Network Layer

Subnetting

- **Subnetting** is the practice of dividing a network into two or smaller networks.
- Subnetting is the process of stealing bits from the HOST part of an IP address in order to divide the larger network into smaller sub-networks called subnets.
- After subnetting, we end up with NETWORK SUBNET HOST fields.
- We always reserve an IP address to identify the subnet and another one to identify the broadcast subnet address.

Why Use Subnetting?

Conservation of IP addresses:

- Imagine having a network of 20 hosts. Using a Class C network will waste a lot of IP addresses (254-20=234).
- Breaking up large networks into smaller parts would be more efficient and would conserve a great amount of addresses.

Why Use Subnetting?

- **Reduced network traffic:** The smaller networks that created the smaller broadcast domains are formed, hence less broadcast traffic on network boundaries.
- **Simplification:** Breaking large networks into smaller ones could simplify fault troubleshooting by isolating network problems down to their specific existence.

The Concept of Subnetting

In upcoming Lecture…….

Routing

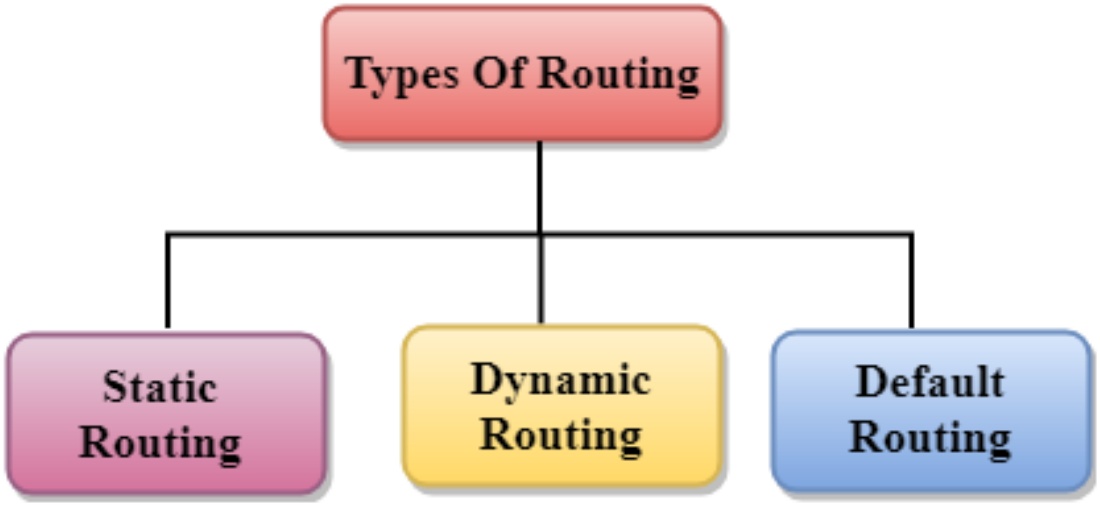
- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.

Routing

- The routing protocols use the metric to determine the best path for the packet delivery.
- The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

Routing Types

Routing can be classified into three categories:



Static Routing

- Static Routing is also known as Non-adaptive Routing.
- It is a technique in which the administrator manually adds the routes in a routing table.
- A Router can send the packets for the destination along the route defined by the administrator.
- In this technique, routing decisions are not made based on the **traffic** condition or topology of the networks

Disadvantages of Static Routing

- For a large network, it becomes a very difficult task to add each route manually to the routing table.
- The system administrator should have a good knowledge of a topology as he has to add each route manually.

Default Routing

- Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing.
- Default Routing is used when networks deal with the single exit point.
- It is also useful when the bulk of transmission networks have to transmit the data to the same hp device.
- When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table.

Dynamic Routing

- It is also known as Adaptive Routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the traffic condition or topology of the network.
- Changes routing table according to the change in topology.
- Dynamic protocols are used to discover the new routes to reach the destination.
- In Dynamic Routing, Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) are the protocols used to discover the new routes.
- If any route goes down, then the automatic adjustment will be made to reach the destination.

The Dynamic protocol should have the following features:

- All the routers must have the same dynamic routing protocol in order to exchange the routes.
- If the router discovers any change in the condition or topology, then router broadcast this information to all other routers.

Advantages of Dynamic Routing

- It is easier to configure.
- It is more effective in selecting the best route in response to the changes in the condition or topology.

Disadvantages of Dynamic Routing

- It is more expensive in terms of CPU and bandwidth usage.
- It is less secure as compared to default and static routing.

Shortest path algorithm

- In computer networks, the shortest path algorithms aim to find the optimal paths between the network nodes so that routing cost is minimized.
- They are direct applications of the shortest path algorithms proposed in graph theory.

Explanation

Consider that a network comprises of N vertices (nodes or network devices) that are connected by M edges (transmission lines). Each edge is associated with a weight, representing the physical distance or the transmission delay of the transmission line. The target of shortest path algorithms is to find a route between any pair of vertices along the edges, so the sum of weights of edges is minimum. If the edges are of equal weights, the shortest path algorithm aims to find a route having minimum number of hops.

Common Shortest Path Algorithms

Some common shortest path algorithms are −

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

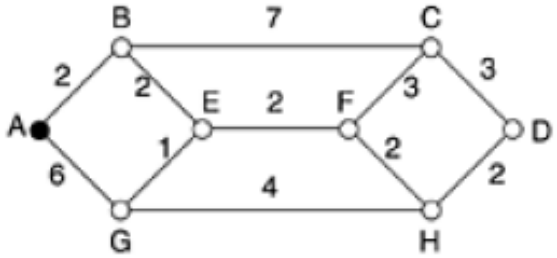
Dijkstra’s Algorithm

- Basically, the Dijkstra’s algorithm begins from the node to be selected, the source node, and it examines the entire graph to determine the shortest path among that node and all the other nodes in the graph.
- Dijkstra's algorithm also allows us to find the shortest path between any two vertices of a graph.
- It differs from the minimum spanning tree because the shortest distance between two vertices might not include all the vertices of the graph.

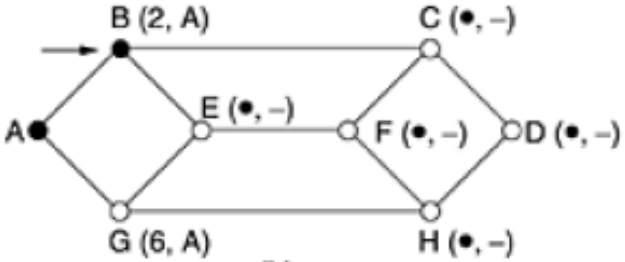
Dijkstra's Algorithm

267 Page Book

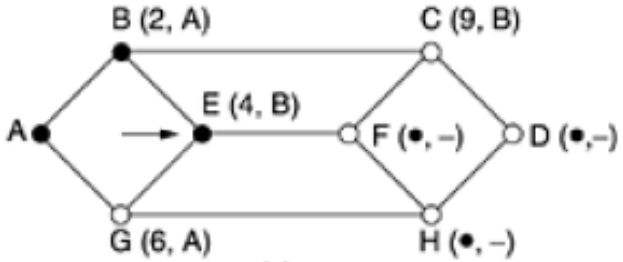
https://www.programiz.com/dsa/dijkstra-algorithm



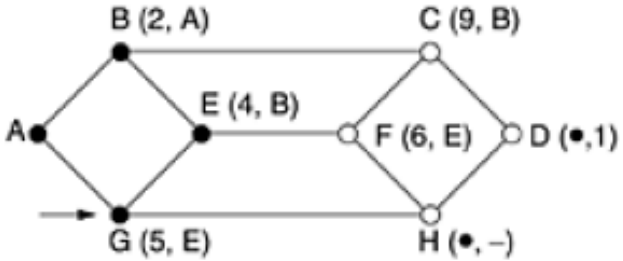
(a)



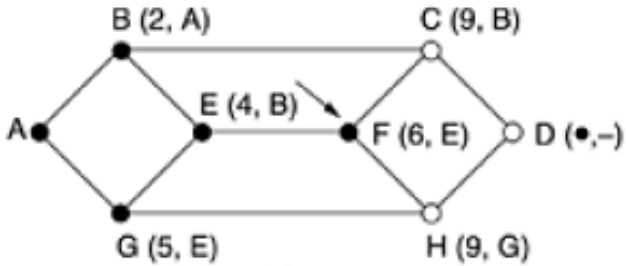
(b)



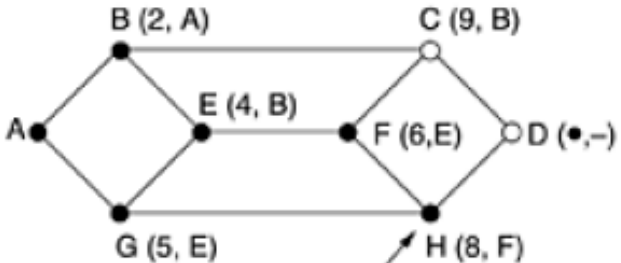
(c)



(d)



(e)



(f)

Flooding

- Flooding is a **non-adaptive routing technique** following this simple method:

when a data packet arrives at a router, it is **sent to all the outgoing links** except the one it has arrived on.

- For example, let us consider the network in the figure, having six routers that are connected through transmission lines.

Using flooding technique −

•An incoming packet to A, will be sent to B, C and D.

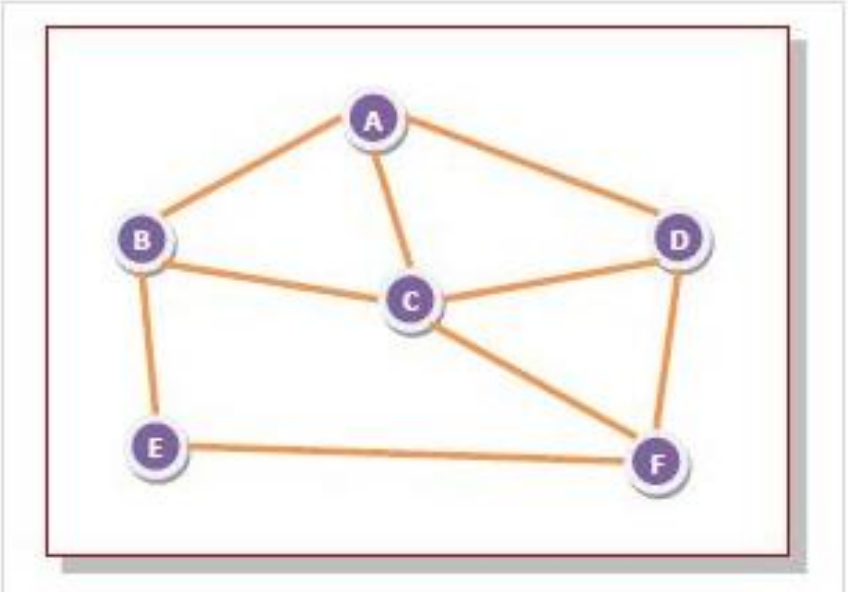
•B will send the packet to C and E.

•C will send the packet to B, D and F.

•D will send the packet to C and F.

•E will send the packet to F.

•F will send the packet to C and E.



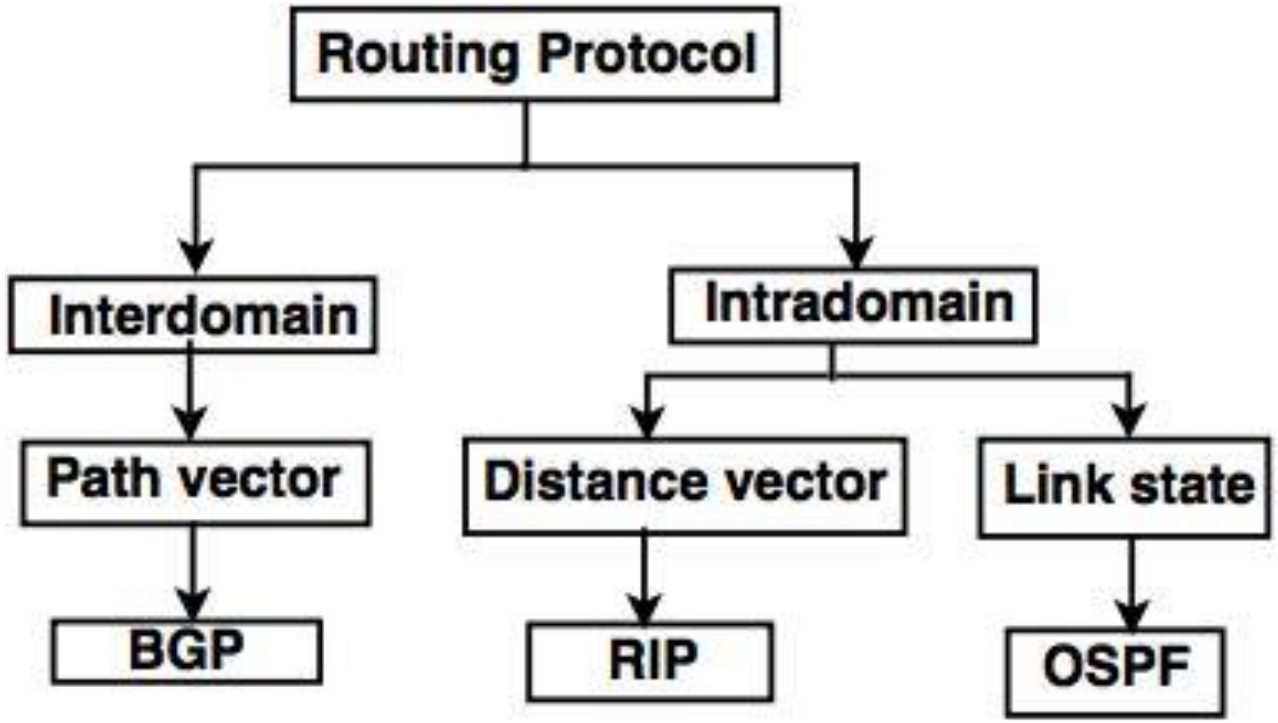
Types of Flooding

Flooding may be of three types −

- **Uncontrolled flooding** − Here, each router unconditionally transmits the incoming data packets to all its neighbours.
- **Controlled flooding** − They use some methods to control the transmission of packets to the neighbouring nodes. The two popular algorithms for controlled flooding are Sequence Number Controlled Flooding (SNCF) and Reverse Path Forwarding (RPF).
- **Selective flooding** − Here, the routers don't transmit the incoming packets only along those paths which are heading towards approximately in the right direction, instead of every available paths.

Routing	Flooding
--> Routing table is required.	--> No routing table is required.
--> May give shortest path.	--> Always gives shortest path.
--> Less reliable.	--> More reliable.
--> Traffic is less.	--> Traffic is high.
--> No duplicate packets.	--> Duplicate packets are present

Routing Protocol



Classification of routing protocol

Distance Vector Routing

- Dynamic routing protocols uses metric, cost and hop count to identify the best path from the path available for destination network. There are mainly 3 different classes of routing protocols:

1. **Distance Vector Routing Protocol –**

- These protocols selects best path in the basis of hop counts to reach a destination network in the particular direction.
- Dynamic protocol like **RIP (Routing Information Protocol)** is an example of distance vector routing protocol.
- Hop count is each router which occurs in between the source and the destination network.
- The path with the least hop count will be chosen as the best path.

- It is a dynamic routing algorithm in which each router computes distance between itself and each possible destination i.e. its immediate neighbors.
- The router share its knowledge about the whole network to its neighbors and accordingly updates table based on its neighbors.
- The sharing of information with the neighbors takes place at regular intervals.
- It makes use of **Bellman Ford Algorithm** for making routing tables.

Link State Routing Protocol

2. Link State Routing Protocol –

- These protocols know more about the Internetwork than any other distance vector routing protocol.
- OSPF is an example of link state routing protocol.

Link State Routing Protocol

- It is a dynamic routing algorithm in which each router shares knowledge of its neighbors with every other router in the network.
- A router sends its information about its neighbors only to all the routers through flooding.
- Information sharing takes place only whenever there is a change.
- It makes use of **Dijkastra's Algorithm** for making routing tables.

Distance Vector Routing	Link State Routing
--> Bandwidth required is less due to local sharing, small packets and no flooding.	--> Bandwidth required is more due to flooding and sending of large link state packets.
--> Based on local knowledge since it updates table based on information from neighbors.	--> Based on global knowledge i.e. it have knowledge about entire network.
--> Make use of Bellman Ford algo	--> Make use of Dijkastra's algo
--> Traffic is less	--> Traffic is more
--> Converges slowly i.e. good news spread fast and bad news spread slowly.	--> Converges faster.
--> Count to infinity problem.	--> No count to infinity problem.
--> Persistent looping problem i.e. loop will there forever.	--> No persistent loops, only transient loops.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

Address Resolution Protocol (ARP)

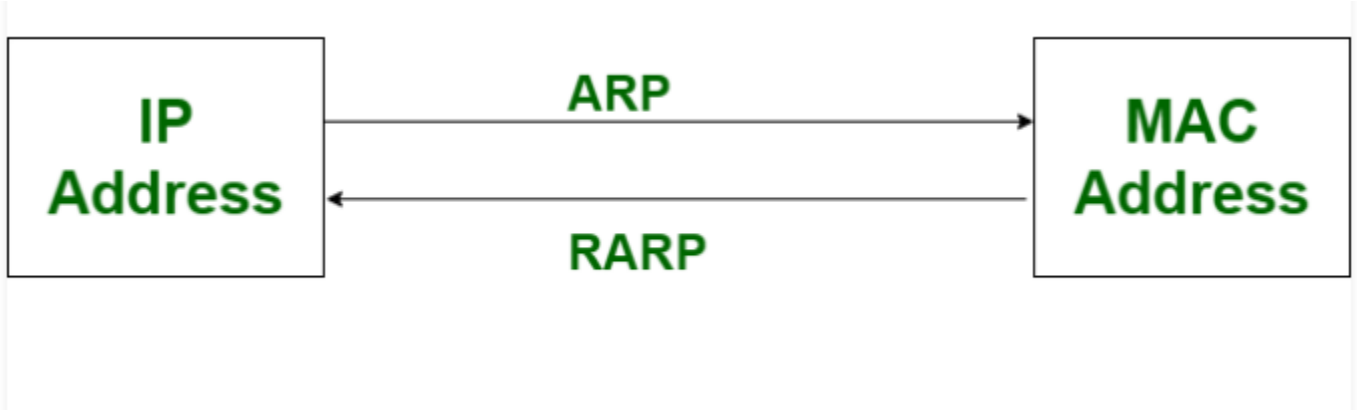
- ARP stands for **Address Resolution Protocol**, which is used to find the MAC address of the device from its known IP address.
- This means, the source device already knows the IP address but not the MAC address of the destination device.
- The MAC address of the device is required because you cannot communicate with a device in a local area network (Ethernet) without knowing its MAC address.
- So, the Address Resolution Protocol helps to obtain the MAC address of the destination device.

Address Resolution Protocol (ARP)

- The purpose of ARP is to convert the 32-bit logical address (IPv4 address) to the 48-bit physical address (MAC address).
- This protocol works between layer 2 and layer 3 of the OSI model. The MAC address resides at layer 2, which is also known as the data link layer and IP address resides at layer 3, this layer is also known as the network layer.

Reverse Address Resolution Protocol (RARP)

- RARP, (48-bit) MAC address of 48 bits mapped into (32-bit) IP address.



ICMP Protocol

- The ICMP stands for **Internet Control Message Protocol**. It is a network layer protocol.
- 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.
- For example, some sender wants to send the message to some destination, but the router couldn't send the message to the destination. In this case, the router sends the message to the sender that I could not send the message to that destination.

ICMP Protocol

- The IP protocol does not have any error-reporting or error-correcting mechanism, so it uses a message to convey the information.
- For example, if someone sends the message to the destination, the message is somehow stolen between the sender and the destination.
- If no one reports the error, then the sender might think that the message has reached the destination.
- If someone in-between reports the error, then the sender will resend the message very quickly.