Computer Network And Network Design(CNND)
ITC402

Subject Incharge

Ms. Jesleena Gonsalves

Assistant Professor

Room No. 326

email: jesleenagonsalves@sfit.ac.in

Whatsapp Group Invite Link -

Module 3

Network Layer

Outline

- Network Layer Services
- Packet Switching
- Network Layer Performance
- IPv4 Addressing (classful and classless)
- Subnetting
- Supernetting
- IPv4 Protocol
- DHCP
- Network Address Translation (NAT).
- **Routing algorithms**: Distance Vector Routing, Link state routing , Path Vector Routing.
- **Protocols** –RIP,OSPF,BGP.
- **Next Generation IP:** IPv6 Addressing,IPv6 Protocol, Transition fromIPV4 to IPV6

NETWORK LAYER SERVICES

1. Packetizing
2. Routing
3. Forwarding
4. Error Control
5. Congestion Control
6. Security

PACKET SWITCHING

- Packet switching is used at network layer because the unit of data at this layer is a packet.
- Packet switched network use two different approaches to route the packets: The datagram approach and the virtual circuit approach.

PACKET SWITCHING

DATAGRAM APPROACH: CONNECTIONLESS SERVICE

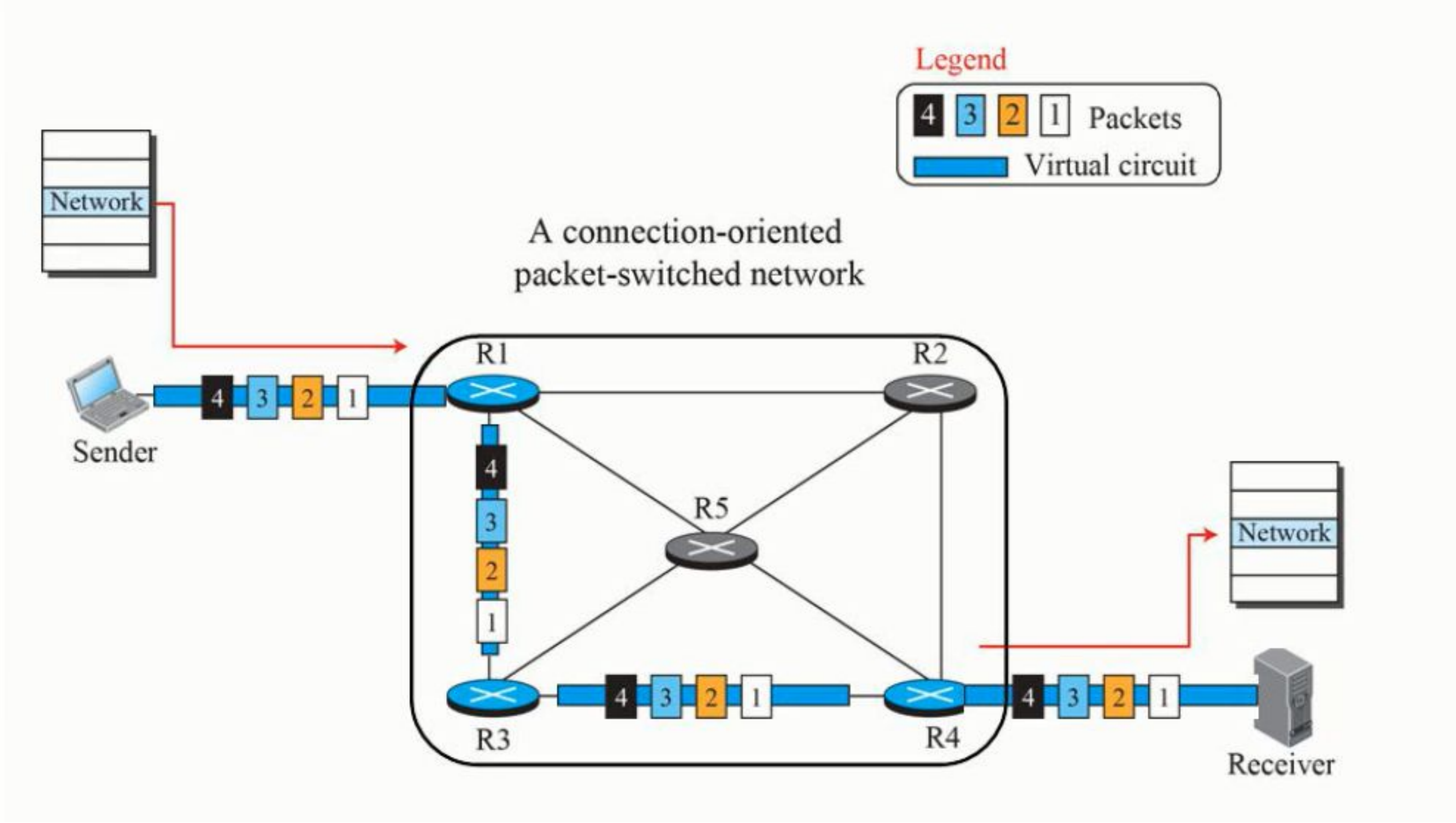
- Initially network layer was responsible only for delivery of packets from the source to the destination.
- Each packet travelling in the Internet is an independent entity: there is no relationship between packets belonging to the same message.
- Each packet is routed based on the information contained in its header.

PACKET SWITCHING

VIRTAUL CIRCUIT APPROACH: CONNECTION ORIENTED SERVICE

- In a connection oriented service there is a relationship between all the packets belonging to a message.
- Before all the datagrams in a message can be sent , a virtual connection should be set up to define the path for the datagrams.
- In this type of service the packet must contain not only the source and the destination addresses, but also a flow label, a virtual circuit identifier that defines the virtual path, the packet should follow.
- To create a connection oriented service, a three phase process is used: setup, data transfer and teardown.

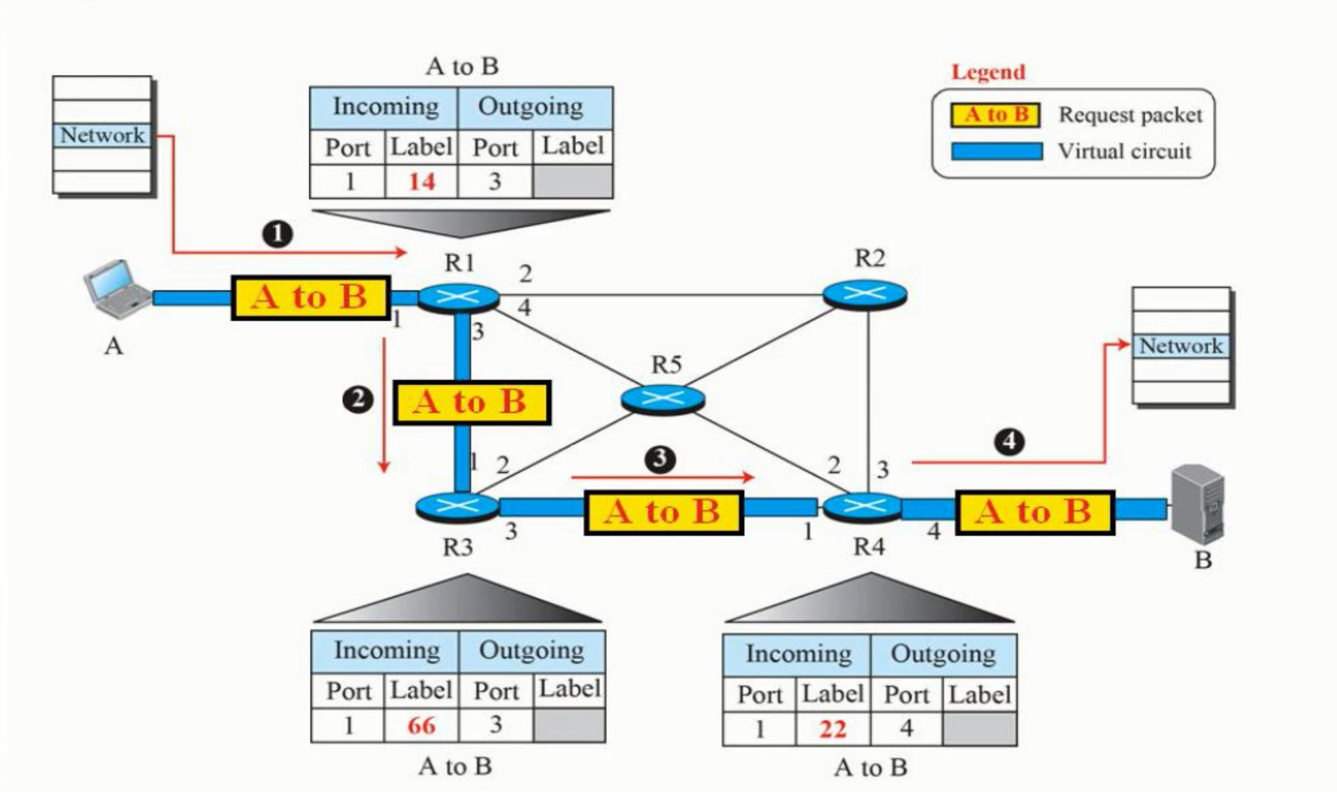
PACKET SWITCHING



PACKET SWITCHING

Setup Phase: In setup phase router creates an entry for a virtual circuit. If source A wants to create a virtual circuit to destination B, two auxiliary packets need to be exchanged between the sender and receiver: the Request packet and the Acknowledgement packet.

Figure 18.7: Sending request packet in a virtual-circuit network



A to B (R1)

Incoming		Outgoing	
Port	Label	Port	Label
1	14	3	

A to B (R3)

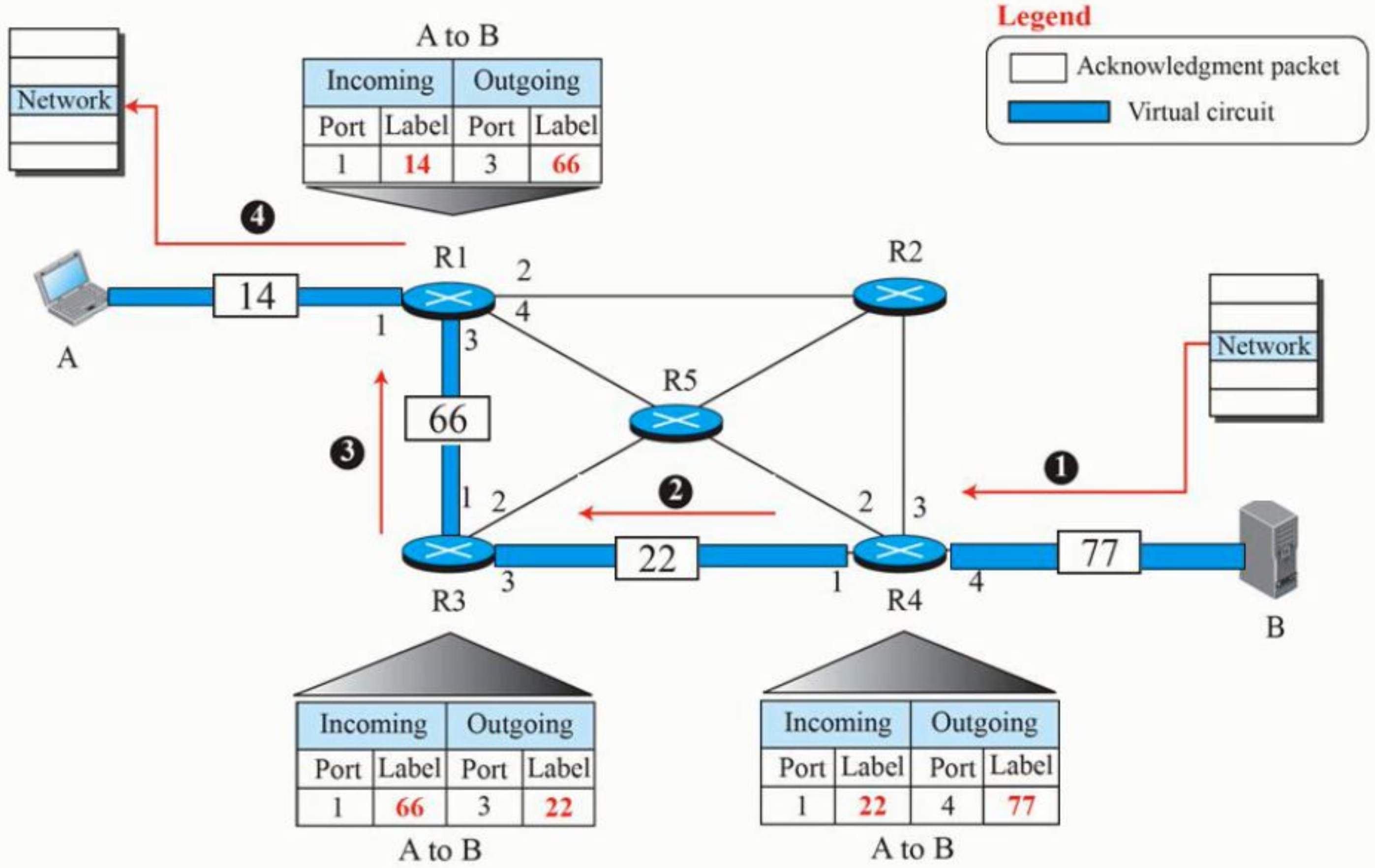
Incoming		Outgoing	
Port	Label	Port	Label
1	66	3	

A to B (R4)

Incoming		Outgoing	
Port	Label	Port	Label
1	22	4	

PACKET SWITCHING

Figure 18.8: Sending acknowledgments in a virtual-circuit network



A to B (R1)

Incoming		Outgoing	
Port	Label	Port	Label
1	14	3	66

A to B (R3)

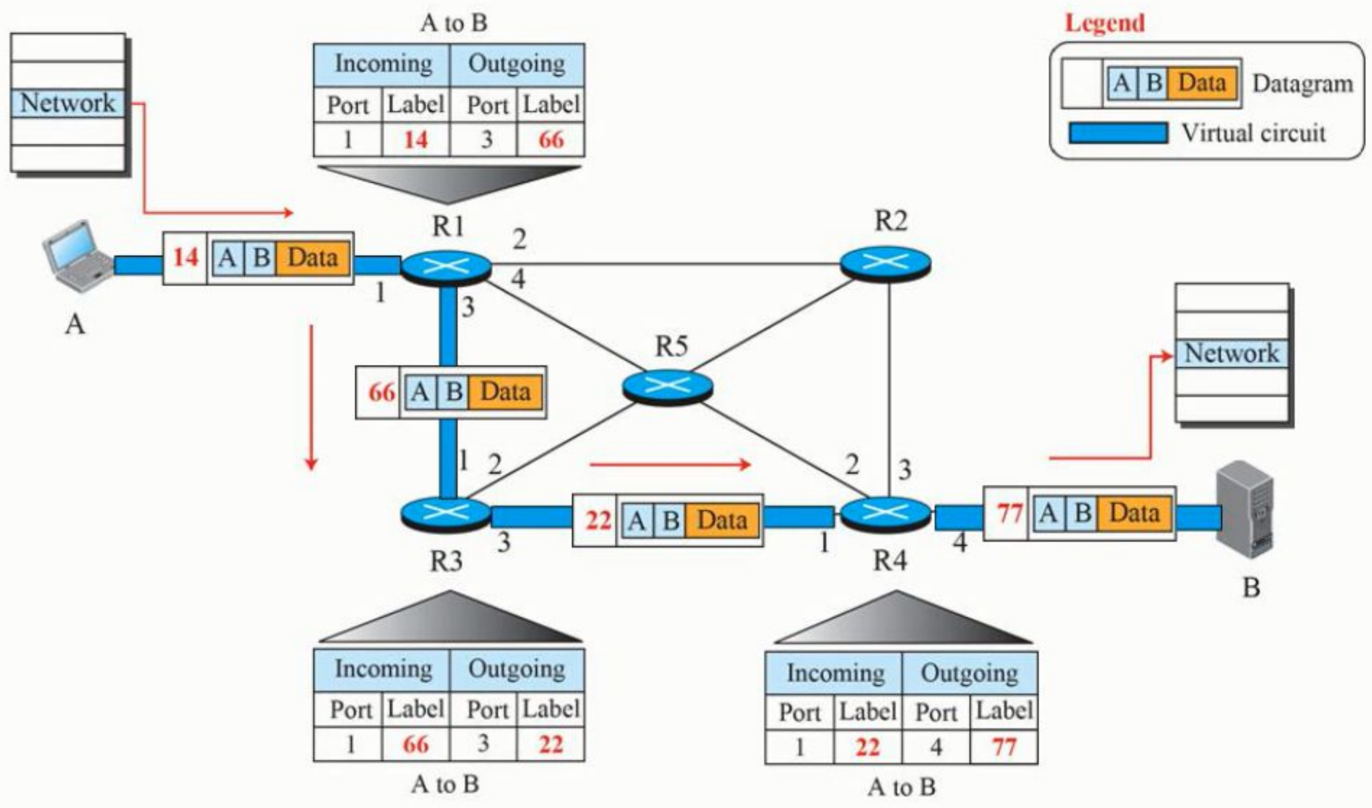
Incoming		Outgoing	
Port	Label	Port	Label
1	66	3	22

A to B (R4)

Incoming		Outgoing	
Port	Label	Port	Label
1	22	4	77

PACKET SWITCHING

Figure 18.9: Flow of one packet in an established virtual circuit



A to B

Incoming		Outgoing	
Port	Label	Port	Label
1	14	3	66

Incoming		Outgoing	
Port	Label	Port	Label
1	66	3	22

A to B

Incoming		Outgoing	
Port	Label	Port	Label
1	22	4	77

A to B

PACKET SWITCHING

Teardown Phase: In this phase , source A after sending all packets to B , sends a special packet called a teardown packet. Destination B responds with a confirmation packet. All routers delete the corresponding entries from their tables.

NETWORK LAYER PERFORMANCE

Delay: Sometimes a packet from its source to destination encounters delays. The delay in a network can be divided into 4 types: Transmission delay, Propagation delay, Processing delay, Queuing delay.

Transmission delay:

A sender needs to put the bits in a packet on the line one by one. If the first bit of the packet is put on the line at time t1 and the last bit is put on the line at time t2, transmission delay of the packet is (t2-t1)

$$\text{Delay}_{tr} = (\text{Packet length})/(\text{Transmission rate})$$

Propagation delay:

Propagation delay is the time it takes for a bit to travel from point A to point B in the transmission media.

$$\text{Delay}_{pg} = (\text{Distance})/(\text{Propagation speed})$$

Processing delay:

Processing delay is the time required for a router or a destination host to receive a packet from the input port, remove the header, perform an error detection procedure and deliver the packet to the output port.

$$\text{Delay}_{pr} = \text{Time required to process a packet in a router or a destination host}$$

NETWORK LAYER PERFORMANCE

Queuing delay:

The queuing delay for a packet in a router is measured as the time a packet waits in the input queue and the output queue of a router.

Delay_{qu} = Time a packet waits in the input queue and the output queue of a router.

Total delay:

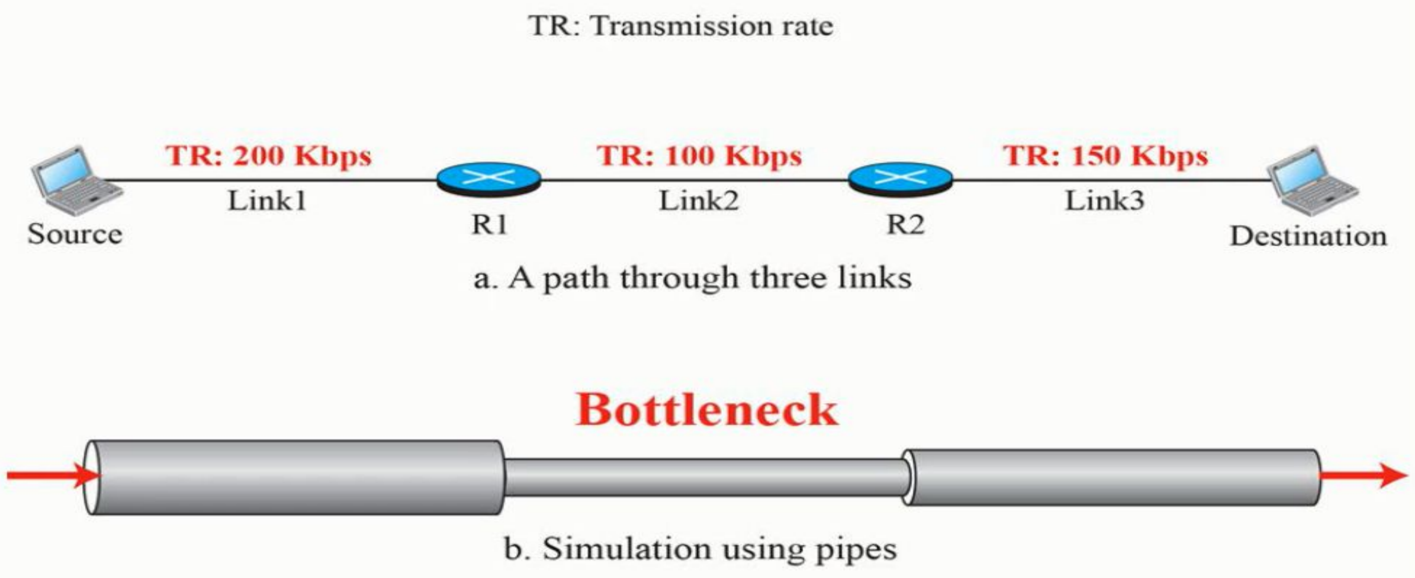
Assuming equal delays for the sender, routers and receivers, the total delay a packet encounters can be calculated if the number of routers(n) in the whole path are known.

$$\text{Total delay} = (n+1)\ (\text{Delay}_{tr} + \text{Delay}_{pg} + \text{Delay}_{pr}) + (n)\ (\text{Delay}_{qu})$$

NETWORK LAYER PERFORMANCE

Throughput: Throughput is defined as the number of bits passing through the point in a second, which is actually the transmission rate of data at that point.

Figure 18.10: Throughput in a path with three links in a series



a. A path through three links

b. Simulation using pipes

$$\text{Throughput} = \text{minimum}\ (TR_1 , TR_2 ,\ldots\ldots .\ TR_n ,)$$

NETWORK LAYER PERFORMANCE

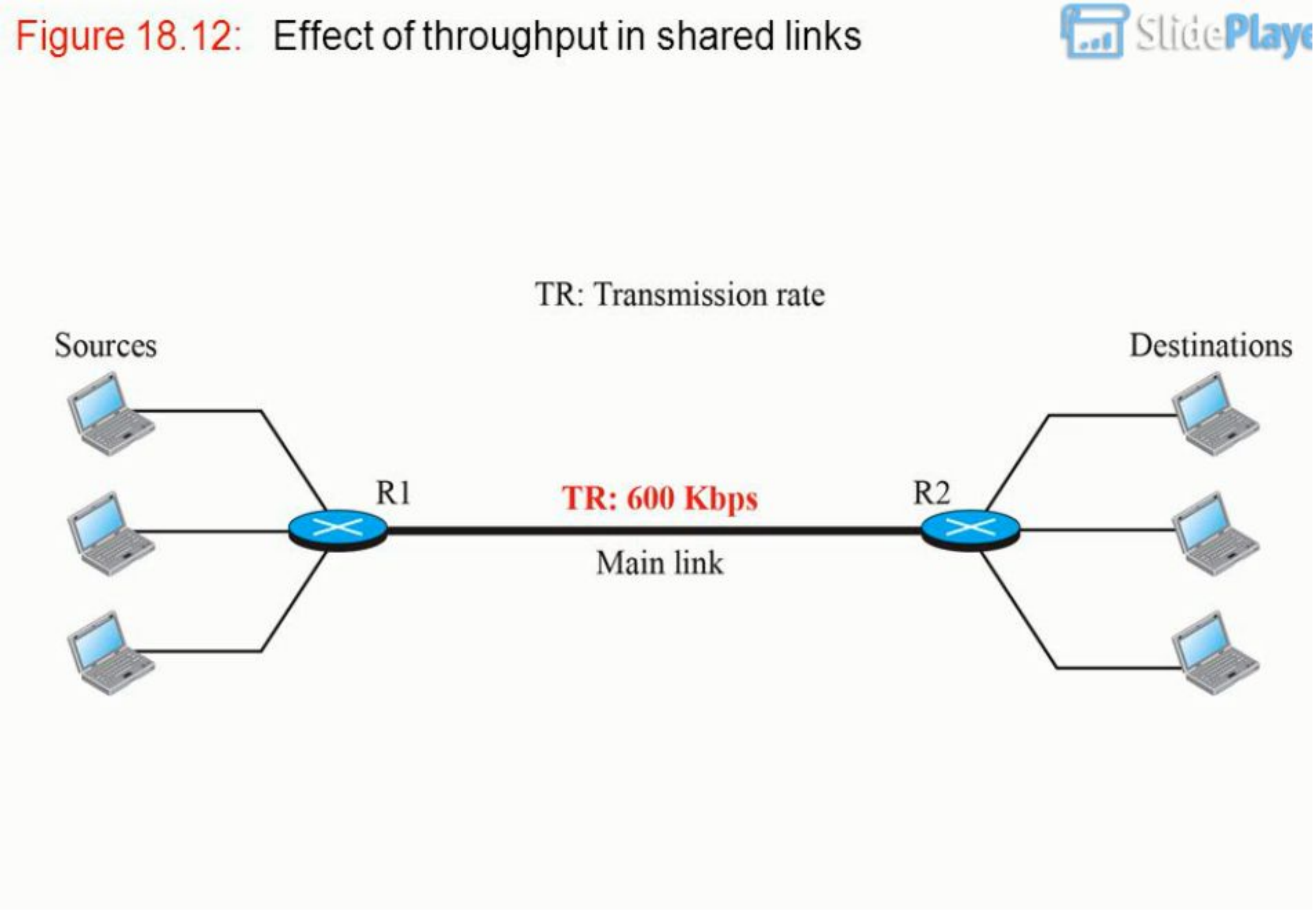


Figure 18.12: Effect of throughput in shared links

NETWORK LAYER PERFORMANCE

Packet Loss:

- When a router receives a packet while processing another packet, the received packet needs to be stored in the input buffer waiting for its turn.
- A router has an input buffer with a limited size.
- At times the buffer may become full and the next packet has to be dropped.

IPV4 ADDRESSING

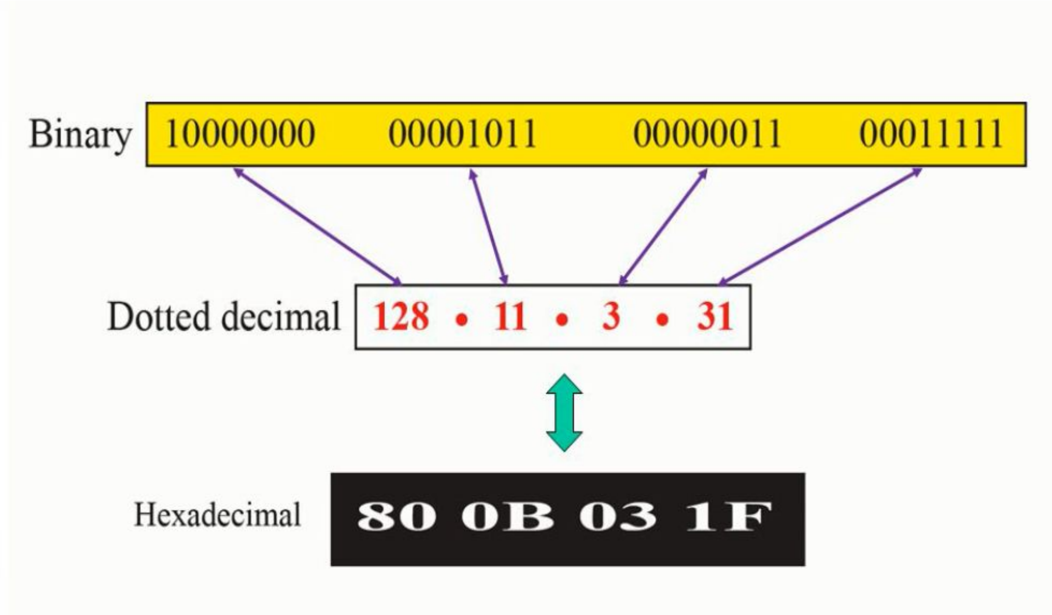
- The identifier used in the IP layer of the TCP/IP protocol suite to identify the connection of each device to the Internet is called the Internet address or IP address.
- An IPv4 address is a 32- bit address that uniquely and universally defines the connection of a host or a router to the Internet.

IPV4 ADDRESSING

ADDRESS SPACE:

- An address space is the total number of addresses used by the protocol.
- If a protocol uses b bits to define an address , the address space is 2^b.

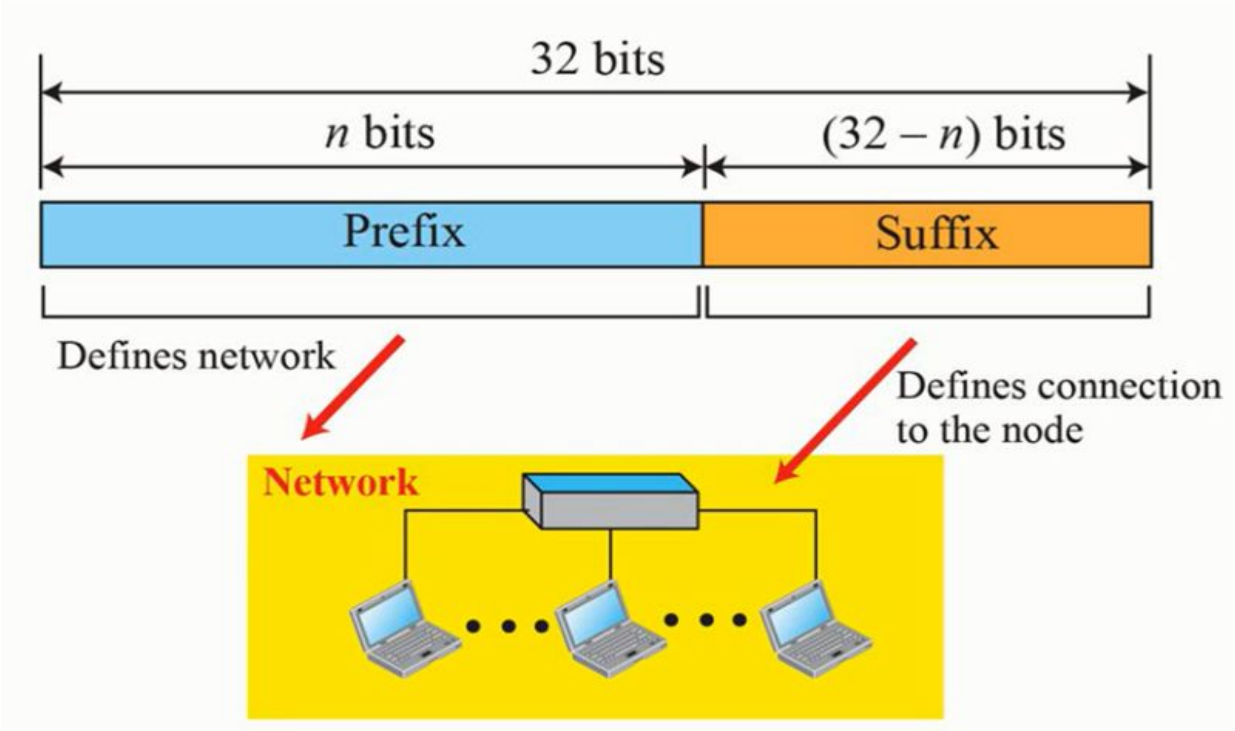
Notation: There are three common notations to show an IPv4 address: Binary notation(base 2), Dotted decimal notation (base 256), and hexadecimal notation (base 16)



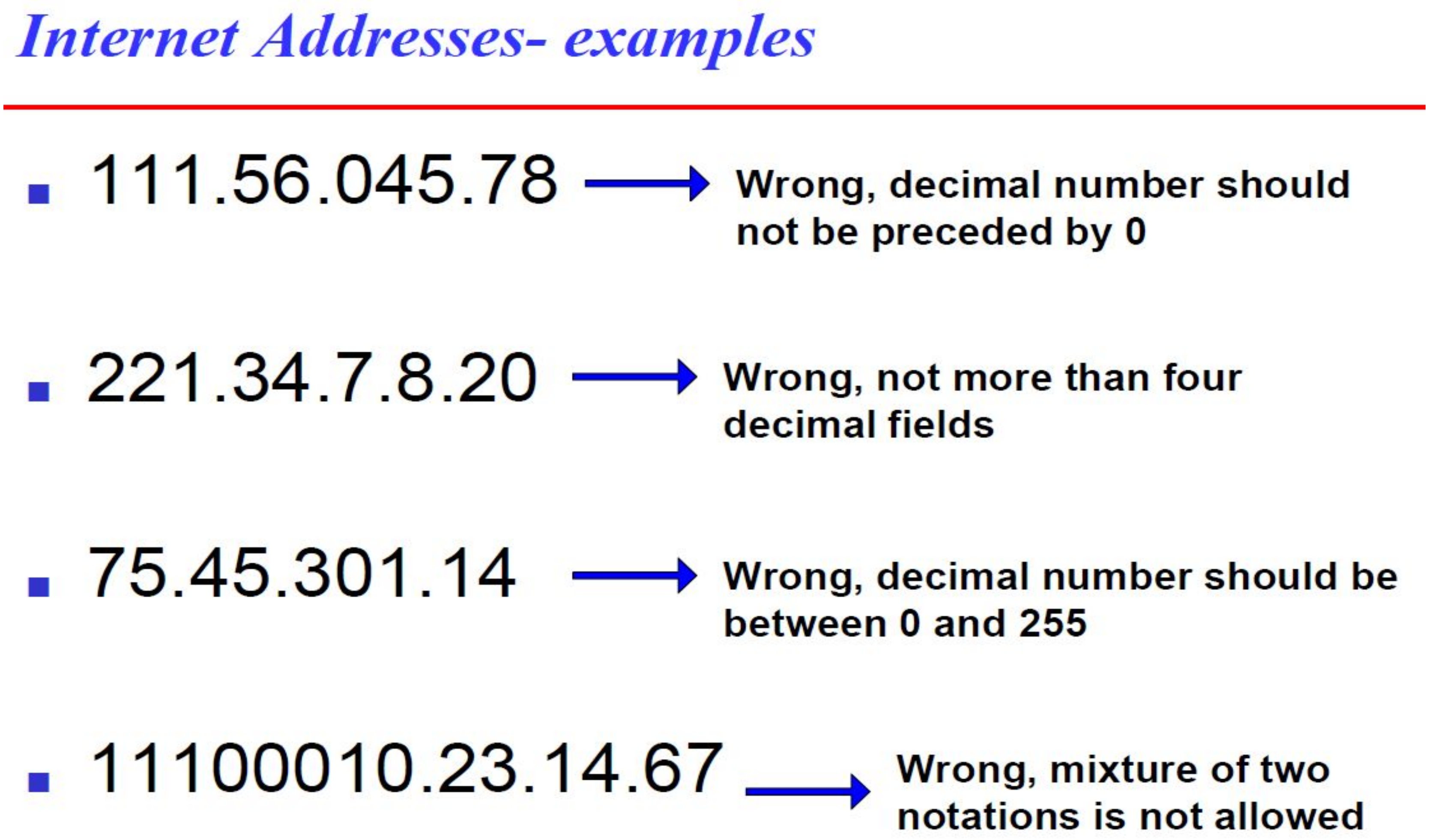
IPV4 ADDRESSING

HIERARCHY IN ADDRESSING

- A 32-bit IPv4 address is hierarchical and divided into two parts.
- The first part of the address , called the prefix , defines the network ; the second part of the address, called the suffix, defines the node.



IPV4 ADDRESSING

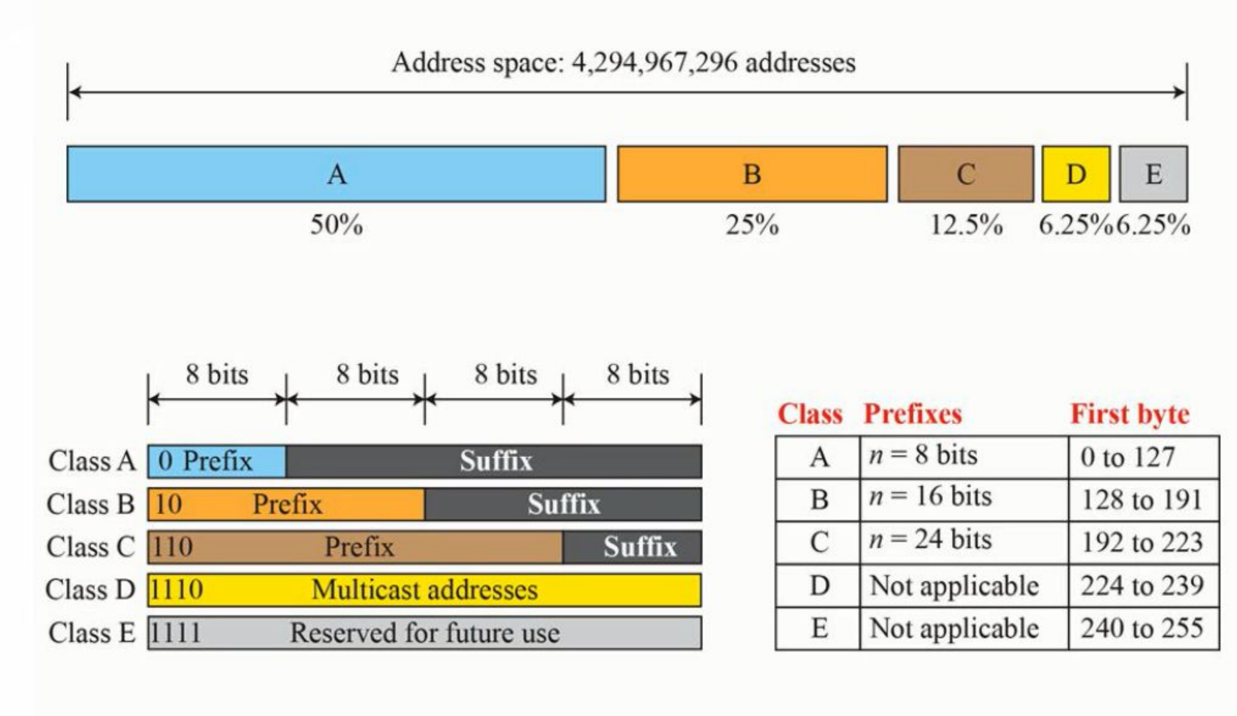


Internet Addresses- examples

- 111.56.045.78 → Wrong, decimal number should not be preceded by 0
- 221.34.7.8.20 → Wrong, not more than four decimal fields
- 75.45.301.14 → Wrong, decimal number should be between 0 and 255
- 11100010.23.14.67 → Wrong, mixture of two notations is not allowed

IPV4 ADDRESSING:CLASSFUL ADDRESSING

- An IPv4 address is designed with a fixed length prefix, but to accommodate both small and large networks, three fixed length prefixes were designed instead of one(n=8,n=16,n=24)
- The whole address space is divided into five classes (class A,B,C,D and E).



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

IPV4 ADDRESSING:CLASSFUL ADDRESSING

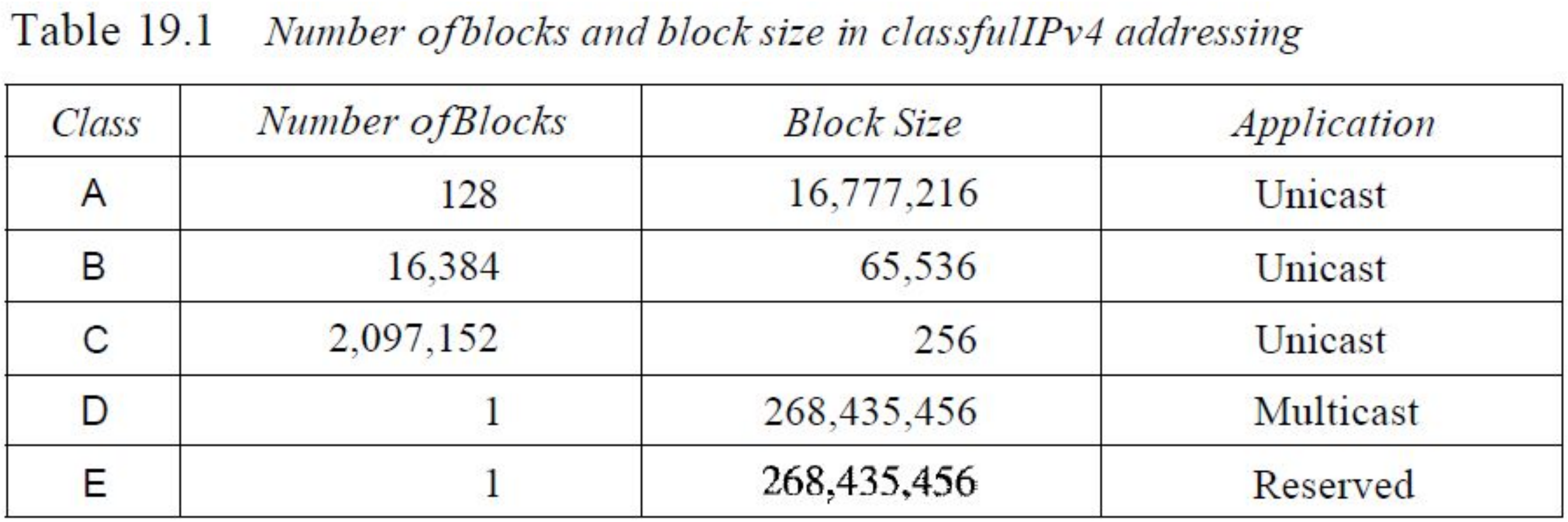


Table 19.1 *Number ofblocks and block size in classfulIPv4 addressing*

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

IPV4 ADDRESSING:CLASSFUL ADDRESSING

Exercise

Find the class of each address

1. 4.23.145.90
2. 227.34.78.7
3. 246.7.3.8
4. 129.6.8.4
5. 198.76.9.23

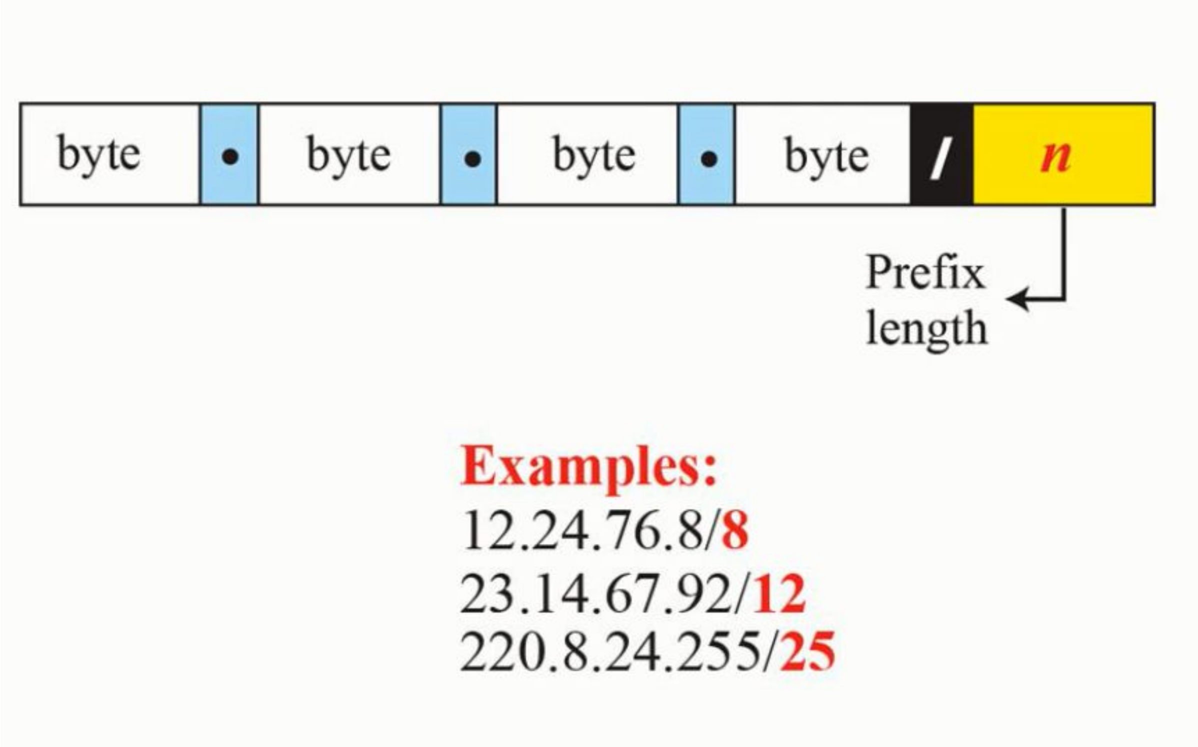
IPV4 ADDRESSING: CLASSLESS ADDRESSING

- In classless addressing, the whole address space is divided into variable length blocks.
- The prefix in an address defines the block(network) ; the suffix defines the node (device).
- The number of addresses in a block must be a power of 2.
- The prefix length in classless addressing is variable and can range from 0 to 32.
- The size of the network is inversely proportional to the length of the prefix.

IPV4 ADDRESSING: CLASSLESS ADDRESSING

PREFIX LENGTH

- The prefix length , n , is added to the address, separated by a slash.
- The notation is informally referred to as Slash notation and formally as Classless Interdomain Routing (CIDR).

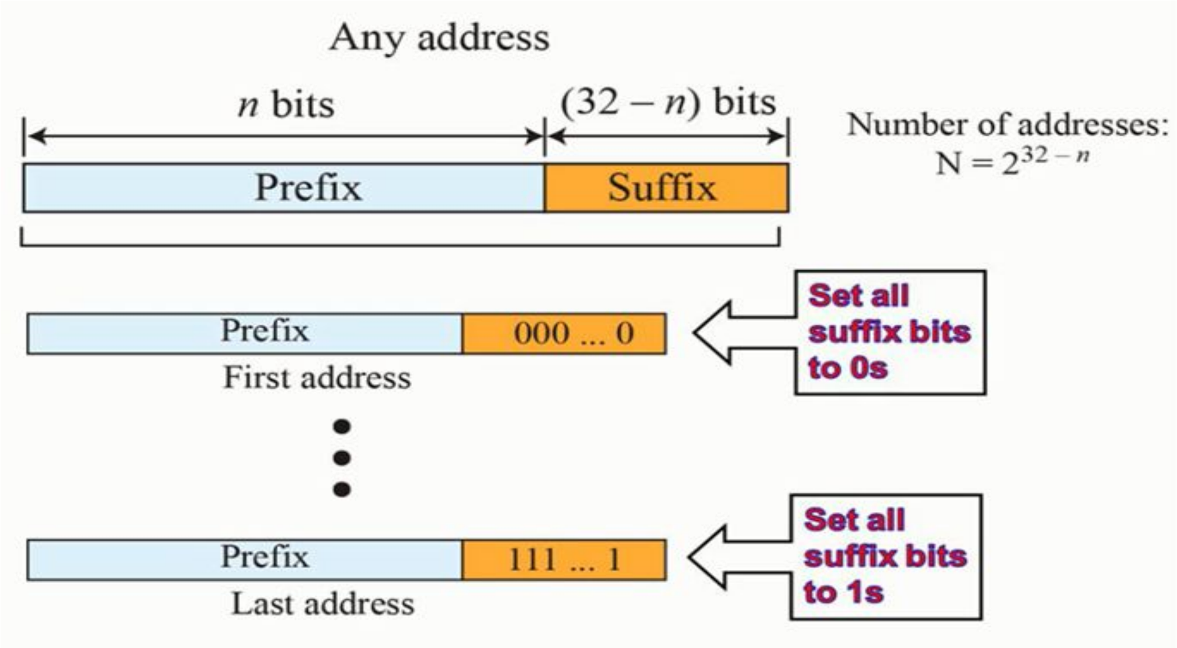


Examples:
12.24.76.8/**8**
23.14.67.92/**12**
220.8.24.255/**25**

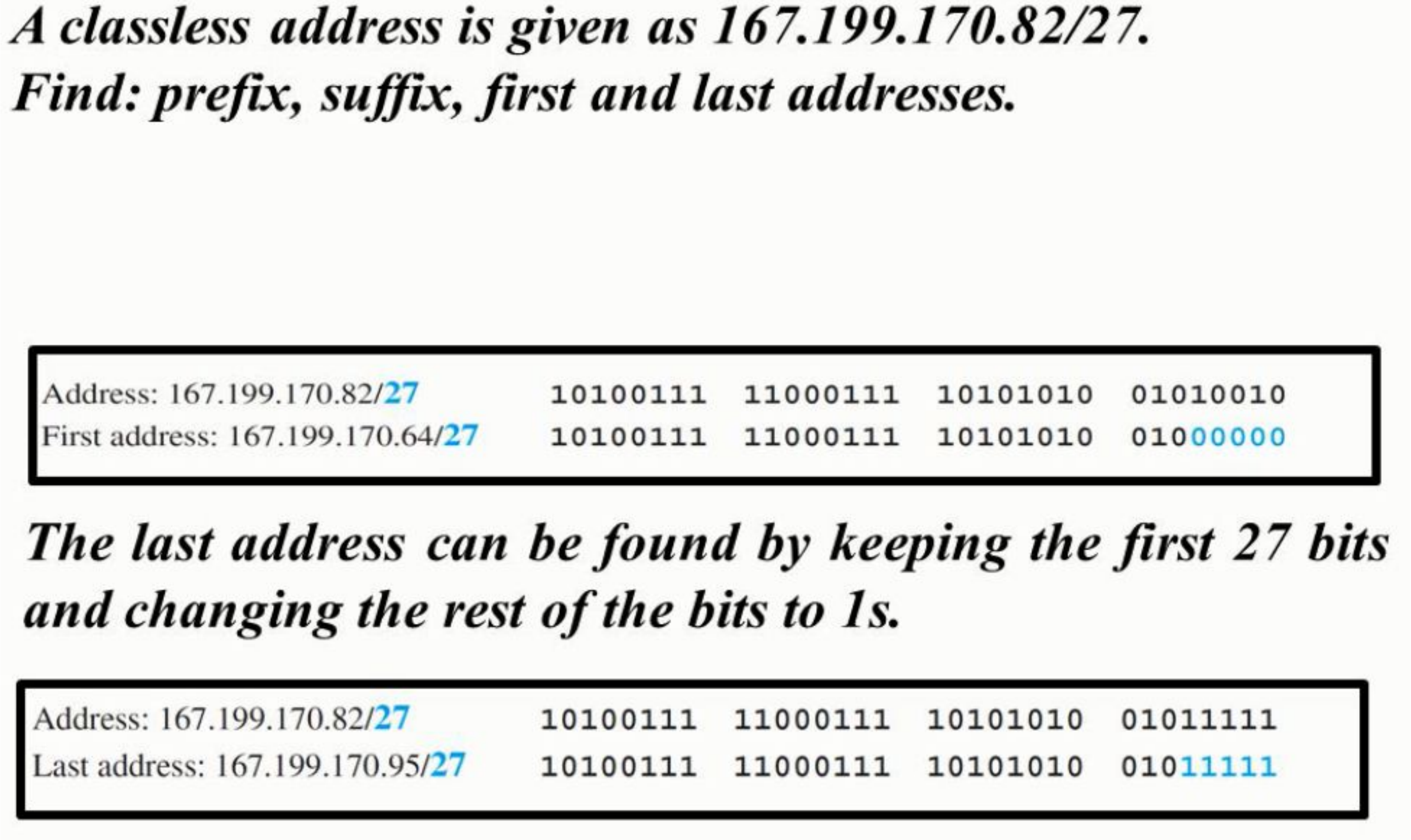
IPV4 ADDRESSING: CLASSLESS ADDRESSING

INFORMATION EXTRACTION IN CLASSSLESS ADDRESSING

1. The number of addresses in the block is found as N= 2^{32-n}.
2. To find the first address, keep the leftmost bits and set the (32-n) rightmost bits all to 0s
3. To find the last address, keep the leftmost bits and set the (32-n) rightmost bits all to 1s



IPV4 ADDRESSING: CLASSLESS ADDRESSING



A classless address is given as 167.199.170.82/27.
Find: prefix, suffix, first and last addresses.

Address: 167.199.170.82/27	10100111	11000111	10101010	01010010
First address: 167.199.170.64/27	10100111	11000111	10101010	01000000

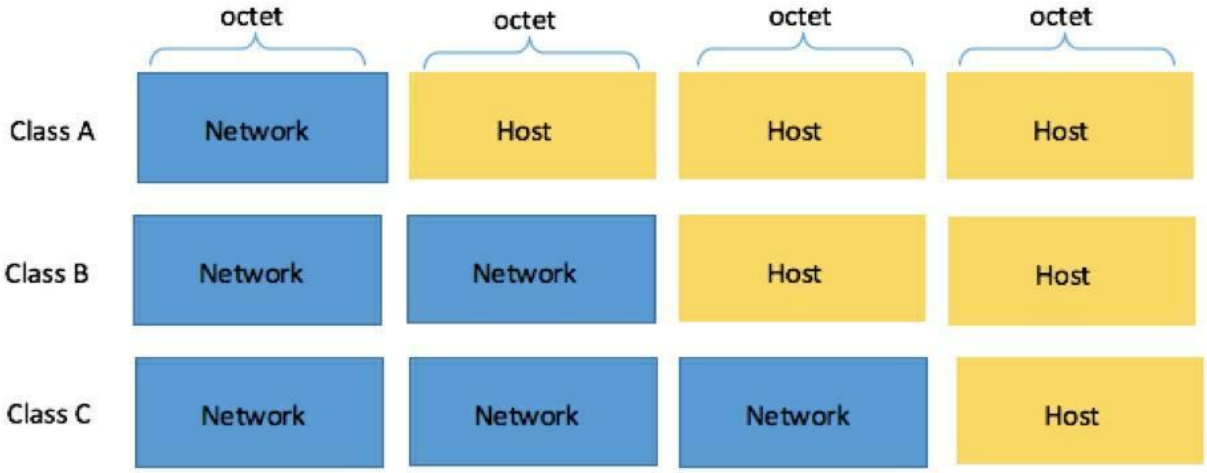
The last address can be found by keeping the first 27 bits and changing the rest of the bits to 1s.

Address: 167.199.170.82/27	10100111	11000111	10101010	01011111
Last address: 167.199.170.95/27	10100111	11000111	10101010	01011111

SUBNETTING

- Each IP address consists of a subnet mask. All the class types, such as Class A, Class B and Class C include the subnet mask known as the default subnet mask.
- The default subnet mask is as follows:

Class A: 255.0.0.0
Class B: 255.255.0.0
Class C: 255.255.255.0



	octet	octet	octet	octet
Class A	Network	Host	Host	Host
Class B	Network	Network	Host	Host
Class C	Network	Network	Network	Host

SUBNETTING

- Subnetting is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets).
- Subnetting take places when we extend the default subnet mask.

Example:

Address given: 188.25.45.48/20

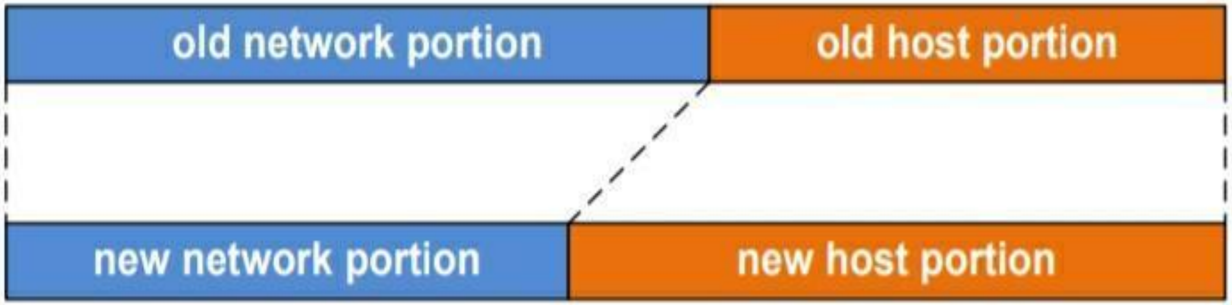
This address belong to class B and class B has default subnet mask 255.255.0.0[/16 in CIDR].

Subnet mask in binary would be 11111111. 11111111.11110000.00000000.

Subnet mask is 255.255.240.0

SUPERNETTING

- Supernetting is the opposite of Subnetting.
- In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.
- Supernetting is used in route aggregation to reduce the size of routing tables.
- Consider two networks **200.20.0.x/24** and **200.20.1.x/24.** Both these networks have the same 23 bits network prefix and differ only in their 24th bit. Hence these two networks could be combined and summarized as a Super network with the address **200.20.0.x/23**.

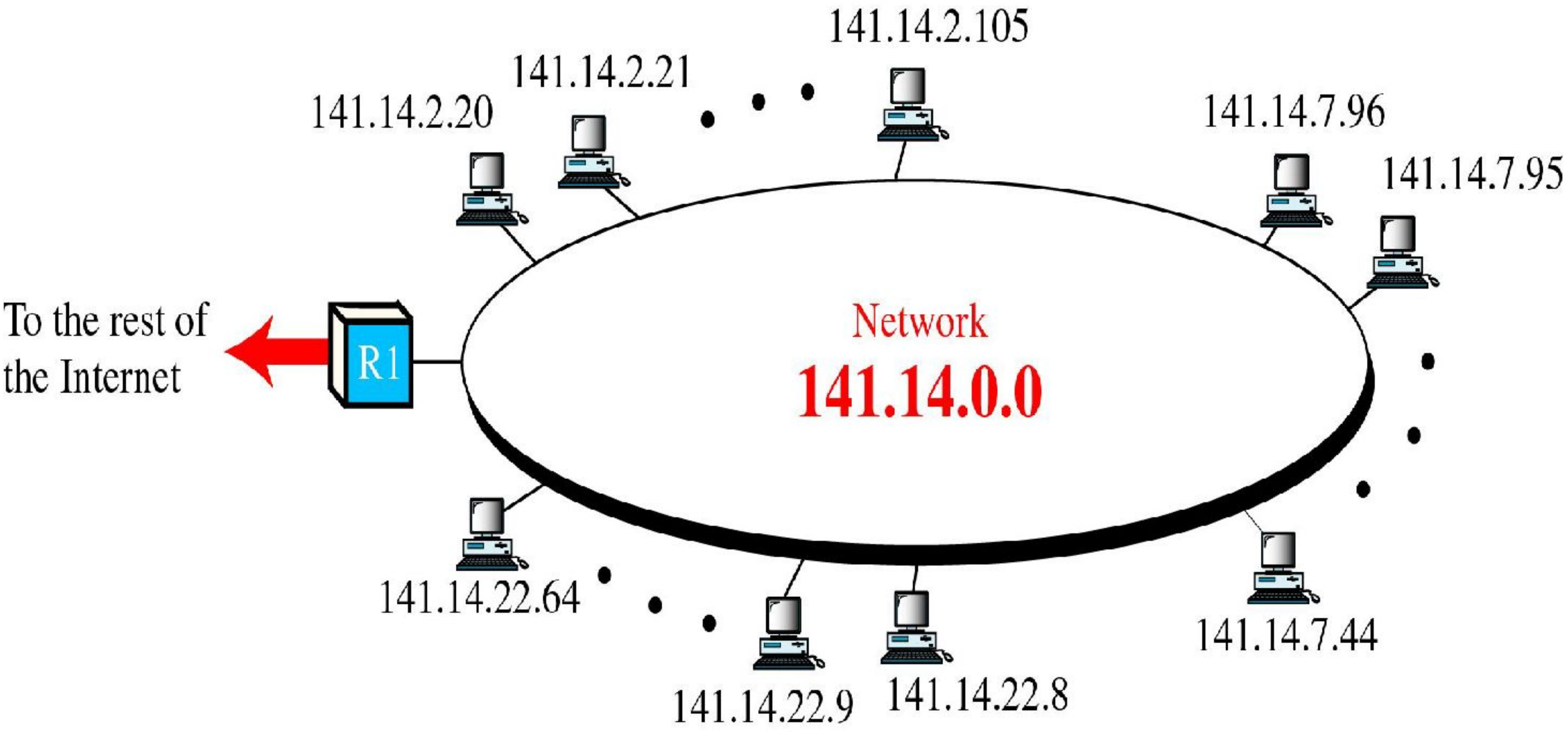


NETWORK WITH TWO LEVELS OF HIERARCHY

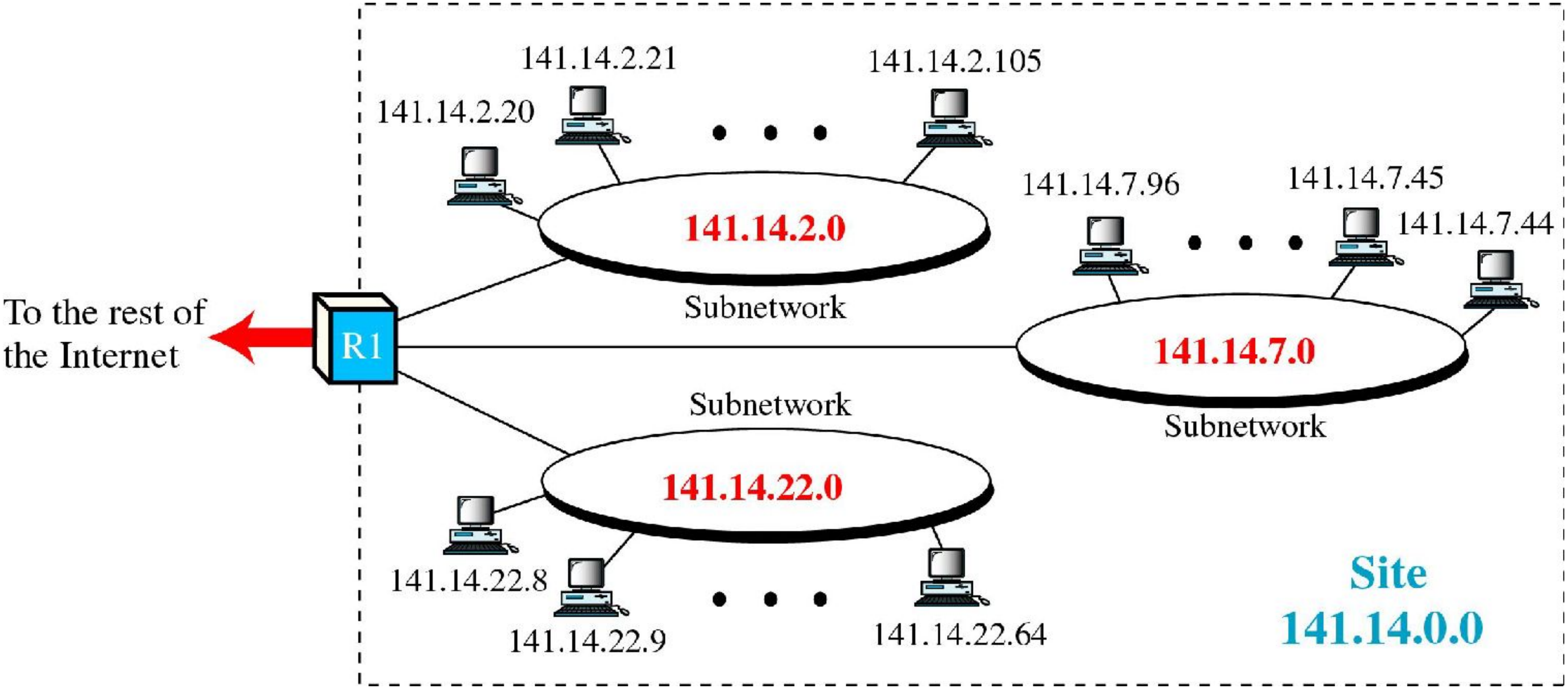
An IP address contains two ID's

- Network ID
- Host ID
- To reach to a host on the Internet, we must first reach the network using netid. Then we must reach to the host using hostid.
- This design of addresses called "Two Levels of Hierarchy" has limitations.

NETWORK WITH TWO LEVELS OF HIERARCHY



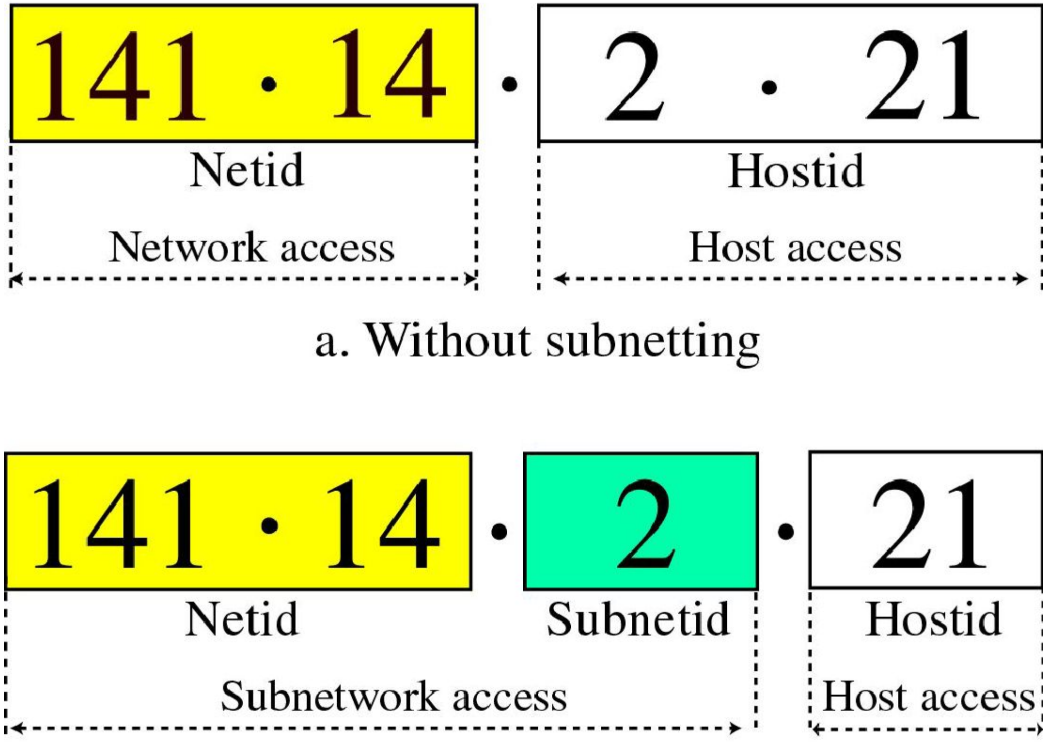
NETWORK WITH THREE LEVELS OF HIERARCHY



NETWORK WITH THREE LEVELS OF HIERARCHY

- Adding subnetworks creates an intermediate level of hierarchy in the IP addressing system.
- Thus the three levels are

1. Netid
2. Subnetid
3. Hostid

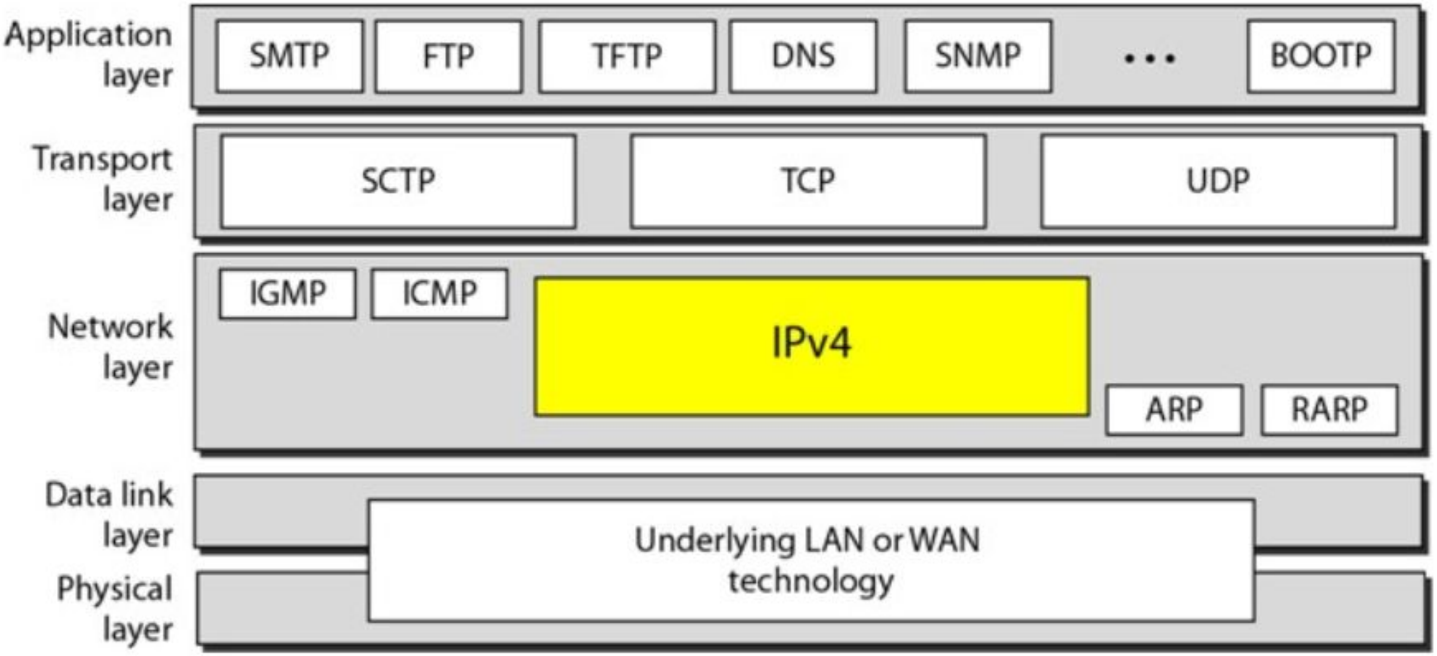


a. Without subnetting

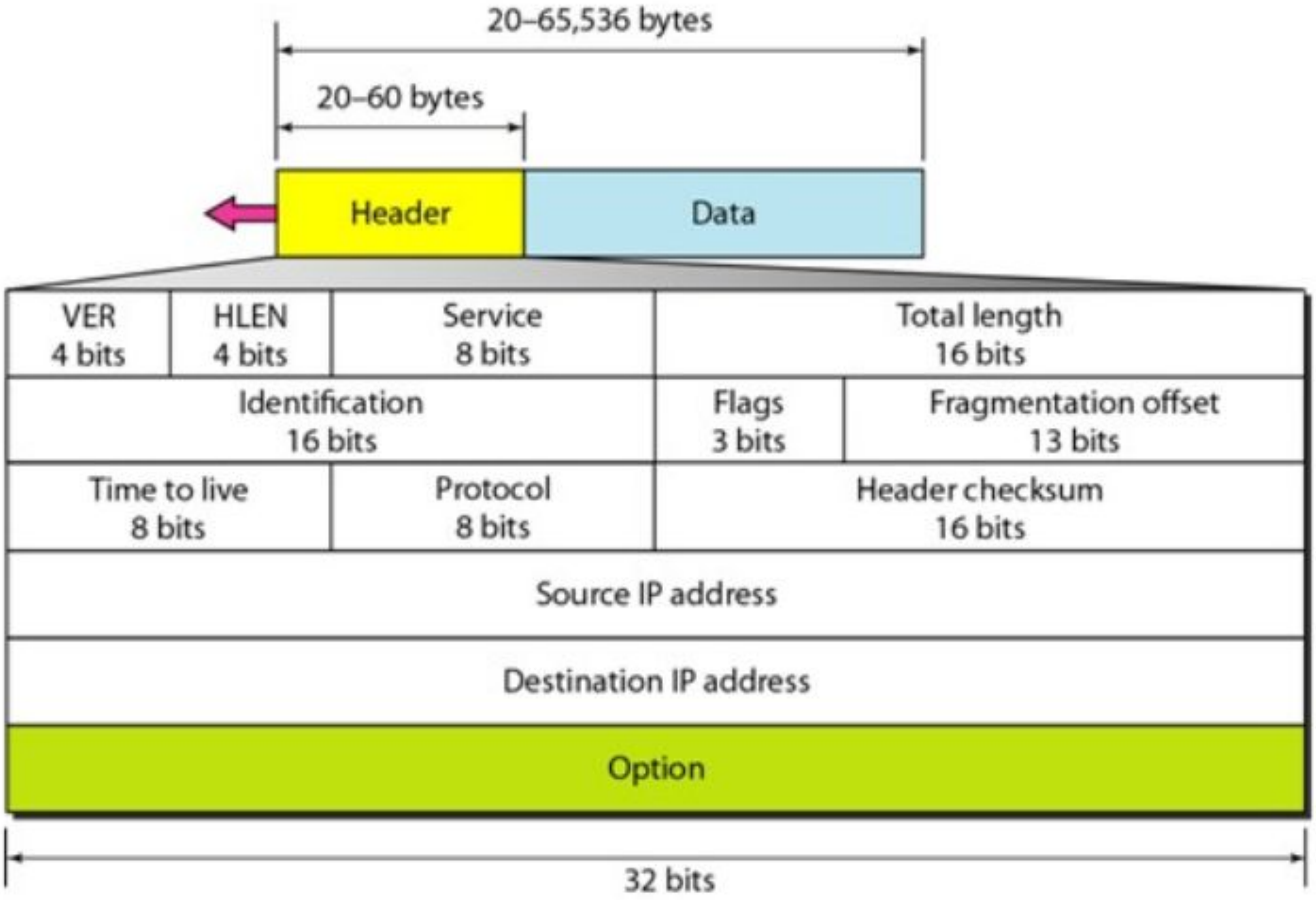
b. With subnetting

IPV4 PROTOCOL

- IPv4 is an unreliable datagram protocol- a best effort delivery service.
- IPv4 is a connectionless protocol that uses the datagram approach.



IPV4 DATAGRAM



20–65,536 bytes

20–60 bytes

Header

Data

VER
4 bits

HLEN
4 bits

Service
8 bits

Total length
16 bits

Identification
16 bits

Flags
3 bits

Fragmentation offset
13 bits

Time to live
8 bits

Protocol
8 bits

Header checksum
16 bits

Source IP address

Destination IP address

Option

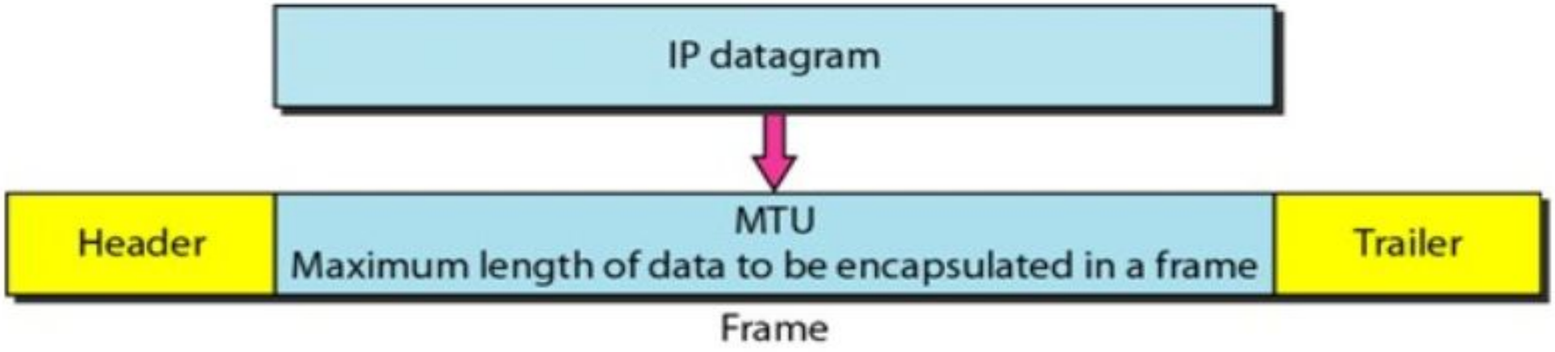
32 bits

FRAGMENTATION

- A datagram travels through different networks.
- The format and size of the received frame depends on the protocol used by physical network through which the frame has just travelled.

Maximum Transfer Unit

- Each link layer protocol has its own frame format. One of the features of each format is the maximum size of the payload that can be encapsulated.



FRAGMENTATION

- When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but some are changed.
- A datagram can be fragmented by the source host or any other router in the path. The reassembly of the datagram is done only by the destination host.
- The host or a router that fragments a datagram must change the values of three fields: flags, fragmentation offset and total length.

FRAGMENTATION

Fields Related to Fragmentation:

1. Identification : The 16-bit identification filed identifies a datagram originating from the source host. The combination of identification and the source IP address must uniquely define a datagram as it leaves the source host.
2. Flags : The 3 bit flags field defines three flags. The leftmost bit is reserved. The second bit (D bit) is called the Do not fragment bit. The third bit (M bit) is called More fragment bit.
3. Fragmentation offset: The 13- bit fragmentation offset field shows the relative position of this fragment with respect to the whole datagram.

FRAGMENTATION

Figure 20.10 *Flags used in fragmentation*

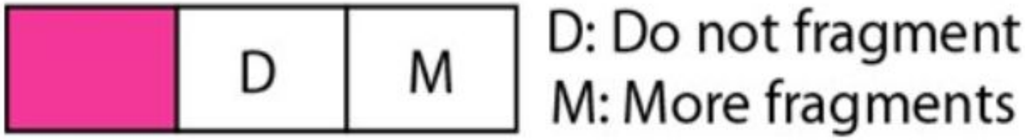
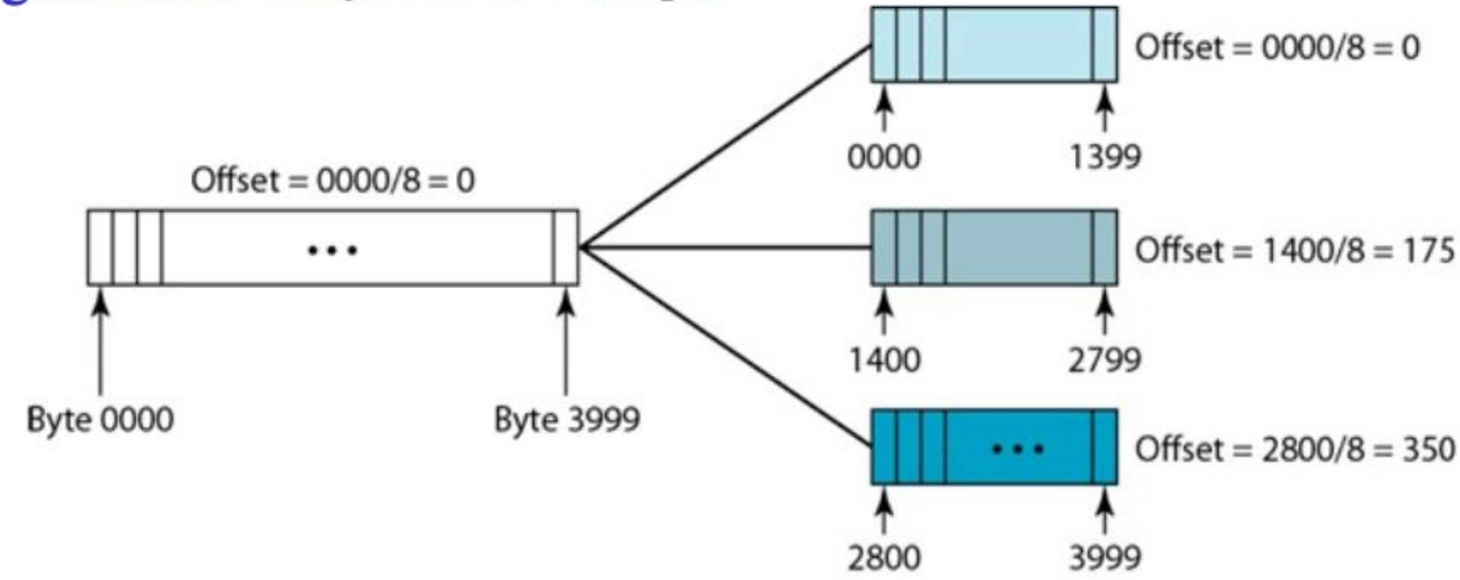
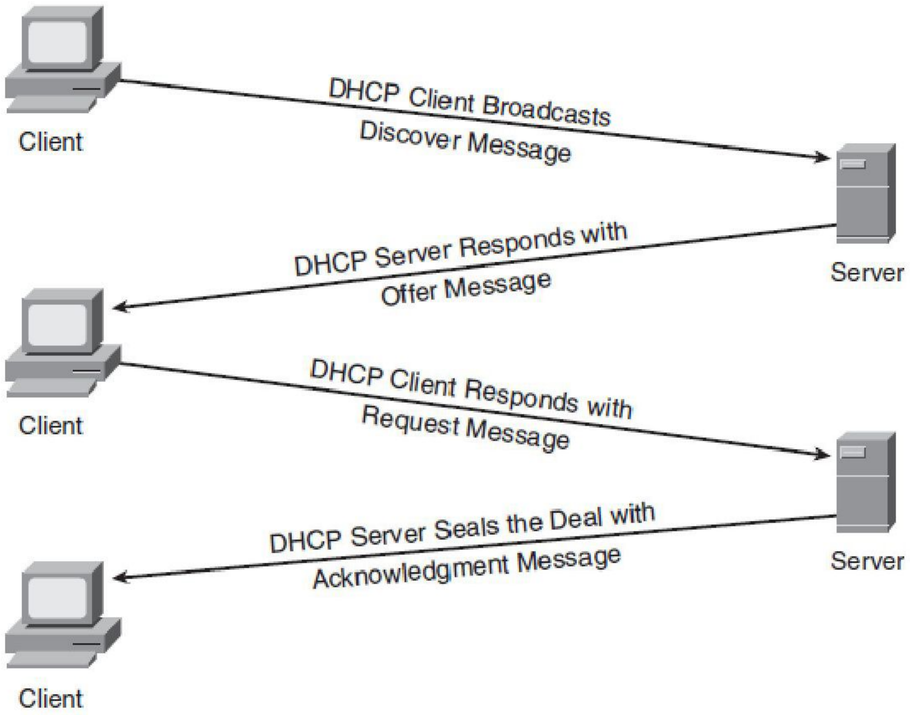


Figure 20.11 *Fragmentation example*



DHCP

- DHCP provides static and dynamic address allocation that can be manual or automatic.
- A host can request a static address from a DHCP server. A DHCP server has a database that statically binds physical addresses to IP addresses.
- DHCP has a second database with a pool of available IP addresses. This second database makes DHCP dynamic.



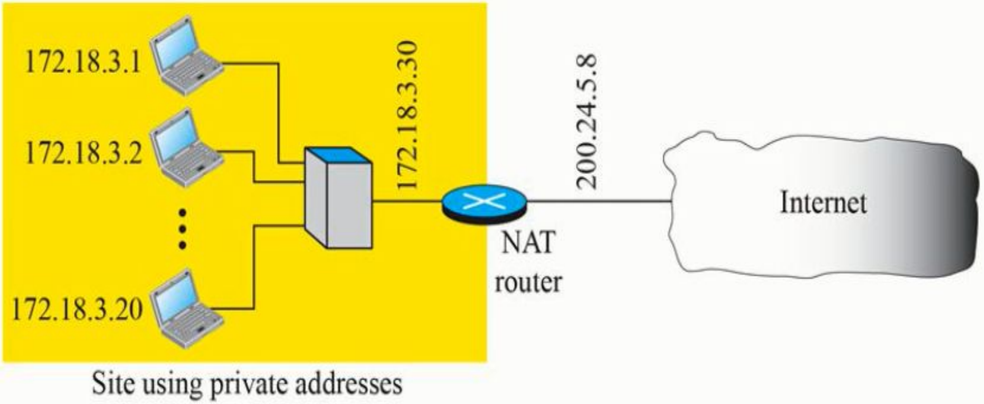
DHCP

- Step 1 : The host sends a DHCPDISCOVER broadcast message to locate a DHCP server.
- Step 2 : A DHCP server offers configuration parameters such as an IP address, a MAC address, a domain name, a default gateway, and a lease for the IP address to the client in a DHCPOFFER unicast message.
- Step 3 : The client returns a formal request for the offered IP address to the DHCP server in a DHCPREQUEST broadcast message.
- Step 4 : The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client.

NETWORK ADDRESS TRANSLATION

- A technology that provides the mapping between the private and universal addresses and at the same time support virtual private networks is called as Network Address Translation.
- NAT allows a site to use a set of private addresses for internal communication and set of global Internet addresses (atleast one) for communication with rest of the world.

Figure 18.29: NAT



NETWORK ADDRESS TRANSLATION

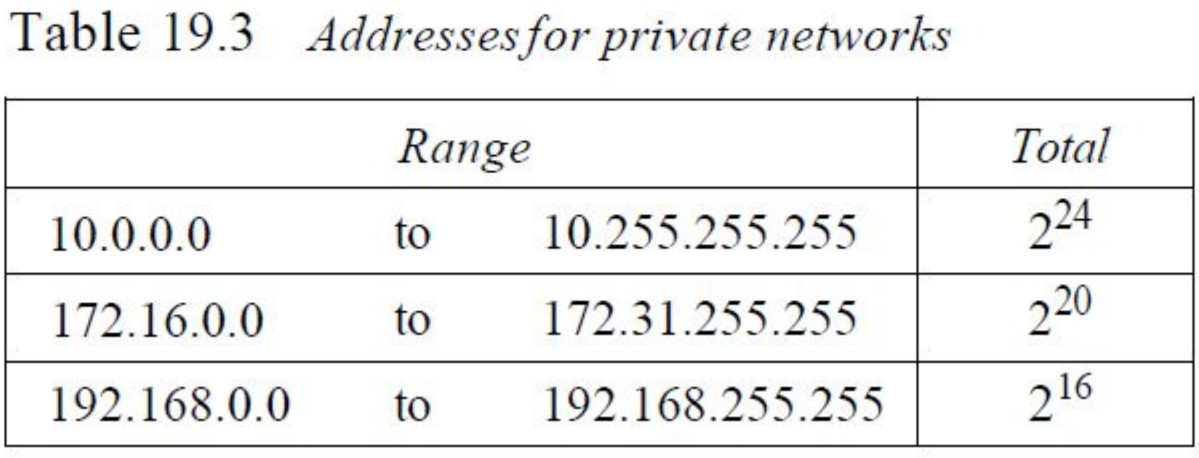
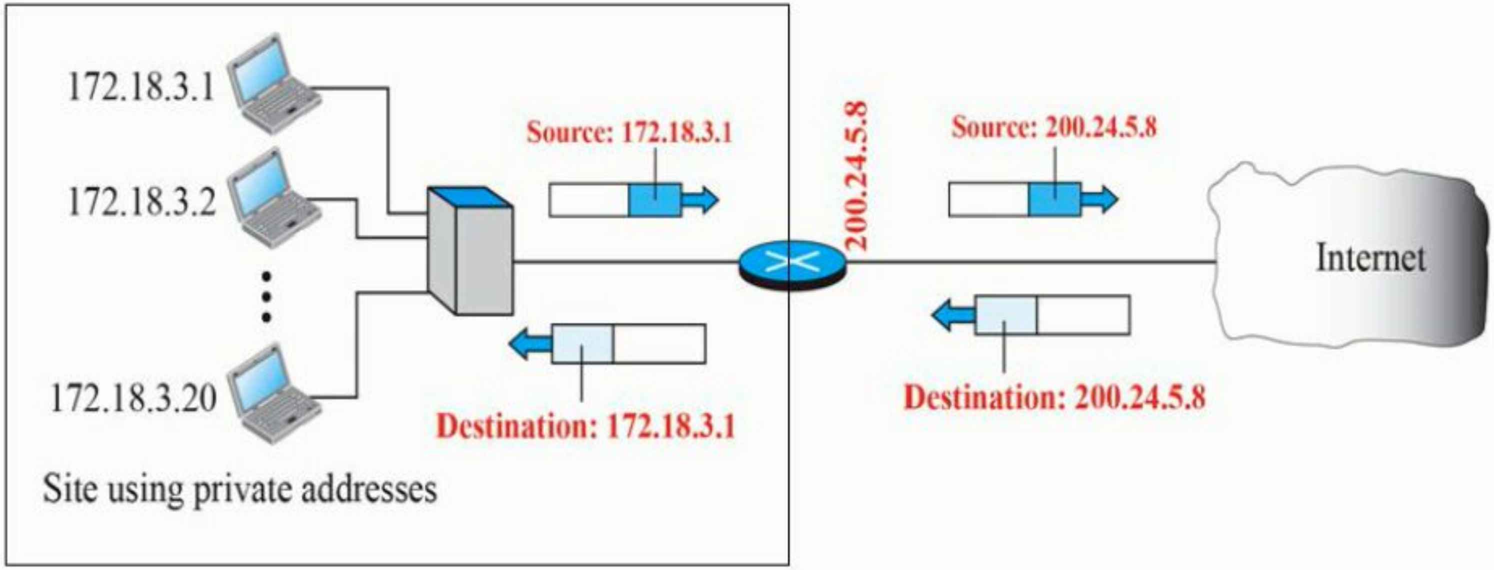


Table 19.3 *Addresses for private networks*

Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

NETWORK ADDRESS TRANSLATION

Figure 18.30: Address translation



NETWORK ADDRESS TRANSLATION

Using Pool of IP addresses:

- The use of only one global address by the NAT router allows only one private network host to access a given external host.
- To remove this restriction NAT uses a pool of addresses. The NAT router can use four addresses(200.24.5.8, 200.24.5.9, 200.24.5.10, 200.24.5.11)

NEXT GENERATION IP

IPV6 ADDRESSING

- An IPv6 address consists of 16 bytes (octets); it is 128 bits long.
- IPv6 addresses are represented using two notations: Binary and Colon hexadecimal.
- The colon hexadecimal divides the address into eight sections each made of four hexadecimal digits separated by colons.

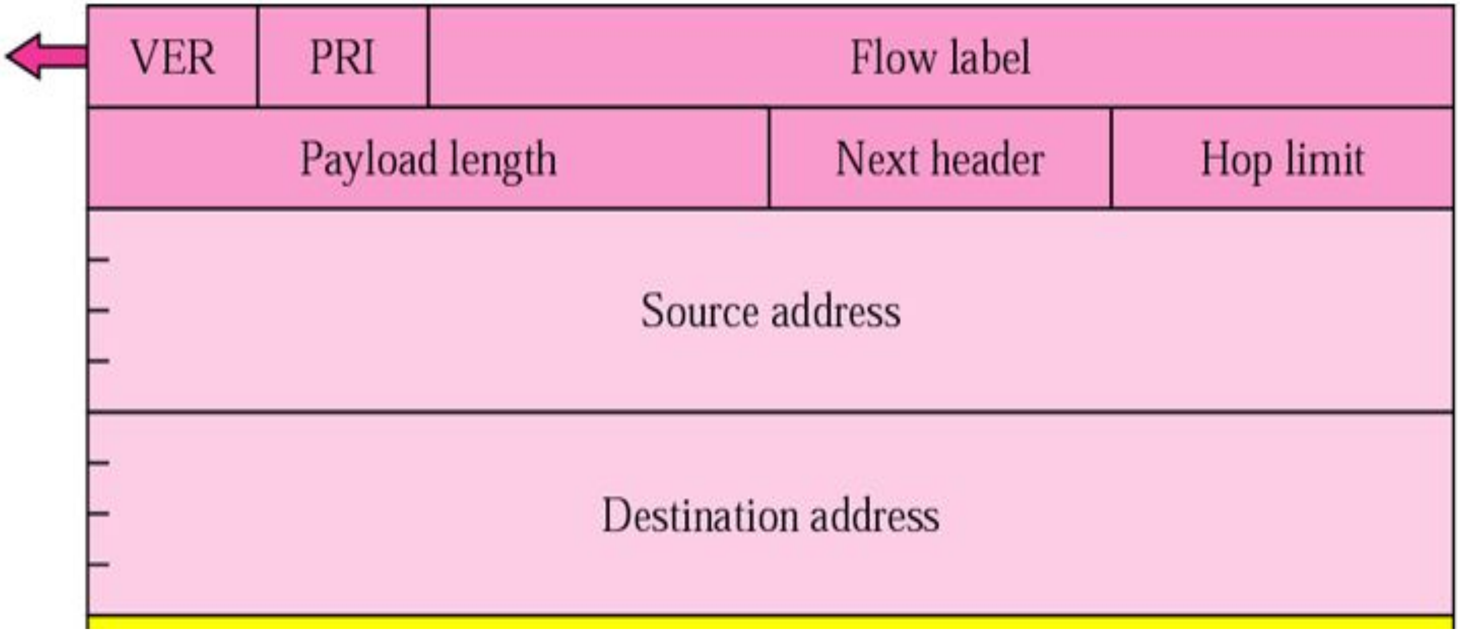
  Original Address:8000:0000:0000:0000:0123:4567:89AB:CDEF

  Compressed Address: 8000::123:4567:89AB:CDEF
- The address space of IPv6 contains 2^{128} addresses. This address is 2^{96} times the IPv4 address.

Address Types:

1. Unicast Address
2. Anycast Address
3. Multicast Address

IPV6 PROTOCOL



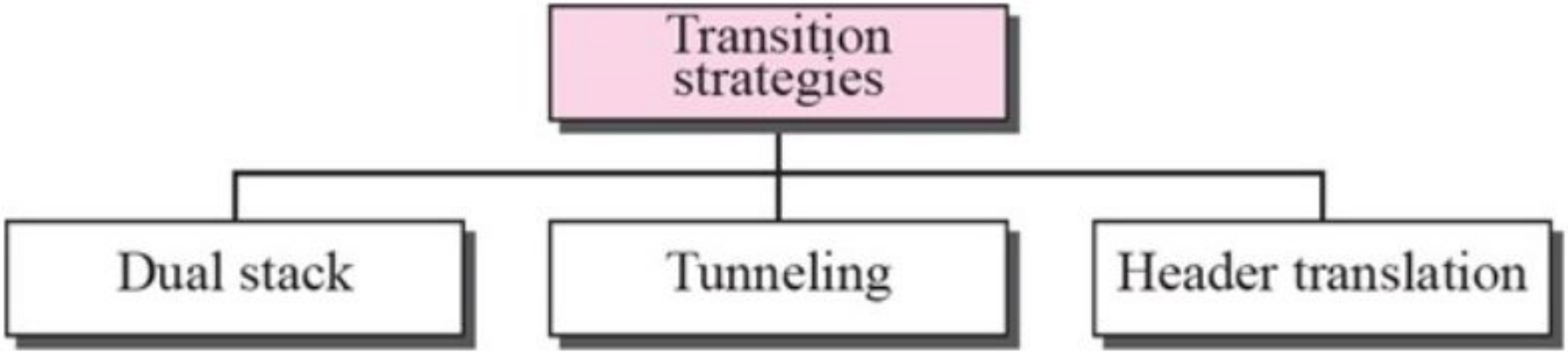
VER PRI Flow label

Payload length Next header Hop limit

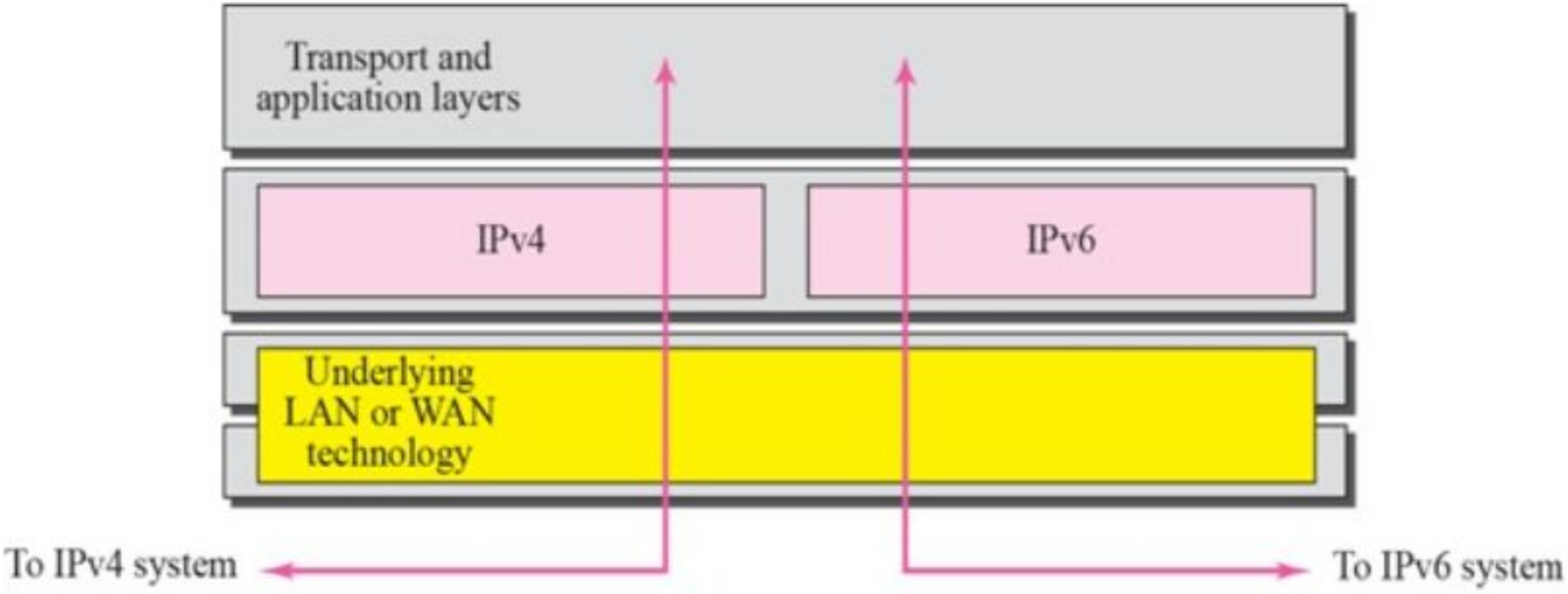
Source address

Destination address

TRANSITION FROM IPV4 TO IPV6

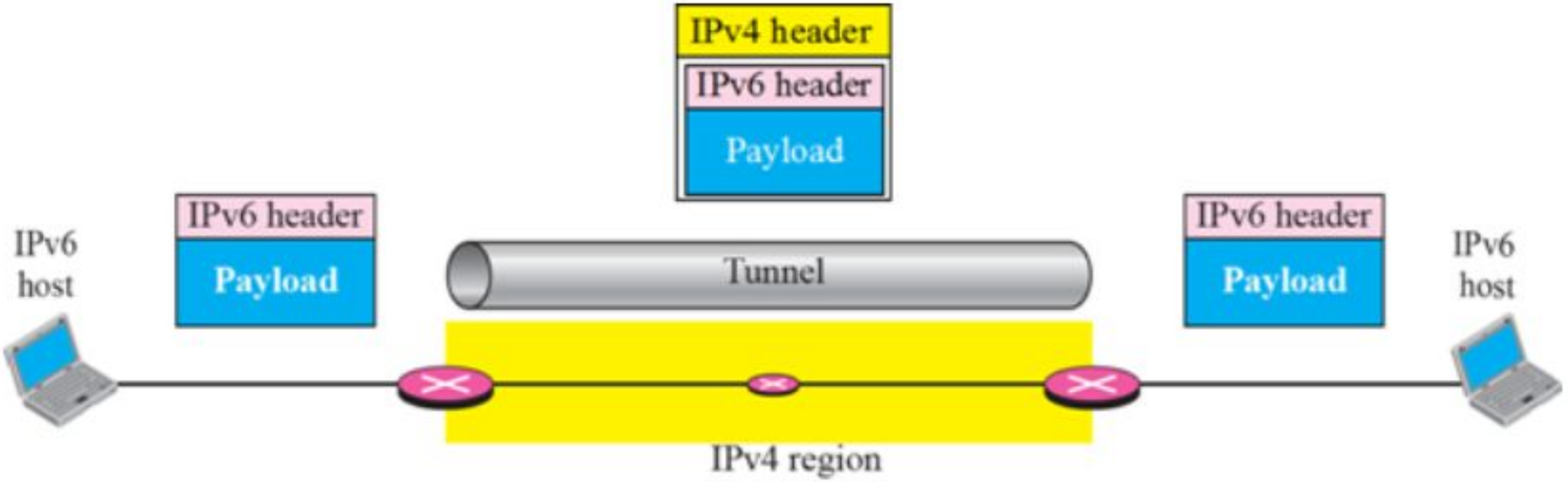


TRANSITION FROM IPV4 TO IPV6


Transport and application layers
IPv4
IPv6
Underlying LAN or WAN technology
To IPv4 system
To IPv6 system

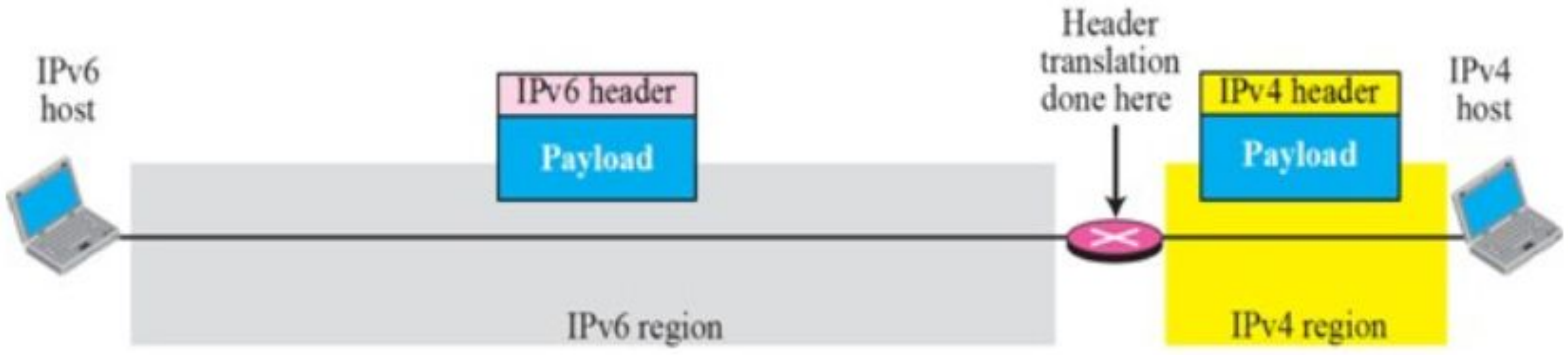
Dual Stack

TRANSITION FROM IPV4 TO IPV6



Tunneling

TRANSITION FROM IPV4 TO IPV6



Header Translation

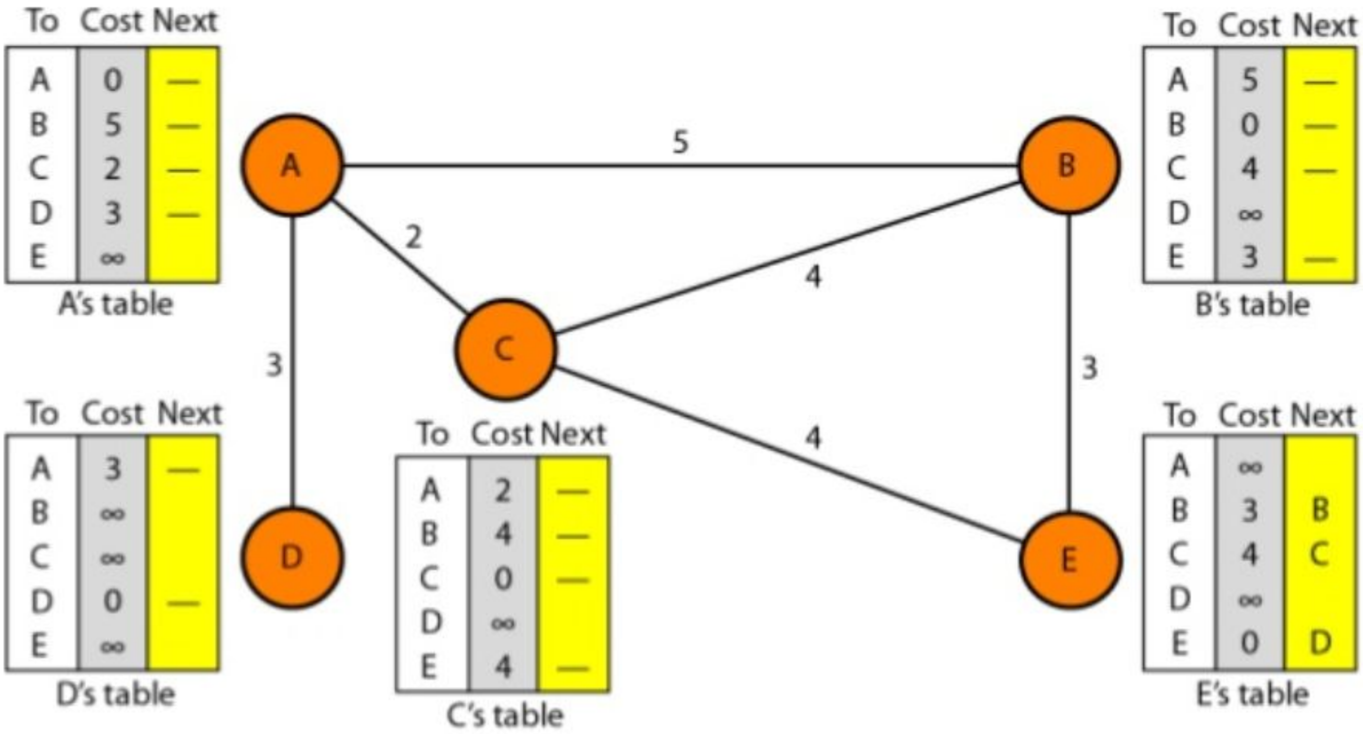
ROUTING ALGORITHMS

DISTANCE VECTOR ROUTING

- A **distance vector routing** algorithm operates by having each router maintain a table (i.e., a vector) giving the best known distance to each destination and which link to use to get there.
- Each router periodically shares its knowledge about the entire network with its neighbors in following 3 steps:

1. Knowledge about the whole network
2. Routing only to neighbors
3. Information sharing at regular intervals

DISTANCE VECTOR ROUTING



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

A's table

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

B's table

To	Cost	Next
A	3	—
B	∞	
C	∞	
D	0	—
E	∞	

D's table

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

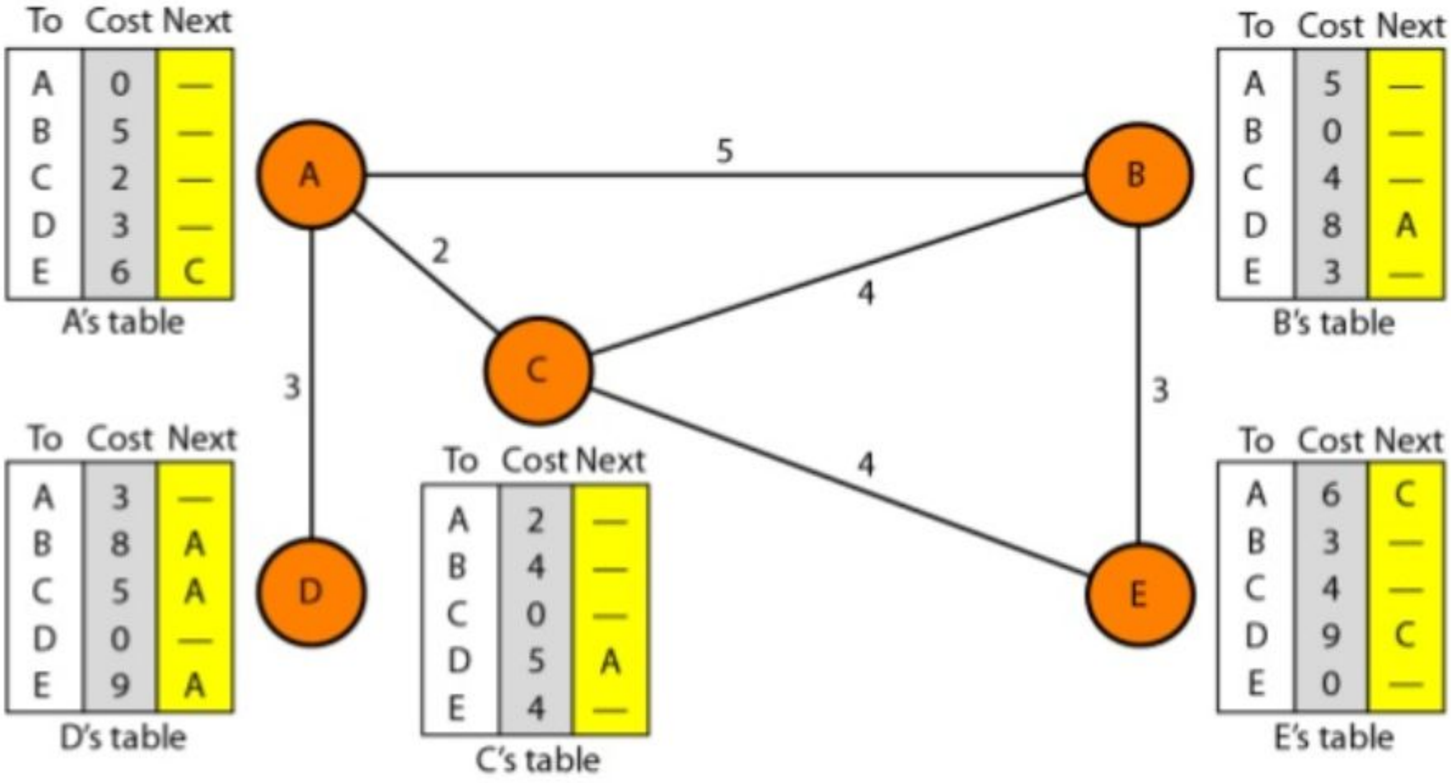
C's table

To	Cost	Next
A	∞	
B	3	B
C	4	C
D	∞	
E	0	D

E's table

Initialization of tables in DVR

DISTANCE VECTOR ROUTING



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	—

Final tables in DVR

DISTANCE VECTOR ROUTING

Updating the Routing table:

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

1. The receiving node needs to add the cost between itself and the sending node to each value in the second column.
2. The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from any row. The sending node is the next node in the route.
3. The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

DISTANCE VECTOR ROUTING

When to Share

- The question now is, When does a node send its partial routing table (only two columns) to all its immediate neighbors? The table is sent both periodically and when there is a change in the table.
- **Periodic Update :** A node sends its routing table, normally every 30 s, in a periodic update.
- **Triggered Update :** A node sends its two-column routing table to its neighbors anytime there is a change in its routing table. This is called a triggered update. The change can result from the following.

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

BELLMAN FORD ALGORITHM

```
1.   Initialize all distance value as infinity except source (0).
2.   Repeat (v-1) times:
         If d[u] + cost (uv) < d[v]
         then update d[v]
         Else skip
3. Relax all vertices once more.
```

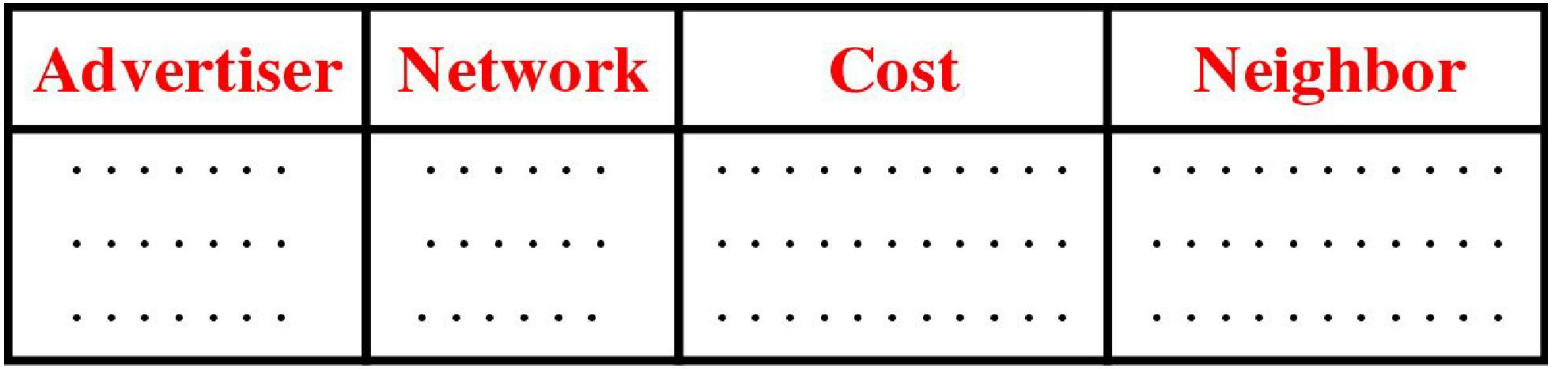
LINK STATE ROUTING

- In this algorithm the cost associated with an edge defines the state of the link.
- To create a least cost tree with this method , each node needs to have a complete map of the network.
- The collection of states for all links, is called link state database(LSDB)
- Link State Packet(LSP) contains the following information:

1. The ID of the node that created the LSP
2. The list of directly connected neighbors of that node, with the cost of link to each one
3. A sequence number
4. A TTL for this packet

LINK STATE ROUTING

- When the router floods the network with information, it is said to be advertising.
- For advertising it uses a short packet called "**Link State Packet**" **(LSP).**
- LSP has four fields: ID of advertiser, ID of destination network, the cost and the ID of neighbor router.



Advertiser	Network	Cost	Neighbor
• • • • • • •	• • • • • •	• • • • • • • • • • •	• • • • • • • • • • •
• • • • • • •	• • • • • •	• • • • • • • • • • •	• • • • • • • • • • •
• • • • • • •	• • • • • •	• • • • • • • • • • •	• • • • • • • • • • •

LINK STATE ROUTING

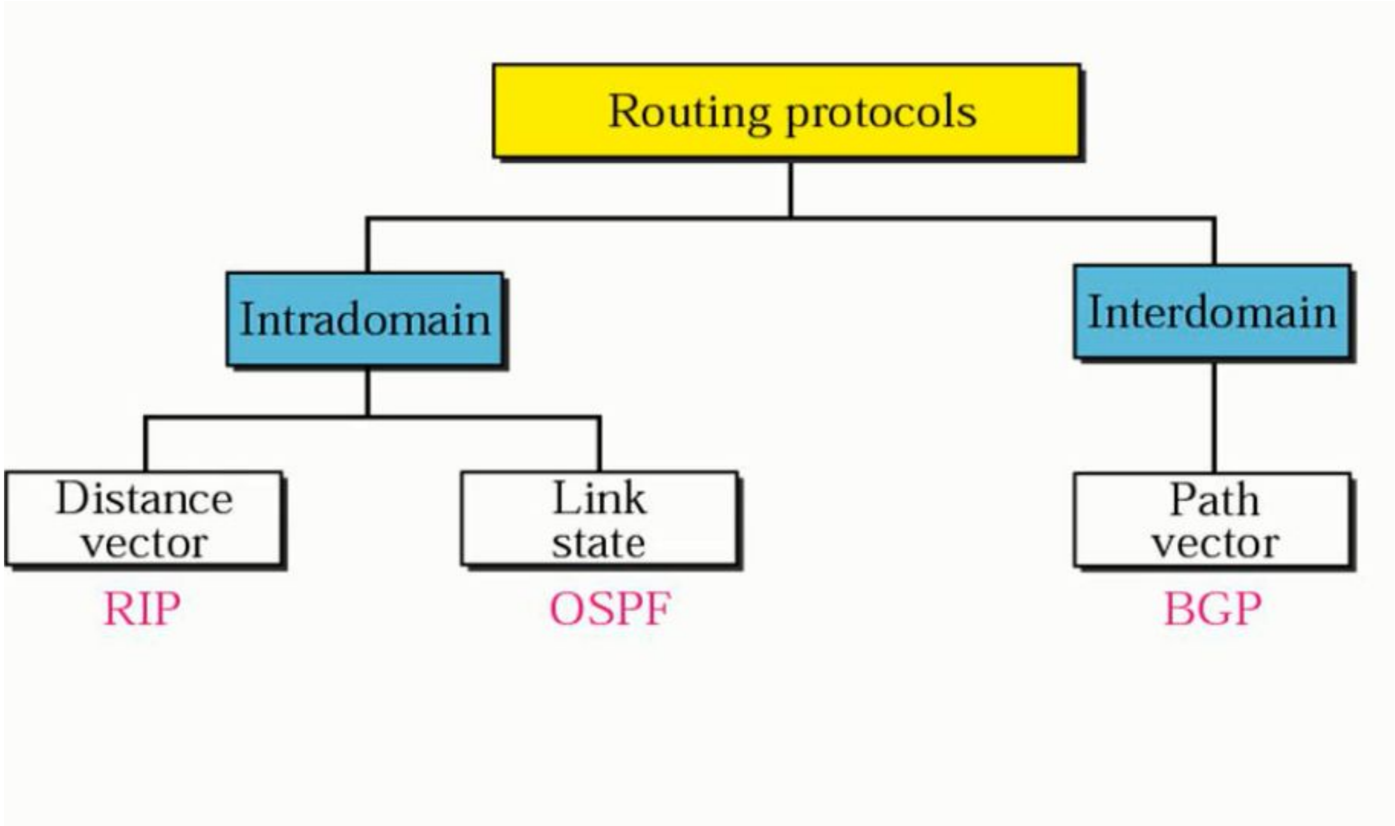
- Initially each router sends a short greeting packet to its neighbors.
- If neighbor replies, it is assumed to be alive and functioning.
- Through this greeting packets each router find out the state of each link.
- Prepares an LSP based on this results and floods the network.
- Every router receives every LSP and puts the information into a "Link State Database".
- This database is stored in router's memory
- Router use this database to calculate the routing table.
- Routers use a static algorithm called "Dijkstra's Algorithm" for calculating the routing table.

PATH VECTOR ROUTING

- Link state and distance vector routing are based on the least cost goal. However there are instances where this goal is not a priority.
- Least cost goal applied by LS or DV routing does not allow a sender to apply specific policies to the route a packet may take.
- In path vector routing the source can control the path.
- In Path vector routing the path from a source to all destination is determined by best spanning tree.
- If there is more than one route to a destination, the source can choose the route that meets its policy best.

$$\text{Path}(x , y) = \text{best}\{\text{Path}(x , y),[x + \text{Path}(v , y)]\}$$

ROUTING PROTOCOLS



ROUTING INFORMATION PROTOCOL

Hop Count

- A router in an AS needs to know how to forward a packet to different networks in an AS, RIP routers advertise the cost of reaching different networks instead of reaching other nodes.
- Any route in an AS cannot have more than 15 hops.

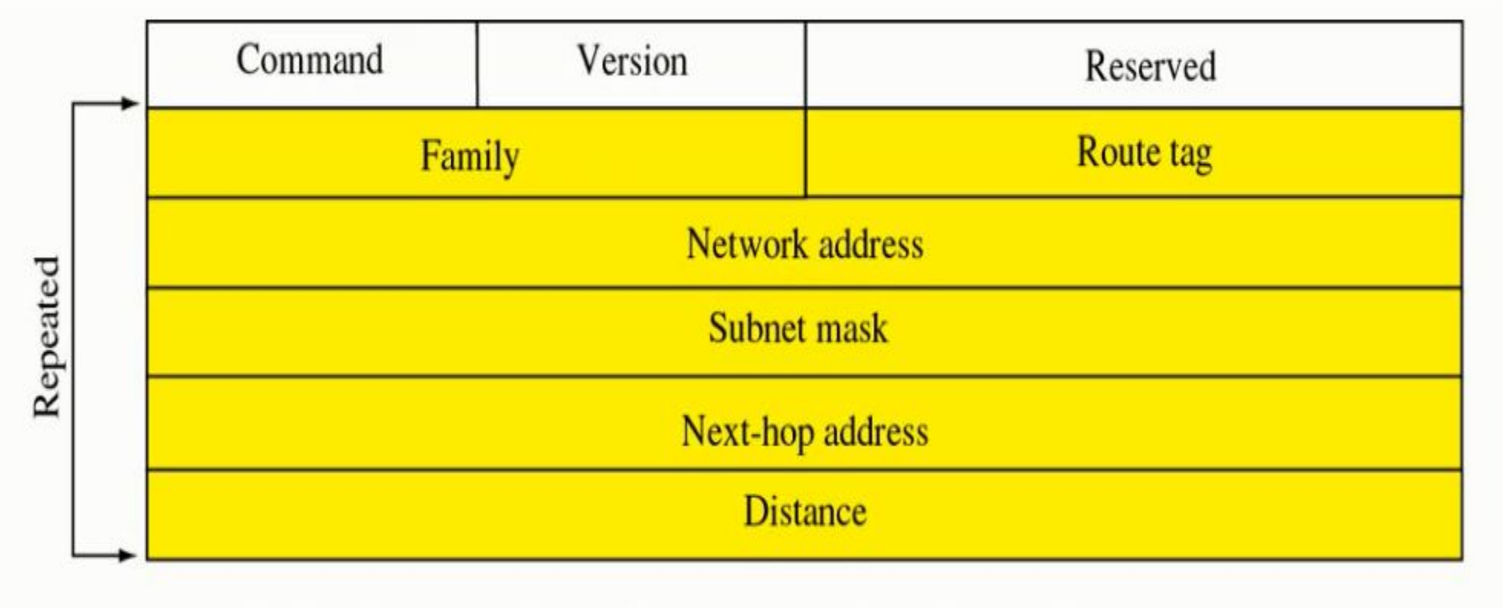
RIP Implementation

- RIP is implemented as a process that uses the service of UDP.
- RIP has two versions: RIP-1 and RIP-2

ROUTING INFORMATION PROTOCOL

RIP Messages

- RIP has 2 types of messages : Request and Response
- A request message can ask about specific entries or all entries.
- A response message can be either solicited or unsolicited.



Command	Version	Reserved
Family		Route tag
Network address		
Subnet mask		
Next-hop address		
Distance		

ROUTING INFORMATION PROTOCOL

Algorithm

1. RIP implements the same algorithm as the DVR algorithm with some minor changes.
2. Instead of sending only distance vectors, a router needs to send the whole contents of its forwarding table.
3. The receiver adds one hop to each cost and changes the next router field to the address of the sending router.

Timers in RIP: RIP uses three timers to support its operation.

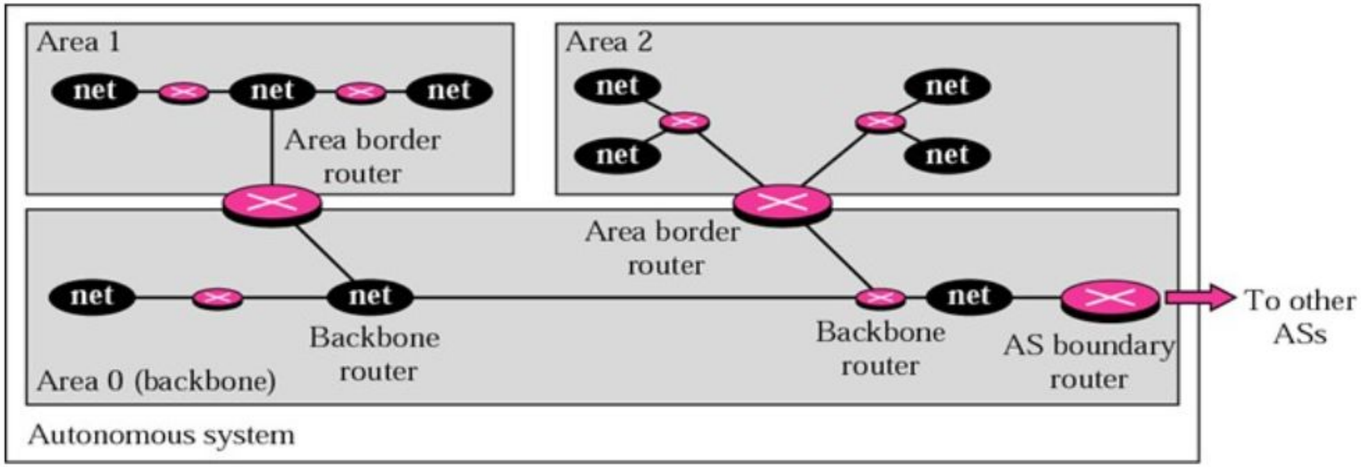
1. Periodic timer(25-35 seconds)
2. Expiration timer(180 seconds)
3. Garbage Collection timer(120 seconds)

ROUTING INFORMATION PROTOCOL

- Version 1 of RIP uses broadcasting to send RIP message to every neighbor .
- All the router and the hosts receive the packets .
- RIP version 2 Uses the multicast address 224.0.0.9 to multicast RIP message only to RIP routers in the network.
- RIP message are encapsulated in UDP user datagram.
- The well-known port assigned to RIP in UDP is port 520.

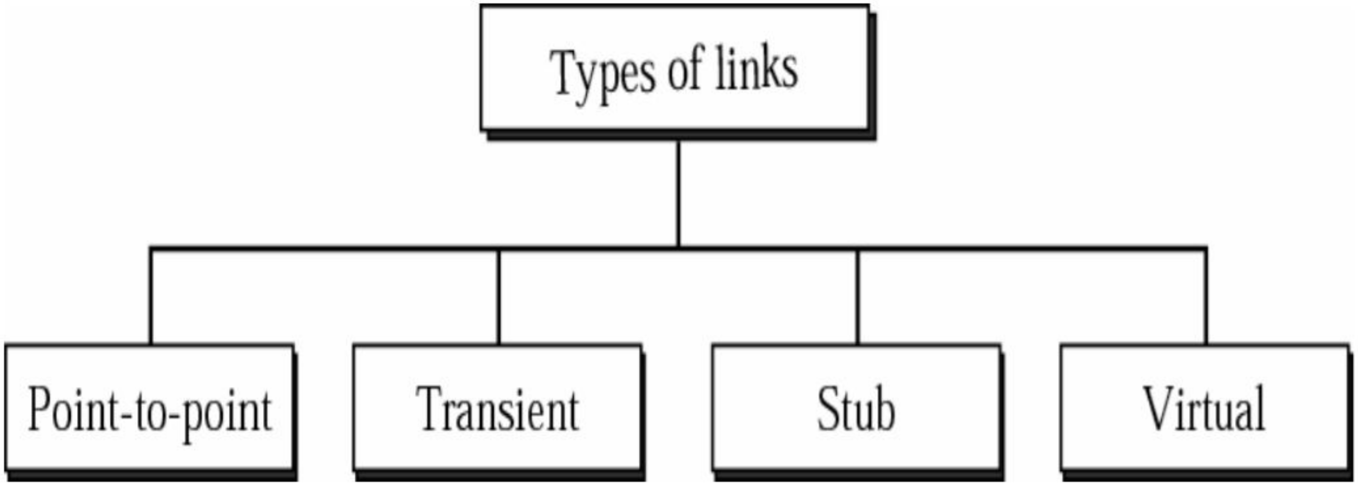
OPEN SHORTEST PATH FIRST (OSPF)

- The Open Shortest Path First or OSPF protocol is an intradomain routing protocol based on link state routing. Its domain is also an autonomous system.
- **Areas :** To handle routing efficiently and in a timely manner, OSPF divides an autonomous system into areas.
- An area is a collection of networks, hosts, and routers all contained within an autonomous system.
- At the border of an area, special routers called area border routers summarize the information about the area and send it to other areas.
- Among the areas inside an autonomous system is a special area called the *backbone*.

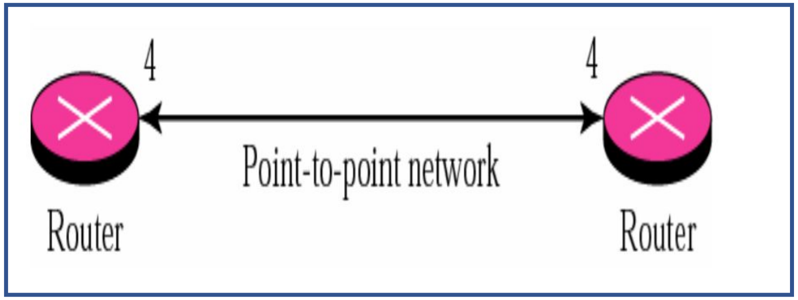


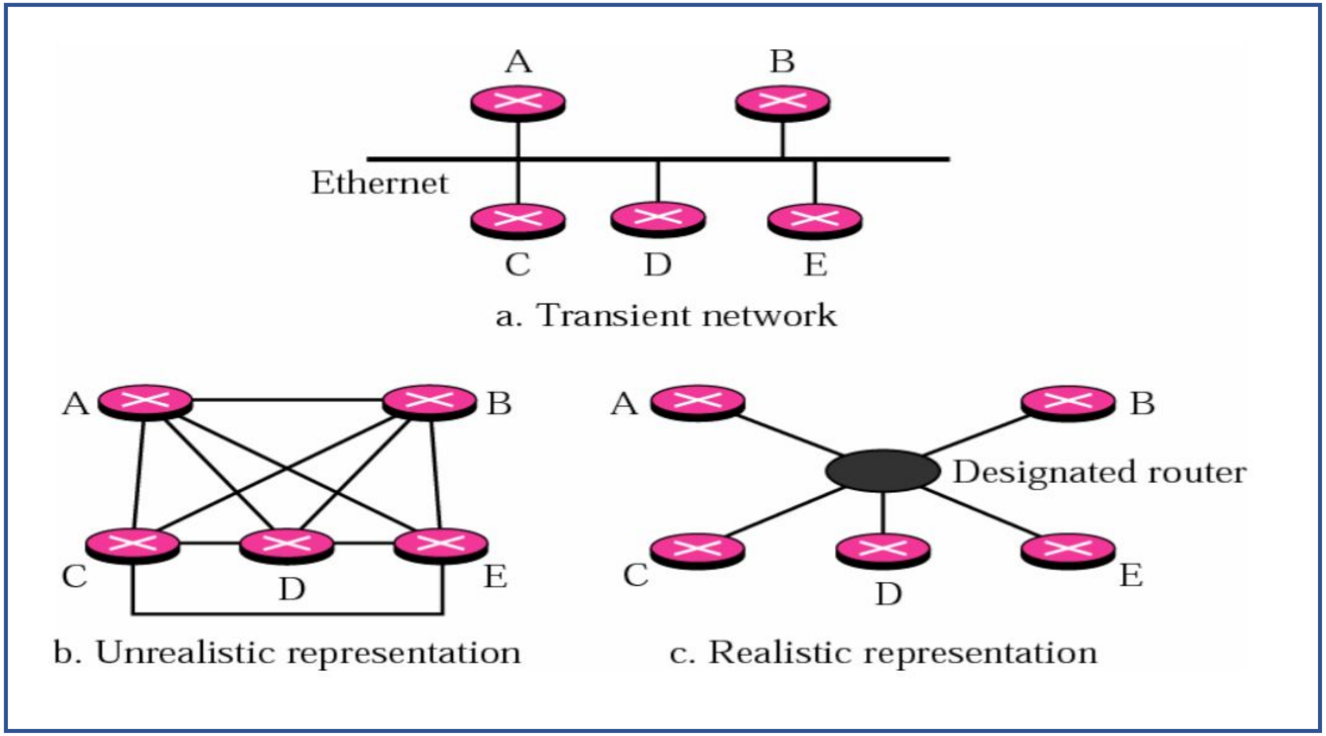
OPEN SHORTEST PATH FIRST (OSPF)

- The OSPF protocol allows the administrator to assign a cost, called the metric, to each route.
- OSPF uses link state routing to update the routing table in an area.
- In OSPF, a connection is called a link



OPEN SHORTEST PATH FIRST (OSPF)



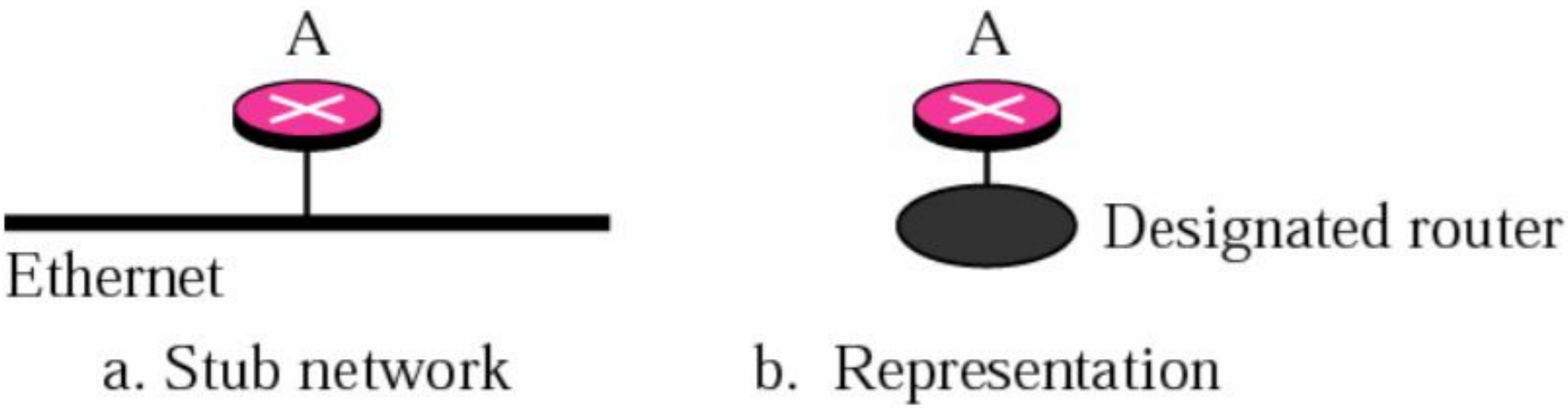


a. Transient network

b. Unrealistic representation

c. Realistic representation

OPEN SHORTEST PATH FIRST (OSPF)



OPEN SHORTEST PATH FIRST (OSPF)

Link State Advertisement

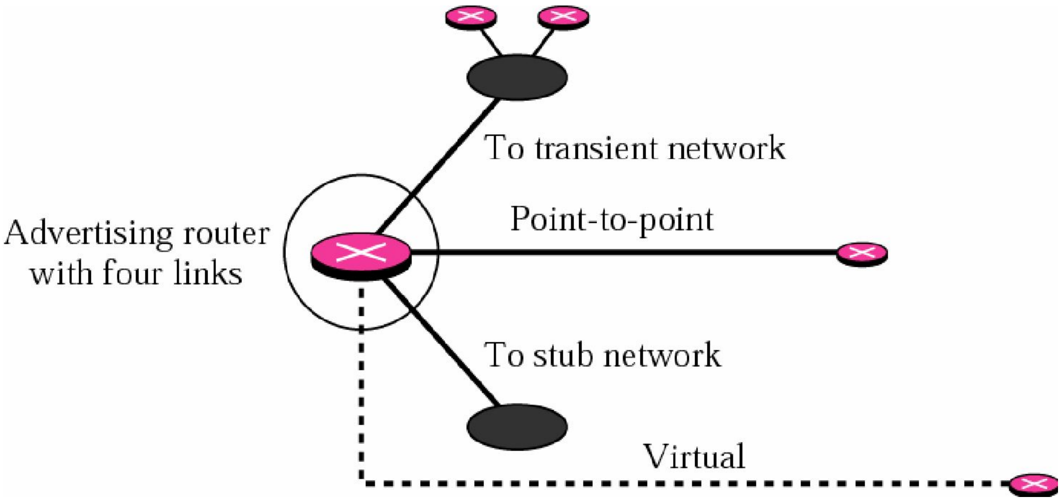
OSPF is based on link state routing algorithm, which requires that a router advertise the state of each link to all neighbors for the formation of LSDB.

Types of advertisement

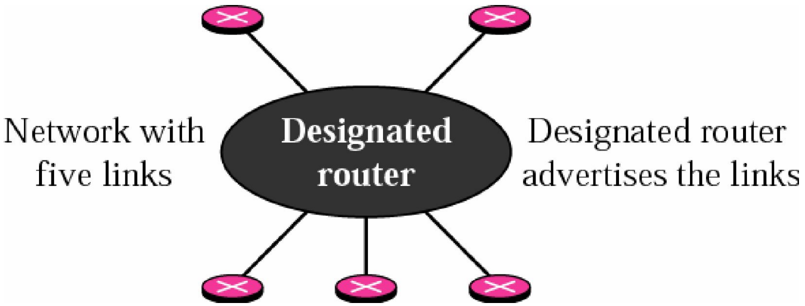
1. Router link
2. Network link
3. Summary link to network
4. Summary link to AS border network
5. External link

OPEN SHORTEST PATH FIRST (OSPF)

Router link

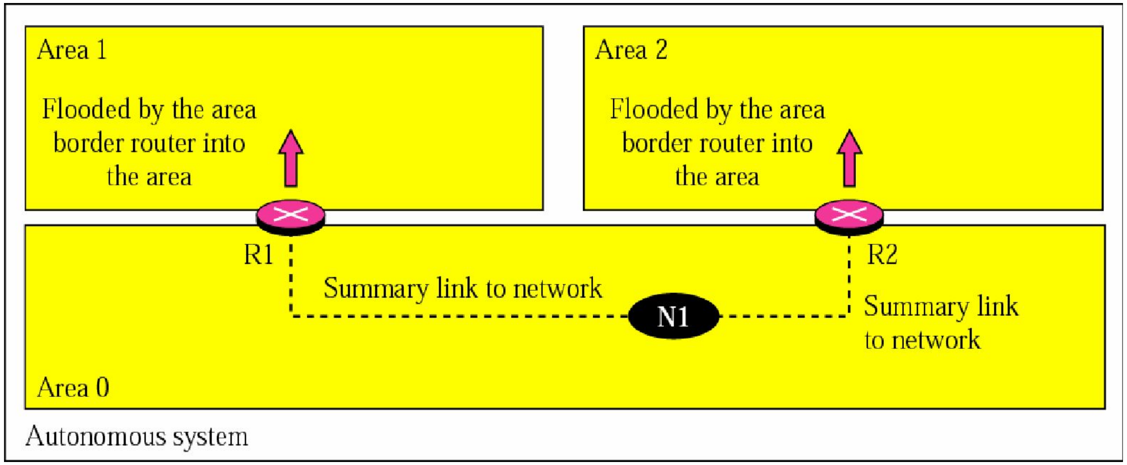


Network Link

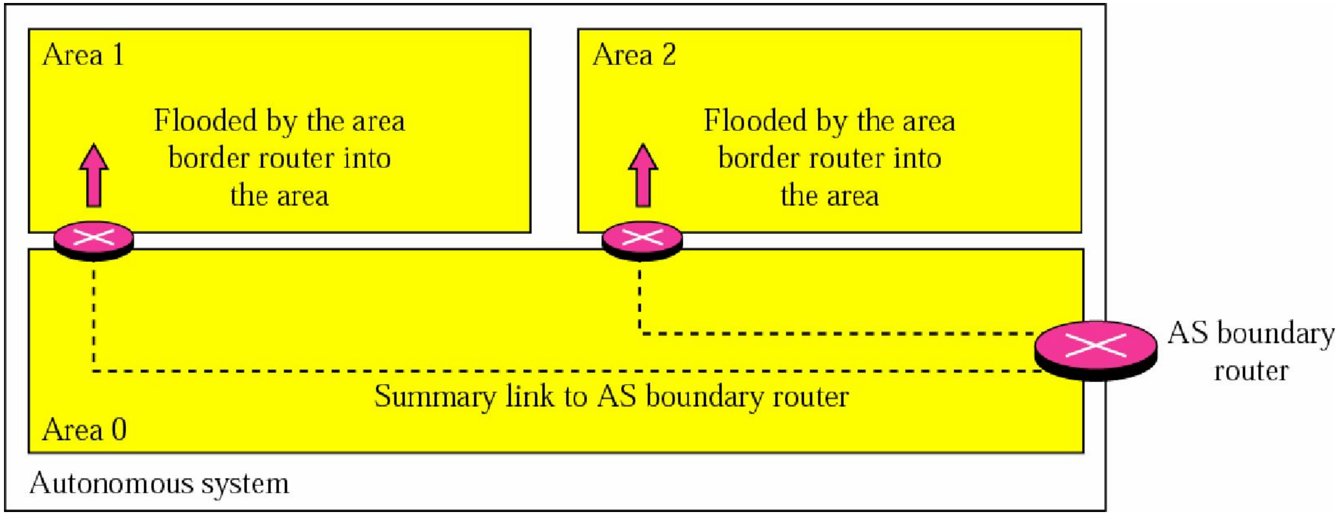


OPEN SHORTEST PATH FIRST (OSPF)

Summary link to network

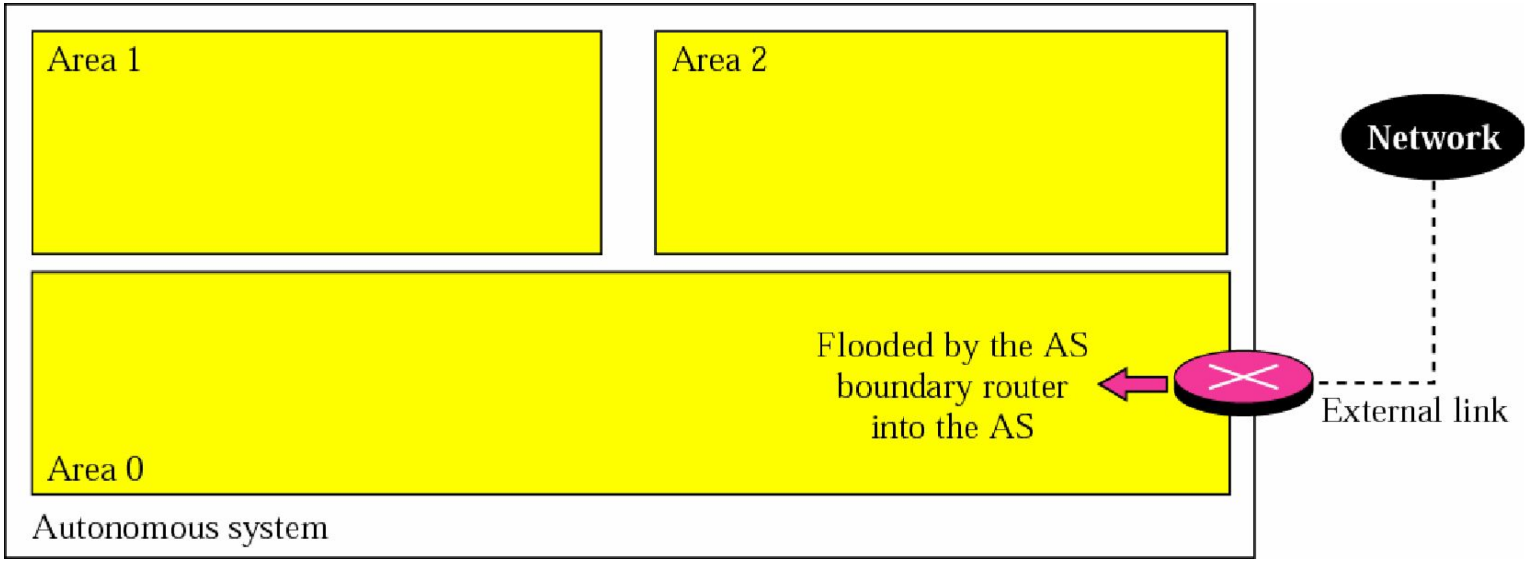

Area 1
Flooded by the area border router into the area
Area 2
Flooded by the area border router into the area
R1
R2
Summary link to network
N1
Summary link to network
Area 0
Autonomous system

Summary link to AS Boundary Router


Area 1
Flooded by the area border router into the area
Area 2
Flooded by the area border router into the area
AS boundary router
Summary link to AS boundary router
Area 0
Autonomous system

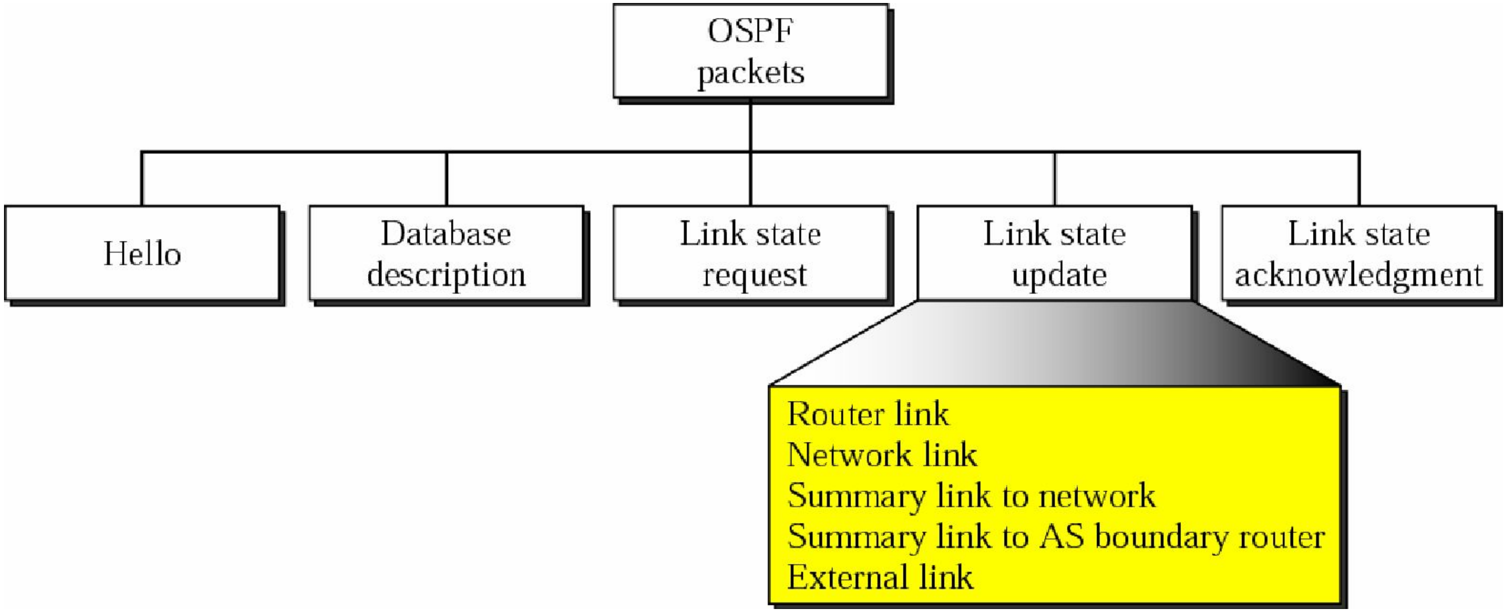
OPEN SHORTEST PATH FIRST (OSPF)

External Link

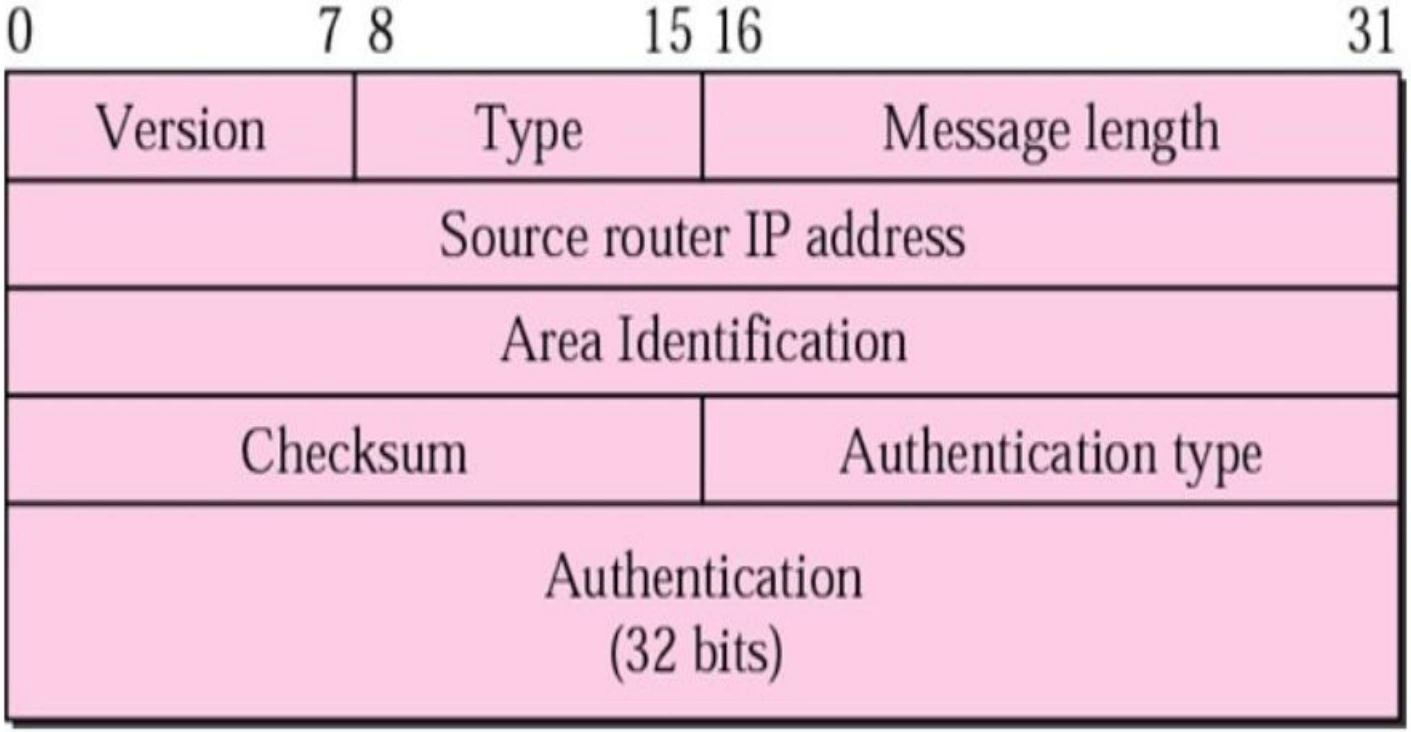


OPEN SHORTEST PATH FIRST (OSPF)

OSPF uses 5 different types of packets



OPEN SHORTEST PATH FIRST (OSPF)



0–7	8–15	16–31
Version	Type	Message length
Source router IP address		
Area Identification		
Checksum		Authentication type
Authentication (32 bits)		

OSPF Common header

BORDER GATEWAY PROTOCOL(BGP)

- The BGP is the only interdomain routing protocol used in the Internet today.
- Each router in each AS knows how to reach a network that is in its own AS, but it does not know how to reach a network in another AS.
- The autonomous systems are divided into three categories:

1. Stub
2. Multihomed
3. Transit.

- To enable each router to route a packet to any network in the Internet, a variation of BGP, called external BGP (eBGP) is installed on each border router.
- A second variation of BGP, called internal BGP (iBGP) is installed on all routers.

BORDER GATEWAY PROTOCOL(BGP)

Operation of External BGP(eBGP)

- BGP is a kind of point-to-point protocol.
- When a software is installed on two routers, they try to create a TCP connection.
- The two routers that run the BGP processes are called BGP peers or BGP speakers.
- Each logical connection in BGP is referred to as a session.

Operation of Internal BGP(iBGP)

- iBGP creates a session between any possible pair of routers inside an AS.
- If an AS has only one router there cannot be an iBGP session.

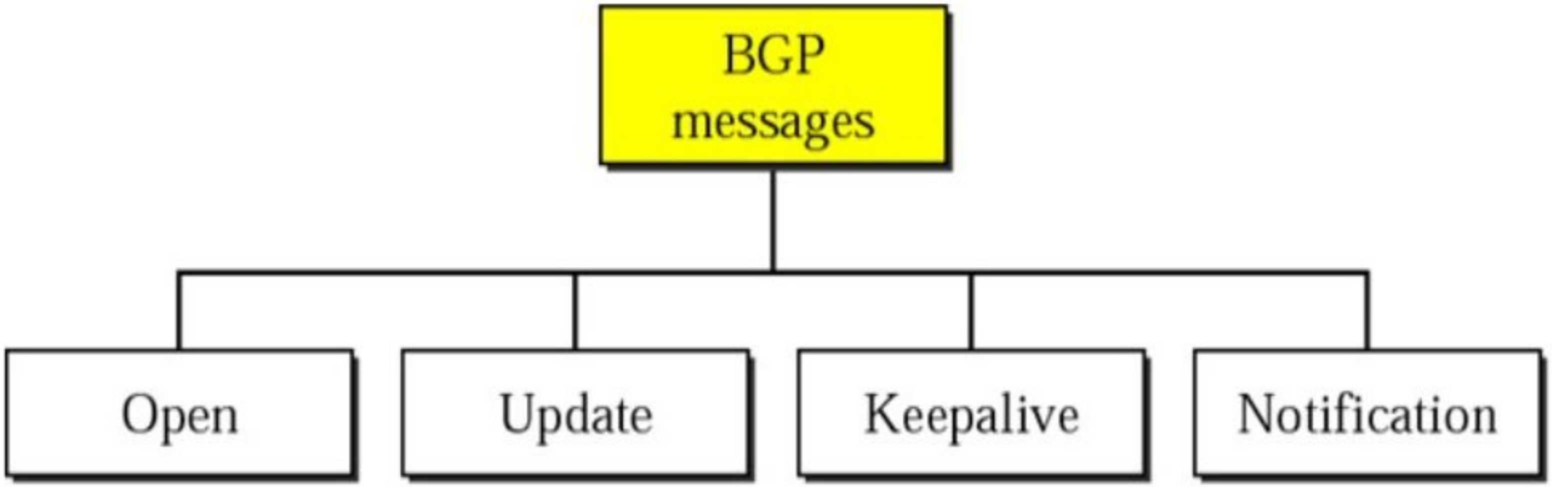
BORDER GATEWAY PROTOCOL(BGP)

Path Attributes

- In both intradomain routing protocols ,a destination is normally associated with two pieces of information: next hop and cost.
- Interdomain routing requires more information about how to reach the final destination. In BGP these pieces are called path attributes.
- Path attributes are divided into two broad categories: well-known and optional.

1. ORIGIN (well-known)
2. AS-PATH (well-known)
3. NEXT HOP (well-known)
4. MULT-EXIT-DISC (optional)
5. LOCAL-PREF (well-known)
6. ATOMIC-AGGREGATE (well-known)
7. AGGREGATOR (optional)

BORDER GATEWAY PROTOCOL(BGP)



Thank you …