CN MODULE 3

P.RAJESHWARI

PART-B

1.) How the routers get the information about the neighbour.

A. Hello packets are multicast packets that are used for neighbour discovery and recovery. Hellos do not require an ACK so are not considered to be transmitted reliably. Hello packets are sent periodically between routers to learn about neighbour routers on the directly connected network. They also allow the router to monitor the state of existing neighbour routers. This is how the router learns if a neighbour router has gone down.

By default, hello packets are sent every 5 s. The exception to this is slow (considered to be T1 speed or slower), nonbroadcast connections, where the hello packets are sent every 30 s by default. The interval for how frequently hello packets are sent is configurable as is the length of time the router should consider the sender valid if it doesn't receive any other communication. This is called the *hold time* and, by default, is three times the hello interval.

2.) How is the packet cost referred to in distance vector and link state routing?

A.) In distance vector routing, cost refers to hop count while in case of link state routing, cost is a weighted value based on a variety of factors such as security levels, traffic or the state of the link. Distance vector protocols send their entire routing table to directly connected neighbours. Link state protocols send information about directly connected links to all the routers in the network.

3.) Describe the Routing Information protocol and Distance vector routing protocol.

A.) **Routing Information Protocol** (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance-vector routing protocol that has an AD value of 120 and works on the Network layer of the OSI model. RIP uses port number 520.

Hop Count

Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hops allowed in a path from source and

destination. The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

DISTANCE VECTOR ROUTING PROTOCOL:

In distance-vector routing (DVR), each router is required to inform the topology changes to its neighbouring routers periodically. Historically it is known as the old ARPANET routing algorithm or Bellman-Ford algorithm.

How the DVR Protocol Works

- In DVR, each router maintains a routing table. It contains only one entry for each router. It contains two parts – a preferred outgoing line to use for that destination and an estimate of time (delay). Tables are updated by exchanging the information with the neighbour's nodes.
- Each router knows the delay in reaching its neighbours (Ex – send echo request).
- Routers periodically exchange routing tables with each of their neighbours.
- It compares the delay in its local table with the delay in the neighbour's table and the cost of reaching that neighbour.
- If the path via the neighbour has a lower cost, then the router updates its local table to forward packets to the neighbour.

4.)Explain Leaky bucket algorithm

https://www.tutorialspoint.com/what-is-leaky-bucket-algorithm-in-computer-networks
REFER THIS LINK

5.)Explain the Traffic Shaping ?

A.Traffic shaping (also known as packet shaping) is a bandwidth management technique that delays the flow of certain types of network packets in order to ensure network performance for higher priority applications. Traffic shaping essentially limits the amount of bandwidth that can be consumed by certain types of applications. It is primarily used to ensure a high quality of service for business-related network traffic.

The most common type of traffic shaping is application-based traffic shaping. Fingerprinting tools are first used to identify the application associated with a data packet. Based on this, specific traffic shaping policies are applied. For example, you might want to use application-based traffic-shaping to throttle peer-to-peer file sharing, while giving maximum bandwidth to a business-critical application such as Voice-over-IP (VoIP), which is especially sensitive to latency.

Many application protocols use encryption to circumvent application-based traffic shaping. To prevent applications from bypassing traffic shaping policies, route-based traffic shaping can be used. Route-based traffic shaping applies packet regulation policies based on the source and intended destination of the previous address of a packet.

6.)Illustrate in detail about non- adaptive algorithms

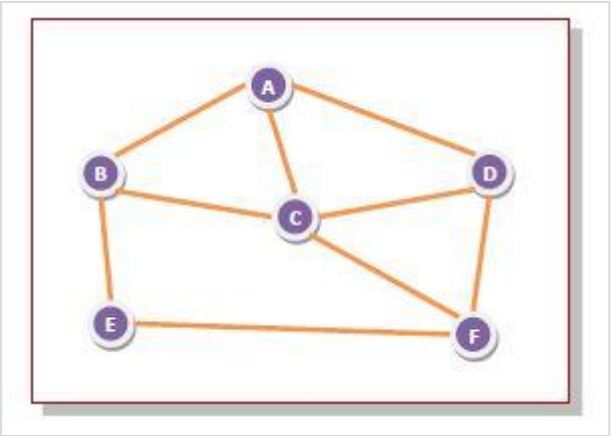
https://www.tutorialspoint.com/non-adaptive-routing-algorithms#:~:text=Non%2Dadaptive%20routing%20algorithms%2C%20also,packets%20are%20to%20be%20sent.

REFER THIS LINK

7.)Explain the Flooding algorithms

A.Flooding is a non-adaptive routing technique following this simple method: when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived on.

For example, let us consider the network in the figure, having six routers that are connected through transmission lines.



Using flooding technique –

- An incoming packet to A, will be sent to B, C and D.
- B will send the packet to C and E.
- C will send the packet to B, D and F.
- D will send the packet to C and F.
- E will send the packet to F.
- F will send the packet to C and E.

Types of Flooding

Flooding may be of three types –

- Uncontrolled flooding – Here, each router unconditionally transmits the incoming data packets to all its neighbours.
- Controlled flooding – They use some methods to control the transmission of packets to the neighbouring nodes. The two popular algorithms for controlled flooding are Sequence Number Controlled Flooding (SNCF) and Reverse Path Forwarding (RPF).
- Selective flooding – The routers don't transmit the incoming packets only along those paths which are heading approximately in the right direction, instead of every available path.

8.)List the fields of an IPv4 datagram header that participate in fragmentation and reassembly.

A,)https://www.geeksforgeeks.org/ipv4-datagram-fragmentation-and-delays/

9.)Demonstrate the link state routing algorithm with an example?

A.)Link state routing is a technique in which each router shares the knowledge of its neighbourhood with every other router in the internetwork.

The three keys to understand the Link State Routing algorithm:

- **Knowledge about the neighbourhood:** Instead of sending its routing table, a router sends the information about its neighbourhood only. A router broadcasts its identities and cost of the directly attached links to other routers.
- **Flooding:** Each router sends the information to every other router on the internetwork except its neighbours. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbours. Finally, each and every router receives a copy of the same information.
- **Information sharing:** A router sends the information to every other router only when the change occurs in the information.

Link State Routing has two phases:

Reliable Flooding

- **Initial state:** Each node knows the cost of its neighbours.
- **Final state:** Each node knows the entire graph.

10)State the major difference between Distance Vector Routing and Link state routing. Discuss

A.)

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 neighbors.	--> Based on global knowledge i.e. it have knowledge about entire network.
--> Make use of Bellman Ford algo	--> Make use of Dijkastra's algo
--> Traffic is less	--> Traffic is more
--> Converges slowly i.e. good news spread fast and bad news spread slowly.	--> Converges faster.
--> Count to infinity problem.	--> No count to infinity problem.
--> Persistent looping problem i.e. loop will there forever.	--> No persistent loops, only transient loops.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

11.)Explain the various congestion control mechanism in detail

A.)https://www.geeksforgeeks.org/congestion-control-techniques-in-computer-networks/
REFER THIS LINK

12.)Explain Internet Protocol with the neat block diagram of IP header format.

A.)IP protocol is one of the main protocols in the TCP/IP stack.
It is in the form of IP datagrams that all the TCP, UDP, ICMP and IGMP data travels over the network.
IP is connection less and unreliable protocol. It is connection less in the sense that no state related to IP datagrams is maintained either on source or destination side and it is unreliable

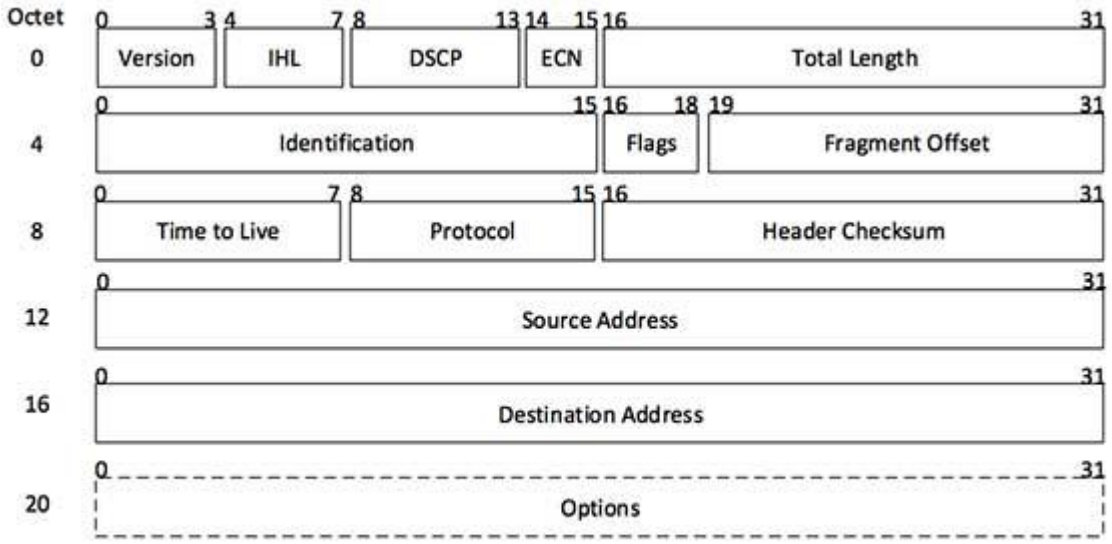
in the sense that it not guaranteed that an IP data gram will get delivered to the destination or not.
https://www.thegeekstuff.com/2012/03/ip-protocol-header/

13.)List and explain the features of the IPv6 Protocol.
A.)https://www.geeksforgeeks.org/introduction-and-ipv4-datagram-header/
REFER THIS LINK

14.)Illustrate the IP packet format with a neat diagram.?
A.) Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data units received from the above layer and adds to its own header information.

(IP Encapsulation)

The encapsulated data is referred to as IP Payload. The IP header contains all the necessary information to deliver the packet at the other end.



[Image: IP Header]

Other details are as follows –

- **Version** – Version no. of Internet Protocol used (e.g. IPv4).

- **IHL** – Internet Header Length; Length of entire IP header.
- **DSCP** – Differentiated Services Code Point; this is Type of Service.
- **ECN** – Explicit Congestion Notification; It carries information about the congestion seen in the route.
- **Total Length** – Length of entire IP Packet (including IP header and IP Payload).
- **Identification** – If the IP packet is fragmented during the transmission, all the fragments contain the same identification number. to identify the original IP packet they belong to.
- **Flags** – As required by the network resources, if an IP Packet is too large to handle, these 'flags' tell if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- **Fragment Offset** – This offset tells the exact position of the fragment in the original IP Packet.
- **Time to Live** – To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- **Protocol** – Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example, the protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- **Header Checksum** – This field is used to keep the checksum value of the entire header which is then used to check if the packet is received error-free.
- **Source Address** – 32-bit address of the Sender (or source) of the packet.
- **Destination Address** – 32-bit address of the Receiver (or destination) of the packet.

- **Options** – This is an optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stam

15.)Explain the IPv6 packet format
A.) https://www.geeksforgeeks.org/internet-protocol-version-6-ipv6-header/
REFER THIS LINK

16.)Discuss the datagram delivery and forwarding in internet protocol.?
A.)**Datagram Delivery Protocol (DDP)** is a member of AppleTalk (AppleTalk is a set of local area network communication protocols originally created for Apple computers.) networking protocol suite that deals with the socket-to-socket delivery of datagrams over an AppleTalk Network.
Applications :
Any application that can tolerate packet loss can use DDP. All application-level protocols of AppleTalk were built on top of DDP.

Datagram Forwarding:In the datagram-forwarding model of packet delivery, packet headers contain a destination address. It is up to the intervening switches or routers to look at this address and get the packet to the correct destination.

17.)Find the class of each IP address. Give a suitable explanation. i) 227.12.14.87 ii) 193.14.56.22 iii) 14.23.120.8 iv) 252.5.15.111 v) 134.11.78.56 vi) 172.18.58.1
A.)

18.)Define IPv6 protocol.
A.)IP address is your digital identity. It's a network address for your computer so the Internet knows where to send you emails, data, etc.
IP address determines who and where you are in the network of billions of digital devices that are connected to the Internet.IPv6 or Internet Protocol Version 6 is a network layer protocol that allows communication to take place over the network. IPv6 was designed by Internet Engineering Task Force (IETF) in December 1998 with the purpose of super seding the IPv4 due to the global exponentially growing internet users.

19.)Explain about Internet Control Message Protocol.
A.)The Internet Control Message Protocol (ICMP) is a protocol that devices within a network use to communicate problems with data transmission. In this ICMP definition, one of the primary ways in which ICMP is used is to determine if data is getting to its destination and at the right time. This makes ICMP an important aspect of the error reporting process and testing to see how well a network is transmitting data. However, it can also be used to execute distributed denial-of-service (DDoS) attacks.

The manner in which ICMP works in network communication is similar to the communication that happens between a carpenter building a house and a home improvement store. The store sends studs, floorboards, roofing materials, insulation, and more, assuming that each component arrives and in the right order.

The number one use of ICMP is for reporting errors. Anytime two devices are connected through the internet, ICMP can be used to create errors that can go from the receiving device to the sending device if some of the data did not arrive as expected. For example, extremely large packets of data may be too big for a router to manage. In that case, the router will discard the data packet and transmit an ICMP message to the sender informing it of the issue.

Another common use of ICMP is as a diagnostic tool to assess a network's performance. Both traceroute and ping use ICMP. Traceroute and ping are messages sent regarding whether data was successfully transmitted. When traceroute is used, the devices that a packet of data went through to get to its destination are displayed in the report. This includes the physical routers that handled the data.

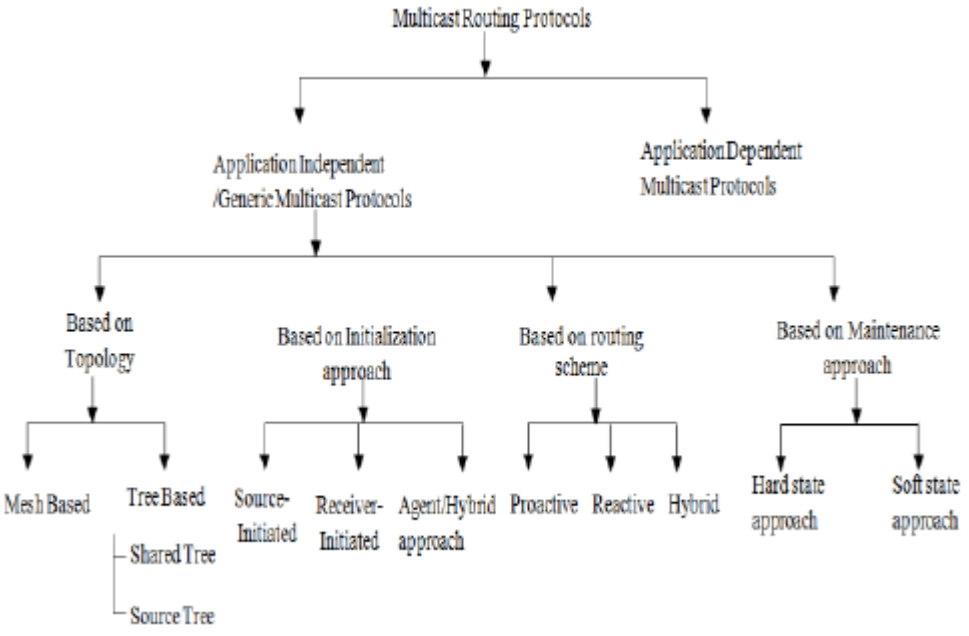
20.)Explain about IP addressing methods.

A.)https://product-help.schneider-electric.com/Machine%20Expert/V1.1/en/ESMEModbusTCP/ESMEModbusTCP/SoM_Industrial_Ethernet_-_Configuration/SoM_Industrial_Ethernet_-_Configuration-5.htm

21.)Classify two groups of multicast routing protocols

A.) https://networklessons.com/multicast/multicast-routing

REFER THIS LINK



PART-A

1.)Define the following MASKS in slash notation (/n). a) 255.0.0.0 b) 255.255.224.0 c) 255.255.255.0 d) 255.255.240.0?

2.)Why are we running out of IPv4 addresses? How does IPv6 solve this problem?

A.)IPv6 uses 128-bit addresses as opposed to the 32-bit addresses used by IPv4, allowing for a substantially larger number of possible addresses. With each bit corresponding to a ‘0’ or ‘1’, this theoretically allows 2^128 combinations or 340 trillion, trillion, trillion addresses. By contrast, IPv4 permits 2^32 combinations for a maximum of approximately 4.7 billion addresses.

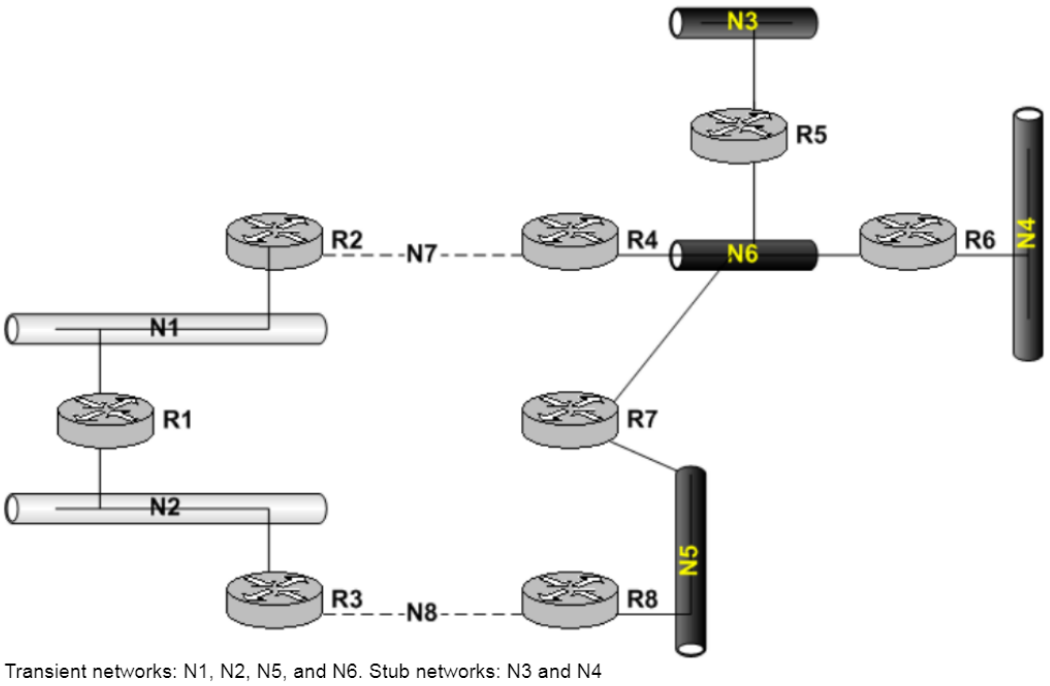
In practice, the actual number of usable addresses is slightly less as IPv6 addresses are structured for routing and other purposes, whilst certain ranges are reserved for special use. The number of IPv6 addresses available, though, is still extremely large.

3.)Find the class of the following IP addresses. a) 237.14.2.1b) 208..35.54.12c) 129.14.6.8 d) 114.34.2.8

A.)

4.)Design the autonomous system with the following specifications : a) There are 8 networks (N1 toN8) b) There are 8 routers (R1 toR8) c) N1,N2,N3,N4,N5 and N6 are Ethernet LANs d) N7 and N8 are point to point WANs e) R1 connects N1 andN2 f) R2 connects N1 andN7 R3 connects N2 andN8

A.)



Transient networks: N1, N2, N5, and N6. Stub networks: N3 and N4

5.)A router with IPV4 address 123.45.21.12 and Ethernet physical address 23:45: BA: 00:67: CD has received a packet for a host destination with IP address 124.10.78.10.Show the entries in the ARP request packet sent by the router. Assume no sub-netting?

A.)

6.)Define Subnet. Consider a company is granted the site address 201.70.64./16. The company needs six subnets of equal size, accordingly design the subnets.

A.)You will need to borrow 3 bits from the host. This gives you the following:
Subnets available = 8

Your subnet mask will be 255.255.255.224

Hosts available per subnet = 30 (32 minus 1 for the network and 1 for broadcast)

Your network addresses available are:

201.70.64

Networks: | Hosts IPs | Broadcast

.0 ……| .1 –. 30 …| 31

.32 ……| .33 - .62 ..| 63

.64 ……| 65 - 94 ..| 95

.96…… | 97 - 126 ..| 127

.128……| 129 - 158 | 159

.160……| 161 - 190 | 191

.192……| 193 - 222 | 223

.224……| 225 - 254 | 255

7.)Consider a host using a leaky bucket strategy for traffic shaping. The host sends burst data at a rate of 15Mbps for the first 3 seconds and remains silent for 2 seconds. Then again a burst data at a rate of 6 Mbps is sent for next 2 seconds and then the host remains silent for next 2 seconds. Now again the host sends data at a rate of 5 Mbps for the next 3 seconds. What will be the output data rate of the leaky bucket?
A.)

8.)Write an example, demonstrate how to make a routing table using distance vector routing. And list down the limitation
A.)

9.)What are the reasons for congestion? What are the problems with congestion?
A.)
Network Congestion occurs when the traffic flowing through a network exceeds its maximum capacity. In most cases, congestion is a temporary issue with the network caused due to a sudden upsurge of traffic, however, sometimes, a network is continually congested, indicating a deeper problem

1. Bandwidth Issues

Probably the most common cause of network congestion is plain old bandwidth. Bandwidth is the maximum rate that data can travel along a given path — that path's total capacity. When there's simply not enough bandwidth to handle the amount of traffic you have for a particular network, you've got network congestion.

2. Latency

Latency is the delay in the time it takes for your data packet to get from point A to point B. So, using our same example above about bandwidth: You're a driver on the highway, and you're travelling the speed limit. Typical day, typical conditions. But what if all of a sudden you hit rush hour traffic? Like we explained above, you'll have to slow down

3. Jitter

Jitter is variability in delay. Computers, like drivers, like to have their traffic consistent and predictable. And when traffic becomes inconsistent, or unpredictable, it causes variability in delay (jitter), and causes further congestion.

Back to the highway. Not all the extra cars appear on the highway at the same time, and they don't all exit at the same time. For networks, that could be a computer that starts sending large bursts of traffic on the network, taking up excessive amounts of bandwidth.

4. Packet retransmissions

Packet retransmissions are usually a result of the first three congestion issues. If a packet doesn't get to its destination, or if it arrives damaged, then it must be resentful. And this has a way of exacerbating the problem. If you need to send each packet two or more times to reach the destination, you're increasing traffic congestion without any incremental benefit. It'd be like taking the family on a road trip, but every person takes their own car!

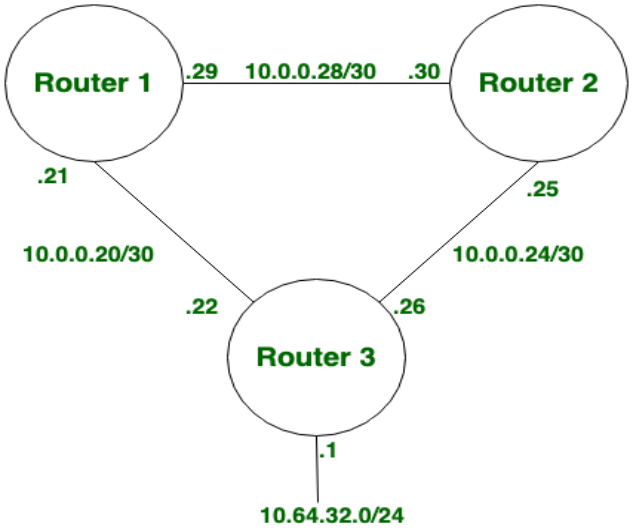
5. Collisions

The back-off process, mentioned in relation to jitter, is a severe situation where all packets have to wait for the network to clear before retransmitting. Normally this is due to packet collisions on the network, the result of bad equipment or poor cabling.

10.)Classify the static and dynamic routing algorithms? Explain the basic concept of flooding.

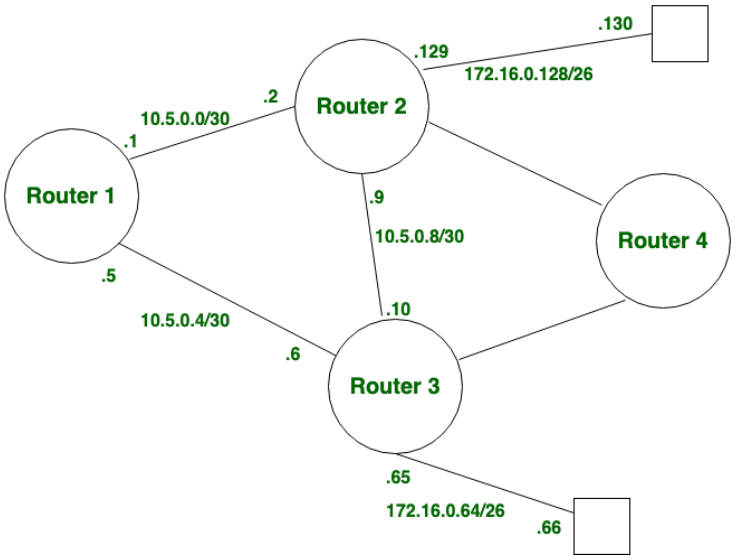
A.)**Static Routing:**

Static Routing is also known as **non-adaptive** routing which doesn't change the routing table unless the network administrator changes or modifies them manually. Static routing does not use complex routing algorithms and It provides high or more security than dynamic routing.



Dynamic Routing:

Dynamic routing is also known as **adaptive** routing which changes the routing table according to the change in topology. Dynamic routing uses complex routing algorithms and it does not provide high security like static routing. When the network change(topology) occurs, it sends the message to the router to ensure that changes then the routes are recalculated for sending updated routing information.



11.)What is the format of the IPv4 header? Describe the significance of each field.

A.)https://www.educba.com/ipv4-header-format/

12.)Rewrite the following IP addresses using binary notation: a. 110.11.5.88 b. 12.74.16.18 c. 201.24.44.32

13.)Rewrite the following IP addresses using dotted-decimal notation: a. 01011110 10110000 01110101 00010101 b. 10001001 10001110 11010000 00110001 c. 01010111 10000100 00110111 00001111

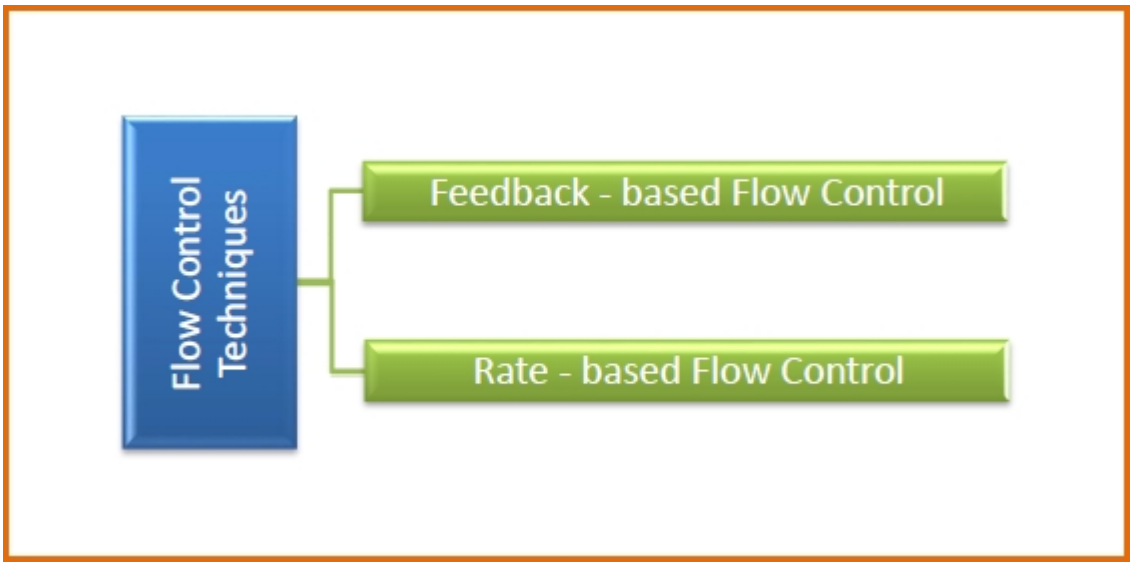
14.)Find the class of the following classful IP addresses: a. 130.34.54.12 b. 200.34.2.1 c. 245.34.2.8

15.)What is the need of Flow control? Explain the common approaches for flow control in the data link layer.

A.) Flow control is a technique that allows two stations working at different speeds to communicate with each other. It is a set of measures taken to regulate the amount of data that a sender sends so that a fast sender does not overwhelm a slow receiver. In the data link layer, flow control restricts the number of frames the sender can send before it waits for an acknowledgment from the receiver.

Approaches of Flow Control

Flow control can be broadly classified into two categories –



- Feedback based Flow Control In these protocols, the sender sends frames after it has received acknowledgments from the user. This is used in the data link layer.
- Rate based Flow Control These protocols have built in mechanisms to restrict the rate of transmission of data without requiring acknowledgment from the receiver. This is used in the network layer and the transport layer.

16.)Classify the static and dynamic routing algorithms? Explain the basic concept of flooding.?

A.)Same as Part-A 10th que

17.)What is the format of the IPv4 header? Describe the significance of each field.

A.)Same as part-a 11th que

18.)What is the format of the IPv6 header? Describe the significance of each field.
A.)https://www.educba.com/ipv6-header-format/