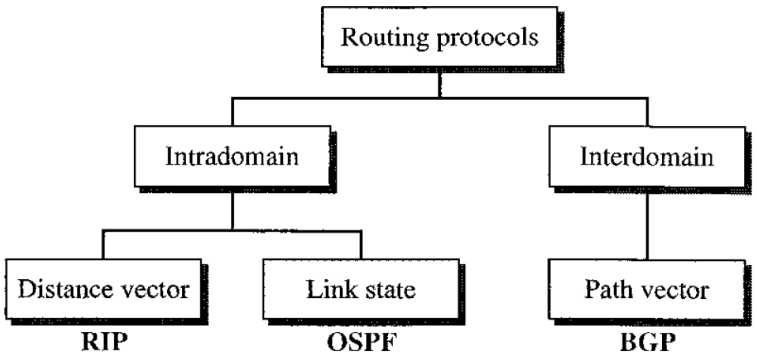
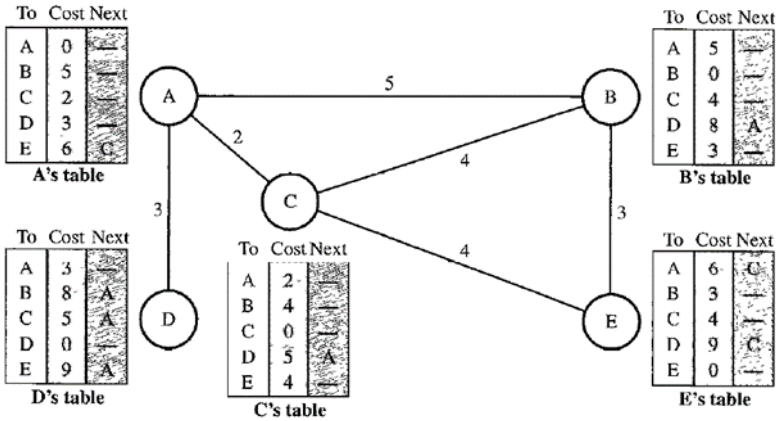
1. Describe Inter and Intra domain routing.

- Today, an internet can be so large that one routing protocol cannot handle the task of updating the routing tables of all routers. For this reason, an internet is divided into autonomous systems.
- An autonomous system (AS) is a group of networks and routers under the authority of a single administration.
- Routing inside an autonomous system is referred to as intradomain routing.
- Routing between autonomous systems is referred to as interdomain routing.
- Based on the above, the routing protocols are divided into two different categories: Intradomain routing protocols and interdomain routing protocols.
- Routing Information Protocol (RIP) is an implementation of the distance vector routing algorithm.
- Open Shortest Path First (OSPF) is an implementation of the link state routing algorithm.
- Border Gateway Protocol (BGP) is an implementation of the path vector routing algorithm.
- The figure shows the overview of routing protocols.

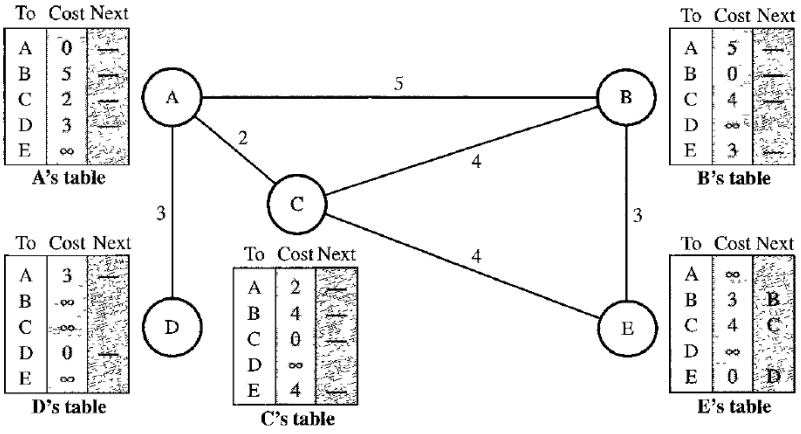


2. Explain distance vector routing algorithm.

- Distance vector routing (DVR) is a routing algorithm that uses a distributed approach to determine the best paths between two nodes(routers) in a graph(network).
- Each node maintains a table that contains the distance to every other node in the network.
- The distance is typically measured in terms of hops, which is the number of nodes a packet must pass through to reach its destination node.
- It uses Bellman-Ford algorithm is used to calculate the shortest path.
- The graph of five nodes with their corresponding tables are shown below.



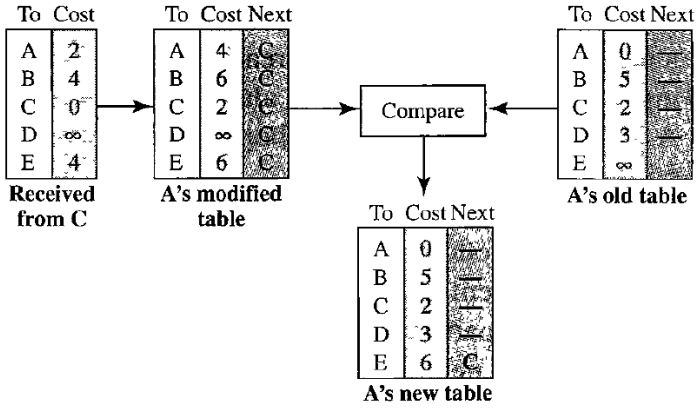
- The distance vector routing algorithm contains the following steps.
  1. Initialization
     - The above given table is stable. But this is not the case in the beginning.
     - At the beginning, however, this is not the case. Each node can know only the distance between itself and its immediate neighbours, those directly connected to it.
     - The distance for any entry that is not a neighbour is marked as infinite (unreachable).
     - The following figure shows the initial table for each node.



  2. Sharing
     - The whole idea of distance vector routing is the sharing of information between neighbours.
     - Although node A does not know about node E, node C does. So, if node C shares its routing table with A, node A can also know how to reach node E.
     - On the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C, node C also knows how to reach node D. In other words, nodes A and C, as immediate neighbours, can improve their routing tables if they help each other.
     - Sharing occurs in one of the following cases.
       - Periodically
       - Triggered update such a new path found or connection lost.
  3. Updating
     - When a node receives a two-column table from a neighbour, it needs to update its routing table. Updating takes three steps.
       I. Add the cost between the receiving node and the sending node to each value in the second column of the received table.
       II. Add the name of the sending node as the third column to each row of the modified received table.
       III. For each row in the receiving node's old table, compare it to the corresponding row in the modified received table:
         a. If the next-node entry is different, choose the row with the smaller cost. If there is a tie, keep the old row.

b. If the next-node entry is the same, choose the new row, even if its distance is infinity.

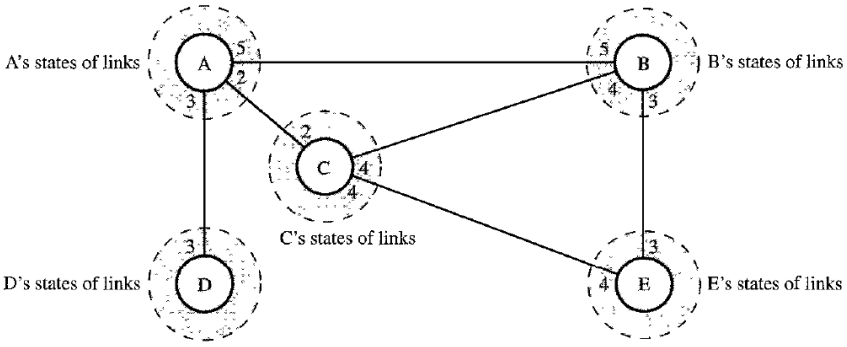
- The following figure shows how node A updates its routing table after receiving the partial table from node C.



- This algorithm can be susceptible to count to infinity problems.
  - Two-node loop.
    - It can be avoided using split-horizon and split-horizon poisoned reverse methods.
  - Three-node loop.
    - It cannot be avoided.

3. Explain link state routing algorithm.

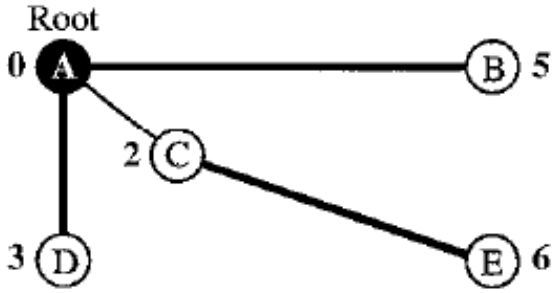
- The focus of the link state routing algorithm is that all the nodes in the graph must have topology of whole graph.
- The link state routing algorithm contains the following four sets of actions that are required to ensure that each node has the routing table showing the least-cost node to every other node.
  - Creation of the states of the links by each node, called the link state packet (LSP).
  - Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way.
  - Formation of a shortest path tree for each node.
  - Calculation of a routing table based on the shortest path tree.
- Consider the following graph to understand the link state routing which contains the immediate link state for each and every node.



- **Creation of Link State Packets**

- A link state packet can carry a large amount of information such as the node identity, the list of links, a sequence number, and age.
- The first two, node identity and the list of links, are needed to make the topology.
- The third, sequence number, facilitates flooding and distinguishes new LSPs from old ones.
- The fourth, age, prevents old LSPs from remaining in the domain for a long time.
- LSPs are generated in two scenarios:
  - Topology changes
  - Periodic updates

- **Flooding of LSPs**
  - LSP flooding ensures all nodes receive the latest network topology information:
  - The originating node broadcasts the LSP to all its interfaces.
  - Upon receiving an LSP, a node compares its sequence number to the one it already has.
    - If the received LSP is older, it is discarded.
    - If the received LSP is newer, it replaces the old one.
  - The node broadcasts the newer LSP to all its interfaces except the one it received it from.
  - This process ensures that flooding terminates when a node has only one interface.
- **Formation of Shortest Path Trees**
  - After receiving all LSPs, each node will have a copy of the whole topology. However, the topology is not sufficient to find the shortest path to every other node; a shortest path tree is needed.
  - A shortest path tree is a tree in which the path between the root and every other node is the shortest. What we need for each node is a shortest path tree with that node as the root.
  - The Dijkstra algorithm creates a shortest path tree from a graph.
  - After applying the Dijkstra algorithm on the node A in the sample graph given above, the shortest path from node A to all other node will be as follows.



- **Calculation of a routing table based on the shortest path tree.**
  - Each node uses the shortest path tree protocol to construct its routing table.
  - The routing table shows the cost of reaching each node from the root.
  - The following shows the routing table for node A.

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

- Link state routing algorithm can be more complex to implement and it generates more traffic.
- There is no count to infinity problem occurs in the link state routing algorithm.

4. Explain Path Vector Routing Algorithm.

- Path vector routing algorithm implements routing not based on the least cost goal but implements it based on the policy decided by the source.
- For example, one organization can use path vector routing to prevent its packets from routing through a particular network, even if that network is part of the least cost path. i.e. path vector routing algorithm allows routing based on the policy.
- In path-vector routing, the path from a source to all destinations is also determined by the best spanning tree. If there is more than one route to a destination, the source can choose the route that meets its policy best.
- A source may apply several policies at the same time. One of the common policies uses the minimum number of nodes to be visited.
- Consider the following figure-1 internet to understand the path vector routing algorithm.

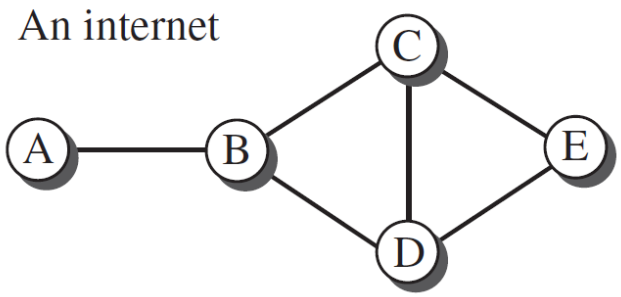


Figure – 1

- The path vector routing algorithm contains the following steps.
  - Initialization of path vector.
  - Sharing of path vector.
  - Updating of the path vector.

Initialization

- When a node is booted, it creates a path vector based on the information it can obtain about its immediate neighbour. A node sends greeting messages to its immediate neighbours to collect these pieces of information.
- The following Figure-2 shows all of these path vectors for our internet (Figure-1). The figure-2 also shows how these path vectors are sent to immediate neighbours after they have been created (arrows).

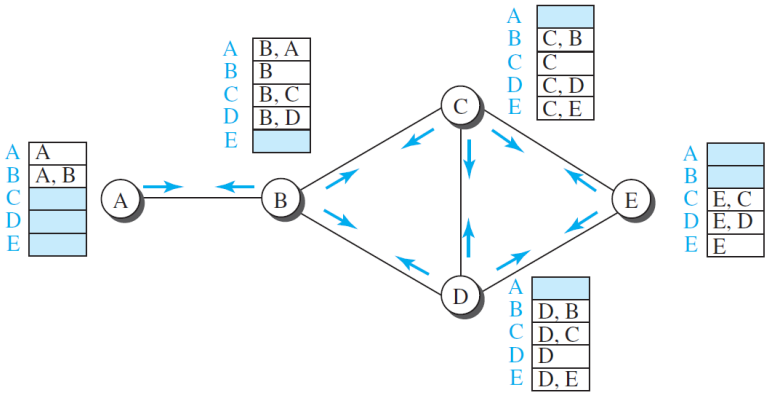


Figure – 2

Sharing

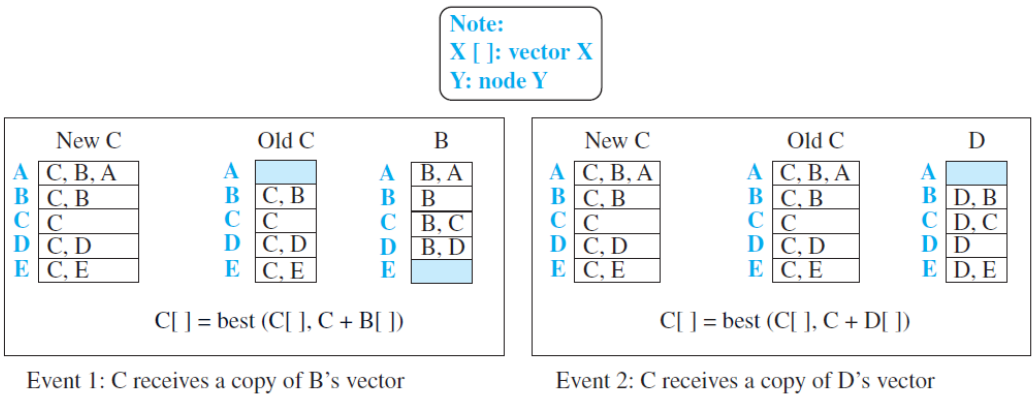
- Each node, after the creation of the initial path vector, sends it to all its immediate neighbours.

Updating

- Each node, when it receives a path vector from a neighbour, updates its path vector using a Bellman-Ford equation, but applying its own policy instead of looking for the least cost.
- This equation prevents looping.

$$\text{Path}(\boldsymbol{x}, \boldsymbol{y}) = \text{best}\,\{\text{Path}(x, y), [(\boldsymbol{x} + \text{Path}(\mathbf{v}, \boldsymbol{y})]\} \qquad \text{for all } \mathbf{v}\text{'s in the internet.}$$

- The Figure-3 shows the path vector of node C after two events.
  - In the first event, node C receives a copy of B's vector, which improves its vector: now it knows how to reach node A.
  - In the second event, node C receives a copy of D's vector, which does not change its vector.
- As a matter of fact, the vector for node C after the first event is stabilized and serves as its forwarding table.



Event 1: C receives a copy of B's vector

Event 2: C receives a copy of D's vector

Figure – 3

5. Describe Autonomous System.

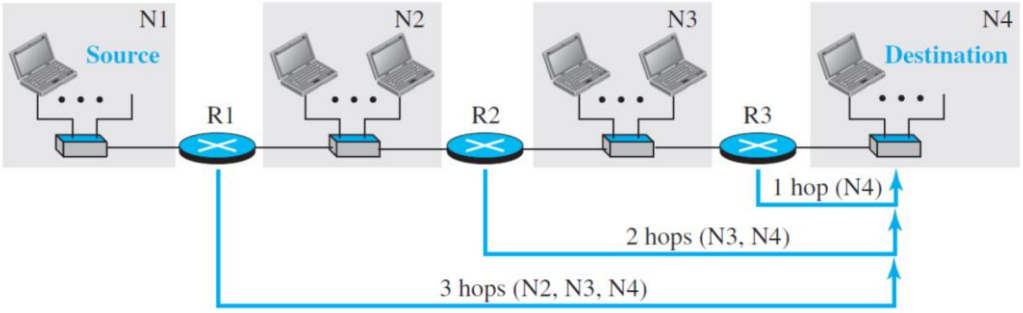
- An autonomous system is defined as the network and routers which are managed by the single organization. The abbreviation for autonomous system is AS.
- ISPs are the example of Autonomous System.
- Each AS is identified by a 16-bit unsigned number provided by ICANN.
- The autonomous systems are categorized according to the way they are connected to other ASs.
- There are three categories of Autonomous systems.
    - Stub AS
    - Multihomed AS
    - Transient AS
- Stub AS
    - A stub AS has only one connection to another AS.
    - The data traffic can be either initiated or terminated in a stub AS; the data cannot pass through it.
    - A good example of a stub AS is the customer network, which is either the source or the sink of data.
- Multihomed AS
    - A multihomed AS can have more than one connection to other ASs, but it does not allow data traffic to pass through it.
    - A good example of such an AS is some of the customer ASs that may use the services of more than one provider network, but their policy does not allow data to be passed through them.
- Transient AS
    - A transient AS is connected to more than one other AS and also allows the traffic to pass through.
    - The service provider networks, and the backbone are good examples of transient ASs.

6. Explain RIP protocol.

- The Routing Information Protocol (RIP) is one of the most widely used intradomain routing protocols based on the distance-vector routing algorithm.

HOP Count

- In RIP, the cost is defined as the number of hops, which means the number of networks (subnets) a packet needs to travel through from the source router to the final destination host.
- The following figure shows the concept of hop count advertised by three routers from a source host to a destination host.



- Ex. The hop count for packet from host from N1 network to destination host in N4 network is 3.
- In RIP, the maximum cost of a path can be 15, which means 16 is considered as infinity (no connection). For this reason, RIP can be used only in autonomous systems in which the diameter of the AS is not more than 15 hops.

Forwarding Tables

- A forwarding table in RIP is a three-column table in which the first column is the address of the destination network, the second column is the address of the next router to which the packet should be forwarded, and the third column is the cost (the number of hops) to reach the destination network.
- The forwarding tables of the above routers is shown below.

Forwarding table for R1

Destination network	Next router	Cost in hops
N1	——	1
N2	——	1
N3	R2	2
N4	R2	3

Forwarding table for R2

Destination network	Next router	Cost in hops
N1	R1	2
N2	——	1
N3	——	1
N4	R3	2

Forwarding table for R3

Destination network	Next router	Cost in hops
N1	R2	3
N2	R2	2
N3	——	1
N4	——	1

- The third column is not needed for forwarding the packet, but it is needed for updating the forwarding table when there is a change in the route.

RIP Implementation

- RIP is implemented as a process that uses the service of UDP on the well-known port number 520.
- RIP has gone through two versions: RIP-1 and RIP-2.

RIP Messages

- RIP uses two types of messages: request and response.
- Request Messages
    - Sent by a router that has just come up or has timed out entries.
    - Can ask about specific entries or all entries.
- Response Messages
    - Can be either solicited or unsolicited.
    - Solicited responses are sent in response to request messages.
    - Unsolicited responses are sent periodically or when there is a change in the forwarding table.

RIP Algorithms

- Initialization: In this step, all routers prepare routing table by adding all the immediate neighbours with the hop count.
- Sharing: In this step, all the routers share their routing tables with their immediate neighbours.
- Updating:
    - The received forwarding table(modified) by a router is known **the received route** and the forwarding table(old) of a router is known as **the old route**.
    - The received router selects the old routes as the new ones except in the following three cases:
        - If the received route does not exist in the old forwarding table, it should be added to the route.
        - If the cost of the received route is lower than the cost of the old one, the received route should be selected as the new one.
        - If the cost of the received route is higher than the cost of the old one, but the value of the next router is the same in both routes, the received route should be selected as the new one. This is the case where the route was actually advertised by the same router in the past, but now the situation has been changed.

Timers in RIP

- RIP uses three timers.
    - The periodic timer
    - The expiration timer
    - The garbage collection timer

Performance

- Update Messages
    - RIP's update messages are simple and local, sent only to neighbours.
- Convergence of Forwarding Tables
    - RIP employs the distance-vector algorithm, which can exhibit slow convergence in large networks.

- Robustness
  - Distance-vector routing can be easily disrupted if a router fails or is corrupted, as it relies on routers sharing information with each other.

7. Explain Timers of RIP protocol.

- RIP uses three timers to support its operation.

The periodic timer

- It controls the advertising of regular update messages.
- Each router has one periodic timer that is randomly set to a number between 25 and 35 seconds.
- The timer counts down; when zero is reached, the update message is sent, and the timer is randomly set once again.

The expiration timer

- It governs the validity of a route.
- When a router receives update information for a route, the expiration timer is set to 180 seconds for that particular route.
- Every time a new update for the route is received, the timer is reset. 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, which means the destination is unreachable.
- Every route has its own expiration timer.

The garbage collection timer

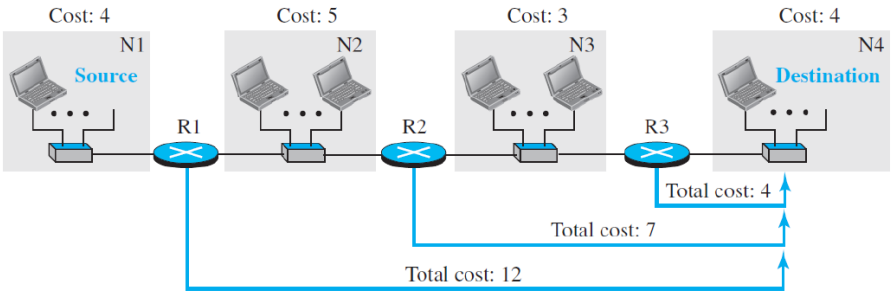
- It is used to purge a route from the forwarding table.
- When the information about a route becomes invalid, the router does not immediately purge that route from its table. Instead, it continues to advertise the route with a metric value of 16.
- At the same time, a garbage collection timer is set to 120 seconds for that route. When the count reaches zero, the route is purged from the table.
- This timer allows neighbours to become aware of the invalidity of a route prior to purging.

8. Explain OSPF protocol.

- Open Shortest Path First (OSPF) is also an intradomain routing protocol based on the link-state routing protocol.

Metric

- In OSPF, the cost of reaching a destination from the host is calculated from the source router to the destination network.
- The cost is either the weight is assigned to the network based on the throughput, round-trip time, reliability, and so on. or cost can be a hop count.
- The following figure shows the idea of the cost from a router to the destination host network.



Forwarding Tables

- Each OSPF router can create a forwarding table after finding the shortest-path tree between itself and the destination using Dijkstra's algorithm.
- The forwarding tables for the AS given above is shown below.

Forwarding table for R1

Destination network	Next router	Cost
N1	——	4
N2	——	5
N3	R2	8
N4	R2	12

Forwarding table for R2

Destination network	Next router	Cost
N1	R1	9
N2	——	5
N3	——	3
N4	R3	7

Forwarding table for R3

Destination network	Next router	Cost
N1	R2	12
N2	R2	8
N3	——	3
N4	——	4

Areas

- OSPF was designed to be able to handle routing in a small or large autonomous system.
- OSPF divides the large autonomous system into small areas to handle the traffic generated through the flooding of LSPs.
- Each area has its own area identification number.
- All the routers within the area must have all the route related information of its area as well as other areas. It can be achieved through backbone area. The area identification number of the backbone area is 0.

Link state advertisements

- OSPF has five different types of link state advertisements.
    - Router link
    - Network Link
    - Summary link to network
    - Summary link to AS border router
    - External Link

OSPF Implementation

- OSPF is implemented as a program in the network layer, using the service of the IP for propagation.
- OSPF has gone through two versions: version 1 and version 2.

OSPF Messages

- It is a very complex protocol.
- It uses five different types of messages
    - Hello message
    - Database description message
    - Link state request message
    - Link-state update message
    - Link-state acknowledgment message

Authentication

- OSPF Authentication in its common header prevents a malicious entity from sending OSPF messages to a router.

OSPF Algorithm

- It implements the link-state routing algorithm.
- OSPF routers floods Link state packets to all the routers inside the autonomous system.
- After getting LSPs, OSPF router prepares Link state database.
- Then OSPF router uses Dijkstra's algorithm to find the shortest path to all the other routers.
- After finding the shortest path, it prepares the routing table.

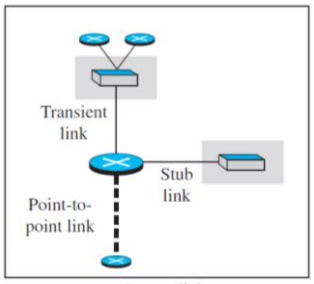
Performance

- Update Messages
    - It floods the messages in the area. If the area is large, then it creates a traffic problem.
- Convergence of Forwarding Tables
    - Convergence fairly quick.
- Robustness
    - This protocol is more robust than RIP.
    - it less susceptible to disruptions caused by individual router failures compared to RIP.

9. Describe Link-state advertisements.

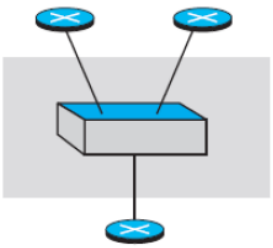
- OSPF is based on the link-state routing algorithm, which requires that a router advertise the state of each link to all neighbors for the formation of the LSDB.
- OSPF uses five different types of Link-state advertisements.
    - Router link,
    - Network link,
    - Summary link to network,
    - Summary link to AS border router,
    - External link.
- Router Link
    - Router links advertise the existence of a router and the types of connections it has to other entities.

- A transient link announces a link to a transient network, a network that is connected to the rest of the networks by one or more routers. This type of advertisement should define the address of the transient network and the cost of the link.
- A stub link advertises a link to a stub network, a network that is not a through network. Again, the advertisement should define the address of the network and the cost.
- A point-to-point link should define the address of the router at the end of the point-to-point line and the cost to get there.



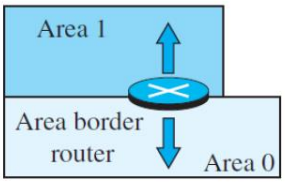
Router links

- Network link
  - A network link advertises the network as a node, and this advertisement is done by a designated router on the network.
  - The network link advertisement includes the IP addresses of all routers connected to the network, but it does not include any cost information.



Network Link

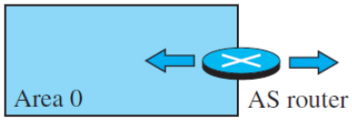
- Summary link to network
  - This is done by an area border router; it advertises the summary of links collected by the backbone to an area or the summary of links collected by the area to the backbone.
  - This type of information exchange is needed to glue the areas together.



Summary Link to network

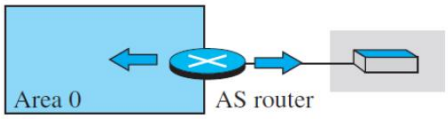
- Summary link to AS border router

- AS routers summarize routing information from other autonomous systems (ASs) and share it with the backbone area of their own AS.
- This information is then distributed to other areas within the AS, allowing routers to learn about networks in other ASs.



Summary link to AS border router

- External link
  - This is also done by an AS router to announce the existence of a single network outside the AS to the backbone area to be disseminated into the areas.



External Link

10. Describe different types of OSPF messages.

- OSPF is a very complex protocol; it uses five different types of messages.
  - The hello message
  - The database description message
  - The link state request message
  - The link-state update message
  - The link-state acknowledgement message
- The hello message (type 1)
  - It is used by a router to introduce itself to the neighbors and announce all neighbors that it already knows.
- The database description message (type 2)
  - It is normally sent in response to the hello message to allow a newly joined router to acquire the full LSDB.
- The link state request message (type 3)
  - It is sent by a router that needs information about a specific LS.
- The link-state update message (type 4)
  - It is the main OSPF message used for building the LSDB.
- The link-state acknowledgment message (type 5)
  - It is used to create reliability in OSPF; each router that receives a link-state update message needs to acknowledge it.

11. Explain Border Gateway Protocol Version 4

- The border gateway protocol version 4 is the interdomain routing protocol, that implements path vector routing algorithm.
- It is used to establish communication among network of ISPs.

- It is a kind of point-to-point protocol. When it is installed on two routers, they try to create a TCP connection using the well-known port 179. The two routers that run the BGP processes are called BGP peers or BGP speakers.
- Consider the following figure-1 of internet with three ASs.

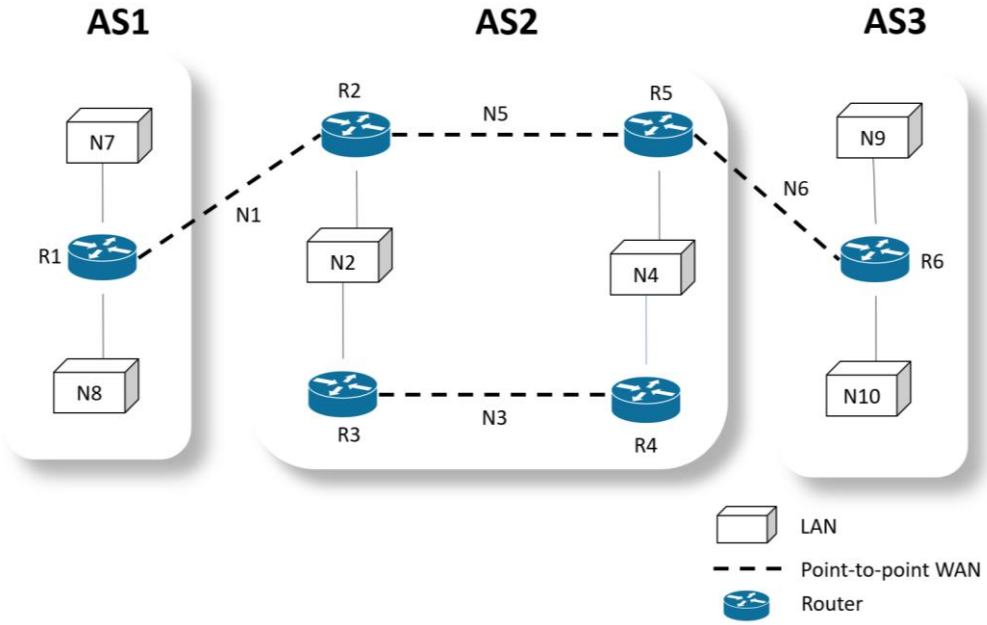


Figure – 1 Internet with three ASs

- In the above figure-1, AS1 and AS3 both are stub ASs and AS2 is the transient AS.
- Each autonomous system in this figure-1 uses one of the two common intradomain protocols, RIP or OSPF. Each router in each AS knows how to reach a network that is in its own AS, but it does not know how to reach a network in another AS.
- To enable routing among the networks shown in the figure - 1, it is required to do as follows.
    - Install a variation of BGP4, called external BGP (eBGP) on each border router.
    - Install a second variations of BGP4, called internal BGP (iBGP) on all routers.
- All the border routers will be running three routing protocols: intradomain, eBGP, iBGP.
- All the non-border routers will be running two routing protocols: intradomain, iBGP.

Operations of External BGP

- The eBGP variation of BGP allows two physically connected border routers in two different ASs to form pairs of eBGP speakers and exchange messages.

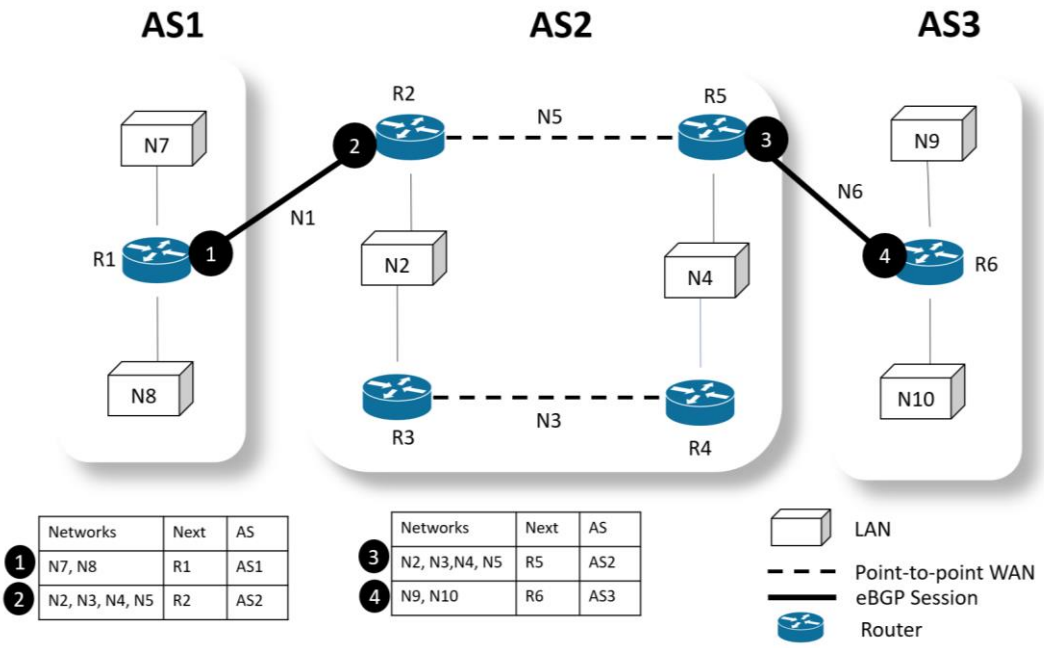


Figure – 2 eBGP operation

- The routers that are eligible in our example (figure-1) form two pairs R1-R2 and R5-R6 as shown in the figure-2.
- The connections between these pairs is established over three physical WANs: N1, N6.
- The circled number defines the sending router in each case.
    - Message number 1 is sent by router r1.
    - Message number 2 is sent by router r2.
    - Message number 3 is sent by router r5.
    - Message number 4 is sent by router r6.
- There are two problems that need to be addressed:
    - Some border routers do not know how to route a packet destined for non-neighbour ASs.
    - None of the non-border routers know how to route a packet destined for any networks in other ASs.
- To address these two problems, it is required to install iBGP protocol.

Operation of Internal BGP

- iBGP creates a session between any possible pair of routers inside an autonomous system.
    - If an AS has only one router, there cannot be an iBGP session. For example, we cannot create an iBGP session inside AS1 or AS3 in our internet.
    - If there are n routers in an autonomous system, there should be [n × (n − 1) / 2] iBGP sessions in that autonomous system (a fully connected mesh) to prevent loops in the system.
- Each router needs to advertise its own reachability to the peer.
- Following figure-3 shows the combination of eBGP and iBGP.

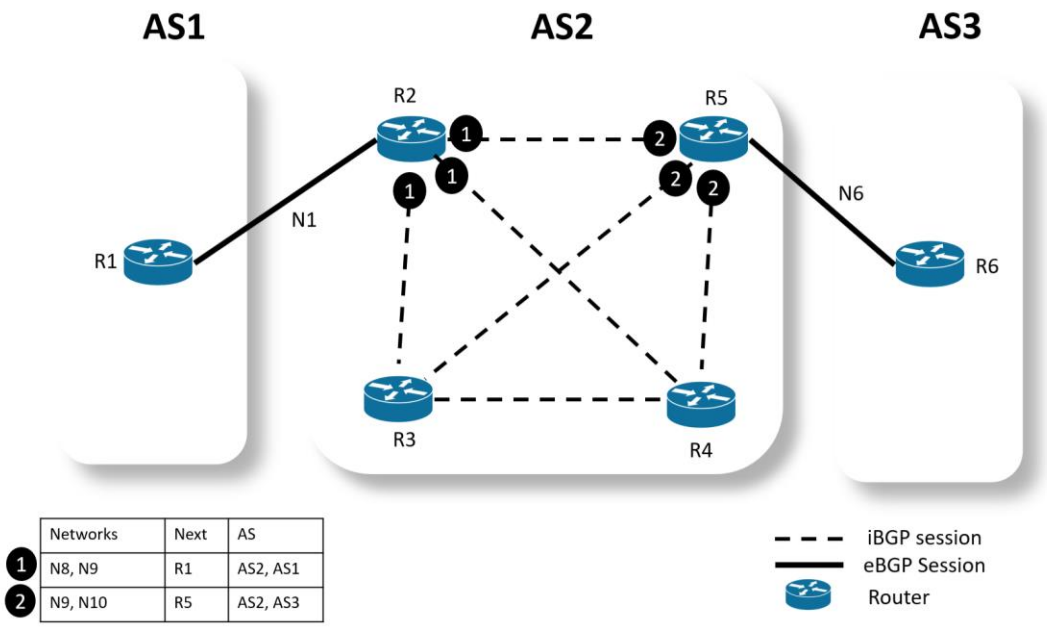


Figure – 3 Operations of iBGP

- Finalized BGP path tables are shown below.

ROUTER R1		
Networks	Next	AS
N2,N3,N4,N5	R2	AS1, AS2
N9,N10	R2	AS1, AS2, AS3

ROUTER R2		
Networks	Next	AS
N7,N8	R1	AS2,AS1
N9,N10	R5	AS2, AS3

ROUTER R3		
Networks	Next	AS
N7,N8	R2	AS2,AS1
N9,N10	R4	AS2, AS3

ROUTER R4		
Networks	Next	AS
N7,N8	R3	AS2,AS1
N9,N10	R5	AS2, AS3

ROUTER R5		
Networks	Next	AS
N7,N8	R2	AS2,AS1
N9,N10	R6	AS2, AS3

ROUTER R6		
Networks	Next	AS
N2, N3,N4,N5	R5	AS3,AS2
N7,N18	R5	AS2, AS3,AS1

Injection of Information into intradomain routing.

- The role of an interdomain routing protocol such as BGP is to help the routers inside the AS to augment their routing information.
- In other words, the path tables collected and organized by BPG are not used, per se, for routing packets; they are injected into intradomain forwarding tables (RIP or OSPF) for routing packets.
- Forwarding tables after injection from BGP are shown below.

ROUTER R1		
Destination	Next	Cost
N7	-	1
N8	-	1
0	R2	1

ROUTER R2		
Destination	Next	Cost
N2	-	1
N4	R5	2
N7	R1	1
N8	R1	1
N9	R5	2
N10	R5	2

ROUTER R3		
Destination	Next	Cost
N2	-	1
N4	R4	2
N7	R2	2
N8	R2	2
N9	R4	3
N10	R4	3

ROUTER R4		
Destination	Next	Cost
N4	-	1
N2	R3	1
N7	R3	3
N8	R3	3
N9	R5	2
N10	R5	2

ROUTER R5		
Destination	Next	Cost
N4	-	1
N2	R2	2
N7	R2	2
N8	R2	2
N9	R6	1
N10	R6	1

ROUTER R6		
Destination	Next	Cost
N9	-	1
N10	-	1
0	R5	1

Address Aggregation

- BGP may use address aggregation to reduce the size of forwarding tables.

Path attributes

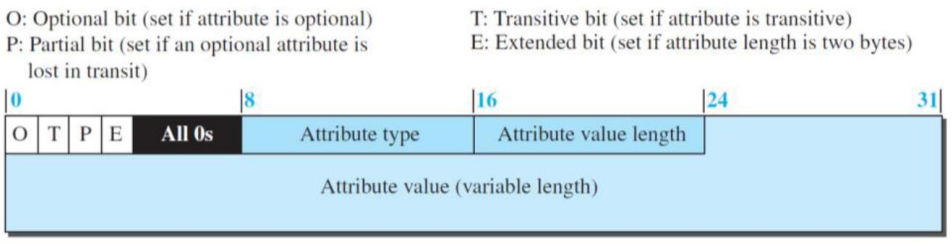
- BGP uses different seven path attributes. Path attributes play a critical role in BGP's operation by providing valuable information for route selection, filtering, handling, troubleshooting, and policy implementation.

Messages

- BGP uses four types of messages for communication between the BGP speaker across the ASs and inside the AS: open, update, keepalive, and notification.
- BGP is free from loops and count-to-infinity.

12. Explain path attributes of BGP.

- Interdomain routing needs more information about how to reach the final destination. In BGP these pieces are called path attributes.
- BGP allows a destination to be associated with up to seven path attributes.
- Path attributes are divided into two broad categories: well-known and optional.
- A well-known attribute must be recognized by all routers; an optional attribute need not be.
    - A well-known attribute can be mandatory, which means that it must be present in any BGP update message, or discretionary, which means it does not have to be.
    - An optional attribute can be either transitive, which means it can pass to the next AS, or intransitive, which means it cannot.
- All attributes are inserted after the corresponding destination prefix in an update message.
- The format of the path attributes is shown below.



- There are seven path attributes which are explain below.

ORIGIN (type 1).

- This is a well-known mandatory attribute, which defines the source of the routing information.
- This attribute can be defined by one of the three values: 1, 2, and 3.
- Value 1 means that the information about the path has been taken from an intradomain protocol (RIP or OSPF).
- Value 2 means that the information comes from BGP.
- Value 3 means that it comes from an unknown source.

AS-PATH (type 2).

- This is a well-known mandatory attribute, which defines the list of autonomous systems through which the destination can be reached.
- The AS-PATH attribute helps to prevent a loop. Whenever an update message arrives at a router that lists the current AS as the path, the router drops that path.

NEXT-HOP (type 3).

- This is a well-known mandatory attribute, which defines the next router to which the data packet should be forwarded.

MULT-EXIT-DISC (type 4).

- The multiple-exit discriminator is an optional intransitive attribute, which discriminates among multiple exit paths to a destination.
- For example, if a router has multiple paths to the destination with different values related to these attributes, the one with the lowest value is selected.
- Note that this attribute is intransitive, which means that it is not propagated from one AS to another.

LOCAL-PREF (type 5).

- The local preference attribute is a well-known discretionary attribute. It is normally set by the administrator, based on the organization policy.
- The routes the administrator prefers are given a higher local preference value
- For example, in an internet with five ASs, the administrator of AS1 can set the local preference value of 400 to the path AS1 → AS2 → AS5, the value of 300 to AS1 → AS3 → AS5, and the value of 50 to AS1 → AS4 → AS5. This means that the administrator prefers the first path to the second one and prefers the second one to the third one. This may be

a case where AS2 is the most secured and AS4 is the least secured AS for the administration of AS1. The last route should be selected if the other two are not available.

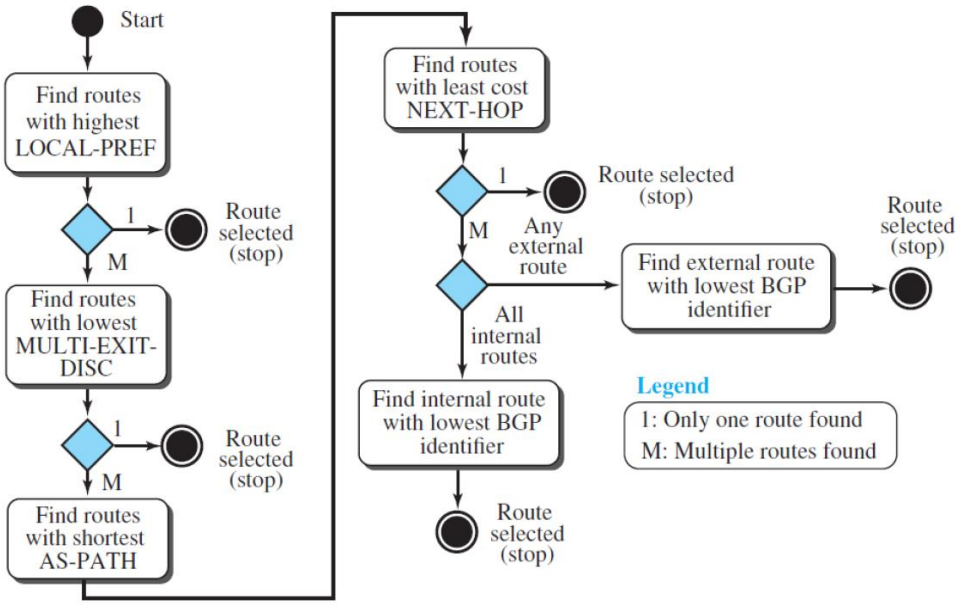
ATOMIC-AGGREGATE (type 6).

- This is a well-known discretionary attribute, which defines the destination prefix as not aggregate; it only defines a single destination network.
- This attribute has no value field, which means the value of the length field is zero.

AGGREGATOR (type 7).

- This is an optional transitive attribute.
- The AGGREGATOR attribute indicates that a BGP route is an aggregate route, and it provides information about the AS that performed the aggregation.

13. Draw flow diagram of Route Selection



14. Describe BGP messages.

- There are four types of BGP messages.
  - Open Message
  - Update Message
  - Keepalive Message
  - Notification
- Open Message.
  - To create a neighborhood relationship, a router running BGP opens a TCP connection with a neighbor and sends an open message.
- Update Message.
  - The update message is the heart of the BGP protocol.
  - It is used by a router to withdraw destinations that have been advertised previously, to announce a route to a new destination, or both.

- Keepalive Message.
    - The BGP peers that are running exchange keepalive messages regularly (before their hold time expires) to tell each other that they are alive.
- Notification.
    - A notification message is sent by a router whenever an error condition is detected or a router wants to close the session.

15. Differentiate RIP and OSPF.

RIP	OSPF
It implements distance-vector routing protocol.	It implements link-state routing protocol.
It uses hop count as a metric.	It uses Type of services such as bandwidth as a metric.
Convergence time is slow compared to OSPF.	Convergence time is quick compared to RIP
It is not well suited for large network.	It can be suitable for large network.
It operates in a flat routing structure.	It operates in a hierarchical routing structure.
Its administrative distance is 120	Its administrative distance is 110
It is less robust than OSPF.	It is more robust than RIP.

16. Differentiate OSPF and BGP4.

OSPF	BGP4
It implements link-state routing algorithm.	It implements path-vector routing algorithm.
It is an interior gateway routing protocol.	It is an exterior gateway routing protocol.
Its scalability is medium.	Its scalability is large.
It is less complex than BGP4.	It is more complex then OSPF.
Application: Enterprise network.	Application: Inter-AS routing.
It is Relatively secure, but not immune to attacks.	It is More complex, and more vulnerable to attacks

17. Differentiate RIP and BGP4.

RIP	BGP4
It implements distance-vector routing protocol.	It implements path-vector routing protocol.
It is an interior gateway routing protocol.	It is an exterior gateway routing protocol.
Its scalability is small to medium network.	Its scalability is large network.
It is less complex than BGP4.	It is more complex than RIP.
Application: Small Enterprise network	Application: Inter-AS routing.
It is Relatively secure, but not immune to attacks.	It is More complex, and more vulnerable to attacks