Network Layer

Outline

- Goal
  - Understanding the IP address Assignment
  - Routing Protocols
  - Frame Formats (IPv4 and IPv6)
  - Other Essential Protocol

- Network Layer Responsibilities
- Logical Addressing
  - Class-full Addressing
  - Classless
- Routing Protocols
  - RIP
  - OSPF
- IPv4 and IPv6 Frame Format
- ICMP, ARP, RARP, DHCP Protocols
- Summary

Network Layer: Responsibilities

- Source to Destination Packet Delivery
- Logical Addressing
- Routing

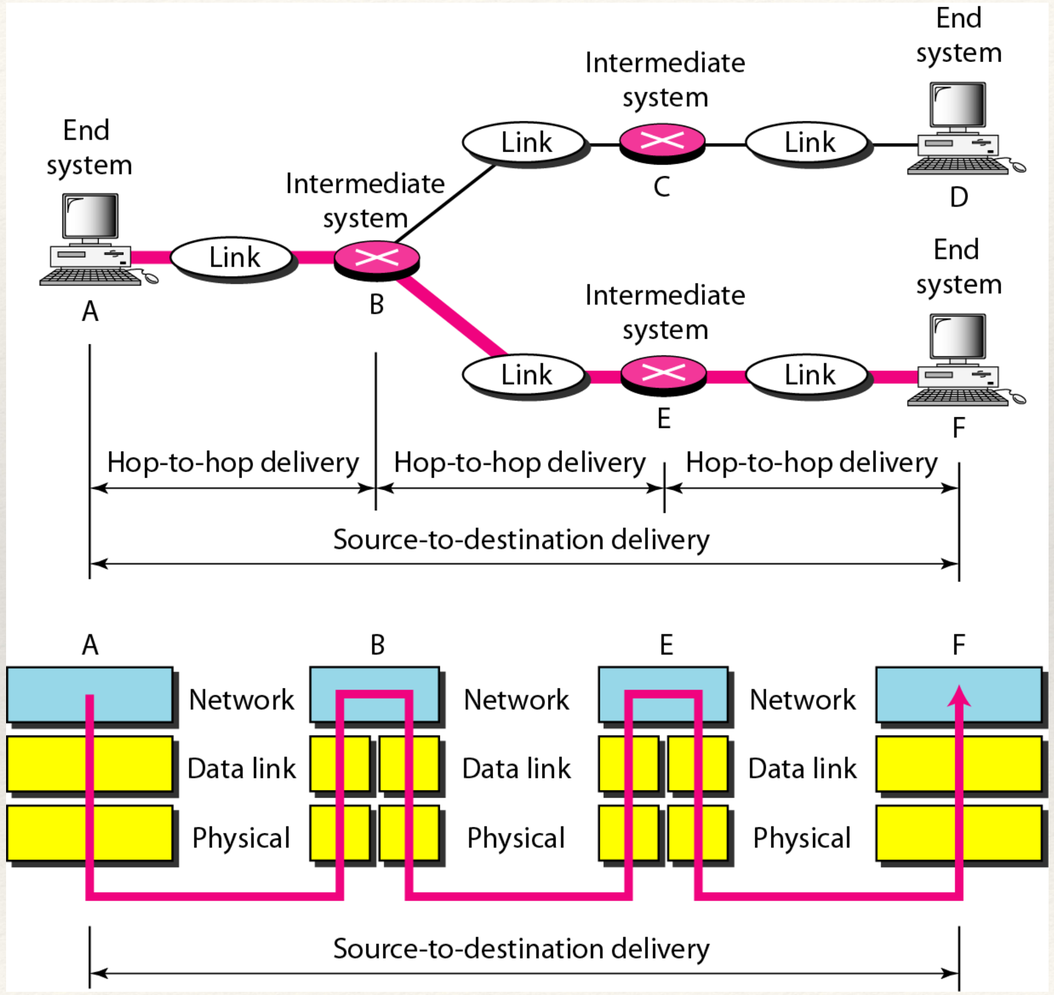


Fig 1: Source-to-destination Delivery

Logical/IP Addressing

- An IPv4 address: that uniquely and universally defines the connection of a device to the Internet.
- An IPv4 address is 32 bits (4 Bytes) long.
- The IPv4 addresses are unique and universal.
- The address space of IPv4 is 2^{32} or 4,294,967,296.
- IPv4 Address Notation: Dotted Decimal and Binary Representation.

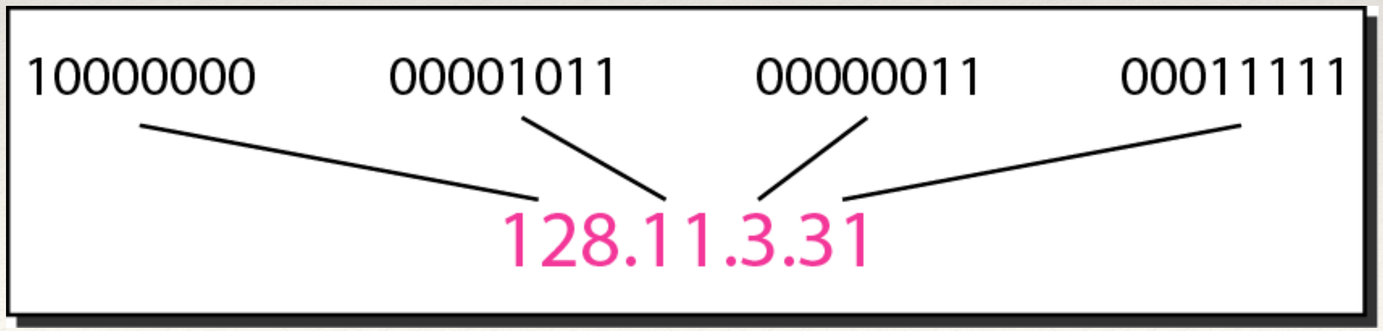


Fig. Dotted Decimal and Binary Representation

IPv4 Address

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

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number (see Appendix B) and add dots for separation.

a. 129.11.11.239

b. 193.131.27.255

IPv4 Address

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

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

Classful Addressing

- In Classful addressing, the address space is divided into five classes: A, B, C, D, and E.

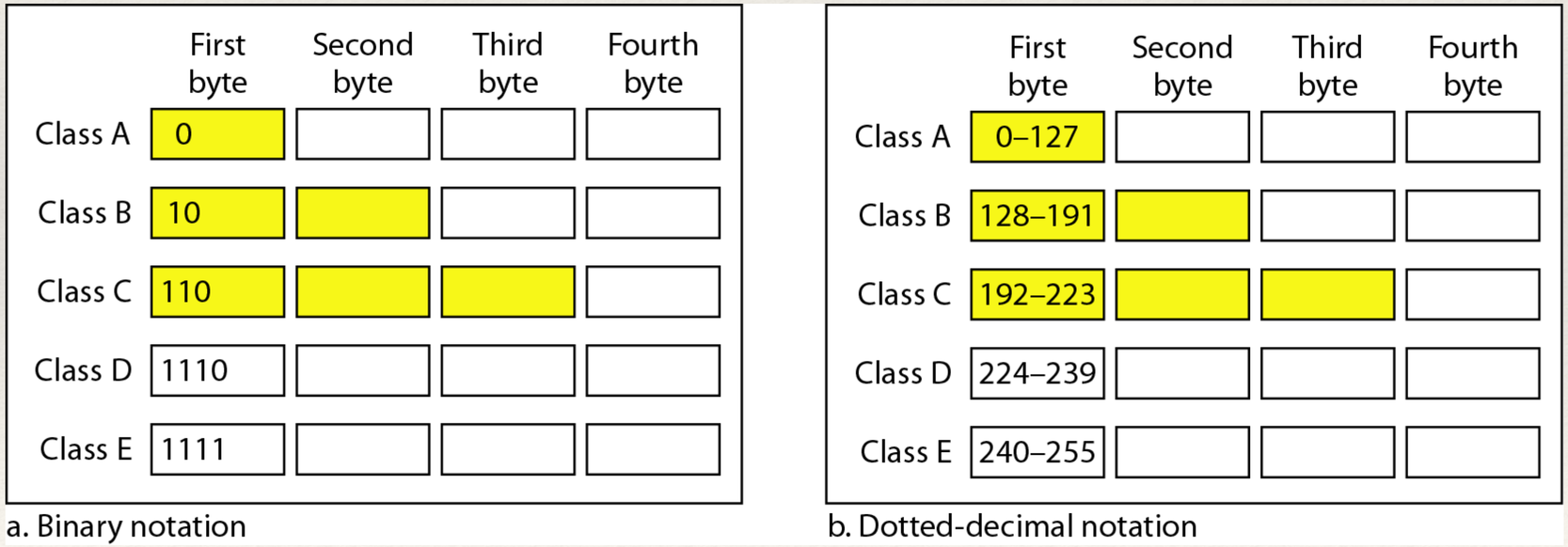


Fig. Class Identification in Binary and Decimal Notations

Problem-1

Find the class of each address.

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 14.23.120.8

d. 252.5.15.111

Solution

a. The first bit is 0. This is a class A address.

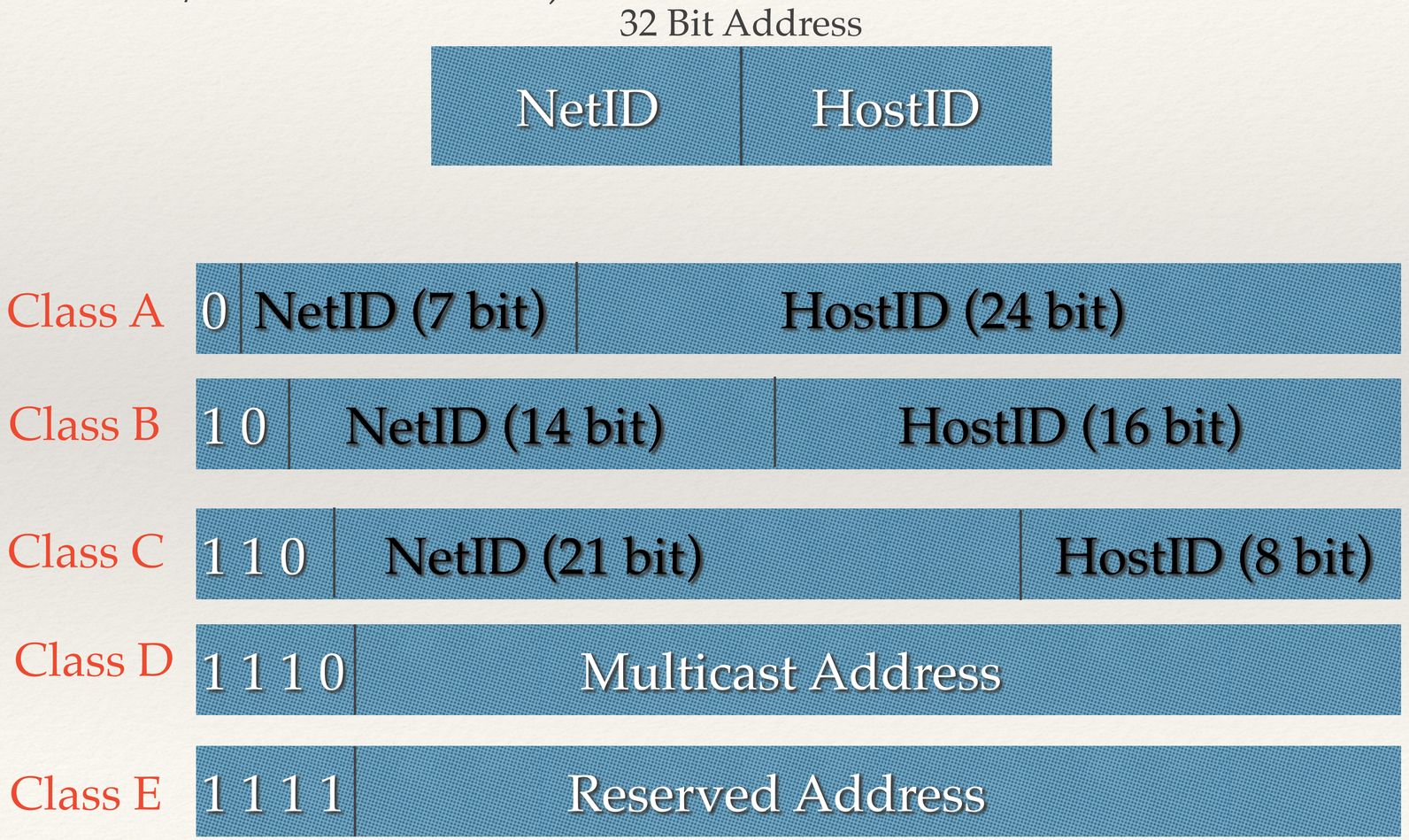
b. The first 2 bits are 1; the third bit is 0. This is a class C address.

c. The first byte is 14; the class is A.

d. The first byte is 252; the class is E.

IPv4 Address

- One Problem with the Classful Addressing is each class divided into NetID (Block) and HostID (Size of the Block/Number of Host).



IPv4 Address

- In c1assful addressing, a large part of the available addresses were wasted.
- Classful addressing, which is almost obsolete, is replaced with classless addressing.
- To overcome address depletion and give more organizations access to the Internet, classless addressing was designed.

Class	*Number of Blocks*	*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

Fig. Number of Blocks and each Block Size

Masking

- Mask is contiguous 1s and 0s which help to identify the NetID and the HostID
- Default masking for the Classful Address is given in the Table.
- The last column shows CIDR (Classless Interdomain Routing) notation which is used in classless addressing/Classless notations where the mask is represented using the slash (/).
- Classful addressing is almost obsolete, it is replaced with the classless 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

Fig: Masks for the Glassful IP Addresses

Classless Addressing

- In Classless addressing the block of addresses are granted
- The size of the block varies depending in the nature and size of the entity.
- Restrictions: To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:
    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 (1, 2, 4, 8, ...).
    3. The first address must be evenly divisible by the number of addresses.

Classless Addressing

- Address are contagious 32-47 (Total 16)
- 16 is power of 2
- The first address is divisible by 16

The first address in a block is normally not assigned to any device; it is used as the network address that represents the organization to the rest of the world.

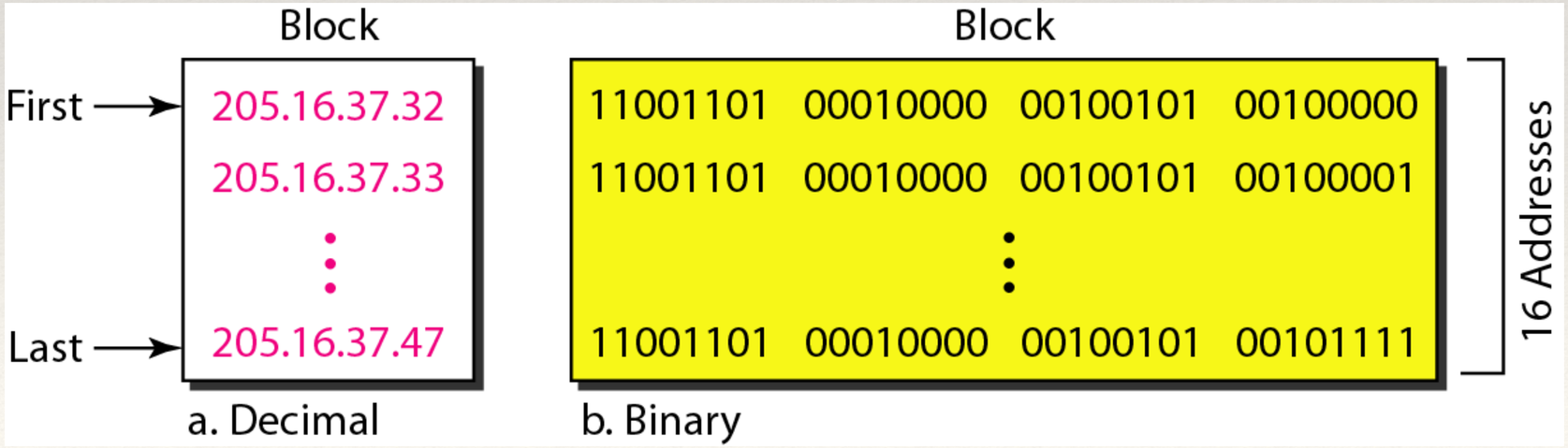


Fig. Block of 16 Addresses

Classless Addressing

- 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 1s and the 32 - n rightmost bits are 0s .
  - In 1Pv4 addressing, a block of addresses can be defined as x.y.z.t/n in which ”x.y.z.t” defines one of the addresses and the “/n” defines the mask.
- 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 0s.
- Last Address: The last address in the block can be found by setting the ”32 - n rightmost” bits in the binary notation of the ”address to 1s”.
- Number of Address: The number of addresses in the block is the difference between the last and first address.
  - The number of addresses in the block can be found by using the formula ”2^{32-n}” .

Classless Addressing

Q1. A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.39/28 then, What is the first address, last address and the number of addresses for the given block.

Two-level Hierarchy

- Each address in the block can be considered as a two-level hierarchical structure:
  - The leftmost n bits (prefix) define the network;
  - The rightmost 32 – n bits define the host.

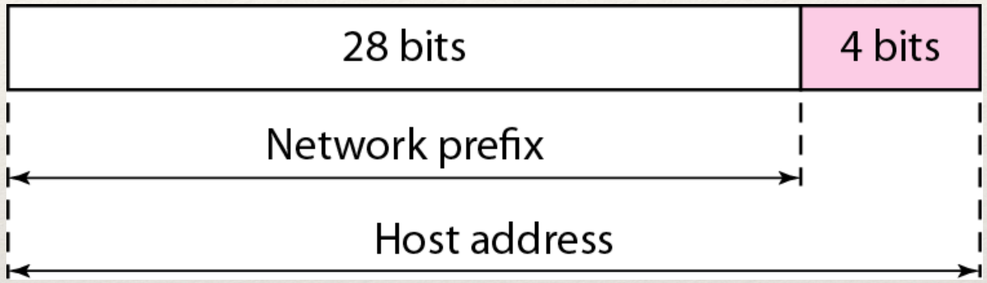


Fig. A frame in a Character Oriented Protocol

Three Level Hierarchy: Subnetting

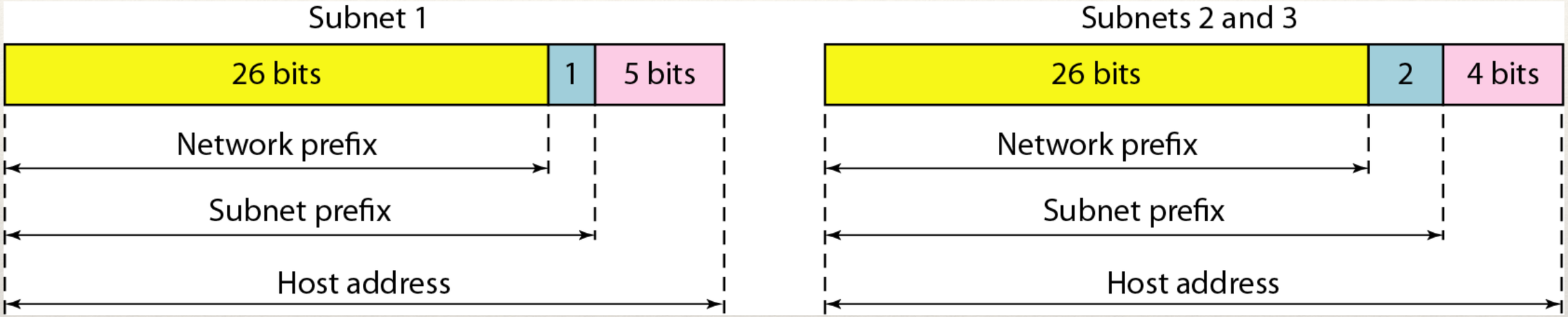


Fig. Three-level Hierarchy Subnetting

Example -1

Suppose an organization is given the block 17.12.14.0/26, which contains 64 addresses.

The organization has three offices and needs to divide the addresses into three sub blocks of 32, 16, and 16 addresses.

The new masks for each subnets can be determined as follows:

1. Suppose the mask for the first subnet is n1, then 2^{32-n1} must be 32, which means that n1=27.

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

3. Suppose the mask for the third subnet is n3, then 2^{32-n3} must be 16, which means that n3=28.

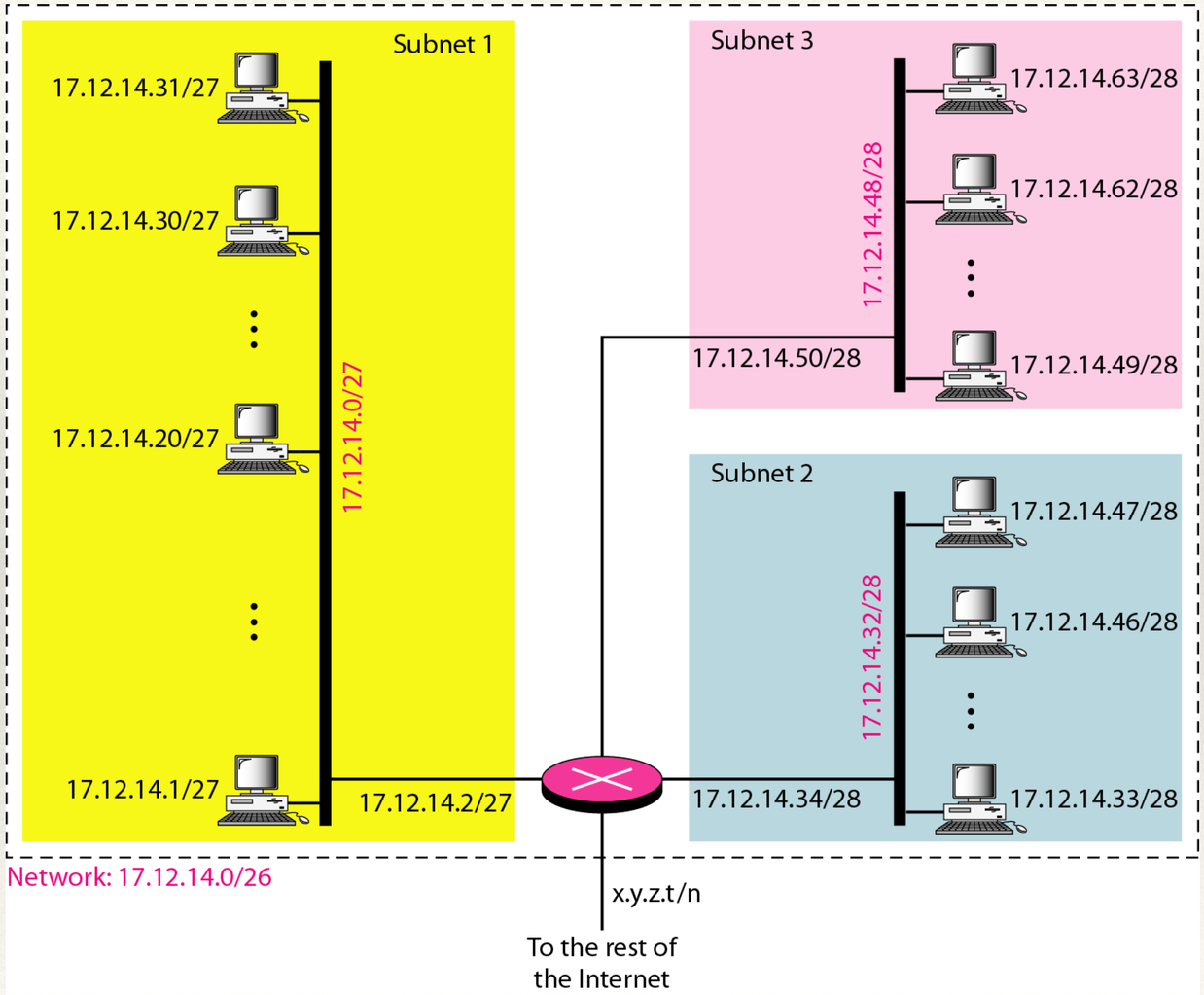


Fig. Example

Address Allocation: Example

An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536 addresses). The ISP needs to distribute these addresses to three groups of customers as follows:

a. The first group has 64 customers; each needs 256 addresses.

b. The second group has 128 customers; each needs 128 addresses.

c. The third group has 128 customers; each needs 64 addresses.

Design the sub-blocks and find out how many addresses are still available after these allocations.

Address Allocation: Example

Group 1:

For this group, each customer needs 256 addresses. This means that 8 ($\log_2 256$) bits are needed to define each host. The prefix length is then $32 - 8 = 24$. The addresses are,

1st Customer:	*190.100.0.0/24*	*190.100.0.255/24*
2nd Customer:	*190.100.1.0/24*	*190.100.1.255/24*
64th Customer:	*190.100.63.0/24*	*190.100.63.255/24*
Total = 64 x 256 = 16,384		

Group 2: For this group, each customer needs 128 addresses. This means that 7 ($\log_2 128$) bits are needed to define each host. The prefix length is then $32 - 7 = 25$. The addresses are,

1st Customer:	*190.100.64.0/25*	*190.100.64.127/25*
2nd Customer:	*190.100.64.128/25*	*190.100.64.255/25*
. . .		
128th Customer:	*190.100.127.128/25*	*190.100.127.255/25*
Total = 128 × 128 = 16,384		

Address Allocation: Example

Group 3: For this group, each customer needs 64 addresses. This means that 6 ($\log_2 64$) bits are needed to each host. The prefix length is then $32 - 6 = 26$. The addresses are

1st Customer:	*190.100.128.0/26*	*190.100.128.63/26*
2nd Customer:	*190.100.128.64/26*	*190.100.128.127/26*
. . .		
128th Customer:	*190.100.159.192/26*	*190.100.159.255/26*

Total $= 128 \times 64 = 8192$

Number of granted addresses to the ISP: 65,536

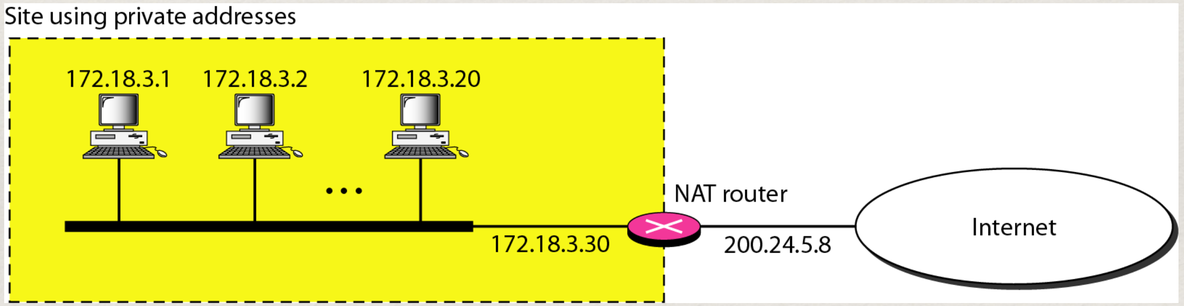
Number of allocated addresses by the ISP: 40,960

Number of available addresses: 24,576

NAT

- Network Address Translation (NAT): It's a way to map multiple private addresses inside a local network to a public IP address before transferring the information onto the internet.
- NAT enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally.

10.0.0.0 to 10.255.255.255
172.16.0.0 to 172.31.255.255
192.168.0.0 to 192.168.255.255



Address Translation

Address Translation:

All the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address.

All incoming packets also pass through the NAT router, which replaces the destination address in the packet (the NAT router global address) with the appropriate private address.

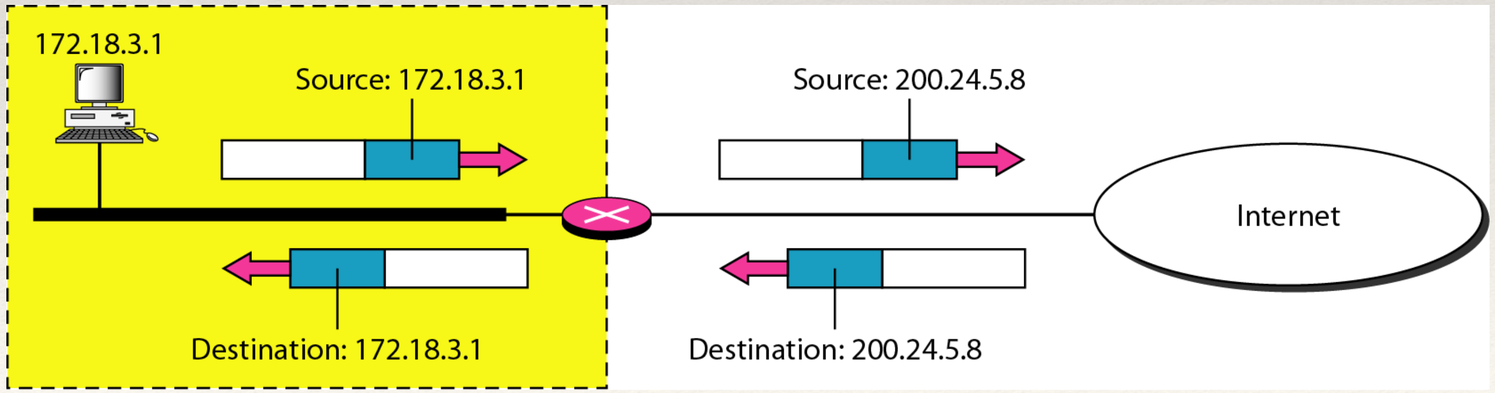


Fig: Address Translation

Address Translation

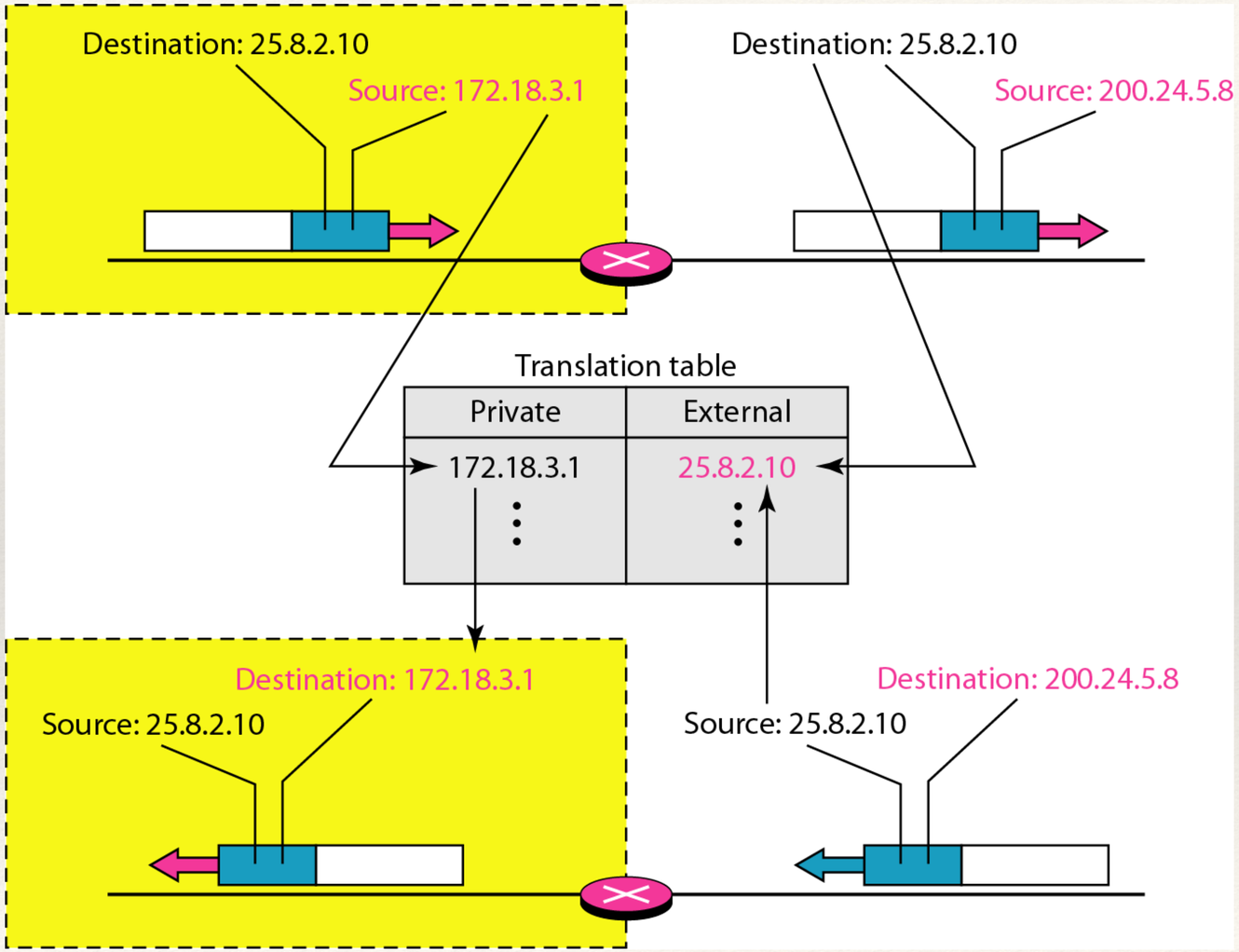


Fig: Translation Table

IPv6 Addresses

- Despite all short-term solutions, address depletion is still a long-term problem for the Internet. This and other problems in the IP protocol itself have been the motivation for IPv6.
- An IPv6 address is 128 bits long.

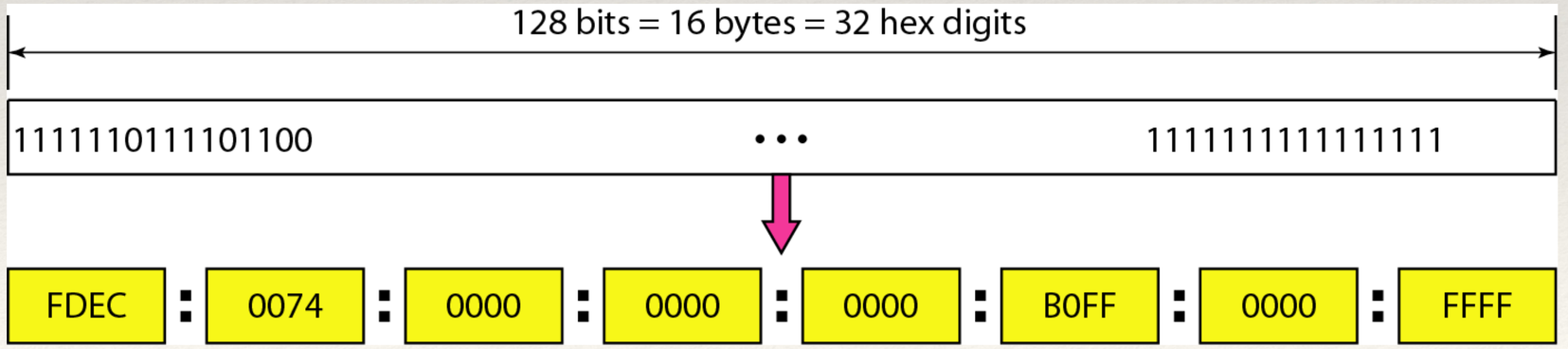


Fig: IPv6 Address Format

IPv6 Addresses

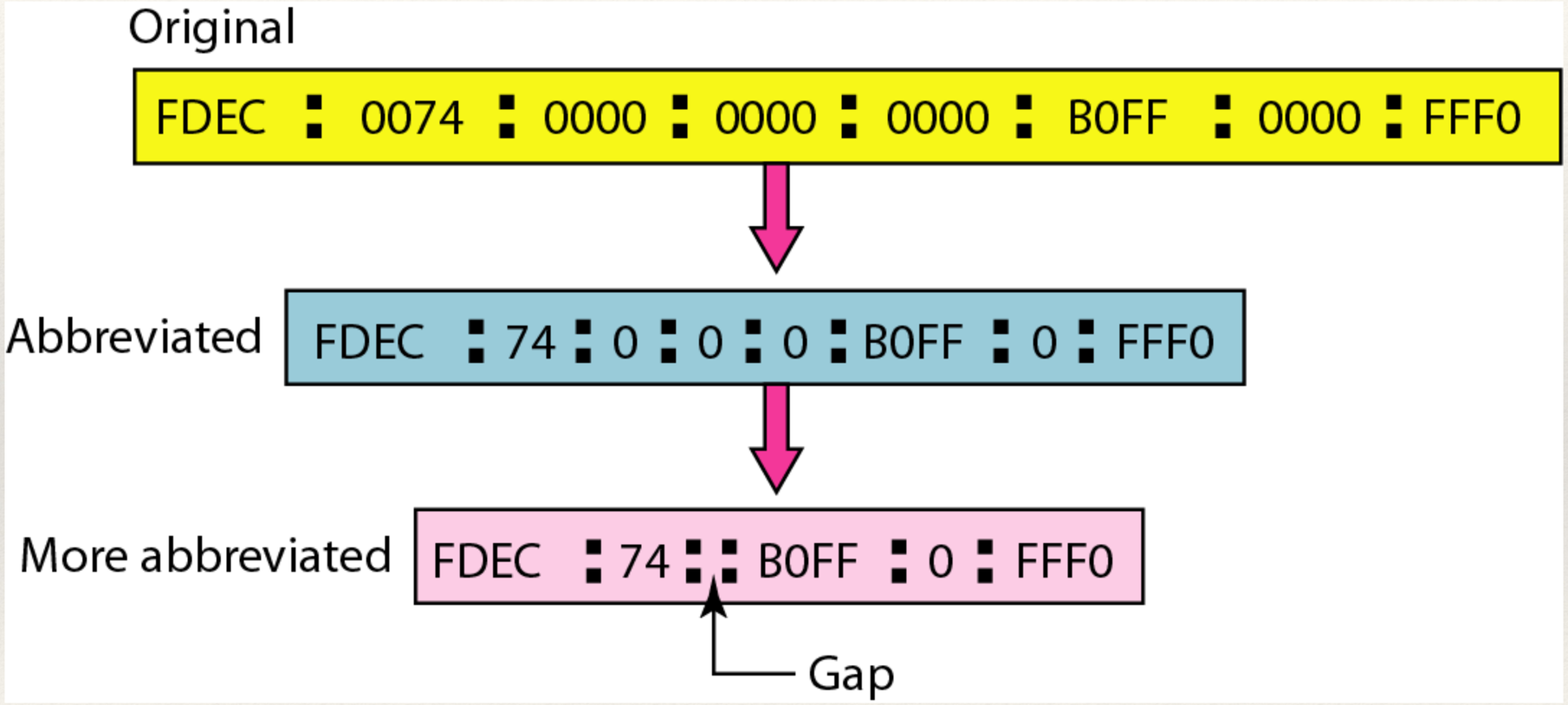


Fig: Abbreviated IPv6 Address Representation

Example

Q1. Expand the address 0:15::1:12:1213 to its original.

Solution:

We first need to align the left side of the double colon to the left of the original pattern and the right side of the double colon to the right of the original pattern to find how many 0s we need to replace the double colon.

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
 0:   15:                    :    1:   12:1213
```

This means that the original address is.

```
0000:0015:0000:0000:0000:0001:0012:1213
```

IPv4 vs IPv6

IPv4 Address	IPv6 Address
Address Length – 32 bits	128 bits
Address Representation - decimal	hexadecimal
Internet address classes	Not applicable in IPv6
Multicast addresses (224.0.0.0/4)	IPv6 multicast addresses (FF00::/8)
Broadcast addresses	Not applicable in IPv6
Unspecified address is 0.0.0.0	Unspecified address is ::
Loopback address is 127.0.0.1	Loopback address is ::1
Public IP addresses	Global unicast addresses
Private IP addresses (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16)	Site-local addresses (FEC0::/10)
Autoconfigured addresses (169.254.0.0/16)	Link-local addresses (FE80::/64)

IPv4 Header Format

- IPv4 header contains 12 fields.
- Each field of the IPv4 header has a specific use.

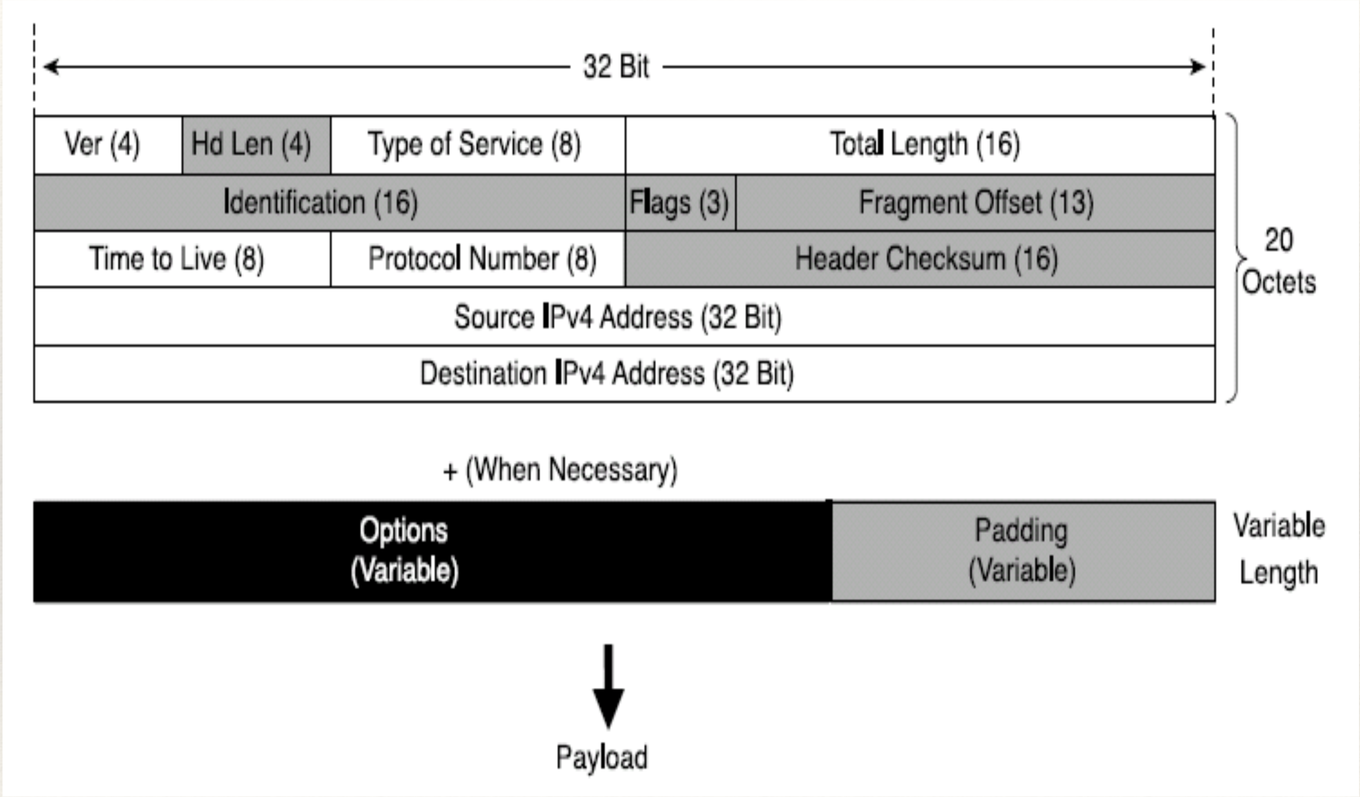


Fig: IPv4 Header Format

IPv4 Header Fields

- Version (4 bits)
  - Indicates the version of IP and is set to 4.
- Internet Header Length (4 bits)
  - Indicates the number of 4-byte blocks in the IPv4 header.
  - Because an IPv4 header is a minimum of 20 bytes in size, the smallest value of the Internet Header Length (IHL) field is 5.
- Type of Service (4 bits)
  - Indicates the desired service expected by this packet for delivery through routers across the IPv4 internetwork.
- Total Length (16 bits)
  - Indicates the total length of the IPv4 packet (IPv4 header + IPv4 payload) and does not include link layer framing.

IPv4 Header Fields

- Identification (16 bits)
  - Identifies this specific IPv4 packet.
  - The Identification field is selected by the originating source of the IPv4 packet. If the IPv4 packet is fragmented, all of the fragments retain the Identification field value so that the destination node can group the fragments for reassembly.
- Flags (3 bits)
  - Identifies flags for the fragmentation process.
  - There are two flags—one to indicate whether the IPv4 packet might be fragmented and another to indicate whether more fragments follow the current fragment.
- Fragment Offset (13 bits)
  - Indicates the position of the fragment relative to the original IPv4 payload.

IPv4 Header Fields

- Time to Live (8 bits)
  - Indicate the maximum number of links on which an IPv4 packet can travel before being discarded.
  - Originally used as a time count with which an IPv4 router determined the length of time required (in seconds) to forward the IPv4 packet, decrementing the TTL accordingly. When the TTL equals 0,an ICMP Time Expired-TTL Expired in Transit message is sent to the source IPv4 address and the packet is discarded.
- Protocol (8 bits)
  - Identifies the upper layer protocol.
  - For example, TCP uses a Protocol of 6, UDP uses a Protocol of 17, and ICMP uses a Protocol of 1.
  - The Protocol field is used to demultiplex an IPv4 packet to the upper layer protocol.

IPv4 Header Fields

- Header Checksum (16 Bits)
  - Provides a checksum on the IPv4 header only.
  - The IPv4 payload is not included in the checksum calculation as the IPv4 payload and usually contains its own checksum..
- Source Address (32 bits)
  - Stores the IPv4 address of the originating host.
- Destination Address (32 bits)
  - Stores the IPv4 address of the destination host.
- Options (multiple of 32 bits)
  - Stores one or more IPv4 options.

IPv4 vs IPv6

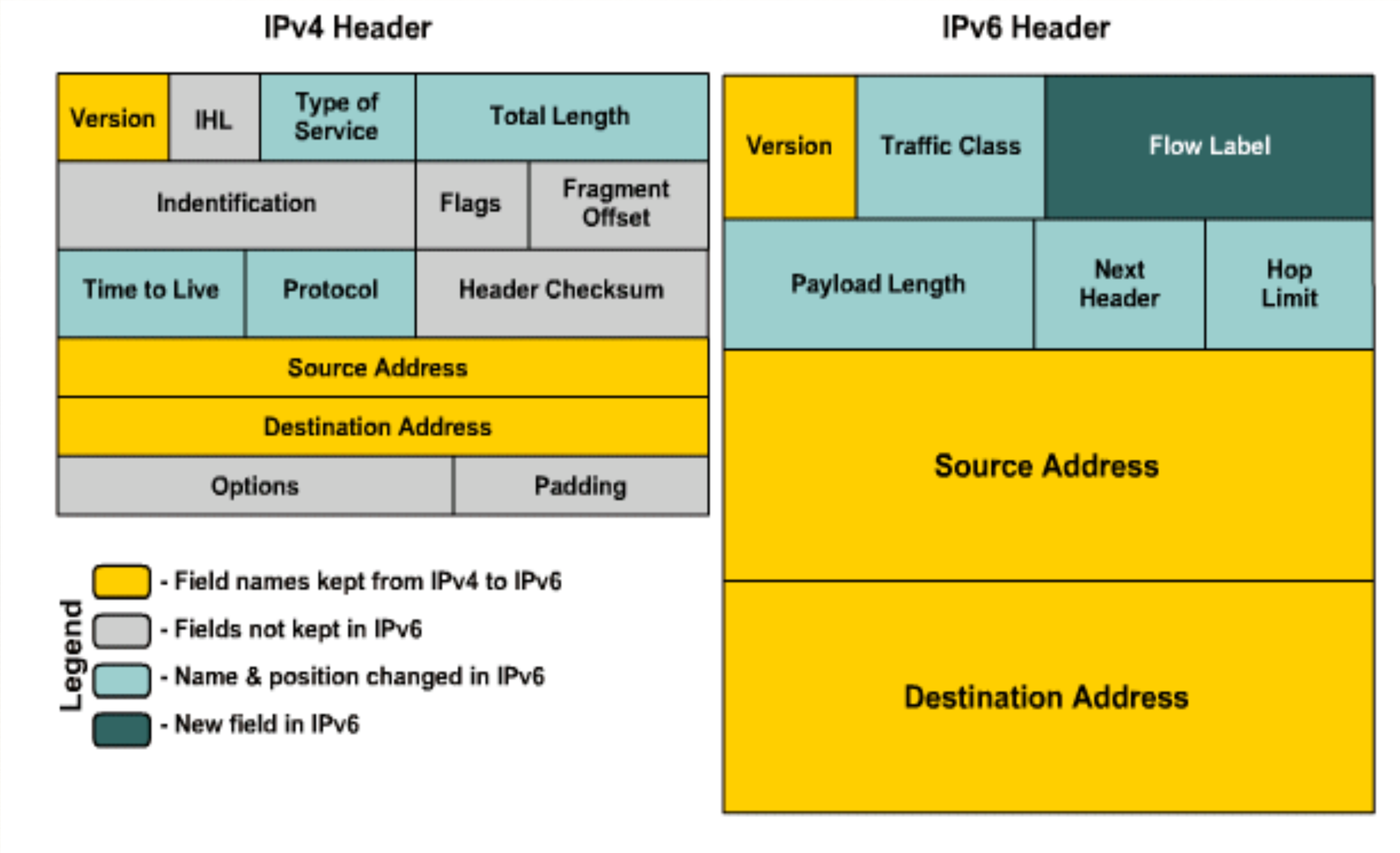


Fig: IPv4 vs IPv6 Header Format

IPv6 Header Fields

- Based on these rules, RFC 2460 defines the following IPv6 header fields:
  - Version (4 bits)
    - 4 bits are used to indicate the version of IP and is set to 6
  - Traffic Class (8 bits)
    - same function as the Type of Service field in the IPv4 header.
  - Flow Label (20 bits)
    - identifies a flow and it is intended to enable the router to identify packets that should be treated in a similar way without the need for deep lookups within those packets.
    - set by the source and should not be changed by routers along the path to destination.

IPv6 Header Fields

- Payload Length (16 bits)
  - With the header length fixed at 40 bytes, it is enough to indicate the length of the payload to determine the length of the entire packet.
- Next Header (8 bits)
  - Indicates either the first extension header (if present) or the protocol in the upper layer PDU (such as TCP, UDP, or ICMPv6).
- Hop Limit (8 bits)
  - In IPv6, the IPv4 TTL was appropriately renamed Hop Limit because it is a variable that is decremented at each hop, and it does not have a temporal dimension.

Transition Strategies

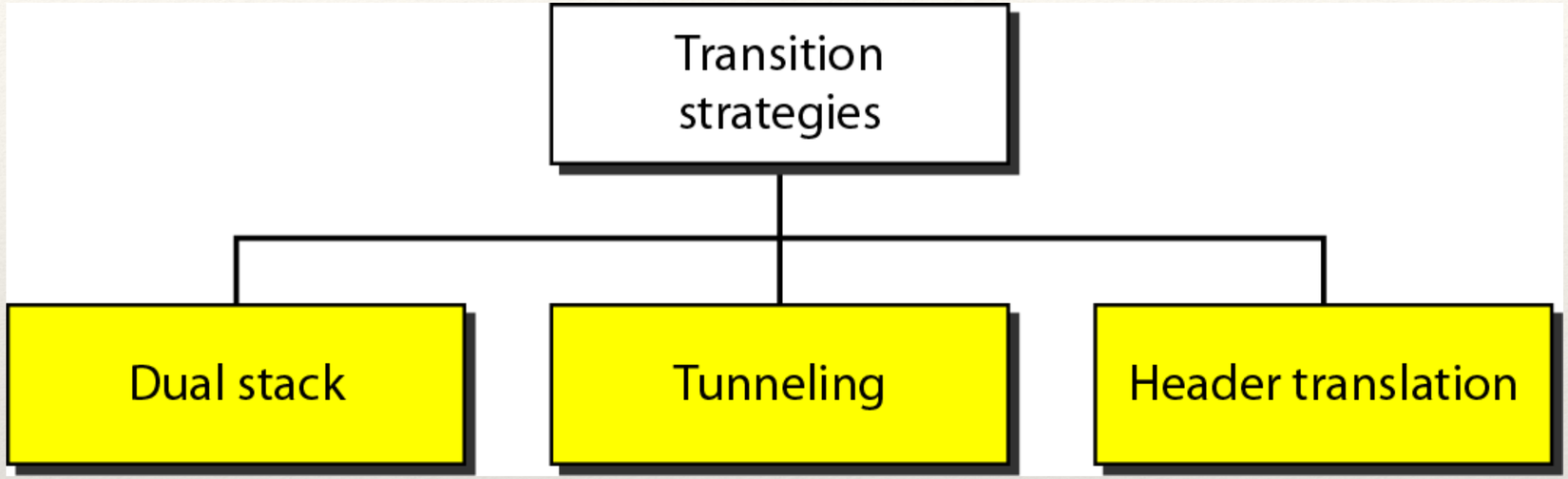


Fig: Transition Strategies

- It takes a considerable amount of time before every system in the Internet can move from IPv4 to IPv6.
- The transition must be smooth to prevent any problems between IPv4 and IPv6 systems

Transition Strategies

- Host uses DNS query result to determine which IP to use.

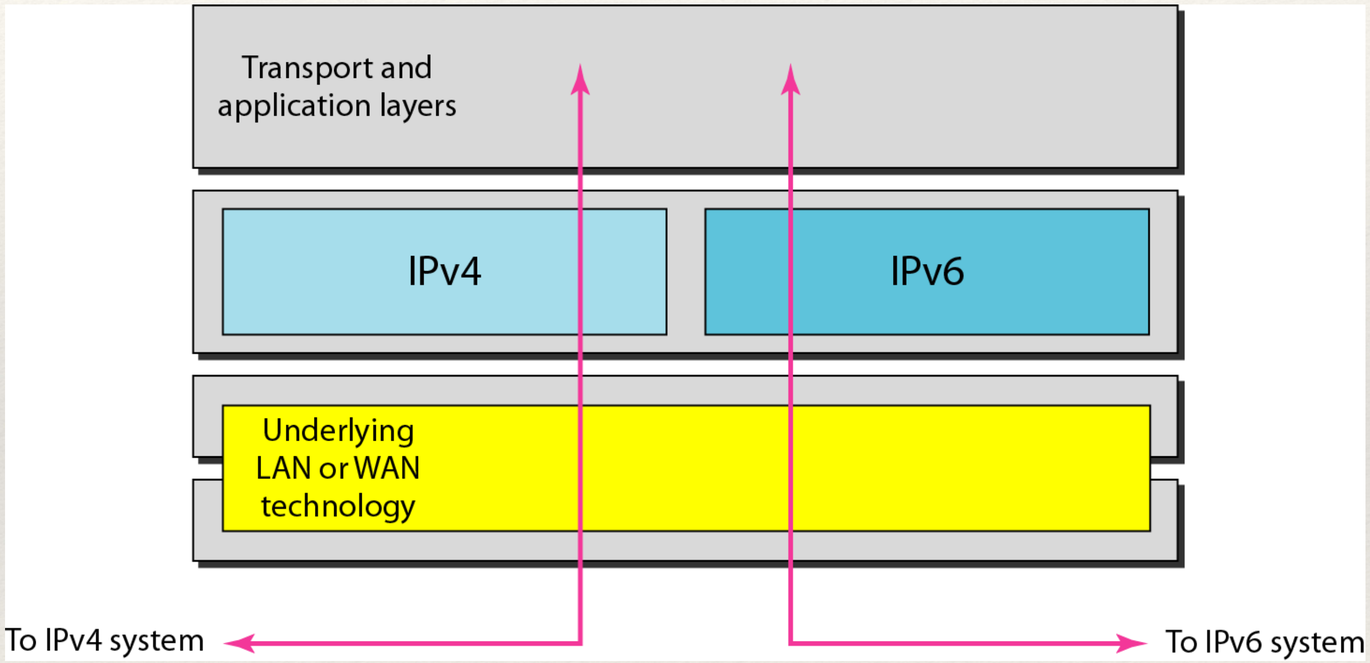


Fig: Dual Stack

Transition Strategies

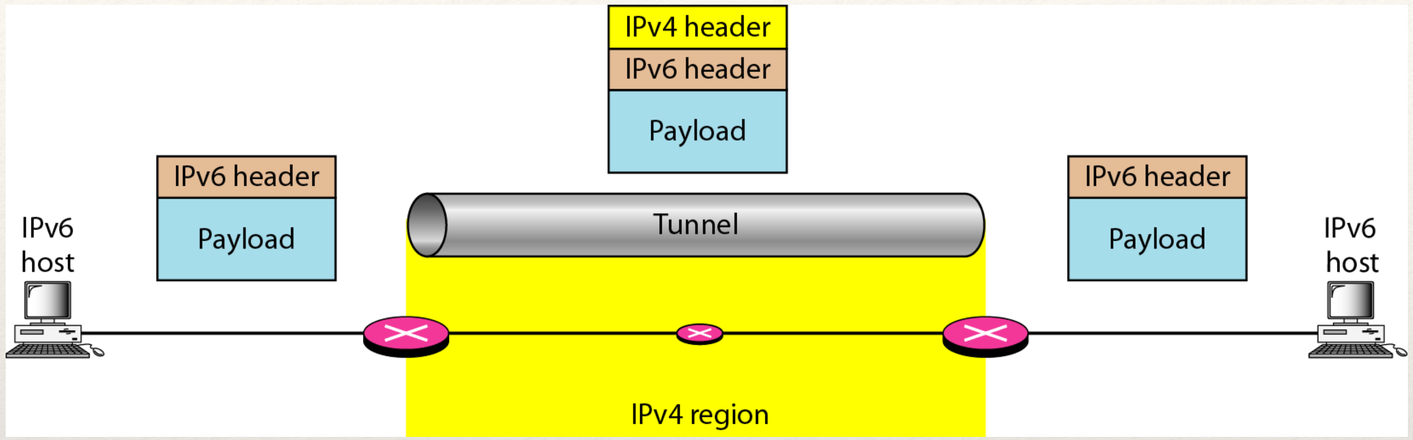


Fig: Tunneling

- Tunnelling 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.
- To pass through this region, the packet must have an IPv4 address.
- So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region.

Transition Strategies

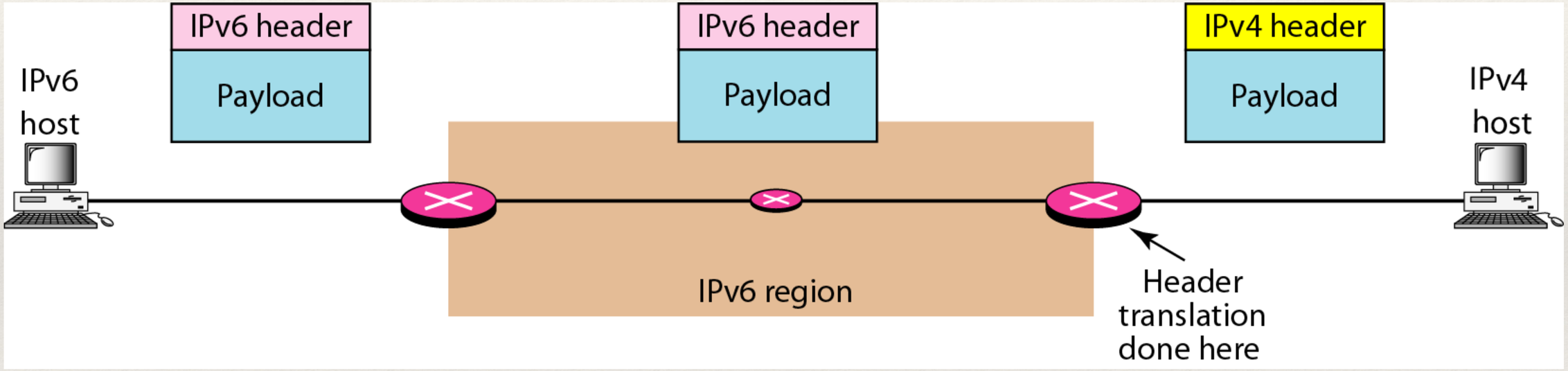


Fig: Header Transition

Header Translation

Header Translation Procedure
1. The IPv6 mapped address is changed to an IPv4 address by extracting the rightmost 32 bits.
2. The value of the IPv6 priority field is discarded.
3. The type of service field in IPv4 is set to zero.
4. The checksum for IPv4 is calculated and inserted in the corresponding field.
5. The IPv6 flow label is ignored.
6. Compatible extension headers are converted to options and inserted in the IPv4 header. Some may have to be dropped.
7. The length of IPv4 header is calculated and inserted into the corresponding field.
8. The total length of the IPv4 packet is calculated and inserted in the corresponding field.

Protocols

- Address Mapping
  - The delivery of a packet to a host or a router requires two levels of addressing: logical and physical.
  - We need to be able to map a logical address to its corresponding physical address and vice versa. This can be done by using either static or dynamic mapping
- ARP: Map Logical to Physical address
- ARP can be useful if the ARP reply is cached (kept in cache memory for a while).

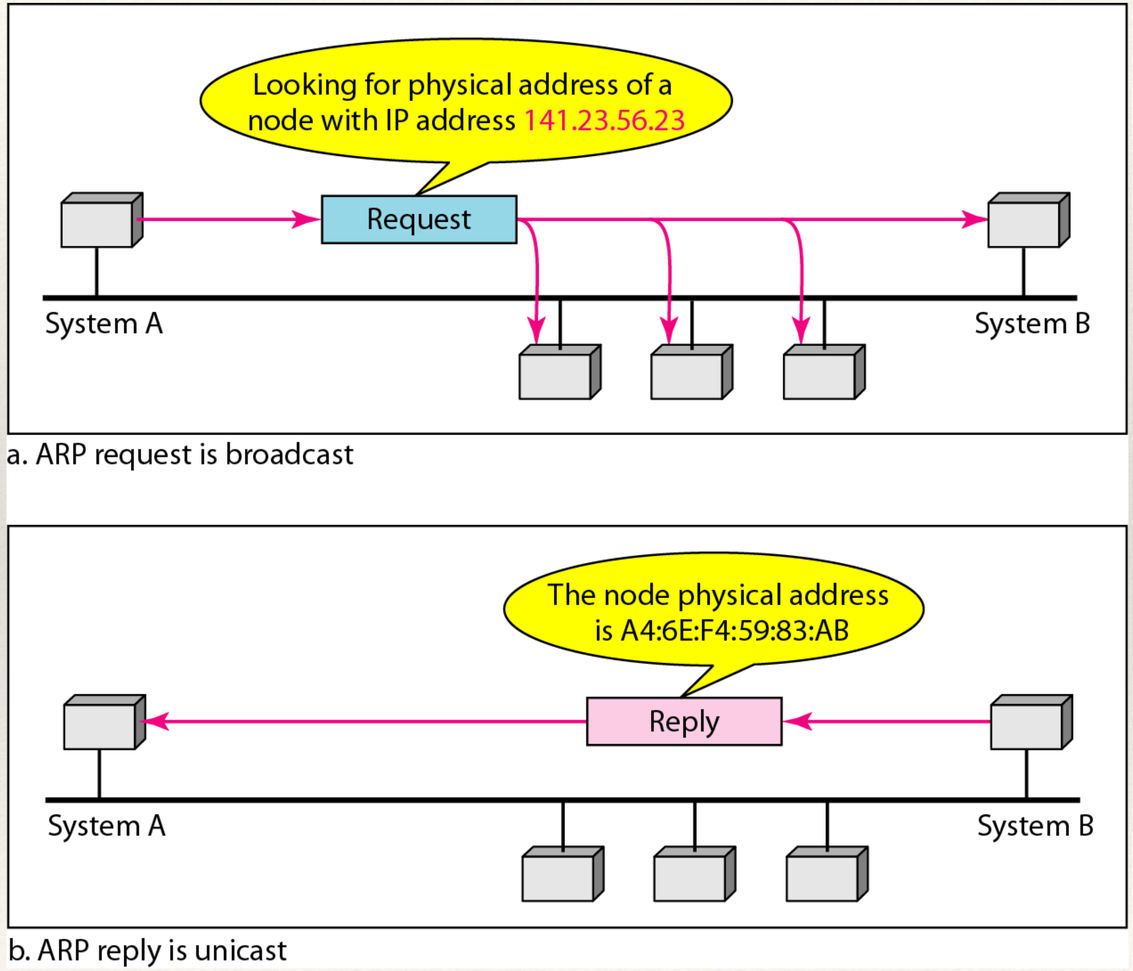


Fig: ARP Request and Response

ARP-Packet Format

- Hardware type. This is a 16-bit field defining the type of the network on which ARP is running. Each LAN has been assigned an integer based on its type. For example, Ethernet is given type 1. ARP can be used on any physical network.
- Protocol type. This is a 16-bit field defining the protocol. For example, the value of this field for the IPv4 protocol is 0800_{16}, ARP can be used with any higher-level protocol.
- Hardware length. This is an 8-bit field defining the length of the physical address in bytes. For example, for Ethernet the value is 6.
- Protocol length. This is an 8-bit field defining the length of the logical address in bytes. For example, for the IPv4 protocol the value is 4.
- Operation. This is a 16-bit field defining the type of packet. Two packet types are defined: ARP request (1) andARP reply (2).
- Sender hardware address. This is a variable-length field defining the physical address of the sender. For example, for Ethernet this field is 6 bytes long.
- Sender protocol address. This is a variable-length field defining the logical (for example, IP) address of the sender. For the IP protocol, this field is 4 bytes long.
- Target hardware address. This is a variable-length field defining the physical address of the target. For example, for Ethernet this field is 6 bytes long. For an ARP request message, this field is allOs because the sender does not know the physical address of the target.
- Target protocol address. This is a variable-length field defining the logical (for example, IP) address of the target. For the IPv4 protocol, this field is 4 bytes long.

ARP Frame Fields

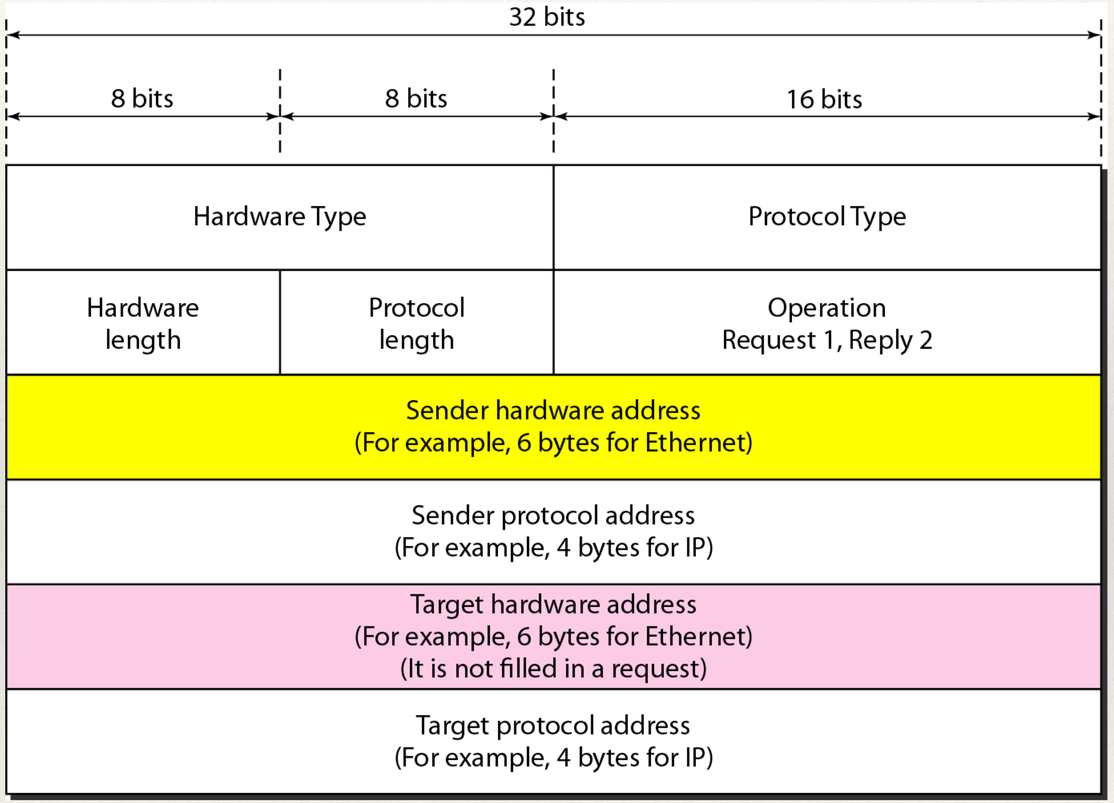


Fig: ARP Frame

Encapsulation

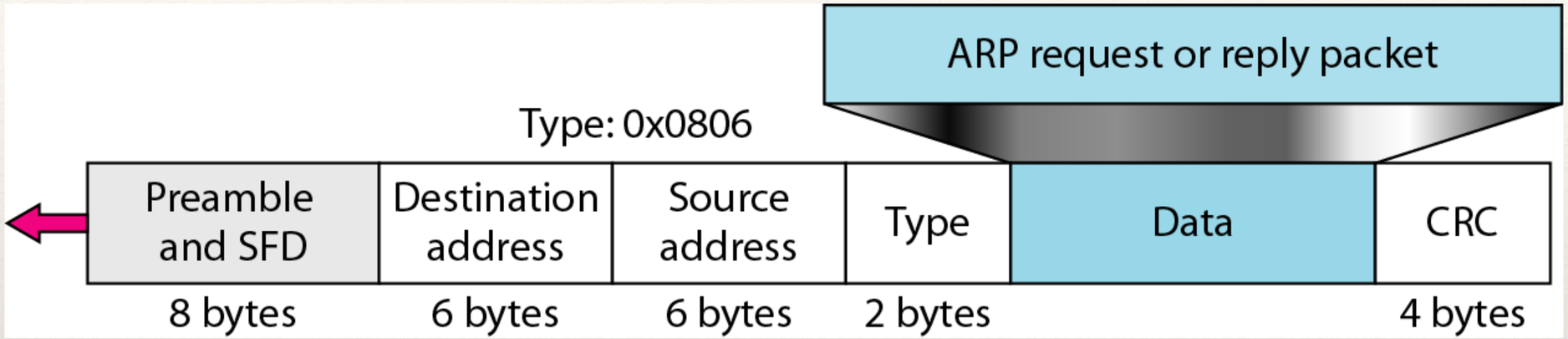
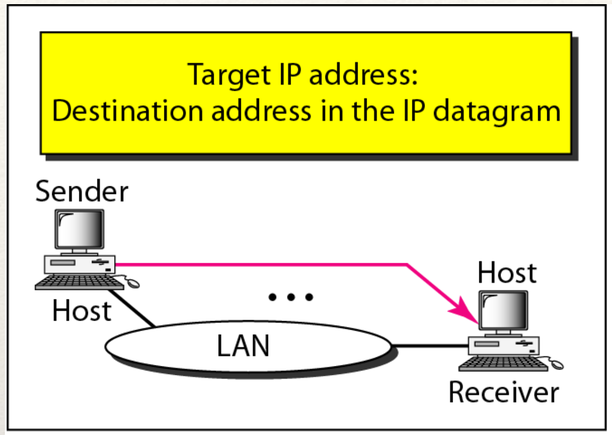
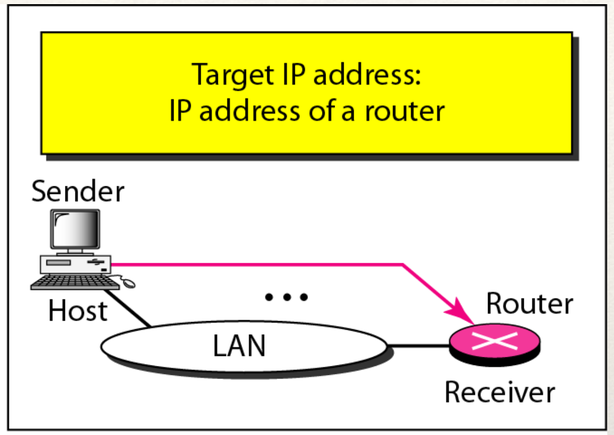


Fig. ARP Encapsulation with Datalink Frame

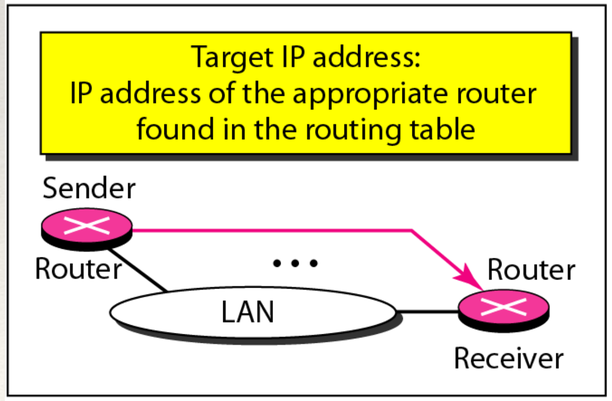
Four Cases of Using ARP



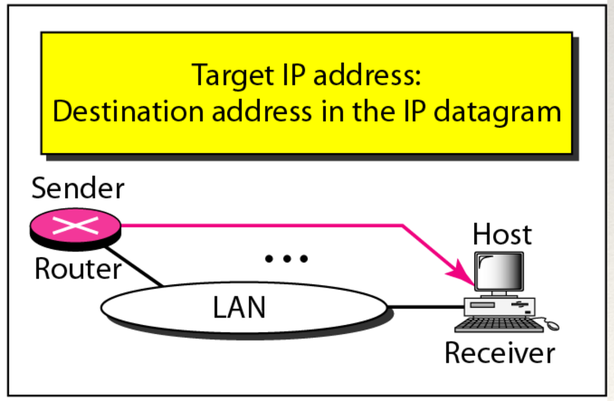
Case 1. A host has a packet to send to another host on the same network.



Case 2. A host wants to send a packet to another host on another network. It must first be delivered to a router.



Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.



Case 4. A router receives a packet to be sent to a host on the same network.

RARP, DHCP

Reverse Address Resolution Protocol

- A machine can use the physical address to get the logical address using RARP.
- A RARP messages is created and broadcast on the local network.
- The machine on the local network that knows the logical address will respond with a RARP reply.
- Broadcasting is done at data link layer.
- Broadcast requests does not pass the boundaries of a network.

Dynamic Host Configuration Protocol (DHCP)

Goal: allow host to dynamically obtain its IP address from network server when it joins network

Can renew its lease on address in use

Allows reuse of addresses (only hold address while connected an "on"

Support for mobile users who want to join network (more shortly)

DHCP overview:

- host broadcasts "DHCP discover" msg
- DHCP server responds with "DHCP offer" msg
- host requests IP address: "DHCP request" msg
- DHCP server sends address: "DHCP ack" msg

ICMP

- The IP protocol has no error-reporting or error-correcting mechanism. The IP protocol also lacks a mechanism for host and management queries.
- The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies.
- It is a companion to the IP protocol.

ICMP always reports error messages to the original source.

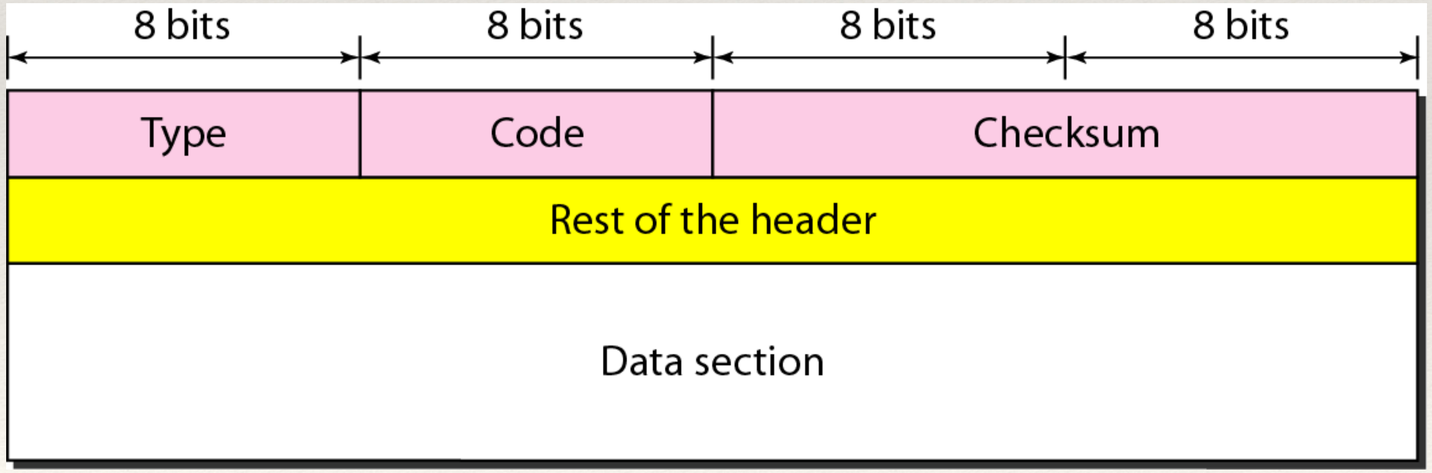


Fig: ICMP Message Format

ICMP Error Reporting Messages

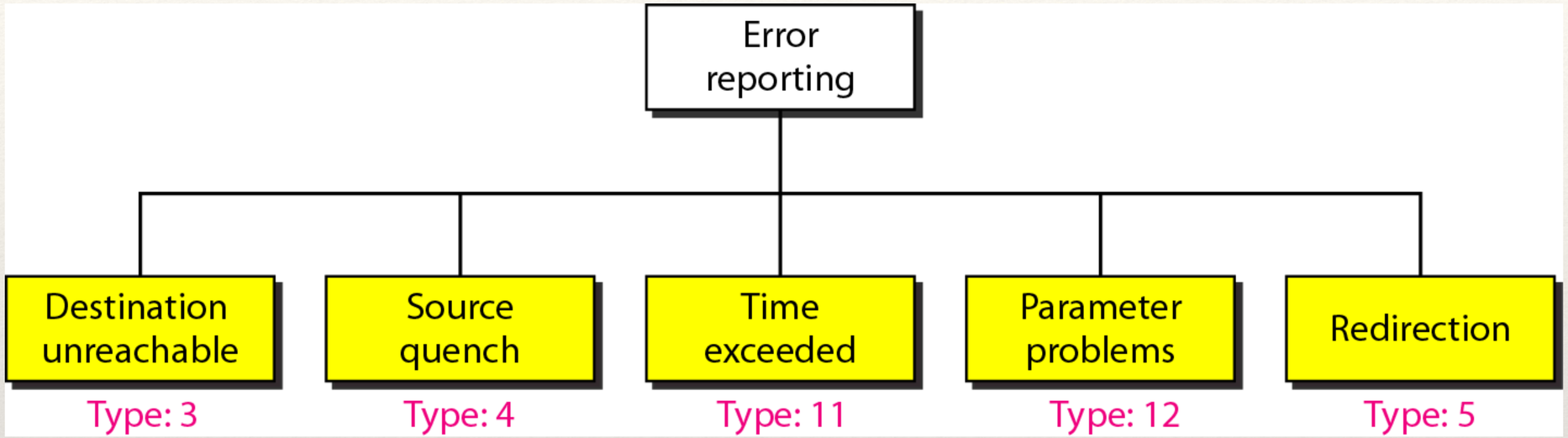


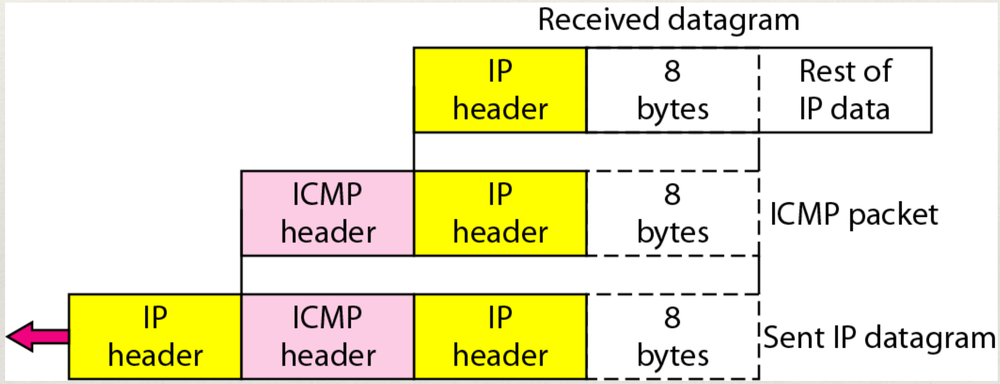
Fig: Error Reporting Messages

Important points about ICMP error messages:

- No ICMP error message will be generated in response to a datagram carrying an ICMP error message.
- No ICMP error message will be generated for a fragmented datagram that is not the first fragment.
- No ICMP error message will be generated for a datagram having a multicast address.
- No ICMP error message will be generated for datagram having a special address such as 127.0.0.0 or 0.0.0.0.

Contents of Data Field for the Error Messages

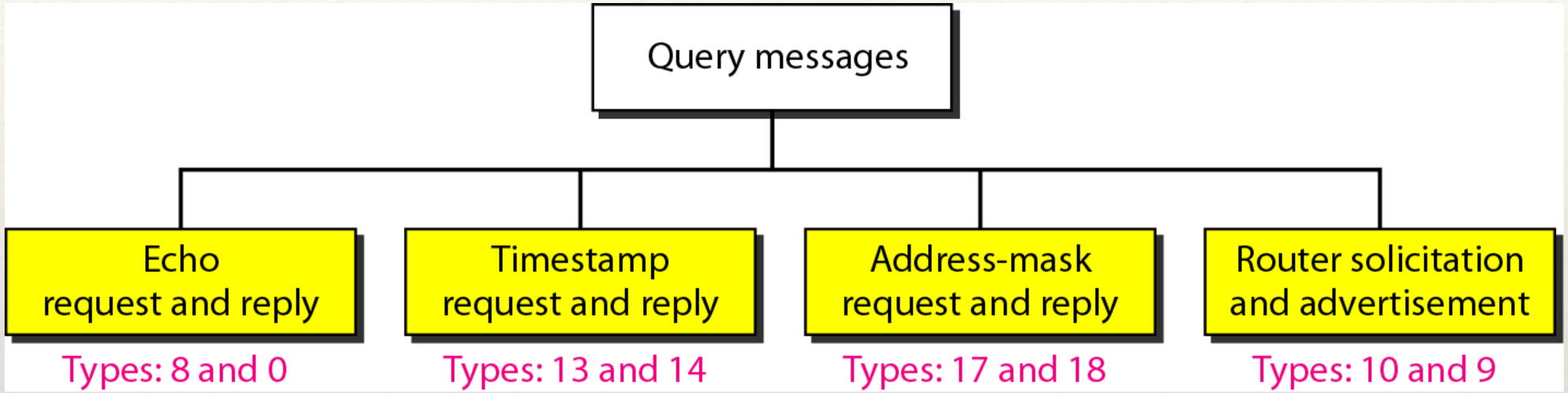
- Destination Unreachable: When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or the host sends a destination-unreachable message back to the source host that initiated the datagram.
- Source Quench: The source-quench message in ICMP was designed to add a kind of flow control to the IP.
- When a router or host discards a datagram due to congestion, it sends a source-quench message to the sender of the datagram.
- This message has two purposes.
  - First, it informs the source that the datagram has been discarded.
  - Second, it warns the source that there is congestion somewhere in the path and that the source should slow down (quench) the sending process.



ICMP Messages

- Time Exceeded: It is generated in two cases:
  - If there are errors in one or more routing tables, a packet can travel in a loop or a cycle, going from one router to the next or visiting a series of routers endlessly. When the time-to-live value reaches 0, after decrementing, the router discards the datagram.
  - A time-exceeded message is also generated when not all fragments that make up a message arrive at the destination host within a certain time limit
- Parameter Problem: If a router or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards the datagram and sends a parameter-problem message back to the source
- Redirection:

ICMP Query Messages



Echo Request and Reply:

- The echo-request and echo-reply messages are designed for diagnostic purposes.
- The echo-request and echo-reply messages can be used to determine if there is communication at the IP level.
- The combination of echo-request and echo-reply messages detennines whether two systems (hosts or routers) can communicate with each other.

ICMP Query Messages

Timestamp Request and Reply:

- Two machines (hosts or routers) can use the timestamp request and timestamp reply messages to determine the round-trip time needed for an IP datagram to travel between them.
- It can also be used to synchronize the clocks in two machines.

Address Mask Request and Reply:

- To obtain its mask, a host sends an address-mask-request message to a router on the LAN.
- If the host knows the address of the router, it sends the request directly to the router. If it does not know, it broadcasts the message.
- The router receiving the address-mask-request message responds with an address-mask-reply message, providing the necessary mask for the host.

ICMP Query Messages

Router Solicitation and Advertisement

- 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.
- Tunnelling does not work in this situation because the packet must be in the IPv4 format to be understood by the receiver.

Debugging Tools

- Ping
  - ping www.google.com
  - use the ping program to find if a host is alive and responding.
  - We use ping here to see how it uses ICMP packets.
  - The source host sends ICMP echo-request messages (type: 8, code: 0); the destination, if alive, responds with ICMP echo-reply messages.
- Traceroute
  - Tracert/traceroute www.google.com
  - used to trace the route of a packet from the source to the destination.
  - The program elegantly uses two ICMP messages, time exceeded and destination unreachable, to find the route of a packet

```
(base) nateshbv@Nateshs-MacBook-Air ~ % ping www.google.com
PING www.google.com (142.250.77.68): 56 data bytes
64 bytes from 142.250.77.68: icmp_seq=0 ttl=117 time=36.730 ms
64 bytes from 142.250.77.68: icmp_seq=1 ttl=117 time=36.861 ms
64 bytes from 142.250.77.68: icmp_seq=2 ttl=117 time=36.893 ms
64 bytes from 142.250.77.68: icmp_seq=3 ttl=117 time=37.147 ms
64 bytes from 142.250.77.68: icmp_seq=4 ttl=117 time=36.986 ms
64 bytes from 142.250.77.68: icmp_seq=5 ttl=117 time=36.931 ms
64 bytes from 142.250.77.68: icmp_seq=6 ttl=117 time=36.825 ms
64 bytes from 142.250.77.68: icmp_seq=7 ttl=117 time=36.986 ms
^C
--- www.google.com ping statistics ---
8 packets transmitted, 8 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 36.730/36.920/37.147/0.117 ms
(base) nateshbv@Nateshs-MacBook-Air ~ %
```

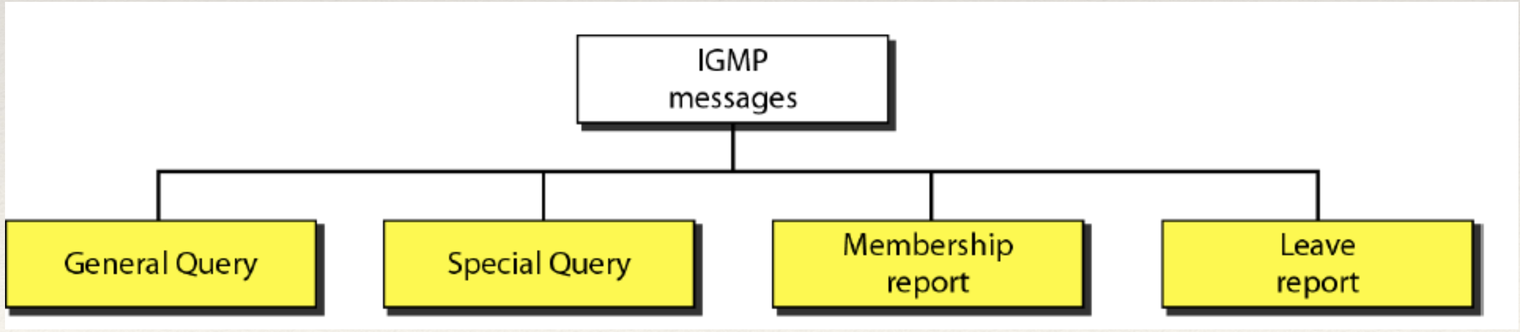
ping

```
(base) nateshbv@Nateshs-MacBook-Air ~ % traceroute www.google.com
traceroute to www.google.com (142.250.77.68), 64 hops max, 52 byte packets
 1  172.16.61.2 (172.16.61.2)  1.386 ms  1.708 ms  0.923 ms
 2  172.16.19.18 (172.16.19.18)  0.809 ms  0.813 ms  0.939 ms
```

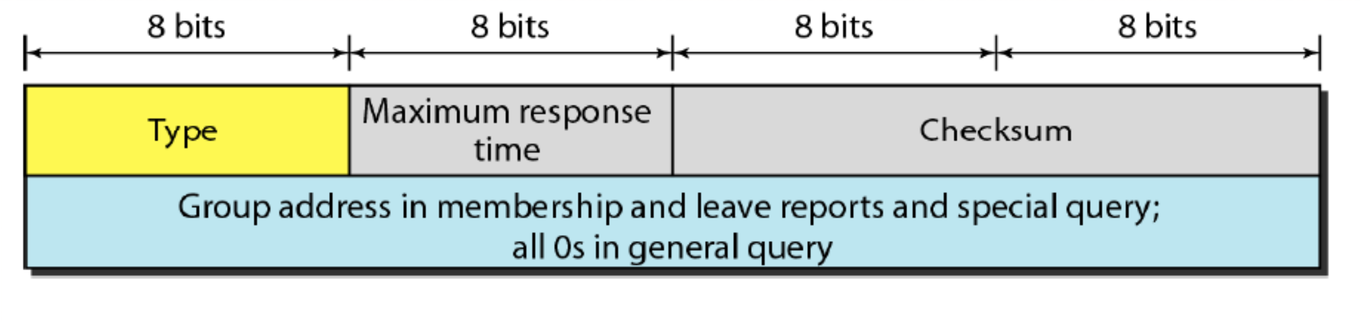
Traceroute

IGMP

- Internet Group Management Protocol (IGMP)
- IGMP is not a multicasting routing protocol; it is a protocol that manages group
- membership
- The IGMP protocol gives the multicast routers information about the membership status of hosts (routers) connected to the network



IGMP Message Format



IGMP Message Format

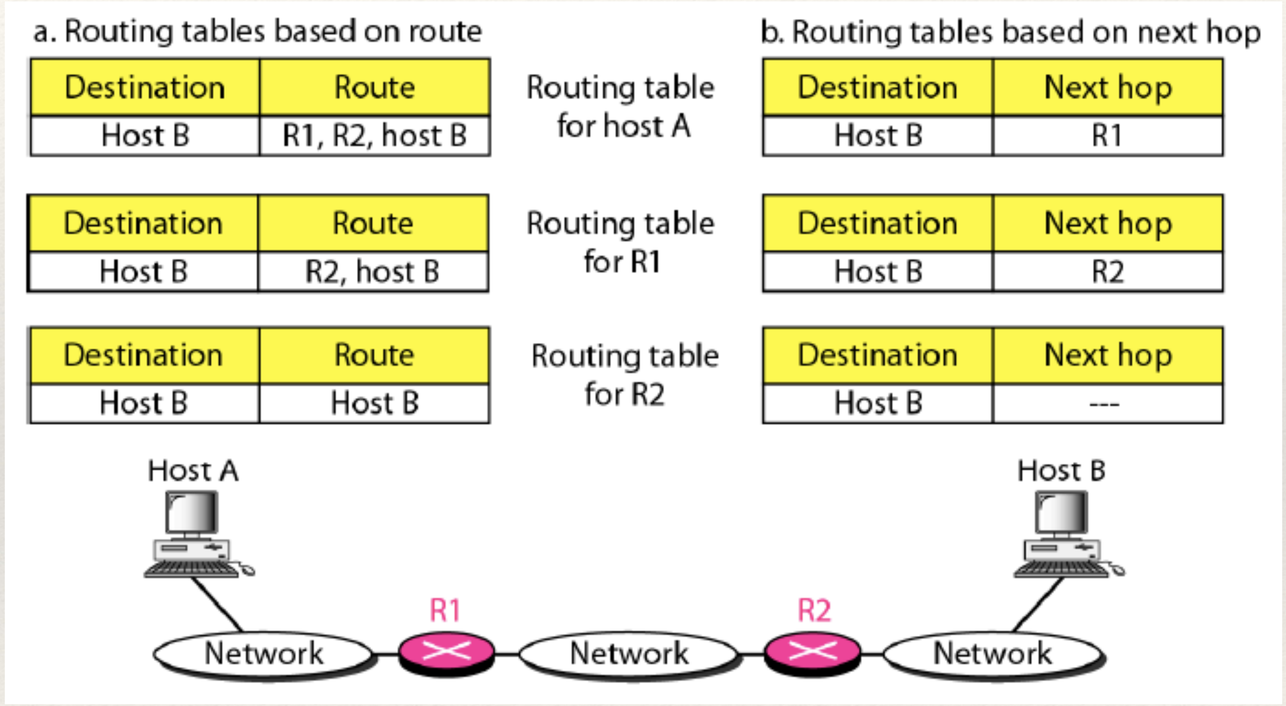
Type	*Value*
General or special query	0x11 or 00010001
Membership report	0x16 or 00010110
Leave report	0x17 or 00010111

Type info

- Type. This 8-bit field defines the type of message
- Maximum Response Time. This 8-bit field defines the amount of time in which a query must be answered
- Checksum. This is a 16-bit field carrying the checksum. The checksum is calculated over the 8-byte message.
- Group address. The value of this field is 0 for a general query message. The value defines the group id (multicast address of the group) in the special query, the membership report, and the leave report messages

Forwarding and Routing

- Forwarding means to place the packet in its route to its destination.
- Forwarding requires a host or a router to have a routing table.
- When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination.



Properties of Routing Algorithms

Desirable properties of Routing Algorithms:

- Correctness (applicable to all)
- Simplicity (applicable to all)
- Robustness: able to cope up with
- Changes in topology, load.
- Fairness (conflicting)
- Optimality (conflicting)

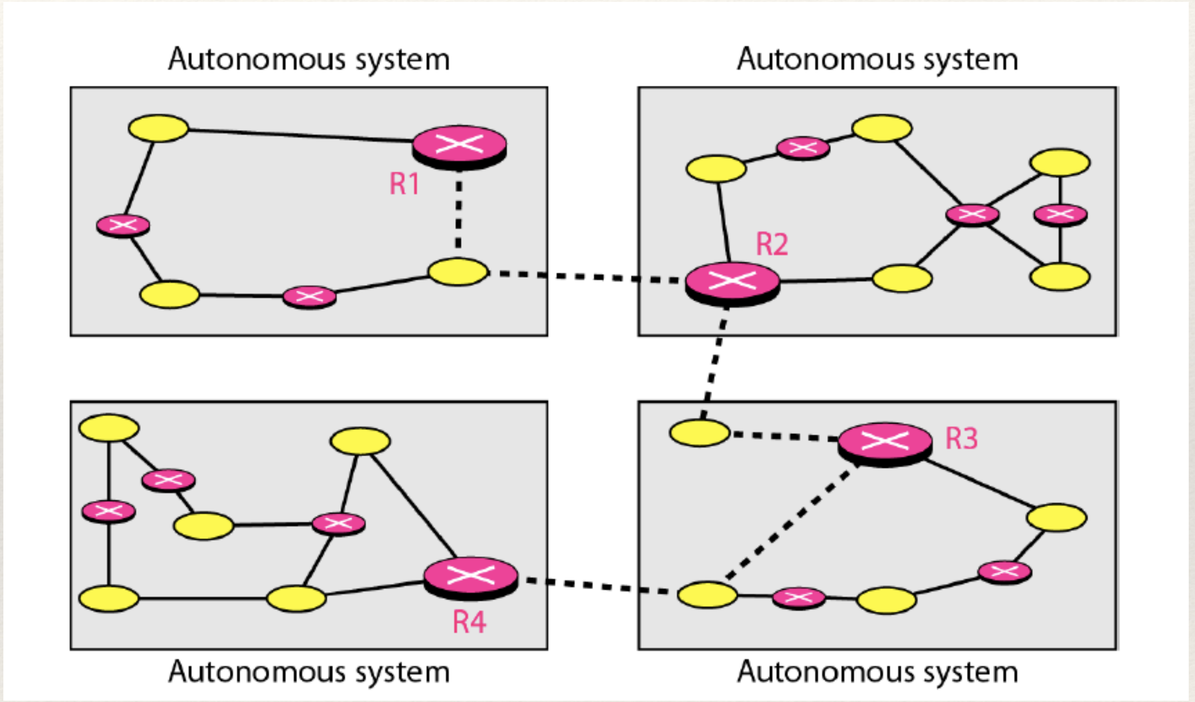
Types of Routing Algorithms:

- Non-Adaptive: Static. Routing decisions computed in advance, off-line and downloaded.
- Adaptive: Dynamic. Adaptive to the changes in topology and load. Issue here is how to get the information? Locally, From adjacent routers, from all routers?

Autonomous System

An autonomous system (AS) is a group of networks and routers under the authority of a single administration.

- Routing inside an autonomous system is referred to as intra-domain routing.
- Routing between autonomous systems is referred to as interdomain routing



Routing Protocols

- Unicast Routing Protocol
  - A routing table can be either static or dynamic.
    - A static table is one with manual entries.
    - A dynamic table is one that is updated automatically when there is a change somewhere in the Internet.
- A routing protocol is a combination of rules and procedures that lets routers in the Internet inform each other of changes.

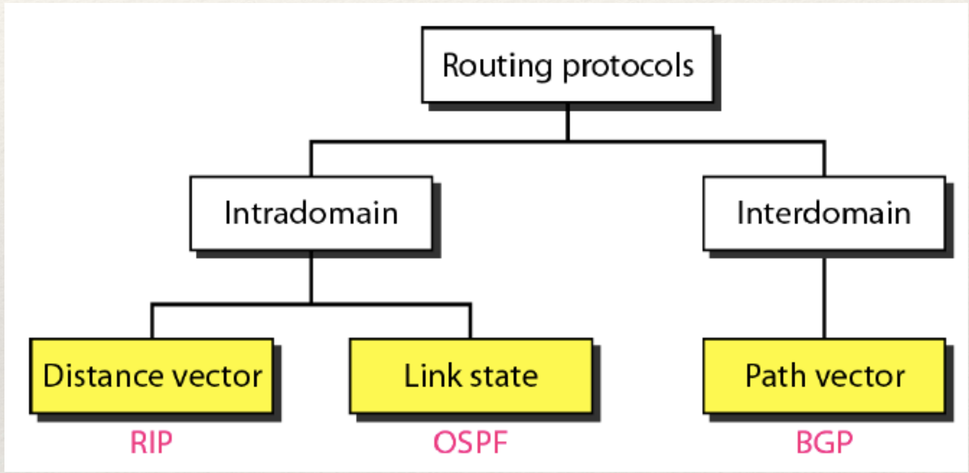


Fig: Routing Protocols

Distance Vector Routing Protocol

- Following two are Dynamic Routing Algorithms:
  - Distance Vector Routing Algorithm. (RIP)
  - Link State Routing Algorithm. (OSPF)
- Distance Vector Routing Algorithm:
  - At each step within a router:
  - Get routing tables from neighbours
  - Compute distance to neighbours
  - Compute new routing table

1.

Distance Vector Algorithms

- Router transmits its distance vector to each of its neighbors.
- Each router receives and saves the most recently received distance vector from each of its neighbors.
- A router **recalculates** its distance vector when:
  - It receives a distance vector from a neighbor containing different information than before.
  - It discovers that a link to a neighbor has gone down (i.e., a topology change).
- The DV calculation is based on minimizing the cost to each destination.
- The distance vector routing algorithm is sometimes called by other names, the **distributed Bellman-Ford** routing algorithm and the **Ford-Fulkerson algorithm.**

RIP Protocol

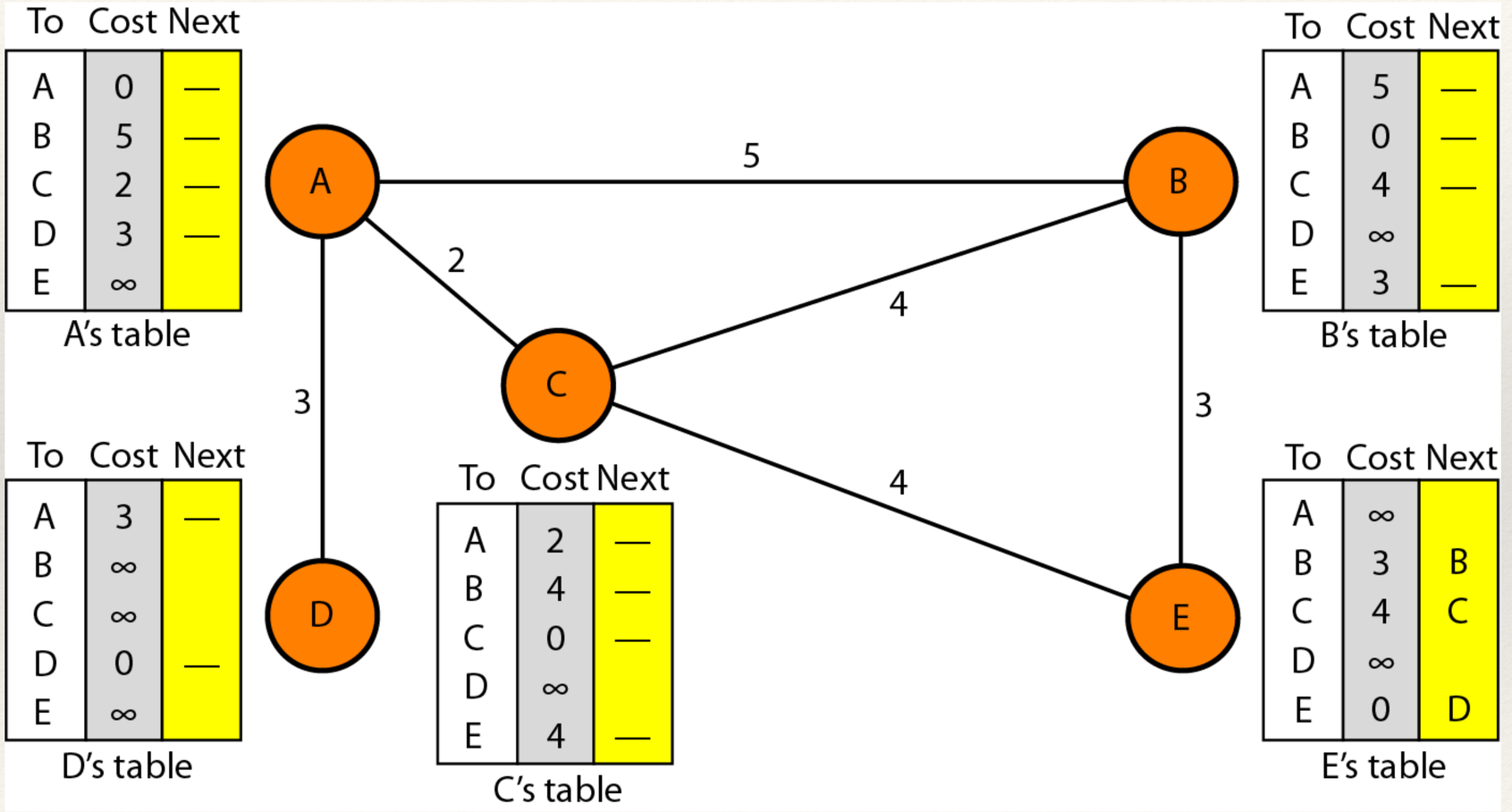


Fig: Initialization of tables in distance vector routing

RIP Protocol

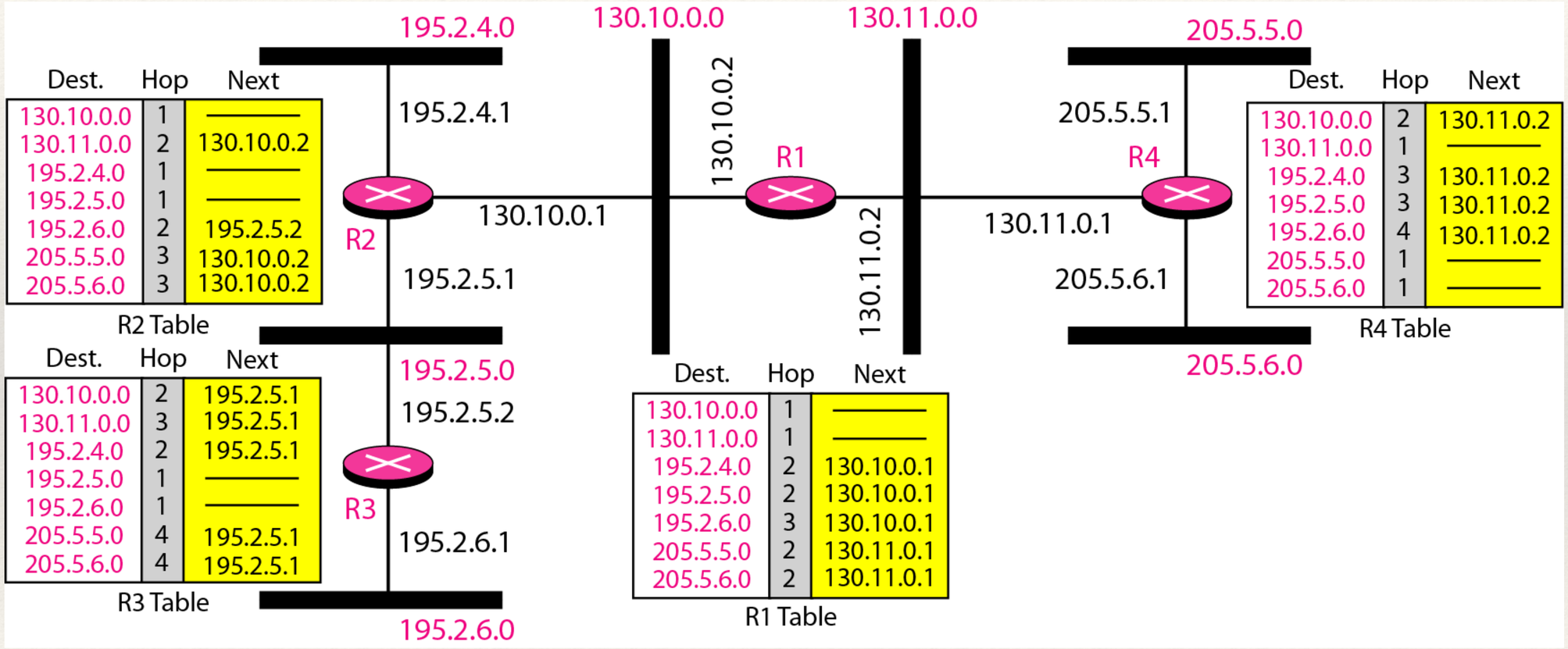
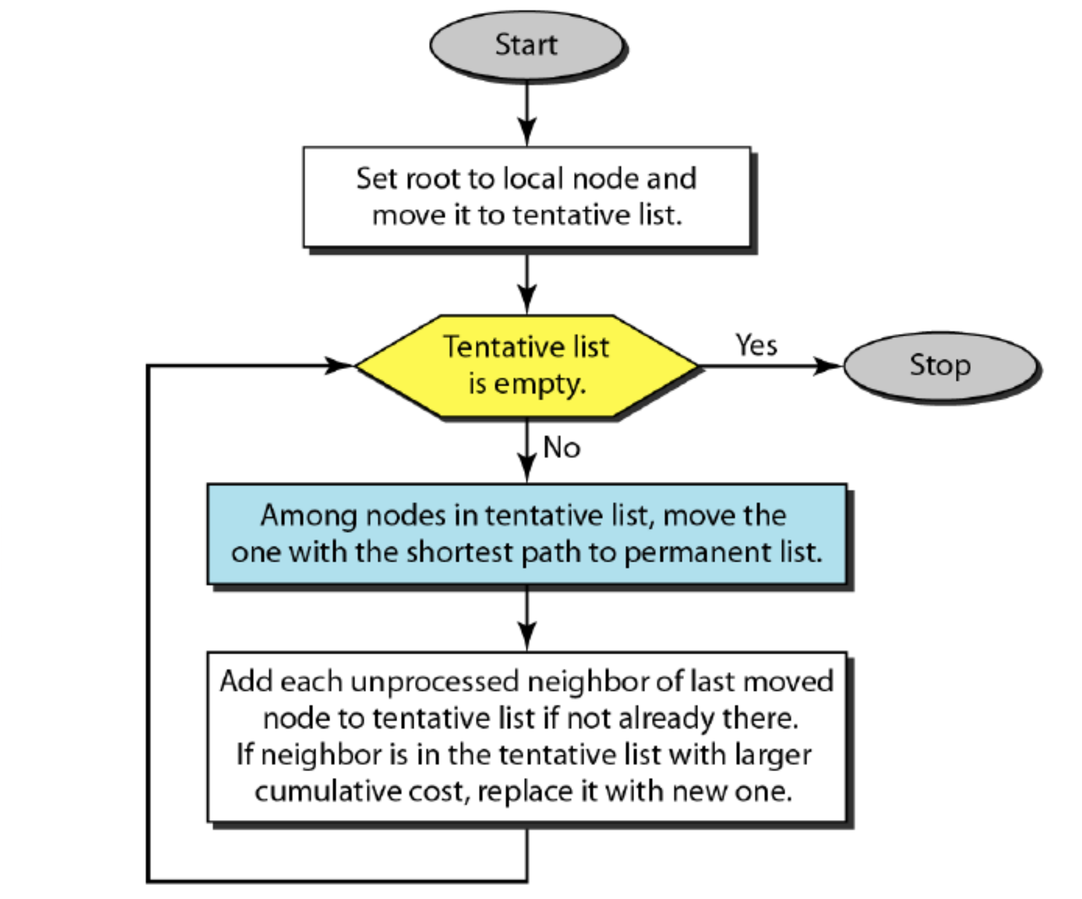


Fig: Example Domain using RIP

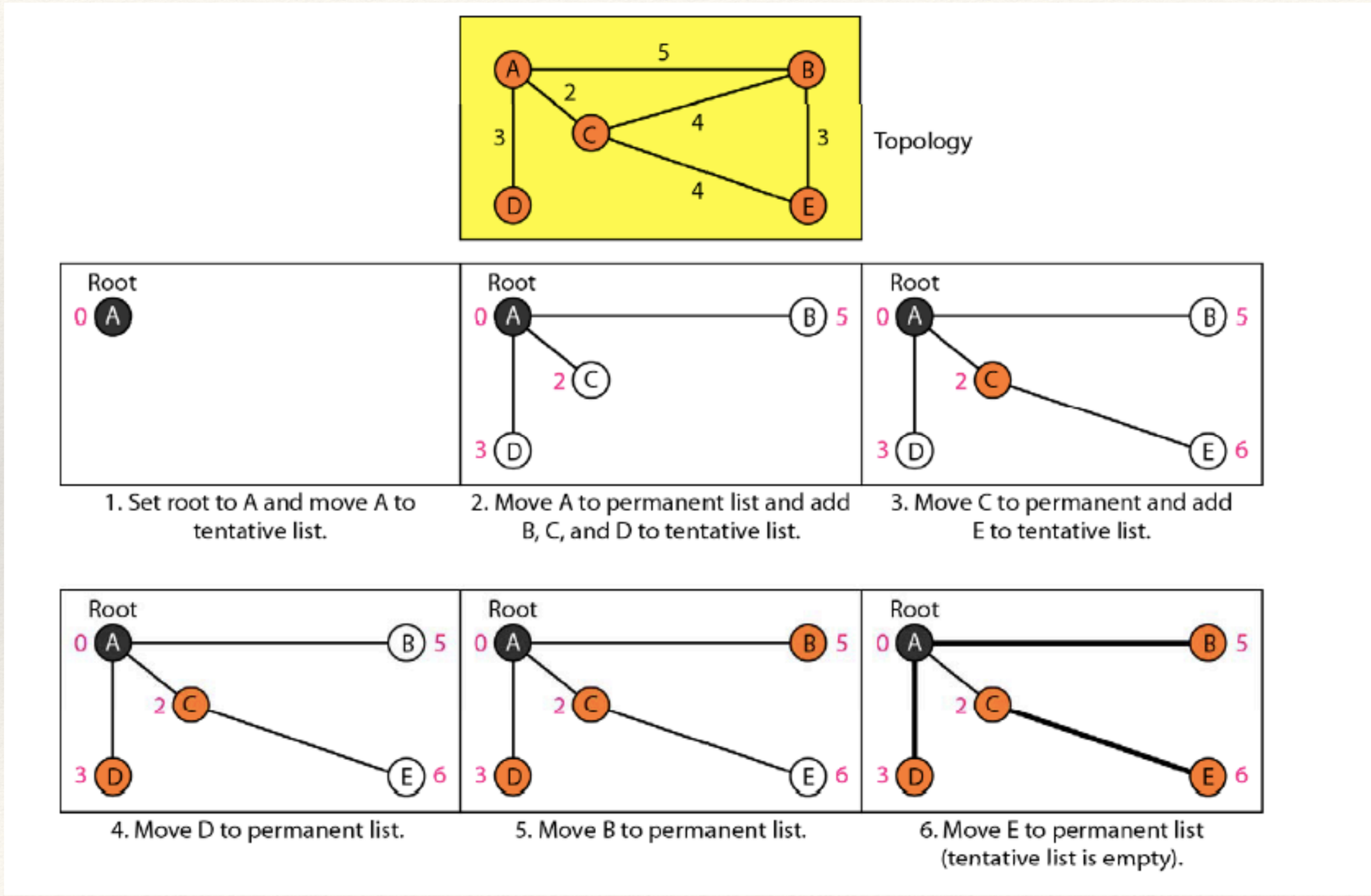
Link State Protocol

- Link State RP: In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links.
- How they are connected including the type, cost (metric), and condition of the links (up or down).
- The node can use Dijkstra's algorithm to build a routing table



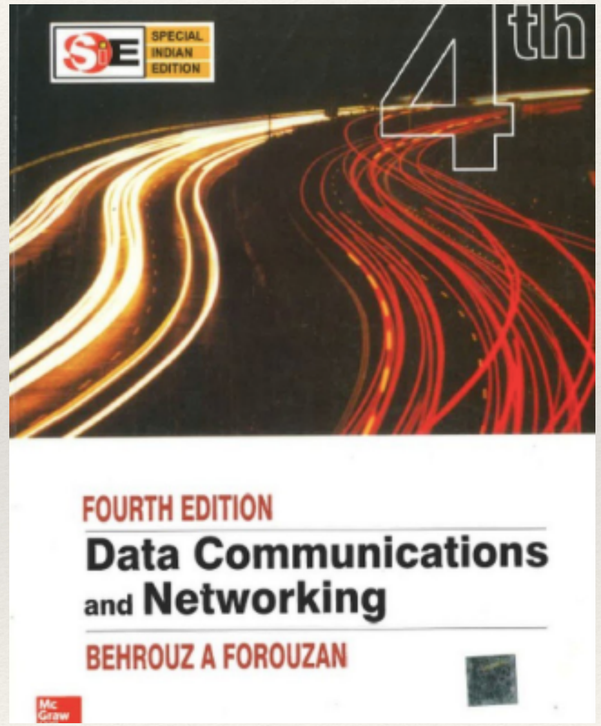
Dijkstras Algorithm

Link State Protocol (Shortest Path)



Summary

- Logical Addressing
- IP address Classful and Classless
- Subnetting
- IPv4 and IPv6 Frame Format
- IP Protocols
- Routing Protocols



Note: **Chapters 19 20.2 to 20.4, 21 and 22 (upto 22.3)**