UNIT - III

Network Layer

Routing

Functions of Net Work layer

1. Routing
2. Congestion Control

Routing algorithms

Shortest Path Routing,

Flooding, Distance Vector Routing,

Link State Routing

Routing

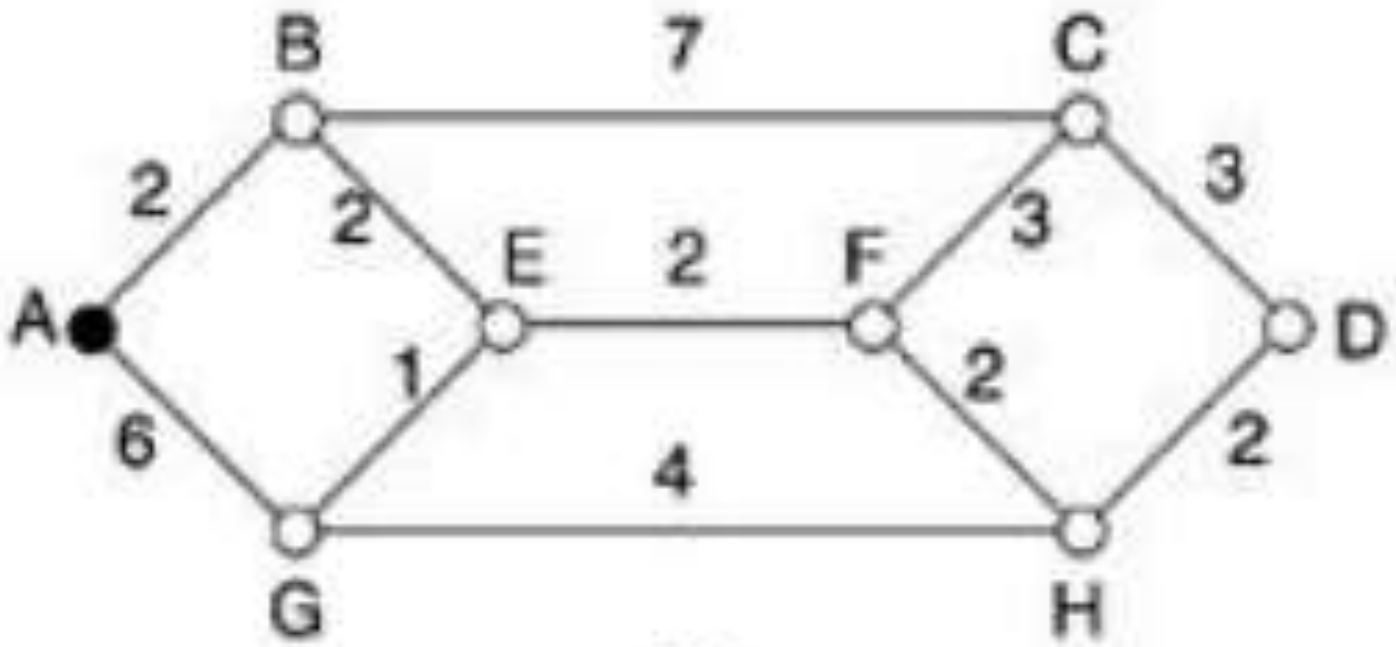
- The main function of the network layer is routing packets from the source machine to the destination machine.
- Routing algorithm can be grouped into two major classes.

  Non adaptive and

  Adaptive algorithms.

Non Adaptive	Adaptive
1.Routing decisions are not based on measurements or estimates of the current traffic and topology.	1.Routing decisions are based on measurements of the current traffic and topology.
2. The route is computed well in advance.	2.The route is computed depends on situation.
3. When the network is booted the routers are downloaded.	3. The routers are not downloaded.
4. This is a static routing.	4. This is a dynamic routing.

SHORTEST PATH ROUTING



(a)

,G,H

- In the diagram
  -- A,B,C,D,E,F Represent the hops(nodes)
  -- The numbers indicate a metric.

SHORTEST PATH ROUTING

- One-way of measuring path length is the number of hops.
  - Using this metric, the paths ABC and ABE are equally long. (two hops).
- Another metric is the Geographic distance in Kilometers.
  - ABC is clearly longer than ABE.

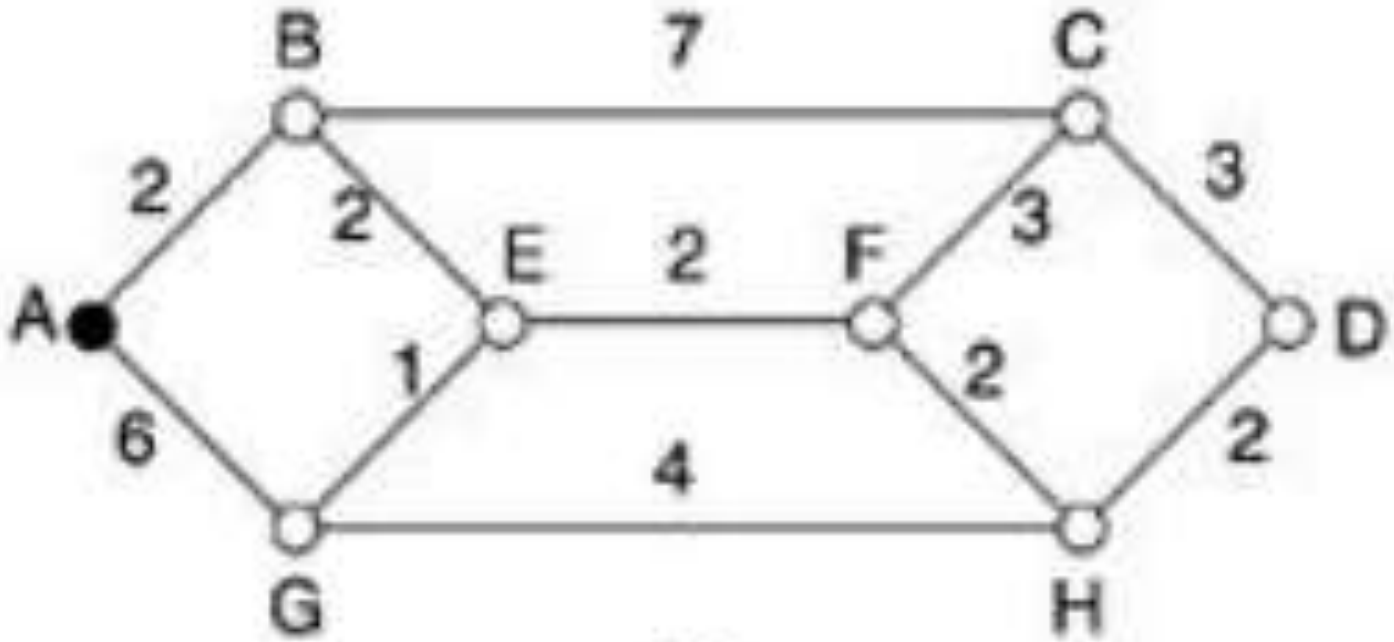
SHORTEST PATH ROUTING

- Many other metrics are also possible besides hops and physical distance.
- Each are could be labeled with the mean queuing and transmission delay for some standard test packets as determined by hourly test runs.
- With this graph labeling, the shortest path is the fastest path, rather than the path with the fewest arc or kilometers.

- In most general case, the labels on the arcs could be computed as a function of

1. the distance,
2. bandwidth,
3. average traffic,
4. communication cost,
5. mean queue length,
6. measured delay and other factors.

- The shortest path can be calculated using Dijkstra method.
- Each node is labeled with its distance from the source along the best known path.
- Initially, no paths are known, so all nodes are labeled with infinity.
- As the algorithm proceeds and paths are found, the labels may change, reflecting better paths.
- Initially all labels are tentative.
- When it is discovered that a label represents the shortest path from the source to that node, it is made permanent and never changed thereafter.



(a)

In the above diagram, let the weights represents the distance.

To find out the shortest path from A to D.

We start by marking A as permanent.

Then examine each one with the distance to A, relabeling each one with the distance to A.

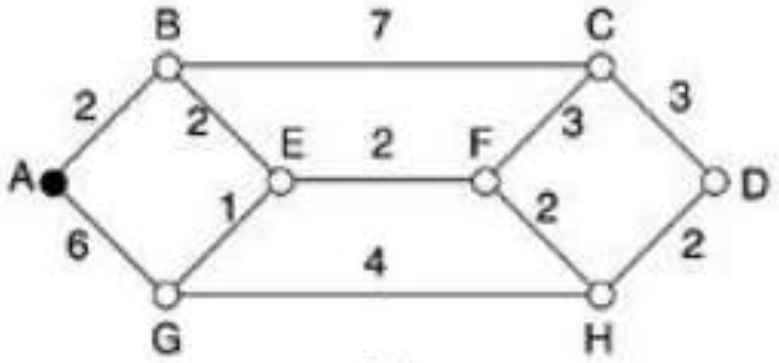
Whenever a node is relabeling,label it with the node from which the probe was made.

After examine each of the nodes adjacent to A, examine all the tentatively labeled nodes in the whole graph and make the one with the smallest label permanent.

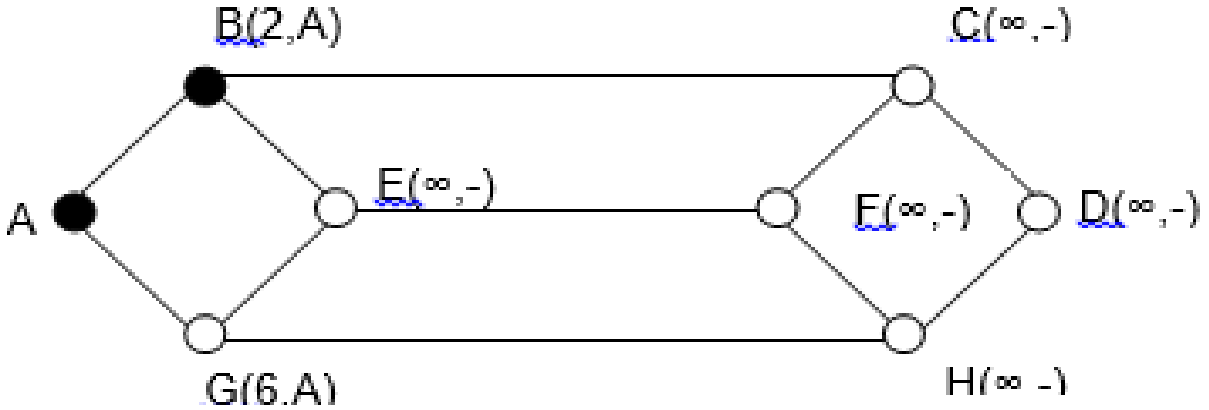
This one becomes the new working node.

The same procedure is adopted to all the nodes and the shortest path is found.

Shortest Path Routing:

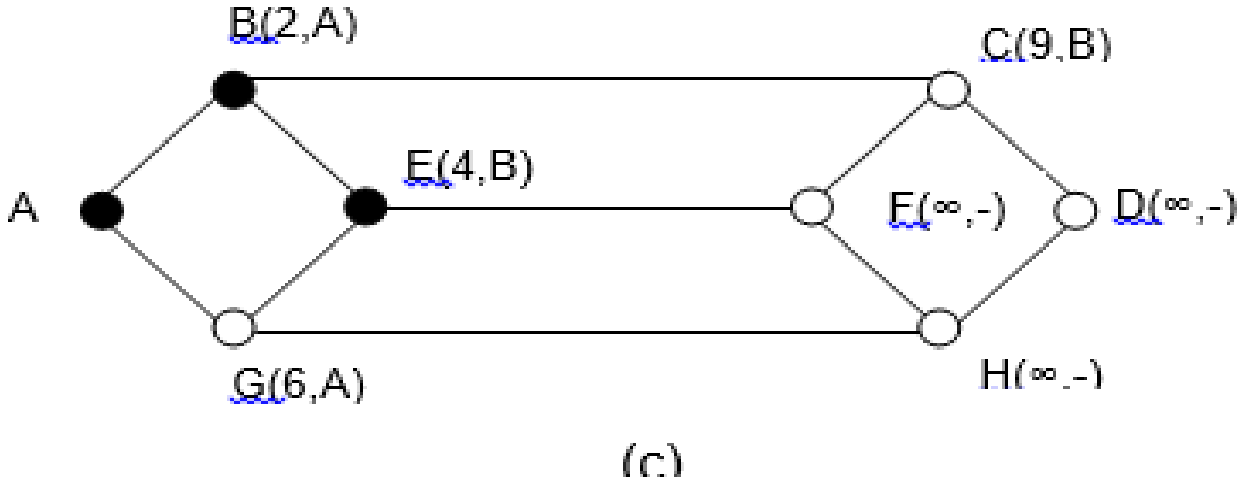


(a)

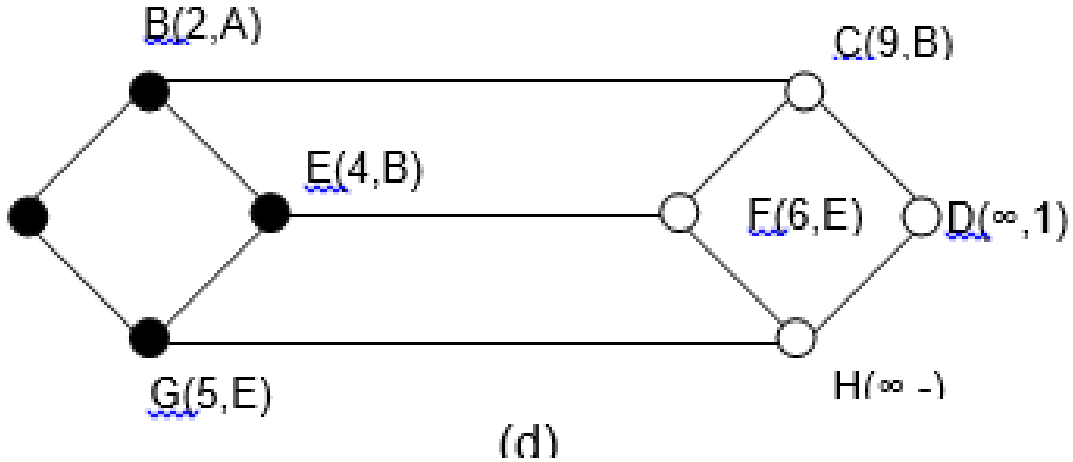


(b)

Shortest Path Routing:

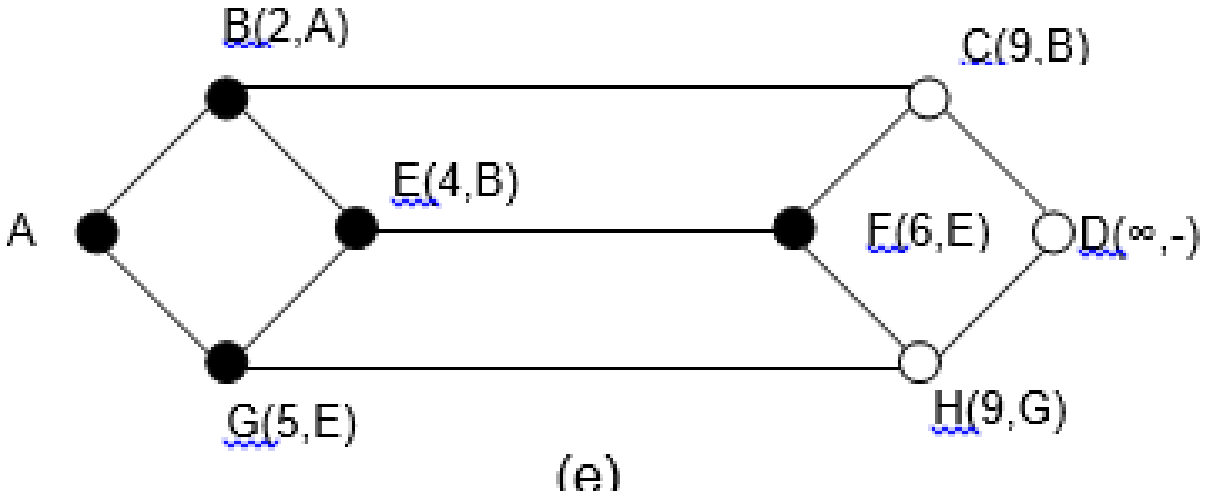


(c)

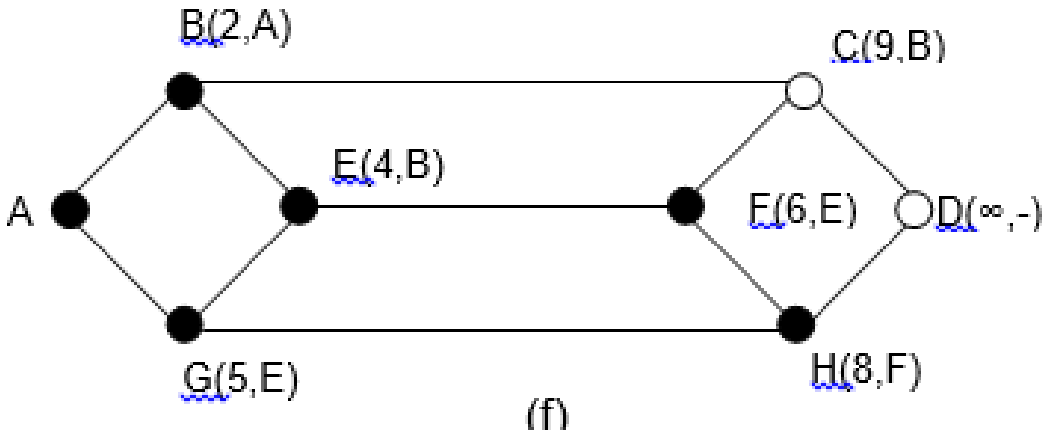


(d)

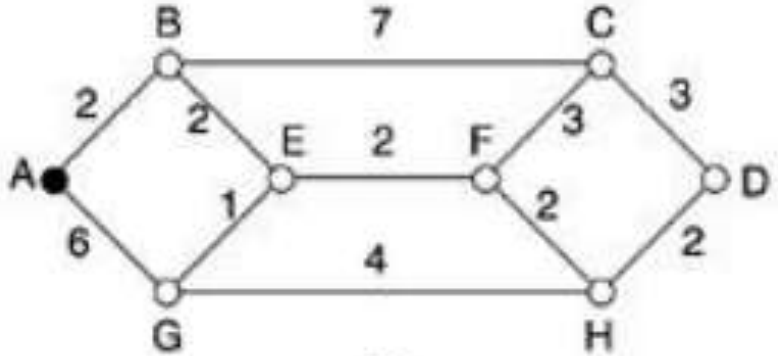
Shortest Path Routing:



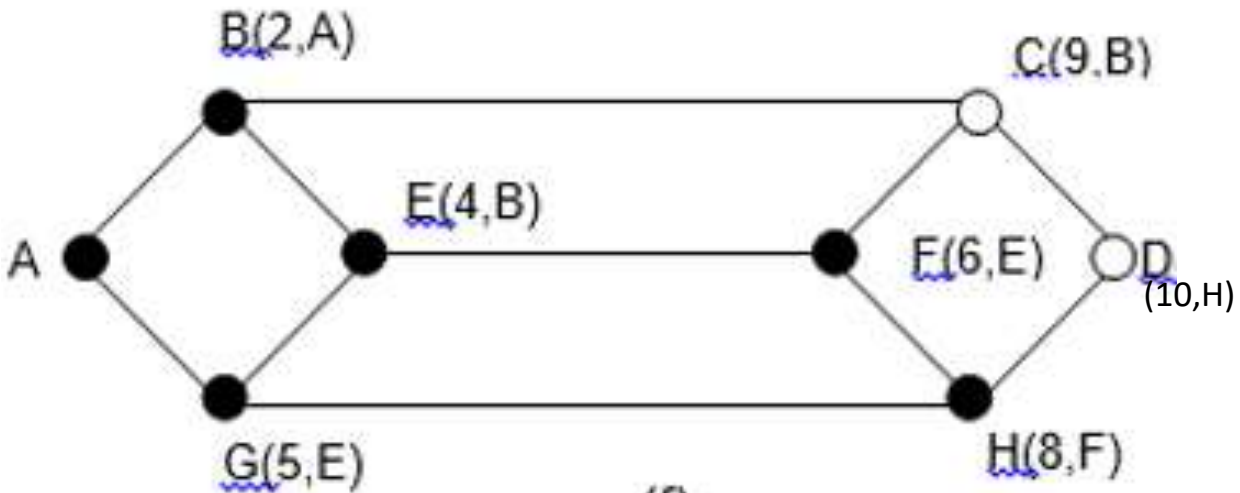
(e)



(f)



(a)

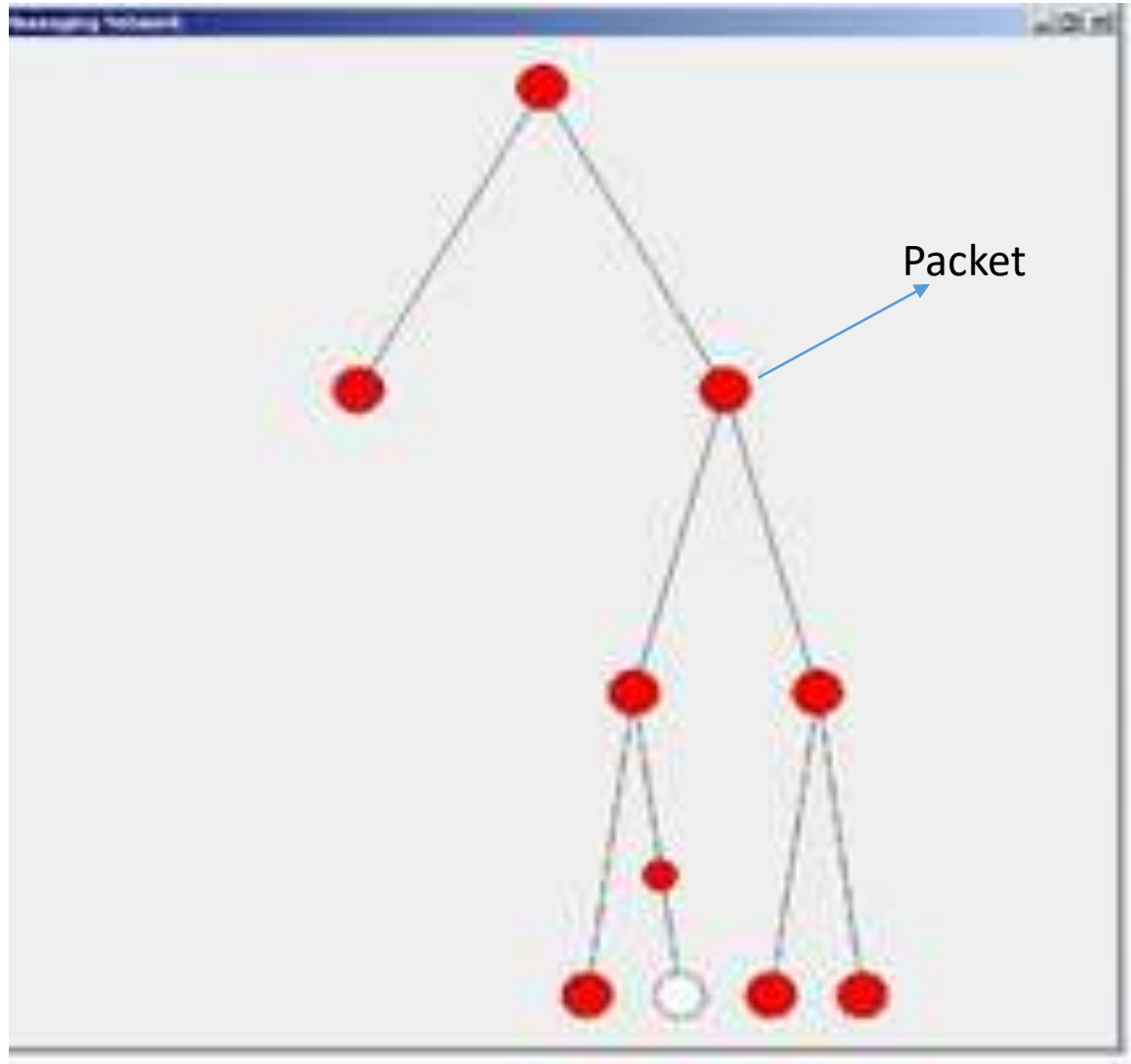


(f)

Flooding

- This is a static algorithm.
- In this, every incoming packet is sent out on every outgoing line except the one it arrived on.
- Flooding will generate vast numbers of duplicate packets, som**e measures have to take to dump the duplicate packets.**
- **One suc**h measure is to have a hop counter contained in the header of each packet, which is decremented at each hop, with the packet being discarded when the counter reaches zero.

- The hop counter should be initialized to the length of the path from source to destination.
- If the sender does not know how long the path is it can initialize the counter to full diameter of the subnet.


Packet

- A variation of flooding is ‘Selective Flooding’.

  -- In this the routers do not send every incoming packet on every line, instead only on those lines that are going approximately in the right direction which leads to the destination.

Advantages

1. In military applications, where large numbers of routers are blown, flooding is desirable.
2. In Distributed database applications, it is some times necessary to update all the databases concurrently, in which flooding is useful.
3. It is used as a metric against which other routing algorithms are compared.
4. Flooding chooses the shortest path, because it chooses all possible path in parallel.

Distance Vector Routing

- This is a dynamic routing algorithm.
- This algorithm operates by having each router maintain a table (i.e. a vector) giving the best known distance to each destination and which line to use.
- These tables are updated by exchanging information with the neighbors.

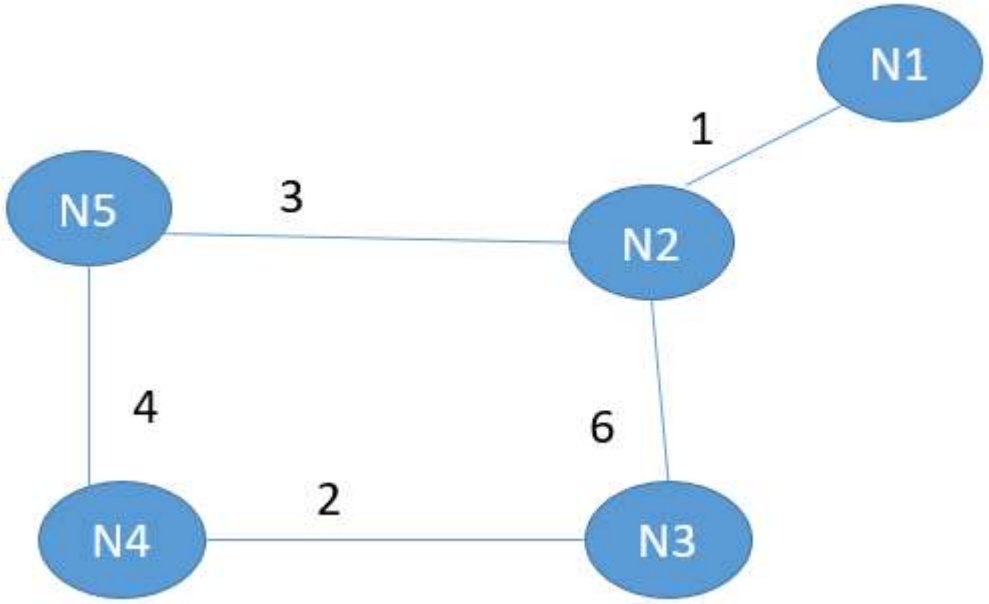


TABLE FOR N1

Dest	Dist	Next
N1		
N2		
N3		
N4		
N5		

TABLE FOR N2

Dest	Dist	Next
N1		
N2		
N3		
N4		
N5		

TABLE FOR N3

Dest	Dist	Next
N1		
N2		
N3		
N4		
N5		

TABLE FOR N4

Dest	Dist	Next
N1		
N2		
N3		
N4		
N5		

TABLE FOR N5

Dest	Dist	Next
N1		
N2		
N3		
N4		
N5		

TABLE FOR N1

Dest	Dist	Next
N1	0	N1
N2	1	N2
N3	∞	-
N4	∞	
N5	∞	

TABLE FOR N2

Dest	Dist	Next
N1	1	N1
N2	0	N2
N3	6	N3
N4	∞	-
N5	3	N5

TABLE FOR N3

Dest	Dist	Next
N1	∞	-
N2	6	N2
N3	0	N3
N4	2	N4
N5	∞	-

TABLE FOR N4

Dest	Dist	Next
N1	∞	-
N2	∞	-
N3	2	
N4	0	N4
N5	4	N5

TABLE FOR N5

Dest	Dist	Next
N1	∞	-
N2	3	N2
N3	∞	-
N4	4	N4
N5	0	N5

Construction of routing table.

By observing the Network diagram, we can observe that

1. The neighbours of N1 is --- N2
2. The neighbours of N2 is --- N3,N5
3. The neighbours of N3 is --- N2 ,N4
4. The neighbours of N4 is --- N3,N5
5. The neighbours of N5 is --- N2,N4

https://www.youtube.com/watch?v=5ZuP5qjbKSI

N2

1
0
6
∞
3

New routing table for N1

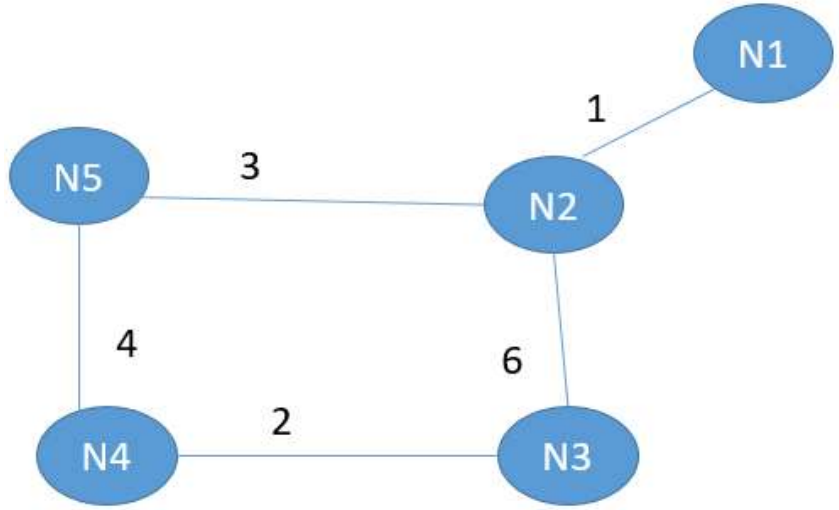
Dest	Dist	Next
N1	0	N1
N2	1	N2
N3	7	N3
N4	∞	-
N5	4	N5

N1 → N2, N1 to N2 AND N2
1 + 0 = 1

N1 → N3, N1 -- N2 -- N3
1 + 6 = 7

N1 → N4, N1 – N2 – N4
1 + ∞ = ∞

N1 → N5, N1 - N2 -- N5
1 + 3 = 4



NEW ROUTING TABLE FOR N5

The neighbours of N5 are --- N2 & N4

N2
1
0
6
∞
3

N4
∞
∞
2
0
4

Dest	Dist	Next
N1	4	N2
N2	3	N2
N3	6	N4
N4	4	N4
N5	0	N5

1. N5 → N1, Two Ways through N2 or through N4

   N5 → N2 → N1, 3 + 1 = 4

   N5 → N4 → N1, 4 + ∞ = ∞ , choose the minimum(4).

2. N5 → N2, directly N2 or through N4

   N5 → N2 , N5 → N4 → N2

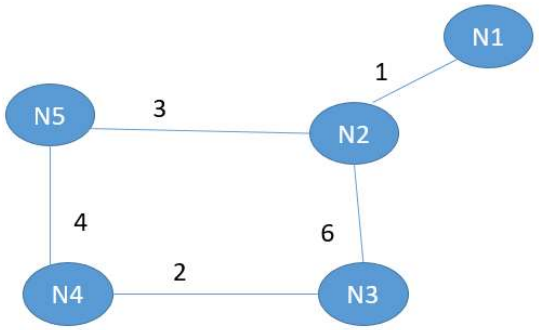
   3 or 4 + ∞ = ∞. Min 3

3. N5 → N3, Two ways through N2 or N4

   N5 → N2 → N3 or N5 → N4 → N3

   3 + 6 = 9 0r 4 + 2 = 6. min 6

4. N5 → N4 , 4



- These protocols select the best path on the basis of hop counts to reach a destination network in a particular direction.

-- Dynamic protocol like RIP is an example of a distance vector routing protocol.

-- Hop count is each router that occurs in between the source and the destination network.

--The path with the least hop count will be chosen as the best path.

Features –

- 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.

Disadvantages –

- As the routing information is exchanged periodically, unnecessary traffic is generated which consumes available bandwidth.
- As full routing tables are exchanged, therefore it has security issues. If an un/authorized person enters the network, then the whole topology will be very easy to understand.
- Also, the broadcasting of the network periodically creates unnecessary traffic.

Distance Vector Routing

- The routing table indexed by and containing one entry for each router in the subnet.
- This entry contains two parts:

  -- The preferred outgoing line to use for the destination and

  --- an estimate of time or distance to that destination.

- The metric used might be number of hops, time delay in m sec, total number of packets queued along the path or something similar.

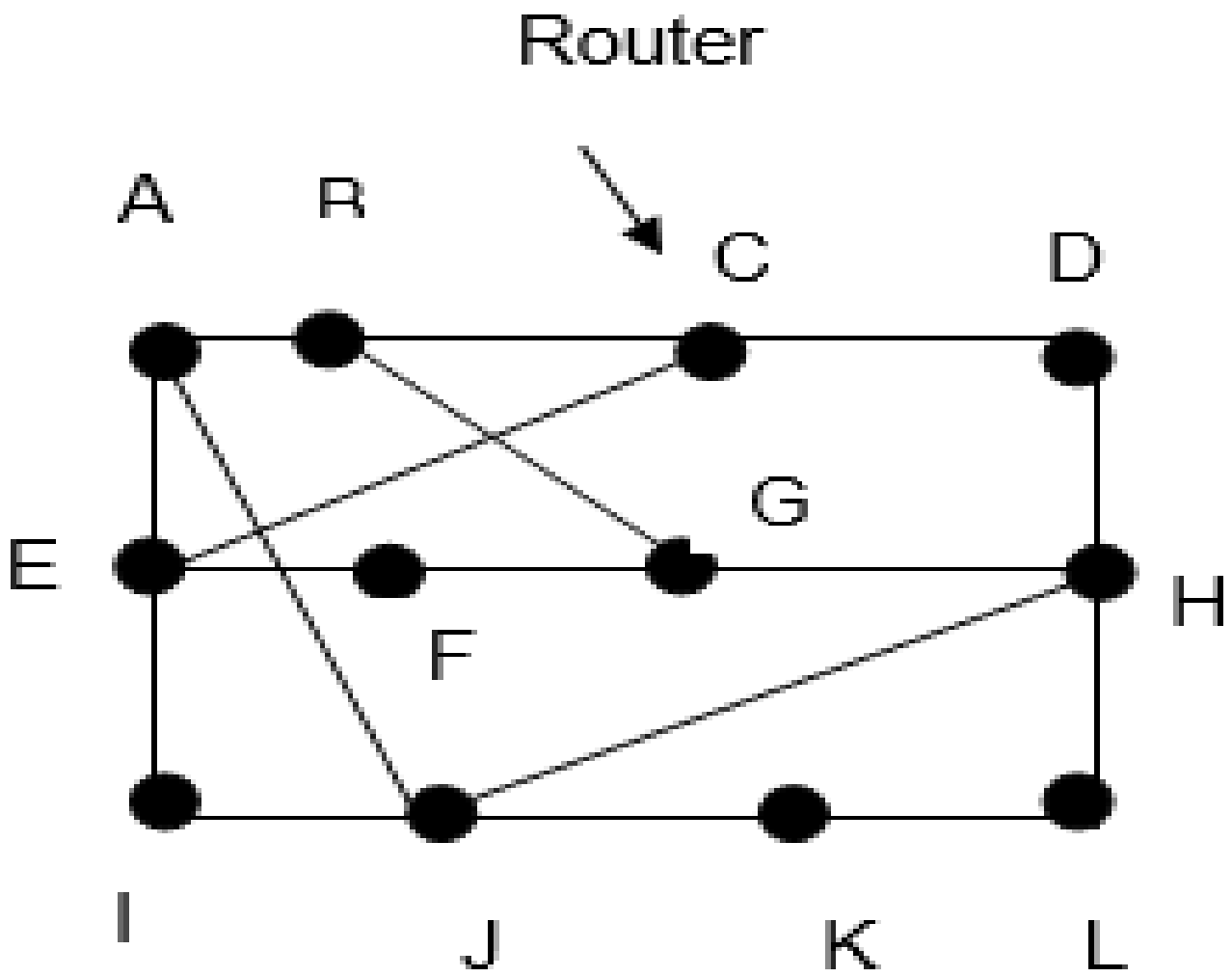
- The router is assumed to know the distance to each of its neighbors. If the metric is hops, the distance is just one hop.
- If the metric is queue length, the router examines each queue.
- If the metric is delay the router can measure it directly with a special ECHO packets.

- Consider an example, in which the delay is used as metric and

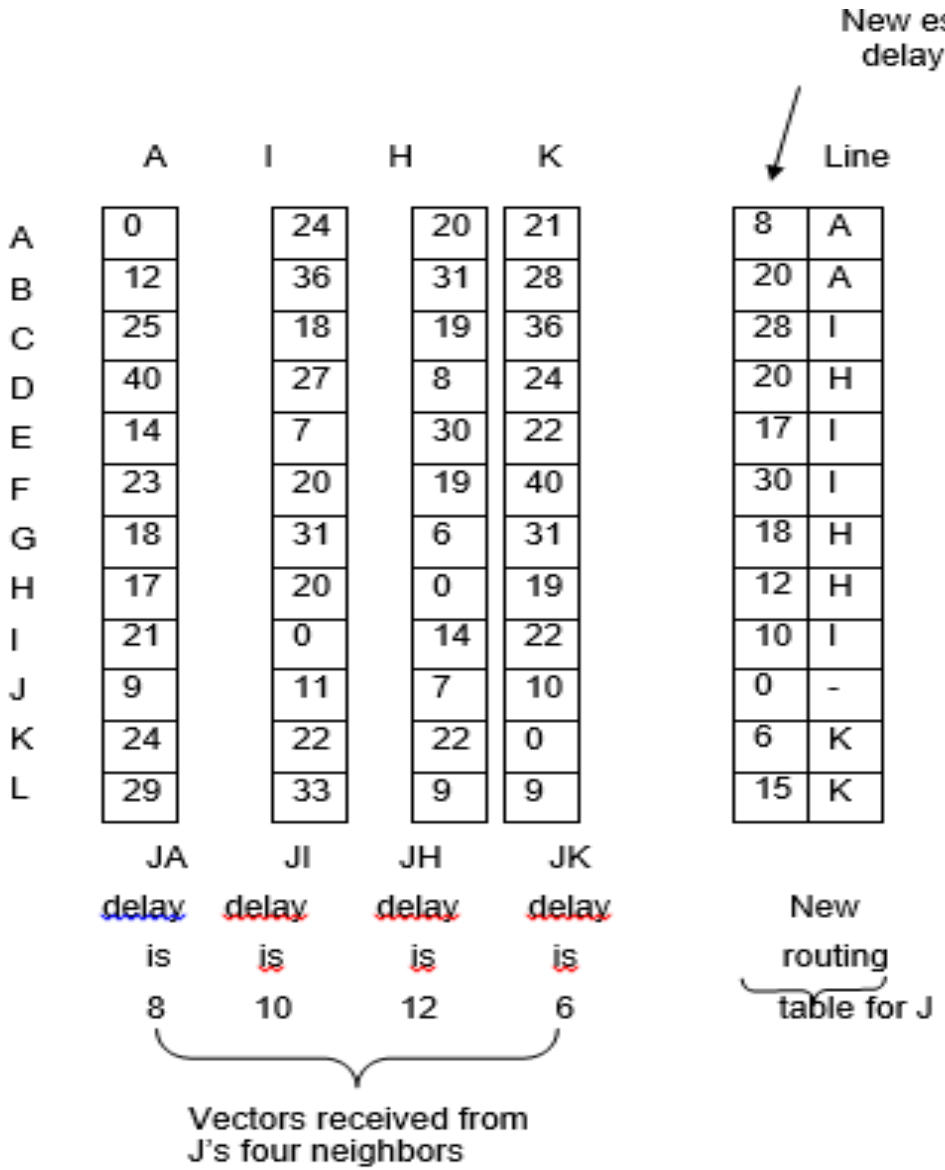
  the router knows the delay to each of its neighbors.
- Once every ’t’ m sec each router send to each neighbor a list of its estimated delays to each destination.
- It also receives a similar list from each neighbor.

- Let x_i being x's estimate of how long it takes to get router 'i'.
- If the router knows that the delay to x is 'm' m sec.
- To get router i via x is (x_i +m) m sec.
- By performing this calculation for each neighbor, a router can find out which estimate is the best and use that estimate and

  the corresponding line in its new routing table.



Subnet



Input from A,I,H, K and new routing table for J

1. JA -- 8

2. JB -- JA → AB, 8 + 12 =20 (through A)

3. JD ---- JH → HD, 12 + 8 = 20 (through H)

4. JG ---- JH → HG, 12 + 6 = 18

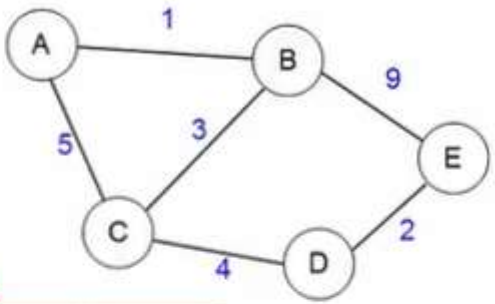
Find out JL, JD, JE

State Maintained

Each node maintains a routing table (distance vector)

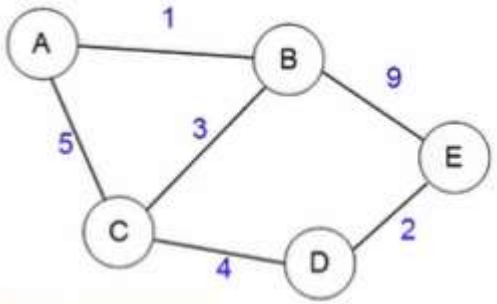
- Destination
- Estimated cost to destination
- Next hop via which to reach destination

Initial state: Cost to neighbors

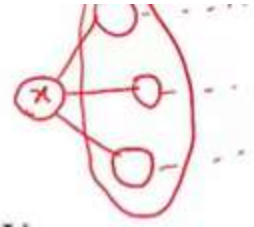


Dest	Cost	Next Hop
A	1	A
C	3	C
E	9	E

Initial Routing table at B

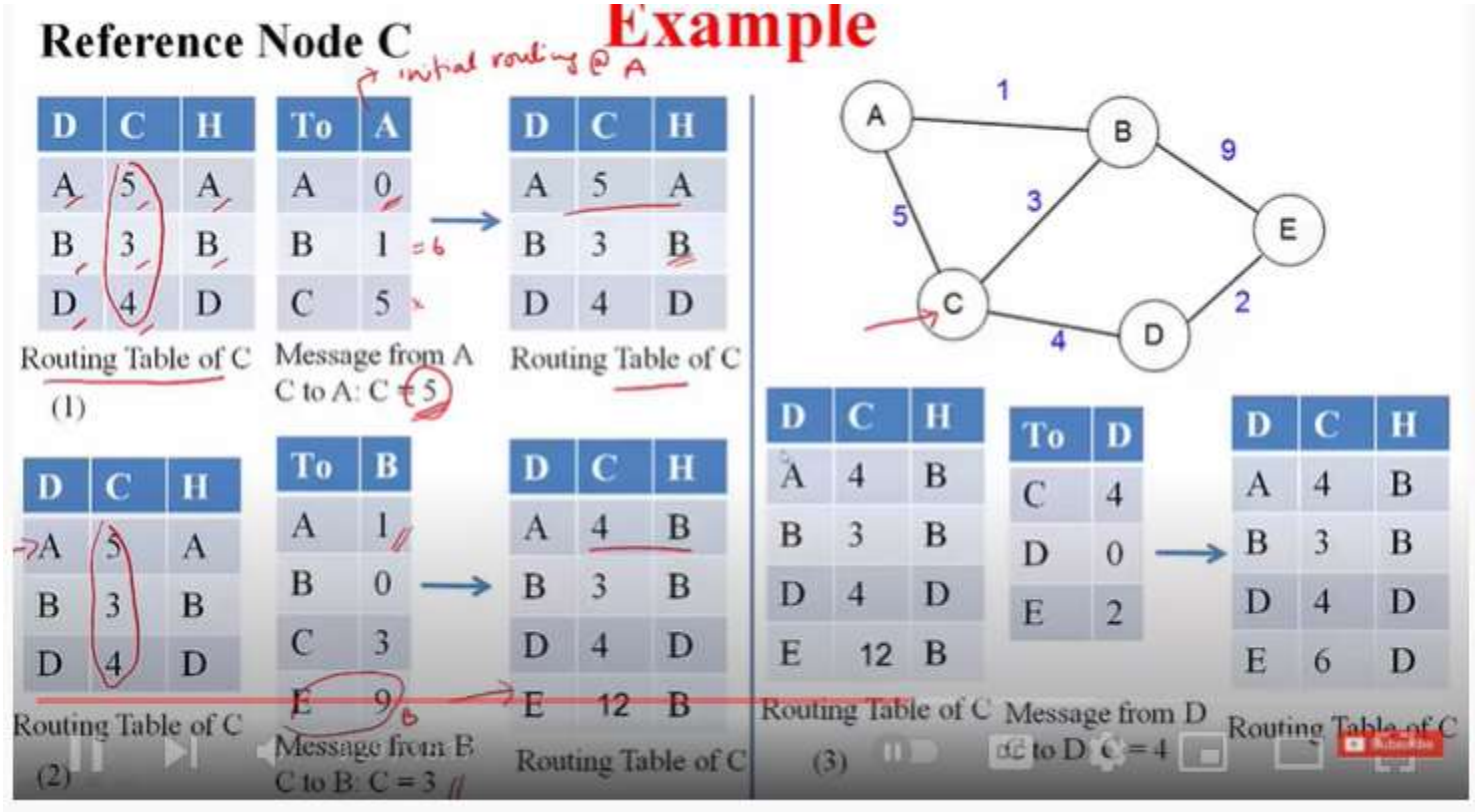


- Bellman-Ford equation
  - $d_x(y) = \min_v\{c(x,v) + d_v(y)\}$
  - $d_x(y)$ – least cost path from node x to y
  - $\min_v$ – apply above eq. over all of x's neighbors



Action at a router

- On receiving a message from a neighbor v,
  - Update cost (estimate) to destinations based on above Bellman-ford equation; change next hop accordingly
  - For each y (destination in routing table of the received message)
    - $D_x(y) = \min\{\text{current estimate}, c(x,v) + D_v(y)\}$
  - Estimated costs finally converge to optimal cost after series of message exchanges


Reference Node C
Example
initial routing @ A
D C H
A 5 A
B 3 B
D 4 D
Routing Table of C
(1)
To A
A 0
B 1 = 6
C 5
Message from A
C to A: C = 5
D C H
A 5 A
B 3 B
D 4 D
Routing Table of C
A
B
C
D
E
1
9
5
3
4
2
D C H
A 5 A
B 3 B
D 4 D
Routing Table of C
(2)
To B
A 1
B 0
C 3
E 9
Message from B
C to B: C = 3
D C H
A 4 B
B 3 B
D 4 D
E 12 B
Routing Table of C
D C H
A 4 B
B 3 B
D 4 D
E 12 B
Routing Table of C
(3)
To D
C 4
D 0
E 2
Message from D
C to D: C = 4
D C H
A 4 B
B 3 B
D 4 D
E 6 D
Routing Table of C

Link State Routing

- **Link-state routing protocols** are one of the two main classes of routing protocols used in packet switching networks for computer communications, the other being distance Vector Routing protocols.
- Examples of link-state routing protocols include

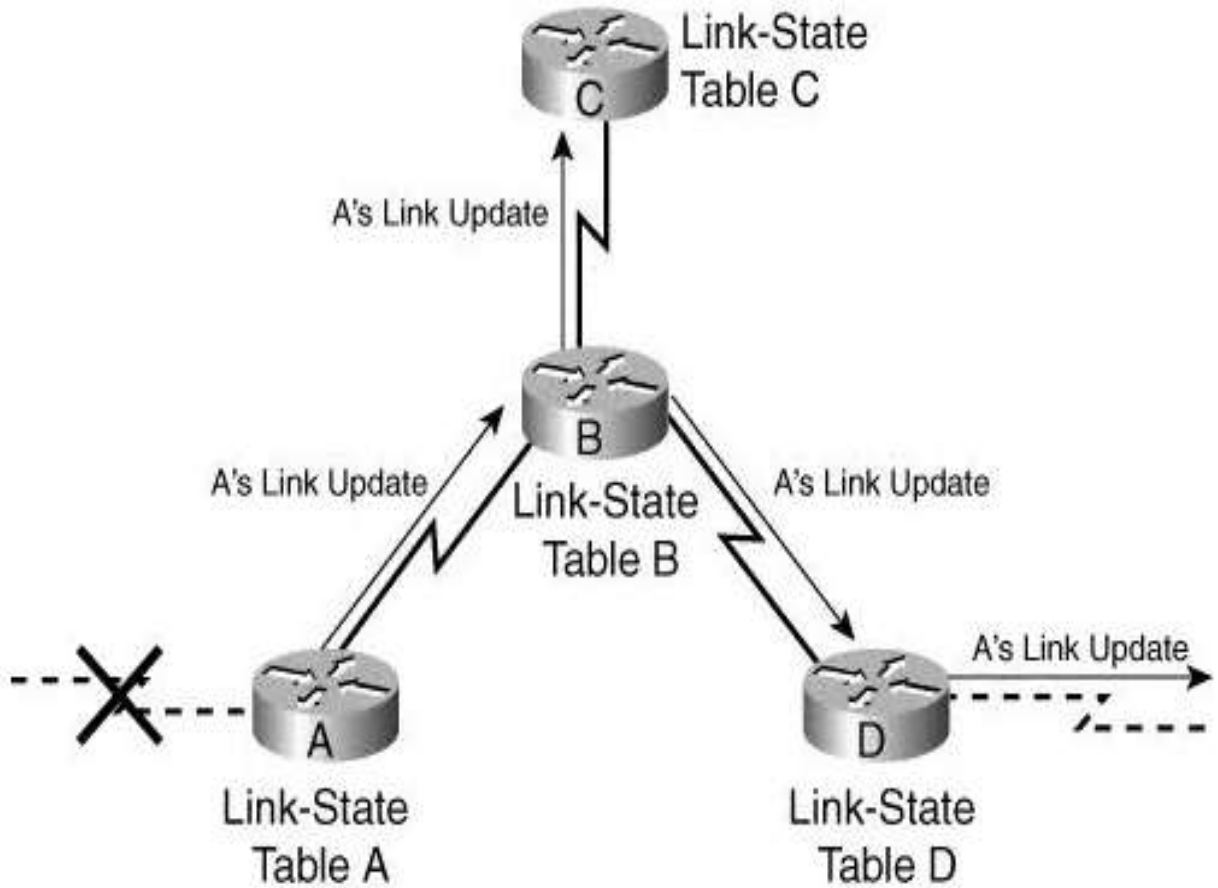
Open Shortest Path First (OSPF) and

Intermediate System to Intermediate System (IS-IS).

- The link-state protocol is performed by every *switching node* in the network (i.e., nodes that are prepared to forward packets; in the Internet, these are called routers).
- The basic concept of link-state routing is that every node constructs a *map* of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes.

- Each node then independently calculates the next best logical *path* from it to every possible destination in the network. Each collection of best paths will then form each node's routing table.
- This contrasts with distance-vector routing protocols, which work by having each node share its routing table with its neighbors, in a link-state protocol the only information passed between nodes is *connectivity related*.
- Link-state algorithms are sometimes characterized informally as each router, "telling the world about its neighbors."

Link-State Routing Sends Changed Data Only When There Is a Change



Link State Routing Algo

Link state routing is the second family of routing protocols. Link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology.

Based on this learned topology, each router is then able to compute its routing table by using the shortest path computation.

Features of link state routing protocols –

Link state packet – A small packet that contains routing information.

Link state database – A collection of information gathered from the link-state packet.

Shortest path first algorithm (Dijkstra algorithm) – A calculation performed on the database results in the shortest path

Routing table – A list of known paths and interfaces.

Calculation of shortest path

To find the shortest path, each node needs to run the famous **Dijkstra algorithm**. This famous algorithm uses the following steps:

Step-1: The node is taken and chosen as a root node of the tree, this creates the tree with a single node, and now set the total cost of each node to some value based on the information in Link State Database

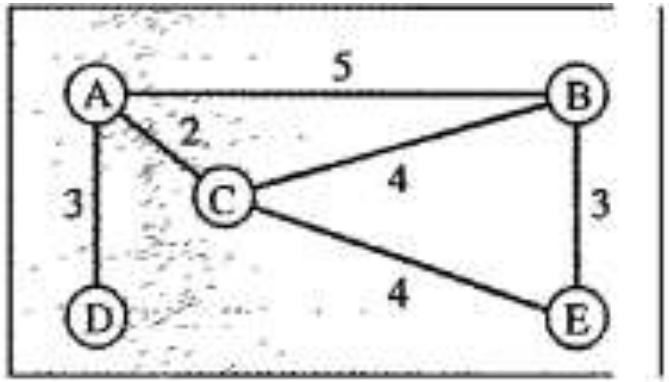
Step-2: Now the node selects one node, among all the nodes not in the tree-like structure, which is nearest to the root, and adds this to the tree. The shape of the tree gets changed.

Step-3:

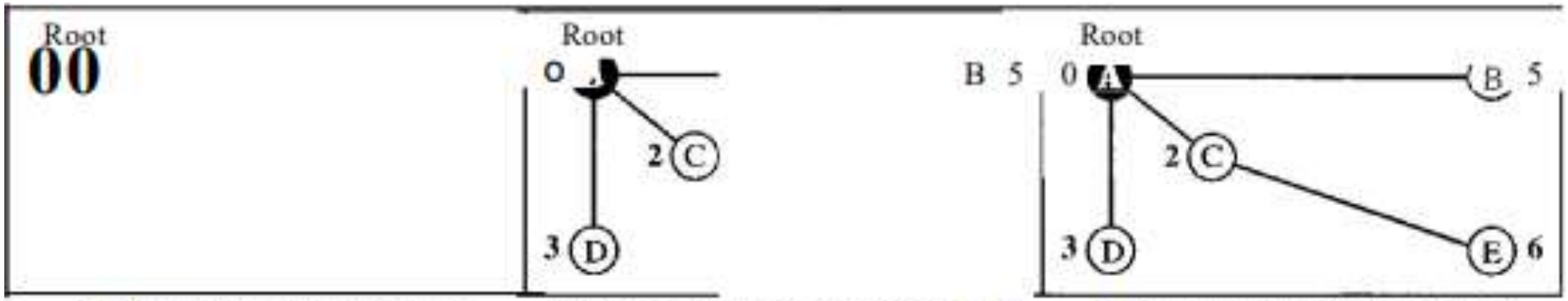
After this node is added to the tree, the cost of all the nodes not in the tree needs to be updated because the paths may have been changed.

Step-4:

The node repeats Step 2. and Step 3. until all the nodes are added to the tree



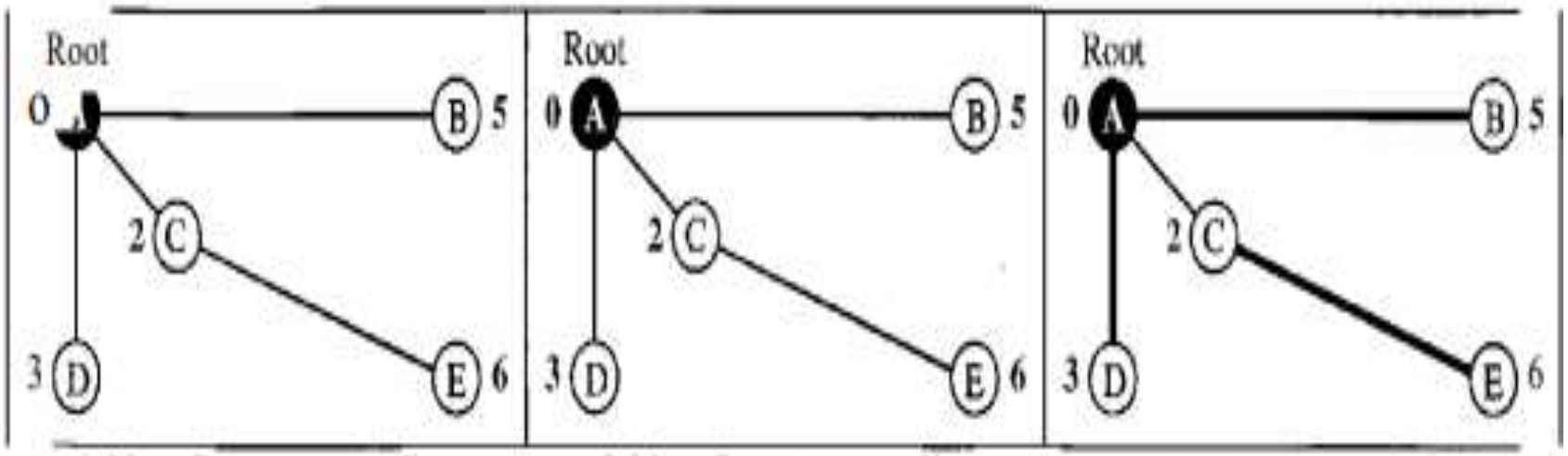
Topology



1. Set root to A and move A to tentative list.

2. Move A to permanent list and add B, C, and D to tentative list.

3. Move C to permanent and add E to tentative list.



4. Move D to permanent list.

5. Move B to permanent list.

6. Move E to permanent list (tentative list is empty).

1. We make node A the root of the tree and move it to the tentative list.

   Our two lists are Permanent list: empty Tentative list: A(O)

2. Node A has the shortest cumulative cost from all nodes in the tentative list.

   We move A to the permanent list and add all neighbors of A to the tentative list.

   Our new lists are Permanent list: A(O) Tentative list: B(5), C(2), D(3

3. Node C has the shortest cumulative cost from all nodes in the tentative list. We move C to the permanent list. Node C has three neighbors, but node A is already processed, which makes the unprocessed neighbors just B and E.

However, B is already in the tentative list with a cumulative cost of 5. Node A could also reach node B through C with a cumulative cost of 6. Since 5 is less than 6, we keep node B with a cumulative cost of 5 in the tentative list and do not replace it.

Our new lists are Permanent list:

A(O), e(2) Tentative list: B(5), 0(3), E(6)

4. Node D has the shortest cumulative cost of all the nodes in the tentative list. We move D to the permanent list.

Node D has no unprocessed neighbor to be added to the tentative list.

Our new lists are Permanent list:

A(O), C(2), 0(3) Tentative list: B(5), E(6)

5. Node B has the shortest cumulative cost of all the nodes in the tentative list.

We move B to the permanent list. We need to add all unprocessed neighbors of B to the tentative list (this is just node E).

However, E(6) is already in the list with a smaller cumulative cost.

The cumulative cost to node E, as the neighbor of B, is 8. We keep node E(6) in the tentative list.

Our new lists are Permanent list:

A(O), B(5), C(2), 0(3) Tentative list: E(6) 6.

6. Node E has the shortest cumulative cost from all nodes in the tentative list.

We move E to the permanent list. Node E has no neighbor.

Now the tentative list is empty.

We stop; our shortest path tree is ready.

The final lists are Permanent list:

A(O), B(5), C(2), D(3), E(6) Tentative list: empty

Calculation of Routing Table from 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.

Table shows the routing table for node A.

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

Link State protocols in comparison to Distance Vector protocols have:

1.It requires a large amount of memory.

2.Shortest path computations require many CPU circles.

3.If a network uses little bandwidth; it quickly reacts to topology changes

4.All items in the database must be sent to neighbors to form link-state packets.

5.All neighbors must be trusted in the topology.

6.Authentication mechanisms can be used to avoid undesired adjacency and problems.

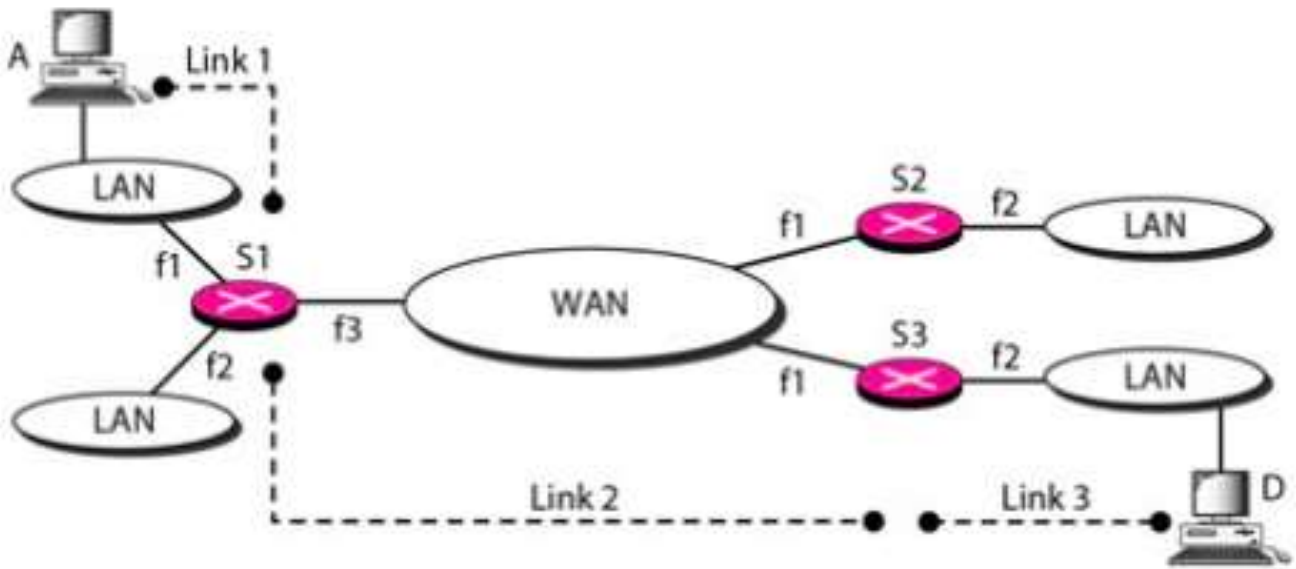
Distance Vector Routing	Link State Routing
--> Bandwidth required is less due to local sharing, small packets and no flooding.	--> Bandwidth required is more due to flooding and sending of large link state packets.
--> Based on local knowledge since it updates table based on information from neighbors.	--> 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.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

Internet,IPV4, IPV6

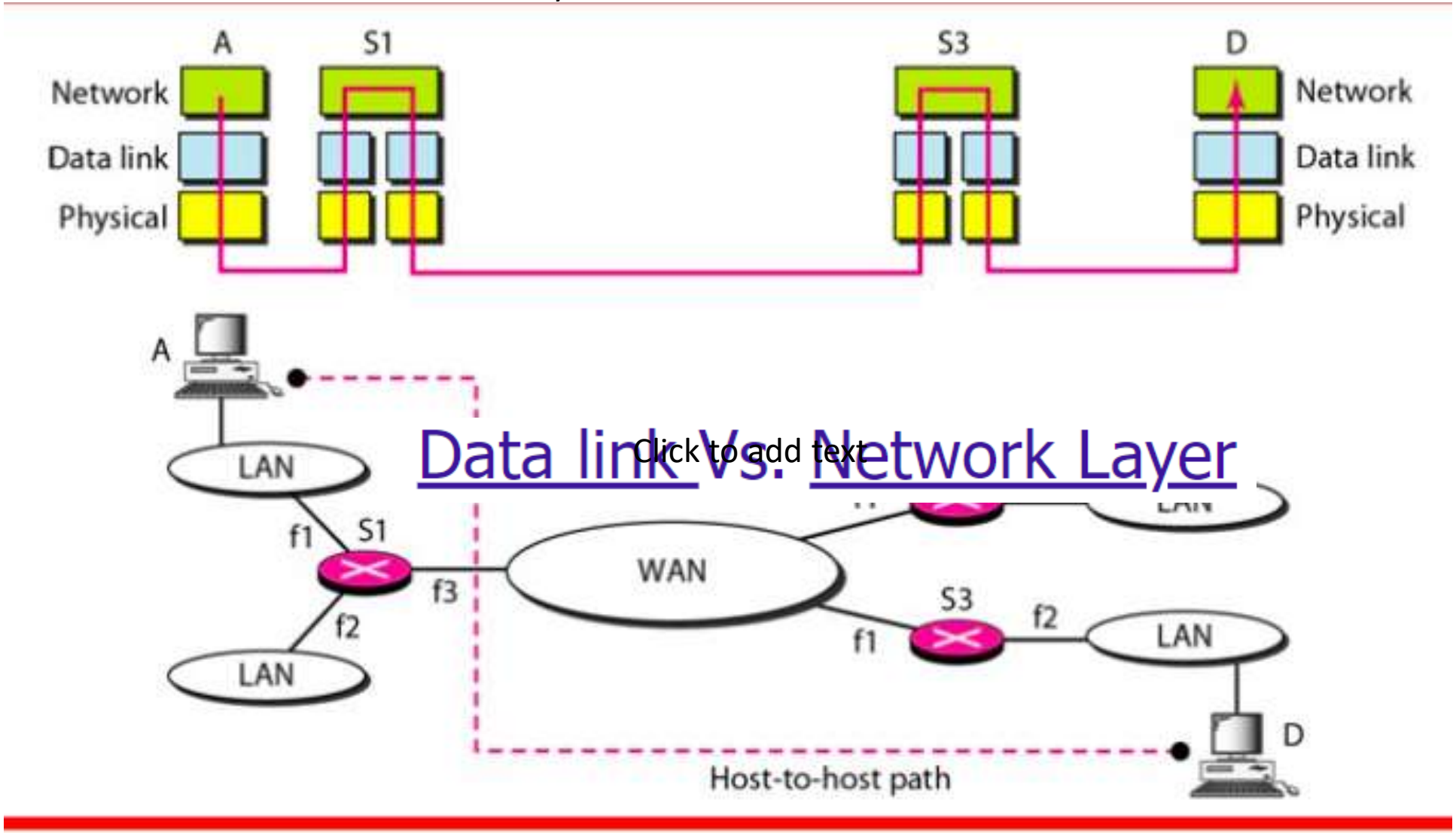
Data link Vs. Network Layer

- Data link layer provides hop to hop delivery.
- Network layer provides host to host delivery.
- If the transmission is within a network we use only physical and data link layer.
- If the transmission is outside the network we use network layer+data link+physical layer.

Links between Two hosts



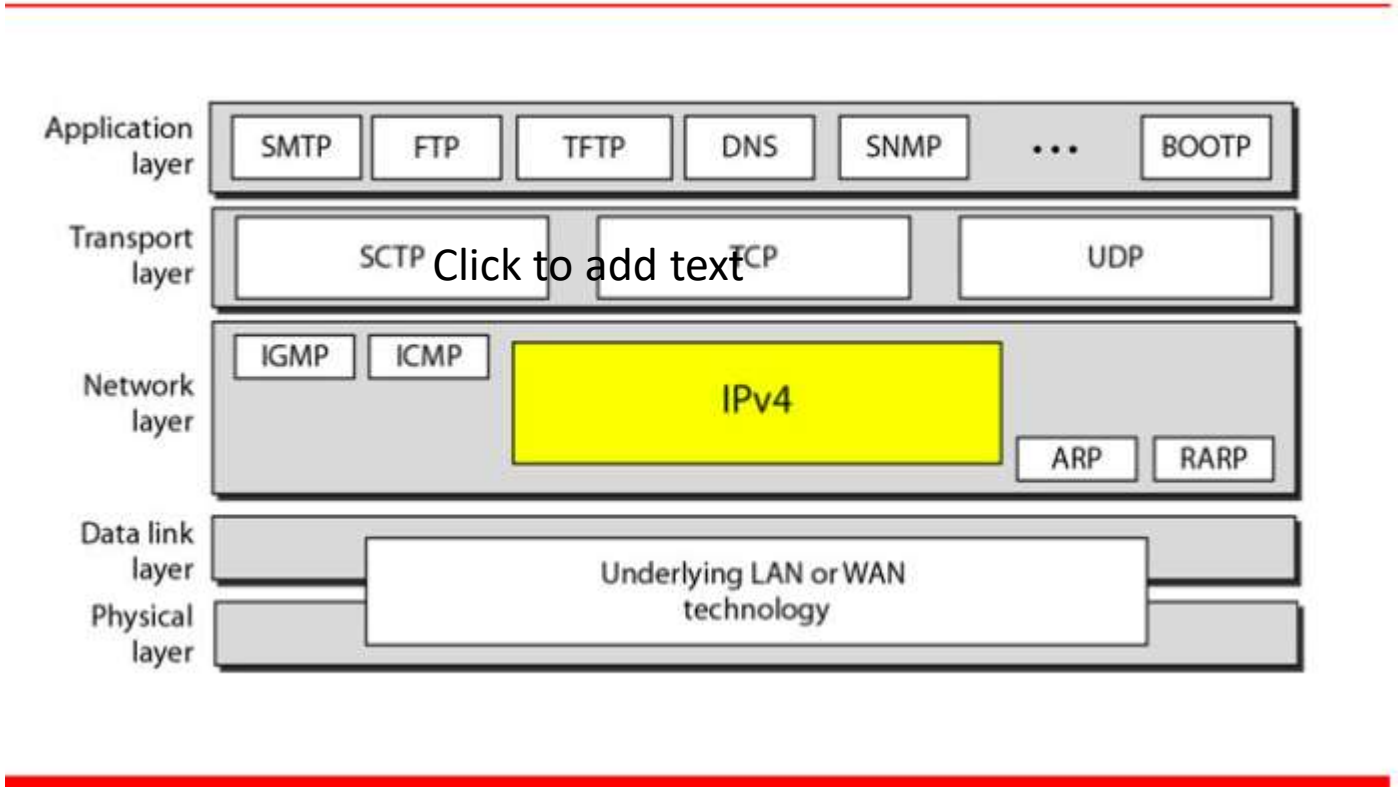
Network layer in an internetwork



Data link Vs. Network Layer

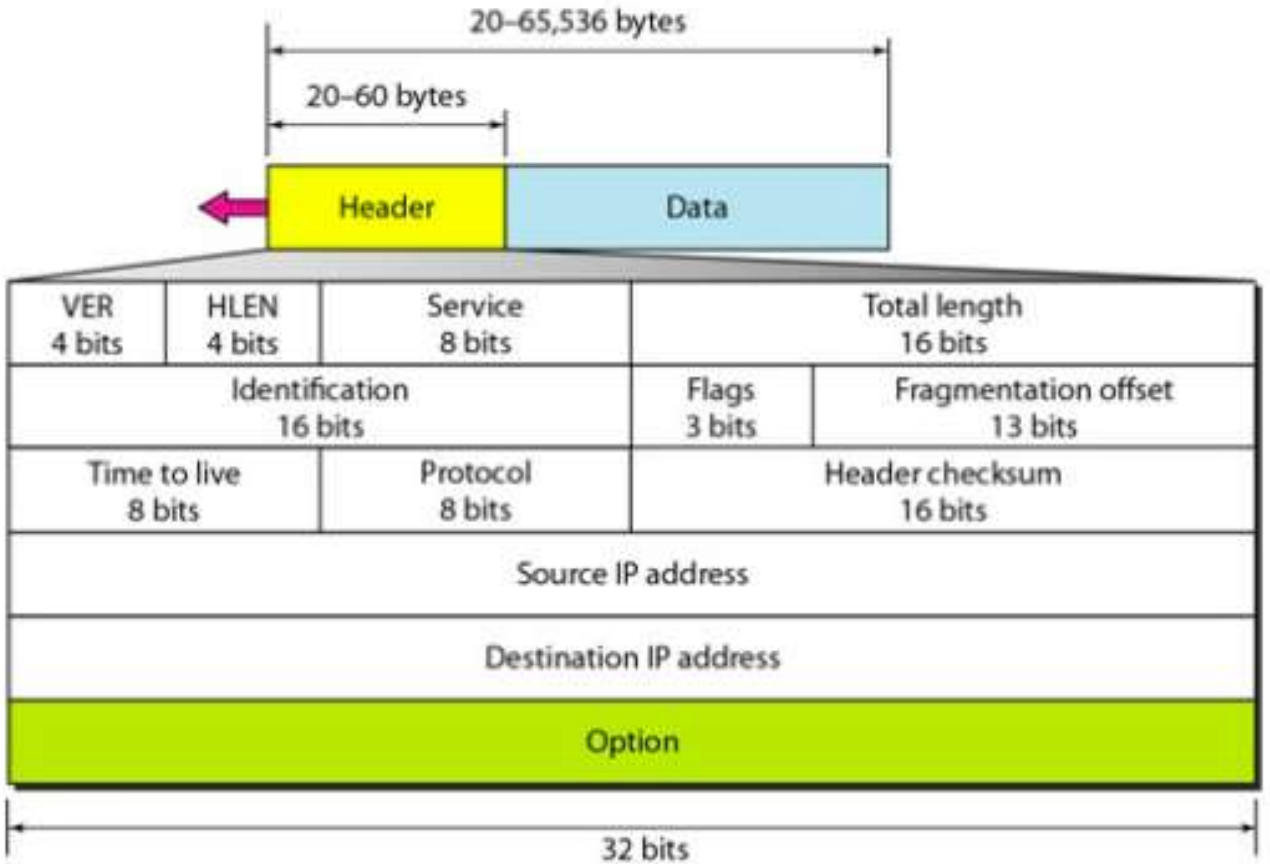
Click to add text

Internet protocol



Click to add text

IPv4 Datagram format.



IPv4 Datagram Format

- IPv4 Packet is called datagram.
- A datagram is of variable length.
- Consists of two parts: Header + Data
- Header's length is 20 to 60 bytes.
- Header contains information essential for routing and delivering Data.
- It is customary in TCP/IP to show the header in 4-byte sections.

Header Fields (1)

- VERSION (VER)
  - 4 bit in length
  - Defines the version of IP (either IPv6 or IPv4)

Header Length (HLEN)

  - 4 bit in length
  - Defines the length of the header.
  - Its value falls between 20 to 60 bytes

Service Type(1)

- First 3 bits are Precedence bits.
- Next 4 bits are called Type of Service (TOS) bits,
- and the last bit is not used.
- Precedence:
  - Value ranges from 000 to 111.
  - Defines priority of the datagram
  - Used in situations of Network Congestion
  - Router discards datagrams of low precedence in case of congestion.

Service Type(2)

- TOS bits
  - 4 bit in length
  - Out of 4 only a single bit can be 1 at a time, thus we have 5 different types of services.
  - Bit patterns and their interpretations are shown below.

TOS Bits	*Description*
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

Total Length

- This field defines the total length of the Datagram (header + Data)
- Value lies between 20 to 65536 bytes.

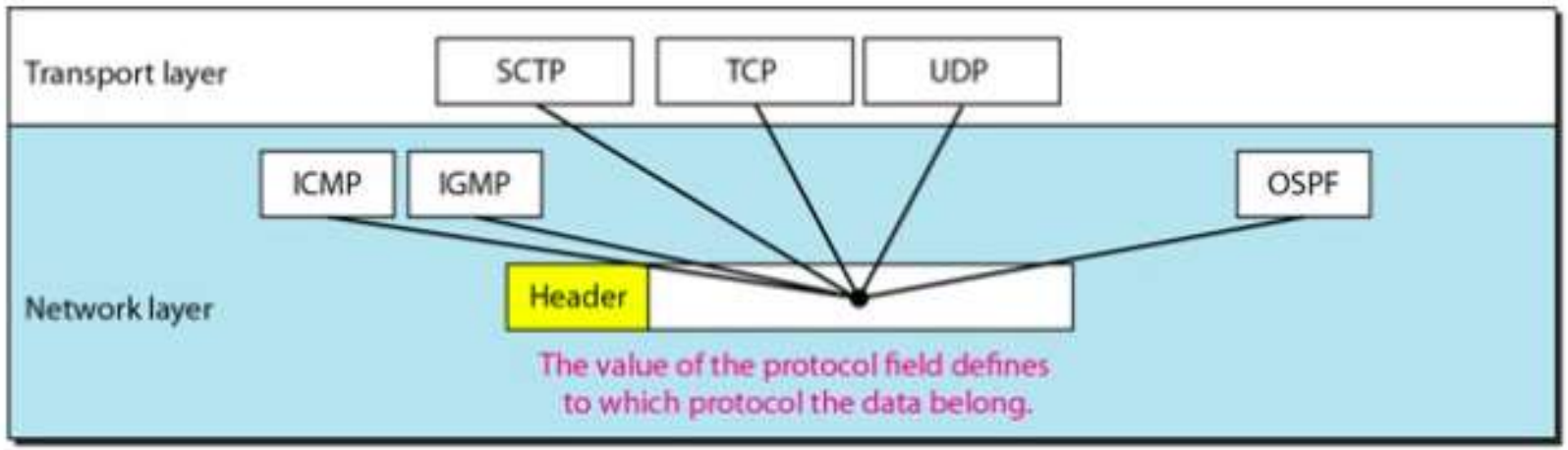
Time to Live

- A datagram has a limited lifetime in its travel through an internet.
- It holds a timestamp which is decremented on each visit of a router.
- The datagram is discarded when the value of this field becomes zero.
- The purpose is prevent datagram from monopolizing the network and causing congestion.

Protocol

- 8-bit length
- It defines the higher level protocol that uses the services of the IPv4 Layer.
- It defines the higher level protocol to which the IPv4 datagram is delivered.

Protocol field and encapsulated data



Protocol Values

Value	*Protocol*
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

Checksum

- An error detection mechanism
- Performed only with header fields
- Detects error in header part of datagram only.

Source/ Destination Address

- Source Address
  - 32 bit field
  - Defines the IPv4 address of the source
  - Remains unchanged during travel from source to destination.
- Destination Address
  - 32 bit field
  - Defines the IPv4 address of the destination
  - Remains unchanged during travel from source to destination.

IP Fragmentation-

•IP Fragmentation is a process of dividing the datagram into fragments during its transmission.

•It is done by intermediary devices such as routers at the destination host at network layer.

Need

- Each network has its maximum transmission unit (MTU).
- It dictates the maximum size of the packet that can be transmitted through it.
- Data packets of size greater than MTU can not be transmitted through the network.
- So, datagrams are divided into fragments of size less than or equal to MTU.

Fragmentation

- Why Fragmentation is Required?
  - A datagram can travel through different networks whose Protocols are defined by the data link and Physical Layer.
  - We know that at the data link layer we deal with ***Frames.***
  - For different network Protocols at data link layer we have different formats and sizes of frames.
  - Now we also know that the Packet from network layer called datagram (Header + data) act completely as data for the data link Frame.

IPv4 & IPv6

- **Internet Protocol** is a **unique identifier** that identifies each and every networking device on the Internet.
- An IP address is the same as our **home address**, which identifies our home location uniquely in the world.
- if you want to connect to the **Google's server** in order to search something you need to have the **google's DNS address.**
- Whenever you type **www.google.com,** internally the query url gets converted into the I**P address (8.8.8.8**) by DNS and we can access Google website.

- An **IPv4** address is a 32-bit address that *uniquely* and *universally* defines the connection of a device (for example, a computer or a router) to the Internet.
- IPv4 addresses are unique. They are unique in the sense that each address defines one, and only one, connection to the Internet.
- Two devices on the Internet can never have the same address at the same time.

- An IP address is a **series of numbers isolated by periods**. IP addresses are communicated as a bunch of four numbers .
- Internet Protocol variant 4, IPv4, was created in the mid 1980s.
- An IPv4 address involves four numbers, each going from 0 to 255, which are isolated by periods.
- Each number in the set can go from **0 to 255**. In this way, the full IP tending to go goes from **0.0.0.0 to 255.255.255.255.**

Key Takeaways

- IPv4 starts from 0.0.0.0 to 255.255.255.255
- It covers 2^{32} i.e around 4 billion addresses.
- IPv4 is a 32-bit address.
- IPv4 can be represented in Decimal, Octal or Hexadecimal notation.
- IPv4 does not have an error checking or acknowledgement mechanism.
- There are two types of IPv4 address: Public and Private
- Private addresses are locally unique.
- Public addresses are globally unique.

- An address may be assigned to a device for a time period and then taken away and assigned to another device.
- On the other hand, if a device operating at the network layer has *m* connections to the Internet, it needs to have *m* addresses.
- The IPv4 addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet.

Address Space

- A protocol such as IPv4 that defines addresses has an address space.
- An address space is the total number of addresses used by the protocol.
- IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 locations.

- There are two notations of an IPv4 address:
  -- binary notation & dotted decimal notation.

Binary Notation

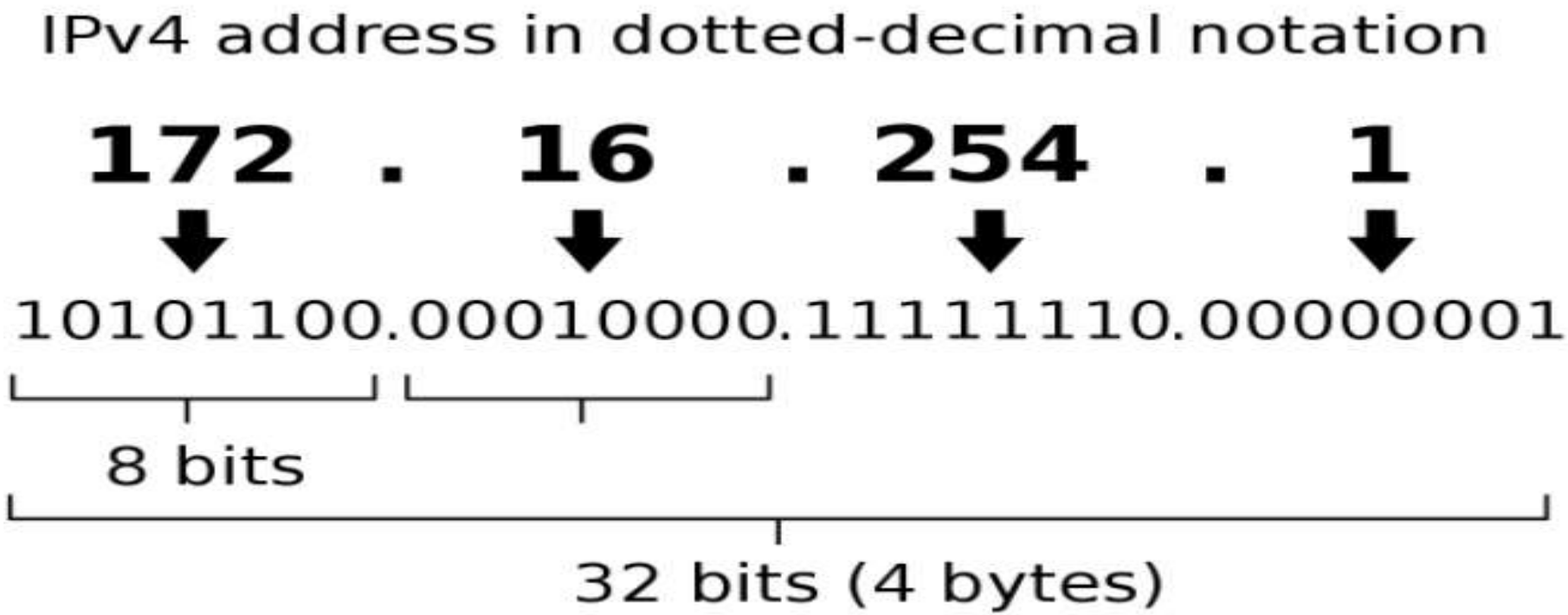
- In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address.
- The following is an example of an IPv4 address in binary notation:

01110101 10010101 00011101 00000010

Dotted-Decimal Notation

- To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes.
- The following is the dotted - decimal notation of the above address:

117.149.29.2


IPv4 address in dotted-decimal notation
172 . 16 . 254 . 1
10101100.00010000.11111110.00000001
8 bits
32 bits (4 bytes)

Ex: Change the following IPv4 addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00100011 11101111

129.11.35.239

b. 11000001 10000011 00011011 11111111

193.131.27.255

Ex: Change the following IPv4 addresses from dotted-decimal notation to binary notation.

a. 111.56.45.78

b. 221.34.7.82

a.01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

Find the error, if any, in the following IPv4 addresses.

a. 111.56.045.78

There must be no leading zero (045).

b. 221.34.7.8.20

There can be no more than four numbers in an IPv4 address.

c. 125.225.55.0

No Error

d. 75.45.301.14

Each number needs to be less than or equal to 255 (301 is outside this range).

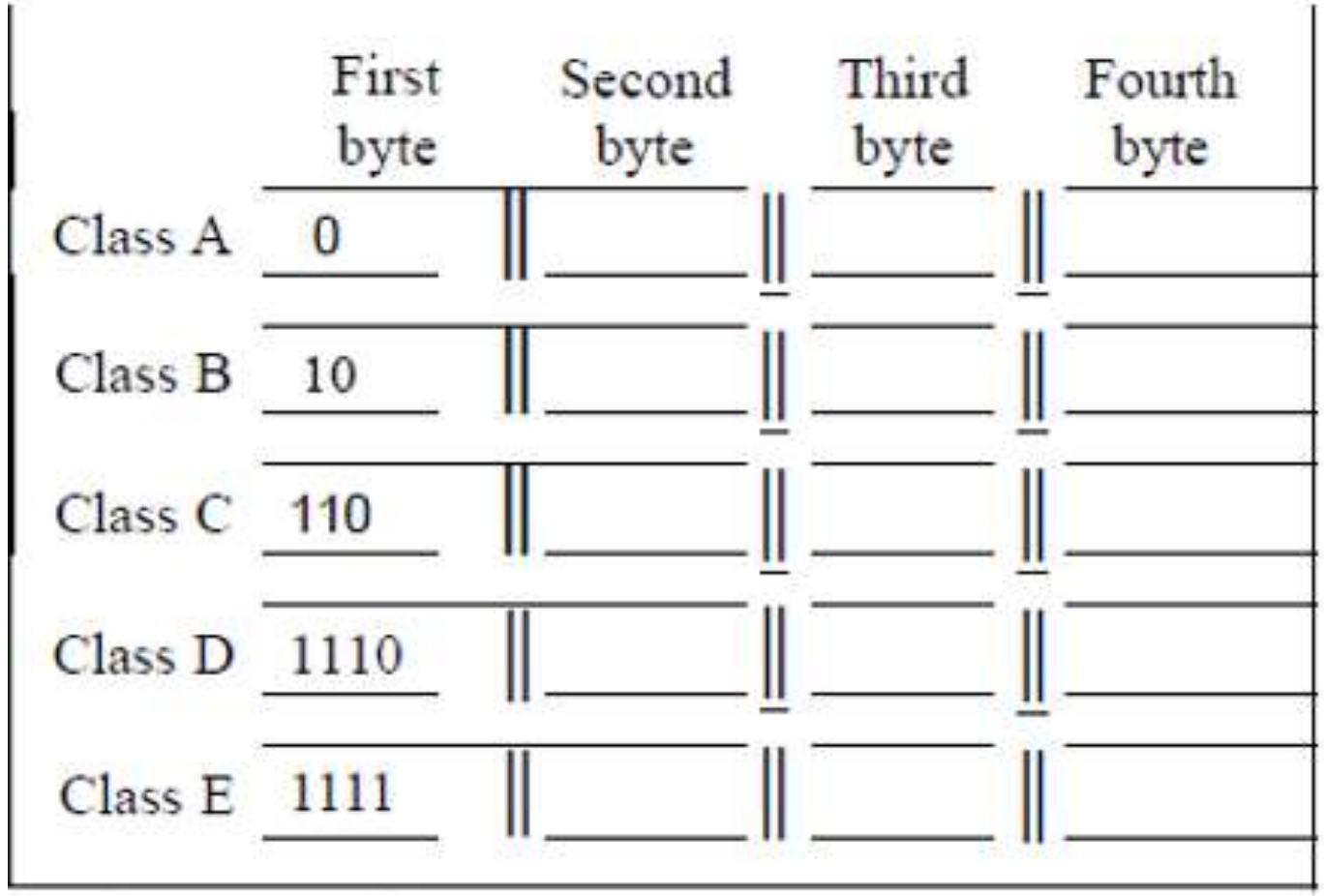
e. 11100010.23.14.67

A mixture of binary notation and dotted-decimal notation is not allowed.

Classful Addressing

- IPv4 addressing, at its inception, used the concept of classes. This architecture is called classful addressing.
- In classful addressing, the address space is divided into five classes:

  A, B, C, D, and E.
- Each class occupies some part of the address space.
- If the address is given in binary notation, the first few bits can immediately tell us the class of the address.
- If the address is given in decimal-dotted notation, the first byte defines the class.



a. Binary notation

DOTTED – DECIMAL NOTATION

CLASS	FIRST BYTE	SECOND BYTE	THIRD BYTE	FOURTH BYTE
A	0 - 127			
B	128 - 191			
C	192 - 223			
D	224 - 239			
E	240 - 255			

Ex: Find the class of each address.

a. 00000001 00001011 00001011 11101111

The first bit is O. This is a class A address.

b. 11000001 10000011 00011011 11111111.

The first 2 bits are 1; the third bit is 0.

This is a class C address.

Ex d : 10000001 00001011 00001011 11101111

e: 11100001 10000011 00011011 11111111

c. 14.23.120.8

The first byte is 14 (between 0 and 127); the class is A.

d. 252.5.15.111

The first byte is 252 (between 240 and 255); the class is E.

Classes and Blocks

- One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size as shown in Table

One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size as shown in Table

Class	*Number ofBlocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Number of blocks and block size in classfulIPv4 addressing

- Class A addresses

  -- were designed for large organizations with a large number of attached hosts or routers.

- Class B addresses

  - were designed for midsize organizations with tens of thousands of attached hosts or routers.

- Class C addresses

  - were designed for small organizations with a small number of attached hosts or routers.

Flaws in classes.

- A block in class A address is too large for any organization. This means most of the addresses in class A were wasted and were not used.
- A block in class B is also very large, probably too large for many of the organizations that received a class B block.
- A block in class C is probably too small for many organizations.

- Class D addresses were designed for multicasting.

  -- Each address in this class is used to define one group of hosts on the Internet.

  -- The Internet authorities wrongly predicted a need for 268,435,456 groups.

  --- This never happened and many addresses were wasted here too.

- the class E addresses were reserved for future use;

  --- only a few were used, resulting in another waste of addresses.

In classful addressing, a large part of the available addresses were wasted.

Netid and Hostid

- In classful addressing,

  an IP address in class A, B, or C is divided into netid and hostid.

  These parts are of varying lengths, depending on the class of the address.
- In class A, one byte defines the netid and three bytes define the hostid.
- In class B, two bytes define the netid and two bytes define the hostid.
- In class C, three bytes define the netid and one byte defines the hostid.

Mask

- **Note that the concept does not apply to classes D and E.**

  Mask

- Although the length of the netid and hostid (in bits) is predetermined in classful addressing, we can also use a mask (also called the default mask), a 32-bit number made of contiguous 1's followed by contiguous 0's.

Default masks for classful addressing

Class	*Binary*	*Dotted-Decimal*	*CIDR*
A	11111111 00000000 00000000 00000000	255.0.0.0	*18*
B	11111111 11111111 00000000 00000000	255.255.0.0	*116*
C	11111111 11111111 11111111 00000000	255.255.255.0	*124*

- The mask can help us to find the netid and the hostid.
- For example, the mask for a class A address has eight 1s, which means the first 8 bits of any address in class A define the netid; the next 24 bits define the hostid.
- The last column of Table shows the mask in the form *1n* where *n* can be 8, 16,or 24 in classful addressing. This notation is also called slash notation or Classless Inter domain Routing (CIDR) notation.

Classless Addressing

- Classful addressing, which is almost obsolete, is replaced with classless addressing.
- In this scheme, there are no classes, but the addresses are still granted in blocks.
- In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses.

- The size of the block (the number of addresses) varies based on the nature and size of the entity.
- For example, a household may be given only two addresses;

  a large organization may be given thousands of addresses.
- An ISP, as the Internet service provider, may be given thousands or hundreds of thousands based on the number of customers it may serve.

Restrictions

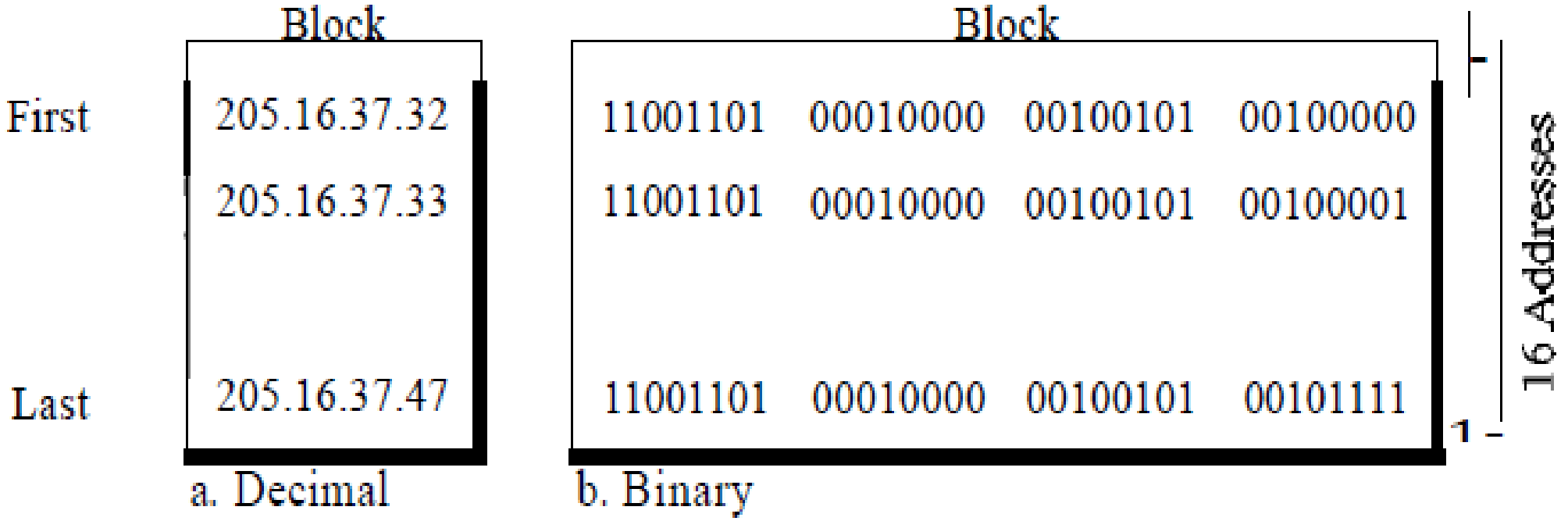
1. The addresses in a block must be contiguous, one after another.

2. The number of addresses in a block must be a power of 2

   (I, 2, 4, 8, ...).

3. The first address must be evenly divisible by the number of addresses.

A block of 16 *addresses granted to a small organization*



- We can see that the restrictions are applied to this block. The addresses are contiguous.
- The number of addresses is a power of 2, and the first address is divisible by 16.
- The first address, when converted to a decimal number, is 3,440,387,360, which when divided by 16 results in 215,024,210.

Mask

- A better way to define a block of addresses is to select any address in the block and the mask.
- A mask is a 32-bit number in which the *n* leftmost bits are 1's and the 32 - *n* rightmost bits are 0's.
- However, in classless addressing the mask for a block can take any value from 0 to 32.
- It is very convenient to give just the value of *n* preceded by a slash (CIDR notation).

- The address and the *In* notation completely define the whole block (the first address, the last address, and the number of addresses).
- First Address : The first address in the block can be found by setting the 32 - *n* rightmost bits in the binary notation of the address to Os.

https://internetofthingsagenda.techtarget.com/definition/IPv6-address

IPv6 address

- An IPv6 address is a 128-bit alphanumeric value that identifies an endpoint device in an Internet Protocol Version 6 (IPv6) network.
- IPv6 is the successor to a previous addressing infrastructure, IPv4, which had limitations IPv6 was designed to overcome.
- Notably, IPv6 has drastically increased address space compared to IPv4.

Format of an IPv6 address

- An IPv6 address is 128 bits long and is arranged in eight groups, each of which is 16 bits.
- Each group is expressed as four hexadecimal digits and the groups are separated by colons.

An example of a full IPv6 address could be:

FE80:CD00:0000:0CDE:1257:0000:211E:729C

- An IPv6 address is split into two parts:

-- a network and a node component.

- The network component is the first 64 bits of the address and is used for routing.
- The node component is the later 64 bits and is used to identify the address of the interface.

- The network node can be split even further into a block of 48 bits and a block of 16 bits.
- The upper 48-bit section is used for global network addresses.
- The lower 16-bit section is controlled by network administrators and is used for subnets on an internal network.

- Further, the example address can be shortened, as the addressing scheme allows the omission of any leading zero, as well as any sequences consisting of only zeros. The shortened version would look like:
- FE80:CD00:0:CDE:1257:0:211E:729C

Types of IPv6 addresses

- There are different types and formats of IPv6 addresses, of which, it's notable to mention that there are no broadcast addresses in IPv6. Some examples of IPv6 formats include:
- **Global unicast.** These addresses are routable on the internet and start with "2001:" as the prefix group. Global unicast addresses are the equivalent of IPv4 public addresses.
- **Unicast address.** Used to identify the interface of an individual node.
- **Anycast address.** Used to identify a group of interfaces on different nodes.

- **Multicast address.** An address used to define multicast Multicasts are used to send a single packet to multiple destinations at one time.
- **Link local addresses.** One of the two internal address types that are not routed on the internet. Link local addresses are used inside an internal network, are self-assigned and start with "fe80:" as the prefix group.
- **Unique local addresses.** This is the other type of internal address that is not routed on the internet. Unique local addresses are equivalent to the IPv4 addresses 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16.

Advantages and disadvantages of IPv6 addresses

- More efficient routing with smaller routing tables and aggregation of prefixes.
- Simplified packet processing due to more streamlined packet headers.
- Support of multicast packet flows.
- Hosts can generate their own IP addresses.

- Eliminates the need for network address translation (NAT).
- Easier to implement services like peer-to-peer (P2P) networks, voice over IP (VoIP) and stronger security.
- IPv6 also still uses the same two families of routing protocols – Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP).

IPv6 vs. IPv4: What are the differences?

- The biggest and most notable difference between IPv4 and IPv6 is the increase in addresses. With IPv4 being a 32-bit IP address and IPv6 being a 128-bit IP address, the number of IP addresses available grows drastically.
- However, one drawback to using an IPv6 address is that IPv4 is still widely used. Communication between IPv4 and IPv6 machines is not directly possible, meaning IPv4 addresses won't be able to see an IPv6 page, and vice versa. Eliminates the need for network address translation (NAT).
- Easier to implement services like peer-to-peer (P2P) networks, voice over IP (VoIP) and stronger security.
- IPv6 also still uses the same two families of routing protocols – Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP).

- Eliminates the need for network address translation (NAT).
- Easier to implement services like peer-to-peer (P2P) networks, voice over IP (VoIP) and stronger security.
- IPv6 also still uses the same two families of routing protocols – Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP).
- IPv6 is based on an alphanumeric addressing method, while IPv4 is only numeric.
- IPv6 binary bits are separated by a colon, while IPv4 binary bits are separated by a period.

- IPv6 binary bits are separated by a colon, while IPv4 binary bits are separated by a period.
- IP security is required by IPv6, while it is optional in IPv4.
- IPv6 uses an IP security (IPSec) protocol, while IPv4 relies on applications.
- Networks can be automatically configured with IPv6, while IPv4 networks have to be configured either manually or through Dynamic Host Configuration Protocol (DHCP).

- IPv6 has eight header fields with a 40-character length; IPv4 has 20 header fields with an eight-character length.
- IPv6 does not have any checksum fields.
- To map MAC addresses, IPv6 uses NDP (Neighbor Discovery Protocol), while IPv4 uses ARP (address resolution protocol).

Address Resolution Protocol (ARP)

- Address Resolution Protocol (ARP) is a procedure for mapping a dynamic IP Address to a permanent physical machine address in a local area network (LAN).
- The physical machine address is also known as a media access control (MAC) address.
- The job of ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice versa.
- This is necessary because IP addresses in IP version 4 (IPv4) are 32 bits, but MAC addresses are 48 bits.

- ARP works between Layers 2 and 3 of the Open Systems Interconnection model (OSI model).
- The MAC address exists on Layer 2 of the OSI model, the data link layer.
- The IP address exists on Layer 3, the network layer.
- https://www.youtube.com/watch?v=N7dM_kD28dM

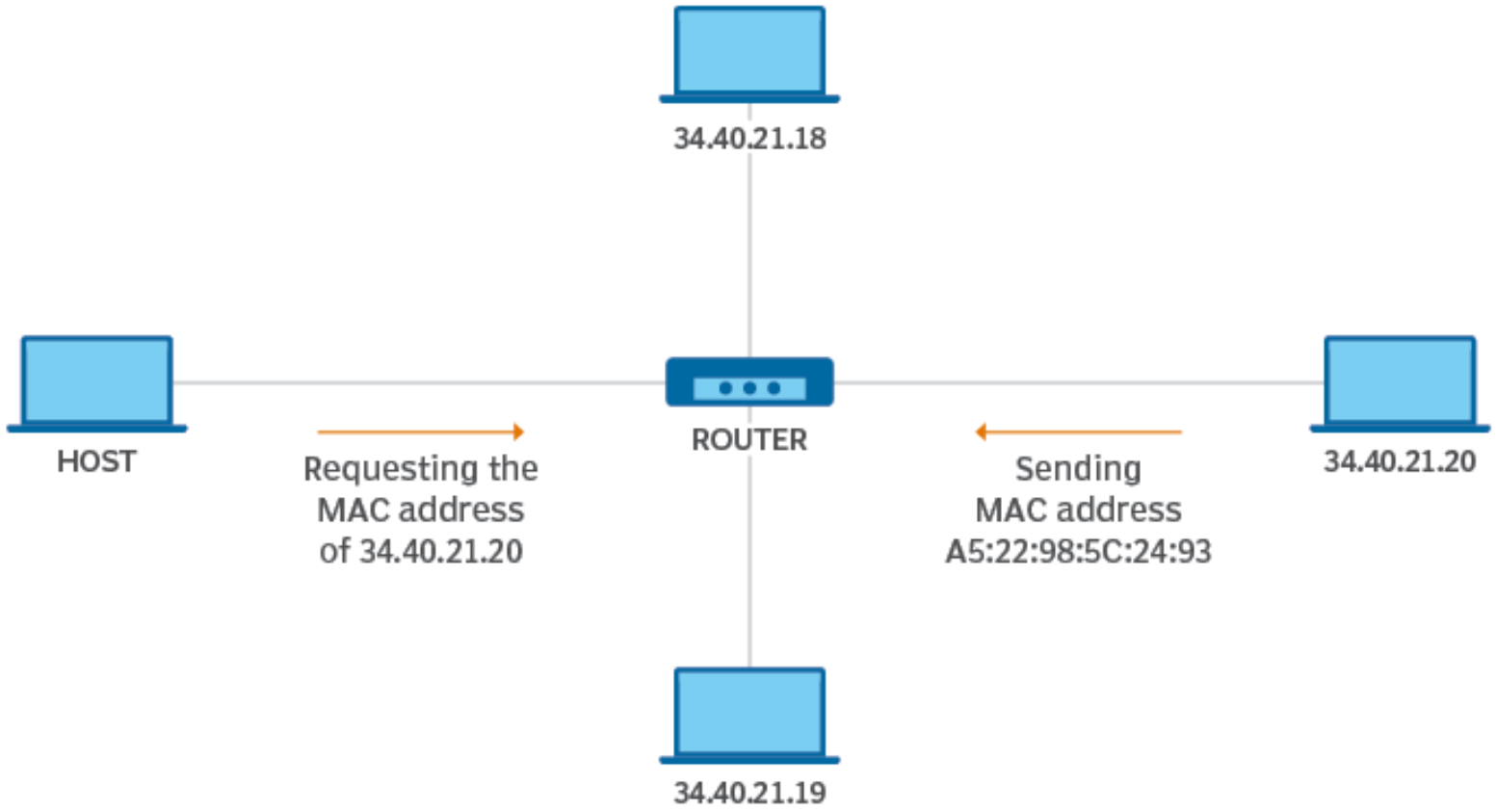
How ARP works

- When a new computer joins a LAN, it is assigned a unique IP address to use for identification and communication.
- When an incoming packet destined for a host machine on a particular LAN arrives at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address.
- A table called the ARP cache maintains a record of each IP address and its corresponding MAC address.

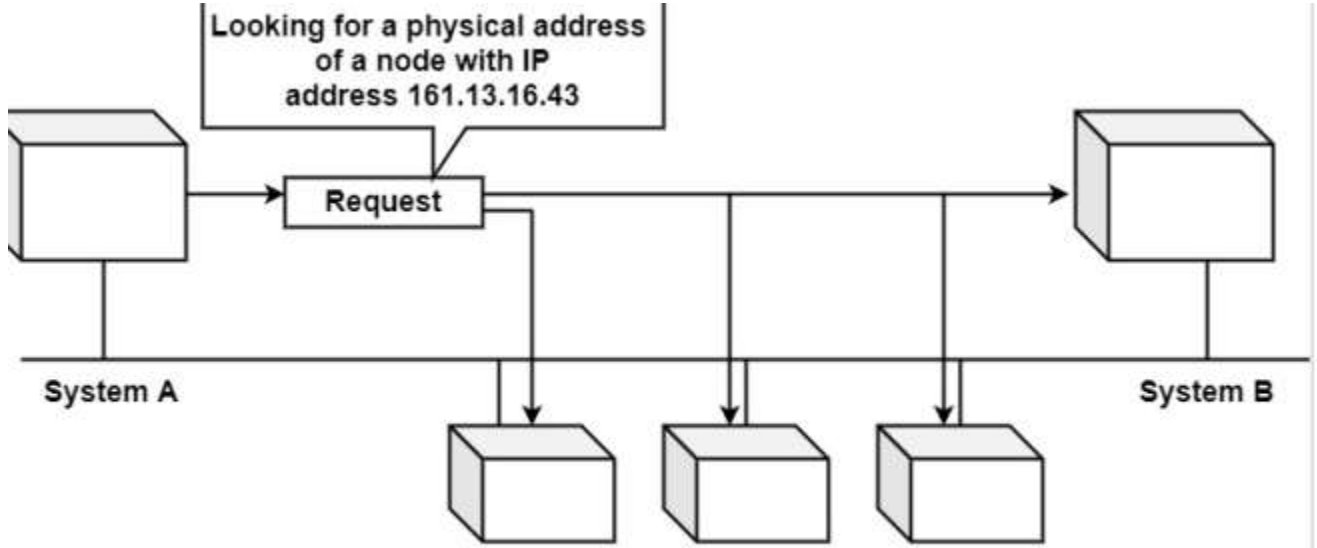
- All operating systems in an IPv4 Ethernet network keep an ARP cache.
- Every time a host requests a MAC address in order to send a packet to another host in the LAN, it checks its ARP cache to see if the IP to MAC address translation already exists.
- If it does, then a new ARP request is unnecessary. If the translation does not already exist, then the request for network addresses is sent and ARP is performed.

- ARP broadcasts a request packet to all the machines on the LAN and asks if any of the machines are using that particular IP address.
- When a machine recognizes the IP address as its own, it sends a reply so ARP can update the cache for future reference and proceed with the communication.

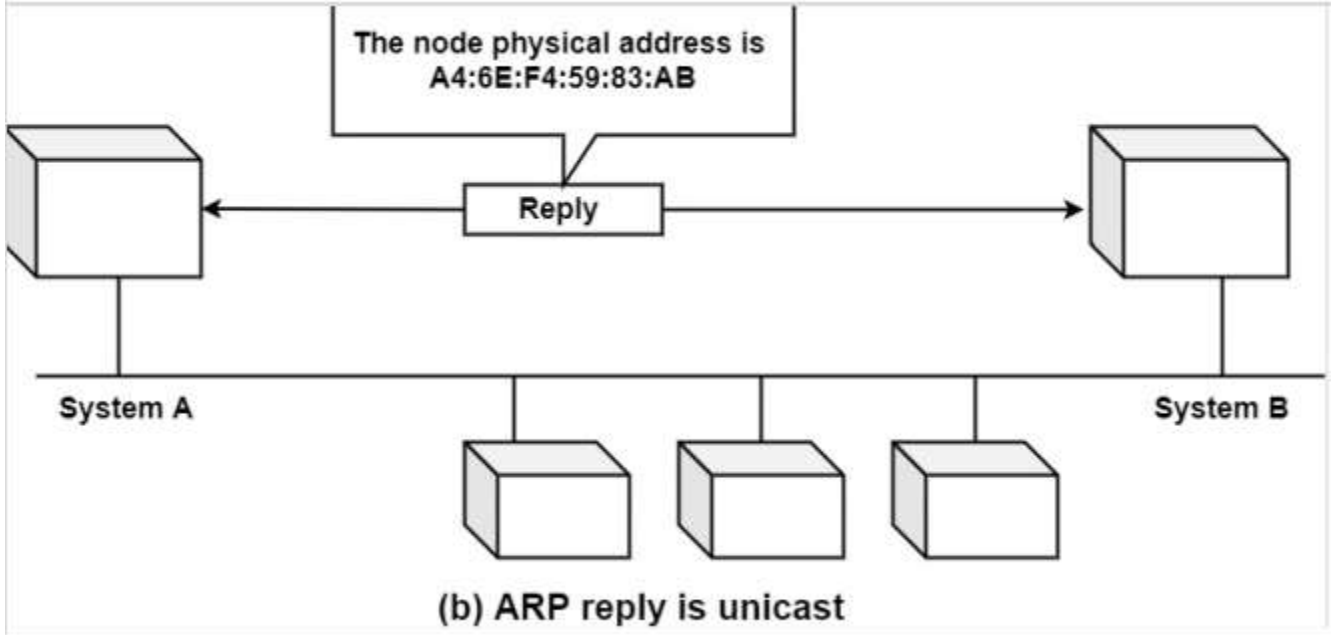
How address resolution protocol (ARP) works



ARP translates IP addresses and MAC addresses so devices can properly communicate and send data.



(a) ARP request is broadcast



(b) ARP reply is unicast

Types of ARP

Proxy ARP

- Proxy ARP is a technique by which a proxy device on a given network answers the ARP request for an IP address that is not on that network. The proxy is aware of the location of the traffic's destination and offers its own MAC address as the destination.

Gratuitous ARP

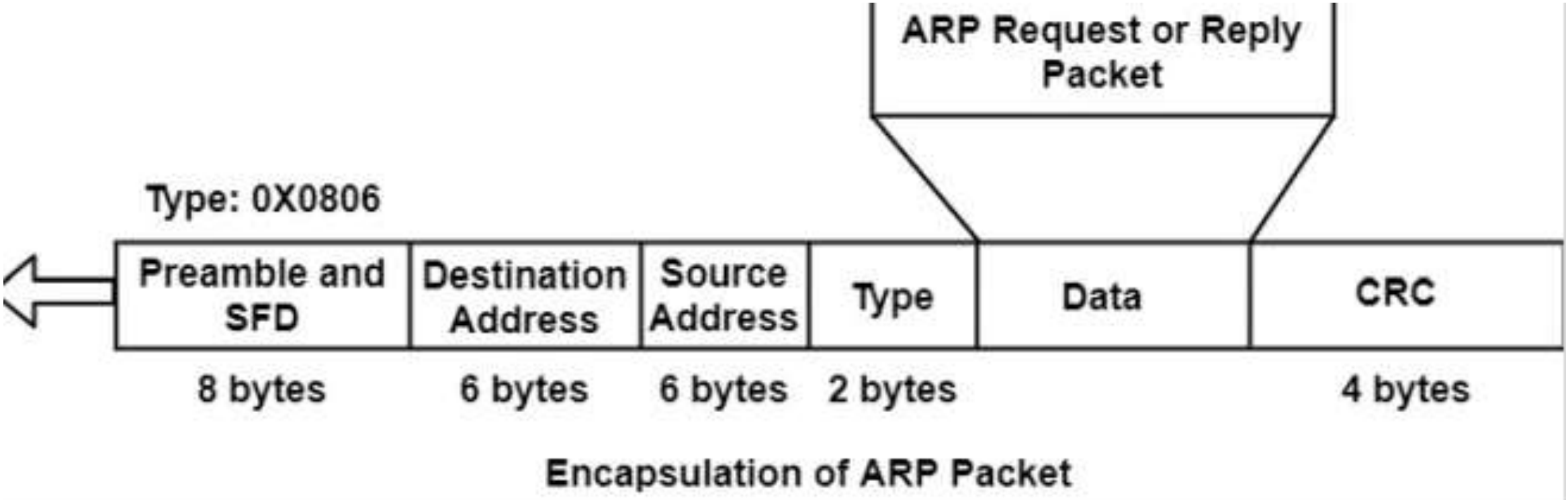
- Gratuitous ARP is almost like an administrative procedure, carried out as a way for a host on a network to simply announce or update its IP-to-MAC address. Gratuitous ARP is not prompted by an ARP request to translate an IP address to a MAC address.

Reverse ARP (RARP)

- Host machines that do not know their own IP address can use the Reverse Address Resolution Protocol (RARP) for discovery.

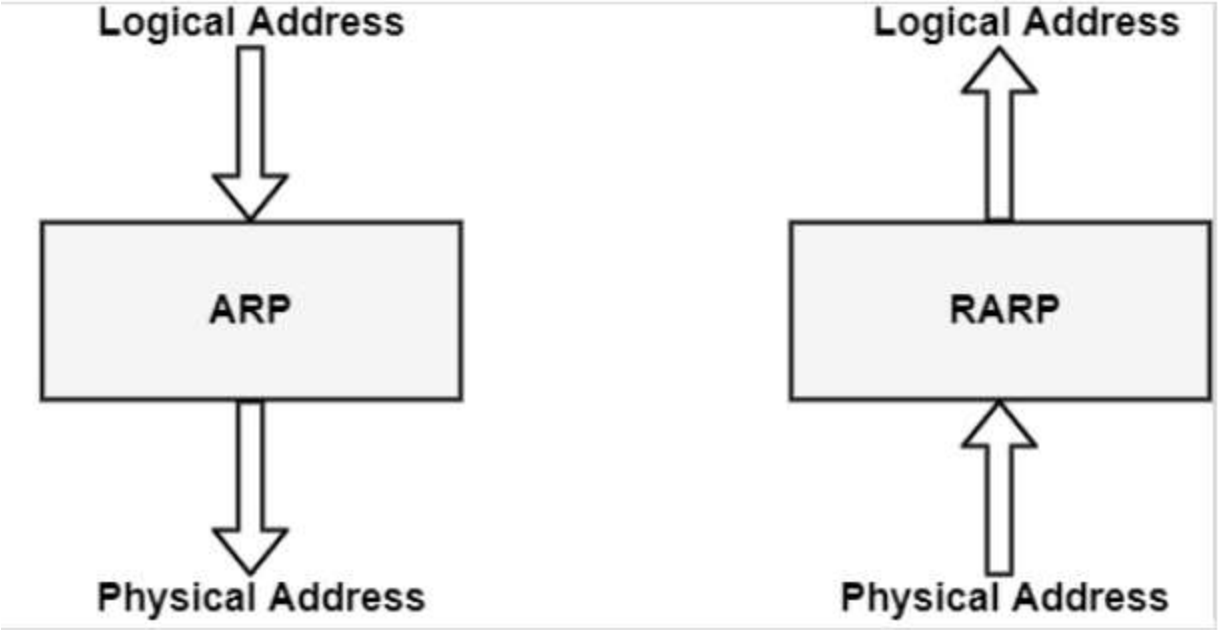
Inverse ARP (IARP)

- Whereas ARP uses an IP address to find a MAC address, IARP uses a MAC address to find an IP address.



Encapsulation of ARP Packet

Reverse Address Resolution Protocol (RARP)



- Reverse Address Resolution Protocol (RARP) is a network-specific standard protocol.
- Some network hosts, such as a diskless workstation, do not know their own IP address when they are booted.
- To determine their own IP address, they use a mechanism similar to ARP, but now the hardware address of the host is the known parameter, and the IP address is the queried parameter.
- The reverse address resolution is performed the same way as the ARP address resolution. The same packet format is used for the ARP.

- An exception is the operation code field that now takes the following values−
  - 3 for RARP request
  - 4 for RARP reply
- The physical header of the frame will now indicate RARP as the higher-level protocol (8035 hex) instead of ARP (0806 hex) or IP-(0800 hex) in the Ether type field.

- When a framework with a local disk is bootstrapped, it generally accepts its IP address from a configuration document that's read from a disk file.
- But a system without a disk, including an X terminal or a diskless workstation, needs some other way to accept its IP address.
- The feature of RARP is for the diskless framework to read its specific hardware address from the interface card and send a RARP request asking for someone to reply with the diskless systems IP address.

- The format of a RARP packet is almost identical to an ARP packet.
- The only difference is that the frame type is 0X8035 for a RARP request or reply, and the op-field has a value of 3 for a RARP request and 4 for a RARP reply.

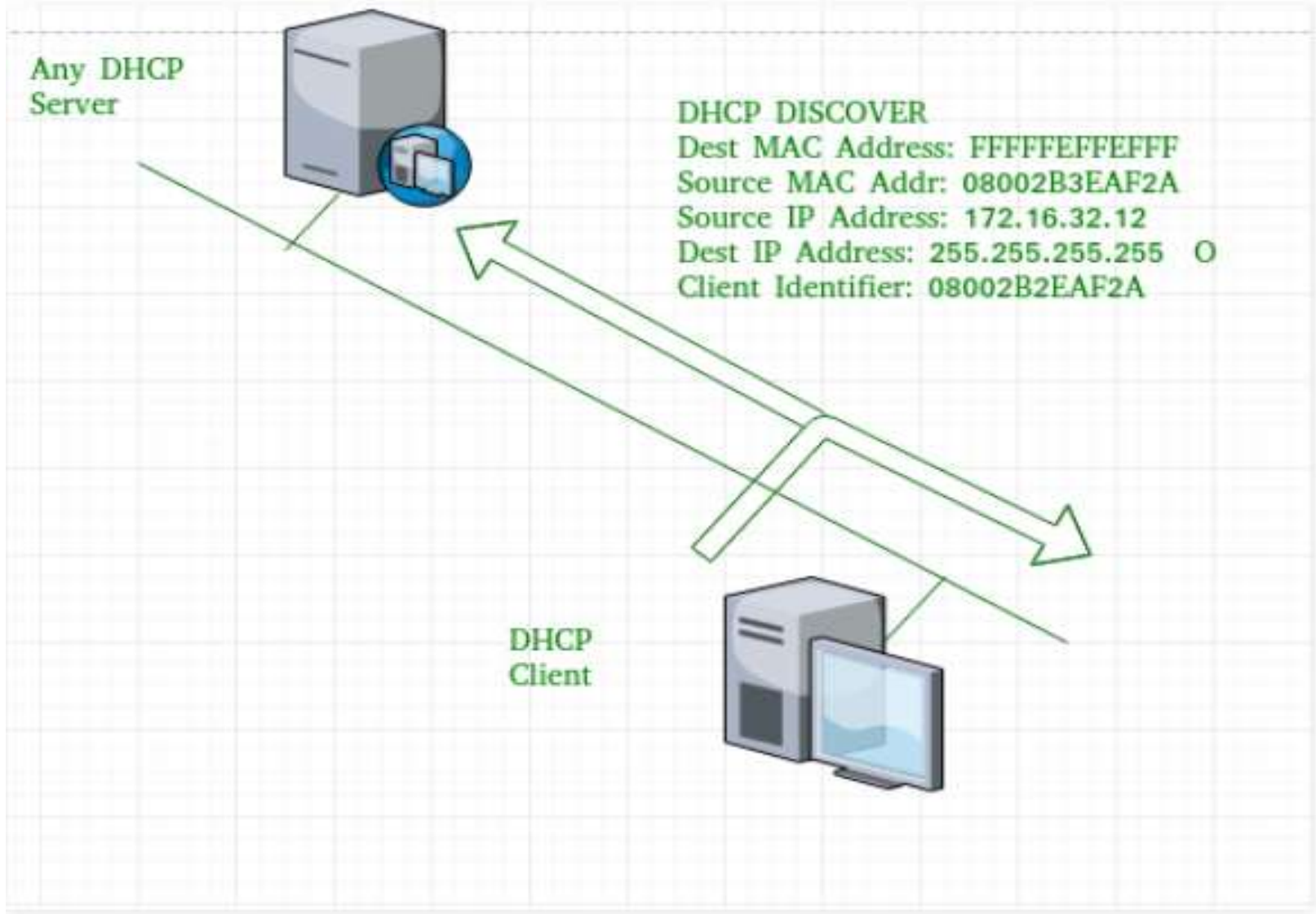
Dynamic Host Configuration Protocol(DHCP)

- DHCP is based on a client-server model and based on discovery, offer, request, and ACK.
- DHCP **port number** for server is 67 and for the client is 68.
- It is a Client server protocol which uses UDP services.
- IP address is assigned from a pool of addresses.
- In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called DORA process, but there are 8 DHCP messages in the process.

These messages are

DHCP discover message –

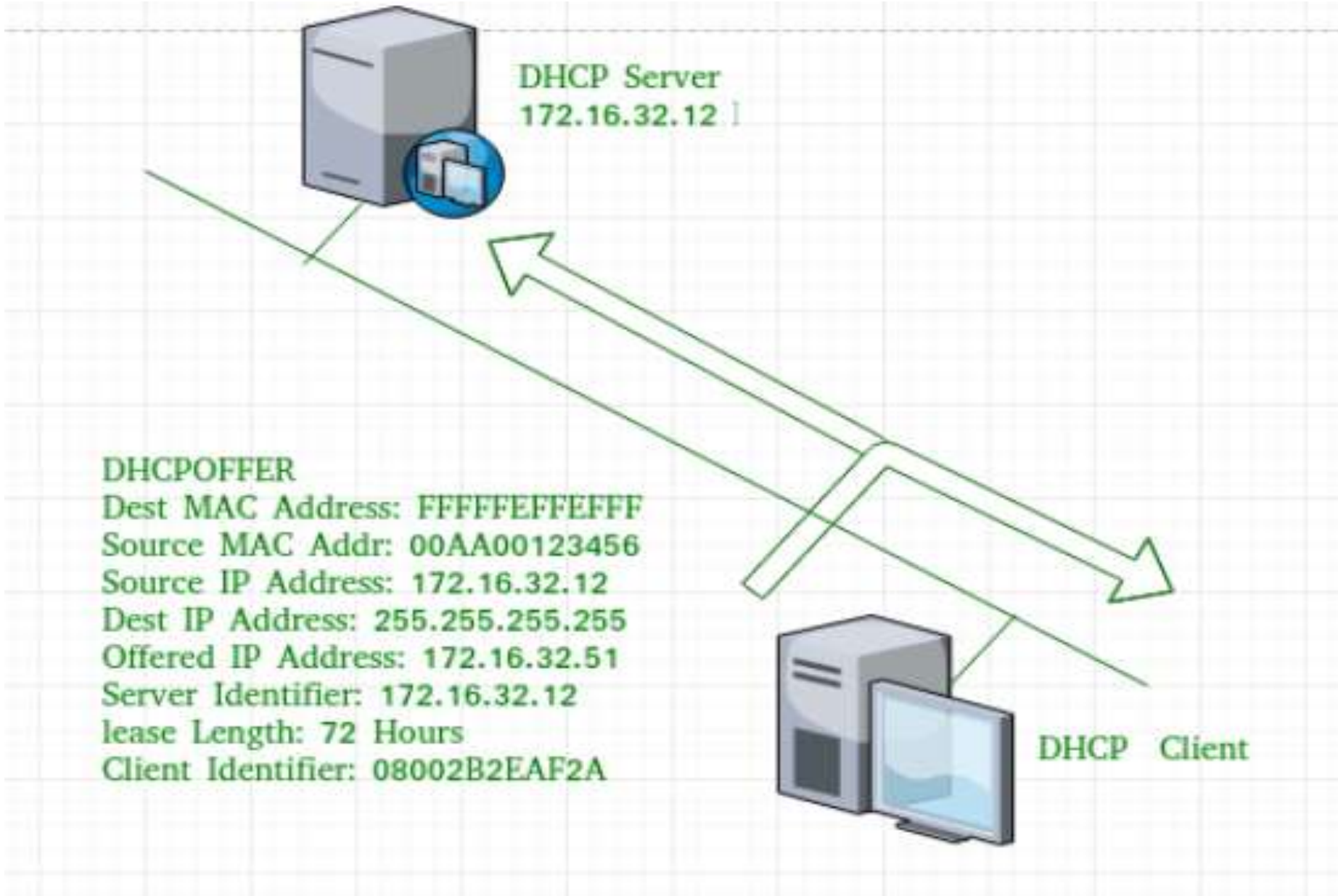
- This is a first message generated in the communication process between server and client.
- This message is generated by Client host in order to discover if there is any DHCP server/servers are present in a network or not.
- This message is broadcasted to all devices present in a network to find the DHCP server.
- This message is 342 or 576 bytes long


Any DHCP
Server
DHCP DISCOVER
Dest MAC Address: FFFFFEFFEFFF
Source MAC Addr: 08002B3EAF2A
Source IP Address: 172.16.32.12
Dest IP Address: 255.255.255.255 O
Client Identifier: 08002B2EAF2A
DHCP
Client

- As shown in the figure, source MAC address (client PC) is 08002B2EAF2A, destination MAC address(server) is FFFFFFFFFFFF, source IP address is 0.0.0.0(because PC has no IP address till now) and destination IP address is 255.255.255.255 (IP address used for broadcasting).
- As the discover message is broadcast to find out the DHCP server or servers in the network therefore broadcast IP address and MAC address is used.

- **DHCP offer message –**

  The server will respond to host in this message specifying the unleased IP address and other TCP configuration information.
- This message is broadcasted by server. Size of message is 342 bytes.
- If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives.
- Also a server ID is specified in the packet in order to identify the server.


DHCP Server
172.16.32.12
DHCPOFFER
Dest MAC Address: FFFFFEFFEFFF
Source MAC Addr: 00AA00123456
Source IP Address: 172.16.32.12
Dest IP Address: 255.255.255.255
Offered IP Address: 172.16.32.51
Server Identifier: 172.16.32.12
lease Length: 72 Hours
Client Identifier: 08002B2EAF2A
DHCP Client

- Now, for the offer message,

--- source IP address is 172.16.32.12 (server's IP address in the example),

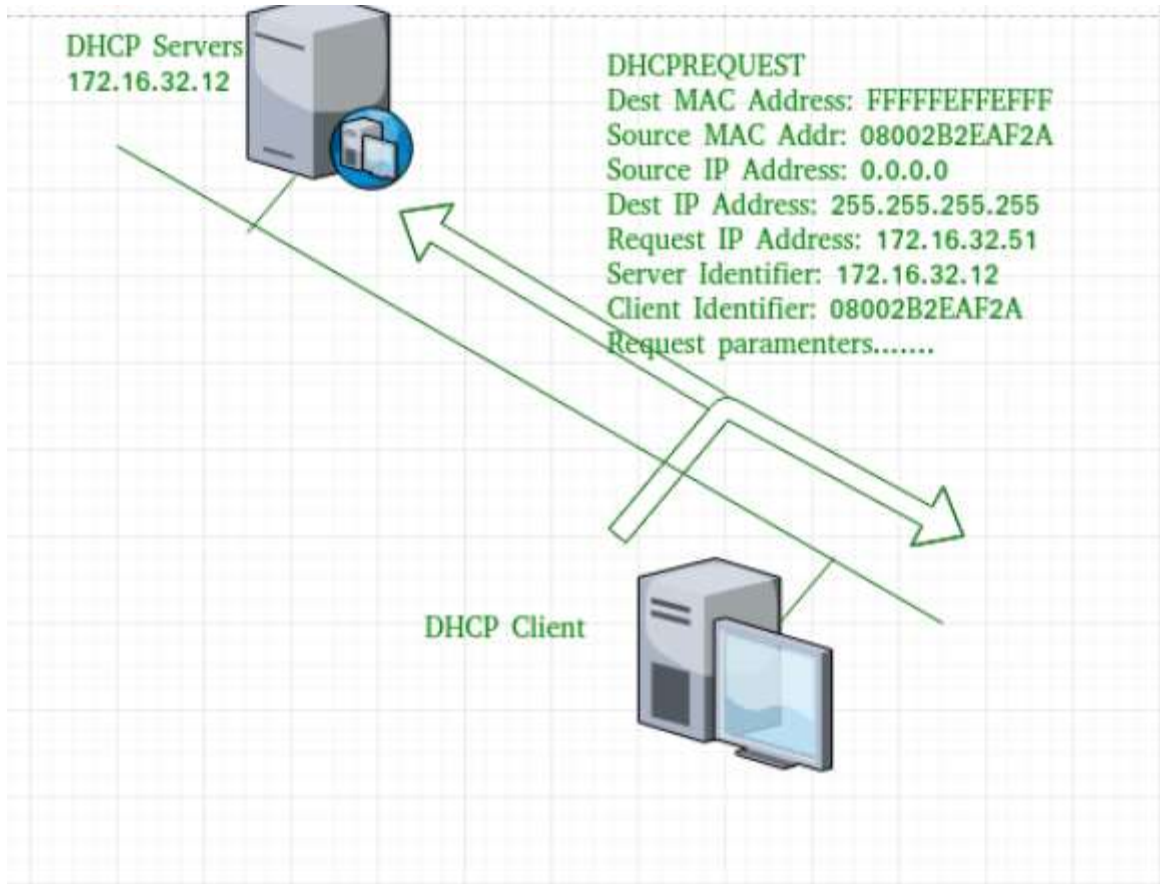
--- destination IP address is 255.255.255.255 (broadcast IP address) ,

--- source MAC address is 00AA00123456,

--- destination MAC address is FFFFFFFFFFFF.

- Here, the offer message is broadcast by the DHCP server
- Therefore destination IP address is broadcast IP address and
- destination MAC address is FFFFFFFFFFFF and
- the source IP address is server IP address and
- MAC address is server MAC address.

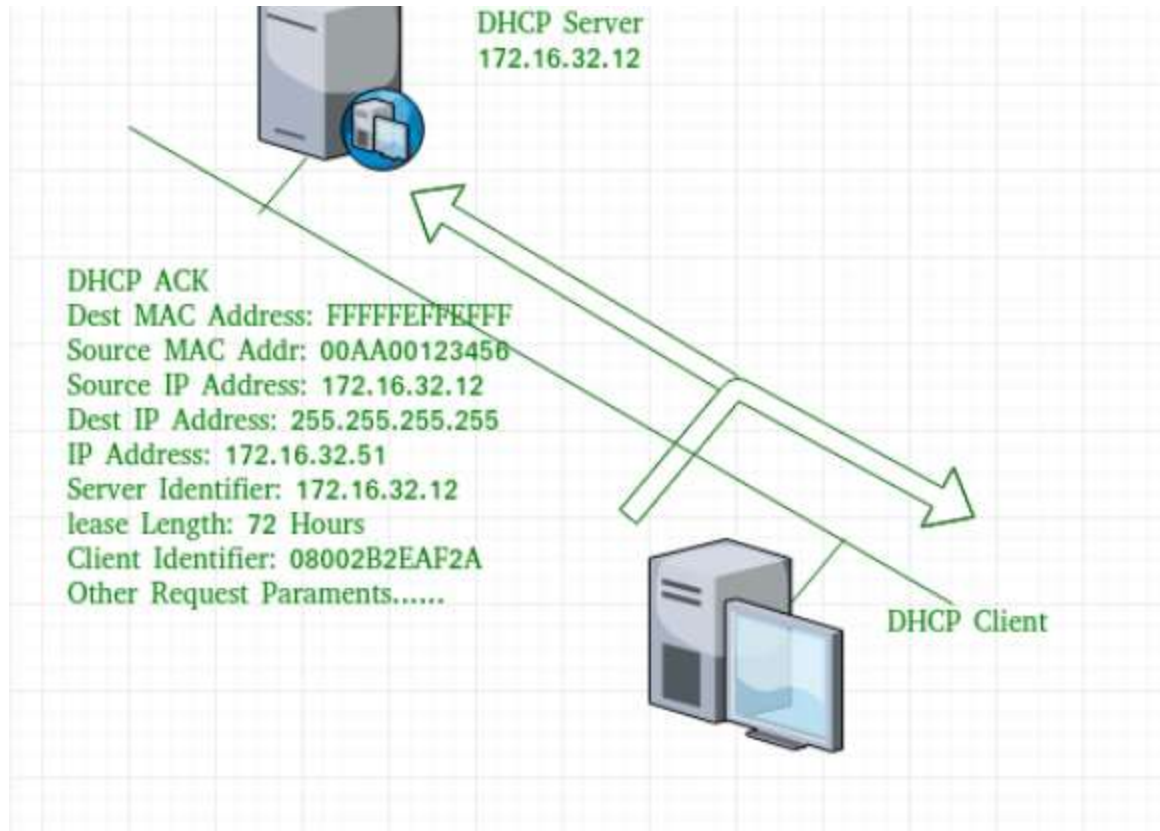
- **DHCP request message –**
  When a client receives a offer message, it responds by broadcasting a DHCP request message.
- The client will produce a gratuitous ARP in order to find if there is any other host present in the network with same IP address.
- If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP address .
- A Client ID is also added in this message.


DHCP Servers
172.16.32.12
DHCPREQUEST
Dest MAC Address: FFFFFEFFEFFF
Source MAC Addr: 08002B2EAF2A
Source IP Address: 0.0.0.0
Dest IP Address: 255.255.255.255
Request IP Address: 172.16.32.51
Server Identifier: 172.16.32.12
Client Identifier: 08002B2EAF2A
Request paramenters.....
DHCP Client

- Now, the request message is broadcast by the client PC therefore source IP address is 0.0.0.0(as the client has no IP right now) and destination IP address is 255.255.255.255 (broadcast IP address) and source MAC address is 08002B2EAF2A (PC MAC address) and destination MAC address is FFFFFFFFFFFF.

- **DHCP acknowledgement message –**

  In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.


DHCP Server
172.16.32.12
DHCP ACK
Dest MAC Address: FFFFFEFFFFFF
Source MAC Addr: 00AA00123456
Source IP Address: 172.16.32.12
Dest IP Address: 255.255.255.255
IP Address: 172.16.32.51
Server Identifier: 172.16.32.12
lease Length: 72 Hours
Client Identifier: 08002B2EAF2A
Other Request Paraments.....
DHCP Client

- Now the server will make an entry of the client host with the offered IP address and lease time.
- This IP address will not be provided by server to any other host.
- The destination MAC address is FFFFFFFFFFFF and the destination IP address is 255.255.255.255 and the source IP address is 172.16.32.12 and the source MAC address is 00AA00123456 (server MAC address).

- **DHCP negative acknowledgement message –**

  Whenever a DHCP server receives a request for IP address that is invalid according to the scopes that is configured with, it send DHCP Nak message to client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to client.

- **DHCP decline –**

  If DHCP client determines the offered configuration parameters are different or invalid, it sends DHCP decline message to the server .When there is a reply to the gratuitous ARP by any host to the client, the client sends DHCP decline message to the server showing the offered IP address is already in use.

- **DHCP release –**

  A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.

- **DHCP inform –**

  If a client address has obtained IP address manually then the client uses a DHCP, inform to obtain other local configuration parameters, such as domain name. In reply to the DHCP inform message, DHCP server generates DHCP ack message with local configuration suitable for the client without allocating a new IP address.

- This DHCP ack message is unicast to the client.

Advantages

- centralized management of IP addresses
- ease of adding new clients to a network
- reuse of IP addresses reducing the total number of IP addresses that are required
- simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client

Disadvantages –

IP conflict can occur

https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/

- Also the server has provided the offered IP address 192.16.32.51 and lease time of 72 hours(after this time the entry of host will be erased from the server automatically) . Also the client identifier is PC MAC address (08002B2EAF2A) for all the messages.