Unit V

5 Network Layer : Routing Protocols

5.1 : Routing

Q.1 Explain routing. State properties of routing algorithm. Classify routing algorithm.

Or Explain following routing
i) Static routing ii) Dynamic routing iii) Default routing.

☞ [SPPU : Jun-22, Marks 9]

Ans. : • A host or a router has a routing table with an entry for each destination, or a combination of destinations, to route IP packets. Routing table can be either static or dynamic.

- A static routing table contains information entered manually. The administrator enters the route for each destination into the table.
- Dynamic routing table is updated periodically by using one of the dynamic routing protocols such as RIP, OSPE or BGP.
- The main function of the network layer is to route packets from source to destination. To accomplish this a route through the network must be selected, generally more than one route is possible.
- The selection of route is generally based on some performance criteria. The simplest criteria is to choose shortest root through the network.
- The shortest root means a route that passes through the least number of nodes. This shortest root selection results in least number of hops per packet. A routing algorithm is designed to perform this task. The routing algorithm is a part of network layer software.

Properties of routing algorithm

- Certain properties which are desirable in a routing algorithm are - Correctness, simplicity, robustness, stability, fairness, optimality and efficiency.

1. **Correctness** and simplicity are self-explanatory.
2. **Robustness** means the ability to cope with changes in the topology and traffic without requiring all jobs in hosts to be aborted and network to be rebooted everytime.
3. **Stability** refers to equilibrium state of algorithm. It is the technique that react to changing conditions such as congestions. Under any conditions the network must not react too slow or experience unstable swings from one extreme to another.
4. Some performance criteria may favour the exchange of data packets between nearby stations and discourage the exchange between distant stations. Some compromise is needed between fairness and optimality.

Routing algorithm classification

- Routing algorithm can be classified in several ways. Based on their responsiveness it can be classified into two types -

1. Static (non-adaptive) Routing Algorithms.
2. Dynamic (adaptive) Routing Algorithms.

1. Static (non-adaptive) routing algorithms

- In static routing the network topology determines the initial paths. The precalculated paths are then loaded to the routing table and are fixed for a longer period.
- Static routing is suitable for small networks. Static routing becomes **cumber some** for bigger networks.
- The disadvantage of static routing is its inability to respond quickly to network failure.

2. Dynamic (Adaptive) routing algorithms

- Dynamic routing algorithms change their routing decision if there is change in topology, traffic. Each router continuously checks the network status by communicating with neighbours.

- Thus a change in network topology is eventually propagated to all the routers. Based on this information gathered, each router computes the suitable path to the destination.
- The disadvantage of dynamic routing is its complexity in the router.

Routing tables

- Once the routing decision is made, this information is to be stored in routing table so that the router knows how to forward a packet.
- In virtual circuit packet switching, the routing table contains each incoming packet number and outgoing packet number and output port to which the packet is to forward.
- In datagram networks, routing table contains the next hop to which to forward the packet, based on the destination address.

Q.2 Differentiate between static & dynamic routing.

Ans. :

Sr. No.	Static routing (Non adaptive)	Dynamic routing (Adaptive)
1.	Static routing manually sets up the optimal paths between the source and the destination computers.	Dynamic routing uses dynamic protocols to update the routing table and to find the optimal path between the source and the destination computers.
2.	The routers that use the static routing algorithm do not have any controlling mechanism if any faults in the routing paths.	The dynamic routing algorithms are used in the dynamic routers and these routers can sense a faulty router in the network.
3.	These routers do not sense the faulty computers encountered while finding the path between two computers or routers in a network.	The dynamic router eliminates the faulty router and finds out another possible optimal path from the source to the destination.
4.	The static routing is suitable for very small networks and they cannot be used in large networks	Dynamic routing is used for larger networks.

5.	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.
6.	The static routing has the advantage that it requires minimal memory.	Dynamic routers have quite a few memory overheads, depending on the routing algorithms used.
7.	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.

5.2 : Routing Algorithm

Q.3 Explain distance vector routing algorithms with example.

☞ [SPPU : April-18, In-Sem, Marks 4]

Ans. : • Distance vector routing algorithm is the dynamic routing algorithm. It was designed mainly for small network topologies. Distance vector routing algorithm is sometimes called by other names, most commonly the distributed **Bellman-Ford** routing algorithm and the **Ford-Fulkerson** algorithm.

- The term distance vector derives from the fact that the protocol includes its routing updates with a vector of distances, or hop counts.
- In this algorithm, each router maintains a routing table indexed by, and containing one entry for, each router in the subnet. This entry contains two parts :
  a. The preferred outgoing line to use for that destination.
  b. An estimate of the time or distance to that destination.
- The metric used might be number of hops, time delay in milliseconds, total number of packets queued along the path, etc.
- Assume that delay is used as a metric and that the router knows the delay to each of its neighbours. All nodes exchange information only

with their neighbouring nodes. Nodes participating in the same local network are considered neighbouring nodes.

- Once every 'T' msec each router sends to each neighbor a list of its estimated delays to each destination. It also receives a similar list from each neighbor.
- By performing calculation for each neighbour, a router can find out which estimate seems the best and use that estimate and the corresponding line in its new routing table. Old routing table is not used in the calculation.
- Fig. Q.3.1 shows the subnet with 12 routers.

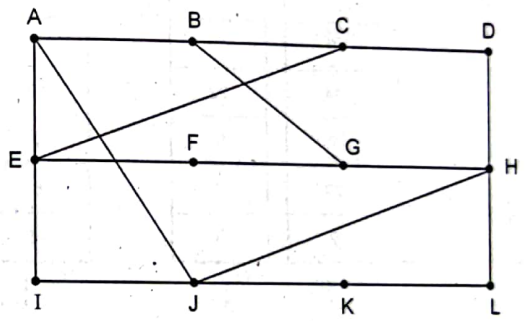


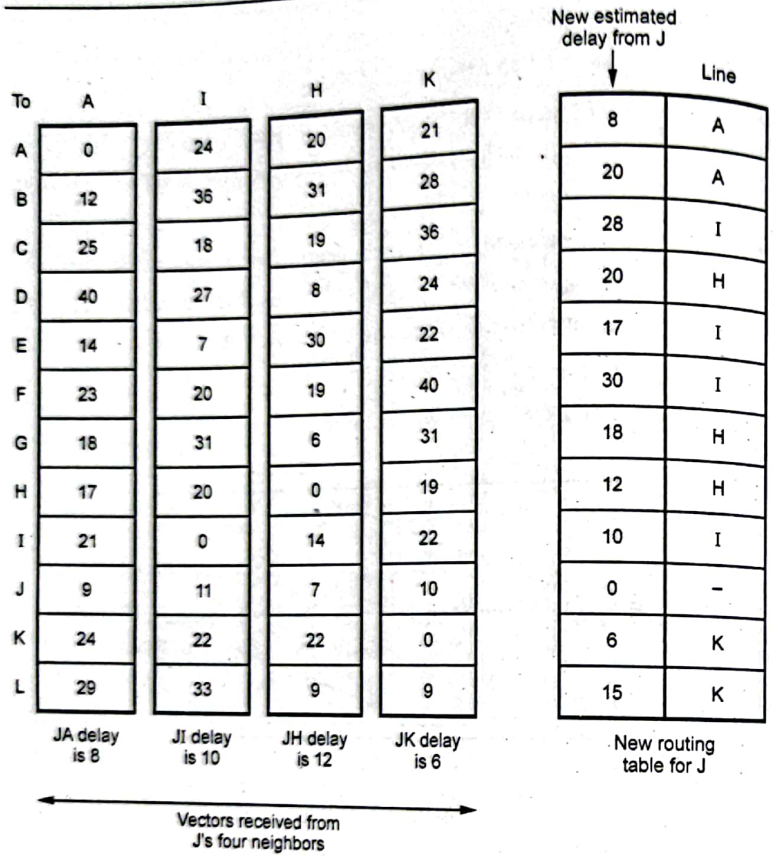
Fig. Q.3.1 Subnet

Routing table is shown below. (Refer table on next page)

Q.4 What are the problems in RIP ? How to overcome the problems ? Compare RIPv1 and RIPv2. ☞ [SPPU : Jun-22, Marks 9]

Ans. : • In RIP, routing updates are exchanged between neighbours approximately every 30 seconds using a so-called **RIP response message**. The response message sent by a router or host contains a list of upto 25 destination networks within an Autonomous System (AS). Response messages are also known as **RIP advertisements**.

- Fig. Q.4.1 shows a portion of an autonomous system.
- Forwarding table in router D before receiving advertisement from router A. For this example, the table indicates that to send a datagram from



router D to destination network W, the datagram should first be forwarded to neighbouring router A; the table also indicates that destination network W is two hops away along the shortest path.

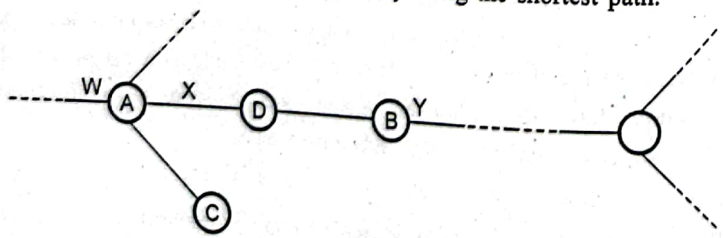


Fig. Q.4.1 Portion of AS

- The Table Q.4.1 also indicates that network Z is seven hops away via router B.

Destination network	Next router	Number of hops to destination
W	A	2
Y	B	2
Z	B	7
X	–	1
.....	.....	.....

Table Q.4.1 Forwarding table

- Now suppose that 30 seconds later, router D receives from router A the advertisement shown in Table Q.4.2.

Destination network	Next router	Number of hops to destination
Z	C	4
W	–	1
X	–	1
.....	.....	.....

Table Q.4.2 Advertisement from router A

- Note that the advertisement is nothing other than the forwarding table information from router A. This information indicates, in particular, that network Z is only four hops away from router A. Router D, upon receiving this advertisement, merges the advertisement with the old routing table.
- Router D learns that there is now a path through router A to network Z that is shorter than the path through router B. Thus, router D updates its forwarding table to account for the shorter shortest path, as shown in Table Q.4.3.

Destination network	Next router	Number of hops to destination
W	A	2
Y	B	2
Z	A	3
.....	.....	.....

Table Q.4.3 Forwarding Table

- RIP routers exchange advertisements approximately every 30 seconds. If a router does not hear from its neighbour atleast once every 180 seconds, that neighbour is considered to be no longer reachable; i.e. either the neighbour has died or the connecting link has gone down. When this happens, RIP modifies the local forwarding table and then propagates this information by sending advertisements to its neighbouring routers.
- A router can also request information about its neighbour's cost to a given destination using RIP's request message. Routers send RIP request and response messages to each other over UDP using port number 520.

RIP Message Format

- Fig. Q.4.2 shows the RIP message format.

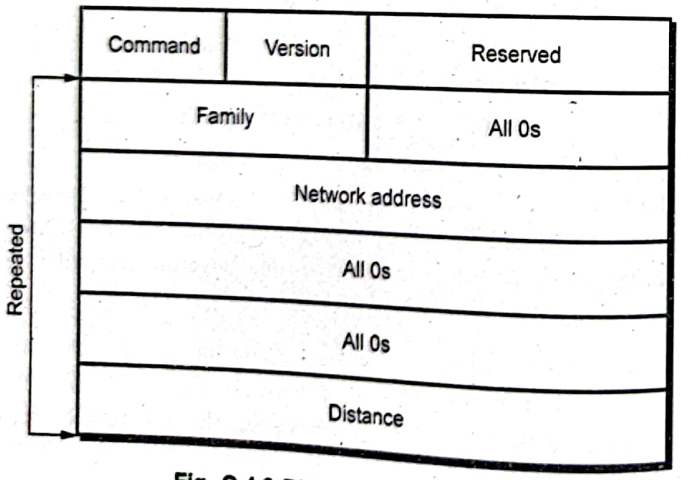


Fig. Q.4.2 RIP message format

1. **Command :** This is 8 bits field specifies the type of message : 1 for request and 2 for response.
2. **Version :** This is 8 bits field define the version.
3. **Family :** This 16 bits field defines the family of the protocol used. For TCP/IP the value is 2.
4. **Network address :** The address field defines the address of the destination network.
5. **Distance :** This 32 bits field defines the hop count from the advertising router to the destination network.

Request and Response

- RIP support two types of messages : Request and Response.

Request

- A request message is sent by a router that has just comp up or by a router that has some time out entries.

Response

- A response message can be either solicited or unsolicited.

1. Solicited response
   - Is sent only in answer to a request.
   - Containing information about the destination specified in the corresponding request.
2. Unsolicited response
   - Is sent periodically, every 30 seconds.
   - **Containing** information covering the whole routing table

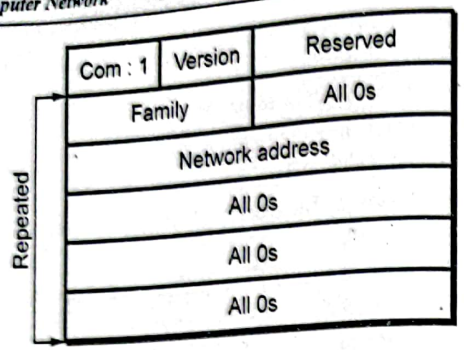
Fig. Q.4.3 shows the request message.

Timers in RIP

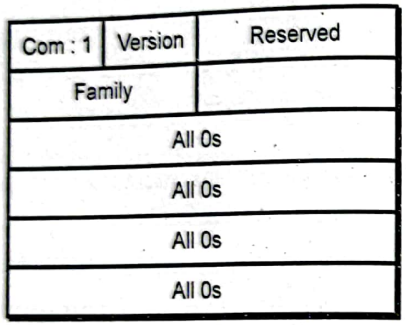
- RIP uses three timers to support its operation.

1. Periodic timer (25 - 35 sec)
2. Expiration (180 sec)
3. Garbage collection (120 sec).

1. **Periodic timer :** This type of timer controls the advertising of regular update messages. Each router has one periodic timer that is randomly set to a number between 25 to 35 seconds.



(a) Request for some



(b) Request for all

Fig. Q.4.3 Request message format

2. **Expiration timer :** The expiration timer governs the validity of a route. In normal situation, the new update for the route occurs every 30 seconds. But, if there is a problem on an internet and no update is received within the allotted 180 seconds, the route is considered expired and the hop count of the route is set to 16. Each router has its own expiration timer.
3. **Garbage collection timer :** When the information about a route becomes invalid, the router continues to advertise the route with a metric value of 16 and the garbage collection timer is set to 120 sec for that route. When the count reaches zero, the route is purged from the table.

RIPv2

- RIP version 2 was designed to overcome some of the shortcomings of version 1. Replaced fields in version 1 that were filled with 0s for the TCP/IP protocols with some new fields.
- **Advantages**
  1. An AS can include several hundred routers with RIP-2 protocol.
  2. Compatible upgrade of RIPv1 including subnet routing, authentication, CIDR aggregation, route tags and multicast transmission.
  3. Subnet support : Uses more convenient partitioning using variable-length subnets
  4. An end system can run RIP in passive mode to listen for routing information without supplying any.
  5. Low requirement in memory and processing at the node .
  6. RIP and RIP2 are for the IPv4 network while the RIPng is designed for the IPv6 network.

Fig. Q.4.4 shows the message format.

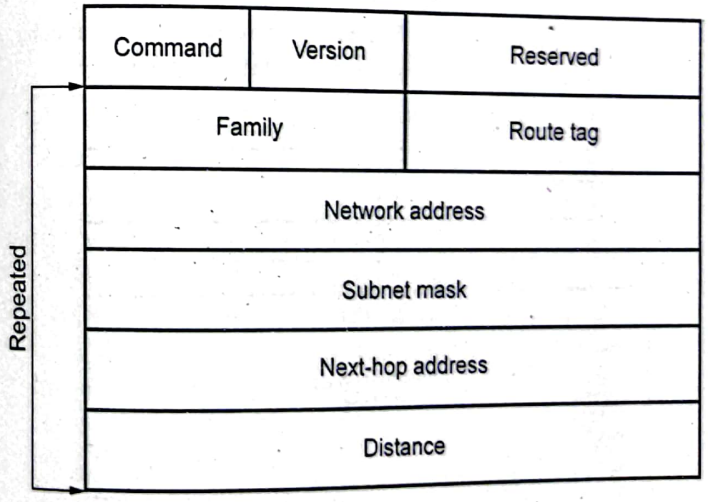


Fig. Q.4.4 Message format of RIPv2

1. **Command** - The command field is used to specify the purpose of the datagram.
2. **Version** - The RIP version number. The current version is 2.
3. **Identifier** - Indicates what type of address is specified in this particular entry.
4. **Route tag** - Attribute assigned to a route which must be preserved and readvertised with a route. The route tag provides a method of separating internal RIP routes from external RIP routes, which may have been imported from an EGP or another IGP.
5. **IP address** - The destination IP address.
6. **Subnet mask** - Value applied to the IP address to yield the non-host portion of the address. If zero, then no subnet mask has been included for this entry.
7. **Next hop** - Immediate next hop IP address to which packets to the destination specified by this route entry should be forwarded.
8. **Distance** - Represents the total cost of getting a datagram from the host to that destination.

Authentication

- Authentication is added to protect the message against unauthorized advertisement. No new field is added to the packet.
- To indicate that the entry is authentication information and not routing information, the value of FFFFH is entered in the family field.
- Fig. Q.4.5 shows the authentication.

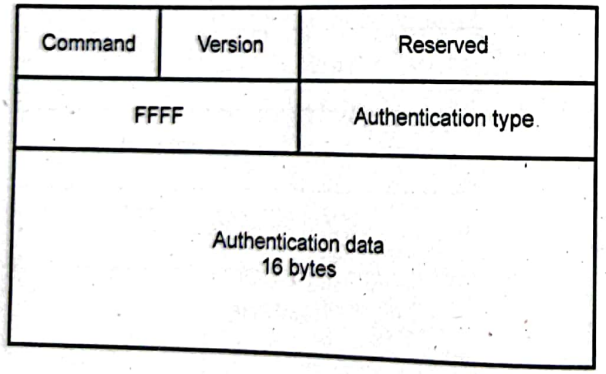


Fig. Q.4.5 Authentication

- Authentication type defines the protocol used for authentication.
- Authentication data is the actual data.

RIP2 - Disadvantages

1. RIP2 supports generic notion of authentication, but only "password" is defined so far. Still not very secure.
2. RIP2 packet size increases as the number of networks increases hence it is not suitable for large networks.
3. RIP2 generates more protocol traffic than OSPF, because it propagates routing information by periodically transmitting the entire routing table to neighbour routers.
4. RIP2 may be slow to adjust for link failures.

Advantages of RIP and Disadvantages of RIP version 1

Advantages of RIP

1. RIP is very useful in a small network, where it has very little overhead in terms of bandwidth used and configuration and management time.
2. Easy to implement than newer IGP's.
3. Many implementations are available in the RIP field.

Disadvantages of RIP1

1. Minimal amount of information for router to route the packet and also very large amount of unused space.
2. Subnet support : Supports subnet routes only within the subnet network.
3. Not secure; anyone can act as a router just by sending RIP1 messages.

RIP1 was developed for an AS that originally included less than a 100 routers.

Q.5 Compare between RIPv1 and RIPv2.

☞ [SPPU : April-18, In-Sem, Marks 4]

Ans. :

Sr. No.	RIPv1	RIPv2
1.	It is classful protocol.	It is classless protocol.

2.	There is no support for router authentication.	It support for authentication.
3.	It does not support variable length subnet mask.	It support variable length subnet mask.
4.	RIPv1 uses broadcasts for updates.	RIPv2 uses multicast for updates.
5.	It does not support variable length subnet mask.	It does not support variable length subnet mask.

Q.6 Explain Link State routing.

Ans. : • Link state routing is the second major class of intradomain routing protocol. It is **dynamic** type routing algorithm.

• The idea behind link state routing is simple and can be stated as five parts. Each router must do the following :

1. **Learning about the neighbors :** When a router is booted, it sends a special HELLO packet on each point-to-point line. The router on the other end is expected to send back a reply telling who it is. When two or more routers are connected by a LAN, the LAN can be modeled as a node.
2. **Measuring line cost :** To determine the cost for a line, a router sends a special ECHO packet over the line that the other side is required to send back immediately. By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay. Should the load be taken into account when measuring the delay ?
3. **Building link state packets :** State packets may be built periodically, or when some significant event occurs, such as a line or neighbour going down or coming back up again.
4. **Distributing the link state packets :** The basic algorithm
   - Each state packet contains a sequence number that is incremented for each new packet sent.
   - Routers keep track of all the (source router, sequence) pairs they see.

- When a new link state packet comes in, it is checked against the list of packets already seen. If it is new, it is forwarded on all lines except the one it arrived on (i.e., flooding). If it is a duplicate, it is discarded. If a packet with a sequence number lower than the highest one seen so far ever arrives, it is rejected as being obsolete.

Problems with the basic algorithm :

1. The sequence numbers may wrap around, causing confusion. Solution : Using a 32-bit sequence number. With one packet per second, it would take 137 years to wrap around.
2. If a router ever crashes, it will lose track of its own sequence number. If it starts again at the sequence number 0, new packets will be rejected as obsolete/duplicate by other routers.
3. If a sequence number is ever corrupted and 65,540 is received instead of 4 (a 1-bit error), packets 5-65540 will be rejected as obsolete.

• The solution to router crashes and sequence number corruption is to associate an age with each state packet from any router and decrement the age once per second. When the age hits zero, the information from that router is discarded. Normally a new packet comes in every 10 seconds, so router information only times out when a router is down.

Some refinements to the basic algorithm make it more robust

- When a state packet comes in to a router for flooding, it is put in a holding area to wait a short while first.
- If another state packet from the same source comes in before it is transferred, their sequence numbers are compared.
- If they are equal, the duplicate is discarded.
- If they are different, the older one is thrown out. To guard against errors on the lines, all state packets are acknowledged.
- When a line goes idle, the holding area is scanned in round robin to select a packet or acknowledgement to send.

5. Computing the new routes : Once a router has accumulated a full set of link state packets, it can construct the entire subnet graph. Then Dijkstra's algorithm can be run locally to construct the shortest path to all possible destinations.

- Link state routing protocols use event driven updates rather than periodic updates. Link state routing is widely used in actual networks. OSPF protocol uses in a link state algorithm.
- Link state routing protocols are as follows :
  a. Open Shortest Path First (OSPF)
  b. Netware Link Services Protocol (NLSP).
  c. Apple's AURP.
  d. ISO's Intermediate System-Intemediate System (IS-IS).

Q.7 Explain with neat diagram OSPF routing protocol.

☞ [SPPU : May-18, Marks 6 Dec.-19, Marks 6]

Ans. : • OSPF is a link state routing protocol. OSPF is based on the distributed map concept all nodes have a copy of the network map, which is regularly updated. Each node contains a routing directory database.

- This database contains informations about the routers interfaces that are operable, as well as status information about adjacent routers. This information is periodically broadcast to all routers in the same domain.
- The OSPF computes the shortest path to the other routers. OSPF protocol is now widely used as the interior router protocol in TCP/IP networks. OSPF computes a route through the internet that incurs the least cost based on a user-configurable metric of cost.
- The user can configure the cost to express a function of delay, data rate, or other factors. OSPF is able to equalize loads over multiple equal cost paths.
- OSPF is classified as an Internal Gateway Protocol (IGP) because it support routing within one autonomous system only. The exchange of routing information between autonomous systems is the responsibility of another protocol an External Gateway Protocol (EGP). OSPF can support one or many networks.
- Following is the features of the OSPF.
  1. OSPF supports multiple circuit load balancing because it can store multiple routes to a destination.
  2. OSPF can converge very quickly to network topology change.

3. OSPF support multiple metrics.
4. OSPF is not susceptible to routing loops.
5. OSPF support for variable length subnetting by including the subnet mask in the routing message.

- OSPF introduces a two level hierarchy for improving scalability. It allows an AS to be partitioned into several groups called areas, that are interconnected by a central backbone area as shown in the Fig. Q.7.1.

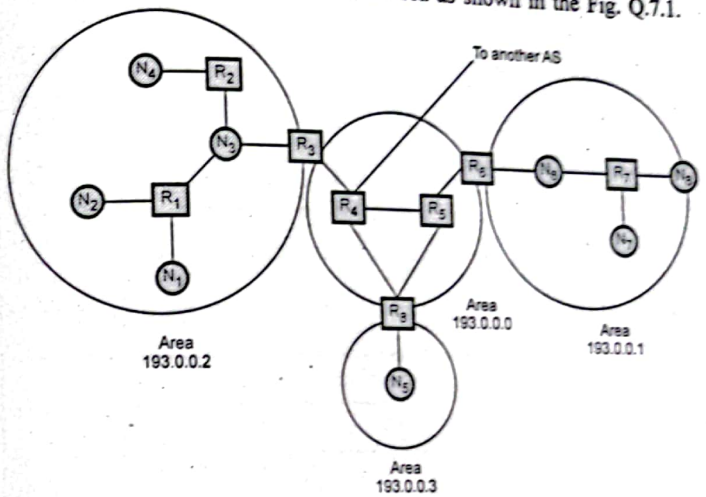


Fig. Q.7.1 OSPF areas

- An area is identified by a 32-bit number known as the area ID. The backbone area is identified with area ID 193.0.0.0. The information from other area is summarized by area border router that have connections to multiple areas.
- OSPF uses four types of routers.
  1. An internal router is a router with all its links connected to the networks within the same area.
  2. An area border router is a router that has its links connected to more than one area.
  3. A backbone router is a router that has its links connected to the backbone.

4. An Autonomous System Boundary Router (ASBR) is a router that has its links connected to another autonomous system.

- As shown in the Fig. Q.7.1 routers R_1, R_2 and R_7 are internal routers. Routers R_3, R_6, R_8 are area border routers. Routers R_3, R_4, R_5, R_6, R_8 are backbone routers. Router R_4 is an ASBR.
- A hello protocol allows neighbours to be discovered automatically. Two routers are said to be neighbours if they have an interface to a common network.
- The OSPF protocol runs directly over IP, using IP protocol 89. The header format for OSPF is shown in the Fig. Q.7.2.

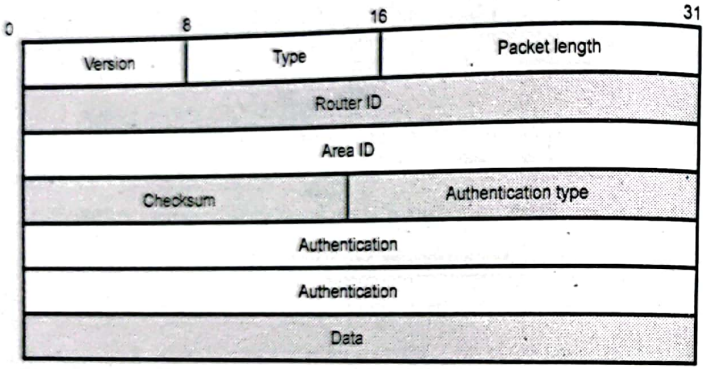


Fig. Q.7.2 OSPF common header

- OSPF header analysis is given below :

1. **Version :** This field specifies the protocol version.
2. **Type :** This field indicates messages as one of the following type.
   a. Hello
   b. Database description
   c. Link status
   d. Link status update
   e. Link status acknowledgement.
3. **Packet length :** This field specifies the length of OSPF packet in bytes, including the OSPF header.
4. **Router ID :** It identifies the sending router. This field is typically set to the IP address of one of its interfaces.

5. **Area ID :** This field identifies the area this packet belongs to (Transmitted).
6. **Checksum :** The checksum field is used to detect errors in the packet. The checksum is performed on the entire packet.
7. **Authentication type :** It identifies the authentication type that is used.
8. **Authentication :** This field includes a value from the authentication type.

- The OSPF operation consists of the following stages.

1. OSPF send the Hello messages for discovering the neighbours and designated routers are elected in multiaccess networks.
2. Adjacencies are established and link state databases are synchronized.
3. Link state advertisement are exchanged by adjacent routers to allow topological databases to be maintained and to advertise inter area and inter AS routes. The routers use the information in the database to generate routing tables.

OSPF Advantages

1. Low traffic overhead. OSPF is enconomical of network bandwidth on links between routers.
2. Fast convergence. OSPF routers flood updates to changes in the network around the internet, so that all routers quickly agree on the new topology after a failure.
3. Larger network metrics. This allows a network planner the freedom to assign costs for each path around the network, to give fine control over routing paths.
4. Area based topology. Large OSPF networks are organized as a set of areas linked by a backbone. Routing within each area is isolated to minimize cross area discovery traffic.
5. Route summaries. OSPF can minimize the routes propagated across an area boundary by collapsing several related sub-net routes into one. This reduces routing table sizes and increases the practical size of a network.
6. Support for complex address structures. OSPF allows variable size sub-netting within a network number and sub-nets of a network number to be physically disconnected. This reduces waste of address space and makes changing a network incrementally much easier.

7. Authentication. OSPF supports the use of passwords for dynamic discovery traffic, and checks that paths are operational in both directions. The main use for this is to prevent misconfigured routers from "poisoning" the routing tables throughout the internet.

OSPF Disadvantages

1. Memory overhead. OSPF uses a link state database to keep track of all routers and networks within each attached area. With a complex topology, this database can be much larger than the corresponding routing pool and may limit the maximum size of an area.
2. Processor overhead. During steady state operation the OSPF CPU usage is low, mainly due to the traffic between routers. However, when a topology change is detected, there is a large amount of processing required to support flodding of changes and recalculation of the routing table.
3. Configuration. OSPF can be complex to configure.

Q.8 Compare and contrast distance vector routing with link state routing. [SPPU : Dec.-18, Marks 4]

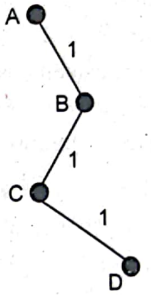
Ans. :

Sr. No.	Distance vector	Link state
1.	Bellman-ford algorithm used to calculate the shortest cost path.	Dijkstra's algorithm used to calculate link state cost.
2.	Sends message to their neighbors.	Sends message to every other node in the network.
3.	It is decentralized routing algorithm.	It is centralized global routing algorithm.
4.	Sends larger updates only to neighbouring routers.	Send small updates every where.
5.	Protocol example - RIP	Protocol example - OSPF and BGP.

6.	Require less CPU power and less memory space.	Require more CPU power and more memory space.
7.	Simple to implement and support.	Expensive to implement and support.

Q.9 Explain distance vector routing with count-to-infinity problem. [SPPU : April-19, Marks 4]

Ans. : • Fig. Q.9.1 shows an imagined network and denotes the distances from router A to every other router. Until now everything works fine.

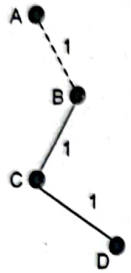


Routing table for A

B	C	D
1	2	3

Fig. Q.9.1

- Suppose that link (A, B) is broken. Router B observed it, but in his routing table he sees, that router C has a route to A with 2 hops. The problem is, that B does not know that C has router B as successor in his routing table on the route to A. That followed **count-to-infinity** problem. Router B actualizes his routing table and takes the router to A over router C.
- In Fig. Q.9.2, we can see the new distances to A. In router C's routing the route to A contains router B as next hop router, so if B has increased his costs to A, C is forced to do so. Router C increases his cost to A about B + 1 = 4.
- Now we see the conseuqence of the distributed Bellman-Ford protocal : Because router B takes the path over C to A, he reactualizes his routing table and so on.



B	C	D
3	2	3

B	C	D
3	4	3

B	C	D
5	4	5

Fig. Q.9.2

- There are several partial solutions to the count-to-infinity problem. The first one is to use some relatively small number as an approximation of infinity. For example, we might decide that the maximum number of hops to get across a certain network is never going to be more than 16 and so we could pick 16 as the value that represents infinity.
- This at least bounds the amount of time that it takes to count to infinity. Of course, it could also present a problem if our network grew to a point where some nodes were separated by more than 16 hops.
- One technique to improve the time to stabilize routing is called **split horizon**. Split horizon technique implies that routing information about some network stored in the routing table of a specific router is never sent to the router from which it was received.

Issues with the Distance Vector Routing

1. The primary drawback of this algorithm is its vulnerability to the 'Count-to-Infinity' problem. There have been proposed many partial solutions but none works under all circumstances.
2. Another drawback of this scheme is that it does not take into account Link Bandwidth.
3. Yet another problem with this algorithm is that it takes appreciably long time for convergence as the network-size grows.
4. A fallout of the Count-to-Infinity issue and slow convergence has been to limit the maximum number of hops to 15 which means more than 16-router subnets, it may not be appropriate routing algorithm.

Q.10 Understand and apply what is routing? Explain different types of routing algorithm. ☞ [SPPU : April-19, Marks 6]

Ans. : Refer Q.1, 3 & 5.

5.3 : EIGRP

Q.11 Explain EIGRP.

Ans. :
- Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance vector routing protocol based on the principles of the Interior Gateway Routing Protocol (IGRP).
- EIGRP is Cisco's IGP (Interior Gateway Protocol) that was made an "open standard" in 2013.
- EIGRP is an enhanced distance vector protocol, relying on the Diffused Update Algorithm (DUAL) to calculate the shortest path to a destination within a network.

Characteristics of EIGRP

- EIGRP has the following characteristics :
  1. Advanced operational efficiency
  2. Capabilities of both link state and distance vector
  3. A classless routing protocol
  4. Unique features including use of Reliable Transport Protocol (RTP), a diffusing update algorithm (DUAL), updates and updated information about neighbors
  5. Faster converging because it precalculates routes and does not broadcast hold-down timer packets before converging

Advantages of EIGRP

- Some of the many advantages of EIGRP are :
  1. Very low usage of network resources during normal operation; only hello packets are transmitted on a stable network.
  2. When a change occurs, only routing table changes are propagated, not the entire routing table; this reduces the load the routing protocol itself places on the network.
  3. Rapid convergence times for changes in the network topology (in some situations convergence can be almost instantaneous).

Q.12 Draw the router architecture. Explain the difference between RIP, EIGRP, OSPF in tabular format. ☞ [SPPU : June-22, Marks 9]

Ans. : A router is a networking device that allows separate individual networks of computers to connect with one another. Fig. Q.12.1 shows router architecture.

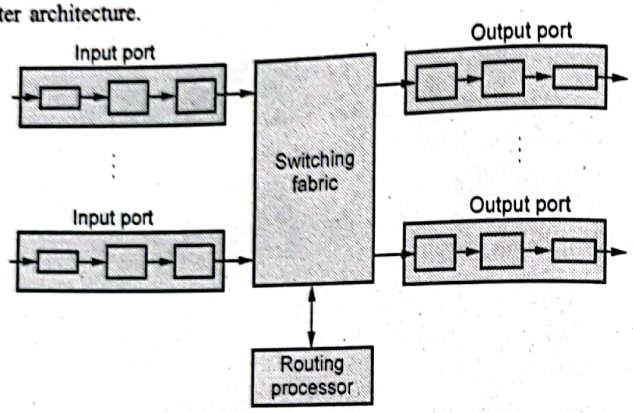


Fig. Q.12.1 Router architecture

- Router components are input port, output port, switching fabric and routing processor.
- Input port : It performs the physical layer functionality of terminating an incoming physical link to a router. It also performs the data link layer functionality and performs a lookup and forwarding function. Control packets are forwarded from the input port to the routing processor.
- Switching fabric : The switching fabric connects the router's input ports to its output ports.
- Output ports : An output port stores the datagrams that have been forwarded to it through the switching fabric and then transmits the datagrams on the outgoing link. The output port thus performs the reverse data link and physical layer functionality as the input port.

- Routing processor : The routing processor executes the routing protocols, maintains the routing tables and performs network management functions within the router.

Difference between RIP, EIGRP and OSPF :

RIP	EIGRP	OSPF
RIP is a distance vector protocol.	EIGRP is derived from Integrated Gateway Routing Protocol.	OSPF is a link state protocol.
It support maximum 15 routers in the network.	It supports maximum 255 routers in the network.	It supports unlimited router in the network.
Metrics used is hop.	Metrics used are bandwidth and delay, load and reliability.	Metrics used are bandwidth and delay.
It is basically use for smaller size organization.	It is basically use for medium to larger size organization in the network.	It is basically use for larger size organization in the network.
Admin cannot create a separate administrative boundary in the network.	Admin can create a separate administrative boundary in the network with the help of autonomous system number.	Admin can create a separate administrative boundary in the network through area number within the same area all of the routers are exchanging the route information from neighbour router in the network.

5.4 : Border Gateway Protocol (BGP)

Q.13 What is BGP ? What are the characteristics of BGP routing protocol ? What are the advantages and disadvantages of BGP routing protocol ? ☞ [SPPU : Jun-22, Marks 9]

Ans. : • The purpose of an exterior gateway protocol is to enable two different Autonomous System (AS) to exchange routing information so that IP traffic can flow across the autonomous system border. BGP was developed for use in conjunction with internets that employ the TCP/IP protocol suite. The BGP is an interdomain routing protocol that is used to exchange network reachability information among BGP routers (Also called BGP speakers). Each BGP speaker establishes a TCP connection with one or more BGP speakers (routers). Two routers are considered to be neighbours if they are attached to the same subnetwork. If the two routers are in different autonomous systems, they may wish to exchange routing information.

- BGP performs three functional procedures.
  1. Neighbour acquisition
  2. Neighbour reachability
  3. Network reachability
- Neighbour acquisition procedures used for exchanging the routing information between two routers in different Autonomous Systems (AS). To perform neighbour acquisition, one router sends an open message to another. If the target router accepts the request, it returns a keepalive message in response.
- Once a neighbour relationship is established, the neighbour reachability procedure is used to maintain the relationship. Both sides needs to be assured that the other side still exists and is still engaged in the neighbour relationship. For this purpose, both routers send keepalive messages to each other. Both sides router maintains a database of the subnetworks that it can reach and the perferred route for reaching that subnetwork.
- If the database changes, router issues an update message that is broadcast to all other routers implementing BGP. By the broadcasting of these update message, all the BGP routers can build up and maintain routing information. BGP connections inside an autonomous system are called internal BGP (iBGP) and BGP connections between different autonomous systems are called external BGP (eBGP).

- Fig. Q.13.1 shows the internal and external BGP.

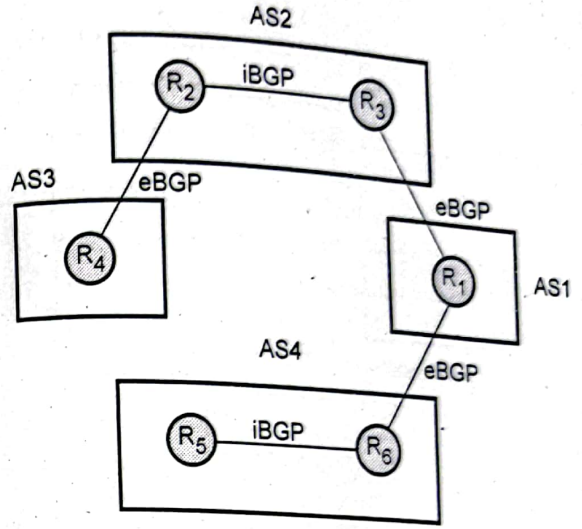


Fig. Q.13.1 Internal and external BGP

BGP messages : Header of the all BGP messages is fixed size that identifies the message type. Fig. Q.13.2 shows the BGP message header format.

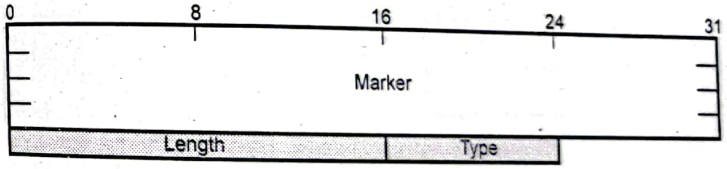


Fig. Q.13.2 BGP header format

1. **Marker :** Marker field is used for authentication. The sender may insert value in this field that would be used as part of an authentication mechanism to enable the recepient to verify the identity of the sender.
2. **Length :** This field indicates the total length of the message in octets, including the BGP header. Value of the length must be between 19 and 4096.

3. **Type :** Type field indicates type of message. BGP defines four message type.

a) OPEN b) UPDATE c) NOTIFICATION d) KEEPALIVE

- Following Fig. Q.13.3 shows the four types of message formats.

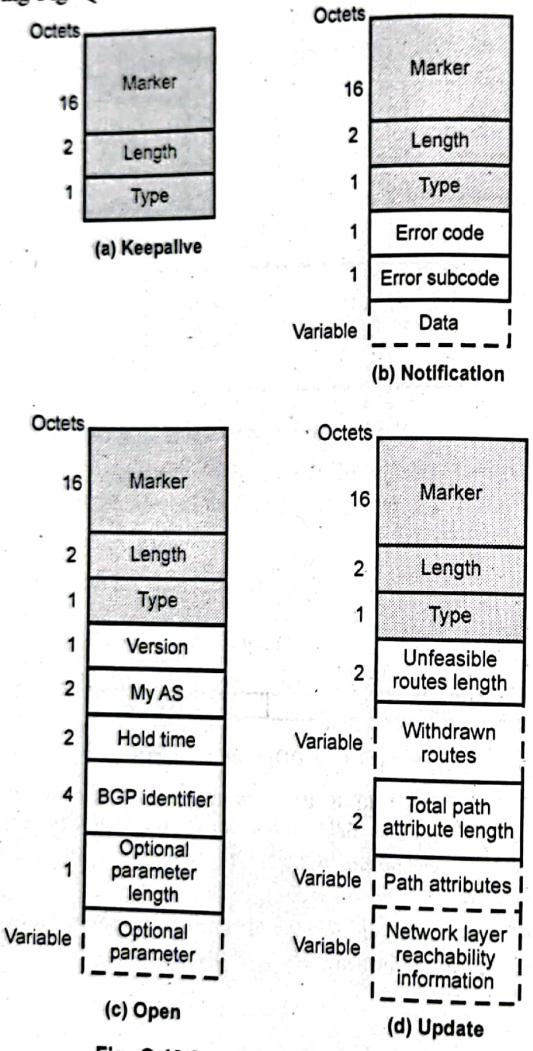


Fig. Q.13.3 BGP message format

- To acquire a neighbour, a router first opens a TCP connection to the neighbour router of interest. It then sends the open message. This message identifies the AS (Autonomous System) to which the sender belongs and provides the IP address of the router. It also includes a Hold time parameter. If the recipient is prepared to open a neighbour relationship, it calculate a value of Hold Timer that is the minimum of its Hold Time in the open message. This calculated value is the maximum number of seconds that may elapse between the receipt of successive keepalive and update message by the sender.
- The KEEPALIVE message is just the BGP header with the type field set to 4. The KEEPALIVE messages are exchanged often enough as to not cause the hold timer to expire. A recommended time between successive KEEPALIVE messages is one-third of the hold time interval. This value ensures that KEEPALIVE messages arrive at the receiving router almost always before the hold timer expires even if the transmission delay of a TCP is variable. If the hold time is zero, then KEEPALIVE messages will not be sent.
- When a BGP router detects an error, the router sends a NOTIFICATION message and then close the TCP connection. After the connection is established, BGP peers exchange routing information by using the UPDATE messages.
- The UPDATE messages may contain three pieces of information. Unfeasible routes, path attributes and network layer reachability information.
- An UPDATE message can advertise a single route and withdraw a list of route. An update message may contain one or both types of information. The UPDATE messages are used to construct a graph of Autonomous System (AS) connectivity. The withdrawn routes field provides a list of IP address prefixes for the routes that need to be withdrawn from BGP routing tables. The unfeasible routes length field indicates the total length of the withdrawn routes field in octates.
- An UPDATE message can withdraw multiple unfeasible routes from service. A BGP router uses Network Layer Reachability Information

(NLRI), the total path attributes length and the path attributes to advertise a route. The NLRI field contains a list of IP address perfixed that can be reached by the route.

Advantages of BGP

1. BGP is a very robust and scalable routing protocol.
2. CIDR is used by BGP to reduce the size of the Internet routing tables.
3. BGP easily solves the count-to-infinity problem.

Disadvantages of BGP

1. BGP is complex.
2. BGP routes to destination networks, rather than to specific hosts or routers.

END...