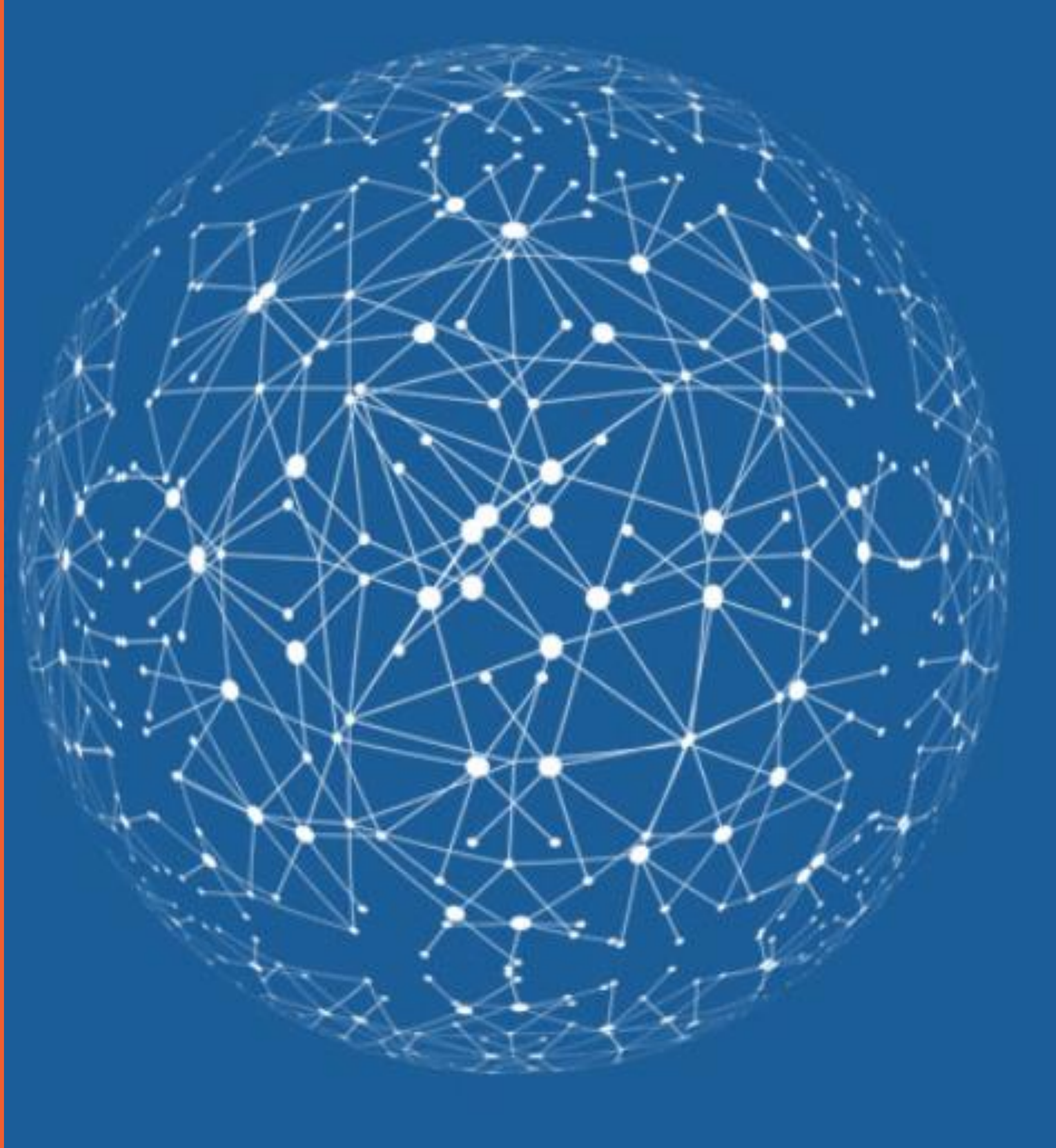
Tutorial
ELEC3506/9506
Communication Networks

School of Electrical and Information Engineering
The University of Sydney

Dr. Shuvashis Saha
shuvashis.saha@sydney.edu.au

Tutorial 05 – Week 06



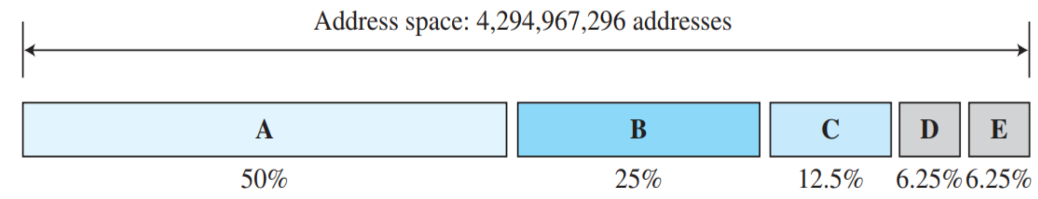
Q1. What are the differences between classful and classless addressing in IPv4

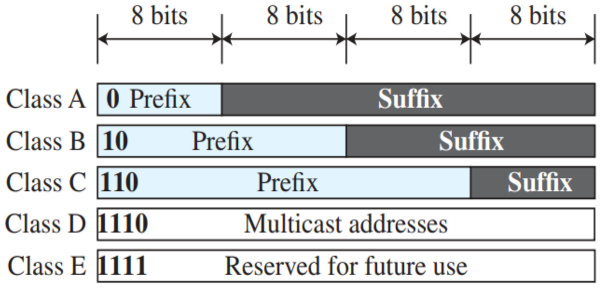
- Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols in the Network Layer.
- IP address (also known as logical address) is a unique addressing scheme to provide a way to identify all hosts in the network (the internet)
- Each node (computer, server, etc.) using the TCP/IP protocol has a unique and universal 32 bit logical IP address.
- There is a total of 2^32 = 4295M IP addresses in IPv4
- Each IP address has 2 parts: the network number (netID) and host number(hostID).

Q1. What are the differences between classful and classless addressing in IPv4

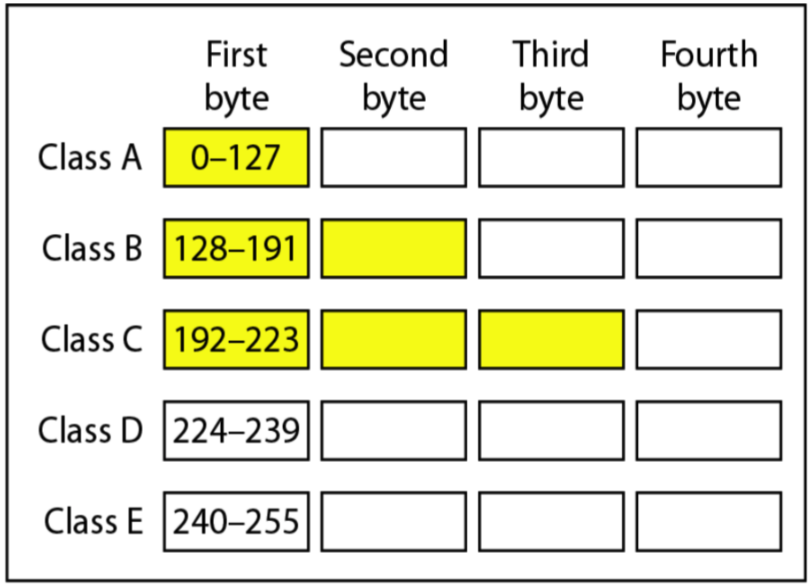
- The IP addresses are distributed based on 2 mechanisms:
- Classful Addressing
  - Address Space is divided into five classes: A,B,C,D,E
  - Assigns an organization a Class A,B, or C block of addresses.

Classful Addressing System





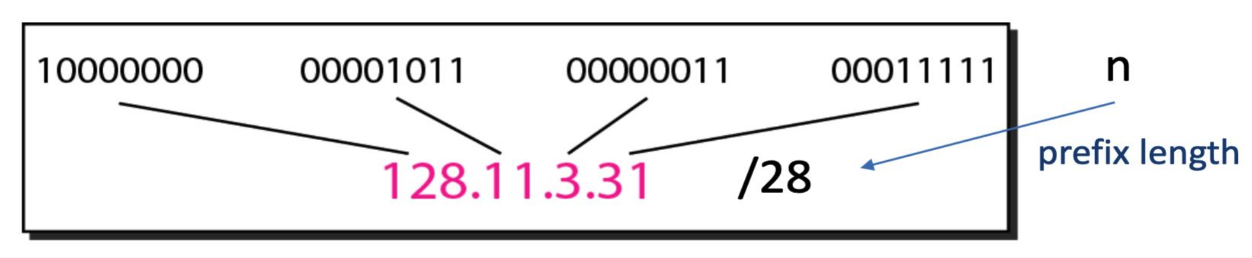
Class	Prefixes	First byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255



Class	Number of Blocks (Networks)	Block (Network) Size
A	128	16 777 216
B	16 384	65 536
C	2 097 152	256
D	1	268 435 456
E	1	268 435 456

Q1. What are the differences between classful and classless addressing in IPv4

- Classless addressing
  - Now more commonly used to deal with address shortage
  - No class definition
  - The address contains a prefix length "n", where n = 0, …. , 32, to classify IP address belong to a specific block.



  - Based on any IP address (that belongs to a specific block), we can calculate the number of available address in that block, as well as the first and last IP addresses that belong to that block.
  - Based on the example above, there is a total of 2^(32-28) = 16 addresses that belong in that block. The first address is 128.11.3.16, and the last address if 128.11.3.31

Q1. What are the differences between classful and classless addressing in IPv4

Example:

- A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.39/28. What is (a) the first address, (b) the last address, and (c) the number of addresses in the block?

Solution

- The binary representation of the given address is:

11001101 00010000 00100101 00100111

(a) If we set $32 - 28 = 4$ rightmost bits to 0, we get the first address:

11001101 00010000 00100101 00100000 i.e. 205.16.37.32

(b) If we set $32 - 28 = 4$ rightmost bits to 1, we get the last address:

11001101 00010000 00100101 00101111 i.e. 205.16.37.47

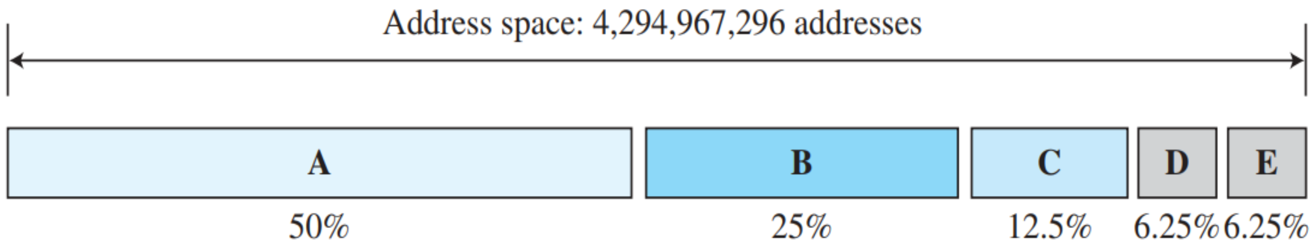
(c) Here, $n = 28$. Hence, the number of addresses:

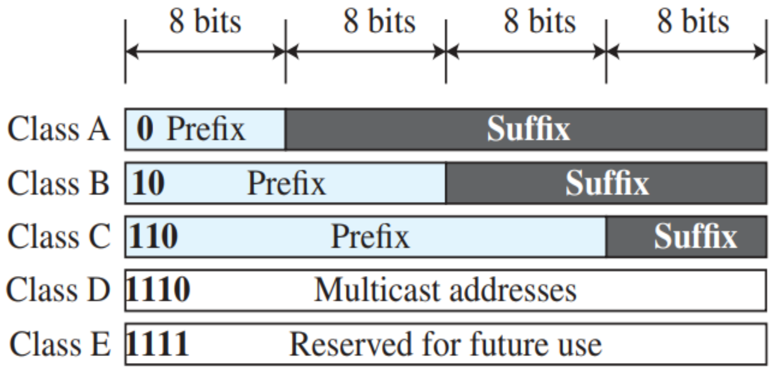
$$= 2^{32-n} = 2^{32-28} = 2^4 = 16$$

Q2. a) Explain why most of the addresses in Class A are wasted? b) Explain why a medium/large size organization does not want a block of class C

a) A block in class a is too large for almost any organisation. This means most of the addresses in class A are wasted and not used

b) A block in class C is too small for many medium/large size organisation.





Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

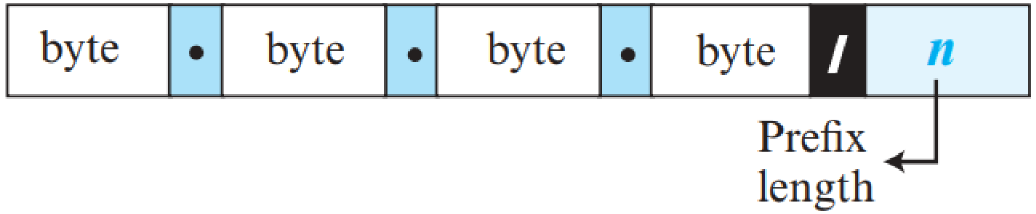
Q3. What is a mask in IPv4 addressing?

- A mask is a 32-bit number in which the n leftmost bits are 1s and the (32-n) rightmost bits are 0s.
- Classful Addressing
  - n = 8,16,24
  - Used to find the netid and hostid
  - The concept of mask does not apply for class D and E

Default masks for classful addressing

Class	*Binary*	*Dotted-Decimal*	*CIDR*
A	**11111111** 00000000 00000000 00000000	**255**.0.0.0	/8
B	**11111111 11111111** 00000000 00000000	**255.255**.0.0	/16
C	**11111111 11111111 11111111** 00000000	**255.255.255**.0	/24

Classless interdomain routing or CIDR



Examples:
12.24.76.8/**8**
23.14.67.92/**12**
220.8.24.255/**25**

Q4. a) What is the network address in a block of address? b) How can we find the network address if one of the addresses in the block is known.

a) The network address in a block of addresses is the first address.

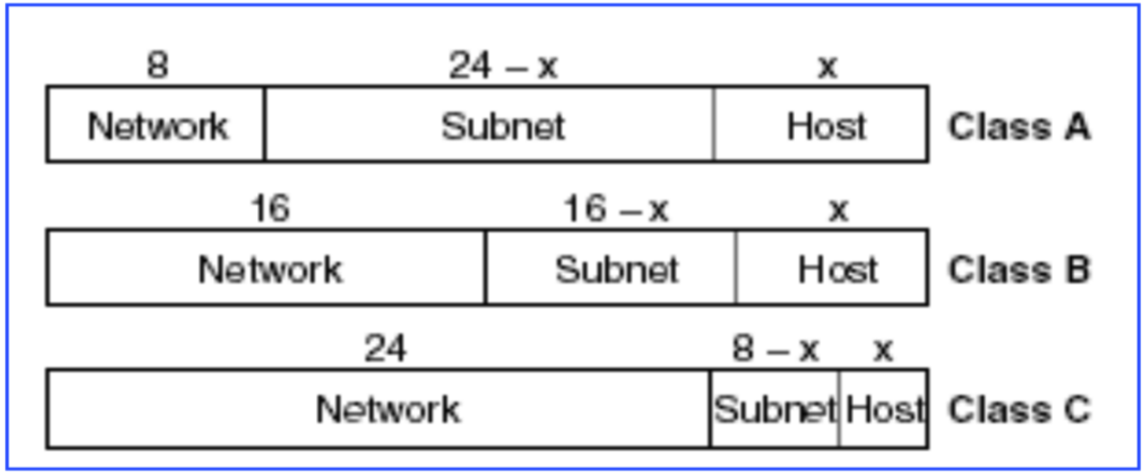
b) The mask can be ANDed with any address in the block to find the network address.

Example: Address is 205.16.37.34/28

Mask :	11111111	11111111	11111111	11110000
Address:	11001101	00010000	00100101	00100010
ANDed :	11001101	00010000	00100101	00100000 => 205.16.37.32

Q5. Briefly define subnetting. How does the subnet mask differ from the default mask in classful addressing?

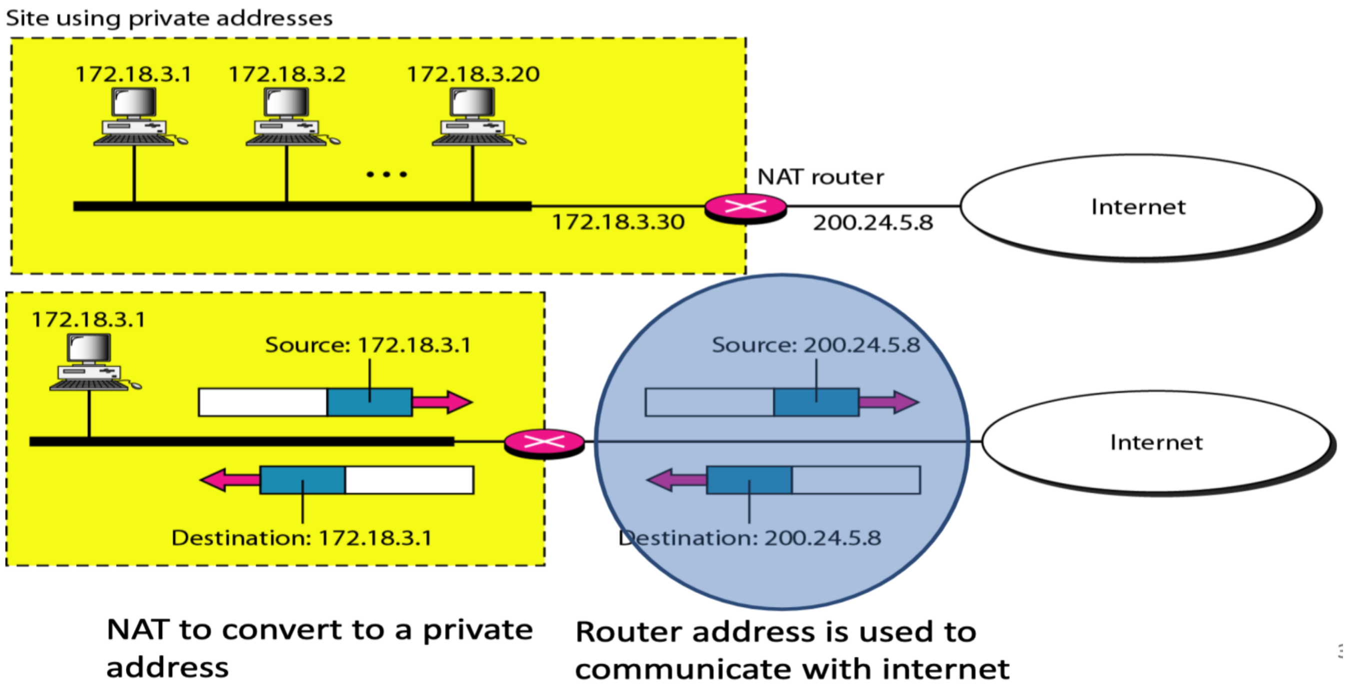
- In Subnetting, a large address block could be divided into several contiguous groups and each group can be assigned to smaller networks classed subnets. This is the foundation of classless addressing.
- With subnetting, the IP address now consist of:
  - ✓network,
  - ✓subnet, and
  - ✓host.



- The number of host per subnet: 2^x – 2 (minus 2 because the first address is used as the network address and the last address is used as broadcast)
- The subnet mask is defined with a value of \n
- The subnet mask has more consecutive 1s than the corresponding default mask

Q6. What is NAT? How can NAT help in address depletion?

- Home users and small businesses may create small networks with several hosts and need an IP address for each host. The shortage of addresses is a serious problem. A quick solution to this problem is the network address translation (NAT)
- NAT is a mechanism that enables user to have a large set of addresses internally and one/small set of addresses externally to communicate with the other networks (the internet).



Q6. What is NAT? How can NAT help in address depletion?

- What happened if two devices are accessing the same server?
  - We use port addresses to specify the destination inside our private network

Private Address	Private Port	External Address	External Port	Transport Protocol
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
. . .	. . .	. . .	. . .	. . .

Q7. What is the difference between Connection-Oriented and Connectionless Services?

Connection-Oriented Service

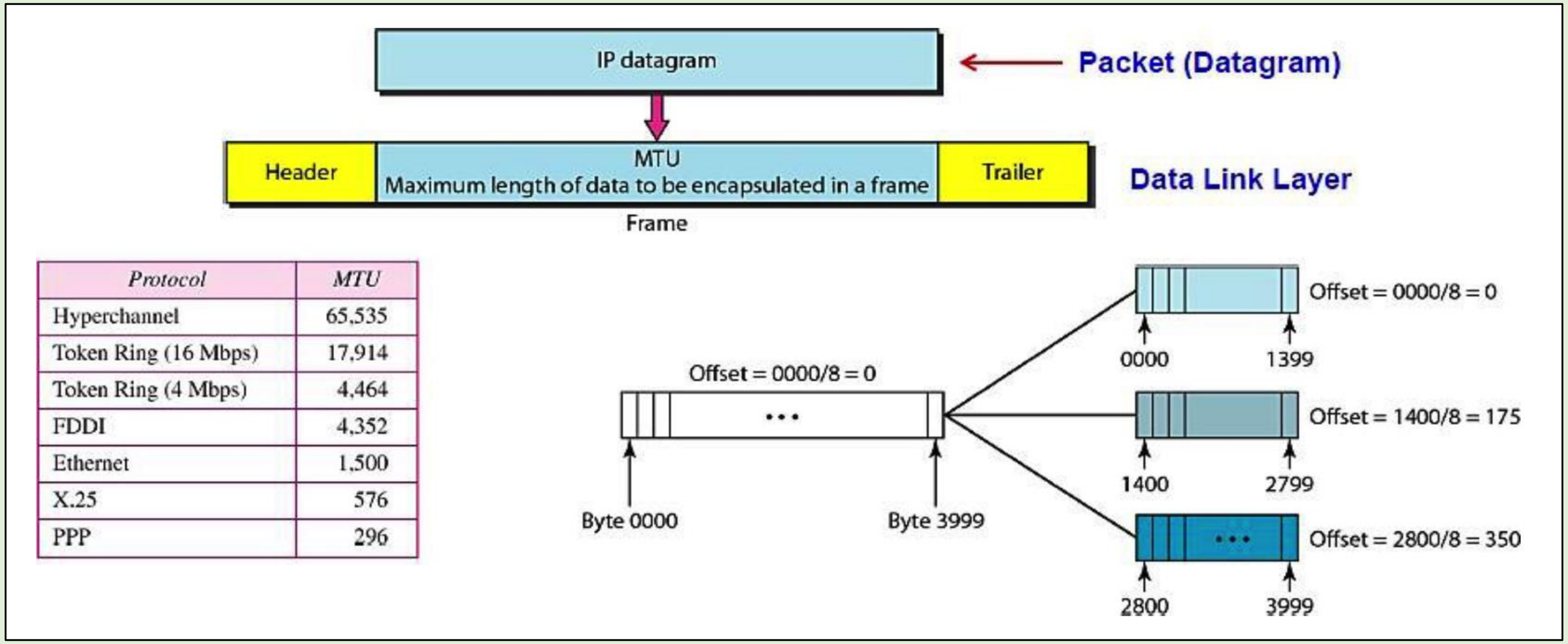
- A virtual connection is established between the sender and the receiver before transferring data
- All packets follow the same path.
- Communication has three phases: setup, data transfer, and teardown
- Example: Virtual circuit approach of packet switching.

Connectionless Service

- Each packet is independent from every other packet and can take different path
- Communication has only one phase: data transfer
- No setup and teardown process
- Example: Datagram approach of packet Switching

Q8. Define Fragmentation and why is it needed?

- Each data link layer protocol has a maximum limit on the size of the packet it can carry. When a datagram is encapsulated in a frame, the total size of the datagram must be less than this limit. Otherwise, the datagram must be fragmented.

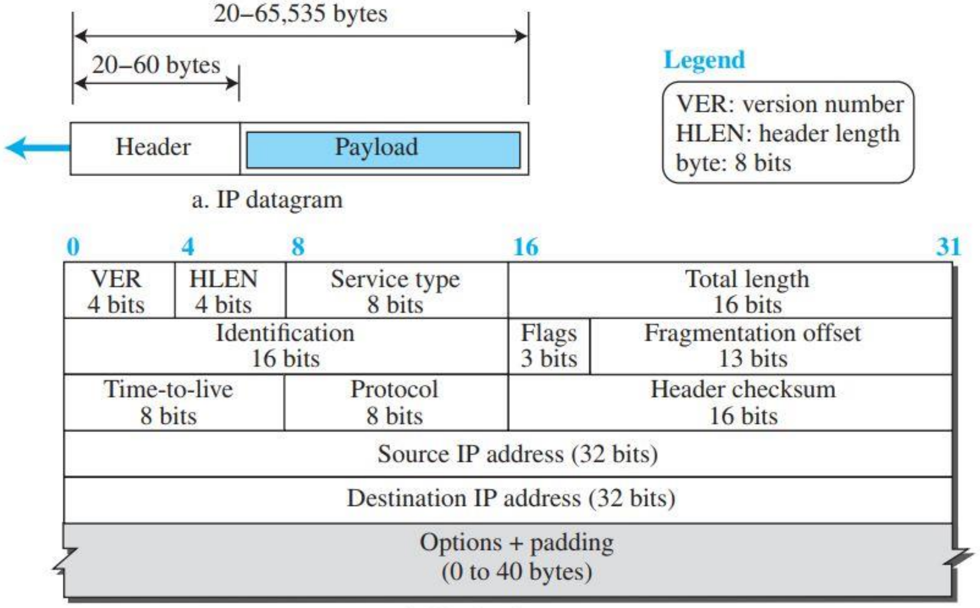


Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

- The fragmentation offset shows the relative position of the fragments with respect to the whole diagram (in units of 8 bytes)

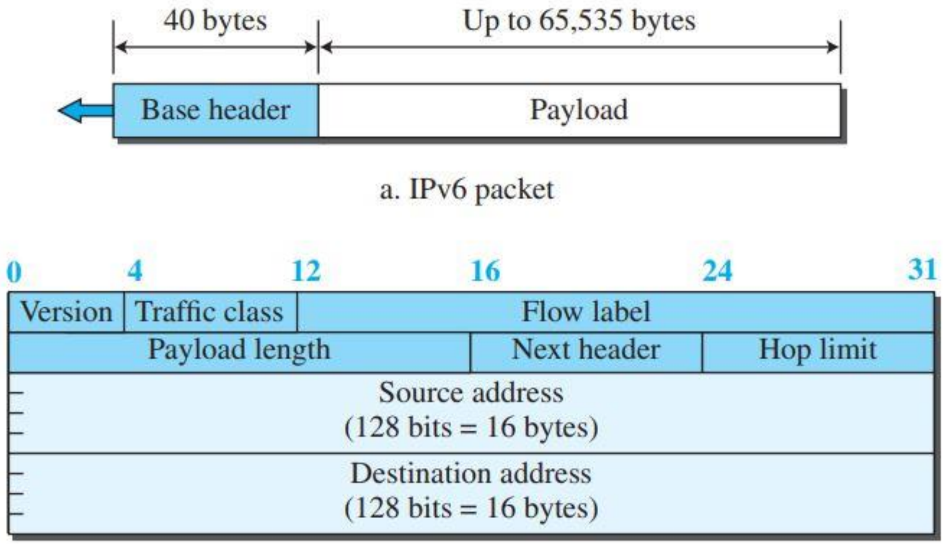
Q9. List transition strategies to move from IPv4 to IPv6. Explain the differences between tunneling and dual stack strategies during the transition period.

IPv4	IPv6
32-bit IP address	128-bit IP address
4.3 billion IP address	7.9×10^{28} IP address
Address must be reused & masked	Every device can have a unique address
Less secure and flexible for the new applications	Highly secured and supports newer applications
167.199.170.82/27 10100111 11000111 10101010 01010010	Binary 1111111011110110 … 1111111100000000 Colon Hexadecimal FEF6:BA98:7654:3210:ADEF:BBFF:2922:FF00



a. IP datagram

b. Header format



a. IPv6 packet

b. Base header

Q9. List transition strategies to move from IPv4 to IPv6. Explain the differences between tunneling and dual stack strategies during the transition period.

- ❑ The main reason for migration from IPv4 to IPv6 is the small size of the address space in IPv4
- ❑ Three strategies have been devised by the IETF to help the transition:

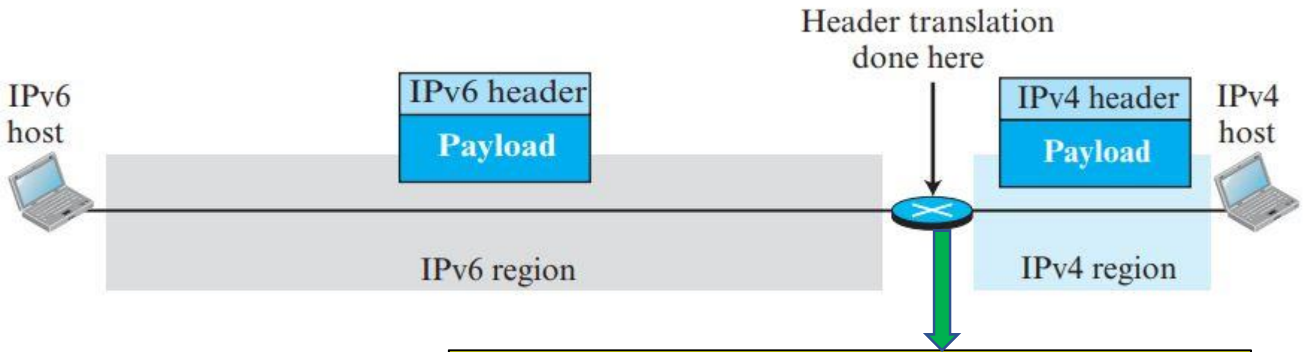
1. Header Translation Technique

2. Tunneling Technique

3. Dual Stack Technique

1. **Header Translation Technique**: Header translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4.

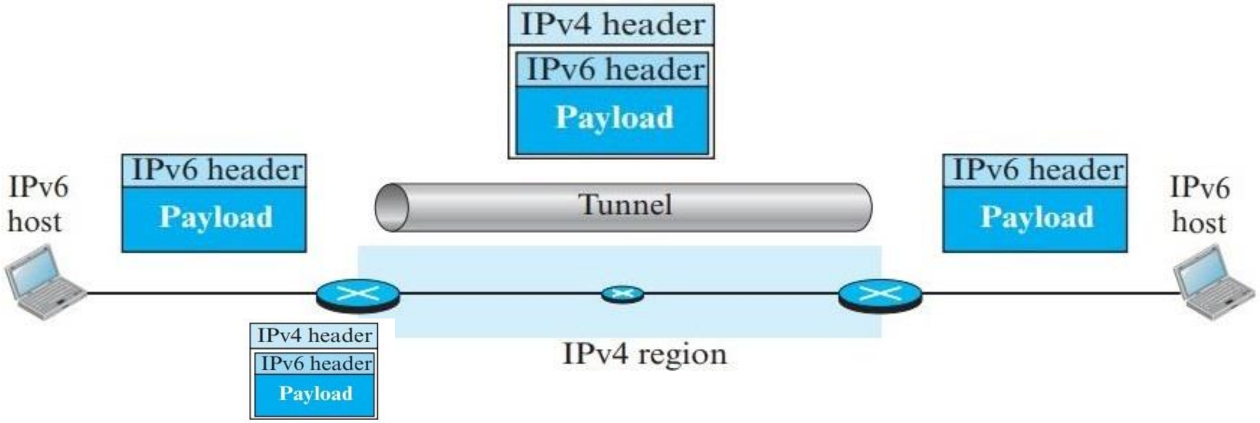
- ❑ The sender wants to use IPv6, but the receiver does not understand IPv6.
- ❑ In this case, the header format must be totally changed through header translation.



The header of the IPv6 packet is converted to an IPv4 header.

Q9. List transition strategies to move from IPv4 to IPv6. Explain the differences between tunneling and dual stack strategies during the transition period.

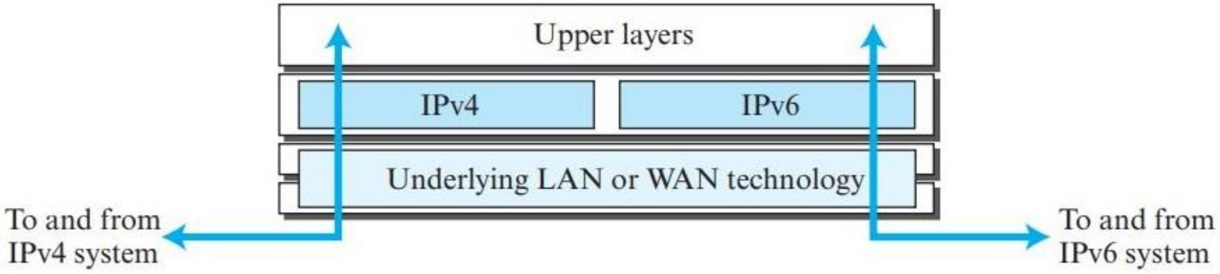
Tunneling



2. **Tunneling Technique**: Tunneling is a strategy used when two computers using IPv6 want to communicate with each other, and the packet must pass through a region that uses IPv4.

✓ So, the IPv6 packet is encapsulated in an IPv4 packet when it enters the region.

Dual Stack



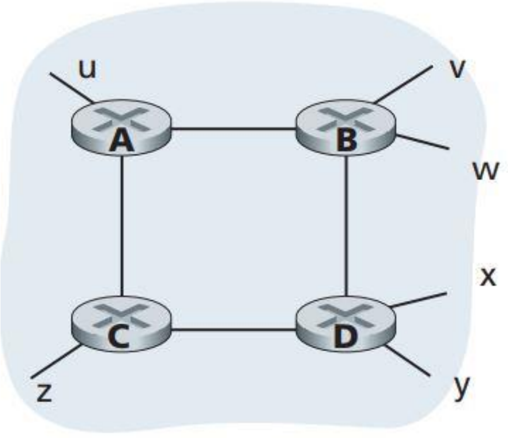
1. **Dual Stack Technique**: According to dual stack protocols, a station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6.

✓ If the DNS returns an IPv4 or IPv6 address, the source host sends an IPv4 or IPv6 packet, respectively.

Q10. What is the purpose of RIP?

- **The Routing Information Protocol (RIP)** is one of the most widely used intradomain routing protocols based on the distance-vector routing algorithm.
- RIP uses **hop count** to determine the shortest path.

- **Hops counting** from source router **A** to various subnets.



Destination	Hops
u	1
v	2
w	2
x	3
y	3
z	2

Purpose of Routing Information Protocol (RIP)

- To forward the packets, one of the available routes is to be chosen by the network layer, routing protocols handle this function

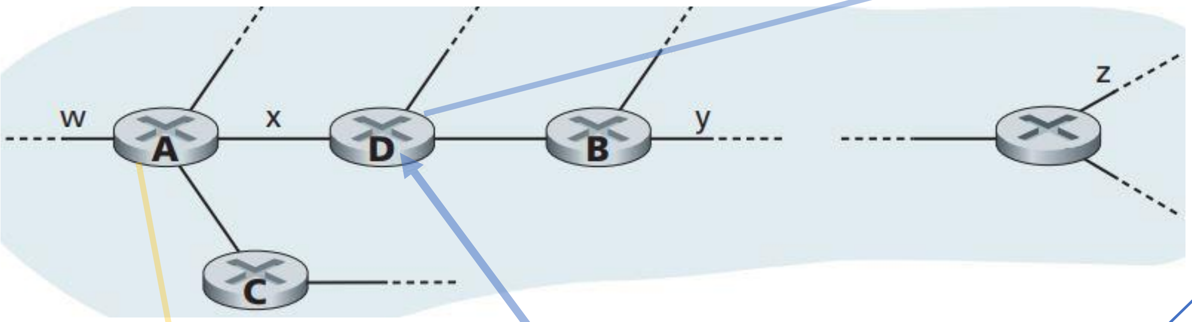
- If more than one possible route exist to reach one subnet, pick the best route based on a hop count.

- In case of link failure, it can forward the packets in different route.

- Advertise routing information about IP subnets to other neighboring routers

Q10. What is the purpose of RIP?

- Each router maintains a RIP table known as a routing table. The routing table has three columns.
- a) **Destination Subnet**, b) **Number of Hops** and c) **Identity of the next Router**



Routing table in router D before receiving advertisement from router A

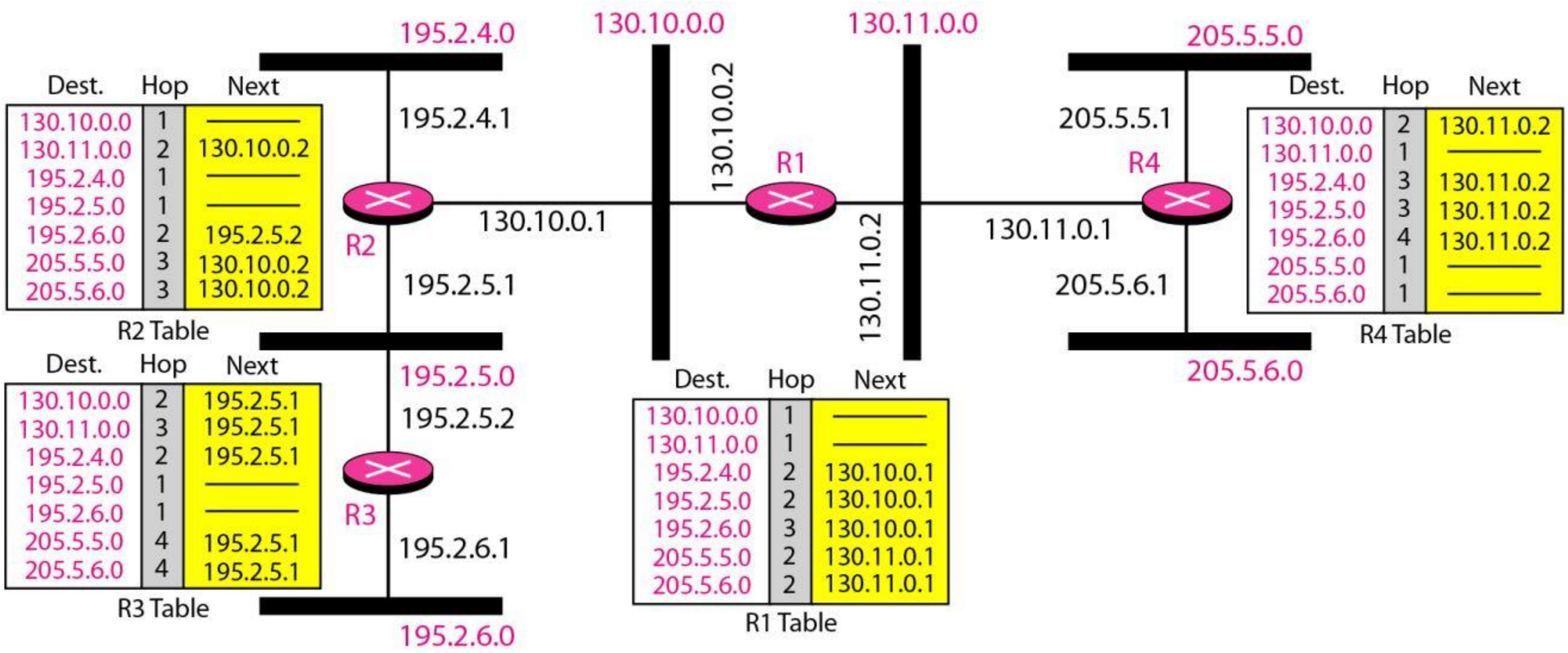
Destination subnet	Hop number	Next router
w	2	A
y	2	B
z	7	B
x	1	---

Routing table in router A, which is advertised to router D

Destination subnet	Hop number	Next router
z	4	C
w	1	---
x	1	---

Q10. What is the purpose of RIP?

Example of a domain using RIP



Q11. What are the functions of a RIP message?

- ❑ RIP has two types of messages:

Request messages

Response messages

Request messages: A request message is sent by a router that has just come up or by a router that has some time-out entries.

Response messages: A response (or update) message can be either solicited or unsolicited.

- ❑ **Solicited**: Sent only in answer to a request message.
- ❑ **Unsolicited**: Sent periodically, every 30 seconds or change in the forwarding table.

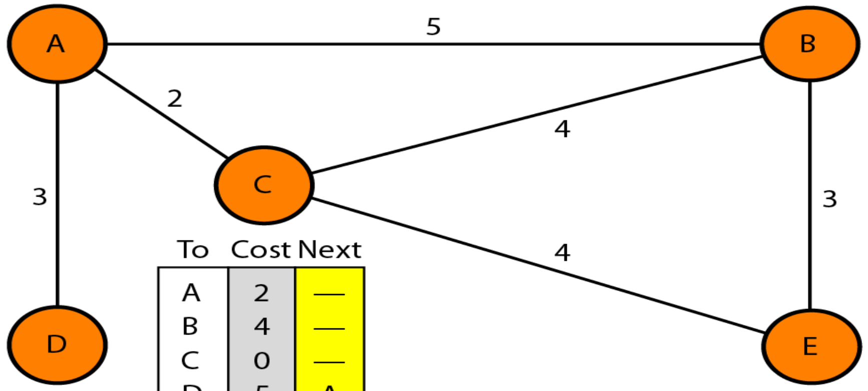
Final State

A's table

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

B's table

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



D's table

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

C's table

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

E's table

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

- ❑ In Figure, we show a system of five nodes with their corresponding tables.

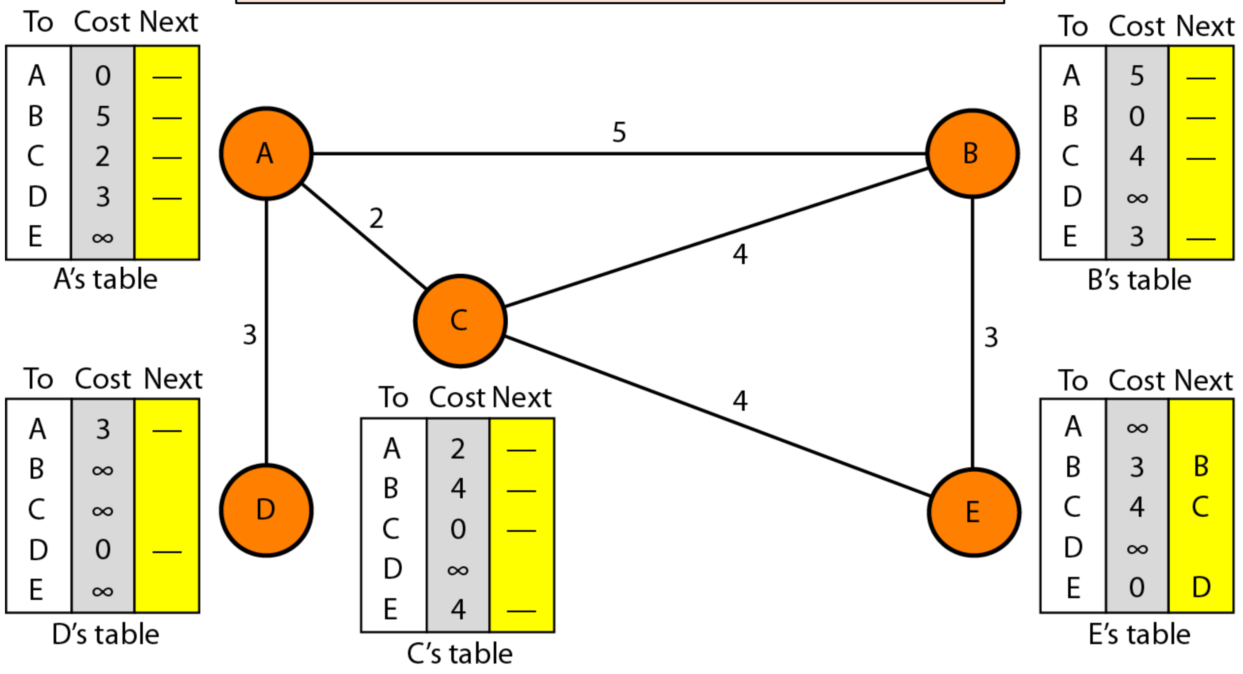
Initialization

- ❑ Stable connection; each node knows how to reach any other node and the cost.
- ❑ **At the beginning**, however, this is not the case.
- ❑ **Only directly connected information.**

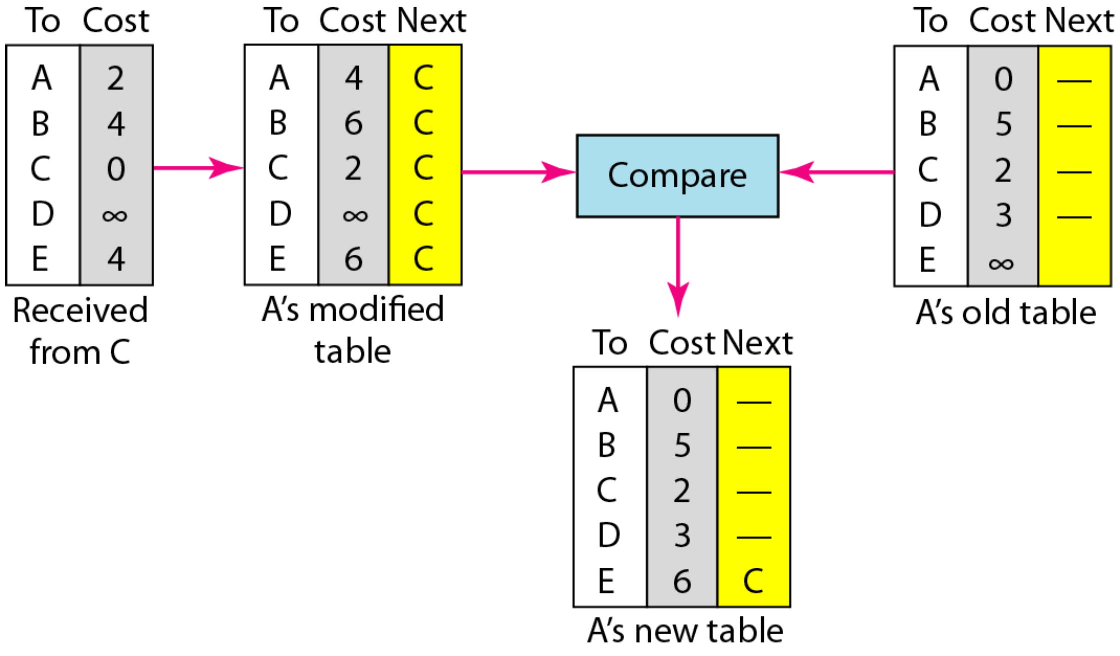
Q11. What are the functions of a RIP message?

- ❑ At the beginning, each of the router shares their routing table to directly connected all the routers also known as **Neighbour Router**.

Initialization State



Sharing and Updating State

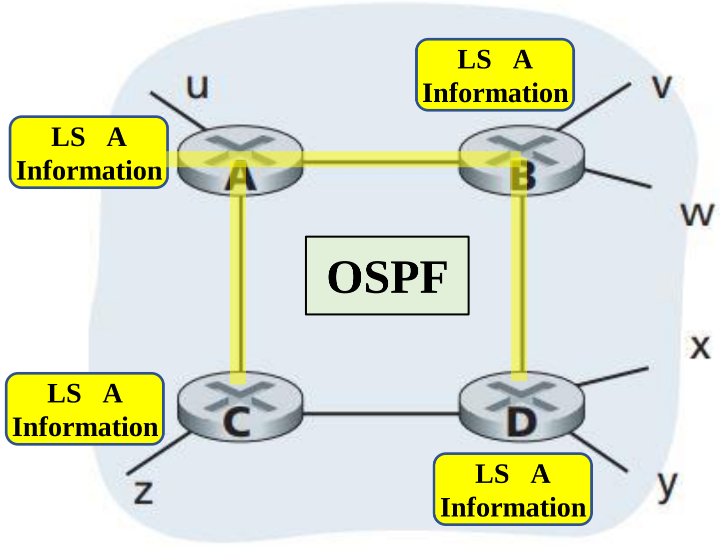


- ❑ Node A does not know about node E, node C does.
- ❑ Node D does not know about node C & B, node A does.

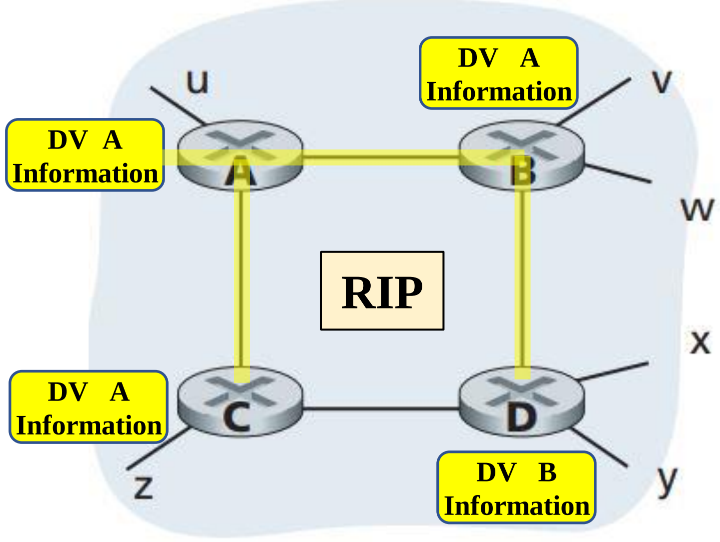
- ❑ Node A updates its routing table after receiving the partial table from node C.

Q12. Why do OSPF messages propagate faster than RIP messages?

- **Open Shortest Path First (OSPF):** OSPF uses Link State (**LS**) Routing Protocols to find the shortest path.
- Whenever a link cost changes, the new link cost must be sent to all nodes (Flooding).
- When the flooding of LSPs is completed, each router can create its own shortest-path tree and forwarding table; convergence is fairly quick.

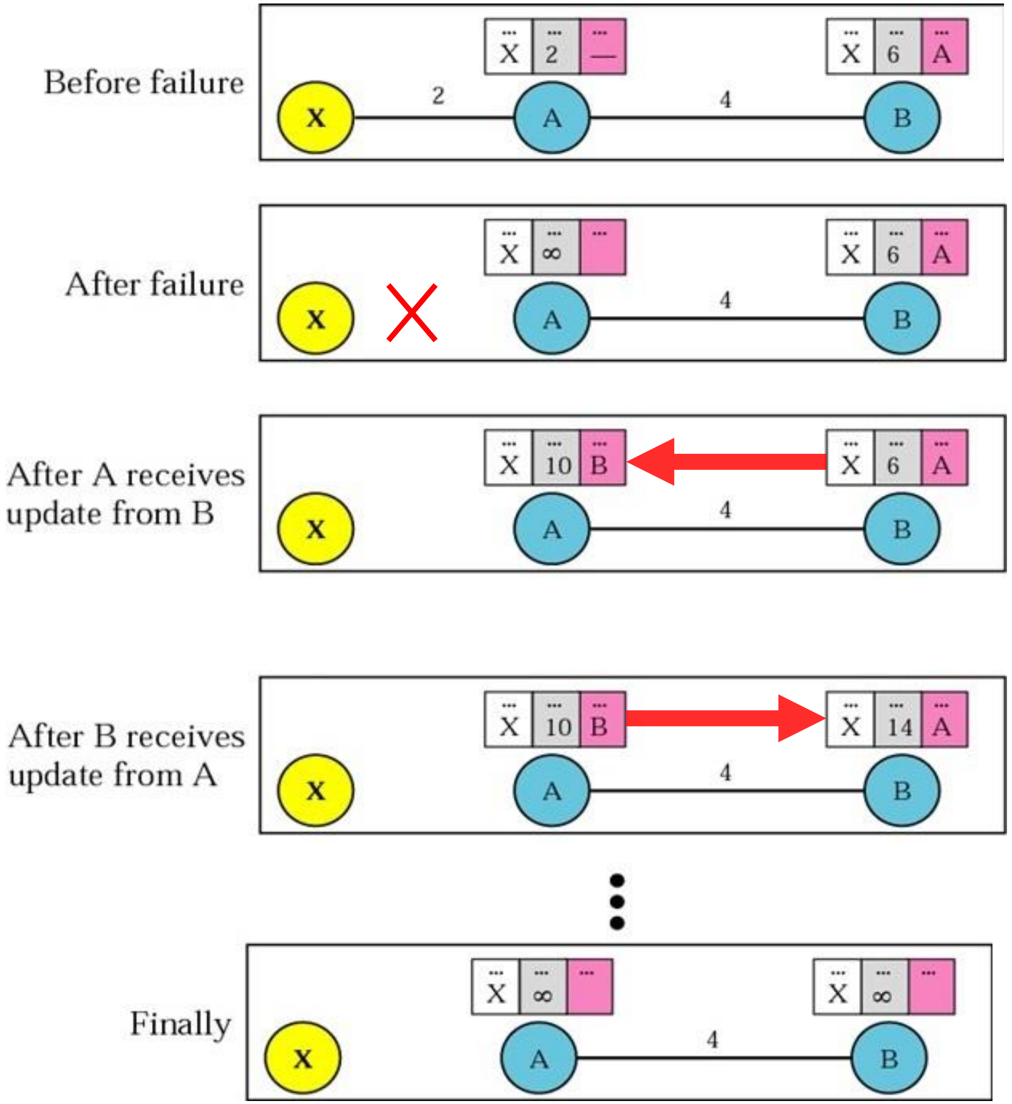


- **Routing Information Protocol (RIP):** RIP uses Distance Vector (**DV**) Routing Protocols to find the shortest path.
- When link costs change, the DV will propagate the results to one node attached to that link.
- The DV can converge slowly and can have routing loops while the algorithm is converging.
- DV also suffers from the count-to-infinity problem.



Q12. Why do OSPF messages propagate faster than RIP messages?

Count-to-infinity problem in RIP Protocol



- ❑ At the beginning, both nodes **A** and **B** know how to reach node **X**.

- ❑ The link between **A** and **X** fails and node **A** changes its table.
- ❑ If **A** can send its table to **B** immediately, everything is fine.

- ❑ **B** sends its routing table to **A** before receiving **A**'s routing table.
- ❑ **A** receives the update and assume that **B** has found a way to reach **X.**

- ❑ A also sends its new update to B. Now B thinks that something has been changed around **A** and updates its routing table.

- ❑ **Infinity Loop**: Node A thinks that the route to X is via B; node B thinks that the route to X is via A.

Q13. What is the purpose BGP?

- ❑ **Border Gateway Protocol** is an interdomain routing and gateway protocol. It connects the individual autonomous system (AS) into together by using path vector routing mechanism.

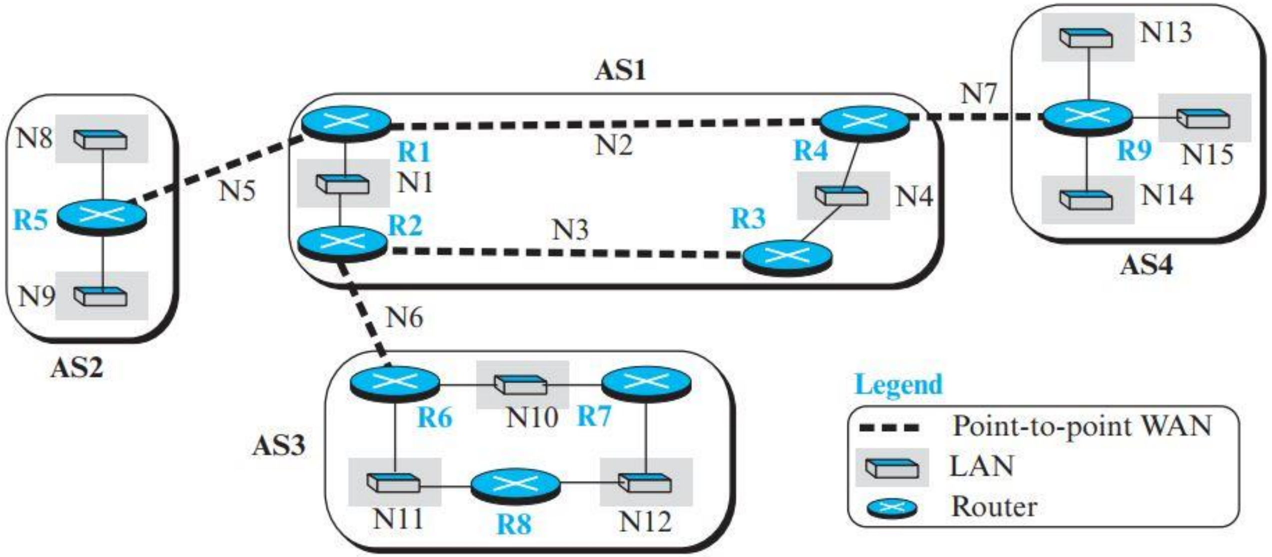
- ❑ Primary purpose of a BGP system is to exchange routing information among the autonomous system on the internet.

- ❑ In BGP, the ASs are divided into three categories;

- ❑ **Stub AS**: A stub AS has only one connection to another AS. The data traffic can be either initiated or terminated in a stub AS; the data cannot pass through it.

- ❑ **Multihomed AS**: A multihomed AS can have more than one connection to other ASs, but it does not allow data traffic to pass through it.

- ❑ **Transient AS**: A transient AS is connected to more than one other ASs and also allows the traffic to pass through.



- AS2, AS3, and AS4 are stub autonomous systems
- AS1 is a transient one.

Q13. What is the purpose BGP?

- **Path vector routing** proved to be useful for interdomain routing.
- The speaker node in an AS creates a routing table and advertises it to speaker nodes in the neighboring ASs.
- A speaker node advertises the path, not the metric of the nodes, in its autonomous system or other ASs.

- **Initialization:** At the beginning, each speaker node can know only the reachability of nodes inside its AS.

Speaker Node:
A1, B1. C1 and D1

Dest.	Path
A1	AS1
A2	AS1
A3	AS1
A4	AS1
A5	AS1

A1 Table

Dest.	Path
C1	AS3
C2	AS3
C3	AS3

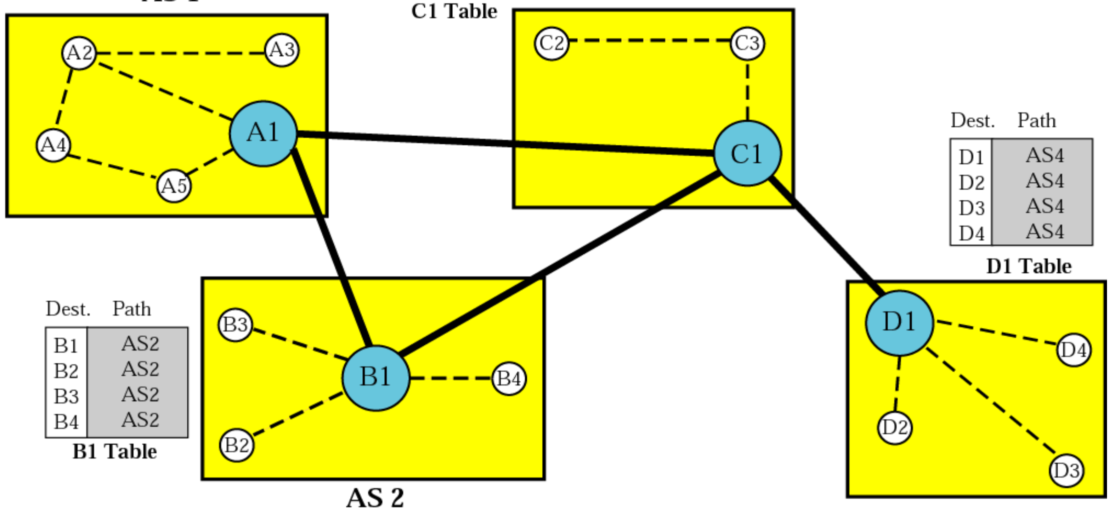
C1 Table

Dest.	Path
D1	AS4
D2	AS4
D3	AS4
D4	AS4

D1 Table

Dest.	Path
B1	AS2
B2	AS2
B3	AS2
B4	AS2

B1 Table



- **Sharing:** In path vector routing, a speaker in AS shares its table with immediate neighbors.

✓ Node **Al** shares its table with nodes **Bl** and **Cl**.

Updating (Speaker A1 of AS1)

- If router **Al** receives a packet for nodes **A3**, it knows that the path is in AS1 (the packet is at home).
- If it receives a packet for Dl, it knows that the packet should go from **AS1**, to **AS2**, and then to **AS3**.

Dest.	Path
A1 ... A5	AS1 ... AS1
B1 ... B4	AS1-AS2 ... AS1-AS2
C1 ... C3	AS1-AS3 ... AS1-AS3
D1 ... D4	AS1-AS3-AS4 ... AS1-AS3-AS4

A1 Table

Dest.	Path
A1 ... A5	AS2-AS1 ... AS2-AS1
B1 ... B4	AS2 ... AS2
C1 ... C3	AS2-AS3 ... AS2-AS3
D1 ... D4	AS2-AS3-AS4 ... AS2-AS3-AS4

B1 Table

Dest.	Path
A1 ... A5	AS3-AS1 ... AS3-AS1
B1 ... B4	AS3-AS2 ... AS3-AS2
C1 ... C3	AS3 ... AS3
D1 ... D4	AS3-AS4 ... AS3-AS4

C1 Table

Dest.	Path
A1 ... A5	AS4-AS3-AS1 ... AS4-AS3-AS1
B1 ... B4	AS4-AS3-AS2 ... AS4-AS3-AS2
C1 ... C3	AS4-AS3 ... AS4-AS3
D1 ... D4	AS4 ... AS4

D1 Table

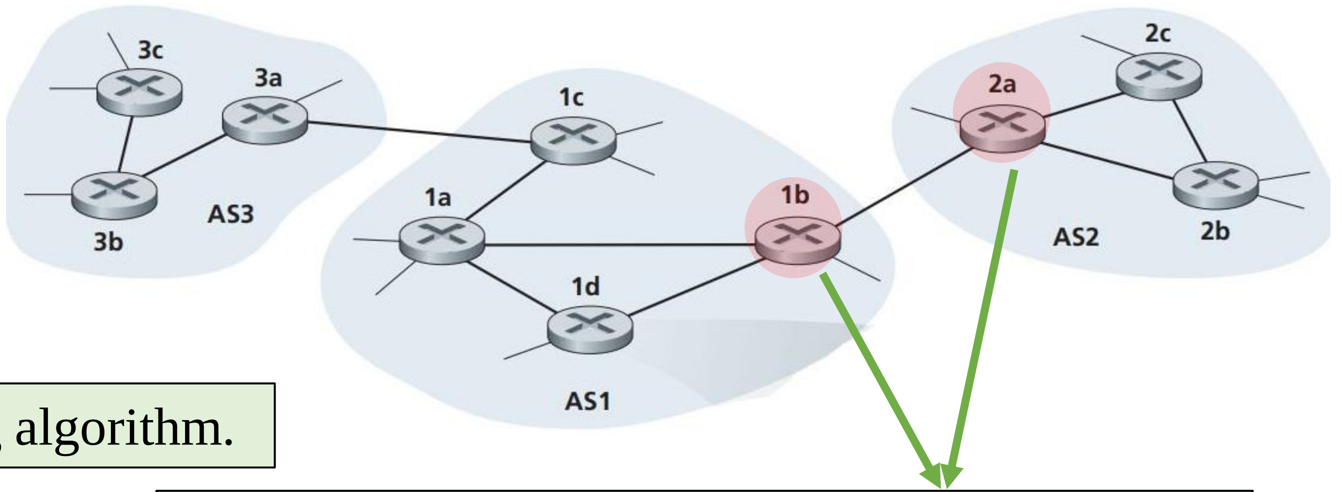
Updating (Speaker D1 of AS4)

- If node **Dl** in **AS4** receives a packet for node **A2**, it knows it should go through **AS4**, **AS3**, and **AS1**.

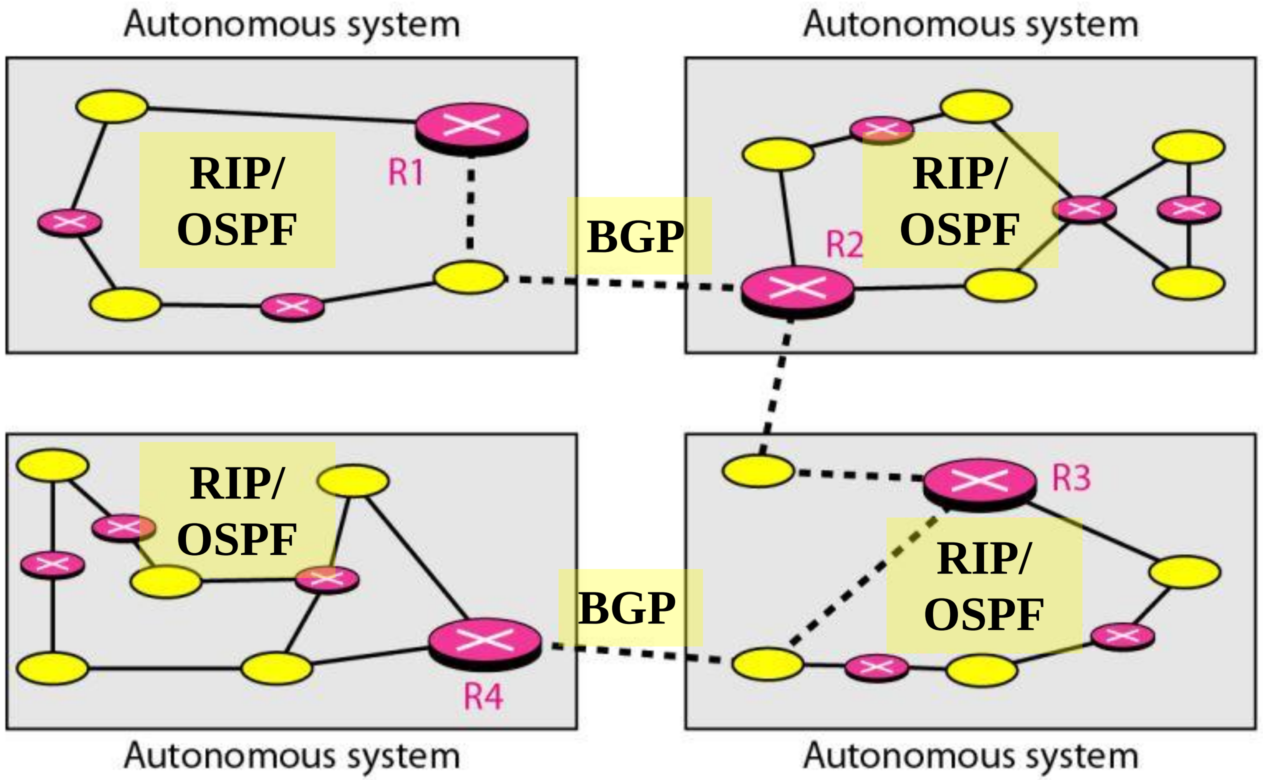
Q14. What is an autonomous system?

- An **autonomous system** (**AS**) is a group consisting of networks and routers, which is controlled by a single administrator.
- Thus, a network can be seen as a large collection of autonomous system.

- Routers within the same **AS** run the same routing algorithm.



- Routers connecting different AS are called as gateway routers.



- **Intradomain**: Routing algorithm running within an autonomous system is called an intra autonomous system routing protocol. Like, **RIP** and **OSPF**.

- **Interdomain**: Routing algorithm used by gateway routers are called as inter-autonomous system routing protocol. Like **BGP**

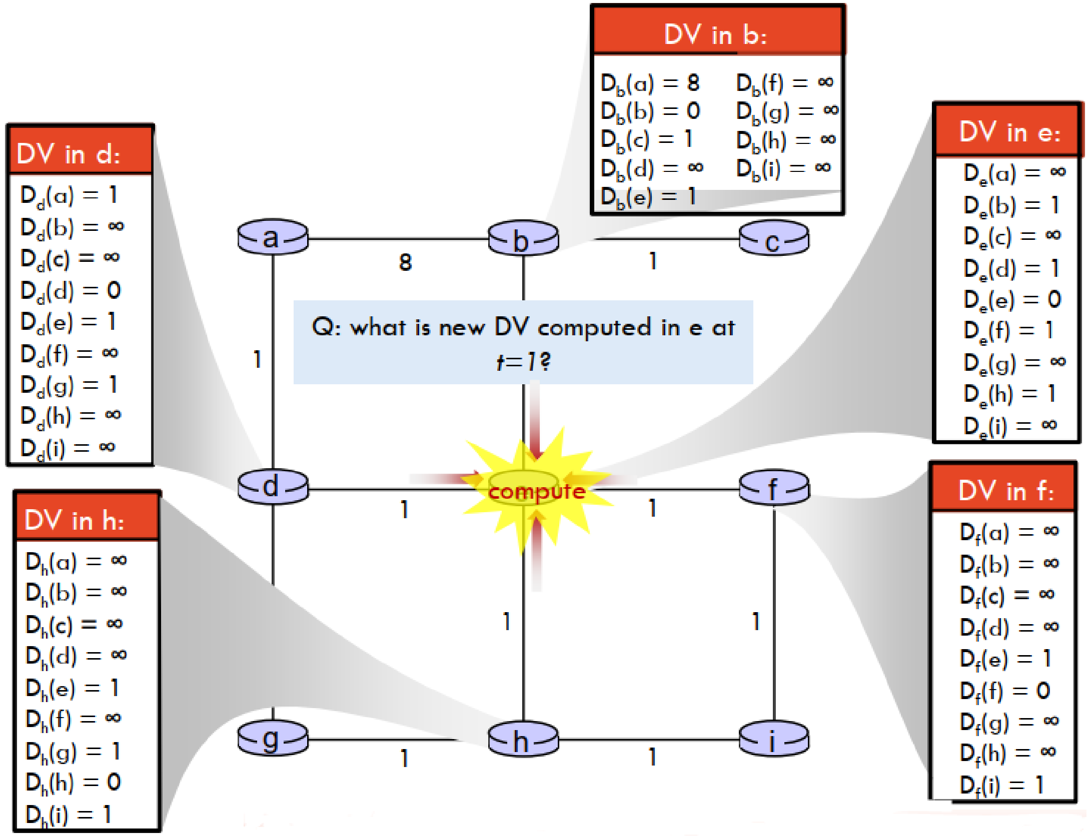
Q15. Compare and contrast distance vector routing method against link state routing method.

Distance vector routing	Link state routing
❑ In **distance vector routing**, each node shares its routing table with its immediate neighbors periodically and when there is a change.	❑ In **link state routing**, each node in the domain has the entire topology of the domain;
❑ The update messages have a very simple format and sent only to neighbors.	❑ The link-state messages in OSPF have a somewhat complex format
❑ They do not normally create heavy traffic	❑ For large area, messages may create heavy traffic.
❑ Slow Convergence.	❑ Convergence is fairly quick.
❑ Corruption or failure in one router affects other routers as seriously.	❑ Corruption or failure in one router does not affect other routers.
❑ Distance vector routing is subject to instability if there are more than a few hops in the domain of operation.	❑ Link state routing needs a huge number of resources to calculate routing tables.
❑ Example: RIP	❑ Example: OSPF

Q16. Workout with your tutor the answers for the following slides 28 and 45 from the lectures.

t=1

- e receives DVs from b, d, f, h



DV in e

$D_e(a) = \min\{9,2, \infty, \infty\} = 2$ via d

$D_e(b) = \min\{1, \infty, \infty, \infty\} = 1$ direct connection

$D_e(c) = \min\{2, \infty, \infty, \infty\} = 2$ via b

$D_e(d) = \min\{1, \infty, \infty\ \infty\} = 1$ direct connection

$D_e(e) = 0$

$D_e(f) = \min\{1, \infty, \infty, \infty\} = 1$ direct connection

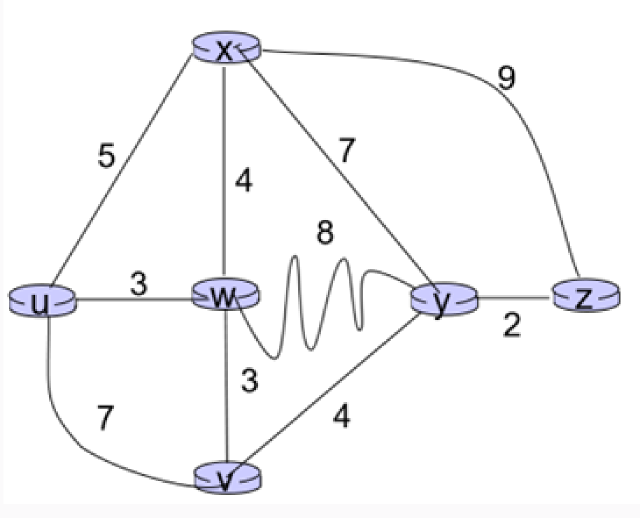
$D_e(g) = \min\{2, \infty, \infty, 2\} = 2$ tie and choose either d and h

$D_e(h) = \min\{1, \infty, \infty\ \infty\} = 1$ direct connection

$$D_x(y) \leftarrow min_v\{c_{x,v} + D_v(y)\}$$

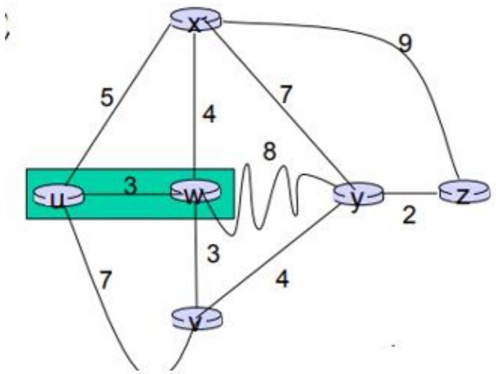
for each node $y \in N$, at node x, achieved via neighboring nodes v

Q16. Workout with your tutor the answers for the following slides 28 and 45 from the lectures.

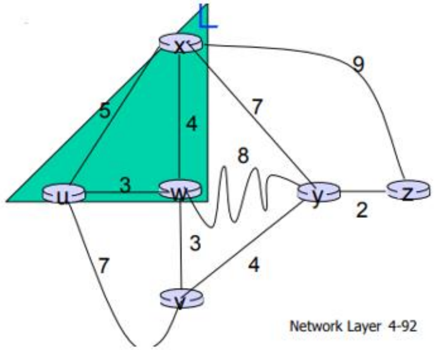


Step	N'	D(v) p(v)	D(w) p(w)	D(x) p(x)	D(y) p(y)	D(z) p(z)
0						
1						
2						
3						
4						
5						

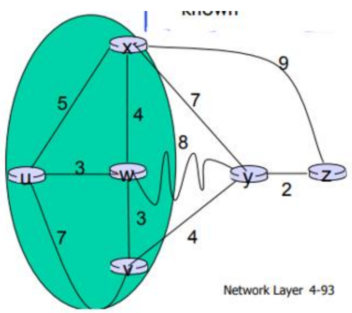
1



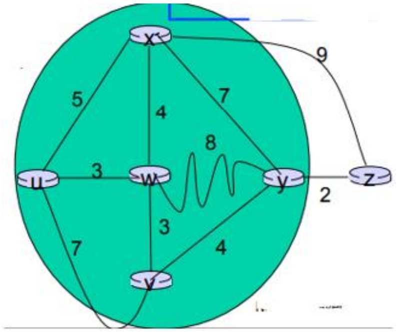
2



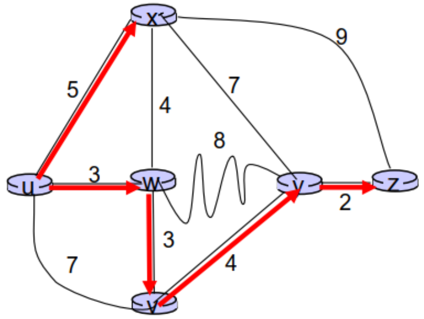
3



4



5



Q17. Workout with your tutor the answers for the Lecture 5, slides 30 and 31.

- A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.36/29. What is the first, the last, and the total number of addresses of this block? 29 bits for network address
- IP Address : 11001101.00100000.00100101.00100100 (205.16.37.36)

  Mask : 11111111.11111111.11111111.11111000 (255.255.255.248)

  Subnet Address : 11001101.00100000.00100101.00100000 (205.16.37.32)

SubNet. Add	11001101 =205	00001000 =16	00100101=37	00100000 = 32
1st Address	11001101 =205	00001000 =16	00100101=37	00100001 = 33
2nd Address	11001101 =205	00001000 =16	00100101=37	00100010 = 34
3rd Address	11001101 =205	00001000 =16	00100101=37	00100011 = 35
4th Address	11001101 =205	00001000 =16	00100101=37	00100100 = 36
5th Address	11001101 =205	00001000 =16	00100101=37	00100101 = 37
6th Address	11001101 =205	00001000 =16	00100101=37	00100110 = 38
Broadcast Add	11001101 =205	00001000 =16	00100101=37	00100111 = 39

Q17. Workout with your tutor the answers for the Lecture 5, slides 30 and 31.

- A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.36/30. What is the first, the last, and the total number of useable addresses of this block?

205.16.37.36/30 implies mask of 255.255.255.252 with two last bits that can be used

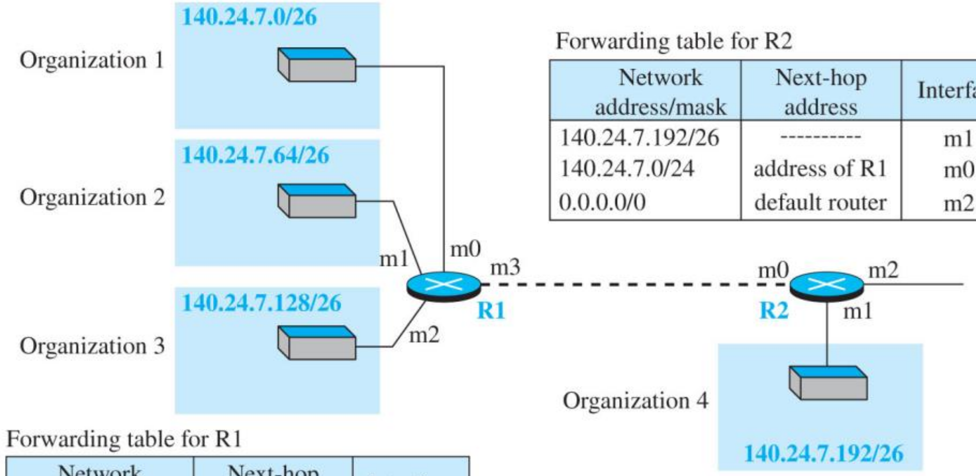
Start from 36=00100100; network address 205.16.37.36; 1st address 205.16.37.37; 2nd (last) address 205.16.37.38; 205.16.37.39 is broadcast address; in total this block has 2^2-2=2 useable addresses

Q17. Workout with your tutor the answers for the Lecture 5, slides 30 and 31.

- A block of addresses is granted to a small organization. We know that one of the addresses is 192.168.10.64/28.
- What is the first, the last, and the number of useable addresses of this block?

192.168.10.64/255.255.255.240; last 6 bits that can be allocated, 64=01000000;
network address 192.168.10.64; 1st address 192.168.10.65; 14th (last) address 192.168.10.78;
192.168.10.79 is broadcast address; in total this block has 2^4-2=14 useable addresses

Q18. Can Router R1 in the figure below receive a packet with destination address 140.24.7.194. How is the packet routed to its final destination?



Forwarding table for R2

Network address/mask	Next-hop address	Interface
140.24.7.192/26	----------	m1
140.24.7.0/24	address of R1	m0
0.0.0.0/0	default router	m2

Forwarding table for R1

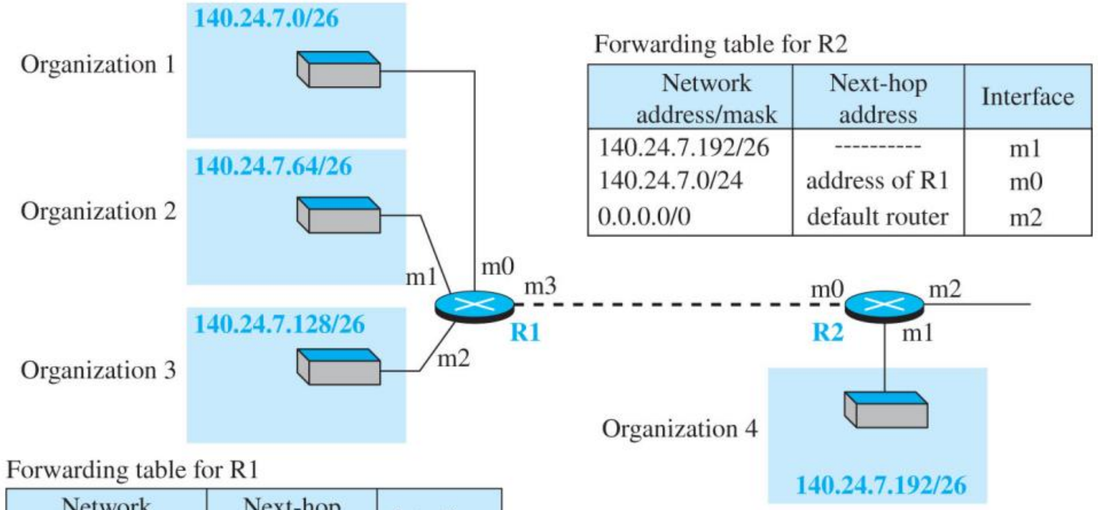
Network address/mask	Next-hop address	Interface
140.24.7.0/26	----------	m0
140.24.7.64/26	----------	m1
140.24.7.128/26	----------	m2
0.0.0.0/0	default router	m3

- Router R1 has four interfaces. Let us investigate the possibility of a packet with destination 140.24.7.194 from each of these interfaces and see how it is routed.

- The packet can arrive from one of the interfaces m0, m1, and m2, because one of the computers in organization 1, 2, or 3 could have sent this packet. The prefix /26 is applied to the address, resulting in the network address 140.24.7.192/26.
- Since none of the network addresses/masks matches this result, the packet is sent to the default router R2

- The packet cannot arrive at router R1 from interface m3 because this means that the packet must have arrived from interface m0 of router R2, which is impossible because if this packet arrives at router R2 (from any interface), the prefix length /26 is applied to the destination address, resulting in the network address/mask of 140.24.7.192/26. The packet is sent out from interface m1 and directed to organization 4 and never reaches router R1

Q19. Assume Router R2 in the figure below receive a packet with destination address 140.24.7.42. How is the packet routed to its final destination?



Forwarding table for R2

Network address/mask	Next-hop address	Interface
140.24.7.192/26	----------	m1
140.24.7.0/24	address of R1	m0
0.0.0.0/0	default router	m2

Forwarding table for R1

Network address/mask	Next-hop address	Interface
140.24.7.0/26	----------	m0
140.24.7.64/26	----------	m1
140.24.7.128/26	----------	m2
0.0.0.0/0	default router	m3

- The packet is sent to router R1 and eventually to organization 1 as shown below:

- Router R2 applies the mask /26 to the address (or it extracts the leftmost 26 bits) resulting in the network address/mask of 140.24.7.0/26, which does not match with the first entry in the forwarding table.

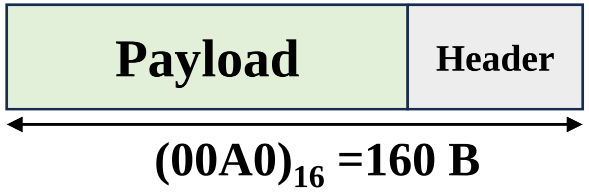
- Router R2 applies the mask /24 to the address (or it extracts the leftmost 24 bits) resulting in the network address/mask of 140.24.7.0/24, which matches with the second entry in the forwarding table. The packet is sent out from interface m0 to router R1.

- Router R1 applies the mask /26 to the address (or it extracts the leftmost 26 bits) resulting in the network address/mask of 140.24.7.0/26, which matches with the first entry in the forwarding table. The packet is sent out from interface m0 to organization 1

Q20. In IPv4 datagram, the value of total-length field is $(00A0)_{16}$ and the value of the header length (HLEN) is $(5)_{16}$. How many bytes of payload are being carried by the datagram? What is this datagram's efficiency (ratio of the payload length to the total length)?

Total Length Field: This field specifies the total length of the IPv4 datagram, including both the header and the payload.

total length of the datagram is: $\mathbf{(00A0)_{16} = (160)_{10}}$

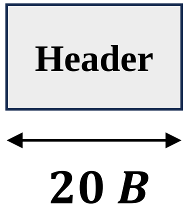


Header Length (HLEN) Field: This field specifies the length of the IPv4 header in 32-bit words.

$$(5)_{16} = (5)_{10}$$

Header length is **5 × 32-bit words.**

$$\boldsymbol{5\ words \times 4\ bytes/word = 20\ bytes}$$

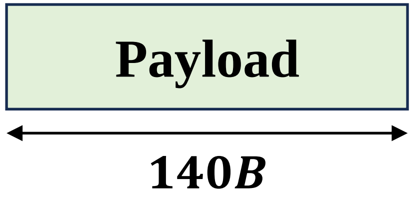


Payload Length:

$$\boldsymbol{Payload\ Length = Total\ Length - Header\ Length}$$

Payload Length:

$$\boldsymbol{Payload\ Length = 160B - 20B = 140B}$$



Q20. In IPv4 datagram, the value of total-length field is $(00A0)_{16}$ and the value of the header length (HLEN) is $(5)_{16}$. How many bytes of payload are being carried by the datagram? What is this datagram's efficiency (ratio of the payload length to the total length)?

Efficiency Calculation: Efficiency is defined as the ratio of the payload length to the total length of the datagram. It can be expressed as a percentage:

$$\eta = \frac{\text{Payload Length}}{\text{Total Length}} \%$$

$$\eta = \frac{140}{160} \times 100\ \% = 87.5\%$$

Q21. A packet has arrived in which the offset value is 100, the value of HLEN is 5, and the total length value is 100. What are the numbers of the first and last bytes?

- The first byte number is **100 × 8 = 800**.
- The total length is **100 bytes** and the header length is **20 bytes** (5 × 4).
  - which means that there are **80 bytes** in this datagram.
- If the first byte number is 800,
- the last byte number must 879.

- Offset = 100
- HLEN = 5
- (Header length is 5 * 4 = 20 bytes, because HLEN is in 32-bit words, and 1 word = 4 bytes)
- First byte = Offset × 8
- Last byte = First byte + Total data length − 1