CHAPTER 3

3. Routing

Objectives

- To understand about routing and its types.
- To know about global internet IPv6.
- To explain about unicast routing – RIP, OSPF, BGP.
- To explain about multicast routing – MOSPF, DVMRP, RPF, RPB, RPM, CBT, PIM.

3. Routing

The means of creating routing tables to support forwarding is referred to as routing and forwarding a packet means, it is supplied to station of its destiny. These protocols constantly update the tables which holds the routing information for forwarding and routing consulted.

Routing Table

A host or path for every destined station, even it might be a mixture of destination to path IP packets constitutes routing table. The routing table might be static otherwise it might be dynamic.

Static Routing Table

Here, the details are entered manually. For each destination, the manager marks the route in the table. If any table is built, it cannot be changed automatically when the internet change. Administration has to manually alter the table.

Dynamic Routing Protocols

These protocols use a table that is updated occasionally by protocols such as RIP, OSPF or BGP. The tables of the routers are updated automatically by dynamic routing protocols when there is a shift in the Internet, such router shutdown or the infringement of connection.

3.1. Unicast Routing Protocols

- A routing table can be made static or dynamic.
- A static table holds manual entries.
- A dynamic table holds information that is routinely changed anywhere on the internet if there is a change.
- Routing protocols are developed based on the response to the demand for expressing dynamism.
- The routing protocol combines the rules and procedures which allow routers to inform each other on the Internet.

Optimization

In general, a packet is received at the router from the network and then transferred to a different one. Metric stays organised in order that cost is assigned to pass through the network. The type of protocol decides the metric that is assigned to each network.

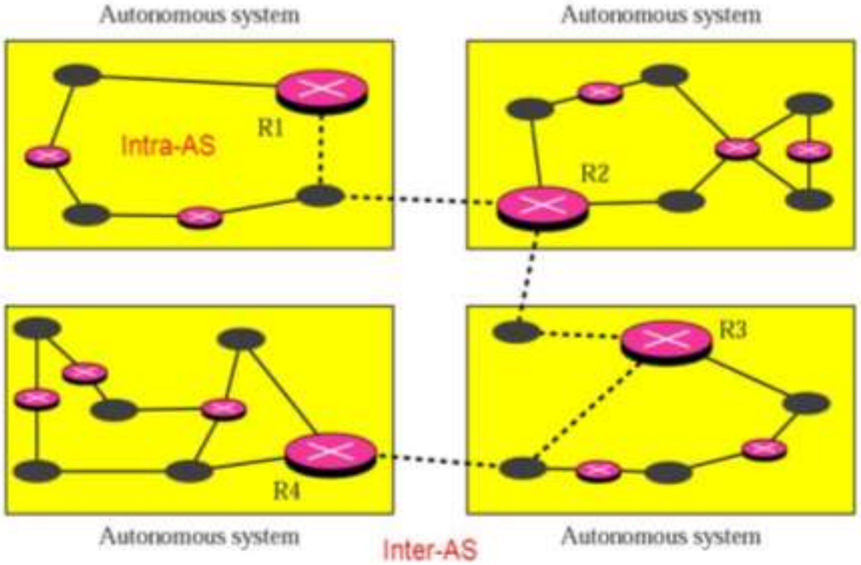
Intra and Inter-domain Routing

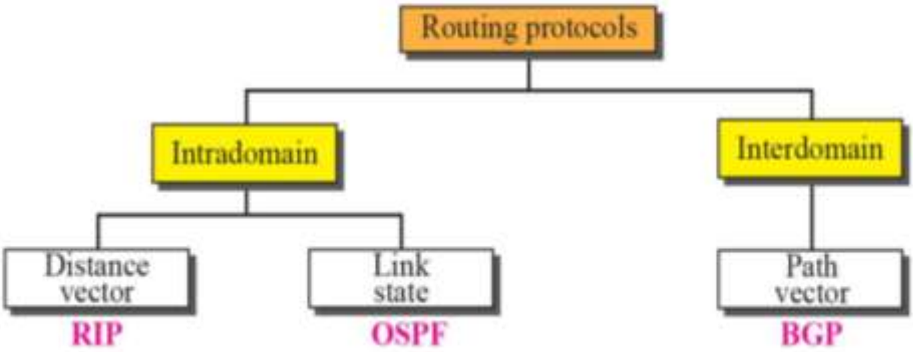
From a network, a router receives a packet and transfers it to another network. Typically, a single router has connections to many networks. The metric is thrown into assigning the passage of network expense. Depending on the type of protocol, metrics are allocated to each network.

The internet is divided into autonomous structures. Under the influence of a single administration, a set of networks and routers forms the autonomous appliance.

In the autonomous system, routing table is called inter-domain routing. Intra-domain routing is known as routing between autonomous systems. One or more intra-domain routing protocols can be chosen by each independent system to handle routing within system possessing autonomy.

Only one inter-domain routing protocol does routing between autonomous systems.

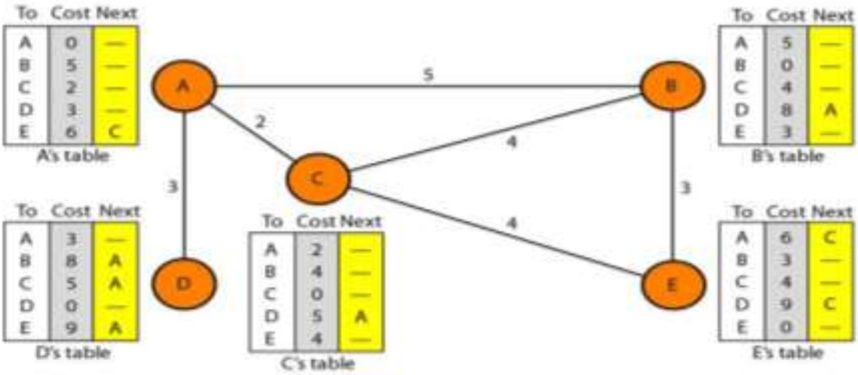




3.1.1. Distance Vector Routing

The minimum weighted route is the minimum cost path between the nodes in distance vector routing.

- A table of vectors with least distance to each node is maintained at each node.
- The packets to the desired node are also guided by the table of each node by displaying further hop routing on the path.



A's table

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

B's table

To	Cost	Next
A	5	—
B	0	—
C	4	—
D	8	A
E	3	—

D's table

To	Cost	Next
A	3	—
B	8	A
C	5	A
D	0	—
E	9	A

C's table

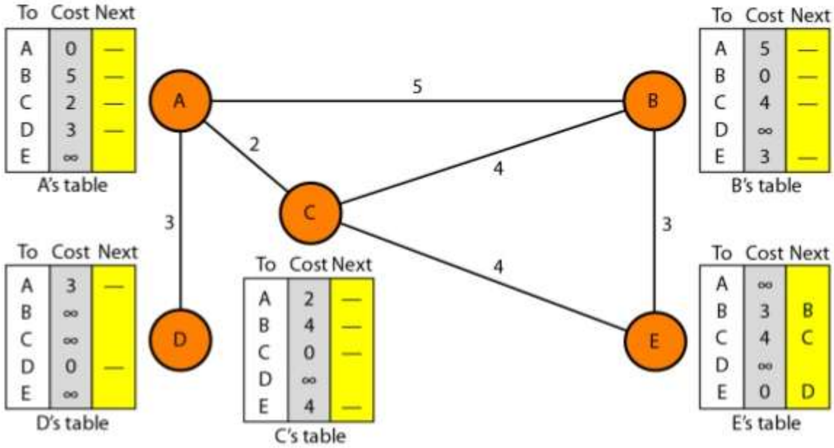
To	Cost	Next
A	2	—
B	4	—
C	0	—
D	5	A
E	4	—

E's table

To	Cost	Next
A	6	C
B	3	—
C	4	—
D	9	C
E	0	—

Initialization

- The cost or way to reach a node is known by every node. Any node knows the distance from self to its adjacent node that are directly connected to it.
- In order to find the distance between their neighbours and themselves, each node will send a message to their immediate neighbours.
- For any entry that is not a neighbour, then the distance noted to be infinite or unreachable.



A's table

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	∞	

B's table

To	Cost	Next
A	5	—
B	0	—
C	4	—
D	∞	
E	3	—

D's table

To	Cost	Next
A	3	—
B	∞	
C	∞	
D	0	—
E	∞	

C's table

To	Cost	Next
A	2	—
B	4	—
C	0	—
D	∞	
E	4	—

E's table

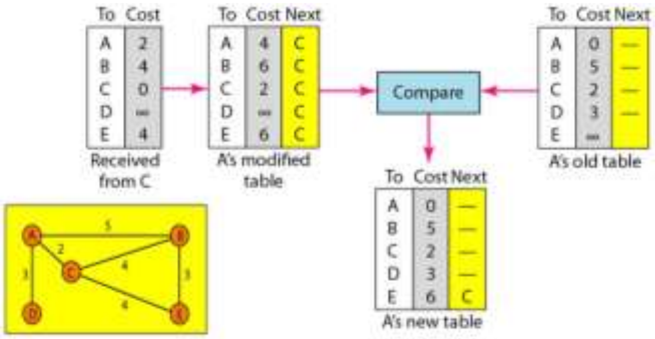
To	Cost	Next
A	∞	
B	3	B
C	4	C
D	∞	
E	0	D

Sharing

- In the routing of distance vectors, whenever there is a shift, the adjacent node of each one can get their table entry regularly.
- Information sharing between neighbours is the whole principal of vector distance routing.
- If Node A is unaware of the E node but node C can and this C node can share its routing table with A, therefore node A can reach node E as well.
- If they render support each other, then the nodes A and C will boost their routing tables as immediate neighbours.

Updating

- If the two nodes receive the neighbouring two-column table, its routing table needs to be modified.
- There are 3 steps while updating.
- In the second column, the receiver must append the cost of any value between itself and the transmitting node.
- If the receiving node uses information from another row, the name of the sender is added to the third column of every row by the receiver.
- The send node will be the next node in the path.
- Each row of the previous table has been compared with the appropriate row of the amended table edition by the receiving node.
- The receiver selects the row with the smallest cost if the next node entry is different. If both remains, the previous node will be held.
- A new row is chosen by the receiver, while the forthcoming station has the same marking.
- By using the tables obtained from other nodes, each node will update its table.



To	Cost
A	2
B	4
C	0
D	∞
E	4

Received from C

To	Cost	Next
A	4	C
B	6	C
C	2	C
D	∞	C
E	6	C

A's modified table

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	∞	

A's old table

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

A's new table

When to Share

Periodic update: Routing table is sent by A node through a constant update of 30's. The duration depends on the protocol which uses the routing of distance vectors.

Triggered update: Whenever a shift is encountered in its routing table, the neighbours receive a routing table with 2 columns from a node. This upholds the update trigger process.

3.1.1.1. Routing Information Protocol (RIP)

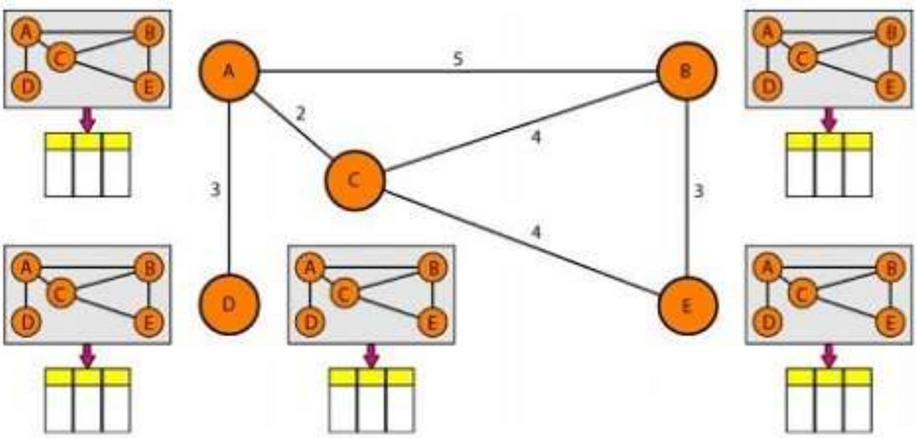
This follows a methodology that implements routing within an autonomous system.

Centred around distance vector routing, this seems to be a very simple protocol. It specifically incorporates distance vector routing with the same specifications:

- Routers as well as networks are dealt in an autonomous system. Routing tables are found in routers where in networks it is missing.
- Routing table refers a network address that is specified in the first column.

3.1.2. Link State Routing

- The RIP uses a very simple metric, the number of links (networks) represent the distance to reach the destination. In RIP, this metric is referred as count of hops.
- 16 is specified instead of infinity, meaning which chosen route may not have more than 15 hops in an autonomous system using RIP.
- The destination address is specified by the next node column.
- The routing table of a node can be constructed by the Dijkstra algorithm when each node in a domain contains the complete domain’s topology, the list of nodes, links and the connection types, the metrics used, and link condition.
- This table is unique for every node even though it uses similar topology, because dissimilar understandings are used in calculating the topology.
- The topology of each node and connexion must be dynamic, reflecting the latest state.
- The topology must be changed for each node if there are adjustments at some point in the network.



Somewhere in the network, the understanding of the topology at the start or post transit is not possible.

Each node has partial knowledge of its relationship to the state in terms of type, cost and condition.

Building Routing Tables

The 4 action sets are the requisites of link state routing in order that the routing table.

Link state routing requires four sets of actions in order that the table containing routing data of every part indicates the least costly node for any other node.

1. Link state packet (LSP) is the creation of states by the links of each node.
2. Effectively and efficiently disseminate LSP to any other router named flood.
3. Forms the shortest tree path for every node.
4. Routing table calculation is determined by the tree which holds the quick routes.

1. Creation of LSP

- The LSP can carry large amount of information.
- Example: It carries minimum amount of data, a list of links, a sequence number and age, the node identity 1.
- The identity of the first two nodes and list of links are required to form a topology.
- A new LSP is set apart from older ones, because flooding is encouraged by the 3rd sequence number.
- The old LSP is avoided staying long in the domain due to the 4th era.

Created LSP on 2 occasions:

1. Where the topology of the domain shifts.
2. Periodically dependent.

2. Flooding of LSP

When the LSP is ready at a node, it must not be disseminated to neighbours alone, but to all other nodes.

This procedure is often referred as flooding, and is built on the following:

1. The node created sends out each interface from a copy of the LSP.
2. A node receiving an the LSP received at a node is compared with the copy that is already available.
   a) The new LSP is preserved, whereas the previous is discarded.
   b) Transmits replica of it from every boundary to presume the one that the interface is from the packet arrived. This means flooding will stop somewhere inside the domain.

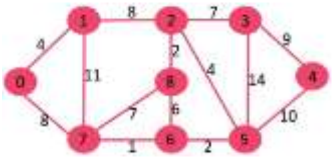
3. Formation of the Shortest Path Tree

Dijkstra's Algorithm

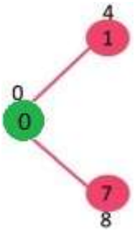
Every other node will have a copy of the entire topology until all LSPs have been sent. A shortest path tree is important for finding the shortest path to another node.

- The tree is a node and a connexion graph, and a single node is known as the root.
- All the other nodes are accessed via a single route from the root.
- If the path from the root to another node is the minimal path, then the path is declared as the shortest path of the tree.
- Algorithm Dijkstra generates the minimal tree path of graphs.
- The split up of nodes as two by algorithm are given as tentative & pentative.
- Neighbours to the new one believes that it alerts, testing it & making them permanent holding a satisfied constraint.

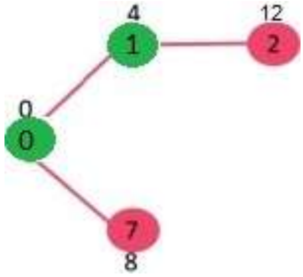
Example



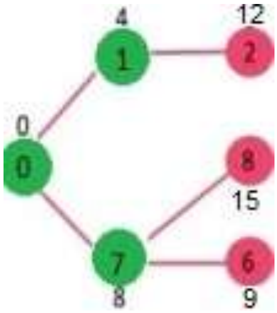
Pass 1:



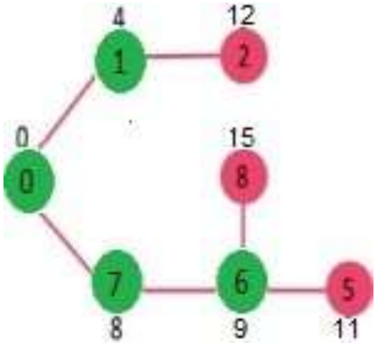
Pass 2:



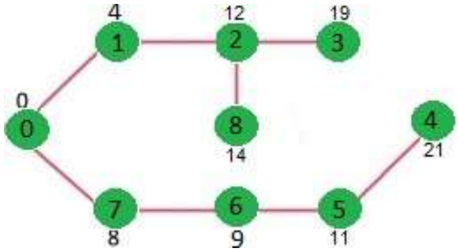
Pass 3:



Pass 4:



Pass 5:



Routing Table Calculation

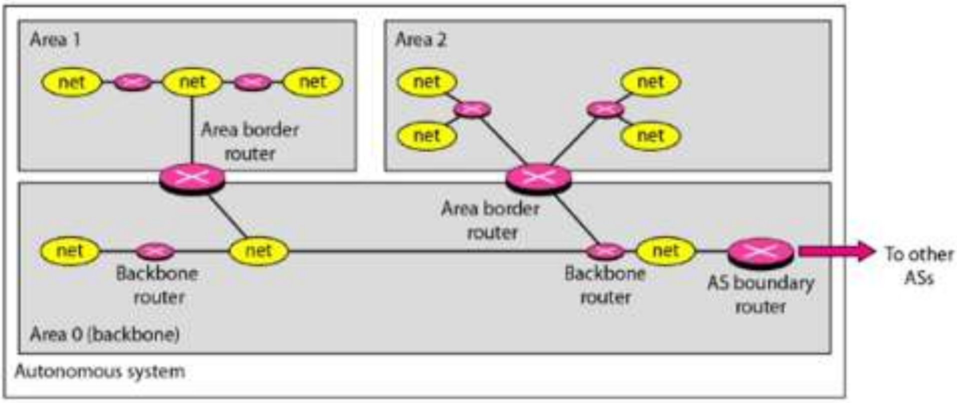
- Each node builds its table using the shortest tree path protocol.
- The routing table indicates the cost from the root to reach each node.

Node	*Cost*	*Next Router*
A	0	-
B	5	-
C	2	-
D	3	-
E	6	C

3.1.2.1. Open Shortest Path First (OSPF)

This routing protocol utilizes LSR method in intra-domain routing-based connection. It also has an autonomous structure as its domain. OSPF breaks an individual system into areas to make it functional. A system is autonomous when it comprises of hosts, different networks and routers. It is possible to split an autonomous system into several different fields. Both networks must be linked to within a network. With routing information, routers within the area cause flood. Special routers called the area boundary routers summarise the area 's details at the boundary of a country and forward it to other regions. Since there is a special backbone, it is important to link all areas within an autonomous system with the backbone. Backbone routers are known as the router within the backbone.

When the backbone with area's connection gets wrecked, an administrator should establish a virtual connexion between routers to allow the backbone functions to be linked as a primary area.



Metric

The OSPF protocol which enables the cost allocation to each path by the administrator, it is termed as the metric.

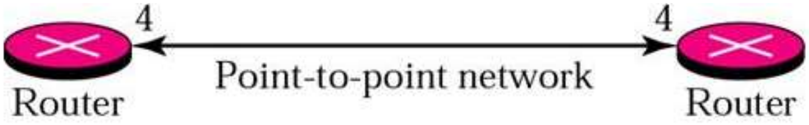
A minimum delay form of operation, the maximum throughput, may be dependent on the metric.

Types of Link

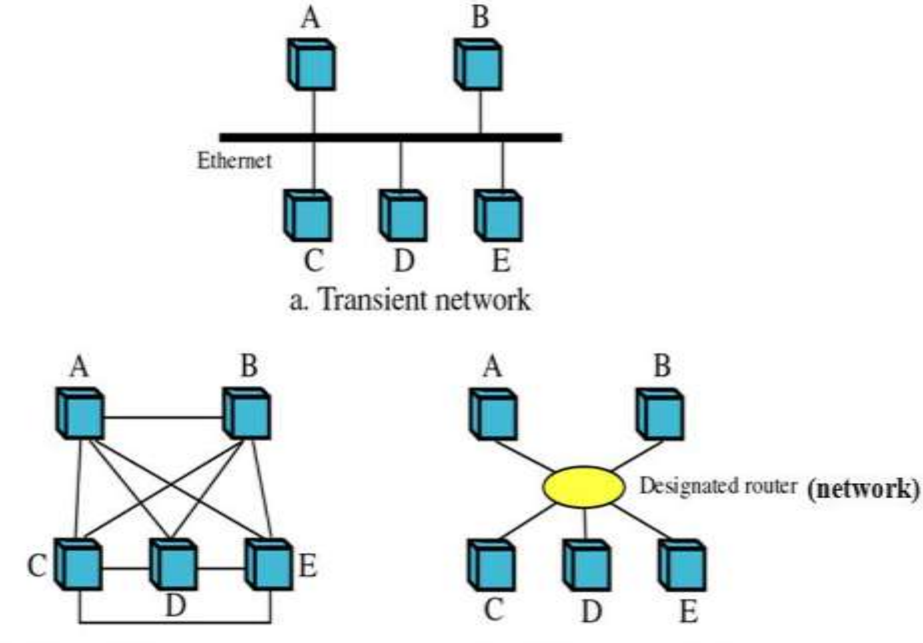
In OSPF, a relation is termed as a connexion.

There are 4 types of links namely Point to point, Transient, Stub and virtual.

- A connection is established between any routers without the presence of extra host or router using direct point link.



- A network getting attached with several routers form a transient link.
- The data is allowed to enter or move off from a routing device.

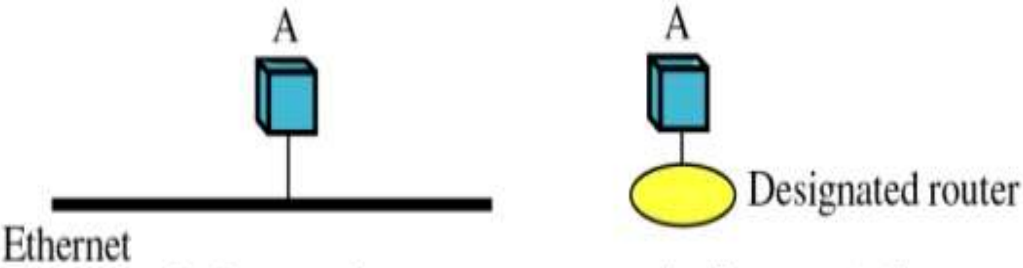


a. Transient network

b. Unrealistic representation

c. Realistic representation

- If a network has no other router connector except one, that network is referred as a stub connection.
- Entry and exit of data packets from the network are done using only one router.

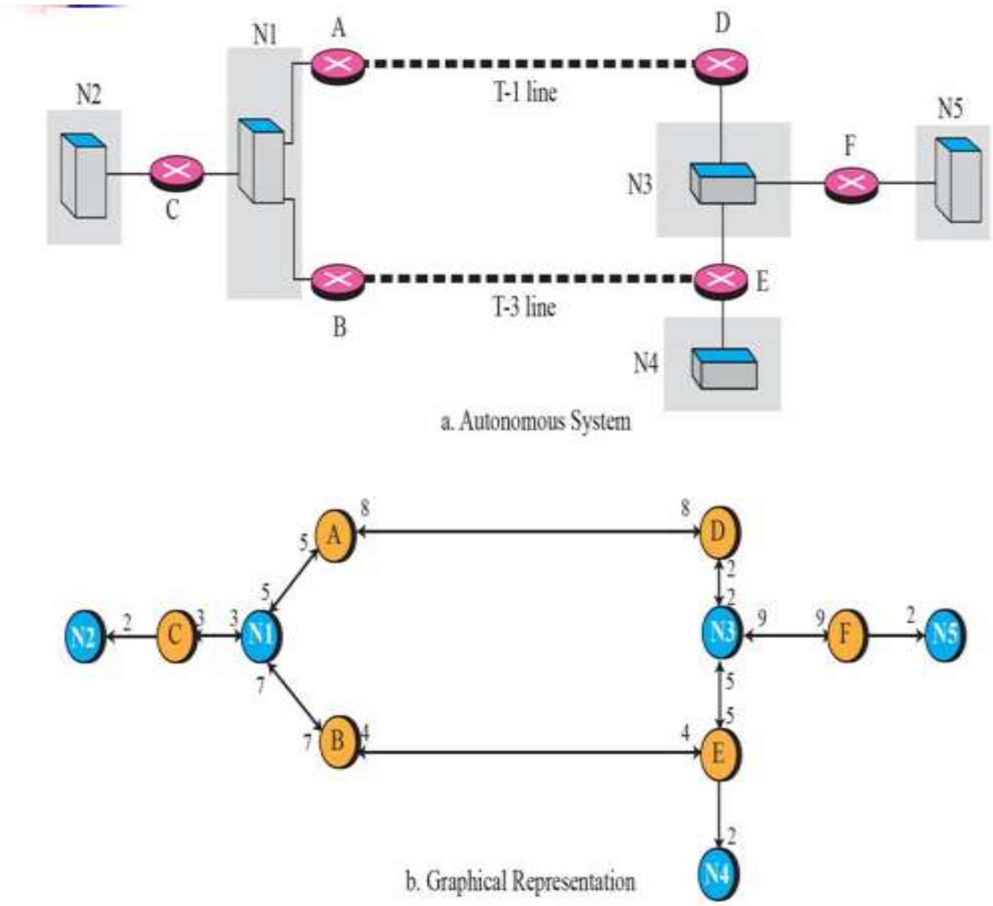


a. Stub network

b. Representation

- The administration can establish a virtual link when the connection with two routers get damaged. It uses the longest path that possibly visits many other routers.

Autonomous System in its Nodal Manipulative Imagery



a. Autonomous System

b. Graphical Representation

3.1.3. *Path Vector Routing*

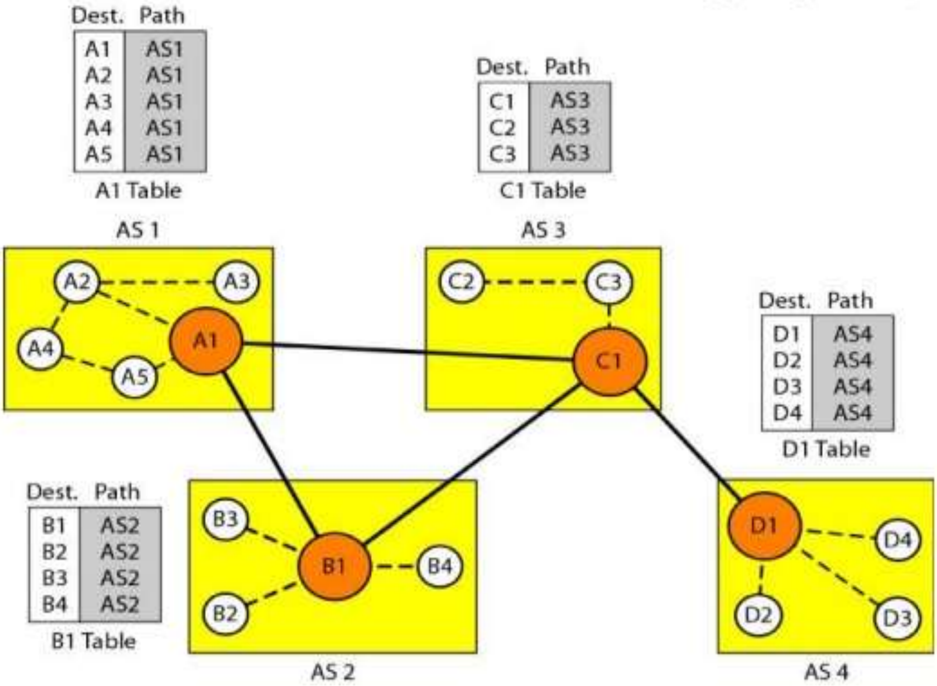
It takes place within the domain and is almost identical with routing over distance vector.

If in any autonomous system, the one node functioning on behalf of the whole autonomous system is the speaker node. The speaker node in an AS generates the routing table and advertises the neighbouring AS t speaker nodes.

The path alone is advertised ignoring the metrics of the nodes.

Initialization

The nodes' reachability is made known only at the beginning of every speaker node within an independent framework.



The speaker nodes of i = 1 to n (here n = 4) for AS1 is A1, B1, C1 and D1 respectively. A1 that creates a starting table showing the location A1 to A5 in AS1 might be reached accordingly.

B1 to B4 is advertised in node B1 and reached via. B1 and so on.

Sharing

With immediate neighbours, the table is shared by a speaker in an autonomous system.

The table of node A1 is shared with nodes B1 and C1. Similarly, the node C1 shares its table with nodes D1, B1 and C1. Also, node B1 shares with C1 also with A1 and finally, the D1 connects with C1 as shown in the figure.

Updating

After showing a while the tables are stabilised for each speaker node after the device.

When a neighbour's two column table is obtained by a speaker node, its table is updated by appending other nodes. After showing a while the tables are stabilised for each speaker node after the device.

The routing table fully shows the route.

Suppose a packet for node A is received by node D1 in AS4, it recognizes that a travel can be made via. AS4 then AS3 and also AS1.

Loop Prevention

Path vector routing helps in avoiding the loops formation as well the unpredictability caused by the distance vector routing. A monitor is performed to all packets received to verify whether the autonomous system is found at the destination path. The message will be overlooked if looping is required.

Policy Routing

It is easy to implement based on path vector routing. It can check the path when a router receives a message. A path and its destination are ignored only if the path violates the policy. With this route, it does not both update its routings and no message is sent to its neighbour.

Optimum Path

Optimum path always suits a company. Every autonomous system can have many routes to reach the destination.

3.1.3.1. Border Gateway Protocol (BGP)

It is an inter-domain routing protocol which uses path vector routing.

Types

The internet canbe divided into autonomous structures called hierarchical domains. An autonomous system is the local ISP which is responsible for providing services to local customers.

It is categorised into 3 types namely Stub, Multi-homed and Transit.

Stub

A separate AS relates to a stub in inter domain traffic which is created otherwise completed in stub.

The traffic is sent from hosts of AS to next ASs for data. Data traffic won't be able to pass through a stub AS. The AS stub can either be a source or sink.

Multi-homed

A multi-homed AS possess more connectivity with another.

AS without data traffic is termed just as a sink or otherwise source. The data traffic observed from other AS is received and it transmits data traffic over to other ASs, it shows non-existence of transient data. It does not allow data to move through from one AS and go to another AS.

Transient

Transient traffic is also allowed in a multi-homed AS which forms a transient AS.

Path Attribute

The route shows a list of autonomous systems, or attributes. Each attribute sets out some path detail. In enforcing its regulation, the attribute list helps the receiving router to make a more conscious division.

The 2 different categories of attributes are given as Well known or Optional.

An attribute is known to be a well-known attribute when it can be recognised by any BGP router. An optional attribute is one that each router does not need to know.

It has 2 categories namely well known mandatory attributes and well known discretionary attributes.

An optional attribute is divided into 2 categories namely, Optional transitive attributes and optional non transitive attributes.

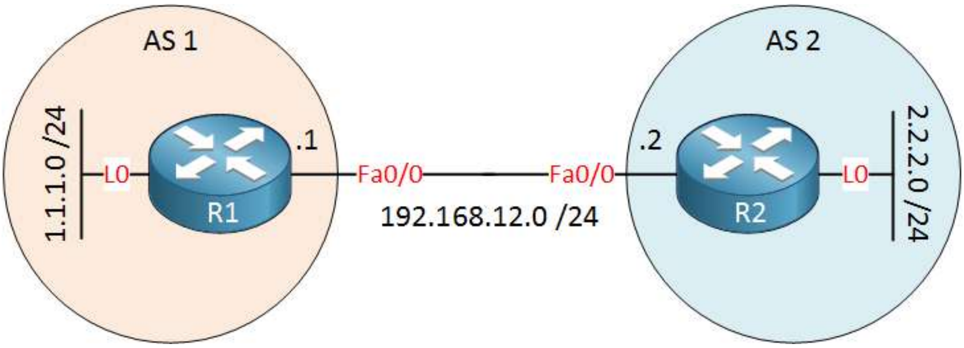
A well-known compulsory feature is the one that appears in the route definition. Each router must recognise one well-known discretionary attribute, but it is not necessary to be included in every update message.

An optional transitive attribute is one that the router who has not implemented this attribute must transfer to the next router, whereas, an optional non-transitive attribute discards when it is not realized by the receiving router.

BGP Sessions

- In BGP sessions, transfer of information happens between the routers.
- The exchange of router details with 2 BGP routers is done by a session.
- BGP is divided into two sessions:
  - External BGP (E-BGP)
  - Internal BGP (I-BGP)
- The E-BGP session is used in data transfer between speaker nodes pertaining to distinct independent systems.
- The I-BGP session is employed in information transmission within an autonomous device between two routers.

Example



- E-BGP session is a session between AS1 and AS2.
- Network data is shared between two speaker routers.
- These two routers in the autonomous system need to gather information from other routers and it happens via I-BGP sessions.

3.2. Global Internet - IPV6

Version 6 of the Internetworking Protocol is often referred to as IPng (internetworking protocol, next generation). It overcomes IPV4 deficiencies. The packet has a stipulated format and duration.

Advantages

- Greater address space.
- Efficient header format.
- Advanced options.
- Life allowance.
- Support for resource allocation and security.

Packet Format

A mandatory base header and a payload forms a packet.

Two sections that forms the payload:

1. Headers for optional extensions
2. Data at the top sectional layer.

The base header covers 40 bytes, while the extension header and the higher layer data comprise to 65,535 data in bytes.

Base Header

Version

The version number of IP is given in 4 bits field. The value of IPV6 is 6.

Priority: The packet's priority in relation to congestion from traffic is given in the 4-bit priority area.

Flow label: The flow mark is a 3-byte field designed for a defined data flow to provide special handling.

Payload data length: The header followed by base of header is given in the next header as 8 bit field. It is an optional IP header with extension otherwise header of an encapsulated packet such as the UDP or TCP.

Also contains the following field in each of the extension header:

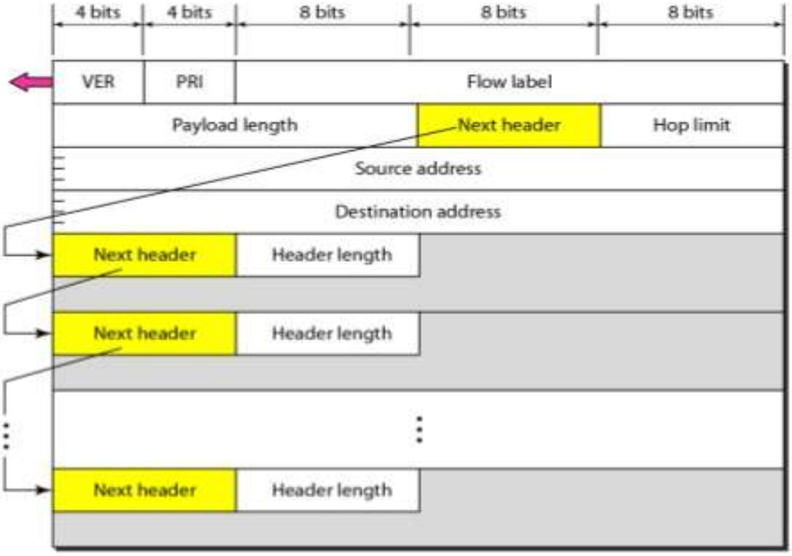
Hop limit: The 8-hop limit area serves the same function as IPV4's TTL area.

Source address: The field whose internet address is of 16 bytes (128 bit) which identifies the original datagram source.

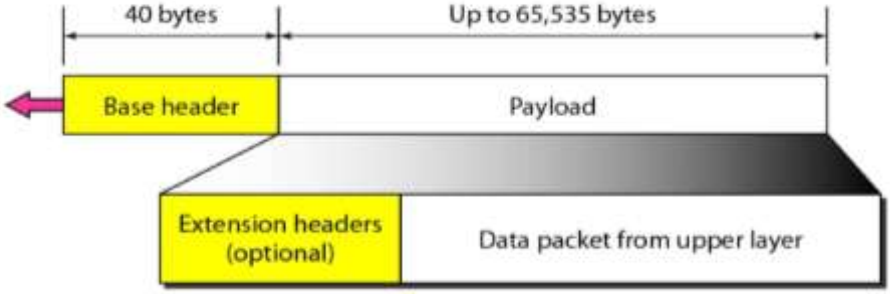
Destination Address

A 16 bytes (128 bit) internet address, which typically specifies the datagram's definite destination.

Datagram Format



Base Header and Payload Format



Priority

The IPV6 packet's priority field determines each packet's priority over other packets comin g from the same source.

There are 2 types of traffics are given below:

a. Congestion controlled traffic

b. Non-congestion controlled traffic

a) Congestion Controlled Traffic

- Congestion controlled traffic is referred as whenever a congestion is encountered and the source can adapt to slowdown of traffic.
- TCP protocol too could respond quickly to traffic by means of the sliding window protocol.
- It is easy to understand that delayed, misplaced or out of order packets will arrive.

Priority Meaning

1. No specific traffic
2. Background data
3. Unattended data traffic
4. Reserved
5. Attended bulk data traffic
6. Reserved
7. Interactive traffic
8. Control traffic

b) Non Congestion Controlled Traffic

This can be applied to the traffic predicted as causing minimal delayed.

Usually, the packets are discarded based on priorities and consistency of the data obtained.

Eg: video and audio.

Data with less redundancy can have a higher priority (15) and a lower priority (8) can be provided by more redundancy.

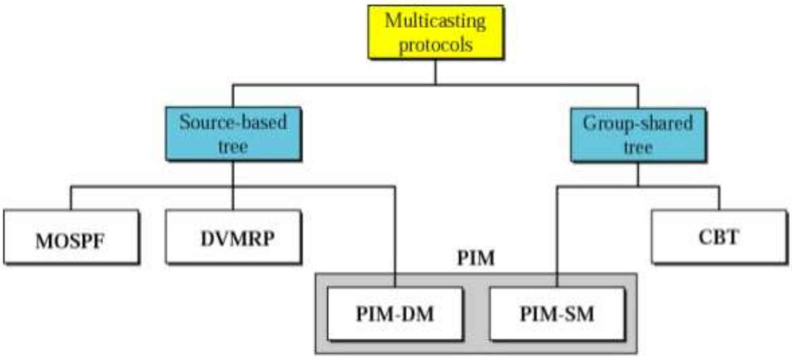
Flow Label

A packet flow is called a series of data packs transmitted between a specific source and destined node which requires a peculiar management of router.

The packet flow is uniquely determined by the combination of source address and flow label value.

3.3. Multicast Link State Routing

Multicast routing are emerged with the extensions of unicast routing protocols.



3.3.1. Multicast Open Shortest Path First (MOSPF)

The source-oriented tree approach is employed in multicast link state routing. Multicast open shortest path first (MOSpF) protocol is an extension of OSPF protocol that uses the routing of multicast link state to create source based trees.

To attach a host's unicast address with the address of the group or addresses that the host supports, the protocol needs a new state of update packet. This is called the group membership LSA. Only the hosts that belong to a specific group are included in the tree. The efficiency of the trees shortest path is calculated on request by router.

The tree can be saved by the same source / group pair for future use in cache memory. MOSPF is a protocol based on data. The datagram is built by the router, revealing the source and group address for the first time that a MOSPF router sees a datagram. the router constructs the shortest path tree for the Dijkstra.

3.3.2. *Multicast Distance Vector (DVMRP)*

Multicast routing can be supported by easily expanding the unicast vector distance routing. It prevents the routing table to be shared by the router.

A table can be built from start using unicast distance vector table.

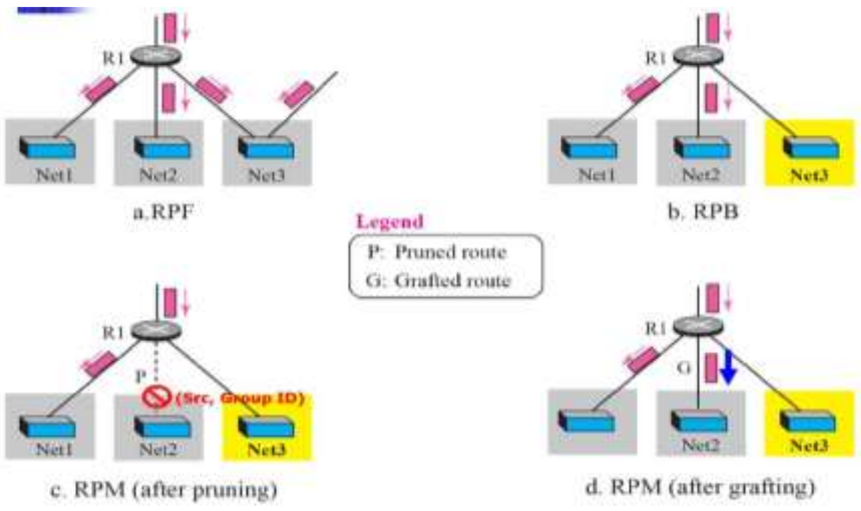
The tree-oriented source is employed for a multicast routing where the router cannot produce routing table. Whenever a multicast packet is received, the packet is forwarded through a routing table.

Flooding

- Broadcast of packets are done by flooding, which also formulates looping in the systems.
- A router receives a packet and sends it out from every interface except the one from which it was sent, leaving the destination group address unnoticed.
- A packet that has left the router can return from another interface again or it is possible to forward the same interface again.

3.3.3. *Reverse Path Forwarding (RPF)*

The looping caused during flooding is eradicated using RPF.



a. RPF

b. RPB

c. RPM (after pruning)

d. RPM (after grafting)

3.3.4. Reverse Path Broadcasting (RPB)

RPB establishes the shortest path to each destination broadcast tree from the source and ensures that only a single copy of a packet is received at the destiny.

3.3.5. Reverse Path Multicasting (RPM)

Pruning along with grafting is added to RPB by RPM which forms a multicast tree with shortest path as and when dynamic association changes.

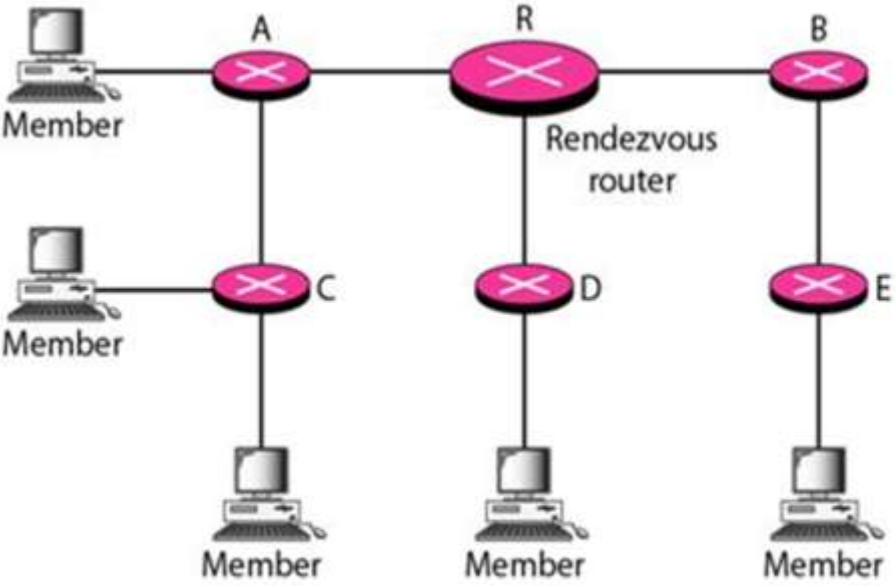
3.3.6. Core Based Tree (CBT)

The CBT is a protocol that is shared by a crew with a tree's base as a core. Each region is chosen as a centre by segregating the autonomous system into regions.

Formation of the Tree

After the core is selected, each router is defined to the unicast address of the selected router.

Each router then sends a unicast join message to indicate that the community wants to be joined.



- The required information is extracted from the message by the intermediate router such as the sender's unicast address along with interface and the successive router receives the message.
- The router can leave from a party by sending a message to its flow routes.

Sending Multicast Packets

- Any source can send a multicast packet to all members of the community after the creation of the tree.
- The packet is then sent to the rendezvous router via the rendezvous unicast address; then distributes the packets to all community members.
- Any hosts within or outside the shared tree may act as the source host.

Selecting the Appropriate Router

The following is the procedure to send packet from the source to the community members:

1. In multicast encapsulation, the part of the tree can either contain the root or not. With unicast destination address, the packet can be sent to the centre of the core. Using the unicast address, this part of distribution is done; the core router is the only re ceiver.
2. Decapsulation of the unicast packet is done at the centre and interfaces that are concerned will have or may receive.
3. The routers receiving the multicast packet, forwards them all to the interested interfaces.

3.3.7. Protocol Independent Multicast (PIM)

The PIM has 2 independent multicast routing protocols:

a. PIM DM - Protocol Independent Multicast, the Dense Mode.

b. PIM SM - Protocol Independent Multicast, the Sparse Mode.

a) PIM DM

- PIM-DM is employed when each router needs to engage in multicasting (dense mode).
- It is a type of protocol that prefers tree routing using strategies such as multicasting RPF with pruning and grafting.
- DVMRP's service is almost identical with PIMDM.
- Unicast protocol is used by independent system. A protocol and a table are contained in each router that helps in identifying or seeking an ideal path to destination for the outgoing interface.
- This unicast protocol can be either a RIP or OSPF.

b) PIM SM

- The usage of PIM-SM is where there is very less multicasting (sparse mode), such as WAN, for each router.
- The CBT protocol that uses a group-shared tree that is not justified by the protocol by which the packet is broadcasted.