BUDDHA SERIES

(Unit Wise Solved Question & Answers)

Course – B.Tech.

College – Buddha Institute of Technology

(AKTU CODE-525)

Department: Computer Science & Allied

PROGRAM: AIML-DS

Subject: Computer Networks

(BCS 603)

Faculty Name: Mr. Shailesh Kumar Patel

Unit - 3

Q1. Explain ICMP BGP protocol and its application in real-world scenarios. **(AKTU 2022-23)**

Solution:

"ICMP BGP" refers to the combination of two network protocols: ICMP (Internet Control Message Protocol), which is used for error reporting and network diagnostics, and BGP (Border Gateway Protocol), which is responsible for routing information exchange between different autonomous systems (AS) on the internet; essentially, ICMP can be used to troubleshoot issues related to BGP routing by sending diagnostic messages when BGP encounters problems connecting to a network or exchanging routing information.

Key points about ICMP and BGP:

ICMP Function:

ICMP primarily sends error messages back to the source when a packet encounters an issue during transmission, like an unreachable host, time exceeded, or a network issue. It is used for error handling in the network layer, and it is primarily used on network devices such as routers. As different types of errors can exist in the network layer, so ICMP can be used to report these errors and to debug those errors.

BGP Function:

BGP is a path vector routing protocol that allows different autonomous systems to exchange routing information, determining the best path to reach a specific network.

How they work together:

BGP Path Issues:

When a BGP router encounters a problem while attempting to establish a routing path, it can use ICMP messages to notify the sending router about the issue.

Troubleshooting with ICMP:

Network administrators can use ICMP "ping" messages to test connectivity between different network segments and identify potential issues with BGP routing.

Example scenarios:

Unreachable Network:

If a BGP router tries to establish a route to a network that is unreachable, it might send an ICMP "Destination Unreachable" message back to the originating router, indicating the problem.

Route Flap Detection:

If a BGP router detects rapid changes in routing information (route flapping), it can use ICMP messages to notify other routers about the instability.

For example, if a packet of data is too large for a router, the router will drop the packet and send an ICMP message back to the original source for the data. A secondary use of ICMP protocol is to perform network diagnostics; the commonly used terminals utilities trace route and ping both operate using ICMP.

Q2. Illustrate the difference between IPv4 and IPv6. **(AKTU 2022-23)**

Solution:

Difference between IPv4 and IPv6:

S. No.	IPv4	IPv6
1	IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
2	It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
3	In IPv4 end to end, connection integrity is Unachievable	In IPv6 end-to-end, connection integrity is Achievable
4	It can generate 4.29×10^9 address space	The address space of IPv6 is quite large it can produce 3.4×10^{38} address space
5	The Security feature is dependent on the application	IPSEC is an inbuilt security feature in the IPv6 protocol

6	Address representation of IPv4 is in decimal	Address representation of IPv6 is in hexadecimal
7	Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation is performed only by the sender
8	In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are available and uses the flow label field in the header
9	In IPv4 checksum field is available	In IPv6 checksum field is not available
10	It has a broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available
11	In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
12	IPv4 has a header of 20-60 bytes.	IPv6 has a header of 40 bytes fixed
13	IPv4 can be converted to IPv6	Not all IPv6 can be converted to IPv4
14	IPv4 consists of 4 fields which are separated by addresses dot (.)	IPv6 consists of 8 fields, which are separated by a colon (:)
15	IPv4's IP addresses are divided into five different classes. Class A , Class B, Class C, Class D , Class E.	IPv6 does not have any classes of the IP address.
16	IPv4 supports VLSM (Variable Length subnet mask).	IPv6 does not support VLSM.
17	Example of IPv4: 66.94.29.13	Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

Q3. Write advantages of Next-generation IPV6 over IPV4. **(AKTU 2018-19, 2024-25)**

Solution:

Advantages:

The next-generation IP, or IPv6, has some advantages over IPv4 that can be summarized as follows:

Larger address space An IPv6 address is 128 bits long, compared with the 32-bit address of IPv4, this is a huge (2^{96}) increase in the address space.

Better header format IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper-layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

New options IPv6 has new options to allow for additional functionalities.

Allowance for extension IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

Support for resource allocation In IPv6, the type-of-service field has been removed, but a mechanism (called flow label) has been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.

Support for more security The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Q4. How is the BOOTP different from DHCP? **(AKTU 2018-19)**

Solution:

BOOTP is a network protocol for assigning an IP address to every piece of networking equipment and providing all the major configuration information, such as the default gateway and the subnet mask. It was

previously invented for the diskless workstations that needed to download their operating systems from a network server.

DHCP refers to Dynamic Host Configuration Protocol. This is a network protocol used for automating the process of assigning IP addresses and other network configurations to devices on a network. Devices request and obtain an IP address and configuration information from the DHCP server; hence, in this case, managing the network becomes easy and efficient.

Difference between BOOTP and DHCP:

S. No.	BOOTP	DHCP
1	BOOTP stands for Bootstrap Protocol.	While DHCP stands for Dynamic host configuration protocol.
2	BOOTP does not provide temporary IP addressing.	While DHCP provides temporary IP addressing for only limited amount of time.
3	BOOTP does not support DHCP clients.	While it support BOOTP clients.
4	In BOOTP, manual-configuration takes place.	While in DHCP, auto-configuration takes place.
5	BOOTP does not support mobile machines.	Whereas DHCP supports mobile machines.
6	BOOTP can have errors due to manual-configuration.	Whereas in DHCP errors do not occur mostly due to auto-configuration.

Q5. What is IP Addressing? How it is classified? How subnet addressing is performed? **(AKTU 2021-22)**

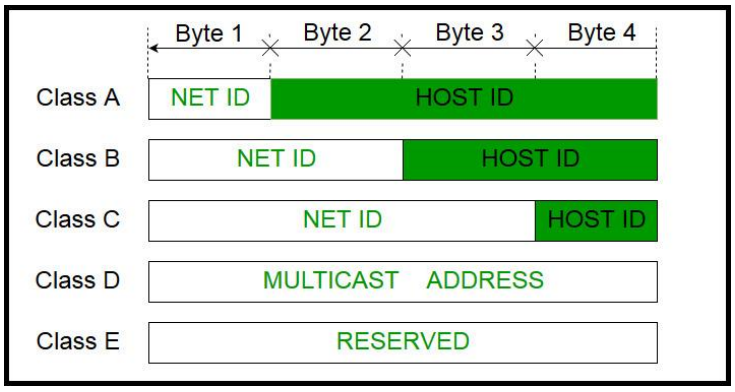
Solution:

An Internet Protocol (IP) address is the unique identifying number assigned to every device connected to the internet. An IP address definition is a numeric label assigned to devices that use the internet to communicate.

An IP address, or Internet Protocol address, is a unique string of numbers assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves as an identifier that allows devices to send and receive data over the network, ensuring that this data reaches the correct destination.

The 32-bit IP address is divided into five sub-classes. These are given below:

- Class A
- Class B
- Class C
- Class D
- Class E



A subnet mask is used to divide an IP address into two parts. One part identifies the host (computer), the other part identifies the network to which it belongs.

A subnet is like a smaller group within a large network. It is a way to split a large network into smaller networks so that devices present in one network can transmits data more easily.

How Does Subnetting Work?

The working of subnets starts in such a way that firstly it divides the subnets into smaller subnets. For communicating between subnets, routers are used. Each subnet allows its linked devices to communicate with each other. Subnetting for a network should be done in such a way that it does not affect the network bits.

An organization that is granted a large block of addresses may want to create clusters of networks (called subnets) and divide the addresses between the different subnets. The rest of the world still sees the organization as one entity; however, internally there are several subnets. All messages are sent to the router address that connects the organization to the rest of the Internet; the router routes the message to the appropriate subnets. The organization, however, needs to create small sub-blocks of addresses, each assigned to specific subnets. The organization has its own mask; each subnet must also have its own.

As an example, suppose an organization is given the block 17.12.40.0/26, which contains 64 addresses. The organization has three offices and needs to divide the addresses into three sub-blocks of 32, 16, and 16 addresses. We can find the new masks by using the following arguments:

- Suppose the mask for the first subnet is nl, then 2^{32-n1} must be 32, which means that n1 = 27.
- Suppose the mask for the second subnet is n2, then 2^{32-n2}must be 16, which means that n2 = 28.
- Suppose the mask for the third subnet is n3, then 2^{32-n3} must be 16, which means that n3 = 28.

This means that we have the masks 27, 28, 28 with the organization mask being 26. Following figure shows one configuration for the above scenario.

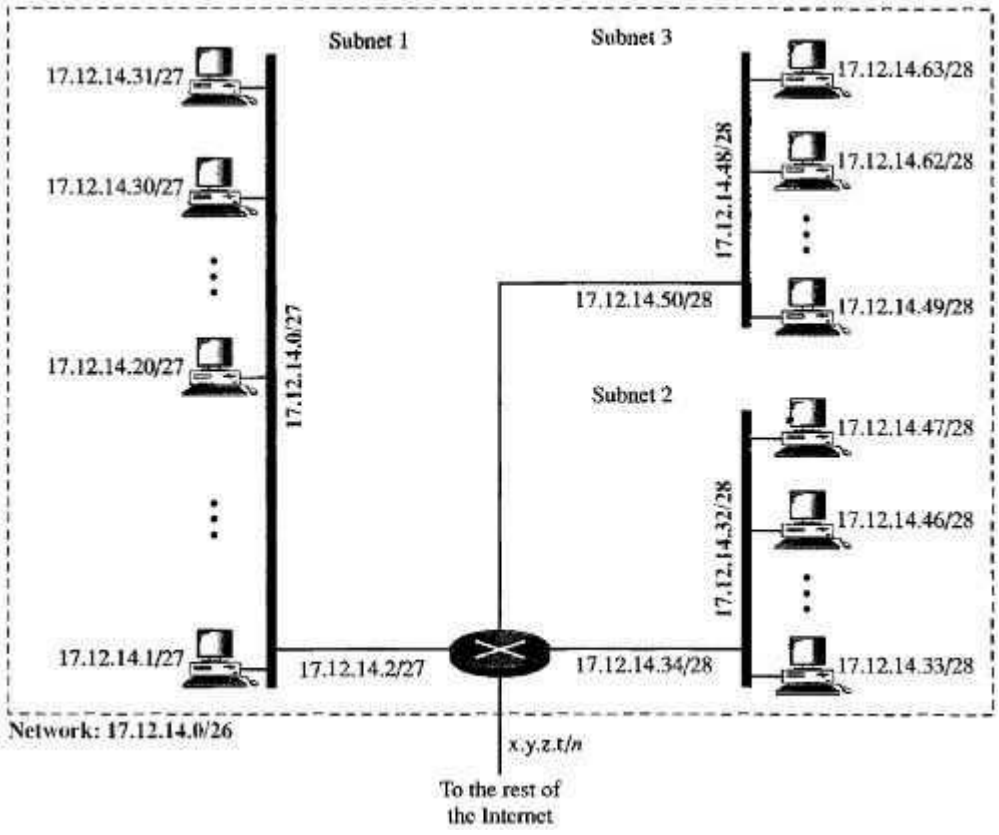


Figure: Configuration and addresses in a sub-netted network

a. In subnet 1, the address 17.12.14.29/27 can give us the subnet address if we use the mask /27 because
Host: 00010001 00001100 00001110 00011101
Mask: /27
Subnet: 00010001 00001100 00001110 00000000 → (17.12.14.0)
b. In subnet 2, the address 17.12.14.45/28 can give us the subnet address if we use the mask /28 because
Host: 00010001 00001100 00001110 00101101
Mask: /28
Subnet: 00010001 00001100 00001110 00100000 → (17.12.14.32)
c. In subnet 3, the address 17.12.14.50/28 can give us the subnet address if we use the mask /28 because
Host: 00010001 00001100 00001110 00110010
Mask: /28
Subnet: 00010001 00001100 00001110 00110000 → (17.12.14.48)

Q6. What is unicast routing? Discuss unicast routing protocols. **(AKTU 2018-19)**

Solution:

Unicast means the transmission from a single sender to a single receiver. It is a point-to-point communication between the sender and receiver. There are various unicast protocols such as TCP, HTTP, etc.

- TCP is the most commonly used unicast protocol. It is a connection-oriented protocol that relies on acknowledgment from the receiver side.
- HTTP stands for Hyper Text Transfer Protocol. It is an object-oriented protocol for communication.

Major Protocols of Unicast Routing

- **Distance Vector Routing:** Distance-Vector routers use a distributed algorithm to compute their routing tables.
- **Link-State Routing**: Link-State routing uses link-state routers to exchange messages that allow each router to learn the entire network topology.
- **Path-Vector Routing:** It is a routing protocol that maintains the path that is updated dynamically.

Distance Vector Routing:

In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, 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).

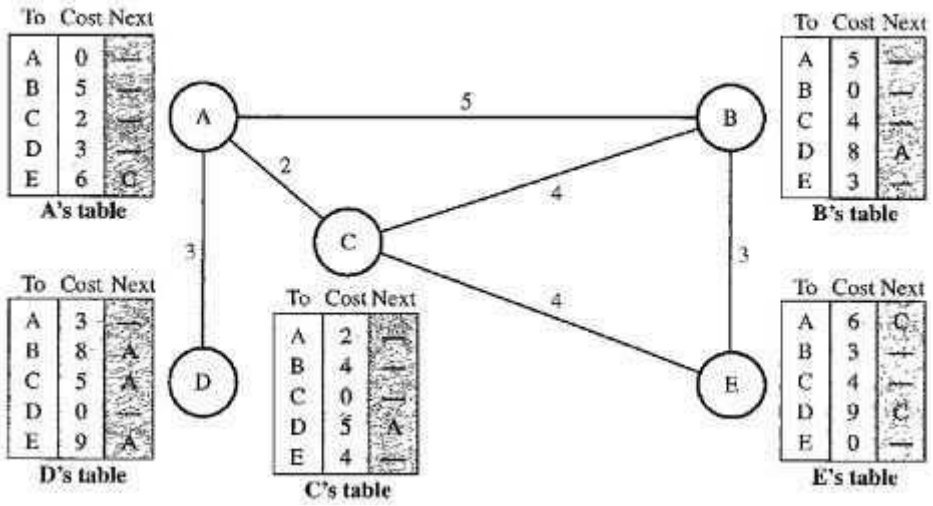


Figure A: Distance vector routing tables

We can think of nodes as the cities in an area and the lines as the roads connecting them. A table can show a tourist the minimum distance between cities. In Figure, we show a system of five nodes with their corresponding 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 in Figure A are stable; each node knows how to reach any other node and the cost. At the beginning, however, this is not the case. Each node can know only the distance between itself and its immediate neighbors, those directly connected to it. So for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors. Figure B shows the initial tables for each node.

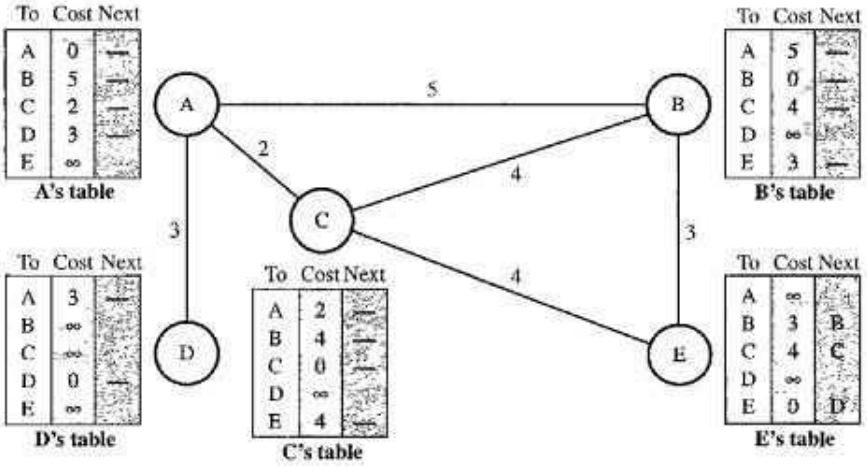


Figure B: Initialization of tables in distance vector routing

Sharing: The whole idea of distance vector routing is the sharing of information between neighbors. 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 each node D. In other words, nodes A and C, as immediate neighbors, can improve their routing tables if they help each other.

There is only one problem. How much of the table must be shared with each neighbor? A node is not aware of a neighbor's table. The best solution for each node is to send its entire table to the neighbor and let the neighbor decide what part to use and what part to discard. However, the third column of a table (next stop) is not useful for the neighbor. When the neighbor receives a table, this column needs

to be replaced with the sender's name. If any of the rows can be used, the next node is the sender of the table. A node therefore can send only the first two columns of its table to any neighbor. In other words, sharing here means sharing only the first two columns.

Updating: When a node receives a two-column table from a neighbor, it needs to update its routing table. Updating takes three steps:

- The receiving node needs to add the cost between itself and the sending node to each value in the second column. The logic is clear. If node C claims that its distance to a destination is x mi, and the distance between A and C is y mi, then the distance between A and that destination, via C, is x + y mi.
- The receiving node needs to add 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.
- The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

1) If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.
2) If the next-node entry is the same, the receiving node chooses the new row. For example, suppose node C has previously advertised a route to node X with distance 3. Suppose that 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 anymore. The new route has a distance of infinity.

Figure C shows how node A updates its routing table after receiving the partial table from node C.

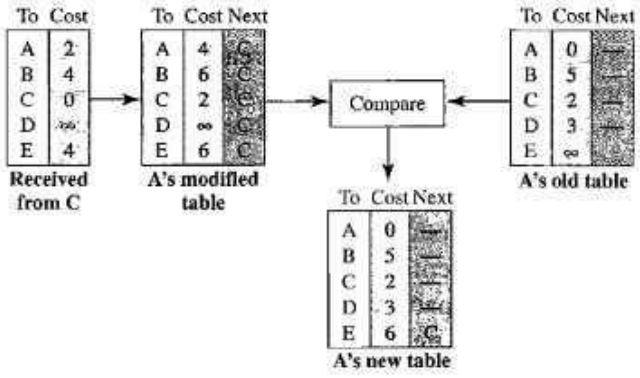


Figure C: Updating in distance vector routing

When to Share: The question now is, when does a node send its partial routing table (only two columns) to all its immediate neighbors? The table is sent both periodically and when there is a change in the table.

Periodic Update: A node sends its routing table, normally every 30 s, in a periodic update. The period depends on the protocol that is using distance vector routing.

Triggered Update: A node sends its two-column routing table to its neighbors anytime there is a change in its routing table. This is called a triggered update. The change can result from the following.

- A node receives a table from a neighbor, resulting in changes in its own table after updating.
- A node detects some failure in the neighboring links which results in a distance change to infinity.

Q7. Describe the problem of count to infinity associated with distance vector routing technique.

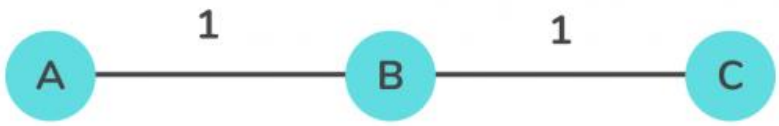
(AKTU 2016-17, 2024-25)

Solution:

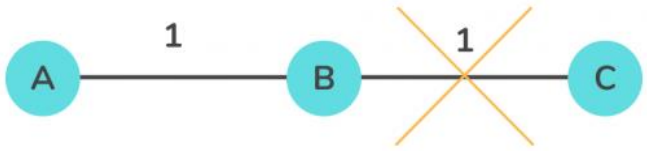
A Distance Vector Routing (DVR) requires that a router informs its neighbors of topology changes periodically. This algorithm is also well known in the Competitive Programming fraternity as the Bellman-Ford algorithm. The Distance Vector Routing (DVR) protocols have a major issue of Routing Loops because the Bellman-Ford algorithm cannot prevent loops. The Count to Infinity problem arises from the routing loop in this Distance Vector Routing (DVR) network. Such Routing Loops usually occurs when 2 routers send an update together at the same time or when an interface goes down.

The Count to Infinity Problem

The crux of the Count to Infinity problem is that if node A tells node B that it has a path somewhere, there is no way for node B to know if the path has node B as a part of it.



Consider the above diagram, for this setup, the Bellman-Ford algorithm will work such that for each router, they will have entries for each other. Router A will infer that it can reach B at a cost of 2 units, and B will infer that it can reach C at a cost of 1 unit.



Consider the case in the above diagram, where the connection between B and C gets disconnected. In this case, B will know that it cannot get to C at a cost of 1 anymore and update its table accordingly. However, it can be possible that A sends some information to B that it is possible to reach C from A at a cost of 2. Then, since B can reach A at a cost of 1, B will erroneously update its table that it can reach C via A at a cost of 1 + 2 = 3 units. A will then receive updates from B and update its costs to 4, and so on. Thus, the process enters into a loop of bad feedback and the cost shoots towards infinity. This entire situation is called the Count to Infinity problem.

Q8. What are different routing algorithms? Write the implementation of shortest path routing.

(AKTU 2002-3)

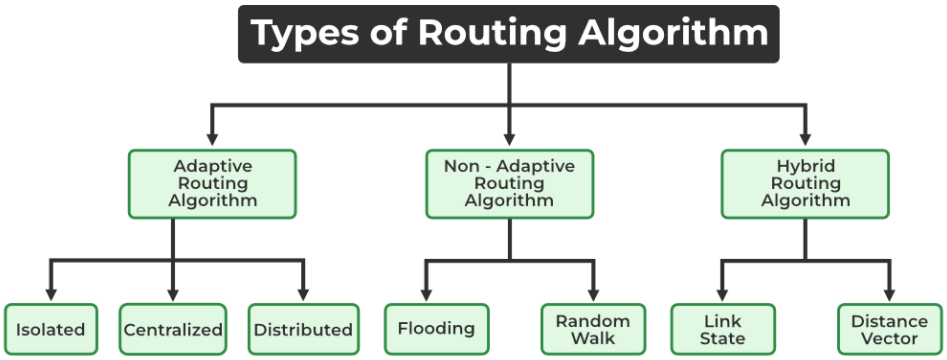
Solution:

Routing is the process of establishing the routes that data packets must follow to reach the destination. In this process, a routing table is created which contains information regarding routes that data packets follow. Various routing algorithms are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach the destination efficiently.

Classification of Routing Algorithms

The routing algorithms can be classified as follows:

- Adaptive Algorithms
- Non-Adaptive Algorithms
- Hybrid Algorithms



In between sending and receiving data packets from the sender to the receiver, it will go through many routers and subnets. So as a part of increasing the efficiency in routing the data packets and decreasing the traffic, we must find the shortest path.

It refers to the algorithms that help to find the shortest path between a sender and receiver for routing the data packets through the network in terms of shortest distance, minimum cost, and minimum time.

- It is mainly for building a graph or subnet containing routers as nodes and edges as communication lines connecting the nodes.
- Hop count is one of the parameters that is used to measure the distance.
- Hop count: It is the number that indicates how many routers are covered. If the hop count is 6, there are 6 routers/nodes and the edges connecting them.
- Another metric is a geographic distance like kilometers.
- We can find the label on the arc as the function of bandwidth, average traffic, distance, communication cost, measured delay, mean queue length, etc.

Common Shortest Path Algorithms

- Dijkstra's Algorithm
- Bellman Ford's Algorithm
- Floyd Warshall's Algorithm

Dijkstra's Algorithm

The Dijkstra's Algorithm is a greedy algorithm that is used to find the minimum distance between a node and all other nodes in a given graph. Here we can consider node as a router and graph as a network. It uses weight of edge .ie, distance between the nodes to find a minimum distance route.

Algorithm:

1: Mark the source node current distance as 0 and all others as infinity.

2: Set the node with the smallest current distance among the non-visited nodes as the current node.

3: For each neighbor, N, of the current node:

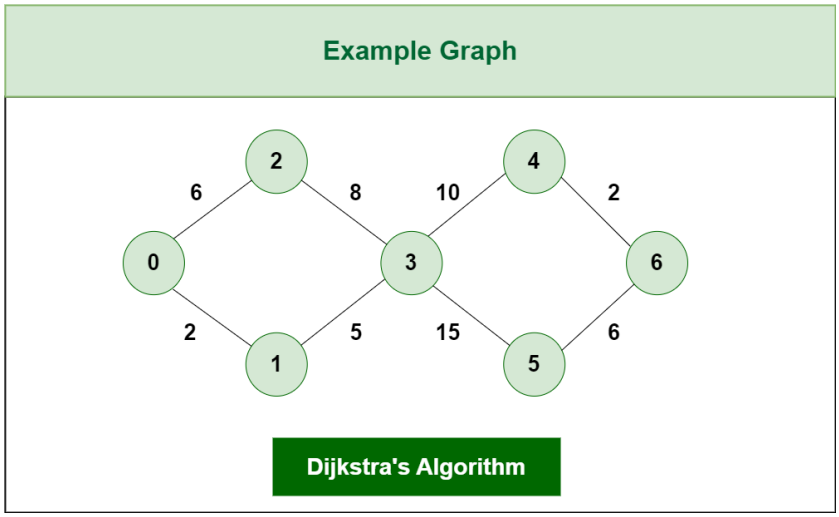
- Calculate the potential new distance by adding the current distance of the current node with the weight of the edge connecting the current node to N.
- If the potential new distance is smaller than the current distance of node N, update N's current distance with the new distance.

4: Make the current node as visited node.

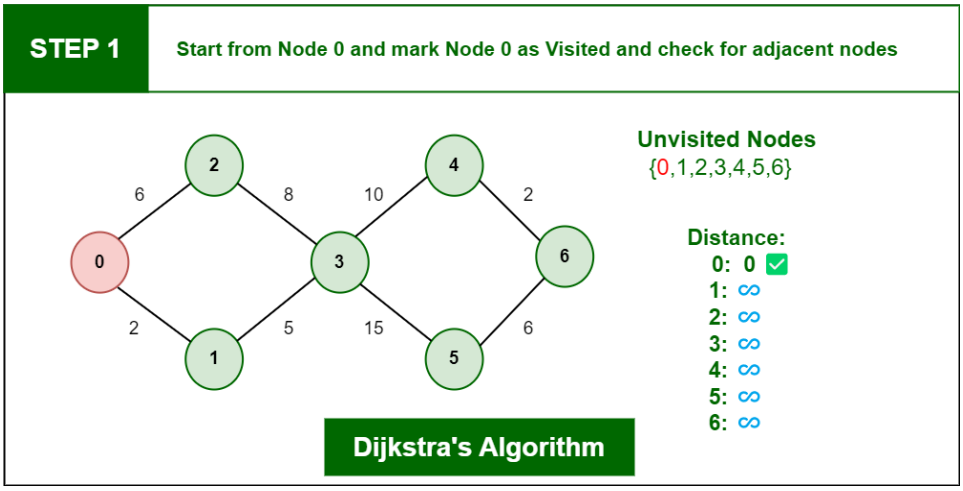
5: If we find any unvisited node, go to step 2 to find the next node which has the smallest current distance and continue this process.

Example:

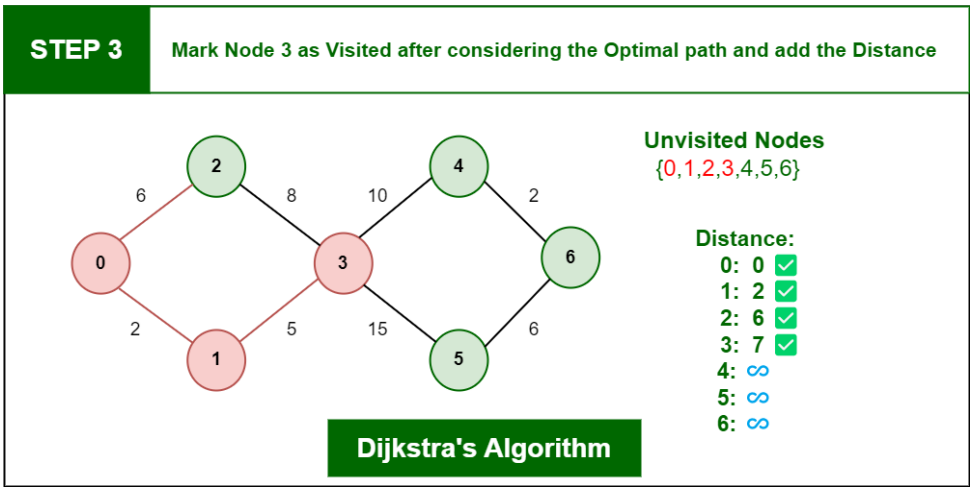
Consider the graph G:



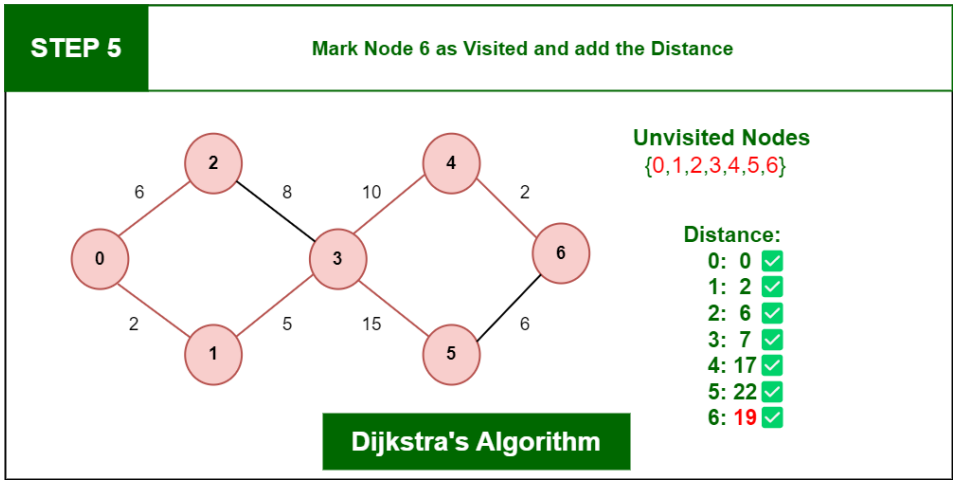
Now, we will start normalising graph one by one starting from node 0.



Nearest neighbour of 0 are 2 and 1 so we will normalize them first.



Similarly we will normalize other node considering it should not form a cycle and will keep track in visited nodes.



Q9. Discuss about the IP range of class A, B, C, and D. **(AKTU 2021-22)**

Solution:

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Q10. Explain distance vector routing with working example in detail. **(AKTU 2021-22)**

Solution:

Distance Vector Routing:

In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, 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).

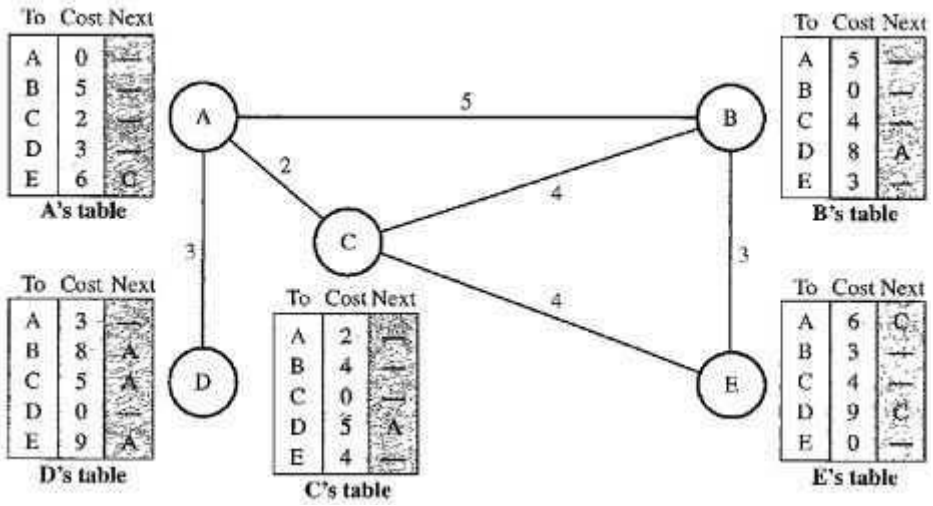


Figure A: Distance vector routing tables

We can think of nodes as the cities in an area and the lines as the roads connecting them. A table can show a tourist the minimum distance between cities. In Figure, we show a system of five nodes with their corresponding 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 in Figure A are stable; each node knows how to reach any other node and the cost. At the beginning, however, this is not the case. Each node can know only the distance between itself and its immediate neighbors, those directly connected to it. So for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors. Figure B shows the initial tables for each node.

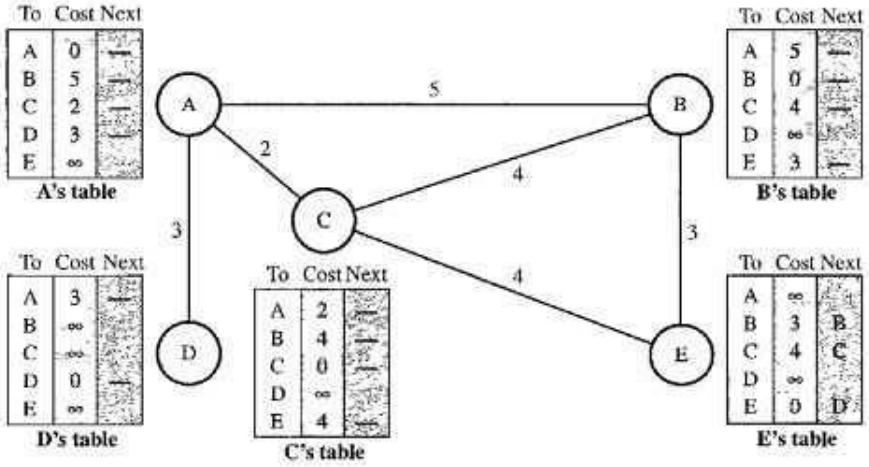


Figure B: Initialization of tables in distance vector routing

Sharing: The whole idea of distance vector routing is the sharing of information between neighbors. 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 each node D. In other words, nodes A and C, as immediate neighbors, can improve their routing tables if they help each other.

There is only one problem. How much of the table must be shared with each neighbor? A node is not aware of a neighbor's table. The best solution for each node is to send its entire table to the neighbor and let the neighbor decide what part to use and what part to discard. However, the third column of a table (next stop) is not useful for the neighbor. When the neighbor receives a table, this column needs

to be replaced with the sender's name. If any of the rows can be used, the next node is the sender of the table. A node therefore can send only the first two columns of its table to any neighbor. In other words, sharing here means sharing only the first two columns.

Updating: When a node receives a two-column table from a neighbor, it needs to update its routing table. Updating takes three steps:

- The receiving node needs to add the cost between itself and the sending node to each value in the second column. The logic is clear. If node C claims that its distance to a destination is x mi, and the distance between A and C is y mi, then the distance between A and that destination, via C, is x + y mi.
- The receiving node needs to add 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.
- The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

3) If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.
4) If the next-node entry is the same, the receiving node chooses the new row. For example, suppose node C has previously advertised a route to node X with distance 3. Suppose that 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 anymore. The new route has a distance of infinity.

Figure C shows how node A updates its routing table after receiving the partial table from node C.

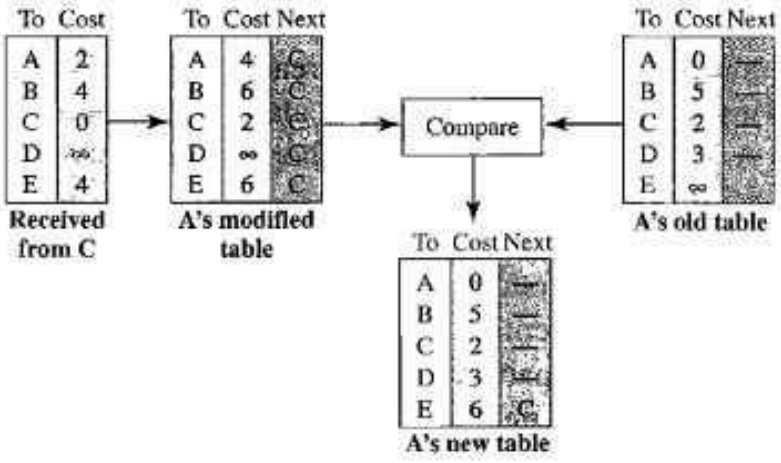


Figure C: Updating in distance vector routing

When to Share: The question now is, when does a node send its partial routing table (only two columns) to all its immediate neighbors? The table is sent both periodically and when there is a change in the table.

Periodic Update: A node sends its routing table, normally every 30 s, in a periodic update. The period depends on the protocol that is using distance vector routing.

Triggered Update: A node sends its two-column routing table to its neighbors anytime there is a change in its routing table. This is called a triggered update. The change can result from the following.

- A node receives a table from a neighbor, resulting in changes in its own table after updating.
- A node detects some failure in the neighboring links which results in a distance change to infinity.

Q11. Explain Routing Information protocol in brief. **(AKTU 2003-4)**

Solution:

Routing Information Protocol (RIP) is a routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network.

The Routing Information Protocol is a distance vector routing protocol that helps routers determine the best path to transfer data packets across the network. RIP works on the Network layer of the OSI model. It uses hop count as its metric for determining the best path, but the maximum hop count allowed in the RIP is 15. Routing Information Protocol is mostly used in small to medium-sized networks.

Hop count is the number of routers occurring between the source and destination network. The path with the lowest hop count is considered the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the hops allowed in a path from source to destination. The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

Features of RIP

- Updates of the network are exchanged periodically.
- Updates (routing information) are always broadcast.
- Full routing tables are sent in updates.
- Routers always trust routing information received from neighbor routers. This is also known as routing on rumors.

How Routing Information Protocol Works?

Routing Information Protocol uses Distance Vector Routing to put the packets to its destination. In RIP, Each router maintains a routing table where the distance to each destination is mentioned. RIP shares its routing tables to neighboring routers at an interval of 30 seconds through broadcasting. Upon receiving the data, each router updates the table according to that. If a router receives a route and it is shorter than the previous one, then router simply updates the data in the table.

RIP has a limit of 15 hops, that is, if some route requires more than 15 hops, then that path in unreachable. It helps in limiting the size of network that a router can handle. In case, if a route is not updated in six successful cycles (180 seconds) in the routing table, the RIP will drop that route and inform rest of the network about the same.

Routing Information Protocol is simple to implement, but it is more efficient for smaller networks, for larger networks, protocols like OSPF or EIGRP are preferred.

Advantages of RIP

- **Simplicity:** RIP is a relatively simple protocol to configure and manage, making it an ideal choice for small to medium-sized networks with limited resources.
- **Easy implementation:** RIP is easy to implement, as it does not require much technical expertise to set up and maintain.
- **Convergence:** RIP is known for its fast convergence time, meaning that it can quickly adapt to changes in network topology and route packets efficiently.
- **Automatic updates:** RIP automatically updates routing tables at regular intervals, ensuring that the most up-to-date information is being used to route packets.
- **Low bandwidth overhead:** RIP uses a relatively low amount of bandwidth to exchange routing information, making it an ideal choice for networks with limited bandwidth.
- **Compatibility:** RIP is compatible with many different types of routers and network devices, making it easy to integrate into existing networks.

Disadvantages of RIP

- **Limited scalability:** RIP has limited scalability, and it may not be the best choice for larger networks with complex topologies. RIP can only support up to 15 hops, which may not be sufficient for larger networks.
- **Slow convergence:** While RIP is known for its fast convergence time, it can be slower to converge than other routing protocols. This can lead to delays and inefficiencies in network performance.
- **Routing loops:** RIP can sometimes create routing loops, which can cause network congestion and reduce overall network performance.
- **Limited support for load balancing:** RIP does not support sophisticated load balancing, which can result in suboptimal routing paths and uneven network traffic distribution.
- **Security vulnerabilities:** RIP does not provide any native security features, making it vulnerable to attacks such as spoofing and tampering.
- **Inefficient use of bandwidth:** RIP uses a lot of bandwidth for periodic updates, which can be inefficient in networks with limited bandwidth.

Limitations of RIP

On using RIP, there can be certain limitations. Some of them are mentioned below:

- **Increase in Network Traffic:** RIP increases traffic to the neighboring routers as it regularly performs updates on them.
- **Limitation of Hop Count:** Since, RIP has a maximum hop count of 15, therefore it is not suitable for large networks.
- **Difference in Closest Path and Shortest Path:** Since, RIP does not consider all factors while calculating shortest path, therefore, it creates a difference between closest path and shortest path.