UNIT 1

- Following table differentiate between Intranet and Internet.

Sr. No.	Feature	Intranet	Internet
1.	Accessibility	Private (restricted to authorized users).	Public (accessible to anyone).
2.	What is?	A private network, within an Enterprise or Organization.	Worldwide/global system of connected networks.
3.	Purpose	Internal communication.	Global information sharing.
4.	Security	Highly secure (Firewalls, VPNs).	Less secure.
5.	User-base	Limited to organization members.	Open to all.
6.	Network	Localized Network.	Worldwide Network.
7.	Expensive	More expensive.	Less expensive.
8.	Content type	Organization-specific resources.	Diverse global content.
9.	Reliability	More reliability.	Less reliability.

Internet	Intranet
Internet is used to connect different networks of computers simultaneously.	Intranet is owned by private firms.
On the internet, there are multiple users.	On an intranet, there are limited users.
Internet is unsafe.	Intranet is safe.
On the internet, there is more number of visitors.	In the intranet, there is less number of visitors.
Internet is a public network.	Intranet is a private network.
Anyone can access the Internet.	In this, anyone can't access the Intranet.
The Internet provides unlimited information.	Intranet provides limited information.
Using Social media on your phone or researching resources via Google.	A company used to communicate internally with its employees and share information
The Internet is a global network that connects millions of devices and computers worldwide.	An intranet is a private network that connects devices and computers within an organization.
It is open to everyone and allows access to public information, such as websites and online services.	An intranet is only accessible to authorized users within the organization.
It is used for communication, sharing of information, e-commerce, education, entertainment, and other purposes.	An intranet is primarily used for internal communication, collaboration, and information sharing within an organization.

Internet	Intranet
Users can access the Internet from any location with an Internet connection and a compatible device.	Access to an intranet is restricted to authorized users within the organization and is typically limited to specific devices and locations.
Security measures, such as firewalls, encryption, and secure sockets layer (SSL) protocols, are used to protect against threats like hacking, viruses, and malware.	Intranets employ similar security measures to protect against unauthorized access and ensure the privacy and integrity of shared data.
The Internet is a public network that is not owned by any particular organization or group.	Intranets are private networks that are owned and managed by the organization that uses them.
Examples of Internet-based services include email, social media, search engines, and online shopping sites.	Examples of intranet-based services include internal communications, knowledge management systems, and collaboration tools

- It delivers flexibility and ...
- Following table illustrates the difference between IPv4 and IPv6.

Parameters	IPv4	IPv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon (:).
Classes	IPv4 has five different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask (means that IPv4 converts IP addresses into a subnet of different sizes)).	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	IPv6 is multicasting, which provides efficient network operations.

Contd...

V2V EdTech LLP | ACN (CO/IT/AIML) (315321)

Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets.
Use in Industry	Many companies have historically used and continue to use IPv4, including major tech companies like Apple, Microsoft, and Google, as well as other organizations like Ford Motor Company and AT&T.	These addresses are used by Comcast, Reliance Jio, T-Mobile USA, Sky broadband, Claro, Softbank, Orange, SK telecom, Cox communication, Kabel Deutschland and many more.

Table 1.11.1 : Comparison between IPv4 and IPv6

Sr. No.	IPv4	IPv6
1.	In IPv4 there are only 2^{32} possible ways to represent the address (about 4 billion possible addresses)	In IPv6 there are 2^{128} possible way (about 3.4×10^{38} possible addresses)
2.	The IPv4 address is written by dotted-decimal notation. e.g. 121.2.8.12	IPv6 is written in hexadecimal and consists of 8 groups, containing 4 hexadecimal digits or 8 groups of 16 bits each, e.g. FABC: AC77: 7834:2222:FACB: AB98: 5432:4567.
3.	The basic length of the IPv4 header comprises a minimum of 20 bytes (without option fields). The maximum total length of the IPv4 header is 60 bytes (with option fields), and it uses 13 fields to identify various control settings.	The IPv6 header is a fixed header of 40 bytes in length, and has only 8 fields. Option information is carried by the extension header, which is placed after the IPv6 header.
4.	IPv4 header has a checksum, which must be computed by each router	IPv6 has no header checksum because checksums are, for example, above the TCP/IP protocol suite, and above the Token Ring, Ethernet, etc.
5.	IPv4 contains an 8-bit field called Service Type. The Service Type field is composed of a TOS (Type of Service) field and a procedure field.	The IPv6 header contains an 8-bit field called the Traffic Class Field. This field allows the traffic source to identify the desired delivery priority of its packets
6.	The IPv4 node has only Stateful auto-configuration.	The IPv6 node has both a stateful and a stateless address autoconfiguration mechanism.
7.	Security in IPv4 networks is limited to tunneling between two networks	IPv6 has been designed to satisfy the growing and expanded need for network security.
3.	Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
).	IPsec support is optional.	IPsec support is required.
0.	No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.
1.	Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.	ARP Request frames are replaced with multicast Neighbour Solicitation messages.
2.	Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP.
3.	ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional	ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.
.	Header includes options	All optional data is moved to IPv6 extension headers.

Feature	IPv4	IPv6
Address Length	32-bit address	128-bit address
Address Format	Decimal format (e.g., 192.168.0.1)	Hexadecimal format (e.g., 2001:0db8::1)
Configuration	Manual and DHCP configuration	Auto-configuration and renumbering supported
Connection Integrity	End-to-end integrity is unachievable	End-to-end integrity is achievable
Security	No built-in security; external tools like IPSec needed	IPSec is built-in for encryption and authentication
Fragmentation	Performed by sender and routers	Performed only by the sender

Feature	IPv4	IPv6
Flow Identification	Not available	Uses Flow Label field in header for packet flow identification
Checksum Field	Present	Not present
Transmission Scheme	Supports broadcast	Uses multicast and anycast; no broadcast
Header Size	Variable: 20–60 bytes	Fixed: 40 bytes
Conversion	Can be converted to IPv6	Not all IPv6 addresses can be converted to IPv4
Field Structure	4 fields separated by dots (.)	8 fields separated by colons (:)
Address Classes	Has address classes (A, B, C, D, E)	No concept of address classes
VLSM Support	Supports Variable Length Subnet Mask (VLSM)	Does not support VLSM
Example	66.94.29.13	2001:0000:3238:DFE1:0063:0000:0000:FEFB

... and RARP:

Sr. No.	Parameters	ARP (Address Resolution Protocol)	RARP (Reverse Address Resolution Protocol)
1.	Purpose	Resolves IP addresses to MAC addresses.	Resolves MAC addresses to IP addresses.
2.	Functionality	Maps IP addresses to MAC addresses for communication.	Maps MAC addresses to IP addresses for address assignment.
3.	Usage	Used by devices to find the MAC address of a device with a known IP address.	Used by diskless or IP-less devices to determine their IP address.
4.	Message Type	ARP Request and ARP Reply messages.	RARP Request and RARP Reply messages.
5.	Resolution Process	Device sends ARP Request to find the MAC address associated with a known IP address.	Device sends RARP Request to find the IP address associated with a known MAC address.
6.	Request Type	Broadcast message requesting the MAC address for a specific IP address.	Broadcast message requesting the IP address for a specific MAC address.
7.	Response Type	Unicast message providing the MAC address corresponding to the requested IP address.	Unicast message providing the IP address corresponding to the requested MAC address.
8.	Packet Format	ARP packets have fields for hardware type, protocol type, hardware address length, protocol address length, operation code, sender hardware address, sender protocol address, target hardware address, and target protocol address.	RARP packets have similar fields as ARP packets.
9.	Usage Status	Widely used in modern networks.	Largely replaced by DHCP (Dynamic Host Configuration Protocol) for IP address assignment.
10.	Encapsulation	ARP messages are encapsulated within Ethernet frames or other suitable link-layer protocols.	RARP messages are encapsulated within Ethernet frames or other link-layer protocols.
11.	Common Use Case	Resolving IP addresses to MAC addresses in Ethernet-based networks.	Assigning IP addresses to diskless workstations or devices without statically configured IP addresses.

ARP	RARP
A protocol used to map an IP address to a physical address	A protocol used to map a physical address to an IP address
To obtain the MAC address of a network device when only its IP address is known	To obtain the IP address of a network device when only its MAC address is known
IP addresses	MAC addresses
ARP stands for Address Resolution Protocol.	Whereas RARP stands for Reverse Address Resolution Protocol.
In ARP, broadcast MAC address is used.	While in RARP, broadcast IP address is used.
In ARP, ARP table is managed or maintained by local host.	While in RARP, RARP table is managed or maintained by RARP server.
In Address Resolution Protocol, Receiver's MAC address is fetched.	While in RARP, IP address is fetched.
ARP is used in sender's side to map the receiver's MAC address.	RARP is used in receiver's side to map the sender's IP.

Table 1.15.1 : Difference between RARP and ARP

Sr. No	RARP	ARP
1.	A protocol used to map a physical (MAC) address to an IP address	A protocol used to map an IP address to a physical (MAC) address
2.	To obtain the IP address of a network device when only its MAC address is known	To obtain the MAC address of a network device when only its IP address is known
3.	Client broadcasts its MAC address and requests an IP address, and the server responds with the corresponding IP address	Client broadcasts its IP address and requests a MAC address, and the server responds with the corresponding MAC address
4.	MAC addresses	IP addresses
5.	Rarely used in modern networks as most devices have a pre-assigned IP address	Widely used in modern networks to resolve IP addresses to MAC addresses
6.	RFC 903 Standardization	RFC 826 Standardization
7.	RARP stands for Reverse Address Resolution Protocol	ARP stands for Address Resolution Protocol
8.	In RARP, we find our own IP address	In ARP, we find the IP address of a remote machine
9.	The MAC address is known and the IP address is requested	The IP address is known, and the MAC address is being requested
10.	It uses the value 3 for requests and 4 for responses	It uses the value 1 for requests and 2 for responses

Subnetting	Supernetting
Subnetting is the procedure to divide the network into sub-networks.	While supernetting is the procedure of combining small networks.
In subnetting, Network addresses' bits are increased.	While in supernetting, Host addresses' bits are increased.
In subnetting, The mask bits are moved towards the right.	While In supernetting, The mask bits are moved towards the left.
Subnetting is implemented via Variable-length subnet masking.	While supernetting is implemented via Classless interdomain routing.
In subnetting, Address depletion is reduced or removed.	While It is used for simplifying the routing process.

UNIT 2

used in exterior routing.

Difference between Intra-Domain and Inter-Domain Routing:

Sr. No.	Intra-Domain Routing	Inter-Domain Routing
1.	Routing takes place within an autonomous network.	Routing takes place between the two autonomous networks.
2.	This protocol ignores the internet outside the autonomous system.	This protocol assumes that internet consists of a collection of interconnected autonomous systems.
3.	Protocols for Intra-domain routing are called as interior gateway protocols.	Protocol for Inter-domain routing are also called as exterior gateway protocols.
4.	For a packet that enters a domain, intra-domain routing will determine the route via which the packet will travel through to the border router connected to the next domain.	Inter-domain routing is the top-level routing. It determines the AS path each packet will travel through to its destination.
5.	Intra-domain multicast routing protocols, by which packets are multicast within a domain.	Inter-domain routing protocols, by which packets multicast among domains.
6.	In Interdomain Routing, Interior-gateway protocols such as RIP (resource information protocol) and OSPF (open shortest path first) are being used.	In Intradomain Routing, additional exterior-gateway protocols such as BGP (Border Gateway Protocol) are used.
7.	Interdomain Routing, as name suggests, is the protocol in which the Routing algorithm works within and in between the domains.	Intradomain Routing is a protocol in which the Routing algorithm works only within the domains.

Intradomain Routing	Interdomain Routing	
1.	Routing algorithm works only within domains.	Routing algorithm works within and between domains.
2.	It need to know only about other routers within their domain.	It need to know only about other routers within and between their domain.
3.	Protocols used in intradomain routing are known as Interior-gateway protocols.	Protocols used in interdomain routing are known as Exterior-gateway protocols.
4.	In this Routing, routing takes place within an autonomous network.	In this Routing, routing takes place between the autonomous networks.

5.	Intradomain routing protocols ignores the internet outside the AS(autonomous system).	Interdomain routing protocol assumes that the internet contains the collection of interconnected AS(autonomous systems).
6.	Some Popular Protocols of this routing are RIP(routing information protocol) and OSPF(open shortest path first).	Popular Protocols of this routing is BGP(Border Gateway Protocol) used to connect two or more AS(autonomous system).

Difference between RIPv1 and RIPv2:

Sr. No.	RIPv1	RIPv2
1.	It uses broadcast for routing update.	It uses multicast for routing update.
2.	It sends broadcast on 255.255.255.255 destination.	It sends multicast on 224.0.0.9 destination.
3.	It does not support VLSM (Variable Length Subnet Masking).	It supports VLSM.
4.	It does not support any authentication.	It supports MD5 authentication.
5.	It only supports classful routing.	It supports both classful and classless routing.
6.	It does not support discontinuous network.	It supports discontinuous network.
7.	RIP v1 uses what is known as classful routing.	RIP v2 is a classless protocol and it supports variable-length subnet masking (VLSM), CIDR, and route summarization.
8.	RIPv1 routing updates are broadcasted.	RIP v2 routing updates are multicasted.
9.	RIP v1 does not carry mask in updates.	RIP v2 does carry mask in updates, so it supports for VLSM.
10.	RIP v1 is an older, no longer much used routing protocol.	IP v2 can be useful in small, flat networks or at the edge of larger networks because of its simplicity in configuration and usag.e

Contd...

RIPv1	RIPv2	
1.	RIPv1 is a Distance-Vector Routing protocol.	RIPv2 is also Distance-Vector Routing Protocol.
2.	The standard used RFC 1058.	The standard used RFC 1721,1722 and 2453.
3.	It can supports class full network only.	It can support class full and classless networks.
4.	It does not support for authentications.	It support for authentications.
5.	It hop count limit is 15.	It hop count limit is 15.
6.	It does not support for VLSM and discontinuous networks.	It supports for VLSM and discontinuous networks.
7.	It is less secure.	It is more secure.
8.	RIPv1 uses Broadcast traffic for updates.	RIPv2 uses Multicast traffic for updates.
9.	The routing update address used for Broadcast is 255.255.255.255.	The routing update address used for Multicast is 224.0.0.9.

RIPv1	RIPv2	
10.	RIPV1 does not provide trigger updates.	RIPv2 provides trigger updates.
11.	RIPV1 does not send a subnet mask to the routing table.	RIPv2 sends subnet mask to the routing table.
12.	RIPv1 doesn't support manual route summarization.	RIPv2 supports manual route summarization.
13.	RIPv1 does not support Classless Inter-Domain Routing (CIDR).	RIPv1 supports Classless Inter-Domain Routing (CIDR).

Table 2.12.1 : Comparison between RIP and OSPF

Sr. No.	Function/Feature	RIPv1	RIPv2	OSPF
1.	Standard number	RFC 1058	RFC 1723	RFC 2178
2.	Link-state protocol	No	No	Yes
3.	Large range of metrics	Hop count (16=Infinity)	Hop count (16=Infinity)	Yes, based on 1-65535
4.	Update policy	Route table every 30 seconds	Route table every 30 seconds	Link-state changes, or every 30 [minutes]
5.	Update address	Broadcast	Broadcast, multicast	Multicast
6.	Dead interval	300 seconds total	300 seconds total	300 seconds total, but usually much less
7.	Supports authentication	No	Yes	Yes
8.	Convergence time	Variable (based on number of routers X dead interval)	Variable (based on number of routers X dead interval)	Media delay + dead interval

Sr. No.	Function/Feature	RIPv1	RIPv2	OSPF
9.	Variable-length subnets	No	Yes	Yes
10	Supports supernetting	No	Yes	Yes
11	Type of Service (TOS)	No	No	Yes
12	Multipath routing	No	No	Yes
13	Network diameter	15 hops	15 hops	65535 possible
14	Easy to use	Yes	Yes	No

RIP	OSPF
RIP Stands for Routing Information Protocol.	OSPF stands for Open Shortest Path First.
RIP works on the Bellman-Ford algorithm.	OSPF works on Dijkstra algorithm.
It is a Distance Vector protocol and it uses the distance or hops count to determine the transmission path.	It is a link-state protocol and it analyzes different sources like the speed, cost and path congestion while identifying the shortest path.
It is used for smaller size organizations.	It is used for larger size organizations in the network.
It allows a maximum of 15 hops.	There is no such restriction on the hop count.
It is not a more intelligent dynamic routing protocol.	It is a more intelligent routing protocol than RIP.
The networks are classified as areas and tables here.	The networks are classified as areas, sub-areas, autonomous systems, and backbone areas here.
Its administrative distance is 120.	Its administrative distance is 110.

RIP	OSPF
RIP uses UDP(User Datagram Protocol) Protocol.	OSPF works for IP(Internet Protocol) Protocol.
It calculates the metric in terms of Hop Count.	It calculates the metric in terms of bandwidth.
In RIP, the whole routing table is to be broadcasted to the neighbors every 30 seconds by the routers.	In OSPF, parts of the routing table are only sent when a change has been made to it.
RIP utilizes less memory compared to OSPF but is CPU intensive like OSPF.	OSPF device resource requirements are CPU intensive and memory.
It consumes more bandwidth because of greater network resource requirements in sending the whole routing table.	It consumes less bandwidth as only part of the routing table is to send.
Its multicast address is 224.0.0.9.	OSPF's multicast addresses are 224.0.0.5 and 224.0.0.6.

Difference between Distance Vector Routing and Link State Routing:

Sr. No.	Distance Vector Routing	Link State Routing
1.	The distance vector routing determines the direction (vector) and distance (such as link cost or number of hops) to any link in the network.	The link state routing uses the Shortest Path First (SPF) algorithm to create an abstract of the exact topology of the entire network.
2.	Distance vector routing protocols do not have an actual map of the network topology.	A link state routing protocol is like having a complete map of the network topology.
3.	The distance vector routing algorithm is a type of routing algorithm that is based on the number of hops in a route between a source and destination computer.	The link state routing algorithm broadcasts information about the cost of reaching each of its neighbors to all other routers in the network.
4.	Uses Bellman-Ford algorithm.	Uses Dijkstra's algorithm.

Contd...

Advance Computer Network 2.24 Routing Protocols

Sr. No.	Distance Vector Routing	Link State Routing
5.	The name 'distance vector' is used because the routers exchange vectors containing distance and direction information.	In link state routing, each routing node makes a connectivity graph for the nodes in the network and independently calculates its shortest path to every other destination in the network.
6.	Less bandwidth is required.	High bandwidth is required.
7.	Distance vector routing updates full routing table.	Link state routing updates only the link state.
8.	Example of distance vector routing protocols is RIP.	Example of link state routing protocols is OSPF.
9.	The utilization of CPU and memory in distance vector routing is lower than the link state routing.	Higher utilization of CPU and memory.
10.	Distance vector routing does not have any hierarchical design.	Link state routing works best for hierarchical routing design and in networks where fast convergence is crucial.

Distance Vector Routing	Link State Routing
Bandwidth required is less due to local sharing, small packets and no flooding.	Bandwidth required is more due to flooding and sending of large link state packets.
Based on local knowledge, since it updates table based on information from neighbours.	Based on global knowledge, it have knowledge about entire network.

Distance Vector Routing	Link State Routing
Make use of Bellman Ford Algorithm.	Make use of Dijakstra's algorithm.
Traffic is less.	Traffic is more.
Converges slowly i.e, good news spread fast and bad news spread slowly.	Converges faster.
Count of infinity problem.	No count of infinity problem.
Persistent looping problem i.e, loop will be there forever.	No persistent loops, only transient loops.
Practical implementation is RIP and IGRP.	Practical implementation is OSPF and ISIS.

Comparison between RIP and OSPF:

Sr. No.	RIP	OSPF
1.	RIP is a distance vector routing protocol that has two versions namely, RIPv1 and RIPv2.	OSPF is a link state routing protocol.
2.	RIP is easy to configure.	OSPF is complicated to configure and Requires network design and planning.
3.	RIP networks cannot grow larger than 15 hops.	OSPF networks are technically unlimited in size.
4.	An end system (a system with only one network interface) can run RIP in passive mode to listen for routing information.	OSPF does not have a passive mode.
5.	RIP uses much more bandwidth because of its distance vector behavior.	OSPF requires lower bandwidth than RIP.
6.	In RIP, the networks are classified as areas and tables.	In OSPF, the networks are classified as areas, sub areas, autonomous systems and backbone areas.
7.	RIP may be slow to adjust for link failures.	OSPF is quick to adjust for link failures.
8.	The RIP routing protocol uses the distance vector algorithm.	OSPF uses the shortest path algorithm Dijkstra to determine the transmission routes.
9.	RIP generates more protocol traffic than OSPF.	OSPF generates less protocol traffic than RIP.
10.	RIP is simpler routing protocol.	OSPF is much more complex protocol.
11.	RIP is not well suited to large networks, because RIP packet size increases as the number of networks increases.	OSPF works well in large networks.

Ans. The following table differentiate between Static Routing and Dynamic Routing.

Sr. No.	Parameters	Static Routing	Dynamic Routing
1.	Routing	In static routing, user-defined routes are used in the routing table.	In dynamic routing, routes are updated as per the changes in network.
2.	Scalability	Limited.	High.
3.	Protocols used	Static routing may not follow any specific protocol. Static routing involves manually configuring routes on network devices.	Dynamic routing uses protocols (like OSPF, RIP, EIGRP) that enable routers to communicate and automatically adjust routes in response to network changes.
4.	Security	Higher security	Less security.
5.	Automation	Static routing is a manual process.	Dynamic routing is an automatic process.

5. Explain any three Intra-domain routing protocols.

Static Routing	Dynamic Routing
In static routing routes are user-defined.	In dynamic routing, routes are updated according to the topology.
Static routing does not use complex routing algorithms.	Dynamic routing uses complex routing algorithms.
Static routing provides high or more security.	Dynamic routing provides less security.
Static routing is manual.	Dynamic routing is automated.
Static routing is implemented in small networks.	Dynamic routing is implemented in large networks.
In static routing, additional resources are not required.	In dynamic routing, additional resources are required.
In static routing, failure of the link disrupts the rerouting.	In dynamic routing, failure of the link does not interrupt the rerouting.
Less Bandwidth is required in Static Routing.	More Bandwidth is required in Dynamic Routing.
Static Routing is difficult to configure.	Dynamic Routing is easy to configure.
Another name for static routing is non-adaptive routing.	Another name for dynamic routing is adaptive routing.

Sr. No.	Distance vector routing	Link state routing
1.	Each router maintains routing table indexed by and containing one entry for each router in the subnet.	It is the advanced version of distance vector routing
2.	Algorithm took too long to converge.	Algorithm is faster.
3.	Bandwidth is less.	Wide bandwidth is available.
4.	Router measure delay directly with special ECHO packets.	All delays measured and distributed to every router.
5.	It doesn't take line bandwidth into account when choosing the routes.	It considers the line bandwidth into account when choosing the routes.

Table 2.7.2 : Comparison of static and dynamic routing

Sr. No.	Parameter	Static routing	Dynamic routing
1.	Updating of the routing tables	Manually done	Automatically done
2.	Bandwidth requirement	Less	More
3.	Application area	In small networks	In large networks
4.	Routing protocols	None	EIGRP, ARP etc.
5.	Security	Highly secure	Less secure
6.	Routing algorithms	Shortest path, flooding, flow based routing	Distance vector, link state
7.	Link failure	Any link failure affects the other routing paths	Does not affect other routing paths
8.	Additional resources	Not required	Required to store information
9.	Routing decision	Not based on the measured or estimated current traffic	Is based on the changes in topology or traffic
10.	Configuration	Difficult to configure	Easy to configure
11.	Security	Highly secure	Less secure
12.	Routing protocols	None	EIGRP, ARP etc.
13.	Cost	Less	More

UNIT 3

Table 3.2.1 : Comparison of CLTS & COTS

Sr. No.	Parameter	Connection oriented	Connectionless
1.	Reservation of resources	Necessary	Not necessary
2.	Utilization of resources	Less	Good
3.	State information	Lot of information required	Not much information is required to be stored
4.	Guarantee of service	Guaranteed	No guarantee
5.	Connection	Connection needs to be established	Connection need not be established
6.	Delays	More	Less
7.	Overheads	Less	More
8.	Packets travel	Sequentially	Randomly
9.	Congestion due to overloading	Not possible	Very much possible

Connection-oriented Service	Connection-less Service
Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
Connection-oriented Service is necessary.	Connection-less Service is not compulsory.
Connection-oriented Service is feasible.	Connection-less Service is not feasible.
In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give a guarantee of reliability.
Includes error detection, correction, and retransmission.	No error handling; errors are not corrected.
In connection-oriented Service, Packets follow the same route.	In connection-less Service, Packets do not follow the same route.
Ensures data is delivered in the correct order.	Data may arrive out of order or not at all.
Less scalable due to the need for maintaining connections.	Highly scalable for large networks with many users.
Higher overhead due to connection setup and maintenance.	Lower overhead as no connection is required.

Connection-oriented Service	Connection-less Service
Connection-oriented services require a bandwidth of a high range.	Connection-less Service requires a bandwidth of low range.
Ex: TCP (Transmission Control Protocol)	Ex: UDP (User Datagram Protocol)
Connection-oriented requires authentication.	Connection-less Service does not require authentication.

Table 3.14.1 : Comparison of UDP and TCP

Sr. No.	Characteristic / Description	UDP	TCP
1.	General Description	Simple, high-speed, low-functionality "wrapper" that interfaces applications to the network layer and does little else.	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
2.	Protocol Connection Setup	Connectionless; data is sent without setup.	Connection-oriented; connection must be established prior to transmission.
3.	Data Interface To Application	Message-based; data is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure.
4.	Reliability and Acknowledgments	Unreliable, best-effort delivery without acknowledgments	Reliable delivery of all messages; data is acknowledged.

Sr. No.	Characteristic / Description	UDP	TCP
5.	Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.
6.	Features Provided to Manage Flow of Data	None	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms.
7.	Overhead	Very low	Low, but higher than UDP
8.	Transmission Speed	Very high	High, but not as high as UDP
9.	Data Quantity Suitability	Small to moderate amounts of data (up to a few hundred bytes)	Small to very large amounts of data (up to gigabytes)
10.	Types of Applications That Use The Protocol	Applications where data delivery speed matters more than completeness, where small amounts of data are sent; or where multicast/broadcast are used.	Most protocols and applications sending data that must be received reliably, including most file and message transfer protocols.
11.	Well-Known Applications and Protocols	Multimedia applications, DNS, BOOTP, DHCP, TFTP, SNMP, RIP, NFS (early versions).	FTP, Telnet, SMTP, DNS, HTTP, POP, NNTP, IMAP, BGP, IRC, NFS (later versions).
12.	Error control	Only checksum.	Provided.

Table 3.19.1 : Comparison between TCP, UDP and SCTP

Sr. No.	Parameter	TCP	UDP	SCTP
1.	Reliability	Reliable	Unreliable	Reliable
2.	Connection management	Connection oriented	Connectionless	Connection oriented
3.	Transmission of message	Byte oriented	Message oriented	Message oriented
4.	Flow control	Yes	No	Yes
5.	Security	Yes	Yes	Improved
6.	Data delivery	Strictly ordered	Unordered	Partially ordered

Following table compare TCP and UDP:

Sr. No.	Characteristics	TCP	UDP
1.	Connection	TCP is connection oriented Protocol.	UDP is connection less protocol.
2.	Reliability	It provides reliable delivery of messages.	It provides unreliable delivery of messages.
3.	Error Handling	TCP makes checks for errors and reporting.	UDP does error checking but no reporting.
4.	Flow controlling	TCP has flow control.	UDP has no flow control.
5.	Data transmission order	TCP gives guarantee that the order of the data at the receiving end is the same as the sending end.	No guarantee of the data transmission order.
6.	Header Size	20 bytes.	8 bytes.
7.	Acknowledgment	TCP acknowledges the data reception.	UDP has no acknowledgment Section.
8.	Use	Used where reliability is important.	Used where time sensitivity is more important.
9.	Data Interface to application	Stream-based: No particular structure for data.	Message based data: Data sent in discrete packages by application.
10.	Overhead	Low.	Very low.
11.	Speed	High.	Very high.
12.	Application	FTP, Telnet, SMTP, DNS, HTTP.	DNS, BOOTP, DHCP, TFTP, RIP.

Contd...

Basis	Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
Type of Service	TCP is a connection-oriented protocol. Connection orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, or terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.
Reliability	TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
Error checking mechanism	TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error-checking mechanism using checksums.
Acknowledgment	An acknowledgment segment is present.	No acknowledgment segment.
Sequence	Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in order at the receiver.	There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer.
Speed	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.

Basis	Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
Retransmission	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
Header Length	TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.
Weight	TCP is heavy-weight.	UDP is lightweight.
Handshaking Techniques	Uses handshakes such as SYN, ACK, SYN-ACK	It's a connectionless protocol i.e. No handshake
Broadcasting	TCP doesn't support Broadcasting.	UDP supports Broadcasting.
Protocols	TCP is used by HTTP, HTTPs , FTP , SMTP and Telnet .	UDP is used by DNS , DHCP , TFTP, SNMP , RIP , and VoIP .
Stream Type	The TCP connection is a byte stream.	UDP connection is a message stream.
Overhead	Low but higher than UDP.	Very low.
Applications	This protocol is primarily utilized in situations when a safe and trustworthy communication procedure is necessary, such as in email, on the web surfing, and in military services.	This protocol is used in situations where quick communication is necessary but where dependability is not a concern, such as VoIP, game streaming, video, and music streaming, etc.

Protocol	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)	SCTP (Stream Control Transmission Protocol)
Reliability	Reliable data delivery with error detection, retransmission, and acknowledgement mechanisms	Unreliable data delivery without error recovery or acknowledgement	Reliable data delivery with error detection, retransmission, and acknowledgement mechanisms
Connection Type	Connection-oriented	Connectionless	Connection-oriented
Ordering	Guarantees ordered delivery of data packets	Does not guarantee the ordered delivery of data packets	Guarantees ordered delivery of data packets

Protocol	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)	SCTP (Stream Control Transmission Protocol)
Speed	Slower due to reliability mechanisms	Faster due to minimal overhead	Comparable to TCP, slower than UDP due to additional functionality
Overhead	Higher overhead due to additional headers and control mechanisms	Lower overhead due to minimal headers and control mechanisms	Moderate overhead due to additional headers and control mechanisms
Applications	Web browsing, email transfer, file transfer (FTP)	Real-time communication, video streaming, online gaming, DNS	Telecommunications, voice and video over IP, signalling transport
Congestion Control	Implements congestion control mechanisms to optimize network performance	No congestion control mechanisms	Implements congestion control mechanisms to optimize network performance
Error Recovery	Detects and retransmits lost or corrupted packets	No error recovery mechanisms	Detects and retransmits lost or corrupted packets
Message-Oriented Delivery	No	No	Yes, supports message-oriented delivery
Multi-streaming	No	No	Yes, supports the simultaneous transmission of multiple streams
Multi-homing	No	No	Yes, supports multiple IP addresses for fault tolerance and resilience

UNIT 4

Sr. No.	Parameter	SMTP	POP3
1.	Full form	Simple mail transfer protocol	Post office protocol version 3
2.	Function	Used for sending email messages	Used for receiving email messages
3.	Port number	25	110
4.	Known as	Push protocol	POP protocol
5.	E-mail storage	Does not store emails on the server	Stores emails on the server until downloaded by the user.

Sr. No.	Parameter	SMTP	POP3
6.	Connection type	Connection oriented	Connection less
7.	Security	Uses SSL / TLS encryption for secure email transmission	Uses SSL / TLS encryption for secure email retrieval.
8.	Protocol used	TCP	TCP

SMTP	POP3
SMTP stands for Simple Mail Transfer Protocol.	POP3 stands for Post Office Protocol version 3.
It is used for sending messages.	It is used for accessing messages.
The port number of SMTP is 25, 465, and 587 for secured connection (TLS connection).	The port number of POP3 is 110 or port 995 for SSL/TLS connection.
It is an MTA (Message Transfer Agent) for sending the message to the receiver.	It is MAA (Message Access Agent) for accessing the messages from mailbox.
It has two MTAs one is client MTA (Message Transfer Agent) and second one is server MTA (Message Transfer Agent).	It has also two MAAs one is client MAA (Message Access Agent) and another is server MAA(Message Access Agent).
SMTP is also known as PUSH protocol.	POP3 is also known as POP protocol.
SMTP transfers the mail from sender's computer to the mail box present on receiver's mail server.	POP3 allows to retrieve and organize mails from mailbox on receiver mail server to receiver's computer.
It is implied between sender mail server and receiver mail server.	It is implied between receiver and receiver mail server.

Table 4.10.2 : Comparison of IMAP and POP 3

Sr. No.	Parameter	POP 3	IMAP
1.	Protocol is defined at	RFC 1939	RFC 2060
2.	TCP port used	110	143
3.	e-mail is stored at	User's PC	Server
4.	e-mail is read	Off line	On line
5.	Time required to connect	Small	Long
6.	Use of server resources	Minimal	Extensive
7.	Multiple mail boxes	Not possible	Possible
8.	Who backs up mailboxes	User	ISP
9.	For mobile users	Not good	Good
10.	User control over download	Little	Great
11.	Partial message downloads	No	Yes
12.	Simplicity in implementation	Yes	No
13.	Support	Wide spread	Increasing

Post Office Protocol (POP3)	Internet Message Access Protocol (IMAP)
POP is a simple protocol that only allows downloading messages from your Inbox to your local computer.	IMAP (Internet Message Access Protocol) is much more advanced and allows the user to see all the folders on the mail server.
The POP server listens on port 110, and the POP with SSL secure(POP3DS) server listens on port 995	The IMAP server listens on port 143, and the IMAP with SSL secure(IMAPDS) server listens on port 993.
In POP3 the mail can only be accessed from a single device at a time.	Messages can be accessed across multiple devices
To read the mail it has to be downloaded on the local system.	The mail content can be read partially before downloading.
The user can not organize mail in the mailbox of the mail server.	On the mail server, the user can directly arrange the email.
The user can not create, delete,e or rename email on the mail server.	The user can create, delete,e or rename an email on the mail server.
It is unidirectional i.e. all the changes made on a device do not affect the content present on the server.	It is Bi-directional i.e. all the changes made on the server or device are made on the other side too.
It does not allow a user to sync emails.	It allows a user to sync their emails.

Post Office Protocol (POP3)	Internet Message Access Protocol (IMAP)
It is fast.	It is slower as compared to POP3.
A user can not search the content of mail before downloading it to the local system.	A user can search the content of mail for a specific string before downloading.
It has two modes: delete mode and keep mode. • In delete mode, the mail is deleted from the mailbox after retrieval. • In keep mode, the mail remains in the mailbox after retrieval.	Multiple redundant copies of the message are kept at the mail server, in case of loss of message on a local server, the mail can still be retrieved
Changes in the mail can be done using local email software.	Changes made to the web interface or email software stay in sync with the server.
All the messages are downloaded at once.	The Message header can be viewed before downloading.

Table 4.15.1 : Comparison of HTTP and SMTP

Sr. No.	SMTP	HTTP
1.	Message is transferred from client to server.	Message transfer is from client to server or the other way round.
2.	Uses TCP.	Uses TCP.
3.	Uses port 25 for transmission.	Uses port 80 for transmission.
4.	SMTP messages are to be read by humans.	HTTP messages are to be read and understood by the HTTP servers and HTTP clients.
5.	These messages are first stored and then forwarded.	These messages are immediately delivered.

SMTP	HTTP
SMTP is used for mail services.	HTTP is mainly used for data and file transfer.
It uses port 25.	It uses port 80.
It is primarily a push protocol.	It is primarily a pull protocol.
It imposes a 7-bit ASCII restriction on the content to be transferred.	It does not impose a 7-bit ASCII restriction. Can transfer multimedia, hyperlinks, etc.

SMTP	HTTP
SMTP transfers emails via Mail Servers.	HTTP transfers files between the Web server and the Web client.
SMTP is a persistent type of TCP connection.	It can use both Persistent and Non-persistent.
Uses base64 encoding for authentication.	Uses different methods of authentication such as basic, digest, and OAuth.
Does not support session management or cookies.	Supports session management and cookies to maintain state.
Has a smaller message size limit compared to HTTP.	Has a larger message size limit compared to SMTP.
Requires authentication for sending emails.	Does not require authentication for browsing web pages.
Supports both plain text and encrypted communication (SMTPS or STARTTLS).	Supports both plain text and encrypted communication (HTTPS).

Fig. 4.32

Difference between SMTP and POP3:

Sr. No.	SMTP	POP3
1.	It is message transfer agent.	It is message access agent.
2.	Stands for Simple Mail Transfer Protocol.	Stands for Post Office Protocol version 3.
3.	Between sender and sender mail server and between sender mail server and receiver mail server.	Between receiver and receiver mail server.
4.	It transfers the mail from sender's computer to the mail box present on receiver's mail server.	It allows to retrieve and organize mails from mailbox on receiver mail server to receiver's computer.
5.	SMTP is an application layer protocol that is used to send e-mail from the client to the mail server.	POP3 is an application layer protocol used by email systems to retrieve mail from e-mail servers.
6.	SMTP is an Internet protocol for transmitting e-mail over IP networks.	POP3 is an Internet protocol used to retrieve e-mail from a mail server POP3 access incoming mails.
7.	It uses port 24 for transfer of all outgoing e-mail.	An e-mail client connects with a POP3 server via port 110.

Contd...

4.27 Application Layer Protocols

Comparison between POP and IMAP:

Sr. No.	POP	IMAP
1.	Generally used to support single client.	Designed to handle multiple clients.
2.	Messages are accessed offline.	Messages are accessed online although it also supports offline mode.
3.	POP does not allow search facility.	It offers ability to search e-mails.
4.	All the messages have to be downloaded.	It allows selective transfer of messages to the client.
5.	Only one mailbox can be created on the server.	Multiple mailboxes can be created on the server.
6.	Not suitable for accessing non-mail data.	Suitable for accessing non-mail data i.e., attachment.
7.	It requires minimum use of server resources.	Clients are totally dependent on server.
8.	POP requires less internet usage time.	IMAP requires more internet usage time.
9.	POP is a stateful protocol until the mail is downloaded as well as stateless across sessions.	IMAP is a stateful protocol because the IMAP server has to maintain a folder hierarchy for each of its users.

Differences between FTP and TFTP: [S-22, S-23, W-24]

Sr. No.	Parameters	FTP	TFTP
1.	Stands for	File Transfer Protocol.	Trivial File Transfer Protocol.
2.	Features	Authentication, encryption, and error recovery.	Basic file transfer only.
3.	Protocol Complexity	More complex and heavier.	Less complex and lightweight.
4.	Ports used	FTP works on ports 20 and 21.	TFTP works on port 69.
5.	Protocol used	FTP is based on TCP.	TFTP is based on UDP.
6.	Authentication	Authentication is must for FTP.	Authentication is not required in case of TFTP.
7.	Use Cases	General file transfer, Web servers etc.	Network device configuration, Booting etc.

Difference between FTP and HTTP:

Sr. No.	FTP	HTTP
1.	FTP is used to access and transfer files.	HTTP is used to view websites.
2.	FTP is efficient in transferring larger files.	HTTP is efficient in transferring smaller files like web pages.
3.	FTP can be accessed via the command line or graphical client of its own.	The common HTTP client is the browser.
4.	FTP establishes two connection one for data and one for the control connection.	HTTP establishes data connection only.
5.	FTP uses TCP's port number 20 and 21.	HTTP uses TCP's port number 80.
6.	If you are using FTP, ftp will appear in URL.	If you are using HTTP, http will appear in URL.
7.	FTP session (stateful).	No session (stateless).
8.	FTP is comparatively simple.	Web clients and servers became very complex since they need to support many protocols, scripting languages, file types etc. Complexity is also a security problem.
9.	FTP is better suited (faster, more efficient) for large files.	HTTP is better suited for the transfer of many small files.
10.	FTP has a control and a data connection and communicates TCP port numbers for data connection in control connection.	HTTP uses a single TCP connection for control and data.
11.	FTP requires a password.	HTTP does not require authentication.
12.	FTP transmits data as ASCII or binary.	HTTP always sends data in binary format.

Feature	FTP	TFTP
Purpose	Transfer files between computers	Transfer files between computers
Connection	Establishes a connection between two computers, allowing for a more complex set of commands and options	Establishes a connection between two computers, but with a more limited set of commands and options
Authentication	Uses username and password for authentication	Does not support authentication
Security	Encrypts data transfer	Does not encrypt data transfer
Error handling	Can recover from errors during transfer	Does not have error recovery
File transfer mode	Supports both ASCII and binary transfer modes	Only supports binary transfer mode
Transfer options	Supports resuming interrupted transfers and setting transfer mode, transfer type, and other options	Does not support any transfer options

UNIT 5

Table 5.1.6 : Comparison of various mobile system generations

Sr. No.	Feature	Generation				
		1G	2G	3G	4G	5G
1.	Generation	First	Second	Third	Fourth	Fifth
2.	Year of introduction	1970	1990	2001	2010	2020
3.	Technology	Analog cellular	Digital cellular	Broadband, IP, FDD, TDD	IP-broadband Wi-Fi, MIMO	IPv6
4.	Standard	AMPS	CDMA, TDMA, GSM	CDMA, UMTS, W-CDMA	Wi-Max and LTE	Yet to be finalized
5.	Switching	Circuit	Circuit / Packet	Circuit/Packet	Packet	packet
6.	Frequency band	824-894 MHz	850-1900 MHz	1.6-2.5 GHz	2-8 GHz	15 GHz
7.	Data speed	2.4 kbps	9.6 kbps	2 Mbps	50 Mbps	Higher than 1 Gbps
8.	Multiplexing	FDMA	CDMA, TDMA	CDMA	MC-CDMA OFDM	MC-CDMA, LAS-CDMA, OFDM
9.	Core network	PSTN	PSTN	Packet Network	Internet	Internet
10.	Services	Only voice or only message	Digital voice, Data, SMS	High speed data, Voice, Video	Dynamic Information Access	Interactive multimedia, Voice over IP

TechKnowledge

Parameter	1G (Analog)	2G (Digital)	3G (Mobile Broadband)	4G (High-Speed IP)	5G (Next-Gen Network)
Launch Era	1980s	Early 1990s	Early 2000s	Late 2000s	2020s
Technology	Analog	GSM, CDMA	UMTS, CDMA2000	LTE, WiMAX	NR (New Radio), mmWave
Data Speed	~2.4 kbps	~64–100 kbps	~2 Mbps	100 Mbps–1 Gbps	Up to 10 Gbps
Latency	High	Moderate	~100 ms	~30–50 ms	~1 ms
Bandwidth	Narrow	Narrow	Medium	Wide	Ultra-wide
Modulation	FM	GMSK	QPSK	OFDMA	OFDMA, Massive MIMO
Security	None	Basic (GSM encryption)	Improved (SSL, VPN)	Strong (IPSec)	Advanced (network slicing, encryption)
Voice Quality	Poor	Good	Better	HD Voice	Crystal-clear
Mobility Support	Basic	Good	Excellent	Excellent	Seamless handover
Coverage	Limited	Wide	Wider	Global	Dense urban + rural
Power Efficiency	Low	Moderate	Moderate	High	Very high
Device Density	Low	Low	Moderate	High	Massive (IoT scale)
Use Cases	Voice calls	SMS, voice	Web browsing, email	Streaming, gaming	AR/VR, IoT, automation

Table 5.3.1 : Comparison of NFV and SDN

Sr. No.	Parameter	Network function virtualization (NFV)	Software defined networks (SDN)
1.	Formalization	ETSI (European Telecommunications Standards Institute).	Open Networking Foundation (ONF)
2.	Basic concept	Relocate network functions from dedicated applications to generic servers.	Separate control and data, centralize control and programmability of network.
3.	Target location	Service provider network	Campus, data center/cloud

SDN	NFV
SDN architecture mainly focuses on data centers.	NFV is targeted at service providers or operators.
SDN separates control plane and data forwarding plane by centralizing control and programmability of network.	NFV helps service providers or operators to virtualize functions like load balancing, routing, and policy management by transferring network functions from dedicated appliances to virtual servers.
SDN uses OpenFlow as a communication protocol.	There is no protocol determined yet for NFV.
SDN supports Open Networking Foundation.	NFV is driven by ETSI NFV Working group.
Various enterprise networking software and hardware vendors are initiative supporters of SDN.	Telecom service providers or operators are prime initiative supporters of NFV.
Corporate IT act as a Business initiator for SDN.	Service providers or operators act as a Business initiator for NFV.
SDN applications run on industry-standard servers or switches.	NFV applications run on industry-standard servers.
SDN reduces cost of network because now there is no need of expensive switches & routers.	NFV increases scalability and agility as well as speed up time-to-market as it dynamically allot hardware a level of capacity to network functions needed at a particular time.
Application of SDN: • Networking	Application of NFV: • Routers, firewalls, gateways

SDN	NFV
• Cloud orchestration	• WAN accelerators • SLA assurance • Video Servers • Content Delivery Networks (CDN)

Sr. No.	Parameter	Network function virtualization (NFV)	Software defined networks (SDN)
4.	Target devices	Commodity servers and switches	Commodity servers and switches
5.	Applications	Routers, firewalls, gateways, content delivery network, WAN accelerators, SLA assurance.	Networking
6.	New protocol	None	Openflow

(GT-68) Table 5.11.1 : Comparison of stored, live and interactive streaming

Sr. No.	Parameter of comparison	Streaming of		
		Stored audio / video	Live audio / video	Interactive audio / video
1.	Principle of operation	The prerecorded audio / video contents on a server, that a client can download	Audio / video contents are broadcast on the internet	People communicate via audio / video, in real time
2.	Real time aspect	Not applicable	Not applicable	Real time interactive communication
3.	Need of downloading	Downloading is needed at the client	Not needed	Not needed
4.	Examples	Audio on demand, video on demand	Internet radio, internet TV	Video conferencing
5.	Sensitivity to delays	System is sensitive to delays	Yes, sensitive to delays	Yes, sensitive to delays
6.	Type of communication	Unicast & on demand	Multicast and live	Multicast and live
7.	Retransmission request	Not accepted	Not accepted	Not accepted
8.	Direction of communication	One way	One way	Two way
9.	Protocols used	HTTP, RTSP, IP	RTP, UDP, IP, TCP	UDP, TCP, IP

Comparison of 3G vs 4G vs 5G:

Feature	3G	4G	4G+ (LTE Advanced)	5G
Peak Data Rate	Up to 42 Mbps	Up to 1 Gbps	Up to 3 Gbps	Up to 20 Gbps
Latency	100-500 ms	20-30 ms	10-20 ms	1-4 ms
Frequency Bands	850 MHz - 2.1 GHz	600 MHz - 2.5 GHz	600 MHz - 6 GHz	600 MHz - 100 GHz
Network Architecture	Circuit-Switched	Packet-Switched	Packet-Switched	Packet-Switched, Virtualized
Download/Upload Speed	3-7 Mbps / 1 Mbps	10-50 Mbps / 10 Mbps	100-150 Mbps / 50 Mbps	100 Mbps-10 Gbps / Up to 10 Gbps
Use Cases	Voice, SMS, MMS	Streaming, VoIP, Web	HD Streaming, IoT	IoT, VR/AR, Autonomous Vehicles
Backwards Compatibility	2G	3G, some 2G	4G, 3G	4G, 3G, 2G

capabilities.

Difference between SDN and NFV:

Features	SDN	NFV
Scope	SDN is primarily focused on the control and management of network traffic flows.	NFV is focused on the virtualization and management of network functions.
Functionality	SDN separates the control plane (which determines how traffic is routed) from the data plane (which handles the actual transmission of data), allowing for more flexible and programmable network management.	NFV virtualizes network functions such as routing, switching, firewalling, and load balancing, allowing these functions to be deployed and managed as software-based virtual network functions (VNFs).
Deployment	SDN typically requires specialized network hardware, such as switches and routers, that support OpenFlow or other SDN protocols.	NFV can be deployed on standard x86 servers, storage, and switches.
Management and Orchestration	SDN typically relies on centralized controllers that manage and orchestrate network traffic flows.	NFV also requires management and orchestration, but this is typically focused on the deployment and management of VNFs.
Standards	SDN is primarily defined by the Open Networking Foundation (ONF) and the OpenFlow protocol.	NFV is defined by the European Telecommunications Standards Institute (ETSI) and its NFV Industry Specification Group (ISG).
	Note: Both technologies are based on open standards, there are some differences in the specific standards and protocols used by each.	

Contd...

Network Architecture	SDN is typically used to create a centralized, software-defined network architecture that is more programmable and easier to manage.	NFV, on the other hand, is focused on virtualizing network functions to create a more flexible and scalable network architecture.
Network Abstraction	SDN abstracts the network infrastructure from the control plane, allowing network administrators to define network policies and configurations that are separate from the underlying hardware.	NFV abstracts network functions from the underlying hardware, allowing them to be deployed and managed independently of the physical infrastructure.
Service Delivery	SDN can be used to enable new service delivery models, such as network slicing, that allow network resources to be allocated dynamically based on the needs of specific applications or services.	NFV can also enable new service delivery models by allowing network functions to be deployed and scaled up or down based on demand.
Vendor Ecosystem	SDN has a larger and more mature vendor ecosystem than NFV, with a wide range of products and solutions available from established networking vendors as well as startups.	NFV is still a relatively new technology, and the vendor ecosystem is still evolving.

Difference between Edge computing and Edge networking:

Feature	Edge Computing	Edge Networking
Definition	Processing data at or near the source of data generation.	The communication infrastructure that connects edge devices.
Main Goal	Reduce latency by minimizing the need to send data to the cloud.	Ensure data can travel efficiently between edge devices and networks.
Focus Area	Computation and data processing.	Data transmission and connectivity.
Key Components	Edge servers, gateways, local devices with processing power.	Routers, switches, edge routers, network protocols.
Example Use Case	A factory floor machine analyzing sensor data locally.	Enabling 5G connectivity to smart traffic lights.
Reduces Load On	Cloud servers and data centers. Cloud servers and data centers.	Backbone networks and central routers.
Latency	Ultra-low, as processing happens locally.	Low, optimized by shorter data travel routes.
Dependency	Relies on edge networking for connectivity.	Relies on edge computing to process and act on data locally.
Common Technologies	AI at the edge, local data analytics, edge containers.	SD-WAN, 5G, edge switches, network slicing.

Feature	Edge Computing	Edge Networking
Definition	Processing data near the source (e.g., IoT devices)	Connecting devices and systems at the network edge
Primary Function	Compute and store data locally	Route and manage data traffic efficiently
Focus Area	Data processing and analytics	Data transmission and connectivity
Key Components	Edge servers, micro data centers, IoT processors	Routers, switches, gateways, access points
Latency Impact	Reduces latency by avoiding cloud round-trips	Optimizes latency through efficient routing
Use Cases	Real-time analytics, autonomous vehicles, smart factories	CDN delivery, 5G networks, IoT device communication
Relation to Cloud	Complements cloud by offloading tasks	Connects edge devices to cloud or central systems

Feature	Edge Computing	Edge Networking
Security Role	Ensures local data privacy and compliance	Secures data in transit across edge devices

used in multimedia streaming.

Feature	RTP	RTSP
Definition	A transport protocol designed to transmit audio and video data in real time.	A control protocol used to manage and control streaming media sessions between clients and servers.
Primary Function	Handles the actual transmission of multimedia data (e.g., audio, video).	Provides commands for session control (e.g., play, pause, stop, teardown).
Role	Focuses on delivering media packets efficiently with synchronization and jitter control.	Acts as a "remote control" for managing media streams but does not transmit the media itself.
Data Transmission	Operates over UDP/IP to ensure low latency in delivering multimedia packets.	Establishes control connections over TCP to manage sessions; uses RTP for actual data transmission.
Session Control	Does not provide session control; only transmits data.	Enables session setup, playback control, and termination using commands like PLAY or PAUSE.
Protocol Interaction	Works alongside RTCP for feedback on stream quality.	Works with RTP to transport media after negotiating session parameters.
Use Cases	Used in live streaming, VoIP (Voice over IP), and video conferencing for transmitting real-time data.	Commonly used for video surveillance (IP cameras), IPTV, and interactive video-on-demand services.
Scenarios	Ideal for transmitting raw multimedia data efficiently across networks.	Suitable for applications requiring user interaction with streams, such as pausing or rewinding content.
Synchronization	Provides mechanisms for synchronizing audio and video streams.	Allows segmented streaming so users can start viewing before full download.
Functionality	RTP focuses solely on transporting multimedia data.	RTSP is responsible for controlling how the multimedia is streamed.
Protocol Dependency	RTP can function independently for raw media transmission.	RTSP relies on RTP (and sometimes RTCP) to handle actual media delivery.
Use Case Focus	RTP is ideal for applications requiring efficient data transfer, such as live broadcasting.	RTSP is better suited for interactive applications like surveillance systems or video-on-demand.

Contd...

Advance Computer Network

Feature	RTP (Real-time Transport Protocol)	RTSP (Real-time Streaming Protocol)
Purpose	Transports real-time audio and video data	Controls the streaming session (play, pause, etc.)
Protocol Layer	Transport layer (typically over UDP)	Application layer (typically over TCP)
Function	Delivers media packets in real time	Manages and controls media delivery
Direction	One-way (server to client)	Bi-directional (client ↔ server)
Transport Protocol	Usually UDP (sometimes TCP)	Usually TCP
Session Control	No session control	Provides session control (start, stop, seek)
Used With	Often used with RTSP or SIP	Often used alongside RTP for control
Example Use Case	Streaming live video/audio	Controlling playback of a video stream