NETWORK LAYER

Multiple Choice Type Questions

1. Which of the following statement(s) is / are TRUE about datagram? [WBUT 2013]
P: Each packet contains the full source and destination address.
Q: Two packets between a source and destination can follow different paths.
a) P only b) Q only c) Both P & Q d) Neither P nor Q
Answer: (c)

2. Identify the class of IP address 229.1.2.3 [WBUT 2013]
a) Class A b) Class B c) Class C d) Class D
Answer: (d)

3. We use _____ algorithm in Link State Routing and _____ algorithm in Distance Vector Routing for shortest path. [WBUT 2013]
a) Dijkstra's Algorithm, Bellman Ford Algorithm
b) Bellman Ford Algorithm, Dijkstra's Algorithm
c) Prim's Algorithm, Bellman Ford Algorithm
d) Dijkstra's Algorithm, Kruskal Algorithm
Answer: (a)

4. In which routhing there is a concept of Speaker Node? [WBUT 2013]
a) Distance vector routing
b) Link state routing
c) Path vector routing
d) Both Path vector and Distance vector routing
Answer: (c)

5. Minimum size of the data portion of the IP datagram is [WBUT 2013]
a) 65515 bytes b) 65555 bytes c) 65535 bytes d) none of these
Answer: (c)

6. ICMP resides at the same layer as [WBUT 2015]
a) TCP b) UDP c) IP d) ARP
Answer: (d)

7. Which of the following is a valid host for network 192.168.10.32/28? [WBUT 2015]
a) 192.168.10.39 b) 192.168.10.47 c) 192.168.10.14 d) 192.168.10.54
Answer: (a)

8. When a host knows its IP address but not its physical address, it can use [WBUT 2015]
a) RARP b) ICMP c) ARP d) IGMP
Answer: (c)

9. Which class of IP address is reserved for multicast communication? [WBUT 2015]

a) Class *A* b) Class *B* c) Class *C* d) Class *D*

Answer: (d)

10. The address space of IPV4 is [WBUT 2015]

a) 2^{16} b) infinite c) 2^{32} d) none of these

Answer: (c)

11. Which of the following IP address class is Unicast? [WBUT 2016]

a) Class A b) Class B c) Class C d) all of these

Answer: (d)

12. Routing information protocol is implemented by [WBUT 2016]

a) distance vector routing b) path vector routing

c) static routing d) none of these

Answer: (a)

13. Which of the following IP address class is Multicast? [WBUT 2017]

a) Class A b) Class B c) Class C d) Class D

Answer: (d)

14. The last address of IP address represents [WBUT 2017]

a) Unicast address b) Network address

c) Broadcast address d) none of these

Answer: (c)

15. Router is a ..... internetworking device. [WBUT 2017]

a) two layered b) three layered

c) both (a) and (b) d) none of these

Answer: (b)

Short Answer Type Questions

1. Indicate the characteristics of BGP. [WBUT 2013]

Answer:

The key characteristics of BGP include the following:

- BGP is termed a path vector protocol.
- BGP uses TCP as the transport layer protocol.
- Full routing tables are exchanged only during the initial BGP session.
- Updates are sent over TCP port 179.
- BGP sessions are maintained by keep alive messages.
- Any network changes result in update messages.
- BGP has its own BGP table. Any network entry must reside in the BGP table first.

- BGP has a complex array of metrics, called attributes, which include the next hop address and origin.
- BGP supports variable-length subnet masking (VLSM) and summarization (sometimes called classless interdomain routing [CIDR]).

2. Draw various fields in IP packet header. What is the significance of total length field? **[WBUT 2013]**

Answer:

The header consists of 13 fields and, of which, only 12 are required. The 13th field is optional.

+	Bits 0 - 3	4 - 7	8 - 15	16 - 18	19	20 - 31
0	Version	Header length	Type of Service (now DiffServ and ECN)	Total Length		
32	Identification			Flags	Evil Bit	Fragment Offset
64	Time to Live		Protocol	Header Checksum		
96	Source Address					
128	Destination Address					
160	Options					
160/192+	Data					

Total Length

This field defines the entire datagram size, including header and data, in bytes. The minimum-length datagram is 20 bytes (20 bytes header + 0 bytes data) and the maximum is 65,535 — the maximum value of a 16-bit word. The minimum size datagram that any host is **required** to be able to handle is 576 bytes, but most modern hosts handle much larger packets.

3. Differentiate between link state and distance vector routing algorithm. **[WBUT 2014]**

Answer:

In the given table we can find differences between distance vector and link state routing protocol

Particular	Distance Vector Routing Protocol	Link State Routing Protocol
Example of	RIP, IGRP	OSPF, IS-IS
Algorithm	Bellmon-ford	Shortest Path first (SPF)
Support subnet	Only Classfull Routing	Classfull, Classless, VLSM, Summarization
Scale	Small, limited hop	Large
Table creation	Only Routing Table	Routing Table, Neighbor Table and Topology Table
Convergence time	Very Slow	Fast
Updating	On Broadcast	On multicast

Particular	Distance Vector Routing Protocol	Link State Routing Protocol
Updating based on	Rumor	Based on topology table
Updating time	When periodic timer expired	Whenever changing occurs
Updating contents	Whole routing table	Only changed information
HOP	Limited	Unlimited
Needs Memory	Less	High
CPU Cycle	Less	High
Configuration	Simple	Advanced
Risk of Layer 3 Loop	Yes	No
Hierarchical Structure	No	Yes
OPEN Standard	Yes	Yes

4. What is distance vector routing protocol? What is the difference Right between RIP and BGP). [WBUT 2016]

Answer:

In computer communication theory relating to packet-switched networks, a distance-vector routing protocol is one of the two major classes of routing protocols, the other major class being the link-state protocol. A distance-vector routing protocol uses the Bellman-Ford algorithm to calculate paths.

A distance-vector routing protocol requires that a router informs its neighbors of topology changes periodically and in some cases, when a change is detected in the topology of a network. Compared to link-state protocols, which require a router to inform all the nodes in a network of topology changes, distance-vector routing protocols have less computational complexity and message overhead.

Distance Vector means that Routers are advertised as vector of distance and direction. 'Direction' is represented by next hop address and exit interface, whereas 'Distance' uses metrics such as hop count.

Routers using distance vector protocol do not have knowledge of the entire path to a destination. Instead DV uses two methods:

Direction in which or interface to which a packet should be forwarded.

Distance from its destination.

Rip is a distance-vector based routing protocol meant to work with smaller IP base networks. RIP uses UDP for propagating routing information.

BGP is designed to work across large networks, usually belonging to one or group of ISP-s. Such group, known as Autonomous Segments (AS-s). BGP is a protocol for routing between AS-s. BGP uses TCP for propagating routing information.

5. a) What is the purpose of subnetting? Find the netid and the hosted of the following IP addresses:

i) 19.34.21.5

ii) 220.34.8.9

b) A network is with subnet mask of 255.255.255.254. Determine maximum number of Hosts in the networks. What is the broadcast address of that network?

[WBUT 2016]

Answer:

a) 1st Part:

The main purpose of subnetting is to help relieve network congestion. Congestion used to be a bigger problem than it is today because it was more common for networks to use hubs than switches. When nodes on a network are connected through a hub, the entire network acts as a single collision domain. What this means is that if one PC sends a packet to another PC, every PC on the entire network sees the packet. Each machine looks at the packet header, but ignores the packet if it isn't the intended recipient.

2nd Part:

Network Address	Class	Host bits	Network-id	Host-id
(i) 19.34.21.5	A	34.21.5	19	34.21.5
(ii) 220.34.8.9	C	9	220.34.8	9

b) Number of Hosts = 12. Here in the Broadcast address, host=11111.So, the broadcast address is 255.255.255.255

6. Show the connection establishment of connection-oriented service of UDP. [WBUT 2016]

Answer:

- TCP provides a connection-oriented service over packet switched networks. Connection-oriented implies that there is a virtual connection between two endpoints.
- There are three phases in any virtual connection. These are the connection establishment, data transfer and connection termination phases.
- In order for two hosts to communicate using TCP they must first establish a connection by exchanging messages in what is known as the three-way handshake.
- Fig. below shows the process of the three-way handshake.

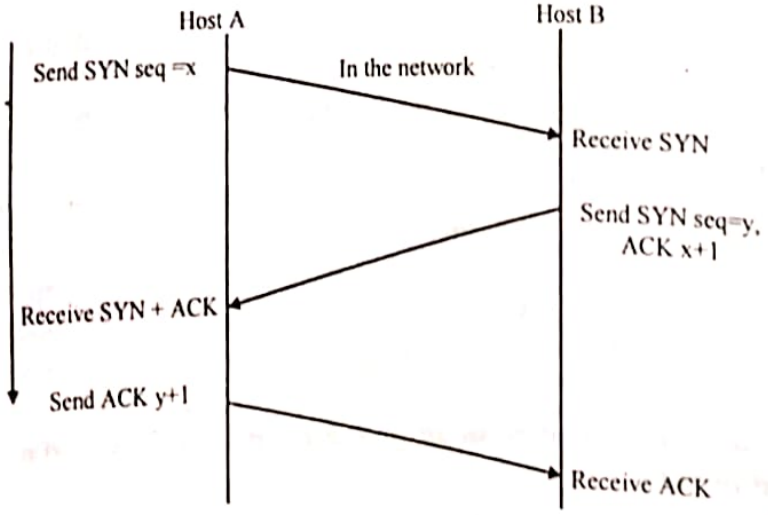


Fig: TCP connection establishment

7. Discuss the function of Network layer of TCP/IP protocol suite. [WBUT 2015]

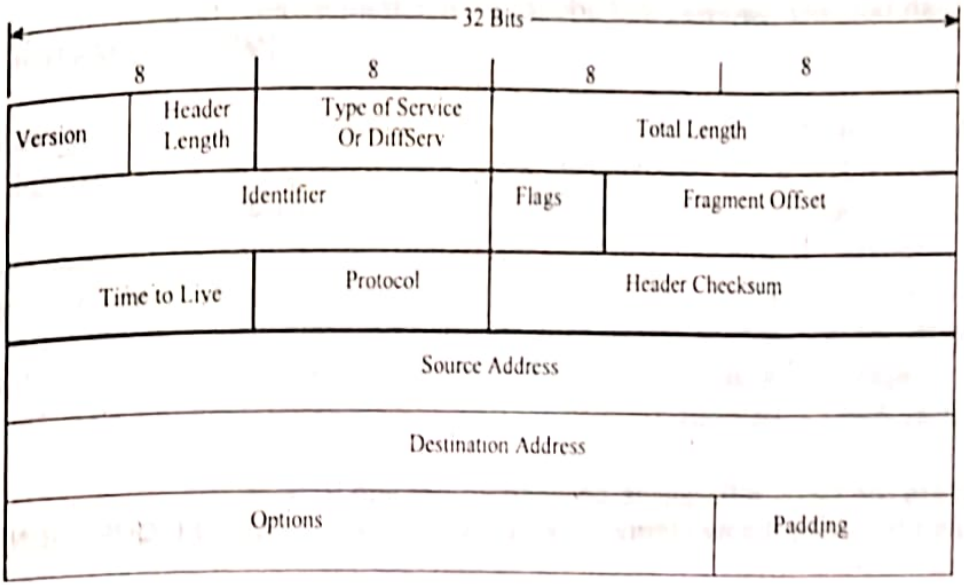
Answer:

Function of Network Layer:

1. It translates logical network address into physical address. Concerned with circuit, message or packet switching.
2. Routers and gateways operate in the network layer. Mechanism is provided by Network Layer for routing the packets to final destination.
3. Connection services are provided including network layer flow control, network layer error control and packet sequence control.
4. Breaks larger packets into small packets.

8. Describe IPV4 header format. **[WBUT 2017]**

Answer:



9. What is subnetting? What are the default subnet masks? Find the subnet address if the IP address is 129.31.72.24 and subnet mask is 255.255.192.0. **[WBUT 2018]**

Answer:

1st part: ***Refer to Question No. 5(a) of Short Answer Type Questions.***

2nd part:

The default subnet masks are–

i) 255.0.0.0 for class A

ii) 255.255.0.0 for class B

iii) 255.255.255.0 for class C

10. Explain DHCP message format. **[WBUT 2018]**

Answer: ***Refer to Question No. 3 of Long Answer Type Questions.***

11. What is Gateways? Differentiate between hub and switch? [MODEL QUESTION]

Answer:

A Gateway is a network node that is equipped to interface with another network that possibly uses different protocols. Gateways are therefore protocol converters that may operate at any layer.

Hubs and switches are networking equipments that inter-connect several hosts. They differ in the way that they pass on network traffic that they receive. A hub repeats everything it receives on all other ports. A switch on the other hand makes a short analysis of the packet received and tries to repeat it only on an appropriate port. For Ethernet, a hub does not isolate collision domain. Switches on the other hand isolate collision domain and hence permit a larger number of hosts to operate smoothly with low collision levels.

12. Distinguish between gateway and bridge. What is transparent bridge? **[MODEL QUESTION]**

Answer:

A bridge is used for connecting two or more networks that have similar topology and technology. It is a device that transfers data without regard to its format. For example, wireless APs with routers can bridge between an Ethernet LAN and WLAN.

To connect networks of different topology or technology, gateways are used. A gateway can be a software or hardware or a combination of both. An office LAN may be connected to the Internet Service Provider's WAN using a gateway.

Transparent bridges are bridges that connect more than one network segments with other bridges and take routing decisions.

13. a) What are the basic differences between Router and Gateway?
b) Distinguish between the two terms 'internet' and 'intranet'. **[MODEL QUESTION]**

Answer:

a) ROUTER: Network device that forwards packets from one network to another. Based on internal routing tables, routers read each incoming packet and decide how to forward it.

Routers work at the network layer (layer 3) of the protocol

GATEWAY: Device that converts one protocol or format to another. A network gateway converts packets from one protocol to another. The gateway functions as an entry/exit point to the network. An earlier name for router.

GATEWAY work at the network layer (layer 4) of the protocol.

b) The Internet is a network of LAN-s that uses the IP protocol at the network layer and covers the entire world. The Intranet is similar, i.e., it is also a network of networks driven by the IP protocol. However, all the networks of the Intranet belong to the same organization.

14. Discuss the functions of Network and Transport layer. **[MODEL QUESTION]**

Answer:

The **Network layer** responds to service requests from the transport layer and issues service requests to the data link layer. The network layer is responsible for end to end (source to destination) packet delivery. The primary objective of this layer is to be able to bind different physical networks to form a single logical mesh (which can be called inter-network). With this, any host in any network can send data to any other host in any other network.

The purpose of the **Transport Layer** is to provide transparent "*peer to peer*" communication, with the remote (peer) transport entity, thus relieving the upper layers from any concern with providing reliable and cost-effective data transfer. The transport layer usually turns the unreliable and very basic service provided by the Network Layer into a more powerful one. It provides end-to-end control and information transfer with the quality of service needed by the application program.

15. a) What do you mean by transparent bridge? **[MODEL QUESTION]**

Answer:

Transparent bridges are devices which connects more than one network segments with other bridges to make all routing decisions. A transparent bridge is essentially used to learn the MAC addresses of all nodes and their associated port, to filter incoming frames whose destination MAC addresses are located on the same incoming port, and to forward incoming frames to the destination MAC through their associated port.

b) Explain link state routing. **[MODEL QUESTION]**

Answer:

A Link-state routing is a concept used in routing of packet-switched networks in computer communications. Link-state routing works by having the routers tell every router on the network about its closest neighbors. The entire routing table is not distributed from any router, only the part of the table containing its neighbors. The following are some key characters of the Link-state routing concept:

- The neighbor information is gathered continuously.
- The neighbor information list is then broadcasted to every router that can answer to this protocol, a process known as flooding, which means that it sends the information to all of its neighbors who in turn send it to all of their neighbors and so on. Soon, all routers on the network have this information.
- The neighbor information is flooded whenever there is a (routing-significant) change in the network. As every router knows everything about the network by structuring the information from other routers, it can calculate the best path to any host on any destination network.

Some of the link-state routing protocols are the OSPF, IS-is and EIGRP. Novell's NLSP (NetWare Link State Protocol) is also a link-state routing protocol, which only supports IPX.

LinkState Routing protocols provide greater flexibility and sophistication than the Distance Vector routing protocols. They reduce overall broadcast traffic and make better

decisions about routing by taking characteristics such as bandwidth, delay, reliability, and load into consideration, instead of basing their decisions solely on distance or hop count.

Long Answer Type Questions

1. Explain about IP addressing with its type. Why is it needed for Networking? [WBUT 2013]

Answer:

In computer networking, an IP address (internet protocol address) is a unique number that devices use in order to identify and communicate with each other on a network utilizing the Internet Protocol standard. IP addresses (more accurately, Ipv4 addresses) are **32 bit integers,** usually represented in the familiar dot-based notation. The dot-based notation is a decimal representation for each byte of the IP address. For example, an IP address with a hex value of 0x800A080B is represented as 128.10.8.11.

Any participating device — including routers, computers, time-servers, printers, Internet fax machines, and nowadays Internet telephones — must have its own globally unique communicable address.

In IP addresses, the assignment of bits to the network id and the host id depends upon the "class" of the address.

Class A: IP address is suitable when the Internet consists of a small number of networks but each network consists of a large number of hosts. The m.s.b (i.e., bit-31) of the address is 0 and the next 7 bits represent the network address, leaving 24 bits to address a host in the network. The range of class A addresses is from 1.0.0.0 to 127.255.255.255 (The IP address 0.0.0.0 has special significance as we shall see later).

Class B: IP addresses allow for 16, 382 networks each having up to 65, 536 hosts. The two most significant bits of class B IP address are 1 and 0. Addresses range from 128.0.0.0 till 191.255.255.255.

Class C: IP addresses allow for 2 million networks each having up to 254 hosts. The three most significant bits of class C IP address are 1, 1 and 0.

IP addresses with four most significant bits as 1110, called ***class D IP addresses*** are reserved for multicast addresses. They range from 224.0.0.0. to 239.255.255.255.

IP addresses with five most significant bits as 11110 (sometimes called ***class E IP addresses***) are reserved for future use.

The address 127.0.0.1 Network id is left out because it is designated for loop-back and cannot be assigned to a network

A few IP addresses have special meanings:

- The address 0.0.0.0 (i.e. all 0-s in binary) always means "this host".
- If the higher 12 bits are all 0-s then it means a host on this network where the host id is given by the lower 20 bits.

- The address 255.255.255.255 (i.e., all 1-s in binary) is reserved for broadcast on this network.
- Any address 127.X.X.X (X can be anything) is a loopback address.

2. Explain the path vector routing. What is Subnet mask in networking? **[WBUT 2013]**

Answer:

1st Part:

A path vector protocol is a computer network routing protocol which maintains the path information that gets updated dynamically. Updates which have looped through the network and returned to the same node are easily detected and discarded. This algorithm is sometimes used in Bellman–Ford routing algorithms to avoid "Count to Infinity" problems.

It is different from the distance vector routing and link state routing. Each entry in the routing table contains the destination network, the next router and the path to reach the destination.

2nd Part:

A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address. Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s. Within a given network, two host addresses are reserved for special purpose. The "0" address is assigned a network address and "255" is assigned to a broadcast address, and they cannot be assigned to a host.

255.255.255.252 252 = 11111100

Subnets						Hosts	
1	1	1	1	1	1	0	0
128	64	32	16	8	4	2	1
32	16	8	4	2	1	2	1

subnets = 62 (64 - 2)
hosts = 2 (4 - 2)

3. What is DHCP? What are the different types of messages are there? Explain DHCP message format. Explain the lease renewal processes. What are interior routing and exterior routing? **[WBUT 2013]**

Answer:

1st Part:

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network.

Different types of DHCP messages are described below.

Message	Use
DHCPDISCOVER	Client broadcast to locate available servers.
DHCPOFFER	Server to client in response to DHCPDISCOVER with offer of configuration parameters.
DHCPREQUEST	Client message to servers either (a) requesting offered parameters from one server and implicitly declining offers from all others, (b) confirming correctness of previously allocated address after, e.g., system reboot, or (c) extending the lease on a particular network address.
DHCPACK	Server to client with configuration parameters, including committed network address.
DHCPNAK	Server to client indicating client's notion of network address is incorrect (e.g., client has moved to new subnet) or client's lease as expired
DHCPDECLINE	Client to server indicating network address is already in use.
DHCPRELEASE	Client to server relinquishing network address and cancelling remaining lease.
DHCPINFORM	Client to server, asking only for local configuration

Here is the DHCP message format.

Description of fields in a DHCP message

FIELD	OCTETS	DESCRIPTION
op	1	Message op code / message type. 1 = BOOTREQUEST, 2 = BOOTREPLY
htype	1	Hardware address type (e.g., '1' = 10Mb Ethernet)
hlen	1	Hardware address length (e.g. '6' for 10Mb Ethernet)
hops	1	Client sets to zero, optionally used by relay agents when booting via a relay agent.
xid	4	Transaction ID. A random number chosen by the client, used by the client and server to associate the request message with it's and response.
secs	2	Seconds passed since client began the request process. Filled in by client.
flags	2	Flags
ciaddr	4	Client IP address. Filled in by client if it knows it's IP address (from previouse requests or from manual configurations). and can respond to ARP requests.
yiaddr	4	'your' (client) IP address. Server's response to client.

FIELD	OCTETS	DESCRIPTION
siaddr	4	Server IP address. Address of sending server or of the next server to use in the next bootstrap process step.
giaddr	4	Relay agent IP address, used in booting via a relay agent.
chaddr	16	Client hardware address.
sname	64	Optional server host name. Null terminated string.
file	128	Boot file name. Null terminated string; "generic" name or null in request, fully qualified directory-path name in reply.
options	var	Optional (BOOTP semantics) parameters field. In real DHCP messages at least one option (message type) must always be present, so this field is never empty.

The renewal process occurs when a client already has a lease, and needs to renew that lease with the server. To ensure that addresses are not left in an assigned state when they are no longer needed, the DHCP server places an administrator-defined time limit, known as a lease duration, on the address assignment.

Halfway through the lease period, the DHCP client requests a lease renewal, and the DHCP server extends the lease. If a computer stops using its assigned IP address (for example, if a computer is moved to another network segment or is removed), the lease expires and the address becomes available for reassignment.

The renewal process occurs as follows:

1. The client sends a request to the DHCP server, asking for a renewal and extension of its current address lease. The client sends a directed request to the DHCP server, with a maximum of three retries at 4, 8, and 16 seconds.
   - If the DHCP server can be located, it typically sends a DHCP acknowledgment message to the client. This renews the lease.
   - If the client is unable to communicate with its original DHCP server, the client waits until 87.5 percent of its lease time elapses. Then the client enters a rebinding state, broadcasting (with a maximum of three retries at 4, 8, and 16 seconds) a DHCPDiscover message to any available DHCP server to update its current IP address lease.
2. If a server responds with a DHCPOffer message to update the client's current lease, the client renews its lease based on the offering server and continues operation.
3. If the lease expires and no server has been contacted, the client must immediately discontinue using its leased IP address. The client then proceeds to follow the same process used during its initial startup to obtain a new IP address lease.

2nd Part:

The names interior and exterior are very descriptive. Interior routing protocols are designed for use within a contained network of limited size, whereas exterior routing protocols are designed to link multiple networks together. They can be used in combination in order to simplify network administration. For example, a network can be built with only border routers of a network running the exterior routing protocol, while all the routers on the network run the interior protocol, which prevents them from connecting outside the network without passing through the border. Exterior routers in such a configuration must have both exterior and interior protocols, to communicate with the interior routers and outside the network.

Nearly all routing protocols are interior routing protocols. Only BGP is commonly used as an exterior routing protocol.

You may see interior gateway protocol (IGP) used to refer to interior routing protocols, and exterior gateway protocol (EGP) used to refer to interior routing protocols.

4. a) What is the function of ICMP? **[WBUT 2014]**

Answer:

ICMP (Internet Control Message Protocol) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.

b) What is the difference between dynamic routing and state routing? **[WBUT 2014, 2015]**

Answer:

Static routing manually sets up the optimal paths between the source and the destination computers. On the other hand, the dynamic routing uses dynamic protocols to update the routing table and to find the optimal path between the source and the destination computers.

- The routers that use the static routing algorithm do not have any controlling mechanism if any faults in the routing paths. These routers do not sense the faulty computers encountered while finding the path between two computers or routers in a network. The dynamic routing algorithms are used in the dynamic routers and these routers can sense a faulty router in the network. Also, the dynamic router eliminates the faulty router and finds out another possible optimal path from the source to the destination. If any router is down or faulty due to certain reasons, this fault is circulated in the entire network. Due to this quality of the dynamic routers, they are also called adaptive routers.
- The static routing is suitable for very small networks and they cannot be used in large networks. As against this, dynamic routing is used for larger networks. The manual routing has no specific routing algorithm. The dynamic routers are based on various routing algorithms like OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol) and RIP (Routing Information Protocol).

- The static routing is the simplest way of routing the data packets from a source to a destination in a network. The dynamic routing uses complex algorithms for routing the data packets.
- The static routing has the advantage that it requires minimal memory. Dynamic router, however, have quite a few memory overheads, depending on the routing algorithms used.
- The network administrator finds out the optimal path and makes the changes in the routing table in the case of static routing. In the dynamic routing algorithm, the algorithm and the protocol is responsible for routing the packets and making the changes accordingly in the routing table.

c) A router has the following RIP routing table: **[WBUT 2014]**

Net1	4	B
Net2	2	C
Net3	1	F
Net4	5	G

What would be the contents of the table if the router received the following RIP message from router C?

Net1	2
Net2	1
.Net3	3
Net4	7

Answer:

After receiving the RIP packet from router C the table of the router is updated as below:

Net1	3 (as 2+1<4)	C
Net2	2 (as 1+1=2)	C
Net3	1 (as 3+1>1)	F
Net4	5 (as 7+1>5)	G

5. a) State the differences between IPV4 and IPV6. **[WBUT 2015]**

Answer:

IPv4	IPv6
Addresses are 32 bits (4 bytes) in length. So, maximum 232 addresses possible.	Addresses are 128 bits (16 bytes) in length. So, maximum 2128 addresses are possible.
Dotted Number notation, e.g., 192.168.10.160	Hexadecimal number notation, e.g., 32FE:4201:39A6:0000:0000:0000:1234:ABCD
IPSec is optional and should be supported externally	IPSec support is not optional
Header does not identify packet flow for QoS handling by routers	Header contains Flow Label field, which Identifies packet flow for QoS handling by router.
Both routers and the sending host fragment packets.	Routers do not support packet fragmentation. Sending host fragments packets.
Header includes a checksum.	Header does not include a checksum.

IPv4	IPv6
Header includes options.	Optional data is supported as extension headers.
ARP uses broadcast ARP request to resolve IP to MAC/Hardware address.	Multicast Neighbour Solicitation messages resolve IP addresses to MAC addresses.
Broadcast addresses are used to send traffic to all nodes on a subnet.	IPv6 uses a link-local scope all-nodes multicast address.
Configured either manually or through DHCP.	Does not require manual configuration or DHCP.
Must support a 576-byte packet size (possibly fragmented).	Must support a 1280-byte packet size (without fragmentation).

b) Describe any shortest path algorithm. **[WBUT 2015]**

Answer:

Let the node at which we are starting be called the initial node. Let the distance of node Y be the distance from the initial node to Y. Dijkstra's shortest path algorithm will assign some initial distance values and will try to improve them step by step.

1. Assign to every node a tentative distance value: set it to zero for our initial node and to infinity for all other nodes.
2. Mark all nodes unvisited. Set the initial node as current. Create a set of the unvisited nodes called the unvisited set consisting of all the nodes except the initial node.
3. For the current node, consider all of its unvisited neighbours and calculate their tentative distances. For example, if the current node A is marked with a distance of 6 and the edge connecting it with a neighbour B has length 2, then the distance to B (through A) will be 6+2=8. If this distance is less than the previously recorded tentative distance of B, then overwrite that distance. Even though a neighbour has been examined, it is not marked as "visited" at this time and it remains in the unvisited set.
4. When we are done considering all of the neighbours of the current node, mark the current node as visited and remove it from the unvisited set. A visited node will never be checked again.
5. If the destination node has been marked visited (when planning a route between two specific nodes) or if the smallest tentative distance among the nodes in the unvisited set is infinity (when planning a complete traversal), then stop. The algorithm has finished.
6. Select the unvisited node that is marked with the smallest tentative distance and set it as the new "current node" then go back to step 3.

c) Differentiate between ARP and RARP. **[WBUT 2015]**

Answer:

ARM basically asks the question — "What is the MAC address of the host in the current network that has a given IP address?" Every host in a LAN uses ARP at some point of time.

RARP asks the reverse question — "What is the IP address that is associated with a given MAC address?" RARP is used mostly by diskless devices to know its own IP address.

6. a) Which one is better: Switch or Router. Explain with example. [WBUT 2015]

Answer:

Ethernet switch and router as a connecting devices are very important to connect to the internet. A router and an Ethernet switch have the same purpose. These tools are used for computer networking purposes. With these devices, we will be able to use the internet all at the same time. But the question is, how do they differ from each other and which one is better. We will elaborate the differences one by one.

Ethernet Switch vs. Router: Round 1 – Function

As per its function, router has won this round. A router can connect to LAN and WAN all at the same time. It also serves as an intermediate pathway for network traffic. The great thing about routers is that it can increase our security while we are browsing the internet. Ethernet switch, on the other hand, is a device which connects numerous computers with just one area network and that is LAN. The downside of switches is that it cannot join multiple networks and share the internet connection. When we use a switch connection, we must use a computer that can be served as the access to the internet. Furthermore, the computer should have two network adapters which can be used for sharing. The first adapter shall be used for the home LAN and the second adapter shall be used for the Internet WAN.

But with the router, we don't have to get two adapters since it can be connected to all area networks with just one tool. And the best part is, it won't affect the connection, even if it is connected with the two networks at the same time.

Ethernet Switch vs. Router: Round 2 – Cost and Connectivity

As per their cost, their price may vary depending on the features, style, functionality and the brand we will buy. If we choose to get a router, the price will range from $10,000 to $74,000. Switch, on the other hand, will range from $12,000 to $93,000.

When it comes to their connectivity, routers can be connected through a Wi-Fi connection, whereas These switches can be connected via wired networking connections.

Ethernet Switch vs. Router: Round 3 – Intelligence

Though switches are more expensive than routers, it doesn't mean that they are more sophisticated. When you break down their functions, routers are more sophisticated than switches. This tool uses software which helps to increase the networks by using numerous techniques such as caching.

b) What is an autonomous system? What is the difference between intra autonomous system and inter autonomous system routings? Give an example of each routing protocol. [WBUT 2016]

Answer:

On the Internet, an autonomous system (AS) is the unit of router policy, either a single network or a group of networks that is controlled by a common network administrator (or group of administrators) on behalf of a single administrative entity (such as a university, a business enterprise, or a business division). An autonomous system is also sometimes

referred to as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN).
Networks within an autonomous system communicate routing information to each other using an Interior Gateway Protocol (IGP) like RIP, OSPF, etc. An autonomous system shares routing information with other autonomous systems using the Border Gateway Protocol (BGP).

Intra-Autonomous System	Inter-Autonomous System
An intra-AS routing protocol is used to configure and maintain the routing tables within an autonomous system (AS). Intra-AS routing protocols are also known as interior gateway protocols RIP: Routing Information Protocol	An inter-autonomous system routing protocol provides routing between autonomous systems (that is, administrative domains). The Border Gateway Protocol (BGP)

7. What is IP addressing? Explain various types of IP addressing. Give basic concepts about unicast and multicast IP addressing. **[WBUT 2016]**

Answer:

1st & 2nd Part: ***Refer to Question No. 1 of Long Answer Type Questions.***

3rd Part:

Application that communicate with a single remote node, such as Web browsing, electronic mail, or conventional Internet telephony, need to address exactly one network interface. This is the purpose of a unicast IP address. A unicast IP address identifies the link to which it belongs, thereby localizing the IP address owner in Internet topology, and it specifies particular interface attached to that link.

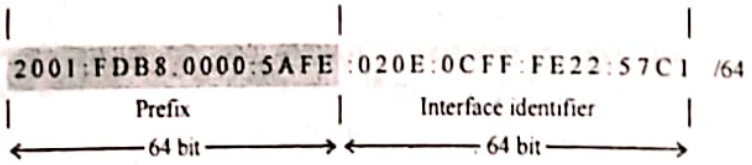


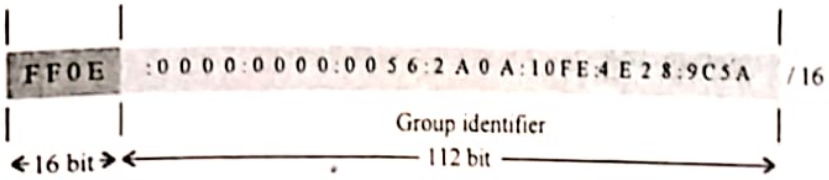
Fig: Unicast IP address

Link identification is the purpose of the IP address prefix, which in case of a unicast IP address is 64 bits long. Each link on the Internet is assigned one or multiple subnet prefixes, which are globally unique numbers of 64 bits length. Nodes that attach to a particular link reuse these subnet prefixes as prefixes for their unicast IP addresses. The remaining 64 bits in a unicast IP address form an interface identifier, which is unique within the scope of a link and thus distinguishes the interface from others on the same link. The IP address shown in above Figure is a unicast IP address.
For administrative purpose, the scope of a unicast IP address can be limited to the link to which the respective interface attaches. Such a link-local IP address can only be used for packet exchange between nodes on the same link. The subnet prefix of a link-local

unicast IP address is set to the prefix FE80:0000:0000:0000::/64, and it does not bear any localization semantics. Link-local IP addresses are primarily used during autoconfiguration when a node gains IP connectivity. To differentiate IP addresses with global scope from link-local IP addresses, the former are also referred to as global IP addresses.

A multicast IP address identifies a group of network interfaces a group of network interfaces of typically different nodes. Since the interfaces may attach to multiple links, there is no single subnet prefix that a multicast IP address could use. The interface group is instead solely identified by a 112-bit group identifier, which is appended to a 16-bit prefix to form a multicast IP address. The semantics of the universal/local and individual/group bits are the same for unicast and multicast IP addresses. Figure below displays an example of a multicast IP address.

Certain autoconfiguration tasks require a node to send a packet to a neighbor for which it does not know the link-layer address. In such cases, the packet can be sent to a so-called solicited-node multicast IP address. This special multicast IP address is derived from the unicast IP address of interest, and it addresses all nodes on a link that use an IP address with a particular pattern in the last 24 bits. In this case, the packet is sent to a multicast link-layer address, so the sender does not require knowledge of the recipient's actual unicast link-layer address. Given a unicast IP address, the corresponding solicited-node multicast IP address is formed by taking the lower 24 bits of the unicast IP address and prepending to this the prefix FF02:0:0:0:1:FF00::/64.



Multicast IP address

8. A company granted a site address 201.70.64.0. The company needs six subnets. Design the subnets. **[WBUT 2018]**

Answer:

A company granted to site address = 201.70.64.0. Assume, subnet mask is 255.255.240.0

Then, 11001000 00101101 00100010 00111000
11111111 11111111 1111<u>0000</u> <u>00000000</u>
11001000 00101101 00100000 00000000

The number of 1's is in the default mask is 24 (class C). The company needs six subnets. This number 6 is not a power of 2. The next number i.e. a power of 2 is 8 [z^3]. We need 3 more 1s in the subnet mask. The total number of 1s in the subnet mask is 27(24+3)

Therefore, the total number of OS is 5(32–27).

The mask is

11111111 11111111 11111111 11100000

or, 255.255.255.224.

So, the number of subnets in 8. The number of addresses in each subnet in 2^5=32.

9. Write short notes on the following:

a) BGP [WBUT 2014, 2015, 2016, 2017]
b) IGMP [WBUT 2016]
c) RIP [WBUT 2017]
d) OSPF [WBUT 2017]
e) Distance Vector Routing [WBUT 2017]
f) Hamming code [WBUT 2018]
g) TCP Datagram with figure [WBUT 2018]

Answer:

a) BGP:

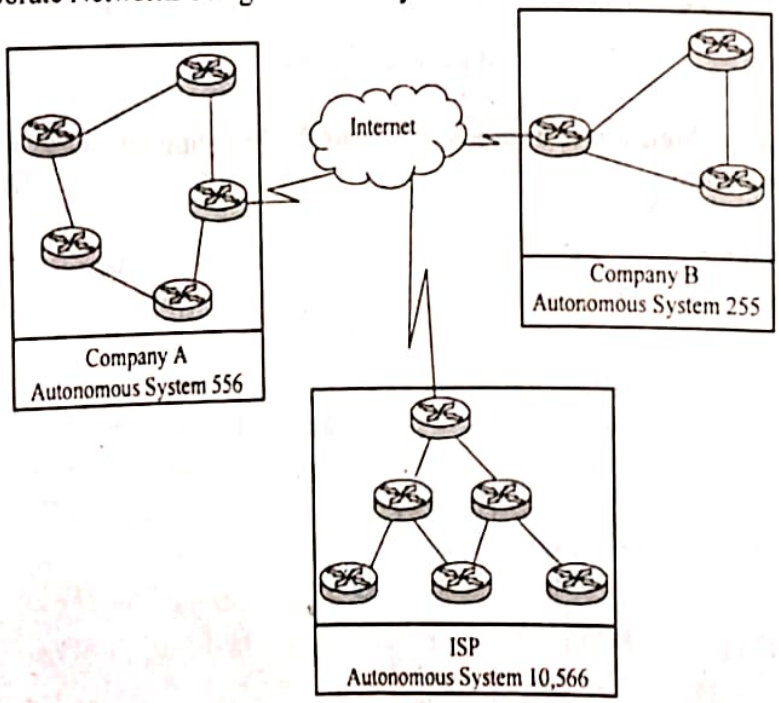
BGP is a complex, advanced distance Exterior Gateway Protocol (EGP). BGP exchange routing information between Autonomous Systems (ASs).

Unlike Interior routing protocols such as RIP, EIGRP, and OSPF that run inside a company's network, BGP uses a different basic algorithm for building a loop-free topology than any of the above mentioned protocols.

BGP is especially used for exchanging routing information between all of the major Internet Service Providers (ISPs), as well between larger client sites and their respective ISPs. And, in some large enterprise networks, BGP is used to interconnect different geographical or administrative regions.

BGP is Primarily used to support the complexity of the public Internet, Cisco has added several clever and useful features to its BGP implementation (BGP 4). Some of the primary attributes of BGP is the use of pieces of information about a known route, where it came from, and how to reach it, A BGP router will also generate an error message if it receives a route that is missing these are mandatory attributes.

Clients/ Corporate Networks being connected by BGP



b) IGMP:

Internet Group Management Protocol (IGMP), a multicasting protocol in the internet protocols family, is used by IP hosts to report their host group memberships to any immediately neighboring multicast routers. IGMP messages are encapsulated in IP diagrams with an IP protocol number of 2. IGMP has versions IGMP v1, v2 and v3.

- **IGMPv1:** Hosts can join multicast groups. There are no leave messages. Routers use a time-out based mechanism to discover the groups that groups that are of no interest to the members.
- **IGMPv2:** Leave messages were added to the protocol, allowing group membership termination to be quickly reported to the routing protocol, which is important for high-bandwidth multicast groups and/or subnets with highly volatile group membership.
- **IGMPv3:** A major revision of the protocol allows hosts to specify the list of hosts from which they want to receive traffic. Traffic from other hosts is blocked inside the network. It also allows hosts to block inside the network packets that come from sources that send unwanted traffic.

The variant protocols of IGMP are:

- DVMRP: Distance Vector Multicast Routing protocol
- IGAP: IGMP for user Authentication Protocol
- RGMP: Router-port Group Management Protocol

c) RIP:

RIP is a dynamic, distance vector routing protocol based around the Berkely BSD application routed and was developed for smaller IP based networks. RIP uses UDP port 520 for route updates. RIP calculates the best route based on hop count. Like all distance vector routing protocols, RIP takes some time to converge. While RIP requires less CPU power and RAM than some other routing protocols, RIP does have some limitations:

Metric: Hop Count

Since RIP calculates the best route to a destination based solely on how many hops it is to the destination network, RIP tends to be inefficient in network using more than one LAN protocol, such as Fast Ethernet and serial or Token Ring. This is because RIP prefers paths with the shortest hop count. The path with the shortest hop count might be over the slowest link in the network.

Hop Count Limit

RIP cannot handle more than 15 hops. Anything more than 15 hops away is considered unreachable by RIP. This fact is used by RIP to prevent routing loops.

Classful Routing Only

RIP is a classful routing protocol. RIP cannot handle classless routing. RIP v1 advertises all networks it knows as classful networks, so it is impossible to subnet a network properly via VLSM if you are running RIP v1.

However, it must be pointed out that RIP is the only routing protocol that all routing devices and software support, so in a mixed equipment environment, RIP may be your only option for dynamic routing. This is changing with the widespread use of OSPF.
The routing-update timer controls the time between routing updates. Default is usually 30 seconds, plus a small random delay to prevent all RIP routers from sending updates simultaneously.
The route-timeout timer controls when a route is no longer available. The default is usually 180 seconds. If a router has not seen the route in an update during this specified interval, it is dropped from the router's announcements. The route is maintained long enough for the router to advertise the route as down (hop count of 16).

d) OSPF:
The OSPF routing protocol has largely replaced the older Routing Information Protocol (RIP) in corporate networks. Using OSPF, a router that learns of a change to a routing table (when it is reconfigured by network staff, for example) or detects a change in the network immediately multicasts the information to all other OSPF hosts in the network so they will all have the same routing table information. Unlike RIP, which requires routers to send the entire routing table to neighbors every 30 seconds, OSPF sends only the part that has changed and only when a change has taken place. When routes change – sometimes due to equipment failure -- the time it takes OSPF routers to find a new path between endpoints with no loops (which is called "open") and that minimizes the length of the path is called the convergence time.
Rather than simply counting the number of router hops between hosts on a network, as RIP does, OSPF bases its path choices on "link states" that take into account additional network information, including IT-assigned cost metrics that give some paths higher assigned costs. For example, a satellite link may be assigned higher cost than a wireless WAN link, which in turn may be assigned higher cost than a metro Ethernet link.

Features and advantage of OSPF
It supports both IPv4 and IPv6 routed protocols.
It supports load balancing with equal cost routes for same destination.
Since it is based on open standards, it will run on most routers.
It provides a loop free topology using SPF algorithm.
It is a classless protocol.

- It supports VLSM and route summarization.
- It supports unlimited hop counts.
- It scales enterprise size network easily with area concept.
- It supports trigger updates for fast convergence.

Just like other routing protocols, OSPF also has its negatives.

Disadvantage of OSPF

- It requires extra CPU process to run SPF algorithm.

- It requires more RAM to store adjacency topology.
- It is more complex to setup and hard to troubleshoot.

This tutorial is the first part of our article "OSPF Routing Protocol Explained with examples". You can read other parts of this article here.

e) Distance Vector Routing:

Refer to Question No. 4(1st part) of Short Answer Type Questions.

Advantages of Distance Vector Routing

- Well Supported
- Protocols such as RIP have been around a long time and most, if not all devices that perform routing will understand RIP.
- Large routing tables.
- Multiple routes to a given network ID can be reflected as multiple entries in the routing table. In a large internetwork with multiple paths, the routing table can have hundreds or thousands of entries.
- High network traffic overhead.
- Route advertising is done periodically even after the internetwork has converged.
- Does not scale.
- Between the size of the routing table and the high overhead, distance vector–based routing protocols do not scale well to large and very large internetworks.
- High convergence time.
- Due to the unsynchronized and unacknowledged way that distance vector information is exchanged, convergence of the internetwork can take several minutes. While converging, routing loops and black holes can occur.

f) Hamming Code:

Hamming code is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver. It is technique developed by R.W. Hamming for error correction.

Redundant bits:

Redundant bits are extra binary bits that are added to the information carrying bits of data transfer to ensure that no bits were lost during the data transfer. The number of redundant bits can be calculated using the following formula:

$2^r \geq m + r + 1$

Where, r = redundant bit, m = data bit

Suppose the number of data bits = 7

$\therefore$ The number of redundant bits = $2^4 \geq 7 + 4 + 1$

Thus, the number of redundant bit = 4

Parity bits:

A parity bit is a bit opened to a data of binary bits to ensure that the total number of 1's in the data are even or odd. Parity bits are used for error detection. There are two types of parity bits:

Example:

Data: 1001101

1	0	0		1	1	0		1		
11	10	9	8	7	6	5	4	3	2	1

Adding r1

1	0	0		1	1	0		1		
11	10	9	8	7	6	5	4	3	2	1

Adding r2

1	0	0		1	1	0		1		
11	10	9	8	7	6	5	4	3	2	1

Adding r4

1	0	0		1	1	0		1		
11	10	9	8	7	6	5	4	3	2	1

Adding r8

1	0	0		1	1	0		1		
11	10	9	8	7	6	5	4	3	2	1

$\therefore$ Final code $\rightarrow$ 10011100101

g) TCP Datagram with figure:

Source Port								Destination Port
Sequence Number								
Acknowledgement Number								
Header Length (4 bits)	Reserved bits (6 bits)	U R G	A C K	P S H	R S T	S Y N	F I N	Window Size
Check sum								Pointer
Options (0 – 40 bytes)								
Data (optional)								

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination of the network.

TCP Header Format:

TCP header contains a set of parameters called fields defined by the protocol technical specifications. TCP header has 10 required fields totaling 20 b bytes i.e. 120 bits in size. They can also optionally include an additional data section up to 40 bytes in size.

10. a) State the advantage of IPV6 over IPV4. **[MODEL QUESTION]**
b) What is the purpose of masking?
c) A class B network on the internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts per subnet?

Answer:

a) Advantage of IPV6 over IPV4:

1. **Larger Address Space:** Address filed in IPv6 is 128 bits long while the address filed of IPv4 is only 32 bits in length. IPv6 offers very large, i.e.296 address space as compared to IPv4.
2. **Better header format:** The header of IPv6 has been designed in a way to speed-up the routing process. In header of IPv6 options are separated from the base header. Options are inserted into base header only when required by the upper-layer data.
3. **Provision for extension:** IPv6 has been designed in a way that a protocol can be extended easily to meet the requirements of emerging technologies or new applications.
4. **Resource Allocation support in IPv6:** IPv6 provides a mechanism called Flow Label for resource allocation. Flow label enables source to send request for the special handling of a packet. This mechanism is really helpful in real-time audio and video transmission.
5. **Security Features:** To ensure confidentiality and packet's integrity encryption and authentication options are included in IPv6.

b) A subnet allows the flow of network traffic between hosts to be segregated based on a network configuration. By organizing hosts into logical groups, subnetting can improve network security and performance.

c) maximum host/subnet=$2^4-2 = 14$.

11. a) What is the difference between Bridge and Router? **[MODEL QUESTION]**
Why switch is preferred over hub for better performance?
b) What is the default mask and broadcast address for class B? Specify the private IP range for class A address.
c) Why dynamic routing algorithm is preferred over static routing algorithm in a network which changes continuously?
d) Describe different steps in Link-state routing algorithm with proper example.

Answer:

a) 1st Part:

1) Routers are more intelligent than bridges in the sense that if runs an algorithm that depends on the contents of a packet. For example, and IP router runs the routing algorithm based on the destination IP address of the packet.
2) Routers can operate on interfaces that lead to identical media types but bridges are meant to interconnect different kinds of media. For example we can have a router connecting Ethernet LANs. A bridge on the other hand can connect an Ethernet LAN with a Token-ring LAN (for example).
3) Routers allow hosts that aren't practically on the same logical network to be able to communicate with each other, while bridges can only connect networks that are logically the same.
4) Routers operate at the layer 3 (network layer) of the OSI model, while bridges are only at the layer 2 (Data link layer).

2nd Part:

A switch is a higher-performance alternative to a hub. Both hubs and switches join multiple computers together within one local area network (LAN). Operationally, switches are nearly identical to hubs, but a switch generally contains more "intelligence" (and a slightly higher price tag) than a hub. Unlike hubs, network switches are capable of inspecting data packets as they are received, determining the source and destination device of that packet, and forwarding it appropriately. By delivering each message only to the connected device it was intended for, a network switch conserves network bandwidth and offers generally better performance than a hub.

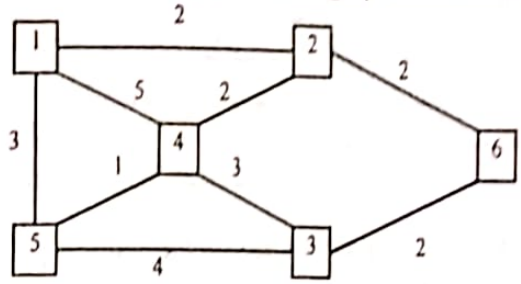
b) Default mask of class B IP addresses: 255.255.0.0

Broadcast address for class B IP address: N.N.255.255, where N.N is the class-B network address. Of course for local broadcast, the address is 255.255.255.255.

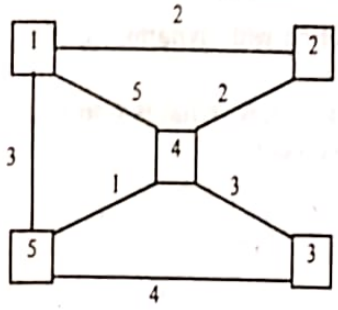
The range of class-A IP addresses in 1.0.0.1 to 1.255.255.254 excluding 'self' and broadcast addresses.

c) Routing algorithms rely on the router's knowledge of the network's topology and condition at that point of time. In a network which changes continuously, the information carried by a router about the network can become stale after a time. To keep the routers up-to-date about the information about the network, the routers must exchange information among themselves after short periods of time. This is the principle of dynamic routing.

d) For the algorithm, ***Refer to Question No. 3 of Short Answer Type Questions.***
As an example, consider the following link-state graph maintained by six routers at t = 0.

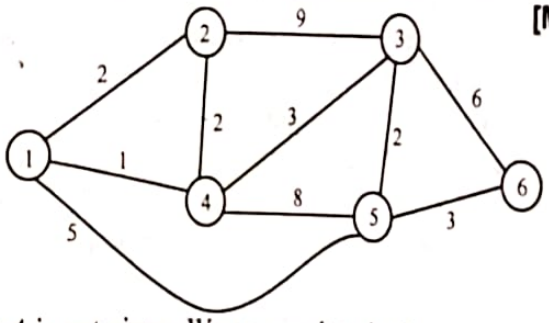


Suppose just after t = 0, router 6 goes down. Only routers 2 and 3 come to know of this at t = 1, i.e. after first exchange and updation of link-state information.
Hence, to routers 2 and 3, the modified network looks like:



But routers 1, 4 and 5 still believes that the network is as before.
However, at t = 2, i.e., after the second exchange and updation of link-state information, all the routers get the modified picture of the network.

12. Using Dijkstra's Routing algorithm find out a least cost route to all other nodes 1 through 6 for the following network. Do the same for Bellman – Ford algorithm. **[MODEL QUESTION]**



Answer:
Note: Cost of edge 2-4 is not given. We assume it to be 1.

Step-1:

Node → Dist	1	2	3	4	5	6	Comments
	0	INF	INF	INF	INF	INF	

Step-2:

Node → Dist	1	2	3	4	5	6	Comments
	0	2	10	1	9	INF	Node 4 selected

Step-3:

Node → Dist	1	2	3	4	5	6	Comments
	0	2	5	1	9	INF	Node 2 selected

Step-4:

Node → Dist	1	2	3	4	5	6	Comments
	0	2	5	1	9	11	Node 3 selected

Step-5:

Node → Dist	1	2	3	4	5	6	Comments
	0	2	5	1	5	8	Node 5 selected

Step-6: the final step does not alter any value. So, the shortest path from node-1 to node-6 is 1-5-6, with a total cost of 8.

According to BELL man ford algo shortest path will be same

As the shortest path from node-1 to node-6 is 1-5-6, with a total cost of 8.

13. a) Differentiate static routing with dynamic routing. Explain various fields of a typical routing table.

b) Explain link state routing principle. What is flooding?

c) Explain count to infinity problem. **[MODEL QUESTION]**

Answer:

a)

static routing	dynamic routing
Static routing is when you statically configure a router to send traffic for particular destinations in preconfigured directions	Dynamic routing is when you use a routing protocol such as OSPF, ISIS, EIGRP, and/or BGP to figure out what paths traffic should take.

The routing table consists of at least three information fields:

the network id: i.e. the destination network id

cost: i.e. the cost or metric of the path through which the packet is to be sent

next hop: The next hop, or gateway, is the address of the next station to which the packet is to be sent on the way to its final destination

Depending on the application and implementation, it can also contain additional values that refine path selection:

Flag: quality of service associated with the route. For example, the U flag indicates that an IP route is up.

links to filtering criteria/access lists associated with the route

interface: such as eth0 for the first Ethernet card, eth1 for the second Ethernet card, etc.

b) A Link-state routing is a concept used in routing of packet-switched networks in computer communications. Link-state routing works by having the routers tell every router on the network about its closest neighbors. The entire routing table is not distributed from any router, only the part of the table containing its neighbors. The following are some key characters of the Link-state routing concept:

The neighbor information is gathered continuously.

The neighbor information list is then broadcasted to every router that can answer to this protocol, a process known as flooding, which means that it sends the information to all of

its neighbors who in turn send it to all of their neighbors and so on. Soon, all routers on the network have this information.

In flooding, a router examines a packet's TTL field and if not zero (in which case the packet is discarded), decrements it and sends the packet on all interfaces except the one it came from. In selective flooding, the router does not send every incoming packet on every line. Instead, the algorithm has a way of finding out the interface in "approximately correct direction" and floods the packet on those

c) The Bellman-Ford algorithm does not prevent routing loops from happening and suffers from the count-to-infinity problem. The core of the count-to-infinity problem is that if A tells B that it has a path somewhere, there is no way for B to know if the path has B as a part of it. To see the problem clearly, imagine a subnet connected like as A-B-C-D-E-F, and let the metric between the routers be "number of jumps". Now suppose that A goes down (out of order). In the vector-update-process B notices that the route to A, which was distance 1, is down - B does not receive the vector update from A. The problem is, B also gets an update from C, and C is still not aware of the fact that A is down - so it tells B that A is only two jumps from C (C to B to A) , which is false. This slowly propagates through the network until it reaches infinity (in which case the algorithm corrects itself, due to the "Relax property" of Bellman Ford).

14. a) Suppose an IP datagram arrives at a router with a TTL field value of zero. What will the router do?
b) ARP and RARP both map addresses from one space to another. In this respect, they are similar. However, their implementations are fundamentally different. In what way do they differ?
c) Briefly explain the selective flooding routing algorithm. Why it differs form-flooding technique? **[MODEL QUESTION]**

Answer:
a) If the TTL value is zero, a router simply discards the packet.

b) **Address Resolution Protocol** (ARP) is a mechanism that can be used by IP to find the link-layer station address that corresponds to a particular IP address. It defines a method that is used to ask, and answer, the question "what MAC address corresponds to a given IP address?"
Reverse ARP (RARP) on the other hand lets a station ask the question "which IP address corresponds to a given MAC address?". RARP is typically used to let a piece of diskless equipment discover its own IP address as part of its boot procedure.

c) In flooding, a router examines a packet's TTL field and if not zero (in which case the packet is discarded), decrements it and sends the packet on all interfaces except the one it came from. In selective flooding, the router does not send every incoming packet on every line. Instead, the algorithm has a way of finding out the interface in "approximately correct direction" and floods the packet on those.

15. a) Distinguish between adapting routing and fixed routing?[MODEL QUESTION]
b) Differentiate between Link State and Distance Vector routing algorithms.

Answer:

a) Adaptive routing (i.e. dynamic routing) that adjusts automatically to network topology or traffic changes. It describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in conditions. The adaptation is intended to allow as many routes as possible to remain valid (that is, have destinations that can be reached) in response to the change.

People using a transport system can display adaptive routing. For example, if a local railway station is closed, people can alight from a train at a different station and use another method, such as a bus, to reach their destination.

The term is commonly used in data networking to describe the capability of a network to 'route around' damage, such as loss of a node or a connection between nodes, so long as other path choices are available. There are several protocols used to achieve this: RIP, OSPF, IS-IS, etc.

Systems that do not implement adaptive routing are described as using static routing, where routes through a network are described by fixed paths (statically). A change, such a loss of a node, or loss of a connection between nodes, is not compensated for. This means that anything that wishes to take an affected path will either have to wait for the failure to be repaired before restarting its journey, or will have to fail to reach its destination and give up the journey.

b) Distance vector routing protocol, like RIP, the routing table is forwarded by each router to neighboring routers. Here, the routers don't know the topology, i.e., how other routers are interconnected.

Link state routing protocol, like OSPF, routers first exchange information about connections within the network and build a topology table. Then each router calculate the best route to each destination by using Dijkstra's algorithm.

16. a) What are the advantages and disadvantages of using Distance Vector Routing algorithm?
b) How do ARP & RARP work in TCP/IP?
c) Draw the IPV4 Datagram Header Format and Explain it. [MODEL QUESTION]

Answer:

a) Advantages of Distance Vector Routing

- Well Supported
- Protocols such as RIP have been around a long time and most, if not all devices that perform routing will understand RIP.
- Large routing tables.
- Multiple routes to a given network ID can be reflected as multiple entries in the routing table. In a large internetwork with multiple paths, the routing table can have hundreds or thousands of entries.
- High network traffic overhead.

- Route advertising is done periodically even after the internetwork has converged.
- Does not scale.
- Between the size of the routing table and the high overhead, distance vector–based routing protocols do not scale well to large and very large internetworks.
- High convergence time.
- Due to the unsynchronized and unacknowledged way that distance vector information is exchanged, convergence of the internetwork can take several minutes. While converging, routing loops and black holes can occur.

b) ARP - Address Resolution Protocol and
RARP - Reverse Address Resolution Protocol

ARP: When an Ethernet frame is sent from one host on a LAN to another, it is the 48-bit Ethernet address that determines for which interface the frame is destined. The device driver software never looks at the destination IP address in the IP datagram. Address resolution provides a mapping between the two different forms of addresses: 32-bit IP addresses and whatever type of address the data link uses. ARP provides a dynamic mapping from an IP address to the corresponding hardware address. We use the term dynamic since it happens automatically and is normally not a concern of either the application user or the system administrator.

RARP: Each system on a network has a unique hardware address, assigned by the manufacturer of the network interface. The principle of RARP is for the diskless system to read its
unique hardware address from the interface card and send an RARP request (a broadcast frame on the network) asking for someone to reply with the diskless system's IP address (in an RARP reply).

c) An IP packet consists of two sections:
header
data
The header consists of 13 fields and, of which, only 12 are required. The 13th field is optional.

+	Bits 0 - 3	4 - 7	8 - 15	16 - 18	19	20 - 31
0	Version	Header length	Type of Service (now DiffServ and ECN)	Total Length		
32	Identification			Flags	Evil Bit	Fragment Offset
64	Time to Live		Protocol	Header Checksum		
96	Source Address					
128	Destination Address					
160	Options					
160/192+	Data					

Version

The first header field in an IP packet is the 4-bit version field. For IPv4, this has a value of 4 (hence the name IPv4).

Internet Header Length (IHL)

The second field is a 4-bit Internet Header Length (IHL) telling the number of 32-bit words in the header. Since an IPv4 header may contain a variable number of options, this field specifies the size of the header (this also coincides with the offset to the data). The minimum header size is 20 bytes, so the minimum value for this field is 5 (5×4 = 20 bytes). Being a 4-bit field the maximum length is 15 words or 60 bytes.

Type of Service (ToS)

bits 0-2: precedence
bit 3: 0 = Normal Delay, 1 = Low Delay
bit 4: 0 = Normal Throughput, 1 = High Throughput
bit 5: 0 = Normal Reliability, 1 = High Reliability
bits 6-7: Reserved for future use

This field is now used for DiffServ and ECN. The original intention was for a sending host to specify a preference for how the datagram would be handled as it made its way through an internetwork. For instance, one host could set its IPv4 datagrams' ToS field value to prefer low delay, while another might prefer high reliability. In practice, the ToS field has not been widely implemented. However, a great deal of experimental, research and deployment work has focused on how to make use of these eight bits. These bits have been redefined, most recently through DiffServ working group in the IETF and the Explicit Congestion Notification codepoints. New technologies are emerging that require real-time data streaming and therefore will make use of the ToS field. An example is Voice over IP (VoIP) that is used for interactive data voice exchange.

Total Length

This field defines the entire datagram size, including header and data, in bytes. The minimum-length datagram is 20 bytes (20 bytes header + 0 bytes data) and the maximum is 65,535 — the maximum value of a 16-bit word. The minimum size datagram that any host is **required** to be able to handle is 576 bytes, but most modern hosts handle much larger packets.

Identification

This field is an identification field and is primarily used for uniquely identifying fragments of an original IP datagram. Some experimental work has suggested using the ID field for other purposes, such as for adding packet-tracing information to datagrams in order to help trace back datagrams with spoofed source addresses.

Flags

A 3-bit field follows and is used to control or identify fragments. They are (in order, from high order to low order):

Reserved, must be zero
Don't Fragment (DF)
More Fragments (MF)

If the DF flag is set and fragmentation is required to route the packet then the packet will be dropped. This can be used when sending packets to a host that does not have sufficient resources to handle fragmentation.

When a packet is fragmented all fragments have the MF flag set except the last fragment, which does not have the MF flag set. The MF flag is also not set on packets that are not fragmented — clearly an unfragmented packet can be considered the last fragment.

Fragment Offset

The fragment offset field is 13-bits long and allows a receiver to determine the place of a particular fragment in the original IP datagram, measured in units of 8-byte blocks. This method allows a maximum offset of 65,528 ((2^13 - 1)*8 which would exceed the maximum IP packet length of 65,535 with the header length counted with it.

Time to Live (TTL)

An 8-bit time to live (TTL) field helps prevent datagrams from persisting (e.g. going in circles) on an internetwork. Historically the TTL field limited a datagram's lifetime in seconds, but has come to be a hop count field. Each packet switch (or router) that a datagram crosses decrements the TTL field by one. When the TTL field hits zero, the packet is no longer forwarded by a packet switch and is discarded. Typically, an ICMP message (specifically the time exceeded) is sent back to the sender that it has been discarded. The reception of these ICMP messages is at the heart of how traceroute works.

Protocol

This field defines the protocol used in the data portion of the IP datagram.

Header Checksum

The 16-bit checksum field is used for error-checking of the header. At each hop, the checksum of the header must be compared to the value of this field. If a header checksum is found to be mismatched, then the packet is discarded. Note that errors in the data field are up to the encapsulated protocol to handle — indeed, both UDP and TCP have checksum fields.

Source address

An IP address is a group of 4 8-bit octets for a total of 32 bits. The value for this field is determined by taking the binary value of each octet and concatenating them together to make a single 32-bit value.

Destination address

Identical to the source address field but indicates the receiver of the packet.

Options

Additional header fields (called options) may follow the destination address field, but these are not often used. Note that the value in the IHL field must include enough extra 32-bit words to hold all the options (plus any padding needed to ensure that the header contains an integral number of 32-bit words). The list of options may be terminated with an EOL (End of Options List) option; this is only necessary if the end of the options would not otherwise coincide with the end of the header.

17. Write short notes on the following:

a) NAT **[MODEL QUESTION]**

b) IPv6 **[MODEL QUESTION]**

Answer:

a) NAT:

The Internet has grown larger than anyone ever imagined it could be. Although the exact size is unknown, the current estimate is that there are about 100 million hosts and over 350 million users actively on the Internet. In fact, the rate of growth has been such that the Internet is effectively doubling in size each year. NAT allows an Internet Protocol (IP) network to maintain public IP addresses separately from private IP addresses. NAT is a popular technology for Internet connection sharing. It is also sometimes used in server load balancing applications on corporate networks.

In it's most common configuration, NAT maps all of the private IP addresses on a home network to the single IP address supplied by an Internet Service Provider (ISP). This allows computers on the home LAN to share a single Internet connection. Additionally, it enhances home network security by limiting the access of external computers into the home IP network space.

NAT works by snooping both incoming and outgoing IP datagrams. As needed, it modifies the source or destination address in the IP header (and the affected checksums) to reflect the configured address mapping. NAT technically supports either fixed or dynamic mappings of one or more internal and external IP addresses.

NAT functionality is usually found on routers and other gateway devices at the network boundary. NAT can also be implemented entirely in software. Microsoft's Internet Connection Sharing (ICS), for example, adds NAT support to the Windows operating system.

By itself, NAT does not provide all the features of a true firewall, but it is often used on servers that feature other firewall and antivirus support. NAT was designed originally to conserve public Internet address space. Internet RFC 1631 contains the basic NAT specification.

b) IPv6:

IP Version 6 (IPv6) is the newest version of IP. IPv6 is fairly well defined but is not yet widely deployed. The main differences between IPv6 and the current widely-deployed version of IP (which is IPv4) are:

- IPv6 uses larger addresses (128 bits instead of 32 bits in IPv4) and so can support many more devices on the network.
- IPv6 includes features like authentication and multicasting that had been bolted on to IPv4 in a piecemeal fashion over the years.

The main improvement brought by **IPv6** (Internet Protocol version 6) is the increase in the number of addresses available for networked devices, allowing, for example, each mobile phone and mobile electronic device to have its own address. IPv4 supports 2^{32} (about 4.3 billion) addresses, which is inadequate for giving even one address to every living person, let alone supporting embedded and portable devices. IPv6, however, supports 2^{128} addresses; this is approximately 5×10^{28} addresses for *each* of the roughly 6.5 billion people alive today. With such a large address space available, IPv6 nodes can have as many universally scoped addresses as they need, and network address translation is not required.