Advance Computer Network (315321)

Model Question Paper — Set C · Model Answers

Q.1

a) Class and default mask

2 M

IP address	First octet (binary)	Class	Default mask
10.45.6.7	00001010	A	255.0.0.0
172.16.5.9	10101100	B	255.255.0.0
192.168.1.5	11000000	C	255.255.255.0
224.0.0.5	11100000	D	No default mask (multicast)

Class ranges: A 0 – 127, B 128 – 191, C 192 – 223, D 224 – 239 (multicast), E 240 – 255 (reserved).

(½ M each)

b) Distance vector vs link state routing

2 M

Sr.	Parameter	Distance vector routing	Link state routing
1	Information shared	Whole routing table, only with neighbours.	State of its own links (LSA), flooded to all routers.
2	Algorithm	Bellman-Ford.	Dijkstra's shortest path.
3	Convergence	Slow; count-to-infinity problem.	Fast; loop-free.
4	Example	RIP.	OSPF.

(Any two points, 1 M each)

c) Role of ISPs

2 M

- An **ISP (Internet Service Provider)** gives Internet access to homes and organizations and connects their networks to the rest of the Internet.
- ISPs form a hierarchy: **international / tier-1 backbone ISPs** interconnect at peering points (NAPs / IXPs); **national / regional ISPs** connect to them; **local ISPs** connect end users.
- They provide IP addresses (from blocks allocated through ICANN / RIRs) and services such as e-mail, web hosting, DNS.

(Role 2 M)

d) SCTP vs TCP

2 M

Sr.	Parameter	SCTP	TCP
1	Data unit	Message-oriented (boundaries preserved).	Byte-stream oriented.
2	Streams	Multiple streams in one association.	Single stream per connection.

3	Multihoming	Supported (several IP addresses per end).	Not supported.
4	Set-up	Four-way handshake with cookie.	Three-way handshake.

(Any two points, 1 M each)

e) TELNET

2 M

TELNET (TErminaL NETwork) is a client-server TCP/IP application (TCP port 23) for **remote logging**: a user at a local terminal logs in to a remote computer and uses it as if directly connected. It uses the **Network Virtual Terminal (NVT)** character set to hide differences between systems.

Use: remote administration of servers, routers and switches, running programs on a remote host. (It sends data, including passwords, in plain text, so SSH is preferred today.)

(Definition 1 M, use 1 M)

f) SDN vs NFV

2 M

Sr.	Parameter	SDN	NFV
1	Basic idea	Separates control plane from data plane; central programmable controller.	Runs network functions as software (VNFs) on standard servers.
2	Target	Switching and routing behaviour of the network.	Network appliances: firewall, load balancer, router, EPC.
3	Standard / protocol	OpenFlow (ONF).	ETSI NFV framework (MANO).

(Any two points, 1 M each)

g) Advantages and disadvantages of FTP

2 M

Advantages: fast transfer of large files and many files at once; supports resume of interrupted transfers; user authentication and permissions control access; widely supported by all platforms.

Disadvantages: user name, password and data travel in plain text (insecure — FTPS/SFTP needed); separate data connection causes firewall / NAT problems; no built-in integrity check; anonymous FTP can be misused.

(Two advantages 1 M, two disadvantages 1 M)

Q.2

a) Characteristics of RIP; RIP timers

4 M

RIP (Routing Information Protocol) is an intra-domain routing protocol based on distance vector routing.

1. Uses **hop count** as metric; maximum 15 hops — 16 means infinity (unreachable), so it suits small networks.
2. Each router sends its **whole routing table to its neighbours every 30 s** (periodic updates) and also triggered updates on change.
3. Runs over **UDP port 520**; RIPv2 carries subnet mask (classless), next hop, route tag and supports authentication; updates sent to multicast 224.0.0.9.

4. Slow convergence and count-to-infinity problem, reduced by split horizon, poison reverse and hold-down.

RIP timers:

- **Periodic timer (≈30 s, random 25 – 35 s):** controls sending of regular update messages.
- **Expiration timer (180 s):** if no update for a route is received within this time, the route is marked invalid (hop count 16).
- **Garbage-collection timer (120 s):** an invalid route is kept (advertised with 16) for this time and then removed from the table.

(Four characteristics 2 M, timers 2 M)

b) Multiplexing and demultiplexing

4 M

The transport layer provides **process-to-process delivery** using the **client/server paradigm**: a client process (ephemeral port, e.g. 52000) requests service from a server process (well-known port, e.g. 80). A **socket address** = IP address + port number identifies a process uniquely.

- **Multiplexing (sender):** many processes need to send data but there is only one transport protocol (e.g. UDP). It accepts messages from the processes, adds a header with source and destination port numbers and passes the packets to IP — a many-to-one relationship.
- **Demultiplexing (receiver):** the transport layer receives segments from IP, checks for errors, reads the **destination port number** and delivers each message to the correct process — a one-to-many relationship.

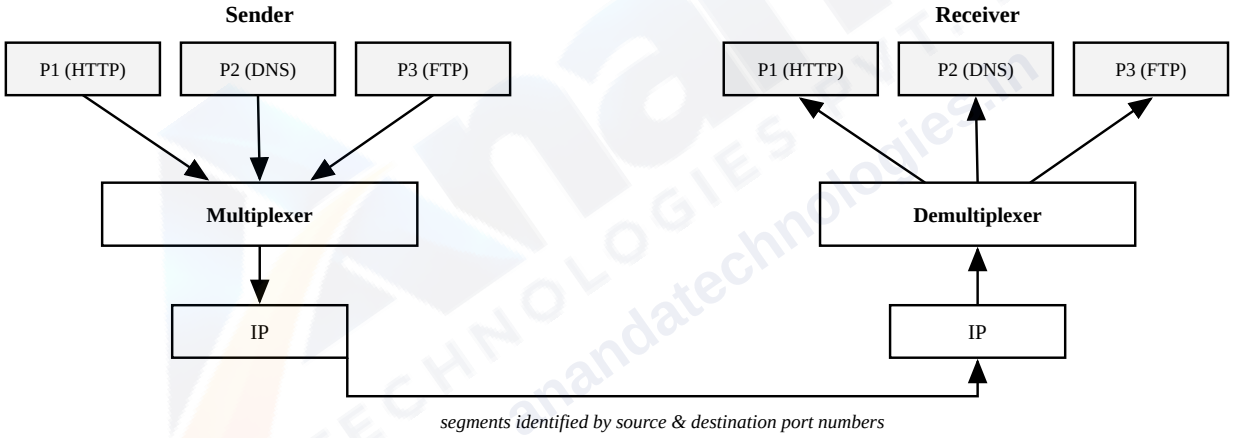


Fig.: Multiplexing at sender and demultiplexing at receiver

(Explanation 2 M, diagram 2 M)

c) Working of SMTP

4 M

SMTP (Simple Mail Transfer Protocol) is the message transfer agent (MTA) protocol. It **pushes** mail from the sender to the sender's mail server and from there to the receiver's mail server, using TCP port 25. The receiver later pulls the mail with POP3 / IMAP4.

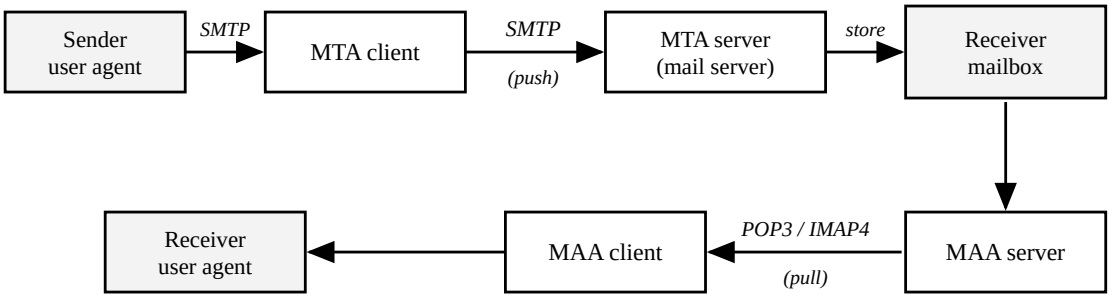


Fig.: E-mail architecture — UA, MTA (SMTP, push) and MAA (POP3 / IMAP4, pull)

Mail transfer takes place in three phases using commands and numeric responses:

1. **Connection establishment:** server sends 220 (service ready); client sends HELO; server replies 250 OK.
2. **Mail transfer:** MAIL FROM (sender), RCPT TO (receiver), DATA, then the message ending with a line containing only a dot; server accepts with 250.
3. **Connection termination:** client sends QUIT; server replies 221 (closing).

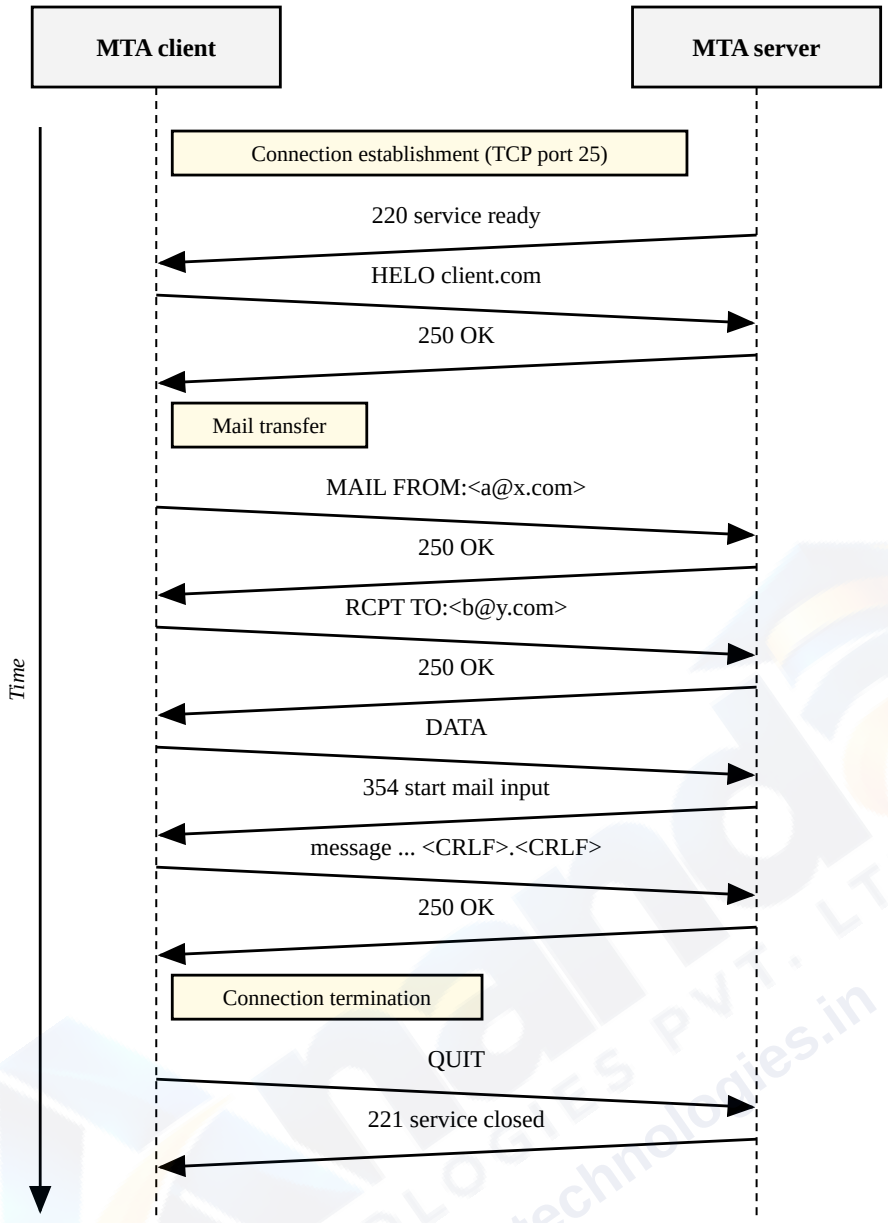


Fig.: SMTP mail transfer phases

(Explanation 2 M, diagram 2 M)

d) Fragmentation numerical (4000 bytes, MTU 1500)

4 M

Data in the datagram = 4000 − 20 = **3980 bytes**. Maximum data per fragment = MTU − header = 1500 − 20 = 1480 bytes; it must be a multiple of 8 → 1480 ✓ (1480 / 8 = 185).

Number of fragments = ⌈3980 / 1480⌉ = **3**. All fragments carry the same Identification value; fragment offset = (byte number of first data byte) / 8.

Fragment	Data bytes	Data byte range	Total length	Fragment offset	M flag
1	1480	0 – 1479	1500	0 / 8 = 0	1
2	1480	1480 – 2959	1500	1480 / 8 = 185	1
3	1020	2960 – 3979	1040	2960 / 8 = 370	0

The last fragment has M = 0; the destination uses Identification, offset and M flag to reassemble the original datagram.

(Fragment sizes 2 M, offsets and flags 2 M)

Q.3

a) UDP header in hexadecimal

4 M

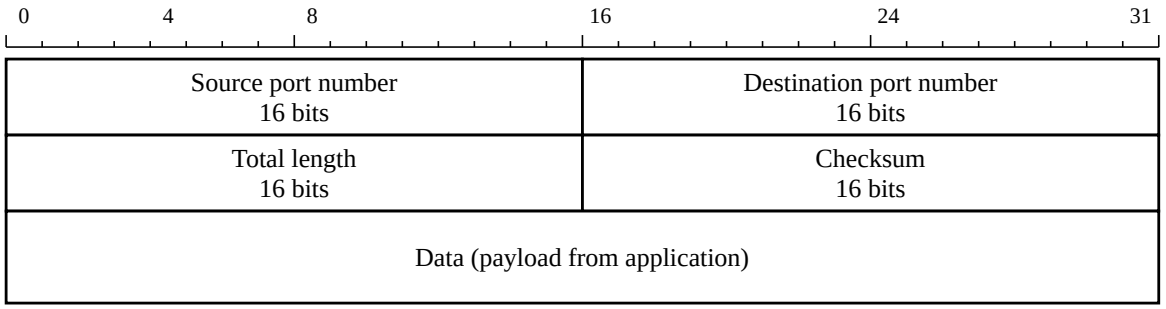


Fig.: UDP user datagram header (8 bytes)

Field	Hex	Decimal / result
i) Source port	CB84	52100
ii) Destination port	000D	13
iii) Total length	001C	28 bytes
iv) Data length	—	28 − 8 = 20 bytes
Checksum	001C	(error check)

v) Destination port 13 is a well-known port and source port 52100 is an ephemeral port (above 49,151), so the packet is from a **client to a server**.

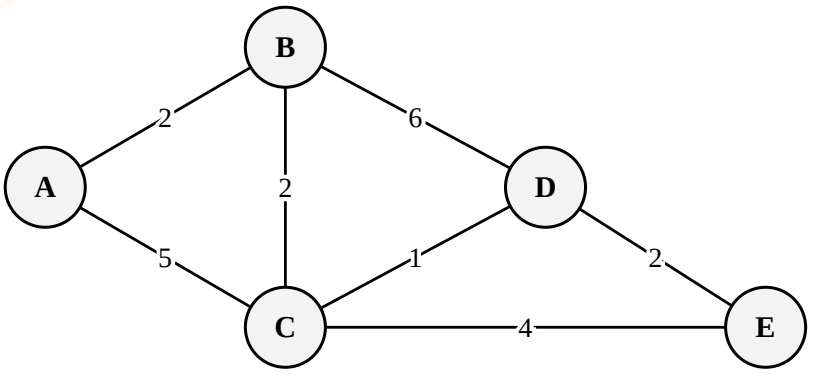
vi) Port 13 is the **Daytime** service, so the client process is the Daytime client.

(Each part ⅔ M)

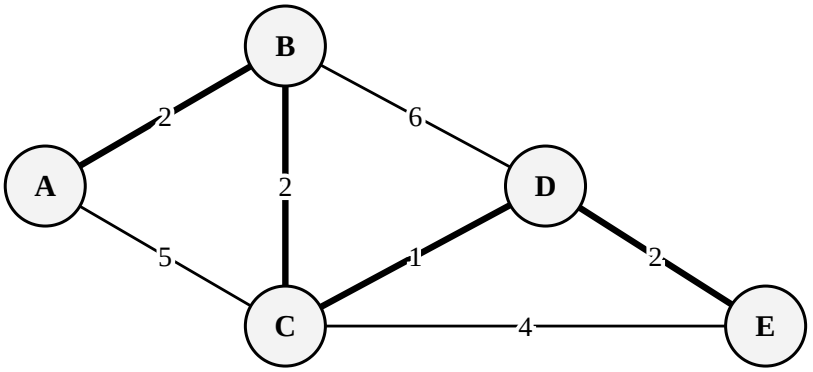
b) Link state routing and Dijkstra

4 M

In **link state routing** every router knows the **complete topology**. Each router floods a **link state packet (LSP / LSA)** describing its links and costs to all routers; every router builds the same link-state database and runs **Dijkstra's algorithm** to make a shortest-path tree with itself as root, from which the routing table is made (used by OSPF).



Given network



Shortest path tree from A (bold)

Step	Permanent set	B	C	D	E
1	A	2	5	∞	∞
2	A, B	2	4	8	∞
3	A, B, C	2	4	5	8
4	A, B, C, D	2	4	5	7
5	A, B, C, D, E	2	4	5	7

Destination	Cost	Path	Next hop
B	2	A → B	B
C	4	A → B → C	B
D	5	A → B → C → D	B
E	7	A → B → C → D → E	B

(Explanation 2 M, Dijkstra steps and tree 2 M)

c) ICMP message format and classification

4 M

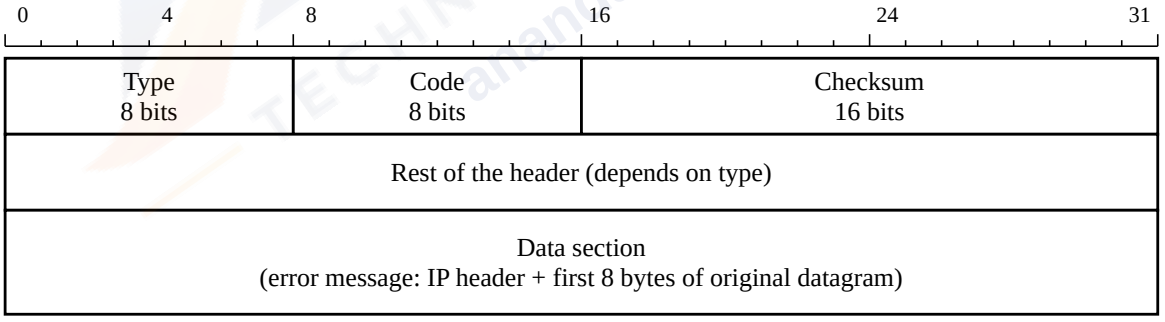


Fig.: General format of ICMP message

- **Type (8 bits):** kind of message. **Code (8 bits):** reason for the particular type. **Checksum (16 bits):** over the whole ICMP message.
- **Rest of header:** depends on type (e.g. identifier and sequence number for echo). **Data section:** for error messages, the original IP header + first 8 bytes of data; for queries, extra information.

Category	Messages (type)

Error-reporting messages	Destination unreachable (3), Source quench (4), Redirection (5), Time exceeded (11), Parameter problem (12)
Query messages	Echo request (8) / Echo reply (0) — used by *ping*; Timestamp request (13) / reply (14); Router solicitation (10) / advertisement (9)

(Format 2 M, classification 2 M)

d) Remote desktop

4 M

Remote desktop lets a user see and control the **full graphical desktop** of a remote computer over a network. The remote computer runs the server; the local computer runs the client. Common protocols: **RDP** (Microsoft Remote Desktop Protocol, port 3389) and **VNC** (RFB protocol). Examples: Windows Remote Desktop Connection, AnyDesk, TeamViewer.

1. Client connects to the server and the user authenticates (connection is encrypted).
2. Keyboard and mouse events from the client are sent to the server.
3. The server runs the applications and sends compressed screen updates back.
4. Clipboard, files, printers and audio can be redirected between the two computers.

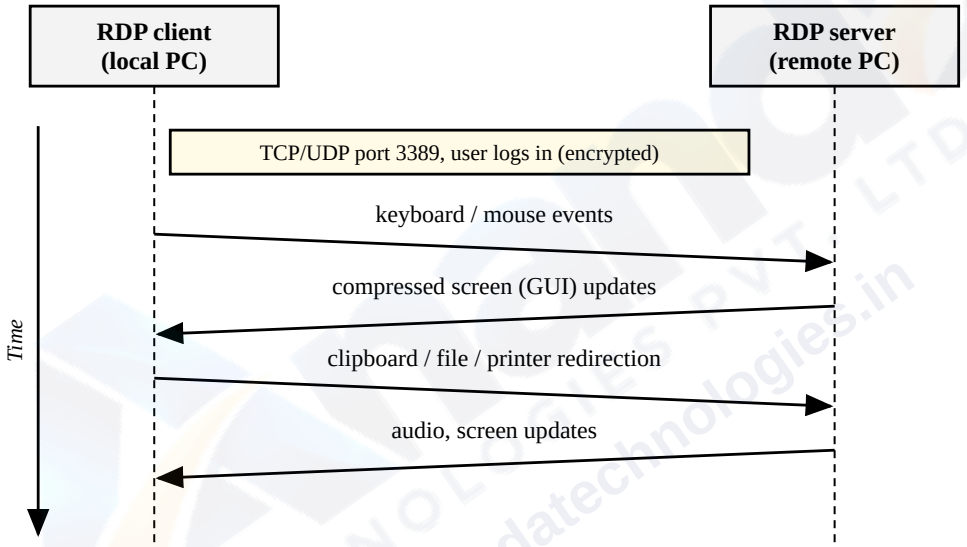


Fig.: Remote desktop — screen updates down, keyboard/mouse events up

Advantages: access office PC / server from anywhere; remote technical support and administration; centralised and secure data (data stays on the server); saves travel time.

(Explanation with diagram 3 M, two advantages 1 M)

Q.4

a) ARP and RARP

4 M

ARP maps a logical (IP) address to a physical (MAC) address. The sender broadcasts an ARP request containing the target IP; only the host with that IP replies (unicast) with its MAC. The result is stored in the ARP cache.

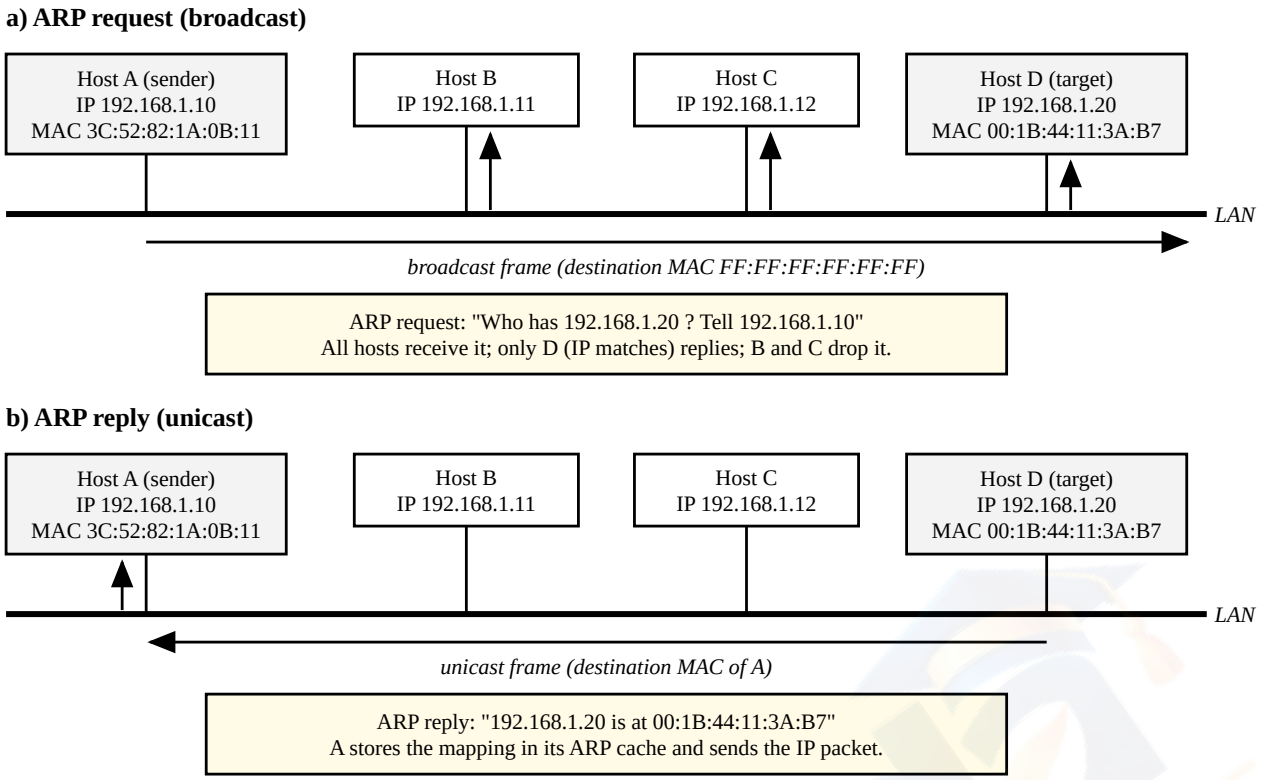


Fig.: ARP operation — request is broadcast to all, reply is unicast to the requester

RARP (Reverse ARP) maps a physical address to a logical address. A diskless machine knows its MAC (from its NIC) but not its IP at boot time; it broadcasts a RARP request and a **RARP server** on the same LAN replies with the IP address. Because the broadcast does not cross routers, a server is needed on every network — so RARP is replaced by BOOTP / DHCP.

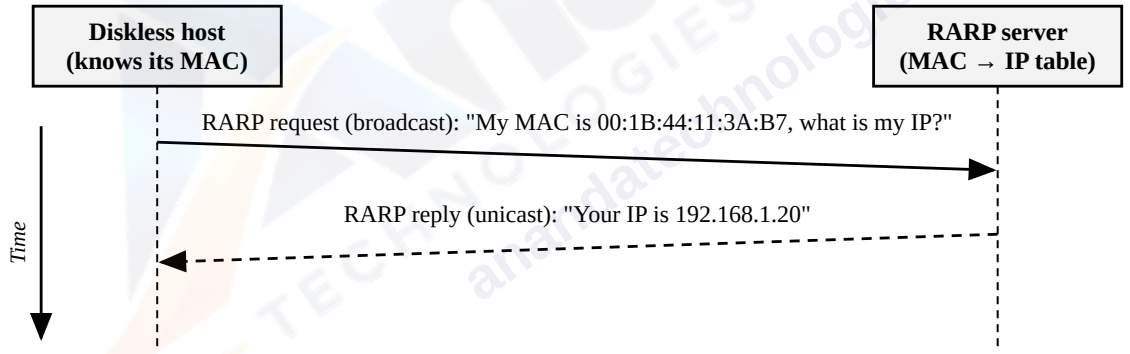


Fig.: RARP — physical to logical address mapping

(ARP with diagram 2 M, RARP with diagram 2 M)

b) Open-loop and closed-loop congestion control 4 M

Open-loop (prevention) methods:

- **Retransmission policy:** good retransmission timers so that unnecessary retransmissions do not add load.
- **Window policy:** selective-repeat window instead of Go-Back-N, so that only lost packets are resent.
- **Acknowledgement policy:** receiver acknowledges N packets at a time or delays ACKs, reducing traffic.

- **Discarding policy** (routers drop less important packets) and **admission policy** (new flow refused if it may cause congestion).

Closed-loop (removal) methods:

- **Back-pressure:** a congested node stops receiving from its upstream node, which in turn becomes congested — pressure propagates back to the source.
- **Choke packet:** a congested router sends a special packet directly to the source to slow down (e.g. ICMP source quench).
- **Implicit signalling:** the source infers congestion from lost packets / delayed ACKs (used by TCP).
- **Explicit signalling:** the congested node sets a bit in packets — backward signalling (towards source) or forward signalling (towards destination), e.g. ECN.

(Three open-loop 2 M, three closed-loop 2 M)

c) Services of PGP; key rings

4 M

1. **Authentication / integrity:** message digest (SHA-1) signed with the sender's private key — the digital signature.
2. **Confidentiality:** message encrypted with a one-time session key (IDEA / 3DES / CAST); the session key is encrypted with the receiver's public key.
3. **Compression:** ZIP after signing and before encryption — saves space and strengthens encryption.
4. **E-mail compatibility:** Radix-64 conversion of binary output into ASCII characters.
5. **Segmentation:** long messages are split to fit e-mail size limits and reassembled at the receiver.

Key rings: each user keeps two key rings — a **private key ring** (own public/private key pairs, the private keys stored encrypted with a passphrase) and a **public key ring** (public keys of other users with their key IDs and trust levels). Key IDs in a message tell the receiver which key to use. PGP certificates follow a **web of trust**: users sign each other's public keys instead of depending on one CA.

(Services 3 M, key rings 1 M)

d) 5G technology — features and applications

4 M

5G is the fifth generation of cellular technology (3GPP Release 15 onwards; 5G NR radio and cloud-native 5G core). It is designed for three service types: **eMBB** (enhanced mobile broadband), **URLLC** (ultra-reliable low-latency communication) and **mMTC** (massive machine-type communication / IoT).

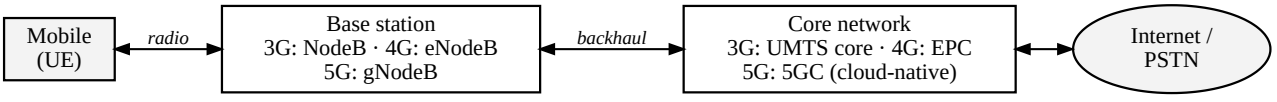


Fig.: Cellular network — handset, base station (eNodeB/gNodeB) and core network

Features:

- Peak data rate up to about 20 Gbps; latency about 1 ms; up to 1 million devices per km².
- Uses sub-6 GHz and millimetre-wave bands; massive MIMO and beamforming.
- Network slicing — many virtual networks on one physical network, each with its own QoS.

- Core network built with SDN / NFV; supports edge computing.

Applications: smart cities and IoT, autonomous / connected vehicles, remote surgery and telemedicine, AR / VR and cloud gaming, industrial automation (Industry 4.0), fixed wireless broadband.

(Features 2 M, applications 2 M)

e) RTP and its header

4 M

RTP (Real-time Transport Protocol) carries real-time audio and video. It runs over **UDP** (even port number; its companion **RTCP** uses the next odd port for control and quality feedback). RTP adds what UDP lacks for multimedia — payload type, sequence numbers, time-stamps and source identification — but does not itself guarantee delivery or QoS.

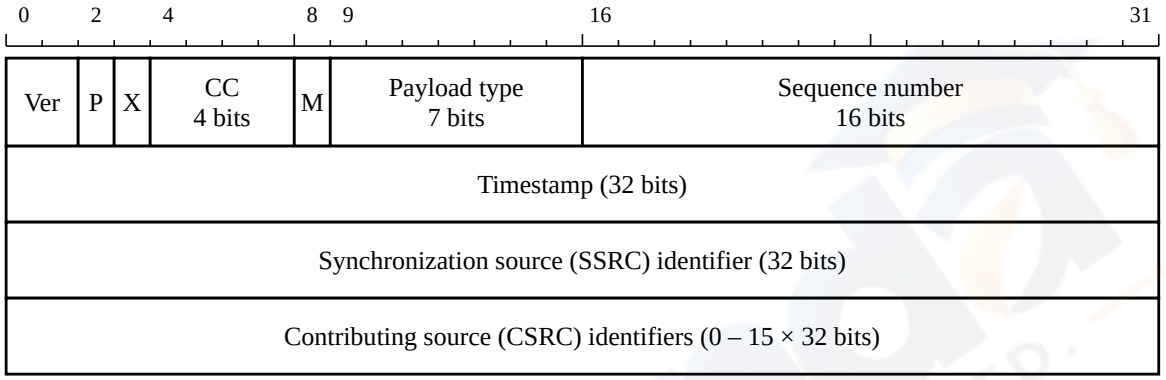


Fig.: RTP packet header format

- **Ver (2):** version 2. **P:** padding present. **X:** extension header present. **CC (4):** number of contributing sources.
- **M:** marker (e.g. end of a video frame). **Payload type (7):** encoding (e.g. PCM μ-law, MPEG video).
- **Sequence number (16):** detects loss and reorders packets. **Timestamp (32):** timing for play-back and jitter removal.
- **SSRC (32):** identifies the source. **CSRC list:** sources mixed into this packet.

Role in streaming: RTSP controls the session (play / pause) while RTP delivers the media packets in order and in time.

(Explanation 1 M, header 2 M, role 1 M)

Q.5

a) TCP and UDP — features and comparison

6 M

TCP (Transmission Control Protocol) is a connection-oriented, reliable, byte-stream transport protocol. Features: three-way handshake connection set-up, sequence and acknowledgement numbers, retransmission of lost segments (error control), sliding-window flow control, congestion control (slow start, congestion avoidance), full-duplex service, segment header 20 – 60 bytes.

UDP (User Datagram Protocol) is a connectionless, unreliable, message-oriented transport protocol. Features: no connection set-up, no acknowledgement or retransmission, no flow or

congestion control, optional checksum only, small fixed 8-byte header, supports broadcast and multicast — so it is fast and simple.

Sr.	Parameter	TCP	UDP
1	Connection	Connection-oriented (three-way handshake).	Connectionless.
2	Reliability	Reliable — ACK, retransmission, in-order delivery.	Unreliable — no ACK, may lose or reorder.
3	Data unit	Byte stream; segments.	Messages; user datagrams.
4	Header size	20 – 60 bytes.	Fixed 8 bytes.
5	Flow / congestion control	Yes (sliding window, cwnd).	No.
6	Speed / overhead	Slower, more overhead.	Faster, less overhead.
7	Broadcast / multicast	Not supported.	Supported.
8	Applications	HTTP, FTP, SMTP, TELNET, SSH.	DNS, SNMP, TFTP, DHCP, VoIP, video streaming.

(TCP 1½ M, UDP 1½ M, any six differences 3 M)

b) NFV — architecture, benefits, applications 6 M

Network Function Virtualization (NFV) decouples network functions from proprietary hardware and runs them as software (VNFs) on standard servers, storage and switches in data centres.

i) Architecture:

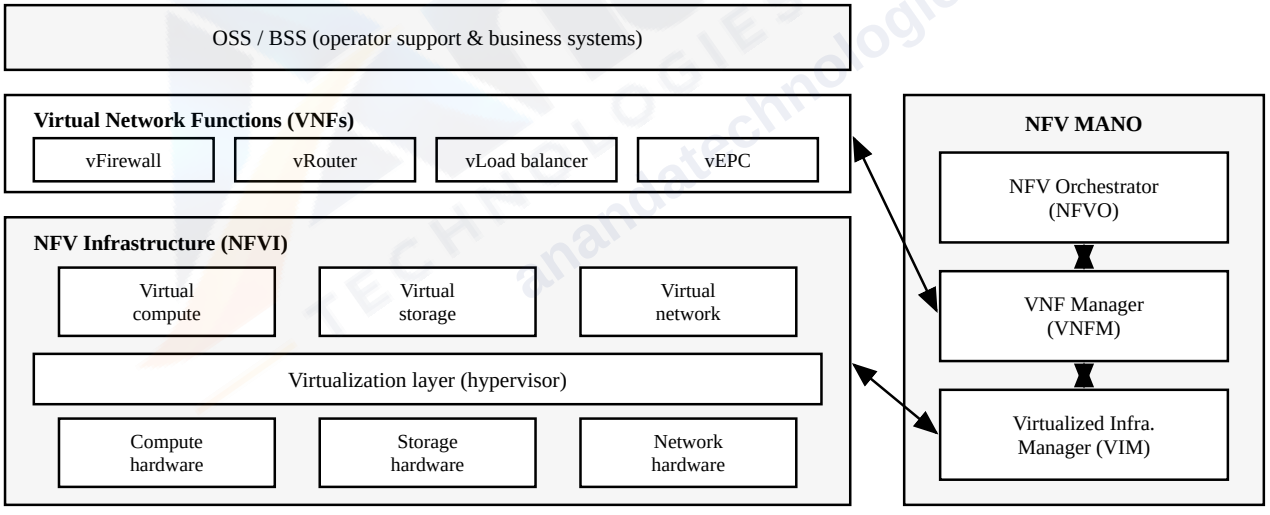


Fig.: NFV reference architecture (ETSI)

- **VNFs:** software network functions (virtual firewall, router, load balancer, EPC) in VMs / containers.
- **NFVI:** compute, storage and network hardware + virtualization layer (hypervisor) providing virtual resources.
- **MANO:** NFV Orchestrator (service life-cycle), VNF Manager (VNF instantiation, scaling, termination), VIM (manages NFVI resources, e.g. OpenStack).

- **OSS / BSS:** operator's operation and business support systems.

ii) Benefits: lower capital and operating cost (commodity hardware), faster deployment of new services, easy scaling up / down, vendor independence, less space and power, easy testing and upgrades.

iii) Applications: virtual CPE for enterprises, virtual EPC / 5G core, virtual firewalls and IDS, load balancers, virtual routers, SD-WAN, content delivery networks, IMS for VoLTE.

(Architecture with diagram 3 M, benefits 1½ M, applications 1½ M)

c) Architecture of WWW and HTTP transaction 6 M

The **World Wide Web (WWW)** is a distributed client-server service in which a client (browser) accesses **web pages** stored on web servers spread over many sites, linked by hyperlinks.

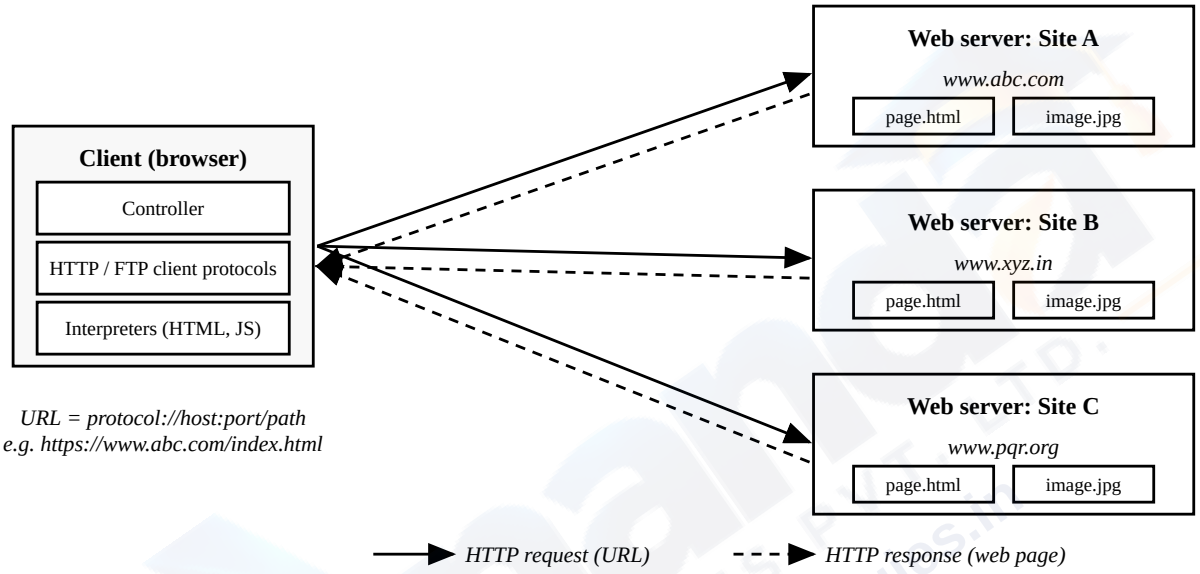


Fig.: Architecture of WWW (client – server, distributed)

- **Client (browser):** controller (takes input from keyboard / mouse), client protocols (HTTP, FTP) to fetch documents, and interpreters (HTML, JavaScript) to display them.
- **Server:** stores web pages and sends them on request; may create dynamic pages; uses caching and multithreading for efficiency.
- **URL (Uniform Resource Locator):** identifies a page — protocol://host:port/path, e.g. https://www.abc.com/index.html.
- **Hypertext / hypermedia:** documents link to other documents, images, audio and video anywhere on the web.

HTTP transaction: HTTP uses TCP (port 80). The client opens a connection and sends a **request message** (request line, headers, body); the server returns a **response message** (status line, headers, body). HTTP is **stateless** (cookies keep state). In HTTP/1.0 the connection is non-persistent (one object per connection); in HTTP/1.1 it is persistent by default.

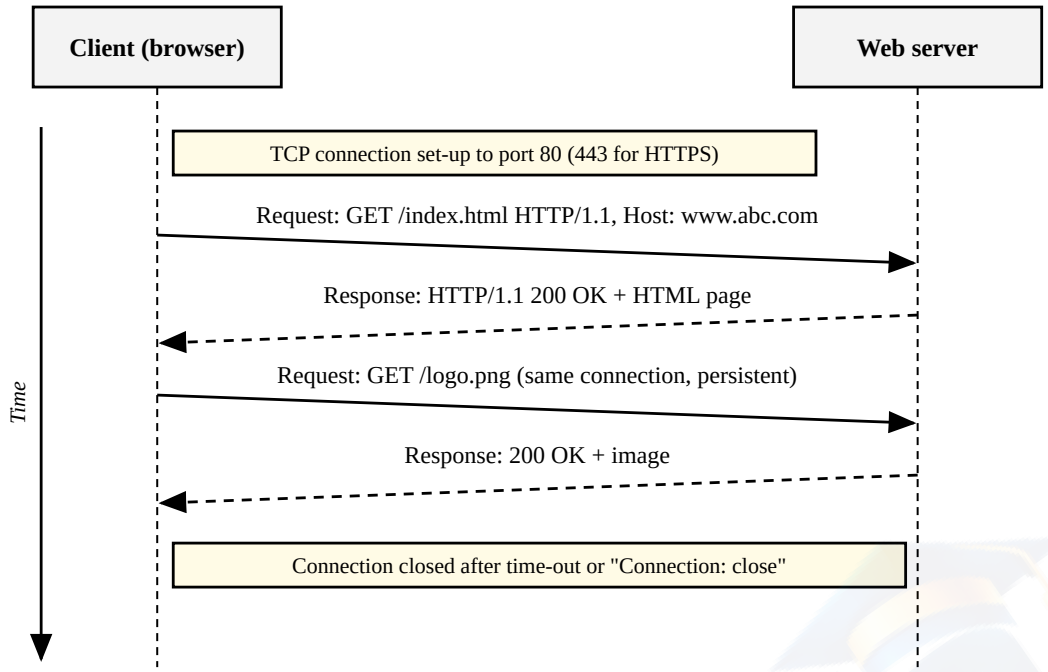


Fig.: HTTP transaction (persistent connection)

(Architecture with diagram 3 M, HTTP transaction 3 M)

Q.6

a) Subnetting 192.168.50.0/24 into 6 subnets 6 M

192.168.50.0 is a **Class C** address (first octet 192), default mask 255.255.255.0 (/24).

i) Bits borrowed: $2^n \geq 6 \rightarrow n = 3$ (gives 8 subnets; 2 bits would give only 4).

ii) Subnet mask: /24 + 3 = /27; last octet = $11100000_2 = 224 \rightarrow$ **255.255.255.224**.

iii) Usable hosts per subnet: $2^5 - 2 = 30$ (block size 32).

iv) Subnets:

Subnet	Network address	First host	Last host	Broadcast address
1	192.168.50.0/27	192.168.50.1	192.168.50.30	192.168.50.31
2	192.168.50.32/27	192.168.50.33	192.168.50.62	192.168.50.63
3	192.168.50.64/27	192.168.50.65	192.168.50.94	192.168.50.95
4	192.168.50.96/27	192.168.50.97	192.168.50.126	192.168.50.127
5	192.168.50.128/27	192.168.50.129	192.168.50.158	192.168.50.159
6	192.168.50.160/27	192.168.50.161	192.168.50.190	192.168.50.191
7	192.168.50.192/27	192.168.50.193	192.168.50.222	192.168.50.223
8	192.168.50.224/27	192.168.50.225	192.168.50.254	192.168.50.255

Any 6 of these 8 subnets are allotted; the remaining 2 are kept for future growth.

(Bits 1 M, mask 1 M, hosts 1 M, table 3 M)

b) BGP — path vector routing, sessions, messages 6 M

BGP (Border Gateway Protocol, version 4) is the inter-domain routing protocol of the Internet; it routes between autonomous systems (ASes).

i) Path vector routing: a speaker router in each AS advertises to its neighbours each reachable network together with the **path — the ordered list of AS numbers** to reach it. Receiving ASes add their own number and pass it on. A router discards any path containing its own AS (loop prevention) and chooses the route according to its **policy** (not just shortest).

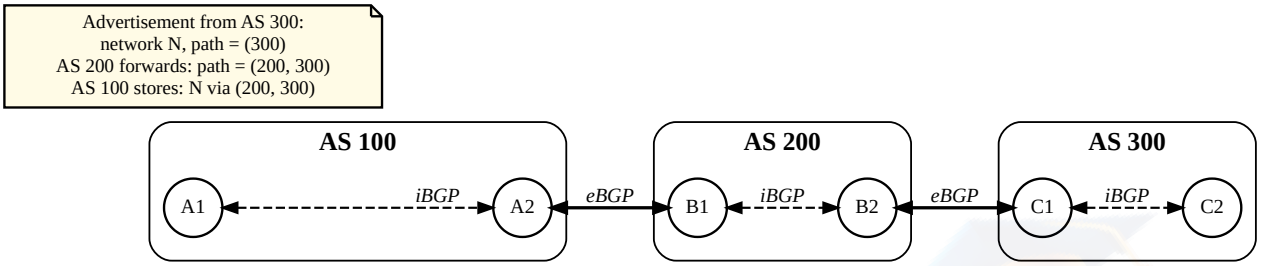


Fig.: Path vector routing with BGP between autonomous systems

ii) Types of BGP sessions: BGP uses TCP (port 179) semi-permanent sessions. **External BGP (eBGP)** — between routers of different ASes; **Internal BGP (iBGP)** — between routers inside the same AS, to spread the routes learnt from outside.

iii) BGP message types:

Message	Purpose
Open	Creates a neighbour relationship; carries AS number, hold time, BGP identifier.
Update	Withdraws old routes and/or advertises a new route with path attributes (AS-PATH, NEXT-HOP, ORIGIN).
Keepalive	Sent regularly (before the hold timer expires) to tell the neighbour the session is alive.
Notification	Reports an error condition and closes the session.

(Path vector with diagram 2 M, sessions 2 M, messages 2 M)

c) VoIP — working, protocols, services 6 M

VoIP (Voice over Internet Protocol) carries voice calls as data packets over an IP network instead of the circuit-switched telephone network.

i) How VoIP works:

1. Analog voice from the microphone is digitised (ADC) and compressed by a codec (G.711, G.729, Opus).
2. Signalling protocol (SIP / H.323) sets up the call — finds the callee, rings, negotiates codecs.
3. Voice samples are put into RTP packets, carried in UDP and IP, and sent over the Internet.
4. At the receiver a jitter buffer re-orders and smooths packets, then the codec decodes and DAC converts back to sound.
5. Gateways connect VoIP calls to ordinary PSTN / mobile phones.

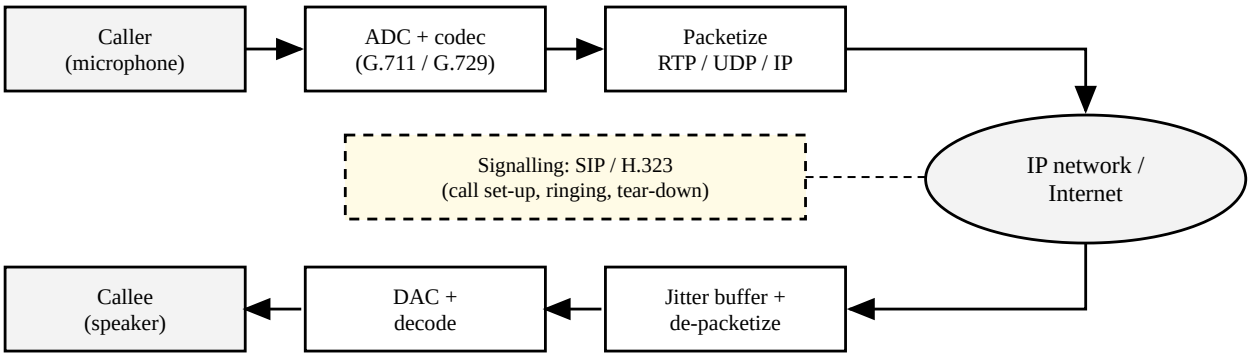


Fig.: How VoIP works — voice → digital → packets → IP network → voice

ii) Protocols: SIP (Session Initiation Protocol, port 5060 — call set-up and tear-down), **H.323** (ITU-T suite), **RTP / RTCP** (media transport and quality feedback), SDP (session description), codecs.

iii) Services: voice and video calls, conferencing, voicemail (and voicemail-to-e-mail), call forwarding, call waiting, caller ID, IVR, virtual numbers, instant messaging and presence (unified communications).

(Working with diagram 3 M, protocols 1½ M, services 1½ 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