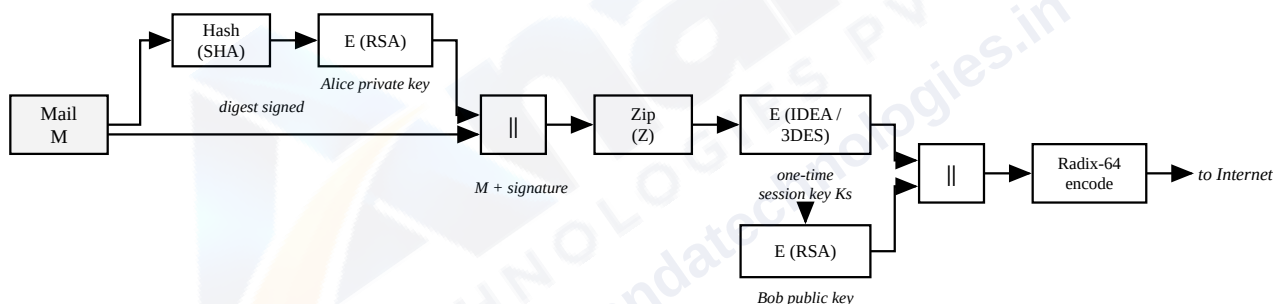


Fig.: PGP at sender (Alice) — authentication, compression and confidentiality

At the receiver (Bob):

1. Radix-64 decoding.
2. Session key is recovered with **Bob's private key**.
3. Message is decrypted with the session key and decompressed.
4. The signature is decrypted with **Alice's public key** to get the original digest.
5. Bob computes a new digest of M; if both digests match, the mail is authentic and unchanged.

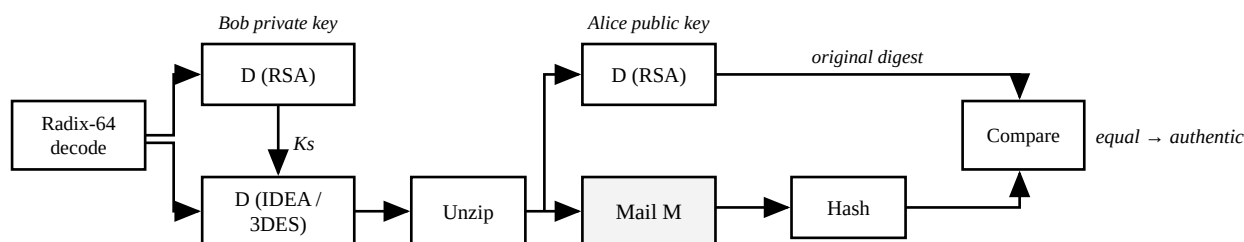


Fig.: PGP at receiver (Bob) — reverse steps and signature check

(Sender steps with diagram 3 M, receiver steps with diagram 3 M)

Note: This is a **model question paper prepared by Ananda Technologies** only for practice and exam preparation, based on the pattern of previous MSBTE question papers and the K-scheme syllabus. It is **not an official MSBTE paper**, and it does **not** mean that these questions will come in the exam. Answers follow standard textbook points; marks shown are indicative. Free for students — anandatechnologies.in