**UNIT 2 ROUTING PROTOCOLS**

**Q: Define Router. Write down its functions.**

**Router**: "router is a networking device which forwards the data packets between computer networks"

- **Functions**:
- Router performs traffic diverting function on the network
- Determination of the path
- Packet forwarding

**Q: What are the major uses of a router?**

1. Multiple Network Connection
2. Managing Congestion
3. Providing connectivity
4. Connecting Subnets
5. Port Forwarding
6. Traffic Classification

**Q: What are different types of routers?**


1. **Edge Router:**
    - Known as gateway router
    - Specialized router act as intermediatory between networks
    - It resides at the **edge** of the network
    - Edge ensures connectivity of its network with WAN, internet or external network
    - For connectivity with remote networks- Edge uses network protocol- External Border Gateway

2. **Wireless Router:**

- Acts as **router** as well as **wireless access point**
- Provides access to private computer networks or internet
- It can function in LAN, wireless LAN or mixed (wired and wireless) network
- These routers have one or two **USB** ports to connect with device

3. **Virtual Router:**
    - It's a **software-based framework** with same function as physical router
    - Run on commodity servers
    - They are either alone or work with other networks
    - They increase the reliability of the network
4. **Distribution router:**
    - It is a router in LAN of **single organization**
    - Also known as **interior router**
    - It receives data from edge and sends it to end user
    - This is usually done through **wi-fi**
5. **Core Router:**
    - Computer communication device that operates at the core of the internet
    - It links all network devices to provide **multiple fast data communication interfaces**
    - Service or cloud providers use core routers
    - It provides maximum bandwidth to connect additional routers
    - It supports multiple telecommunication interfaces of highest speed

**Q: Explain Routing Architecture in details.**

- **Routing Architecture: "**Design and organization of routers which is responsible for forwarding packets in a network"
- This architecture performs **2 main functions**:
    - Process routable protocols
    - Use routing protocols to determine the best path
- Router has 4 components as shown in the diagram

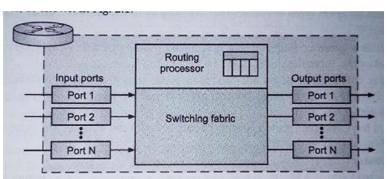
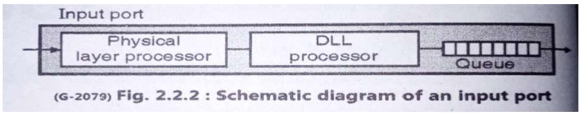


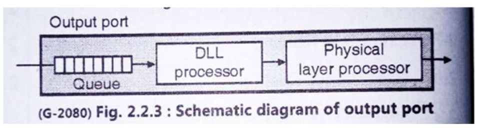
Fig. 2.1: Router Architectural Components

**Input Port:**




- Performs the physical and data link layer functions of the router
- **Functions of inout port**:
  - Constructs **bits** from received signal
  - **Decapsulates** packet from the frame
  - Detects and corrects the **errors**
  - Packet is **ready** to be forwarded
  - Buffer will **hold** the ready to forward packet before directing the to switching fabric

**Output Port:**




- Performs same functions like input port but in **reverse** order
  - The outgoing packets are buffered and queued
  - Packets are encapsulated to create the frames
  - Physical layer function are applied to the frame
  - This will create signal that can be sent on the line

**Routing Processor:**

- Performs function of **network** layer
- Uses destination address to **find** :
  - Output port number from where the packet is to be sent out
  - The address of the next hop
- Routing processor works by accessing routing table
- Activity of routing processor is called as **table lookup**

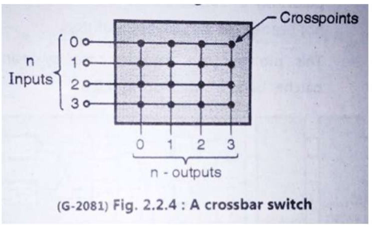
**Switching Fabric in a router:**

- **Connects** the router's input port to output port
- It is a combination of hardware abd software which moves data coming into network node out by correct port to the next node in the network
- Modern days routers use different typer=s of switching fabrics
  - Crossbar switch

- Banyan switch
- Batcher banyan switch

**Q: Explain different Type of switching fabrics**

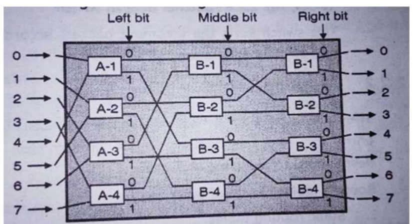
**Crossbar Switch:**



(G-2081) Fig. 2.2.4 : A crossbar switch

- Uses electronic microswitches at each crosspoint and connects n inout to n outputd in a grid using the switches

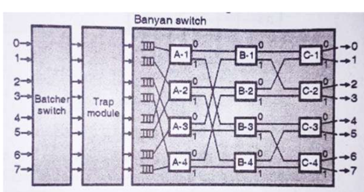
**Banyan Switch:**



(G-145) Fig. 2.2.5 : A three layer switch

- Named after banyan tree
- It's a ultistage switch with microswitches used at every stage
- Fig. shpws 3 layer banyan switch
- n=no. of inputs= no. of outputs= 8
- n/2 = 4 switches at each stage
- no of stages= log base 2 (n)= log base 2(8)=3

**Batcher-banyan switch:**



(G-146) Fig. 2.2.6 : Batcher banyan switch

- banyan switch has problem of collision
- this problem is solved by batcher banyan switch'

- this switch sorts the incoming packets according to their final destination

**Q: Explain the concept of Routing Tables with example and its types.**

**Routing Table:** routing table for host or router consist of an entry for each destination or a combination of destinations to route the IP packet

**Entries in routing table:**

1. Network ID: (destination)
2. Subnet Mask: (destination)
3. Next Hop: (IP address)
4. Outgoing Interface:
5. Metric: (minimum number of hops)

**2 types routing tables :**

1. **Static Routing Table:**
    - Information in tables is entered manually
    - The route of a packet to each destination is entered into the table by the table administrator
    - Routing table cannot update itself automatically
    - Has to be changed manually as and when required
    - Static routing is useful only for small networks
2. **Dynamic Routing Table:**
    - Gets automatically updated by using dynamic routing protocol such as – RIP, OSPF, BGP
    - **Table 2.2.1 : Format of dynamic routing table**

| Mask | Network Address | Next hop address | Interface | Flags | Reference count | Use |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |

**Q: What is Queueing and Switching in routing architecture?**

Crucial components of routing architecture are

1. **Switching:** It determines how packets move through the router
2. **Queueing:** Ensures proper packets scheduling and congestion control

Both are essential for high-speed networks and quality of service.

Manages network traffic

**Queueing** stores packet temporarily Switching determines the path packets take to their destination

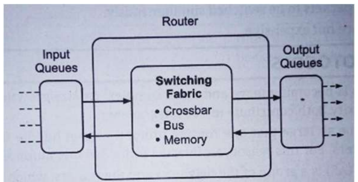


Fig. 2.4: Queuing and Switching in Router Architecture

**Queueing in router:**

- Store packet temporarily when arrival rate exceeds the departure rate –> preventing packet loss due to congestion.
- Store packets in buffer before forwarding them
- Ensure fair packet transmission

**Types of Queueing in router:**

1. **FIFO (First-In-First-out):**
   - simplest form of queuing,
   - Packets are processed in the order they arrive
   - NO priority mechanism → causes delay for important packets
2. **Priority Queue (PQ):**
   - Assign priority levels to packets
   - Higher priority packets are transmitted first
   - Risk: Lower priority packets might starve
3. **WFQ (Weighted Fair Queuing):**
   - Ensure fair distribution of bandwidth among different flows
   - Packets are classified based on traffic type and assigned weights
   - Efficient for multimedia application
4. **Round Robin Queueing:**
   - Each queue gets an equal opportunity to send packet
   - Useful for ensuring fairness in resource allocation.

**Switching in Router:**

- Process of moving packets from input interface to appropriate output interface
- Router follows a switch fabric to interconnect input and output port efficiently

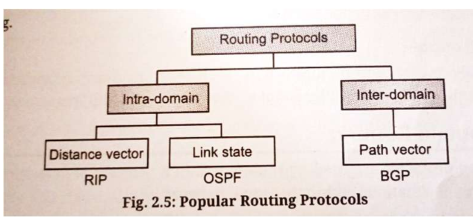
**Types of switching fabrics in router:**

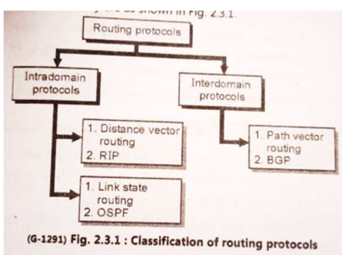
1. **memory-Based Switching:**
    - Router stores incoming packets in memory before forwarding them
    - Works like CPU based application
    - Slow and limited by memory speed
2. **Bus-Based Switching:**
    - Shred bus connects input and output posts
    - Packets wait for their turn
    - Faster than memory switching but suffers from congestion
3. **Crossbar-Based Switching:**
    - Uses a matrix to directly connect input ports to output ports
    - Allows multiple ports to be switched simultaneously
    - High performance but expensive

**Q: What are different types of routing?**

- Router creates its routing tables
- It helps for forwarding data graph in connectionless services
- It helps in creating a virtual circuit in connection-oriented services

**Types of routing**




- Unicast
- Broadcast
- Multicast

We can also classify as:

- Inter domain

- Intra domain

**Q: Differentiate between Intra-Domain Routing and Inter-Domain Routing**

used in exterior routing.

**Difference between Intra-Domain and Inter-Domain Routing:**

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

**Q: Purpose and function of Routing protocols?**

**Purpose:**

- Essential for enabling data packets to travel efficiently and reliably across inter connected networks
- Ensuring packets – they reach their intended destination through the most optimal path

**Function**:

- To determine how routers communicate with each other
- How they share information about network topology, allowing router to dynamically adopt to changes like link failure or network congestion

**Q: Define Intra domain routing**

- Routing inside an autonomous system is known as Intra Domain Routing
- Used by routers within a network to determine the best path for forwarding packets to destination
- Routing algorithm is used to determine mathematically the best path
- Examples of intra domain routing protocols:
    - Distance Vector Routing
    - Link State Routing

- Routing Information Protocol- an implementation of distance vector routing
- OSPF is an implementation of link state protocol

**Q: Define Inter Domain Routing**

- Routing between autonomous system is known as Inter Domain Routing
- Inter-domain routing directs network traffic between different autonomous systems on the internet
- Example of inter domain routing protocol is Path Vector Routing
- Each autonomous system is allowed to choose one or more intra domain routing protocols in order to handle routing inside A.S.
- But only inter domain routing protocol will handle routing between autonomous systems
- BGP is an implementation of path vector protocol

**Q: Define routing algorithm**

- Routing algorithm is a part of network layer software
- It is responsible for deciding the output line over which a packet is to sent
- Desirable Properties of routing algorithm:
    - Correctness
    - Robustness
    - Stability
    - Fairness
    - Optimality

**Q: Explain types of routing algorithms.**

**2 types**

1) **Static Routing (Non-Adaptive)**

- Routing decision is not based on the measurement or estimation of current traffic and topology
- All the possible paths which are already calculated are loaded into the routing table
- Choice of route is done in advance, offline and it is downloaded to the routers
- Suitable for small networks
- **Disadvantage:** inability to respond quickly in case of network failure

2) **Dynamic Routing (Adaptive)**

- Modern computer networks use dynamic routing algorithms
- Suitable for packet switched networks

- Algorithm assume that packet knows the address of each neighbouring router and coast of reaching each neighbour
- Algorithms are of distributed type- so suitable for large internetworks
- Algorithm can change their decision based on changes in topology
- Each router can check network status by communicating with neighbours
- Changes are reflected to all routers
- Router can calculate suitable path for destination
- **Disadvantage:** complexity in router

**Q:Differentitate between Static Routing and Dynamic Routing**

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

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

5. Explain any three Intra-domain routing protocols.

**Table 2.7.2 : Comparison of static and dynamic routing**

| Sr. No. | Parameter | Static routing | Dynamic routing |
|---|---|---|---|
| 1. | Updating of the routing tables | Manually done | Automatically done |
| 2. | Bandwidth requirement | Less | More |
| 3. | Application area | In small networks | In large networks |
| 4. | Routing protocols | None | EIGRP, ARP etc. |
| 5. | Security | Highly secure | Less secure |
| 6. | Routing algorithms | Shortest path, flooding, flow based routing | Distance vector, link state |
| 7. | Link failure | Any link failure affects the other routing paths | Does not affect other routing paths |
| 8. | Additional resources | Not required | Required to store information |

| Sr. No. | Parameter | Static routing | Dynamic routing |
|---|---|---|---|
| 9. | Routing decision | Not based on the measured or estimated current traffic | Is based on the changes in topology or traffic |
| 10. | Configuration | Difficult to configure | Easy to configure |
| 11. | Security | Highly secure | Less secure |
| 12. | Routing protocols | None | EIGRP, ARP etc. |
| 13. | Cost | Less | More |

**Q: What is Distance Vector Routing?**

- The least-cost route between any two nodes →the route with minimum distance.
- each node maintains a vector (table) of minimum distances to every node.
- The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).

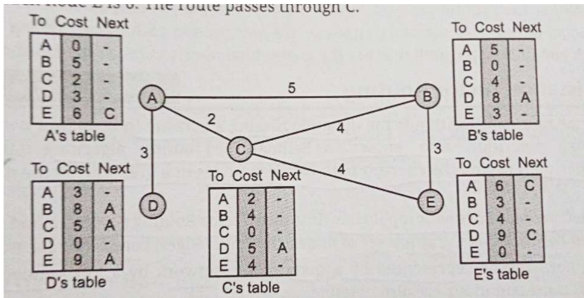



Fig. 2.7: Distance Vector Routing Tables

- The table for node A shows how we can reach any node from this node.
- For example, our least cost to reach node E is 6.
- The route passes through C.
- ***Initialization***
- The tables are stable
- each node knows how to reach any other node and the cost.
- At the beginning→Each node can know only the distance between itself and its neighbours (directly connected)

- each node can send a message to the immediate neighbours and find the distance between itself and these neighbours.
- The distance for any entry that is not a neighbour is marked as **infinite** (unreachable).

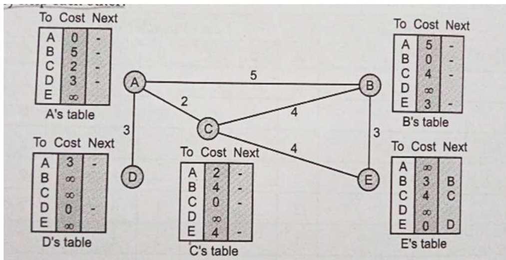



Fig. 2.8 (a): Initialization of Tables in Distance Vector Routing (DVR)

- ***Sharing***
- sharing of information between neighbours.
- node A does not know about node E, node C does.
- if C shares its routing table with A→ node A can also know how to reach node E.
- node C does not know how to reach node D, but node A does.
- A shares its routing table with node C→node C also knows how to reach node D.
- A and C – neighbours→ can **improve** their routing tables if they **help** each other.
- each node → sends its entire table to neighbour →neighbour decides what part to use and what part to discard.
- third column (next stop) →not useful to neighbour.
- this column → replaced with the **sender's** name.
- If any row can be used - the next node is the sender of the table.
- node can send - only first two columns
- each node shares its routing table with its immediate neighbours **periodically** and when there is a **change**.
- ***Updating***
- node receives →two-column table from neighbour →updates its routing table.
- Three steps:

1. receiving node adds the cost between itself and the sending node to each value in the second column.
   If node C claims that its distance to a destination is *x* mi and distance between A and C is *y* mi→ then distance between A and destination (via C) is *x* + *y* mi.
2. receiving node adds the name of the sending node to each row as the third column if the receiving node uses information from any row→The sending node is the next node in the route.

3. receiving node compares each row of its old table with the corresponding row of modified version of the received table.
    a. If the next-node entry is different→ chooses the row with the smaller cost.
    b. If there is a tie, the old one is kept.
    c. If the next-node entry is the same, the receiving node chooses the new row. **example**, suppose node C has previously advertised a route to node X with distance 3 → now there is no path between C and X →node C now advertises this route with a distance of infinity. Node A must not ignore this value even though its old entry is smaller. The old route does not exist any more. The new route has a distance of infinity.

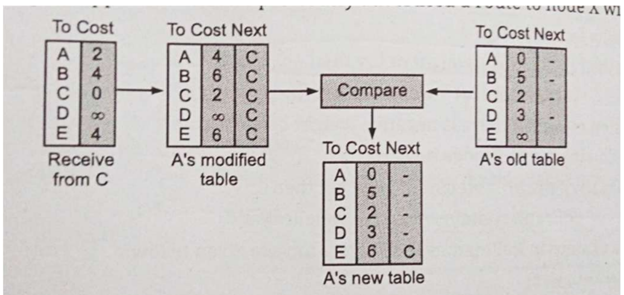
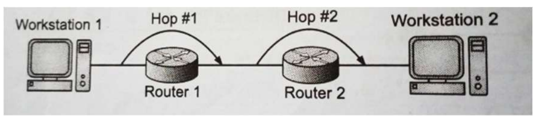


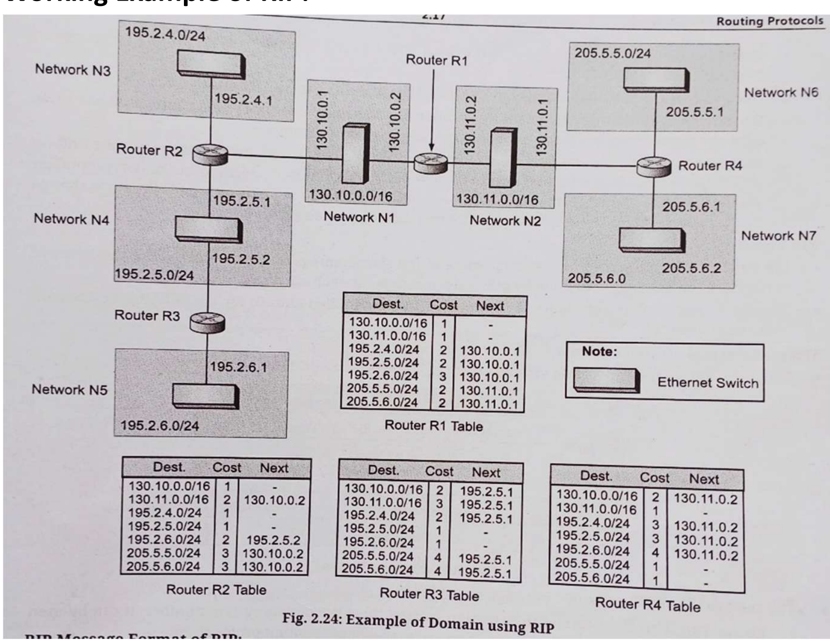
Fig. 2.8 (b): Updating Distance Vector Routing

- when we add any number to infinity, the result is still infinity.
- The modified table shows how to reach A from A via C.
- If A needs to reach itself via C, it needs to go to C and come back, a distance of 4.
- the only benefit from this updating of node A is the last entry, how to reach E. it knows that the cost is 6 via C.
- Each node can update its table by using the tables received from other nodes.
- if there is no change in the network - each node reaches a stable condition in which the contents of its table remain the same.

**Q: Explain Routing Information Protocol (RIPv2) working**

- Intra domain routing protocol
- Used inside autonomous system
- One routing protocol cant handle table updating over internet
- **RIP** → is distance vector protocol→uses Bellman Ford algorithm→ for calculating routing tables
- **RIP uses port 520**
- It's a dynamic routing protocol

- Routing metric→ hop count
- **HOP COUNT:**
  - Hop→ portion of a path
  - Data packet passes through → bridges, routers and gateways → to reach the destination
  - Passing through a device → HOP occurs
  - Hop→ no. of routers occurring on the way (source to destination)
  - Lowest hop count→ best route→places in routing table
  - RIP→ prevents routing loops→ by limiting no. of hops
  - max. Hop count→ 15 :: 16→ network unreachable
  - " hop count means number of intermediate devices through which data must pass between source and destination"
  - 

- **Features of RIP:**
  - Updates of network are exchanged periodically
  - Updates are always broadcasted
  - Full routing tables are sent in updates
  - Router always trusts on routing information received from neighbours→ known as routing on rumours
- **Working Example of RIP:**
- 


| Dest. | Cost | Next |
|---|---|---|
| 130.10.0.0/16 | 1 | - |
| 130.11.0.0/16 | 1 | - |
| 195.2.4.0/24 | 2 | 130.10.0.1 |
| 195.2.5.0/24 | 2 | 130.10.0.1 |
| 195.2.6.0/24 | 3 | 130.10.0.1 |
| 205.5.5.0/24 | 2 | 130.11.0.1 |
| 205.5.6.0/24 | 2 | 130.11.0.1 |

Router R1 Table

| Dest. | Cost | Next |
|---|---|---|
| 130.10.0.0/16 | 1 | - |
| 130.11.0.0/16 | 2 | 130.10.0.2 |
| 195.2.4.0/24 | 1 | - |
| 195.2.5.0/24 | 1 | - |
| 195.2.6.0/24 | 2 | 195.2.5.2 |
| 205.5.5.0/24 | 3 | 130.10.0.2 |
| 205.5.6.0/24 | 3 | 130.10.0.2 |

Router R2 Table

| Dest. | Cost | Next |
|---|---|---|
| 130.10.0.0/16 | 2 | 195.2.5.1 |
| 130.11.0.0/16 | 3 | 195.2.5.1 |
| 195.2.4.0/24 | 2 | 195.2.5.1 |
| 195.2.5.0/24 | 1 | - |
| 195.2.6.0/24 | 1 | - |
| 205.5.5.0/24 | 4 | 195.2.5.1 |
| 205.5.6.0/24 | 4 | 195.2.5.1 |

Router R3 Table

| Dest. | Cost | Next |
|---|---|---|
| 130.10.0.0/16 | 2 | 130.11.0.2 |
| 130.11.0.0/16 | 1 | - |
| 195.2.4.0/24 | 3 | 130.11.0.2 |
| 195.2.5.0/24 | 3 | 130.11.0.2 |
| 195.2.6.0/24 | 4 | 130.11.0.2 |
| 205.5.5.0/24 | 1 | - |
| 205.5.6.0/24 | 1 | - |

Router R4 Table

Fig. 2.24: Example of Domain using RIP

- AS with -7 networks and 4 routers
- Routing table of R1 – 7 entries – to reach each network in AS
- R1 is directly connected to 130.10.0.0 and 130.11.0.0→ no next hop for this entry
- For reaching N3, N4 and N5 → packet has to pass through R2
- So next node entry is of 130.10.0.1
- For sending packet to N6 and N7 – it has to pass through R4 – with IP 130.11.0.1

**Q: draw and explain RIP Message Format:**

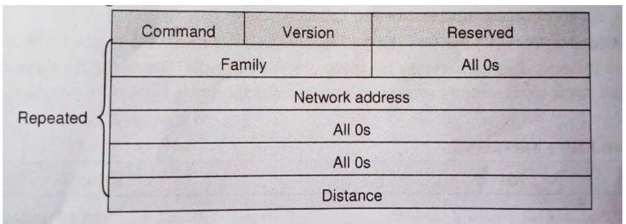
- 

Fig. 2.25: RIP Message Format
- **Command:**
  - 8-bit field
  - Specifies type of message
  - Request -1
  - Response - 2
- **Version:**
  - 8-bit field
  - Defines version
- **Family:**
  - 16-bit field
  - Defines family of the protocol
  - For TCP/IP value is 2
- **Network Address:**
  - Defines address of destination network
  - 14 bytes allocated to this filed
  - Applicable to any protocol
  - IP currently uses 4 bytes
  - Rest of the address is filled with 0's
- **Distance:**
  - 22-bit field
  - Defines hop count(cost)
  - From advertising router to destination router
- 2 types of messages

- **Request:**
  - sent by → router that just has come up or sent only in answer to a request
  - request can ask about specific entries or all entries
- **Response:**
  - Response can be→ solicited or unsolicited
  - Solicited response → sent only in answer toa request
  - Contains information about destination specified in corresponding request
  - Unsolicited Response→ sent periodically→ every 20 seconds→ when there is a change in routing table
  - Response is sometimes called→ update packet

**Q: Draw and explain RIP version 2**

**Features:**

- **Authentication by simple text password**
- **Subnet masking used**
- **Multicasting is used to allow for variable length subnet mask to be implemented**
- **Route tag to provide a method of separating RIP routes from externally learned routers**

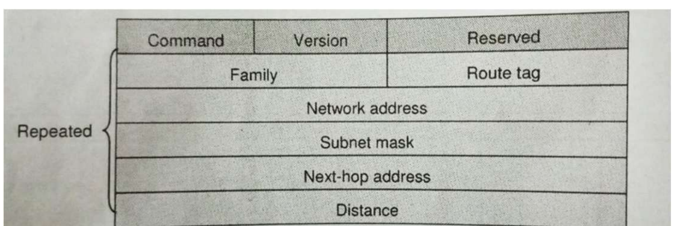


Fig. 2.26: RIP Version 2 Format

- **Route Tag:**
  - Carries information like autonomous system number
  - Can be used to enable RIP to receive information from – inter domain routing protocol
- **Subnet Mask:**
  - 4 byte field
  - Carries subnet mask or prefix
  - This means RIP 2 supports classless addressing or CIDR
- **Next-Hop Address:**

- Shows address of next hop
- Useful if AS share a network
- Message can define router in same AS or another AS → to which the packet next goes.

**Q: What are the drawbacks of RIP?**

1. **Width restriction:**
   - For RIP infinity is defined as 16 → corresponds to 15 hops
2. **No direct subnet support:**
3. **Bandwidth consumptive:**
   - Router broadcasts list of networks and subnets after every 30 seconds→ consumes large amount of bandwidth.
4. **Difficult to diagnose fault:**
5. **Weak security:**
   - Does not have any security feature on its own
6. **Looping problem:**
   - RIP faces routing loop problem

**Q: Differentiate between RIPv1 and RIPv2**

**Difference between RIPv1 and RIPv2:**

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

**Q: Explain 'Link State Routing-Open Shortest Path'**

- Each router shares knowledge of neighbourhood with every other router in the inter network
- If each node in a domain has entire topology of the domain, list of nodes handling
- They are connected including the type, cost, and condition of link (up or down)
- Node can use Dijkstra's algorithm to build routing table.

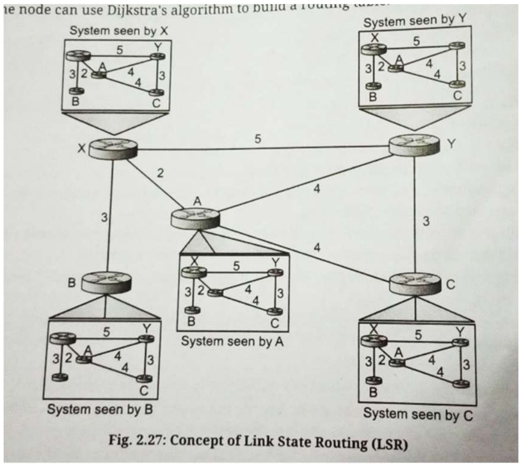


Fig. 2.27: Concept of Link State Routing (LSR)

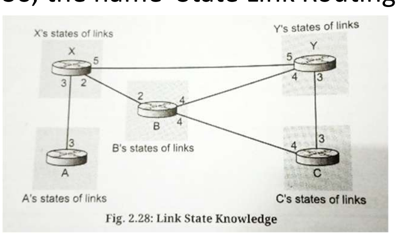
- Link state routing protocol - creates topological map of networks
- Each router has this map to determine shortest path
- Routing protocol sends information about the state of it's links to other router in the routing domain
- Stat of those links refer to → directly connected networks,
- Includes information about type of network and neighbouring routers
- So, the name 'State Link Routing Protocol' is given.
- 

Fig. 2.28: Link State Knowledge
- Fig shows – simple domain with 5 nodes
- Each node uses same topology to create a routing table
- Routing table for each node is unique
- Analogous to city map
- **Building routing Table:**

- 4 sets of actions are required – to ensure each node has routing table -with least cost node to every other node
- Creation of states of the links by each node – called as link state packet (LSP)
- Dissemination of LSP to every other router → called flooding
- It is an efficient and reliable way
- Formation of shortest path tree for each node
- Calculating routing table based on shortest path tree

**Formation of shortest path tree: Dijkstra Algorithm**

- Tree→ graph of nodes and links
- One root node
- Other nodes can be reached from root node
- Shortest path- is a tree in which the path between root and every node is shortest
- **Algorithm uses following steps:**
- **Initialization:**
    - Select the root node of the tree
    - Add it to the path
    - Set shortest distances for all root's neighbours to the cost between root and those neighbours
    - Set the shortest of the root to zero
- **Iteration:** repeat following steps until all nodes are added to the path
    - **Adding the next node to the path:** search the node not in the path→select the one with minimum shortest distance and add it to the path
    - **Updating:** updating the shortest distance for all remaining nodes using the shortest distance of the node just moved to the path in step 2
    - Dj = minimum (Dj, Di + cij) for all remaining nodes

**Dijkstra Algorithm:**

```
Dijkstra ( )
{
// Initialization
```

```
Path = {s}                  // s means self
for (i = 1 to N)
{
if(i is a neighbor of s and I≠ s)    Di= csi
if (i is not a neighbor of s)        Di=∞
}
Ds = 0
} // Dijkstra
// Iteration
Repeat
{
// Finding the next node to be added
Path = Path ∪ i if Di is minimum among all remaining nodes
// Update the shortest distance for the rest
for (j = 1 to M)              // M number of remaining nodes
{
Dj = minimum (Dj , Dj + cij)
}
} until (all nodes included in the path, M = 0)
```

- **Q: Differentiate between Distance Vector Routing and Linked State Routing**

**Difference between Distance Vector Routing and Link State Routing:**

| Sr. No. | Distance Vector Routing | Link State Routing |
|---|---|---|
| 1. | The distance vector routing determines the direction (vector) and distance (such as link cost or number of hops) to any link in the network. | The link state routing uses the Shortest Path First (SPF) algorithm to create an abstract of the exact topology of the entire network. |
| 2. | Distance vector routing protocols do not have an actual map of the network topology. | A link state routing protocol is like having a complete map of the network topology. |
| 3. | The distance vector routing algorithm is a type of routing algorithm that is based on the number of hops in a route between a source and destination computer. | The link state routing algorithm broadcasts information about the cost of reaching each of its neighbors to all other routers in the network. |
| 4. | Uses Bellman-Ford algorithm. | Uses Dijkstra's algorithm. |
| 5. | The name 'distance vector' is used because the routers exchange vectors containing distance and direction information. | In link state routing, each routing node makes a connectivity graph for the nodes in the network and independently calculates its shortest path to every other destination in the network. |
| 6. | Less bandwidth is required. | High bandwidth is required. |
| 7. | Distance vector routing updates full routing table. | Link state routing updates only the link state. |
| 8. | Example of distance vector routing protocols is RIP. | Example of link state routing protocols is OSPF. |
| 9. | The utilization of CPU and memory in distance vector routing is lower than the link state routing. | Higher utilization of CPU and memory. |
| 10. | Distance vector routing does not have any hierarchical design. | Link state routing works best for hierarchical routing design and in networks where fast convergence is crucial. |

Contd...

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

**Examples:**

**Example 1:** Fig. 2.29 shows the formation of the shortest path tree for the graph of seven nodes.

In the initialization step, node A selects itself as the root. It then assigns shortest path distances to each node on the topology. The nodes that are not neighbors of A receive a shortest path distance value of infinity

tree found in above Fig. 2.29.

| Destination | Cost | Next Router |
|---|---|---|
| A | 0 | – |
| B | 2 | – |
| C | 7 | B |
| D | 2 | – |
| E | 6 | B |
| F | 8 | B |
| G | 9 | B |

**Fig. 2.29: Routing Table for Node A**

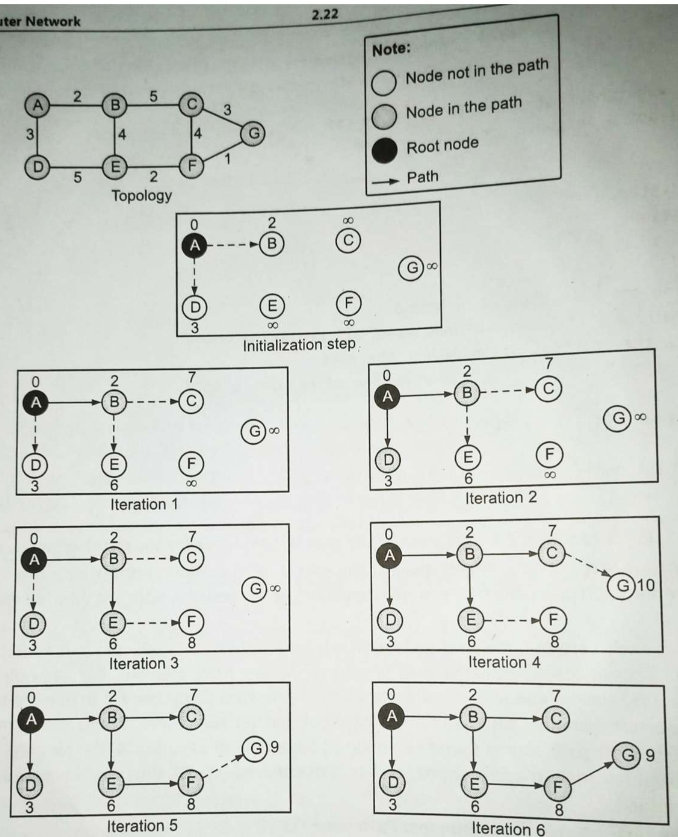



Fig. 2.30

**Example 2:** Consider Fig. 2.31. Find the shortest path.

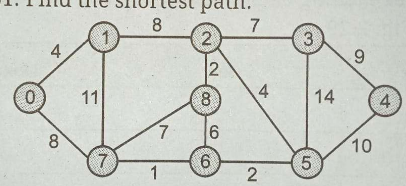


Fig. 2.31

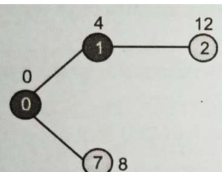


Fig. 2.33

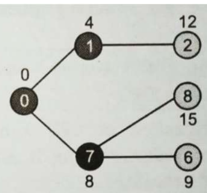


Fig. 2.34

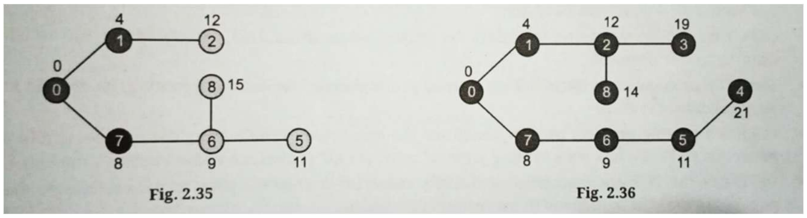


Fig. 2.35 Fig. 2.36

**Q: What is OSPF?**

- **OSPF:** Open Shortest Path First
- An Alternative to RIP
- It's an interior routing protocol
- Overcome limitations of RIP
- Uses link state routing for updating routing tables
- OSPF is an intradomain protocol
- Its domain is an autonomous system

**Area:**

- OSPF divide as AS into areas
- Network, hosts and routers are collectively called as Area
  AS is made of various arias
- All network inside an area should be connected.

**Area Border Router:**

- Special types of routers used at boarder of an area
- Summarizes information about area
- Sends it to other areas

**Backbone**

- special area inside AS called backbone
- All area inside AS should be connected to backbone
- Backbone is a primary area
- Other areas are called as secondary areas

**Backbone routers**

- Routers inside backbone area are called as backbone routers
- Backbone router can also work as area border router

- If connectivity between backbone and area is broken→ administration should create a virtual link

**Area Identification**

- Each area has area identification
- For backbone it is equal to zero

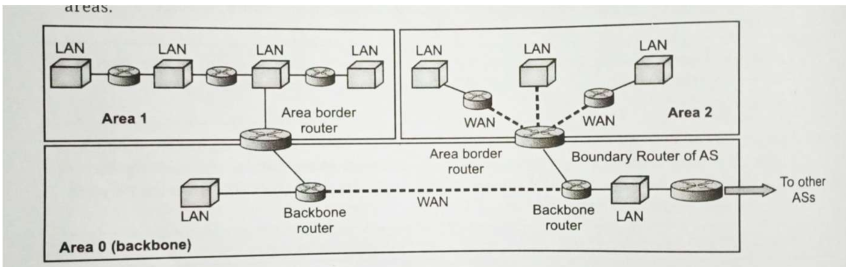


Fig. 2.37

**Q: Explain Types of links in OSPF**

- Link → connection

1. **Point to point link**
   - Connects 2 router without any host or router in between
   - Do not need IP address at each end
   - Un numbered inks can save IP addresses

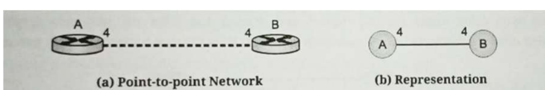


Fig. 2.38: Point-to-point links

2. **Transient link**
   - It’s a network with several routers attached to it.
   - Data can enter and leave through any router.
   - All LANs and some WANs with 2 or more routers are of this type.

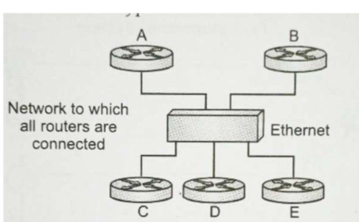


Fig. 2.39: Transient Link

3. **Stub link**

- It's a network that is connected to only one router
- Data packets enter and leave through same router

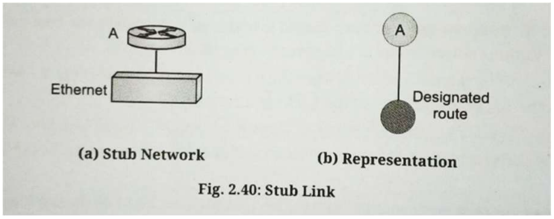


Fig. 2.40: Stub Link

**4. Virtual link**

- When link between 2 routers is broken → administration create virtual link
- Virtual link may use longer path that goes through several routers

**Graphical representation:**

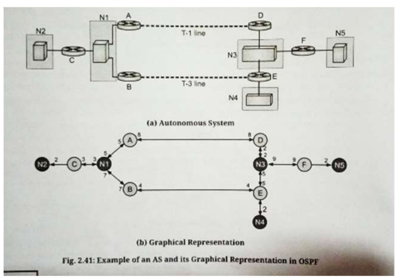
- 

Fig. 2.41: Example of an AS and its Graphical Representation in OSPF
    - Figure shows AS with 7 networks and 6 routers
    - Both networks are point to point
    - Symbols N1 & N2 – used for transient and sub networks
    - No need to assign identity to point to point network
    - Colour nodes are used for routers
    - Shaded nodes are used for network
    - OSPF sees both has nodes
    - Figure has 3 stub networks

**Q: what are different types of OSPF packets?**

- **There are 5 different types of packets**

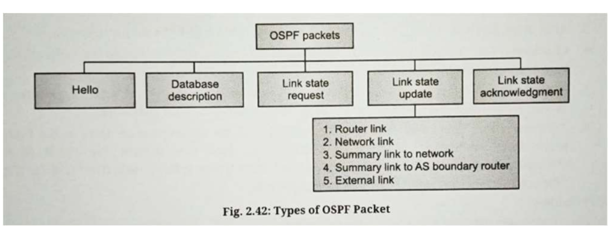


Fig. 2.42: Types of OSPF Packet

1. **Hello:** establishes and maintains neighbour relationship
2. **Database description:** describes content of topological database → exchanged at initialization
3. **Link State Request:** exchanged after router discovers→ that parts of its topological database are out of date
4. **Link State Update:** responds to link state request packet→also used for regular dispersal of Link State Acknowledgement (LSA)→several LSA in single packet
5. **Link State Acknowledgement:** acknowledges link state update packet

**Q: Draw and explain OSPF common header format.**

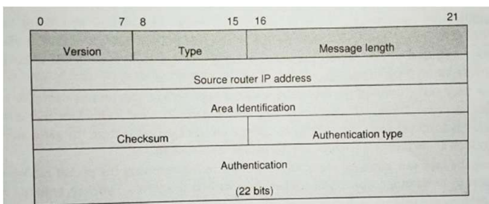



Fig. 2.43: OSPF Common Header

1. **Version:**
- 8-bits field
- Defines version of OSPF
- Currently 2
2. **Type:**
- 8-bit field
- Defines type of packet
- 5 types (values 1 to 5)
3. **Message Length:**
- 16-bit field
- Defines length of total message including header
4. **Source Router IP Address:**
- 22-bits filed
- Defines IP address of router that sends the packet
5. **Area Identification:**
- 22-bits field
- Defines area within which routing takes place
6. **Checksum:**
- Used for error detection → on entire packet excluding- authentication type and authentication data field
7. **Authentication Type:**

- 16-bits field
- Defines authentication protocol used int this area
- 0 – none, 1 - password

8. **Authentication:**

- 64 bits field
- Actual value of authentication data
- 0 for authentication type 0
- 1 for 8 characters password

**Q: what are the advantages and disadvantages of OSPF?**

- **Advantages:**
- Open standard- not related to any vender
- Area 0 is at the top of the hierarchy
- Uses link state algorithm→ diameter is larger than RIP
- Supports VLSM (variable length subnet mask)
- Uses multicasting within areas
- Sends only those tables which have changed
- Conserves bandwidth
- Decreased size of routing tables
- **Disadvantages:**
- It is processor intensive
- Maintains multiple copies of routing information
- Increased amount of memory needed
- More complex to implement than RIP

**Q: Differentiate between RIPv1, RIPv2, and OSPF**

**Table 2.12.1 : Comparison between RIP and OSPF**

| Sr. No. | Function/Feature | RIPv1 | RIPv2 | OSPF |
|---|---|---|---|---|
| 1. | Standard number | RFC 1058 | RFC 1723 | RFC 2178 |
| 2. | Link-state protocol | No | No | Yes |
| 3. | Large range of metrics | Hop count (16=Infinity) | Hop count (16=Infinity) | Yes, based on 1-65535 |
| 4. | Update policy | Route table every 30 seconds | Route table every 30 seconds | Link-state changes, or every 30 [minutes] |
| 5. | Update address | Broadcast | Broadcast, multicast | Multicast |
| 6. | Dead interval | 300 seconds total | 300 seconds total | 300 seconds total, but usually much less |
| 7. | Supports authentication | No | Yes | Yes |
| 8. | Convergence time | Variable (based on number of routers X dead interval) | Variable (based on number of routers X dead interval) | Media delay + dead interval |
| 9. | Variable-length subnets | No | Yes | Yes |
| 10 | Supports supernetting | No | Yes | Yes |
| 11 | Type of Service (TOS) | No | No | Yes |
| 12 | Multipath routing | No | No | Yes |
| 13 | Network diameter | 15 hops | 15 hops | 65535 possible |
| 14 | Easy to use | Yes | Yes | No |

**Q: Define Inter domain Routing**

- Routing between autonomous systems

- Directs network traffic between different AS on the internet
- Distributes routing information between domains
- E.g. path vector routing, BGP

**Q: Explain Path Vector Routing**

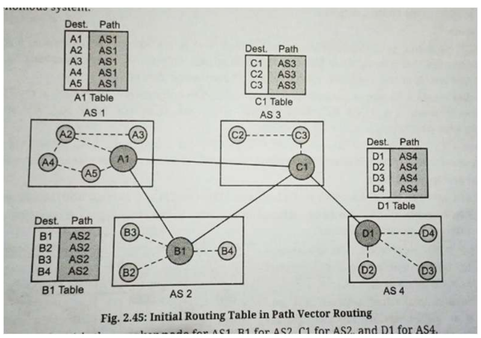
- Exchanges→ information about existence of destination network and path on how to reach the destination
- Path information → used to find best path
- Prevents routing loops
- Widely used path vector protocol is→ BGP
- Used for inter domain routing
- Low computational overhead
- Supports heterogeneous policies and is secure
- Assumes – one node for each AS
- **Initialization:**
- Begins with the knowledge of internal nodes
- 

Fig. 2.45: Initial Routing Table in Path Vector Routing
- A1 -speaker of AS1
- B1 – speaker of AS2
- C1 – speaker of AS3
- D1- speaker of AS4
- Initial tables show list of all nodes and their location as respective AS
- **Disadvantages:**
  - **lack of congestion control:** as it supports heterogeneous systems
  - **complex:** complex to configure
  - **load balancing:** multiple paths for packets are not selected for load balancing
  - **inefficient load balancing:** alternative path is selected only on failure of existing path

**Q: Explain in details Border Gateway Protocol (BGPv4)**

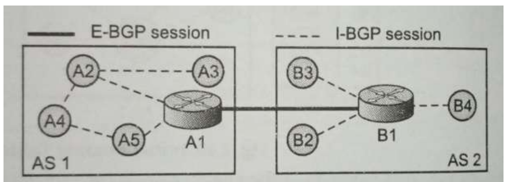
- exterior gateway protocol
- communicates between routers and different AS
- based on path vector routing
- current version- 4
- **BGP Session:**
- Exchange of routing information between routers takes place in a session
- It's a connection between 2 routers for information exchange
- BGP uses services of TCP
- When TCP connection is created for BGP → it can last for long time
- Until something unusual happens
- Called as – semi-permanent connection
- **External and Internal BGP:**
- 

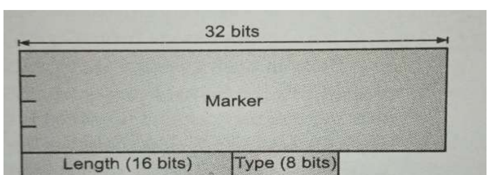
Fig. 2.46: Internal and External BGP Sessions
- E-BGP session- used to exchange information between 2 speaker nodes from 2 different AS
- I-BGP session – used to exchange information between 2 routers inside an AS
- Session between AS1 and AS2 is E-BGP session
- When routers collect information about other routers within same AS is I-BGP
- **BGP Packet Format:**
- 

Fig. 2.47: BGP Packet Header
- All BGP packets share same header
- Message format – 32 bits long
- 5 types of messaging functions -used for message encoding
- Establish, maintain, update- relationship with neighbour
- Notify- formatting errors
- Fields:

1. **Type:**

- 8-bits long

- States- type of packet and type of information contained by packet
- 5 types of message code
- Defined by → Internet Engineering Task Force
- 1- open
- 2- update
- 3- notification
- 4- keepalive
- 5- Route-Refresh (defined only in RFC2918) (Request For Comment)
- 1-4 defined in RFC 1771

2. **Length:**

- 2 byte long
- Min value 19 bits
- Max value 4096 bytes

3. **Marker:**

- Used for authentication of BGP
- If no authentication information → all bits set to 1's
- If message→ its an open message

**Types of BGP**

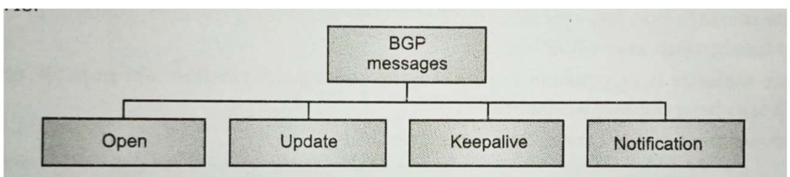


Fig. 2.48: Types of BGP Messages

**Error Codes in BGP**

Error Codes:

| Error Code | Error Code Description | Error Subcode Description |
|---|---|---|
| 1. | Message header error | Three different sub codes are defined for this type of error: synchronization problem (1), bad message length (2), and bad message type (2). |
| 2. | Open message error | Six different sub codes are defined for this type of error: unsupported version number (1), bad peer AS (2), bad BGP identifier (2), unsupported optional parameter (4), authentication failure (5), and unacceptable hold time (6). |
| 3. | Update message error | Eleven different sub codes are defined for this type of error: malformed attribute list (1), unrecognized well-known attribute (2), missing well-known attribute (2), attribute flag error (4), attribute length error (5), invalid origin attribute (6), AS routing loop (7), invalid next hop attribute (8), optional attribute error (9), invalid network field (10), malformed AS_PATH (11). |
| 4. | Hold timer | No sub code defined. |
| 5. | Finite state | This defines the procedural error. No sub code defined. |
| 6. | Cease | No sub code defined. |

**Q: what is Internet Control Message Protocol (ICMP)**

- Simplest protocol in TCP/IP suite
- Used for reporting errors and management queries
- Communication is considered smooth until no one reports problem
- If middleman reports mistake→ ICMP helps to notify sender(feedback)
- Communication can be adjusted or rerouted to keep everything running smoothly

**Types of messages**

amp Request and Time stamp Reply.

ICMP Messages

Error-reporting

| Type | Message |
|---|---|
| 3 | Destination unreachable |
| 4 | Source quench |
| 11 | Time exceeded |
| 12 | Parameter problem |
| 5 | Redirection |

Query

| Type | Message |
|---|---|
| 8/0 | Echo (request/reply) |
| 13/14 | Timestamp (req/rep.) |
| 18/18 | Address mask (req/rep.) |
| 10/9 | Router solicitation/advertisement |

**Types of ICMP Messages:**

| Category | Type | Message Name | Description |
|---|---|---|---|
| Error-Reporting Messages | 3 | Destination Unreachable | Indicates that a datagram could not be delivered to its destination. The Code value provides more information on the nature of the error. |
| | 4 | Source Quench | Lets a congested IP device tell a device that is sending it datagrams to slow down the rate at which it is sending them. |
| | 11 | Time Exceeded | Sent when a datagram has been discarded prior to delivery due to expiration of its Time to Live field. |
| | 12 | Parameter Problem | Indicates a miscellaneous problem (specified by the Code value) in delivering a datagram. |
| | 5 | Redirect | Allows a router to inform a host of a better route to use for sending datagrams. |
| | 0 | Echo Reply | Sent in reply to an Echo (Request) message; used for testing connectivity. |
| | 8 | Echo Request | Sent by a device to test connectivity to another device on the internetwork. The word Request sometimes appears in the message name. |

Advance Computer Network 2.38

| | | | |
|---|---|---|---|
| | 13 | Timestamp Request | Sent by a device to request that another send it a timestamp value for propagation time calculation and clock synchronization. The word Request sometimes appears in the message name. |
| Query Message | 14 | Timestamp Reply | Sent in response to a Timestamp (Request) to provide time calculation and clock synchronization information. |
| | 17 | Address Mask Request | Used to request that a device send a subnet mask. |
| | 18 | Address Mask Reply | Contains a subnet mask sent in reply to an Address Mask Request. |
| | 9 | Router Advertisement | Used by routers to tell hosts of their existence and capabilities. |
| | 10 | Router Solicitation | Used by hosts to prompt any listening routers to send a Router Advertisement. |

**Message packet format**

| Type (8 bit) | Code (8 bit) | CheckSum (16 bit) |
|---|---|---|
| Extended Header (32 bit) | | |
| Data/Payload (Variable Length) | | |

**Fig. 2.53: ICMPv4 Packet Format**

- **First 32 bits contain 3 fields**
- **Type:**
- 8-bit
    - Type 0 – Echo Reply
    - Type 3 – Destination Unreachable
    - Type 5 – Redirect Message
    - Type 8 – Echo Request
    - Type 11 – Time Exceeded
    - Type 12 – Parameter Problem
- **Code:**
- 8-bits
- Carries additional information about error message and type

- **Checksum:**
- Last 16 bits
- Used to check number of bits of complete message
- Enables ICMP tool to ensure that complete data is received
- **Extended Header:**
- 32 bits
- Points out problem in IP message
- Byte's location is identified by pointers which causes the problem message
- Receiving device looks here for pointing to a problem
- **Data or Payload:**
- Variable length field

**Error reporting messages**

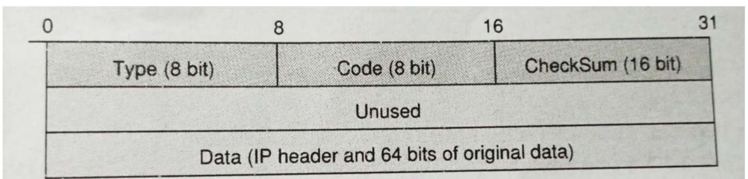



**Fig. 2.54: ICMP Basic Error Message Format**

- **Type:**
- Identifies type of the message
- **Code:**
- Describes purpose of the message
- **Checksum:**
- Used to validate ICMP message
- **Unused:**
- Reserved for future use
- Set to 0
- **Data:**
- Includes IP header of datagram
- Also contains first 8 bytes of data
- Used by sender to get more details about error that has occurred