COMPUTER NETWORKS MODULE 4.1

MR. SANDY JOSEPH

ASST. PROF, CSE

RSET

Network Layer in the Internet -10 principles

1. Make sure it works: Do not finalize the design or standard until multiple prototypes have successfully communicated with each other.
2. Keep it simple: use the simplest solution.
3. Make clear choices: Choose one out of several ways of doing the same thing.
4. Exploit modularity: use of protocol stacks, each of its layers is independent of all the other ones.
5. Expect heterogeneity: possibility of different types of hardware, transmission facilities and applications can occur on large network. Network design must be simple, general and flexible.

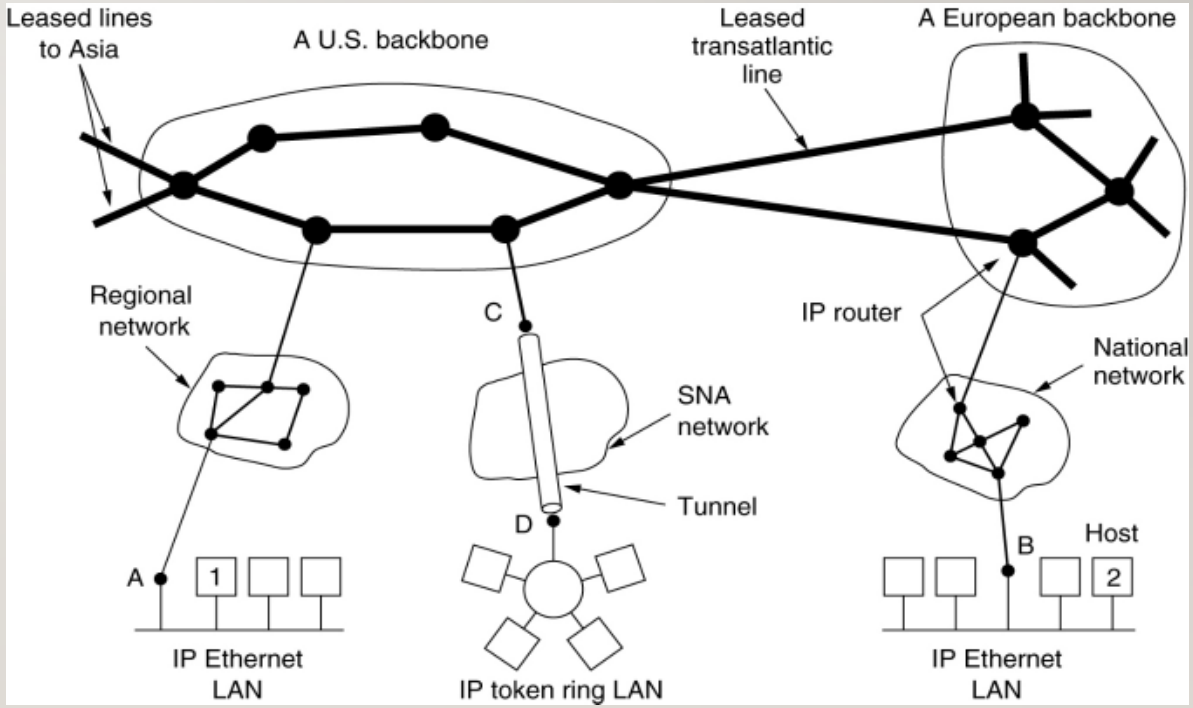
RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

Network Layer in the Internet -10 principles

6. Avoid static options and parameters: if parameters are unavoidable, it is best to have the sender and receiver negotiate a value rather than defining fixed choices.
7. Look for a good design; it need not be perfect.
8. Be strict when sending and tolerant when receiving: send only packets that comply with the standards, but expect packets that may not be fully conformant.
9. Think about scalability: on networks with billions of users, load must be spread as evenly as possible over the available resources.
10. Consider performance and cost: if a network has poor performance or outrageous costs, no one will use it.

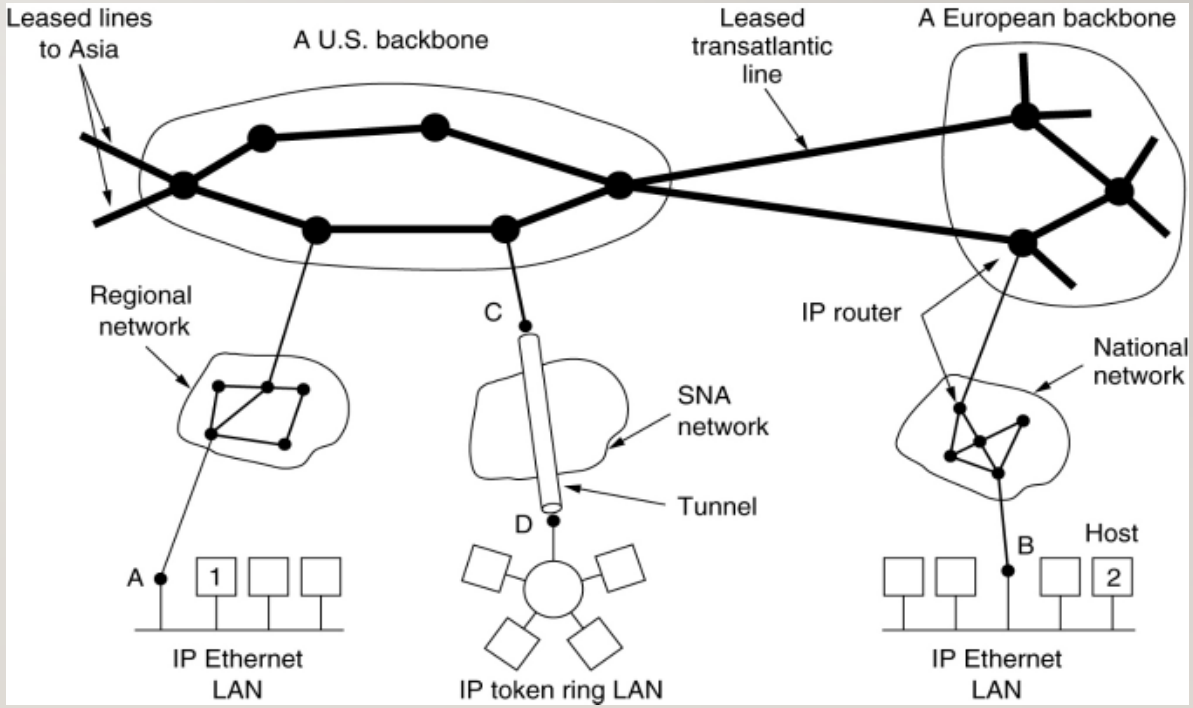
Internet- Collection Of Subnets

- Internet collection of networks or **AS**es (Autonomous Systems) that are interconnected.
- An autonomous system (AS) is **a very large network or group of networks with a single routing policy**.
- Each AS is assigned a unique ASN, which is a number that identifies the AS.
- ASNs, are unique 16-bit numbers between 1 and 65534 or 32-bit numbers between 131072 and 4294967294.



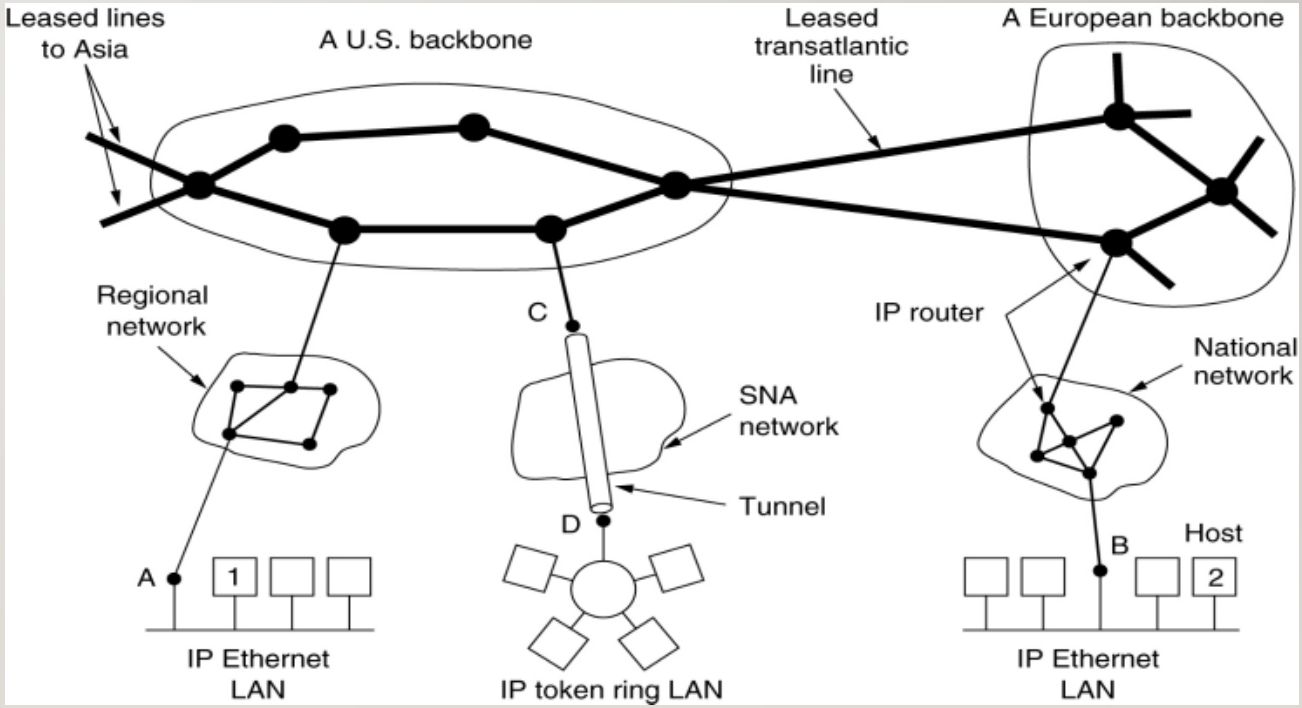
Internet- Collection Of Subnets

- ASNs are only required for external communications with inter-network.
- Internal routers and computers within an AS may not need to know that AS's number, since they are only communicating with devices within that AS.



Internet- Collection Of Subnets

- **ISP** (Internet Service Provider) provide internet access to homes and businesses, data centers, and regional networks.
- An **Internet service provider** (**ISP**) is an organization that provides services for accessing, using, or participating on the internet.
- **IP** (Internet Protocol) The glue that holds the whole Internet together.



IP-Internet Protocol

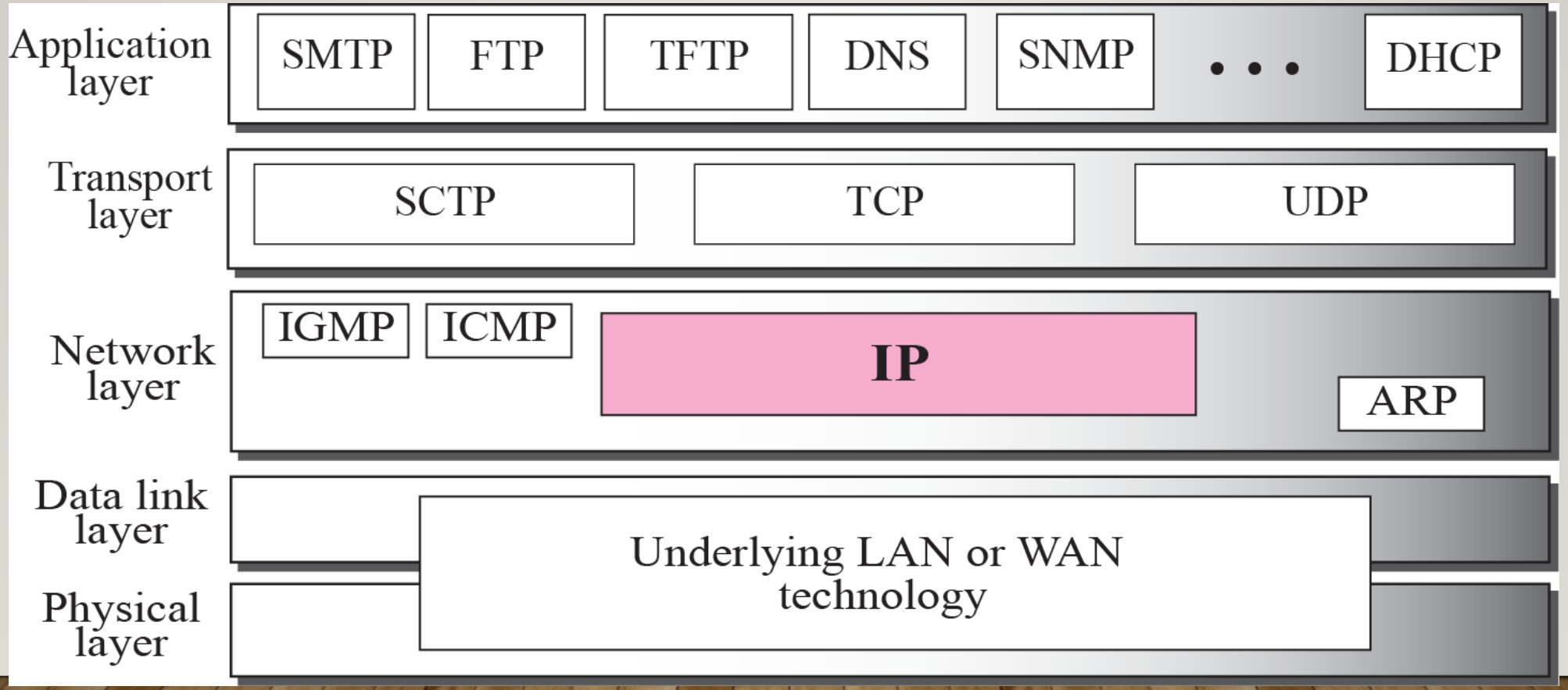
- The principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.
- Its routing function enables internetworking, and essentially establishes the Internet.
- IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers.
- IP defines packet structures that encapsulate the data to be delivered.

IP-Internet Protocol

- It also defines addressing methods that are used to label the datagram with source and destination information.
  - Unicast Addressing : data is sent only to one destined host; 32-bit destination address.
  - Broadcast Addressing: packet is addressed to all the hosts in a network segment; Destination Address field contains a special broadcast address, i.e. 255.255.255.255.
  - Multicast Addressing: packet is addressed to a group of hosts in a network segment; Destination Address contains a special address which starts with 224.x.x.x.

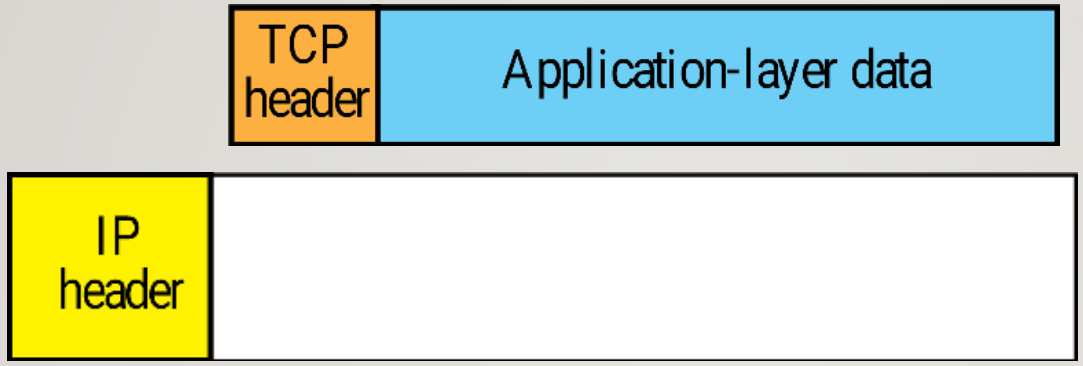
RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

Position of IP in the TCP/IP Suite



RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

Encapsulation



- Packets in the network (internet) layer are called datagrams.
- A datagram is a variable-length packet consisting of two parts: header and data.
- The header is 20 to 60 bytes in length.

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address

- An IPV4 address is a 32-bit address that uniquely and universally defines the connection of a device to the internet.
- IP address is the address of the connection, not the host or router.
- Address Space: the total number of addresses used by the protocol.
- The address space of IPV4 is $2^{32} = 4{,}294{,}967{,}296$ (more than 4 billion)

IPV4 Address

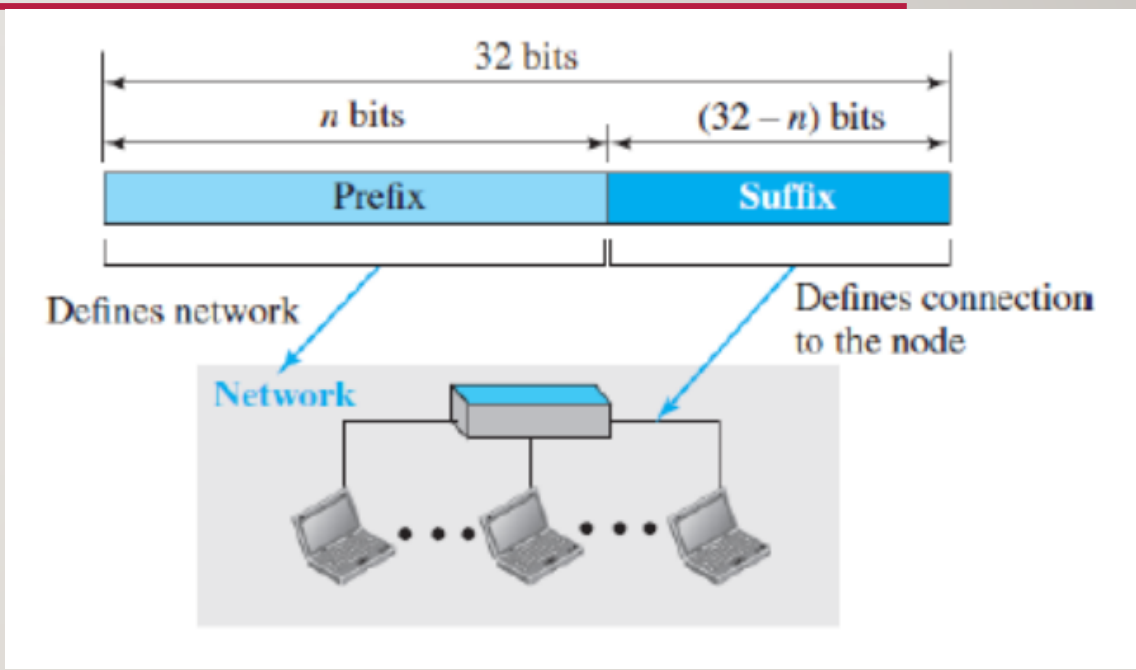
- Notation:
  - Binary notation : represented as 32 bits; with space between octets; 10000000 11010000 00000010 10010111
  - Dotted decimal notation: each of the four bytes in decimal (0 to 255); each octet is separated by dot; 128.208.2.151.
  - Hexadecimal notation: in 8 hexadecimal digits; 80 0B 03 1F.

IPV4 Address

- Static IP Address:
  - IP Address that once assigned to a network element always remains the same.
  - They are configured manually.
- Dynamic IP Address:
  - Dynamic IP Address is a temporarily assigned IP Address to a network element.
  - It can be assigned to a different device if it is not in use.
  - DHCP assigns dynamic IP addresses.

IPV4 Address- Hierarchy in Addressing

- Hierarchical addressing system.
- Prefix: first part of the address defines the network.
- Suffix: defines the host (connection of a device to the internet).
- Prefix: defines the network; can be fixed length (Classful addressing), or variable length (Classless addressing).



IPV4 Address- Classful Addressing

- Whole address space is divided into 5 classes (A, B, C, D, E)

Class	HOB	NET ID Bits	Host ID Bits	No of Networks	Host Per Network	Start Address	End Address
Class A	0	8	24	2^7=128	2^{24}=16,777,216	0.0.0.0	127.255.255.255
Class B	10	16	16	2^{14}=16,384	2^{16}=65,536	128.0.0.0	191.255.255.255
Class C	110	24	8	2^{21}=2,097,152	2^8=256	192.0.0.0	223.255.255.255
Class D	1110	-	-	-	-	224.0.0.0	239.255.255.255
Class E	1111	-	-	-	-	240.0.0.0	255.255.255.255

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address- Subnetting

- IP addresses are the identity of the device in the network.
- Subnet Mask
  - Subnet Mask helps to extract the Network ID and the Host from an IP Address
  - Separate 32-bit pattern to define the network and host portion of an address.
  - To know who are the neighbors in the network.
  - Classes A, B, C are accompanied with default subnet mask.

IPV4 Address- Subnetting

- Subnet Mask
  - Does not contain network or host portion of an IPV4 address; tells where to look for these portions in a given IPV4 address.
  - 255 in octet means network portion; remaining octets are host portion.
  - A higher-class subnet mask can be used for lower class.
  - If the IP address in binary is ANDed with its Subnet Mask, the result yields the Network address.

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address- Subnetting

- Question 1: Check whether the following addresses belong to the same network or not.
  - 10.10.10.1 and 10.10.20.16 (subnet mask: 255.0.0.0)
  - 10.10.10.1 and 10.10.20.16 (subnet mask: 255.255.255.0)
  - 172.16.200.1 and 172.16.165.2 (subnet mask: 255.255.0.0)
  - 172.16.200.1 and 172.16.165.2 (subnet mask: 255.255.255.0)

IPV4 Address- Subnetting

- Question 2: How many bits are allocated for Network ID and Host ID in 23.192.157.234 address?
- Question 3: What is the network ID of the IP Address 230.100.123.70?

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address- Subnetting

- Advantages
  - Subnetting reduces broadcast volume and hence reduces network traffic.
  - The network security may easily be utilized amongst sub-networks instead of using it on the entire network.
  - Subnetworks are simple to handle and maintain.
- Disadvantages
  - require a qualified administrator to perform the subnetting process.
  - subnetting process is quite expensive.

IPV4 Address- Address Depletion

- Disadvantage of classful addressing.
- Means inefficient address use.
- Class A Maximum 128 organizations with maximum 16777216 nodes per network.
- Only few organizations were this much large.

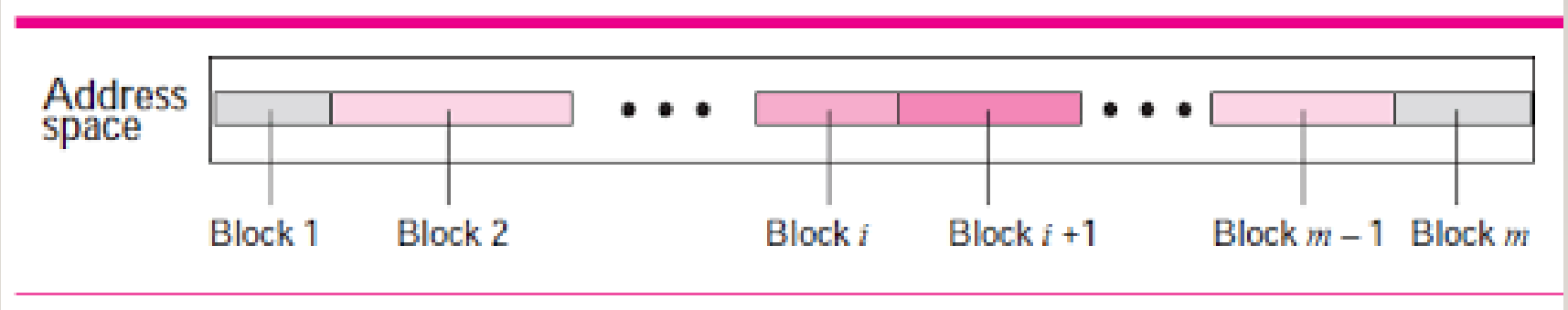
RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address- Classless Addressing

- Formal Name is Classless Inter-Domain Routing (CIDR).
- With the growth of internet, large address space is needed. Allow service providers to allocate IPV4 addresses on any address bit boundary instead of classes A, B, C.
- Number of addresses in a block needs to be a power of 2.
- Classless addressing is possible with the help of subnetting.

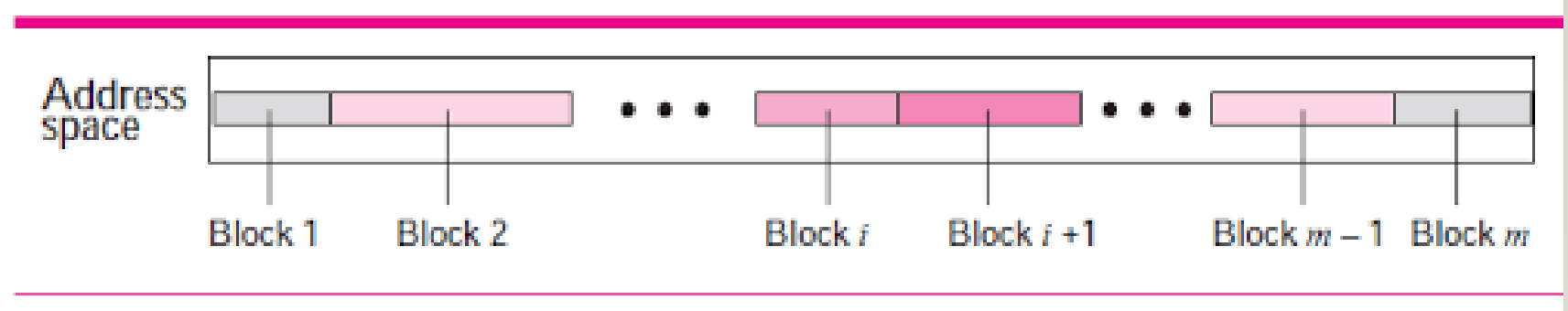
IPV4 Address- Classless Addressing

- Whole address space is divided into variable length blocks.
  - Prefix: defines the network; variable length; ranges from 0 to 32.
  - Suffix: defines the host.



IPV4 Address- Classless Addressing

- Whole address space is divided into variable length blocks.
  - Prefix: defines the network; variable length; ranges from 0 to 32.
  - Suffix: defines the host.
- How to find prefix length?
  - Slash Notation



IPV4 Address- Classless Addressing

- Slash Notation (/n)
  - Slash notation is a compact way to write an IPv4 subnet mask.
  - **Format:** write the IP address, a forward slash (/), and the subnet mask number.
  - To find the subnet mask number:
    - Convert the decimal representation of the subnet mask to a binary.
    - Count each "1" in the subnet mask. The total is the subnet mask number.
  - E.g. 192.168.42.23 with a subnet mask of 255.255.255.0 → 192.168.42.23/24

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address- Classless Addressing

- An address in classless addressing does not define the block or network to which the address belongs to with out knowing prefix length.

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address- Classless Addressing – Extracting information from an address

- Number of addresses in a block, N= 2^{32-n}
- To find first address, keep the 'n' leftmost bits and set the (32-n) rightmost bits all to 0s.
- To find last address, keep the 'n' leftmost bits and set the (32-n) rightmost bits all to 1s.

IPV4 Address- Classless Addressing – Extracting information from an address

- Q1. A classless address is given as 167.199.170.82/27. Find the number of addresses, first address, and last address?
  - Number of addresses= 32
  - First address=10100111 11000111 10101010 01000000 (167.199.170.64/27)
  - Last address= 10100111 11000111 10101010 01011111 (167.199.170.95/27)

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address- Subnetting

- Number of valid hosts in a subnet

$$2^{32\ -network\ bits}\ -\ 2$$

IPV4 Address-Subnetting

- Qn.1 How many usable IP addresses can we get from a /19 subnet?

  Ans: 8190

- Qn. 2. How many usable IP addresses can we get from a /24 subnet?

  Ans: 254

- Qn. 3. how many usable IP addresses are there in 172.16.23.0 255.255.240.0?

  Ans: 255.255.240.0 is /20

  4094

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address-Subnetting

- Qn.4 What is the minimum subnet size we need to accommodate 20 hosts?

  Ans: minimum number of host bits required is 5 bits

  /27

- Qn. 5. What is the minimum subnet size we need to accommodate 127 hosts?

  Ans: /24

- Qn. 6. What is the maximum number of IP addresses that can be assigned to hosts on a local subnet that uses the 255.255.255.224 subnet mask?

  Ans: 30

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address- Questions

- Q7. Write the IP address 222.1.1.20 mask 255.255.255.192 in CIDR notation.

  Ans: 222.1.1.20/26

- Q8. You have been allocated a class C network address of 211.1.1.0 and are using the default subnet mask of 255.255.255.0 how may hosts can you have?

  Ans: 2^8 -2 =254 hosts

- Q9. You have an interface on a router with the IP address of 192.168.192.10/29. Including the router interface, how many hosts can have IP addresses on the LAN attached to the router interface?

  Ans: 8 hosts

IPV4 Address- Questions

- Q10. An address space has a total of 1024 addresses. How many bits are needed to represent an address?.

  Ans: 10
- Q11. In a block of addresses, we know the IP address of one host is 25.34.12.56/16. What are the first address (network address) and the last address (limited broadcast address) in this block?

  first address: 25.34.0.0

  Last address: 25.34.255.255
- Q12. An address space uses the three symbols 0, 1, and 2 to represent addresses. If each address is made of 10 symbols, how many addresses are available in this system?

  Ans: 3^10 =59049

IPV4 Addresses –Subnet Id and Number of Subnets

- The subnet mask defines the size of the network.
- For more subnets, "borrow" bits from the host part.
- $n_{sub} = n + log_2(S)$

n_{sub} is the length of the subnet id
S is the number of subnets

IPV4 Address- Questions

Qn. 13. Find the subnet mask in each case:

a. 1024 subnets in class A

$n_{sub} = n + \log S$
$= 8 + \log 1024 = 18$

Subnet mask is 255.255.192.0

b. 256 subnets in class B

$n_{sub} = 16 + \log 256 = 24$

Subnet mask is 255.255.255.0

c. 4 subnets in class C

$n_{sub} = 24 + \log 4 = 26$

Subnet mask is 255.255.255.192

IPV4 Address- Questions

- Q14. An organization is granted the block 211.17.180.0/24. The administrator wants to create 32 subnets.
  - a. Find the subnet mask.
  - b. Find the number of addresses in each subnet.
  - c. Find the first and last addresses in subnet 1.
  - d. Find the first and last addresses in subnet 32.
- Ans: a. Mask: /29 (24 + 5)
- b. 2^(32− 29) = 8 Addresses per subnet
- c. First address in subnet 1: **211 . 17 . 180 . 0/29** and last address in Subnet 1 is **211 . 17 . 180 . 7/29**
- d. First address in subnet 32: **211 . 17 . 180 . 248/29** and last address in Subnet 32 is **211 . 17 . 180 . 255/29**

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address- Questions

- Q15. Find the range of addresses in the following blocks.
- a. 123.56.77.32/29
- b. 200.17.21.128/27
- c. 17.34.16.0/23
- d. 180.34.64.64/30

- Ans:
- a. From: 123 . 56 . 77 . 32
  0 . 0 . 0 . 7
  To: 123 . 56 . 77 . 39
- b. From: 200 . 17 . 21 . 128
  0 . 0 . 0 . 31
  To: 200 . 17 . 21 . 159
- c. From: 17 . 34 . 16 . 0
  0 . 0 . 1 . 255
  To: 17 . 34 . 17 . 255
- d. From: 180 . 34 . 64 . 64
  0 . 0 . 0 . 3
  To: 180 . 34 . 64 . 67

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address- What Subnet an Address Belongs to?

- Steps:
  - Determine how many network bits are in use.
  - Determine the maximum number of bits in the octet in which the subnet is
  - Determine the subnet block size by subtracting the network bits from the answer in step 2 above and raising to the power of 2.
  - To find the subnet to which the address belongs, start at 0 (in whatever octet the subnet is) and increase by the block size.

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address- What Subnet an Address Belongs to?

Qn.1. On what subnet does the 156.67.154.75/28 IP address belong

- No. of network bits =28.
- /28 is in the fourth octet and the maximum number of bits from the first to fourth octet is 32 bits.
- Subnet block size : 2^(32-28) = 16 subnet blocks.
- To find the subnet: 156.67.154.0/28 156.67.154.16/28
  156.67.154.32/28 156.67.154.48/28
  156.67.154.64/28 156.67.154.80/28
  156.67.154.96/28, etc
- 156.67.154.75 belongs to156.67.154.64

IPV4 Address- What Subnet an Address Belongs to?

Qn.2. What subnet does the address 77.81.23.45/19 belong?

- No. of network bits =19.
- /19 is in the third octet and the maximum number of bits from the first to third octet is 24 bits.
- Subnet block size : 2^(24-19) = 32 subnet blocks.

- To find the subnet: 77.81.0.0/19 77.81.32.0/19

  77.81.64.0/19, etc.

- Since .23 is greater than .0 and less than .32, then the 77.81.23.45/19 IP address belongs in the 77.81.0.0/19 subnet.

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address- What Subnet an Address Belongs to?

Qn.3. Do the following addresses belong on the same subnet? 10.21.45.137/13 and 10.23.156.198/13?

- Ans: same network

IPV4 Address

Qn. 4. An organization is granted the block 16.0.0.0/8. The administrator wants to create 500 fixed-length subnets.
a. Find the subnet mask.
b. Find the number of addresses in each subnet.
c. Find the first and last addresses in subnet 1.
d. Find the first and last addresses in subnet 500.

- a- Mask = /17
- b- 32768
- c- 16.0.0.0 , 16.0.127.255
- d- 16.249.128.0 , 16.249.255.255

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

IPV4 Address- Subnetting

- Steps:
  - Identify the class of the IP address and note the default subnet mask.
  - Convert the default subnet mask into binary
  - Note the number of hosts required per subnet and find the subnet generator (SG) and octet position.
  - Generate the new subnet mask.
  - Use the SG and generate the network ranges (subnets) in the appropriate octet position.

IPV4 Address- Subnetting

- Question 1: Subnet the IP address 216.21.5.0 into 30 hosts in each subnet.
  1. Class C – Default subnet mask 255.255.255.0
  2. Binary 11111111 11111111 11111111 00000000
  3. **No. of hosts per subnet** =30 (11110 in binary); 5 bits. Reserve 5 bits from the right (remaining bits will be 1's).

     11111111 11111111 11111111 11100000 (1st one from right side =32)

     Subnet Generator (SG) = 32 ; **Octet Position** (of SG)= 4.
  4. **New Subnet Mask** = 11111111 11111111 11111111 11100000 or 255.255.255.224 or /27

IPV4 Address- Subnetting

- Question 1: Subnet the IP address 216.21.5.0 into 30 hosts in each subnet.
  5. Subnets:
     - 216.21.5.0 - 216.21.5.31
     - 216.21.5.32 - 216.21.5.63
     - 216.21.5.64 - 216.21.5.95
     - 216.21.5.96 -216.21.5.127

     and so on

IPV4 Address- Subnetting

- Question 2: Subnet the IP address 196.10.20.0 into 52 hosts in each subnet.
  1. Class C – Default subnet mask 255.255.255.0
  2. Binary 11111111 11111111 11111111 00000000
  3. **No. of hosts per subnet** =52 (110100 in binary); 6 bits. Reserve 6 bits from the right (remaining bits will be 1's).

     11111111 11111111 11111111 11000000 (1st one from right side =64)

     Subnet Generator (SG) = 64 ; **Octet Position** (of SG)= 4.
  4. **New Subnet Mask** = 11111111 11111111 11111111 11000000 or 255.255.255.192 or /26

IPV4 Address- Subnetting

- Question 2: Subnet the IP address 196.10.20.0 into 52 hosts in each subnet.
  5. Subnets:

     196.10.20.0 - 196.10.20.63

     196.10.20.64 - 196.10.20.127

     196.10.20.128 - 196.10.20.191

     196.10.20.192 - 196.10.20.255

     and so on

IPV4 Address- Subnetting

- Question 3: Subnet the IP address 150.15.0.0 into 500 hosts in each subnet.
  1. Class B – Default subnet mask 255.255.0.0
  2. Binary 11111111 11111111 00000000 00000000
  3. **No. of hosts per subnet** =500 (111110100 in binary); 9 bits. Reserve 9 bits from the right (remaining bits will be 1's).

     11111111 11111111 11111110 00000000 (1st one from right side =2)

     Subnet Generator (SG) = 2 ; **Octet Position** (of SG)= 3.
  4. **New Subnet Mask** = 11111111 11111111 11111110 00000000 or 255.255.254.0 or /23

IPV4 Address- Subnetting

- Question 3: Subnet the IP address 150.15.0.0 into 500 hosts in each subnet.
  5. Subnets:

     150.15.0.0 - 150.15.1.255

     150.15.2.0 - 150.15.3.255

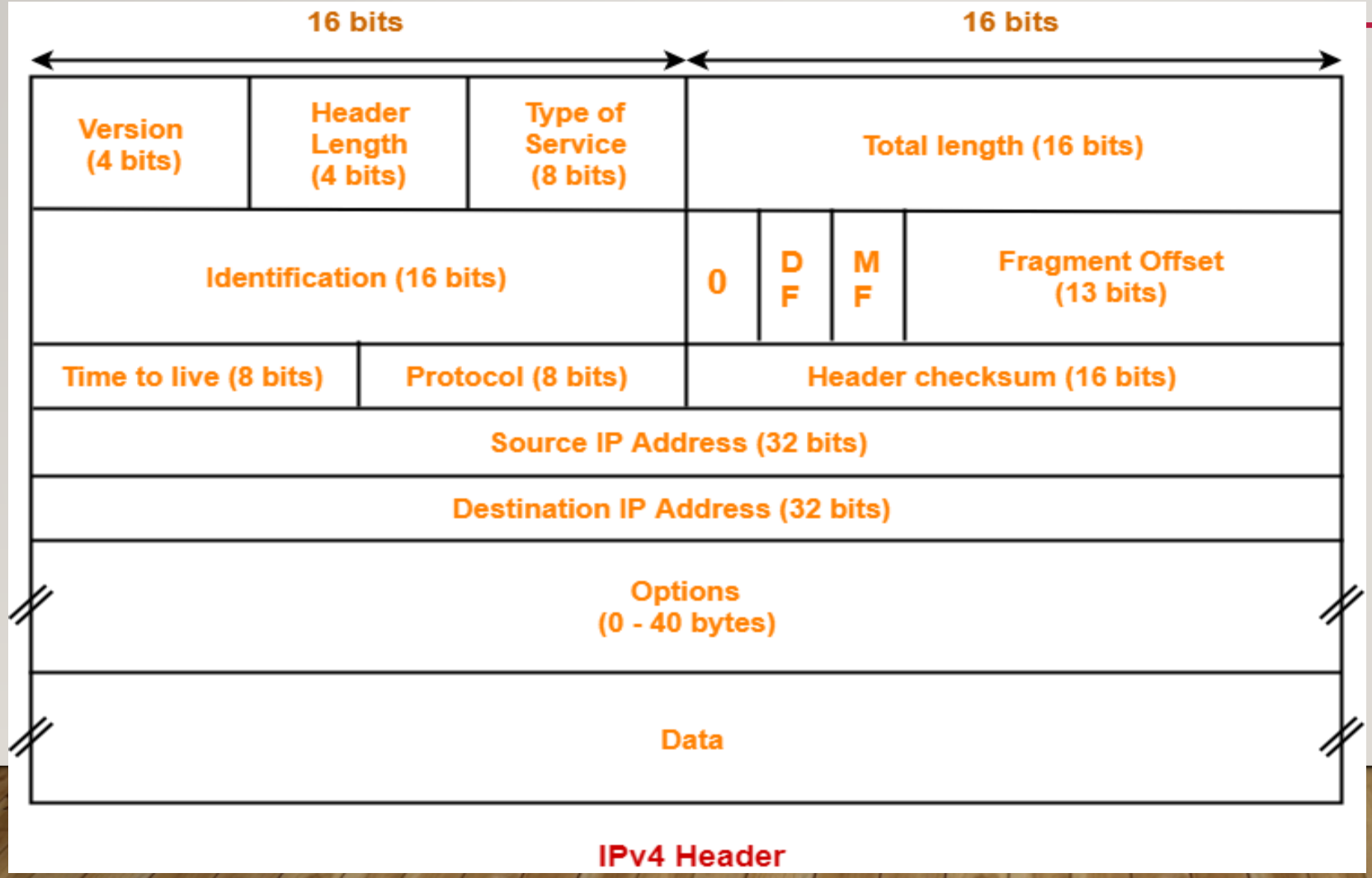
     150.15.4.0 - 150.15.5.255

     and so on

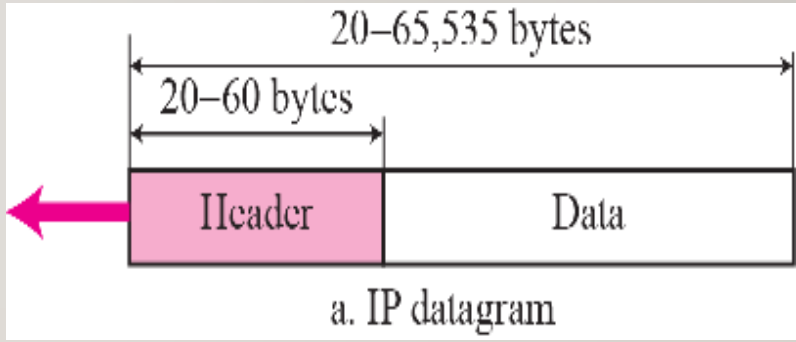
IPV4 Header

- Provides a Connectionless, datagram service
- Datagram = Header + Data
- Header 20 – 60 bytes.
- Data 0-65515 bytes
- Size of Datagram 65535 bytes.

IPV4 Header Format



IPv4 Header

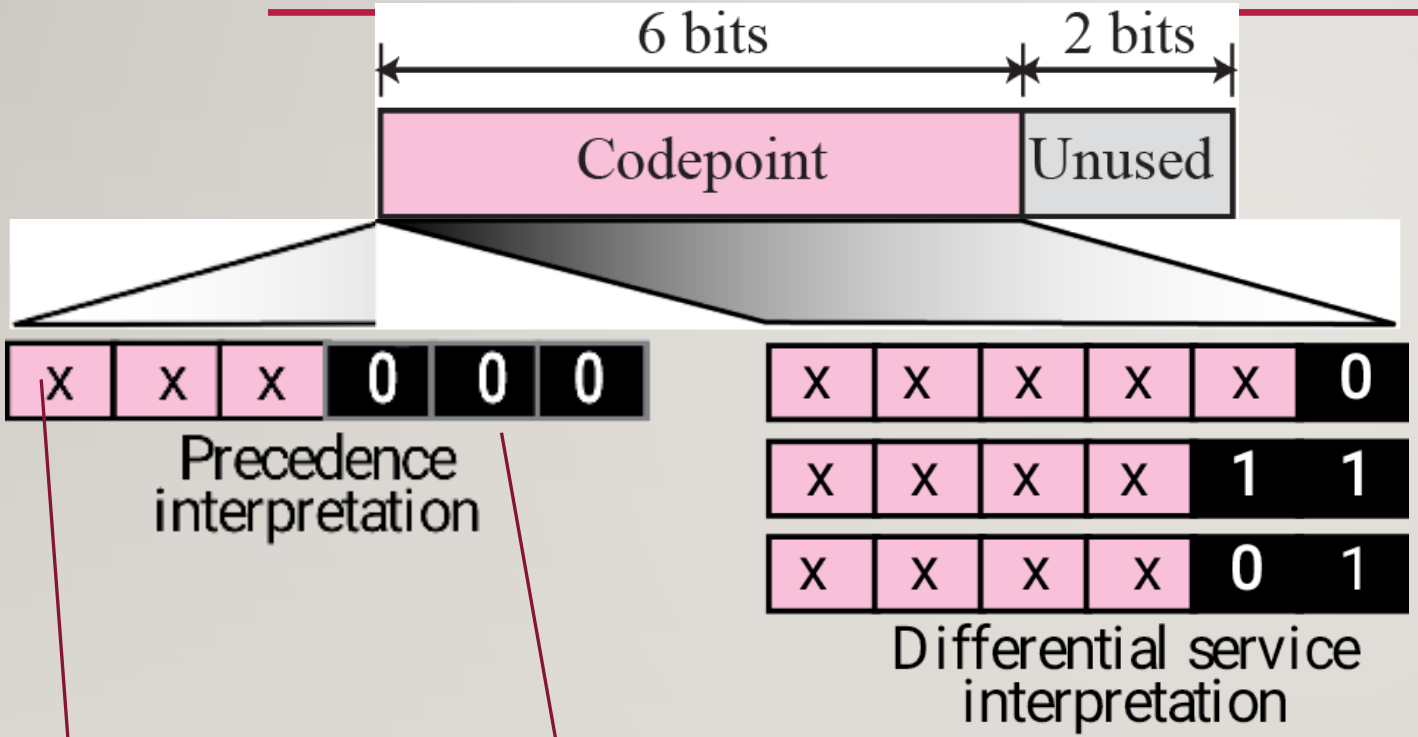


a. IP datagram

IPV4 Header Format

- **Version (4 bits)**: version of IP protocol – IPv4 or IPv6.
- **Header length (4 bits)**: total length of the datagram header, in 4-byte words.
  - If header length is 20 bytes, the value of the field is 5
- **Service Type (8 bits):** defines a set of differentiated services.
  - First 3 bits defines priority of the packets.
  - Next 3 bits defines whether a host cares about delay, throughput and reliability.
  - Next 2 bits defines congestion notification information.

IPV4 Header Format



Priority of the datagram 0 - 7

Flags D, T, R (hosts cares about delay/throughput/ reliability)

Table 7.1 *Values for codepoints*

Category	*Codepoint*	*Assigning Authority*
1	XXXXX0	Internet
2	XXXX11	Local
3	XXXX01	Temporary or experimental

IPV4 Header Format

- **Total Length (16 bits):** defines the total length of the IP datagram in bytes.
  - Length of data = total length – header length
  - Total length is limited to 65,535 bytes (since the field length is 16 bits).
- **Identification (16 bits):** allow the destination to determine which packet a newly arrived fragment belongs to. All the fragments of a packet contains same Identification value.

IPV4 Header Format

- **Flags (3 bits):**
  - First bit 0 (unused bit).
  - Second bit DF Don't Fragment: order to the routers not to fragment the packet.
  - Third bit MF More Fragments: All fragments except the last one have this bit set. It is needed to know when all fragments of a datagram have arrived.

IPV4 Header Format

- **Fragmentation offset (13 bits):** where in the current packet this fragment belongs. All fragments except the last one in a datagram must be a multiple of 8 bytes. With 13 bits, there is a maximum of 8192 fragments per datagram.
- **Time to live (8 bits):** counter used to limit packet lifetimes. Maximum lifetime of 255 sec.
  - Holds a timestamp (approximately twice the maximum number of routers between any two hosts) which is decremented by each visited router.
  - Datagram is discarded when the value becomes zero.

Fragmentation

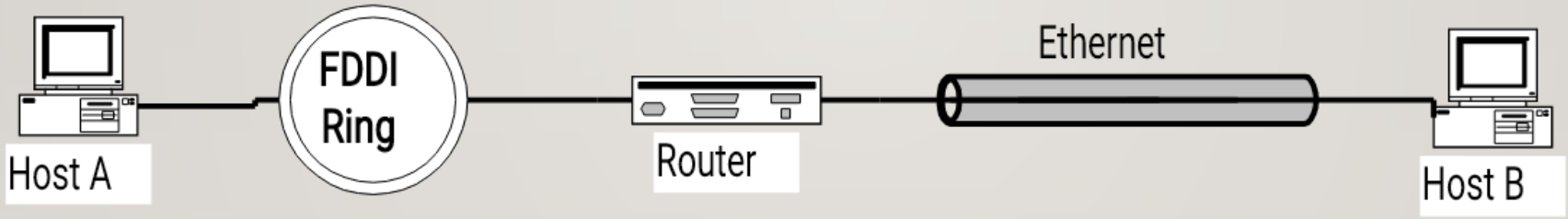
- Maximum size of IP datagram is 65,535 bytes.
  - But the data link layer protocol generally imposes a limit that is much smaller.
- For example:
  - Ethernet frames have a maximum payload of 1500 bytes.
  - IP datagrams encapsulated in Ethernet frame cannot be longer than 1500 bytes.
- The limit on the maximum IP datagram size, imposed by the data link protocol is called **Maximum Transmission Unit (MTU).**

Fragmentation

- MTUs for various data link layers protocols:
  - Ethernet : 1500
  - FDDI : 4352
  - PPP : 296
  - 802.3 : 1492
  - ATM AAL5 : 9180
  - 802.5 : 4464

Fragmentation

- What if the size of an IP datagram exceeds the MTU?
- What if the route contains networks with different MTUs?



- IP datagram has to be divided to make it possible to pass through these networks – Fragmentation.

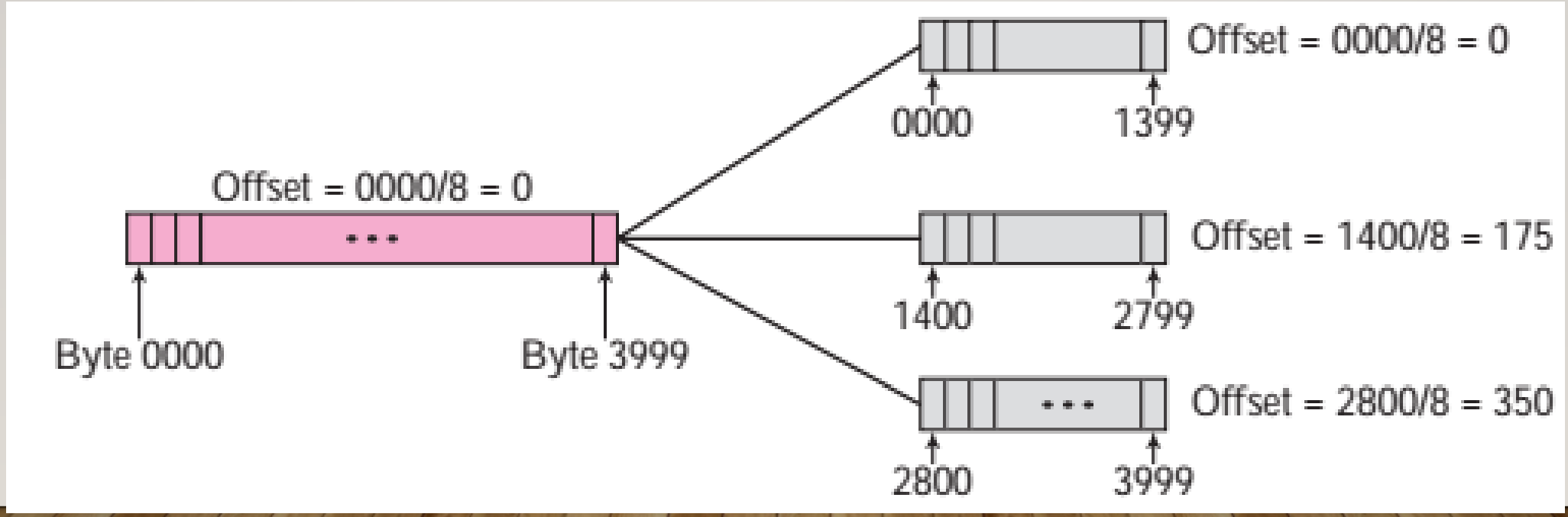
RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

Fragmentation

- Fragmentation can be done at the sender or at intermediate routers.
- The same datagram can be fragmented several times.
- Reassembly of original datagram is only done at destination host.

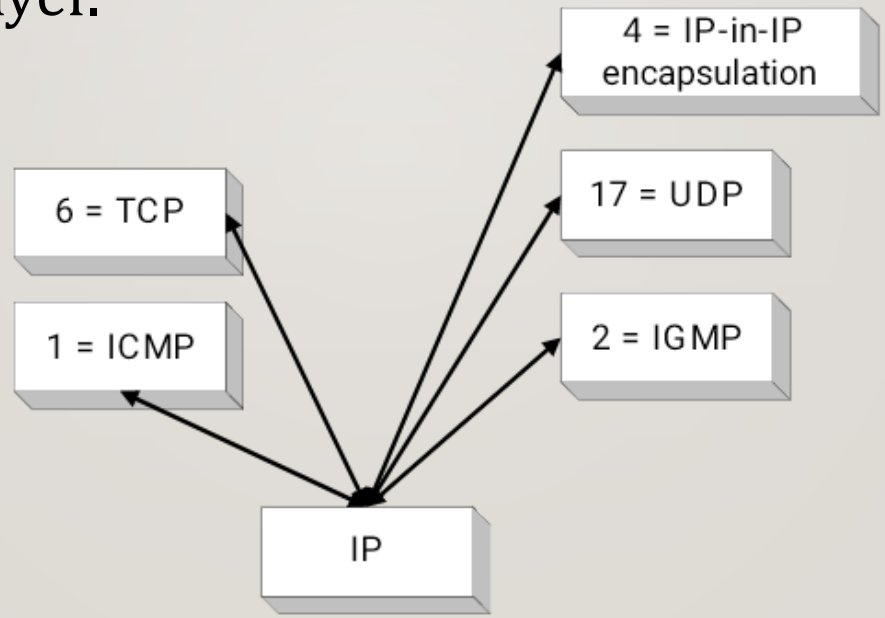
Fragmentation

- Fragmentation offset (13 bits): Offset of the payload of the current fragment in the original datagram



IPV4 Header Format

- **Protocol (8 bits):** defines the higher-level protocol that uses the services of the IP layer.



IPV4 Header Format

- **Header checksum (16 bits)**
  - IP is not a reliable protocol; it does not check whether the payload is corrupted during transmission.
  - Used to verify the header. It is recomputed at every router.
- **Source Address (32 bits)**
  - Indicate the IP address of the source machine.
- **Destination Address (32 bits)**
  - Indicate the IP address of the destination machine.

IPV4 Header Format

- **Options + Padding (0 to more)**
  - Options can be used for network testing and debugging.
  - It provides an escape to allow subsequent versions of the protocol to include information not present in the original design.

Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

Questions

- Q1. An IPV4 packet has arrived with the first 8 bits as (01000010)2 . The receiver discards the packet. Why?

  [Ans: invalid header length]

- Q2. In an IPV4 packet, the value of HLEN is (1000)2. How many bytes of options are being carried by this packet?

  [Ans: 12 bytes]

- Q3. In an IPV4 packet, the value of HLEN is 5 and the value of the total length field is (0028)16. How many bytes of data are being carried by this packet?

  [Ans: Total length= 40 bytes, Data size = 20 bytes]

Questions

- Q4. A packet has arrived with an MF bit value of 0. Is this the first fragment, the last fragment, or a middle fragment?

  [Ans: Last fragment]

- Q5. A packet has arrived with an MF bit value of 1 and a fragmentation offset value of 0. Is this the first fragment, the last fragment, or a middle fragment?

  [Ans: First fragment]

Questions

- Q6. A packet has arrived in which the offset value is 100. What is the number of the first byte?

  [Ans: 800]

- Q7. A packet has arrived in which the offset value is 100, the value of HLEN is 5, and the value of the total length field is 100. What are the numbers of the first byte and the last byte ?

  [Ans: first byte number= 800,

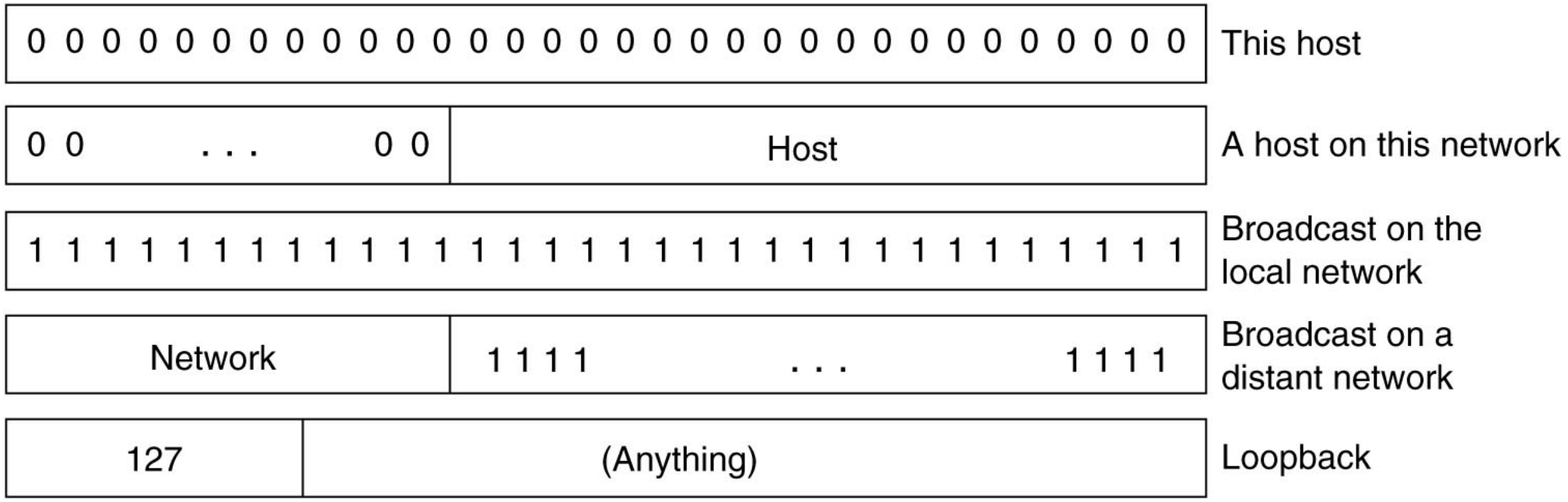
  80 bytes in the datagram, last byte number =879]

Private Address

- IP addresses are publicly registered with the Network Information Center (NIC) to avoid address conflicts.
- Devices that need to be publicly identified, must have a globally unique IP address and are assigned a public IP address.
- Devices that do not require public access (network printer) may be assigned a private IP address.
- For organizations to freely assign private IP addresses, NIC has reserved certain address blocks for private use.

Class	Range of Private Address
Class A	10.0.0.0 to 10.255.255.255
Class B	172.16.0.0 to 172.31.255.255

Special Addresses



THANK YOU!!!

COMPUTER NETWORKS MODULE 4.2

MS. JINCY J. FERNANDEZ

ASST. PROF, CSE

RSET

WHY ICMP?

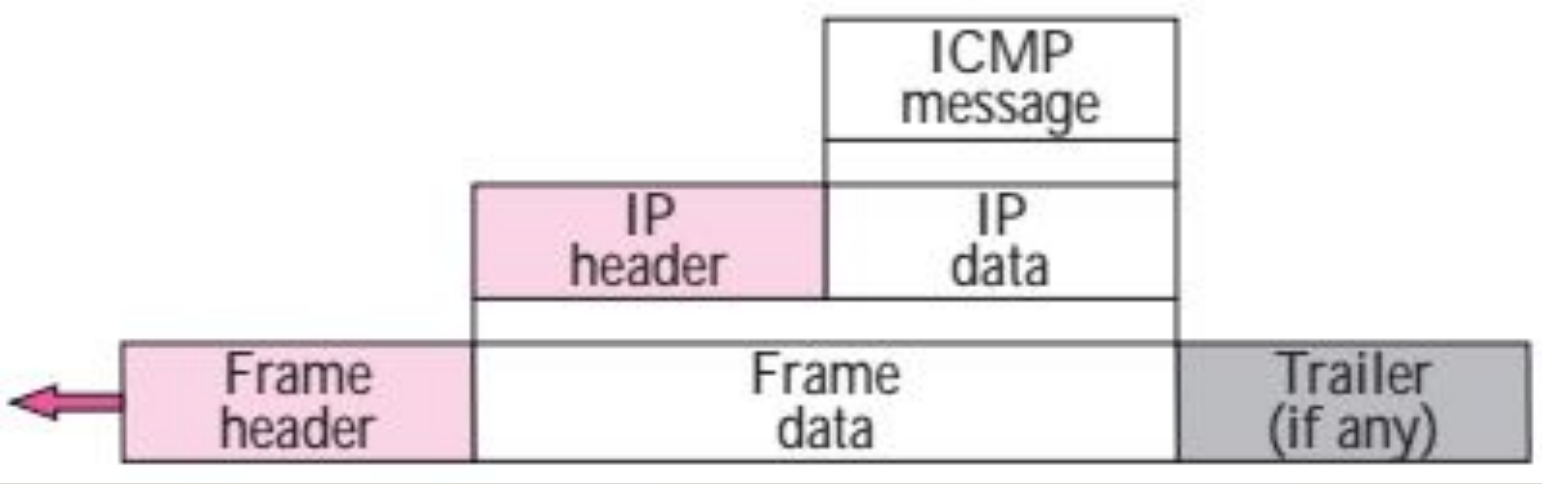
- The IP protocol has no error-reporting or error correcting mechanism.
- What happens if a router must discard a datagram because it cannot find a router to the final destination, or because the time-to-live field has a zero value?
- What happens if the final destination host must discard all fragments of a datagram because it has not received all fragments within a predetermined time limit?
- IP protocol has no built-in mechanism to notify the original host.

Introduction to ICMP

- Internet Control Message Protocol (ICMP)
- Companion to the IP protocol.
- Designed to compensate for the deficiencies of the IP protocol:
  - No error reporting or error correcting mechanism.
  - No mechanism for host and management queries.

Features

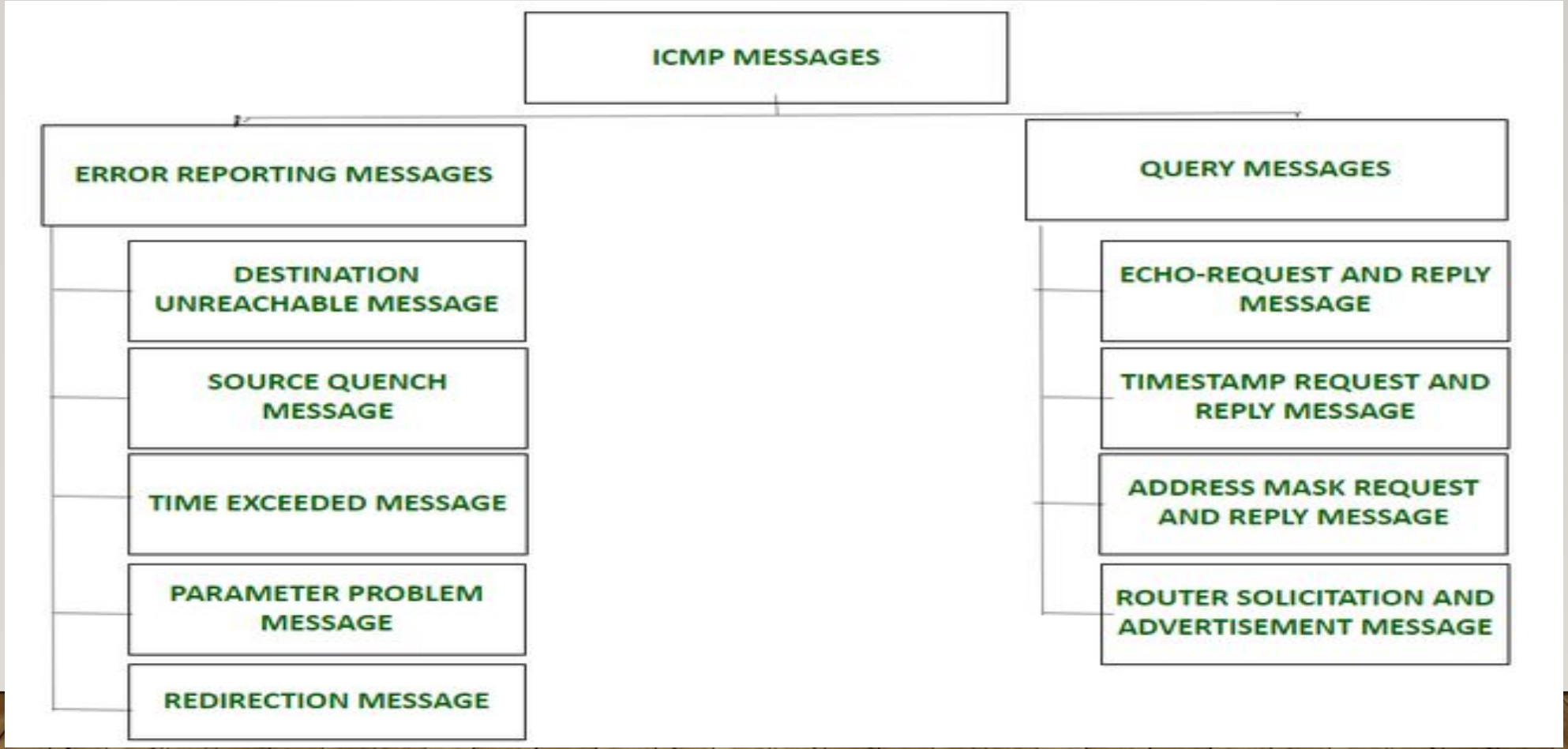
- ICMP messages are encapsulated within IP datagrams.
- Value in the protocol field is set to 1 for an ICMP message.



ICMP Messages

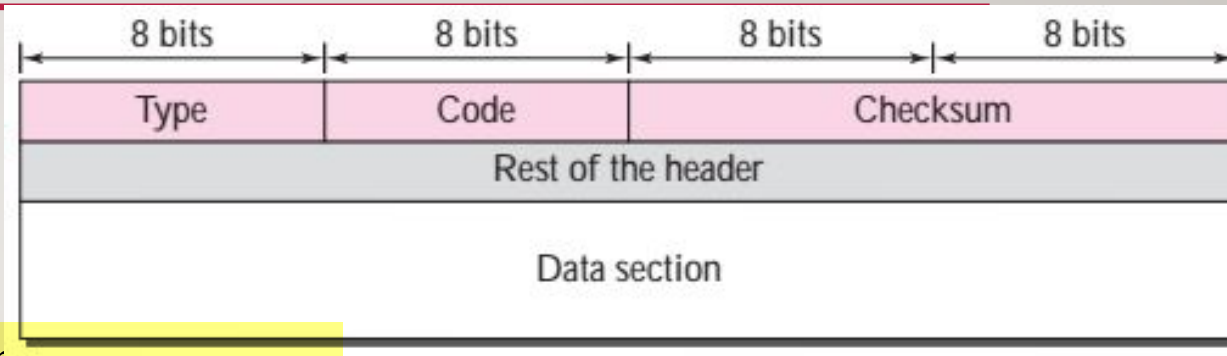
- Divided into two categories:
- Error reporting messages
  - Reports problems that a router or a host (destination) may encounter when it processes an IP packet.
- Query messages
  - Occurs in pairs.
  - Helps a host or a network manager get specific information from a router or another host.

ICMP Messages



Message Format

- 8-byte header and a variable size data section.



- ICMP Type: defines the type of the message.
- Code field: specifies the reason for the particular message type.
- Checksum field: for error control.
- Rest of the header: is specific for each message type.
- Data section: in error messages carries information for finding the original packet that had the error. In query messages, the data section carries extra information based on the type of the query.

Message Format

Category	Type	Message
Error Reporting messages	3	Destination Unreachable
	4	Source Quench
	11	Time Exceeded
	12	Parameter Problem
	5	Redirection
Query Messages	8 or 0	Echo Request or Reply
	13 or 14	Timestamp Request or Reply
	17 or 18	Address Mask Request & Reply
	9 or 10	Router-solicitation & Advertisement

ERROR REPORTING

Message Type- 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.

Message Type- Source Quench

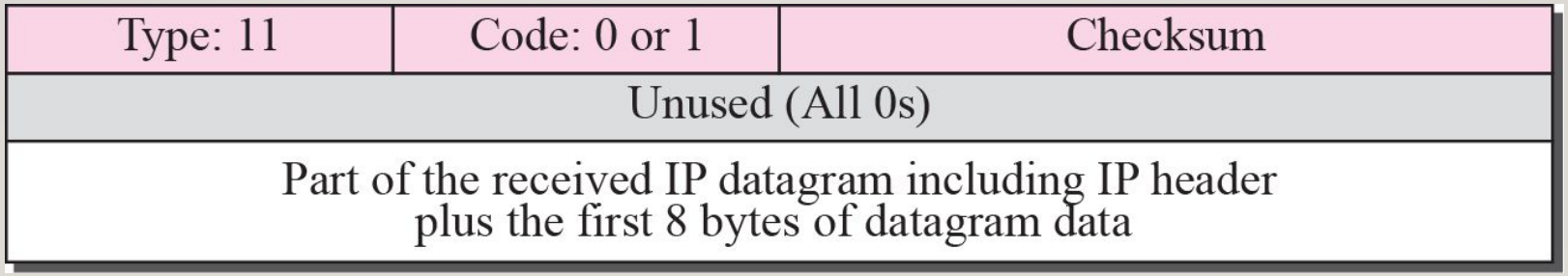
- Is a request to decrease the traffic rate.
- A source-quench message informs the source that a datagram has been discarded due to congestion in a router or the destination host.
- The source must slow down the sending of datagrams until the congestion is relieved.
- Take the source IP address from the discarded packet and informs the source by sending a source quench message.

Message Type- Time Exceeded

- Each datagram contains a field called *time to live*. When a datagram visits a router, the value of this field is decremented by 1.
- Whenever a router decrements a datagram with a time-to-live value to zero, it discards the datagram and sends a time-exceeded message to the original source.
- When the final destination does not receive all of the fragments in a set time, it discards the received fragments and sends a time-exceeded message to the original source.

Message Type- Time Exceeded

- Code 0 - by routers to show that the value of the time-to-live field is zero.
- Code 1 - by the destination host to show that not all of the fragments have arrived within a set time.



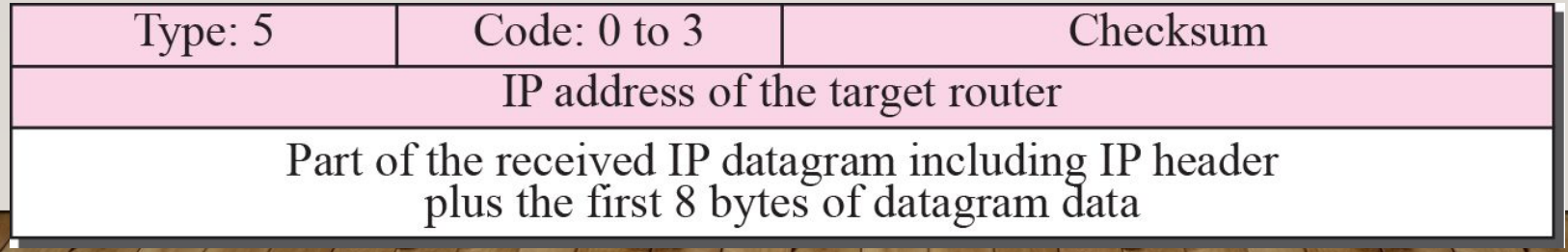
Message Type- Parameter Problem

- 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.

- Can be created by a router or a destination host.
- E.g. checksum error

Message Type- Redirection

- Used in the building of routing tables of hosts.
- Used when the source uses a wrong router to send out its message. The router informs the source that it needs to change its default router in the future.
- For efficiency, hosts do not take part in the routing update process because there are many more hosts in an internet than routers.
- Updating the routing tables of hosts dynamically produces unacceptable traffic. Hence the hosts usually use static routing with help of routers.



QUERY MESSAGE

Message Type- Echo Request And Echo Reply

- An echo-request message can be sent by a host or router.
- An echo-reply message is sent by the host or router that receives an echo-request message.
- Echo-request and echo-reply messages can be used by network managers to check the operation of the IP protocol.
- Echo-request and echo-reply messages can test the reachability of a host.
- This is usually done by invoking the ping command.
- It is used to ping a message to another host that “Are you alive”.

Message Type- Echo Request and Echo Reply

Type 8: Echo request
Type 0: Echo reply

Type: 8 or 0	Code: 0	Checksum
Identifier		Sequence number
Optional data Sent by the request message; repeated by the reply message		

Message Type- Time Stamp Request and Reply

- Timestamp-request and timestamp-reply messages can be used to calculate the round-trip time between two devices or to check whether the clocks in two devices are synchronized.
- The timestamp request message sends a 32-bit number □ defines the time the message is sent.
- The timestamp reply resends that number and two new 32-bit numbers representing the time the request was received and the time the response was sent.
- The sender can calculate the one way and round-trip time.

Message Type- Address Mask Request & Reply

- A host may know its IP address, but it may not know the corresponding mask.
- 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.

Message Type- Router-solicitation & Advertisement

- A host can broadcast (or multicast) a router-solicitation message.
- The router or routers that receive the solicitation message broadcast their routing information using the router-advertisement message.
- Router Advertisement message is sent by a router on the local area network to announce its IP address as available for routing.
- A router can also periodically send router-advertisement messages even if no host has solicited.
- When a router sends out an advertisement, it announces not only its own presence but also the presence of all routers on the network of which it is aware.

THANK YOU!!!

COMPUTER NETWORKS MODULE 4.3

MS. JINCY J FERNANDEZ

ASST. PROF, CSE

RSET

Logical Addresses

- An Internet is a combination of physical networks.
- The physical networks are connected together by routers.
- The hosts and routers are recognized at the network level by their logical addresses.
- Logical address is unique globally.
- Logical addresses are the IP addresses – 32 bits long.

Physical Addresses

- At the physical level the hosts are recognized by their physical addresses.
- Physical address is the local address.

- 48-bit MAC address in the Ethernet
- Delivery of a packet to a host or a router requires two levels of addressing: logical and physical.

Issues with IP address

- IP addresses are not sufficient for sending packets.
- Data link layer NICs do not understand IP addresses.
- Every NIC equipped with 48-bit Ethernet address.
- NICs send and receive frames based on 48-bit Ethernet address.
- Need to map a logical address to its corresponding physical address and vice versa.
- Mapping is of two types:
  - Static Mapping
  - Dynamic Mapping

Static Mapping

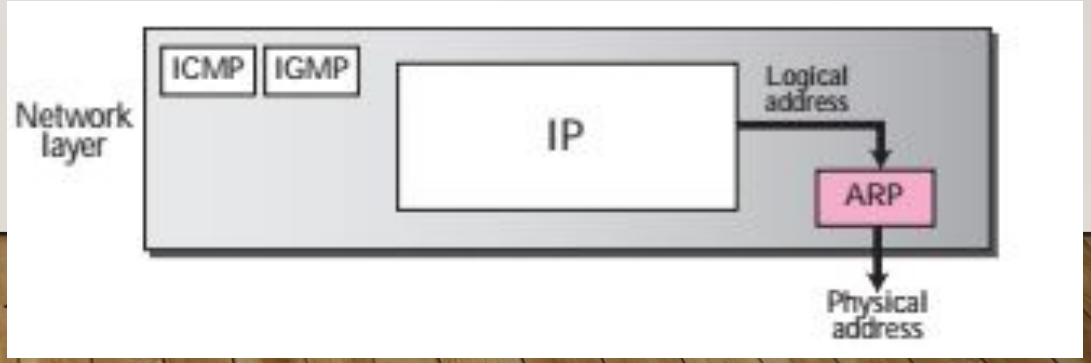
- Table which associates a logical address to a physical address is stored in each machine.
- Limitations
  1. A machine could change its NIC, resulting in a new physical address.
  2. In some LANs, the physical address changes every time the computer is turned on.
  3. A mobile computer can move from one physical network to another, resulting in a change in its physical address.
  - Static mapping table has to be updated periodically.
  - It can affect network performance.

Dynamic Mapping

- Each time a machine knows the logical address of another machine it uses a protocol to find the physical address and vice versa.
- Two protocols are designed to perform dynamic mapping are:
- Address Resolution Protocol (ARP)
  - ARP maps a logical address to a physical address
- Reverse Address Resolution Protocol (RARP)
  - RARP maps a physical address to a logical address

Address Resolution Protocol (ARP)

- IP datagram has to be encapsulated in a frame and passed to the physical network.
- Sender needs the physical address of the receiver but it knows only the logical address of the receiver.
- ARP accepts a logical address from the IP protocol, maps the address to the corresponding physical address and pass it to the data link layer.

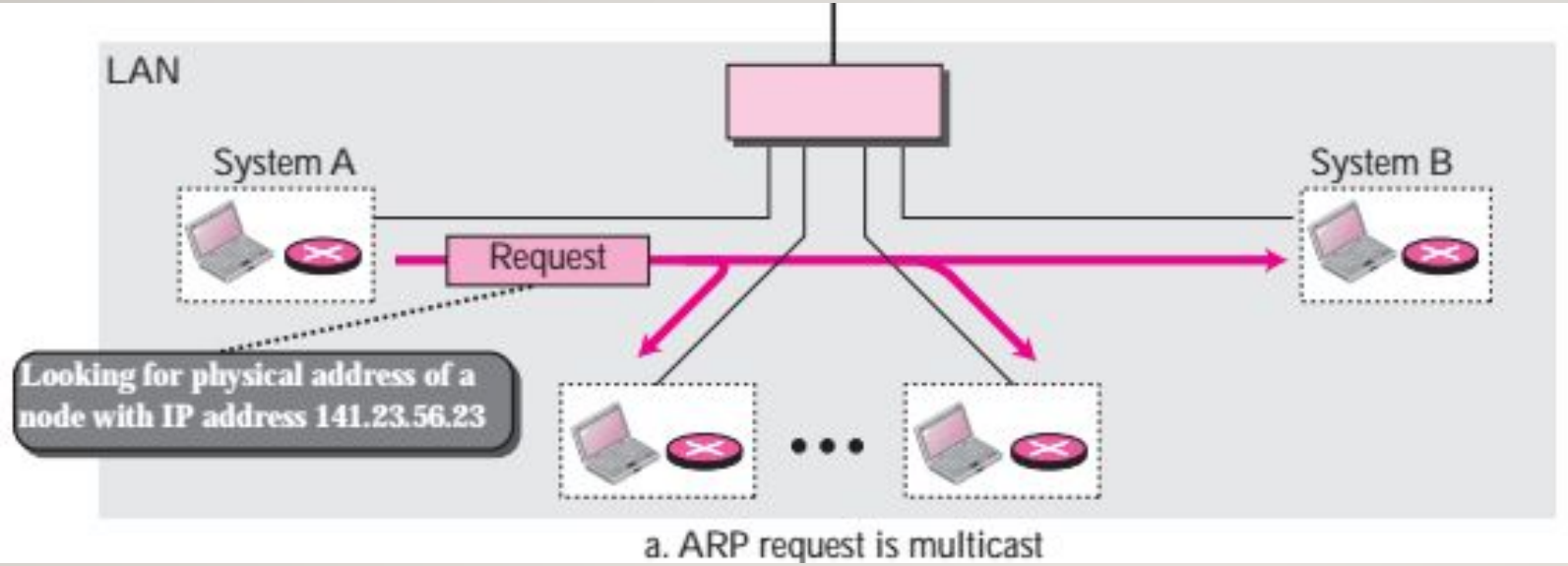


ARP Process

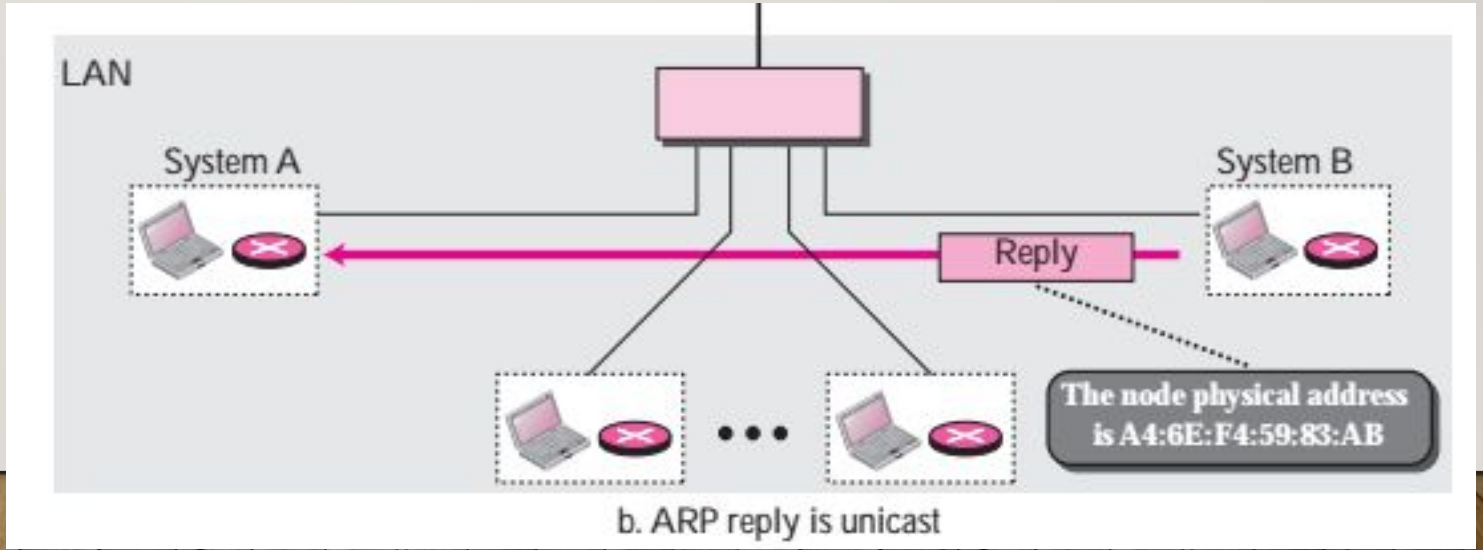
- Anytime a host, or a router, needs to find the physical address of another host it sends an ARP request packet.
- The packet includes the physical and IP addresses of the sender and the IP address of the receiver.
- Broadcast ARP request.

Arp Process

- Every host or router on the network receives and processes the ARP request packet.
- Only the intended recipient recognizes its IP address and sends back an ARP response packet.
- The response packet contains the recipient's IP and physical addresses.
- The packet is unicast directly to the inquirer using the physical address received in the query packet.

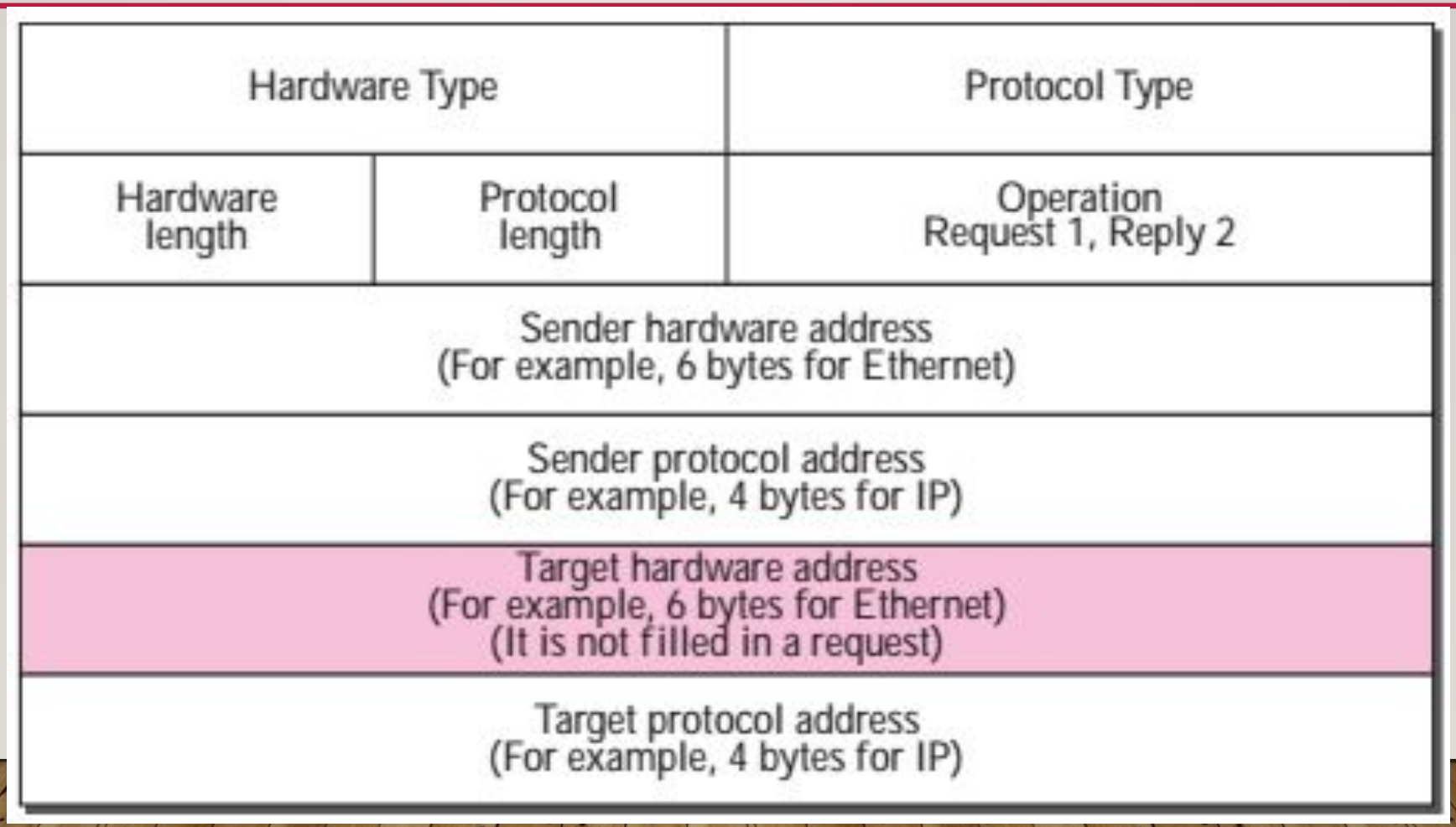


a. ARP request is multicast



b. ARP reply is unicast

ARP Packet Format



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 – e.g. Ethernet is given the type 1.
- Protocol type
  - This is a 16-bit field defining the protocol.
  - For example, the value of this field for the IPv4 protocol is $(0800)_{16}$.
- 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.

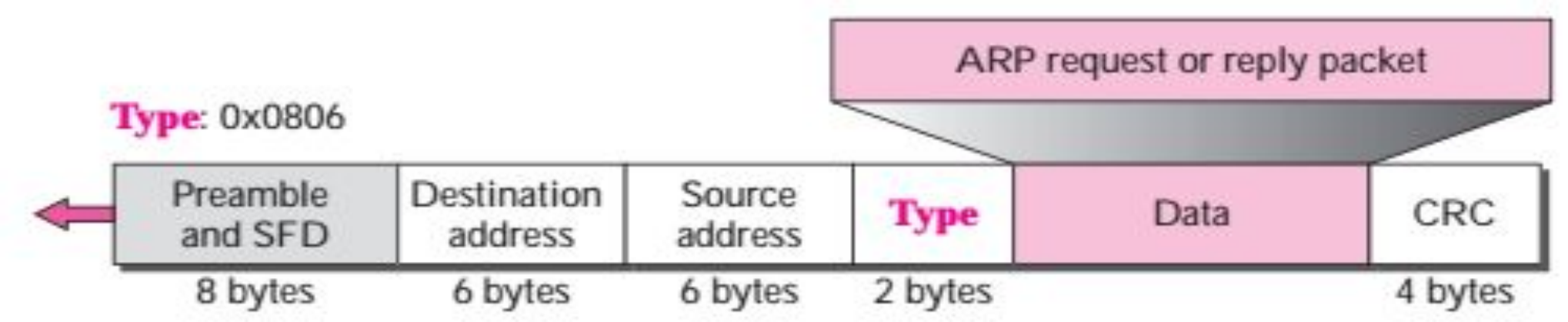
ARP Packet Format

- 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) and ARP 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.

ARP Packet Format

- Sender protocol address
  - This is a variable-length field defining the logical (for example, IP) address of the sender.
- Target hardware address
  - This is a variable-length field defining the physical address of the target.
  - In an ARP request message, this field is all 0s because the sender does not know the physical address of the target.
- Target protocol address
  - This is a variable-length field defining the logical address of the target.

Encapsulation of an ARP Packet



- An ARP packet is encapsulated in an Ethernet frame

Steps in an ARP Process

1. The sender knows the IP address of the target.
2. IP asks ARP to create an ARP request message, filling in :
   - The sender physical address, the sender IP address, and the target IP address
   - The target physical address field is filled with 0s
3. The message is passed to the data link layer where it is encapsulated in a frame using the physical address of the sender as the source address and the physical broadcast address as the destination address

Steps in an ARP Process

4. Every host or router receives the frame, because the frame contains a broadcast destination address
   - All machines except the one targeted drop the packet
   - The target machine recognizes the IP address

5. The target machine replies with an ARP reply message that contains its physical address
   - The message is unicast

Steps in an ARP Process

6. The sender receives the reply message
   - It now knows the physical address of the target machine
7. The IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination

RARP

- Given an Ethernet address, what is the corresponding IP address?
- Use RARP- Reverse ARP.
- This protocol allows a newly booted workstation to broadcast its Ethernet address.
- RARP server sees this request, looks up the Ethernet address in its configuration files, and sends back the corresponding IP address

Disadvantage

- RARP server is needed on all networks.
- RARP can provide only IP address, no information on subnet mask, IP address of router, IP address of file server etc.
- Broadcast messages will be blocked by certain routers.

- So go for an alternative Protocol:
  - **BOOTP**

BOOTP

- It is a client-server protocol designed to overcome deficiencies of RARP protocol.
- It can run anywhere in the Internet.
- BOOTP uses UDP messages, which are forwarded over routers.
- Provides a diskless workstation with all information like:
  - IP address of the file server
  - IP address of the default router
  - Subnet mask

Disadvantage of BOOTP

- It is a static configuration protocol.
- Requires manual configuration of tables mapping IP address to Ethernet address.
- Administrator has to assign an IP address and enter mapping of (Ethernet Address, IP Address) into the BOOTP configuration tables.
- So go for an extended version named as **DHCP.**
- **Dynamic Host Configuration Protocol**

Dynamic Host Configuration Protocol(DHCP)

- Large organizations or ISP receive block of addresses from ICANN(Internet Corporation for Assigned Names and Numbers)
- Small organizations receive block of addresses from ISP.
- Network administrator manually assign the IP addresses to the hosts or routers tedious and error prone.

Dynamic Host Configuration Protocol(DHCP)

- Address assignment in an organization can be done automatically using DHCP.
- Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.
- With DHCP, every network must have a DHCP server that is responsible for configuration.

DHCP - Working

- A newly booted machine broadcasts a DHCP DISCOVER packet. It must reach the DHCP server.
- Router will be configured to receive DHCP broadcasts and relay them to the DHCP server.
- For this, the router should be aware of the IP address of the DHCP server.
- When the server receives the packet, it allocates a free IP address and sends it to the host in a DHCP OFFER packet

DHCP

- Issue with automatic assignment is how long an IP address should be allocated?
  - If a host leaves a network and does not return its IP address to the DHCP server, the address will be permanently lost.
- Leasing: technique of assigning an IP address for a fixed period of time.
- Just before the lease expires, the host must ask for a DHCP renewal.

ADVANTAGES OF DHCP

- **Reliable IP address configuration.**
  - DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.
- **Reduced network administration.**
  - Centralized and automated TCP/IP configuration.

Configuration

- Automatic allocation—The DHCP server assigns a permanent IP address to a client from its IP Pools. On the firewall, a Lease specified as Unlimited means the allocation is permanent.
- Dynamic allocation—The DHCP server assigns a reusable IP address from IP Pools of addresses to a client for a maximum period of time, known as a lease. This method of address allocation is useful when the customer has a limited number of IP addresses; they can be assigned to clients who need only temporary access to the network.
- Static allocation—The network administrator chooses the IP address to assign to the client and the DHCP server sends it to the client. A static DHCP allocation is permanent. The DHCP assignment remains in place even if the client logs off, reboots, has a power outage, etc.

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

THANK YOU!!!

COMPUTER NETWORKS MODULE 4.4

MS. JINCY J FERNANDEZ

ASST. PROFESSOR

RSET

Terminologies

- The Internet is divided into hierarchical domains called Autonomous Systems (ASs).
- Autonomous System is a set of networks which share common routing polices, e.g. AT&T.
  - A large corporation that manages its own network and has full control over it, is an autonomous system.
  - A local ISP that provides services to local customers is an autonomous system.

Autonomous System

- Autonomous Systems are divided into three categories:

1. Stub AS
   - A stub AS has only one connection to another AS.
   - A stub AS is either a source or a sink.
   - The hosts in the AS can send data traffic to other AS and can receive data coming from hosts in other AS.
   - Data traffic cannot pass through a stub AS.
   - An example of a stub AS is a small corporation or a small local ISP.

Autonomous System

2. Multihomed AS

- Has more than one connection to other AS.
- It is still only a source or sink for data traffic - can receive data from more than one AS and can send data to more than one AS.
- There is no transient traffic - does not allow data coming from one AS and going to another AS to pass through.
- An example is a large corporation that is connected to more than one regional or national AS that does not allow transient traffic.

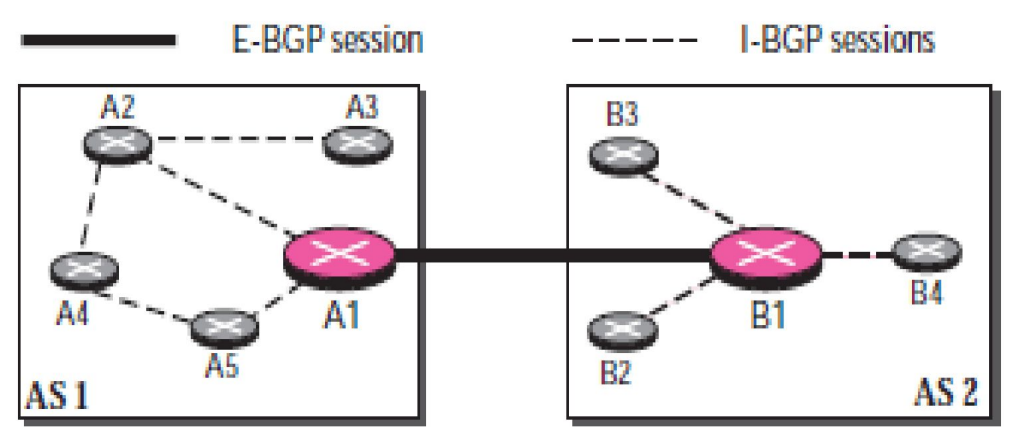
Autonomous System

3. Transit AS

- A transit AS is a multihomed AS that also allows transient traffic
- Examples of transit ASs are national and international ISPs.

Gateway Protocols

- Interior Gateway Protocols are routing protocols within an Autonomous System, e.g. RIP, OSPF
- Exterior Gateway Protocols are routing protocols used between Autonomous Systems, e.g. BGP
  - E-BGP session
    - To exchange info between two different AS.
  - I-BGP session
    - To exchange info within the same AS.



Collect info using I-BGP and exchange using E-BGP.

BGP- Border Gateway Protocol

- Interdomain protocol (exterior gateway protocol).
- Distance vector protocol for routing between different Autonomous Systems.
- BGP uses a TCP connection to exchange information between peers.
- Policy based:
  - A corporate AS might be unwilling to carry transit packets originating in a foreign AS and ending in a different foreign AS, even if its own AS is on the shortest path between the two foreign AS.
  - On the other hand, it might be willing to carry transit traffic for its neighbors, or even for specific other AS that paid it for this service.

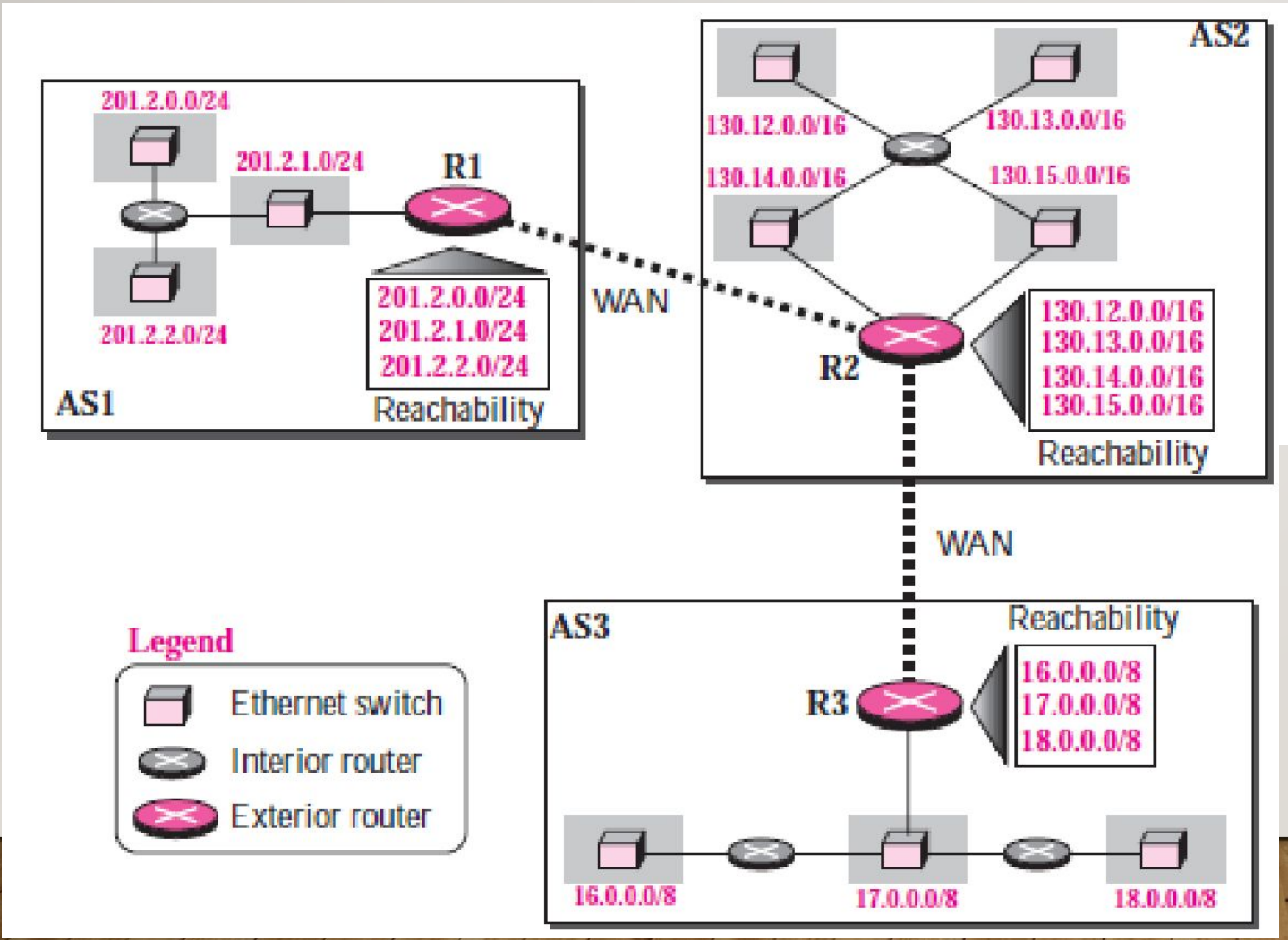
BGP

- Routing policy is implemented by deciding what traffic can flow over which of the links between AS.
- One common policy is that a customer ISP pays another provider ISP to deliver packets to any other destination on the Internet and receive packets sent from any other destination.
- The customer ISP is said to buy transit service from the provider ISP.

BGP

- Each BGP router keeps track of the exact path to reach the destination not just the cost .
- Instead of periodically giving each neighbor its estimated cost to each destination, each BGP router tells its neighbors the path it is using to reach each destination.
- BGP solves the count to infinity problem as whole path is known.

BGP USES PATH VECTOR ROUTING



R1

Network	Path
201.2.0.0/24	AS1 (This AS)
201.2.1.0/24	AS1 (This AS)
201.2.2.0/24	AS1 (This AS)
130.12.0.0/16	AS1, AS2
130.13.0.0/16	AS1, AS2
130.14.0.0/16	AS1, AS2
130.15.0.0/16	AS1, AS2
16.0.0.0/8	AS1, AS2, AS3
17.0.0.0/8	AS1, AS2, AS3
18.0.0.0/8	AS1, AS2, AS3

Path-Vector Routing Table

R2

Network	Path
201.2.0.0/24	AS2, AS1
201.2.1.0/24	AS2, AS1
201.2.2.0/24	AS2, AS1
130.12.0.0/16	AS2 (This AS)
130.13.0.0/16	AS2 (This AS)
130.14.0.0/16	AS2 (This AS)
130.15.0.0/16	AS2 (This AS)
16.0.0.0/8	AS2, AS3
17.0.0.0/8	AS2, AS3
18.0.0.0/8	AS2, AS3

Path-Vector Routing Table

R3

Network	Path
201.2.0.0/24	AS3, AS2, AS1
201.2.1.0/24	AS3, AS2, AS1
201.2.2.0/24	AS3, AS2, AS1
130.12.0.0/16	AS3, AS2
130.13.0.0/16	AS3, AS2
130.14.0.0/16	AS3, AS2
130.15.0.0/16	AS3, AS2
16.0.0.0/8	AS3 (This AS)
17.0.0.0/8	AS3 (This AS)
18.0.0.0/8	AS3 (This AS)

Path-Vector Routing Table

EXAMPLES

- Consider the routing table of F.
- After all path information come from the neighbors F examines them to get the best.
- It discards paths from I and E, as they pass through F itself.
- Choice remains between B and G.
- Every BGP router contains a module to examine routes and score them.
- The scoring will consider policy violations as well.

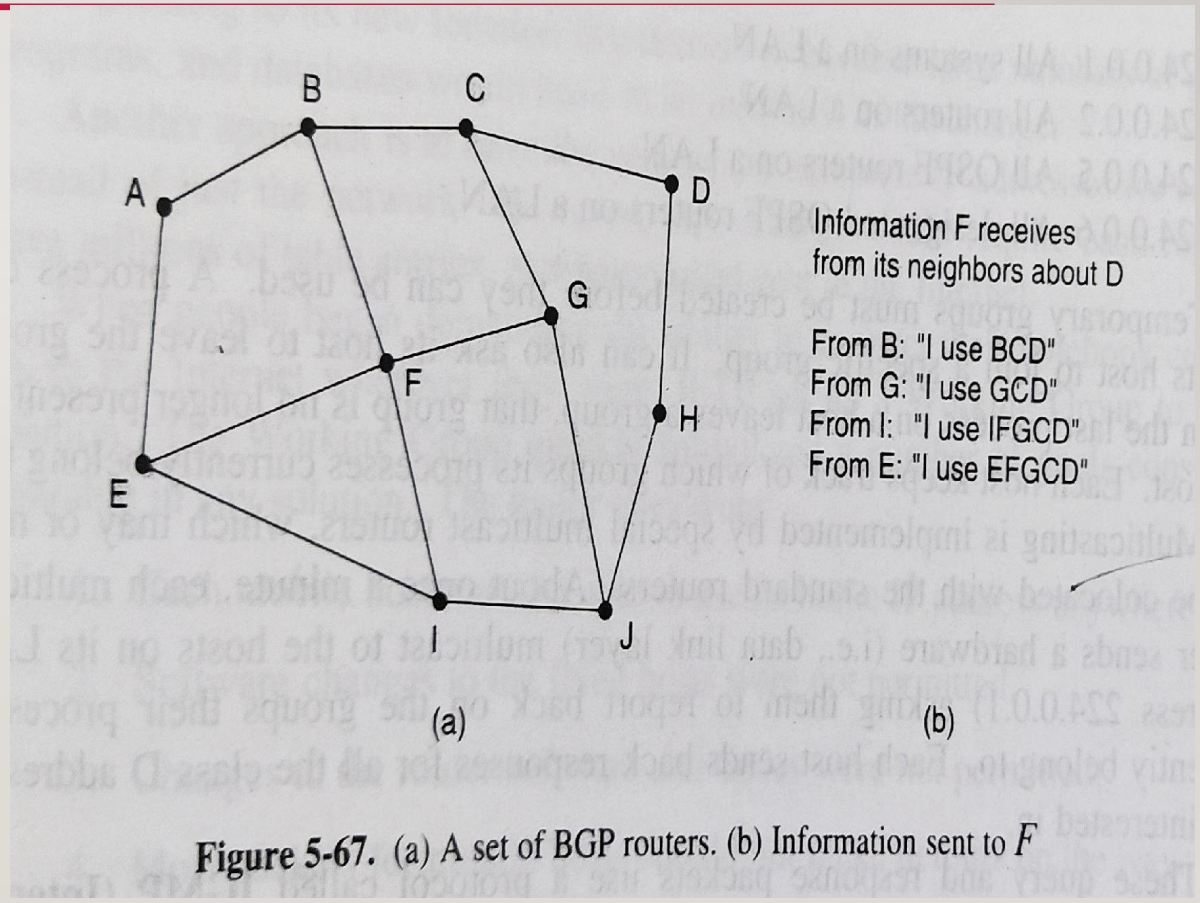


Figure 5-67. (a) A set of BGP routers. (b) Information sent to *F*

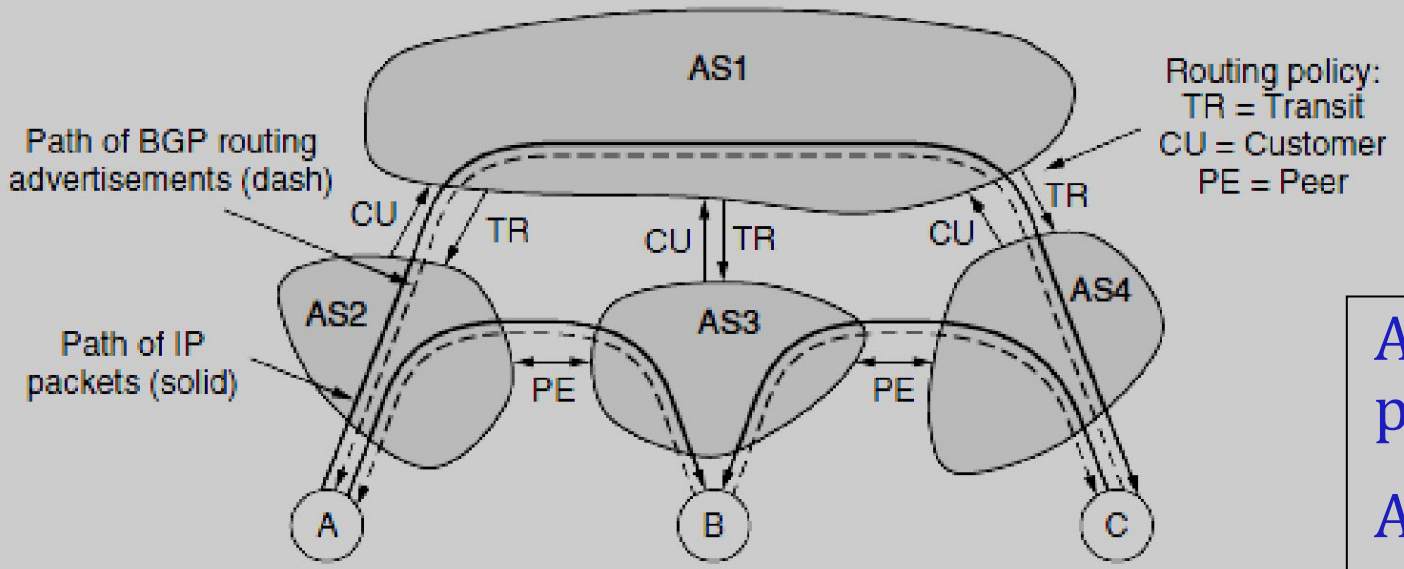


Figure 5-67 Routing policies between four autonomous systems

- Transit
- AS2, AS3 and AS4 are customers of AS1 and buy transit service from AS1.
- Suppose source A wants to send packets to C.
- AS4 advertises C as a destination to its transit provider AS1.
- AS1 now advertises a route to C to its other customers.

AS2 now knows that it can send a packet to C via AS1(paid).

A – AS2 – AS1 – AS4 – C

Peering

AS2 and AS3 can send traffic directly to each other for free.

Two AS send routing advertisements to each other for addresses that reside in their network.

A - AS2 - AS3 – B

But a packet from A to C should be send through the transit.

COMPUTER NETWORKS MODULE 4.5

MS. JINCY J FERNANDEZ

ASST. PROFESSOR

RSET

INTERNET MULTICASTING

- Normal IP Communication: between one sender and one receiver.
- However, for some applications, it is useful for a process to able to send to large number of receivers simultaneously.
  - Updating distributed systems.
- IP supports multicasting using class D address.
- Each class D identifies a group of hosts.

INTERNET MULTICASTING

- When a process sends a packet to a class D address, best attempt is made to deliver it to all the members of the group addressed. But no guarantee.
- Two kinds of group addresses are supported: Temporary and Permanent.
- Permanent:
  - Always there and does not need to setup.
  - Each permanent group has a permanent group address.
  - E.g. 224.0.0.1 □ all systems on a LAN

    224.0.0.2 □ all routers on a LAN

    224.0.0.5 □ all OSPF routers on a LAN

INTERNET MULTICASTING

- Temporary:
  - Must be created before they can be used
  - A process can ask its host to join or leave the group.
  - Each group keep tracks of which groups its process currently belongs to.
  - About once a minute, each multicast router sends a query packet to all the hosts on its LAN asking them to report back on the groups to which they currently belong.
  - Each host sends back responses for all the class D addresses it is interested in.
  - These query and response packets use a protocol called IGMP (**Internet Group Management Protocol**)

IPV6

- Main reason for migration from IPV4 to IPV6 is the small size of the address space in IPV4.
- Uses 128 bit addresses.

IPV6

- Representations
  - Binary notation: 128 bits
  - Colon hexadecimal notation: divides the address into eight sections, each made of four hexadecimal digits separated by colons; FEF6:BA98:7654:3210:ADEF:BBFF:2322:FF00
  - CIDR notation: IPV6 uses hierarchical addressing; FDEC::BBFF:0:FFFF/60

IPV6

- Abbreviation:
  - Abbreviate the address if many of the digits are zeros.
  - 0074 74; 000F F; 0000 0
- Zero compression:
  - Applied to colon hex notation if there are consecutive sections of zeros only.
  - Remove all the zeros and replace them with a double semicolon.
  - FDEC:0:0:0:0:BBFF:0:FFFF FDEC::BBFF:0:FFFF
  - zero compression with **a double colon can be applied only once.**

IPV6

- Address Space
  - 2^{128} addresses
  - No address depletion
- Expand the address 0:16::1:12:1214

Ans: 0000:0016:0000:0000:0000:0001:0012:1214

IPV6- ADDRESS SPACE ALLOCATION

- Like IPV4, the address space of IPV6 is divided into several blocks of varying size and each block is allocated for a special purpose.

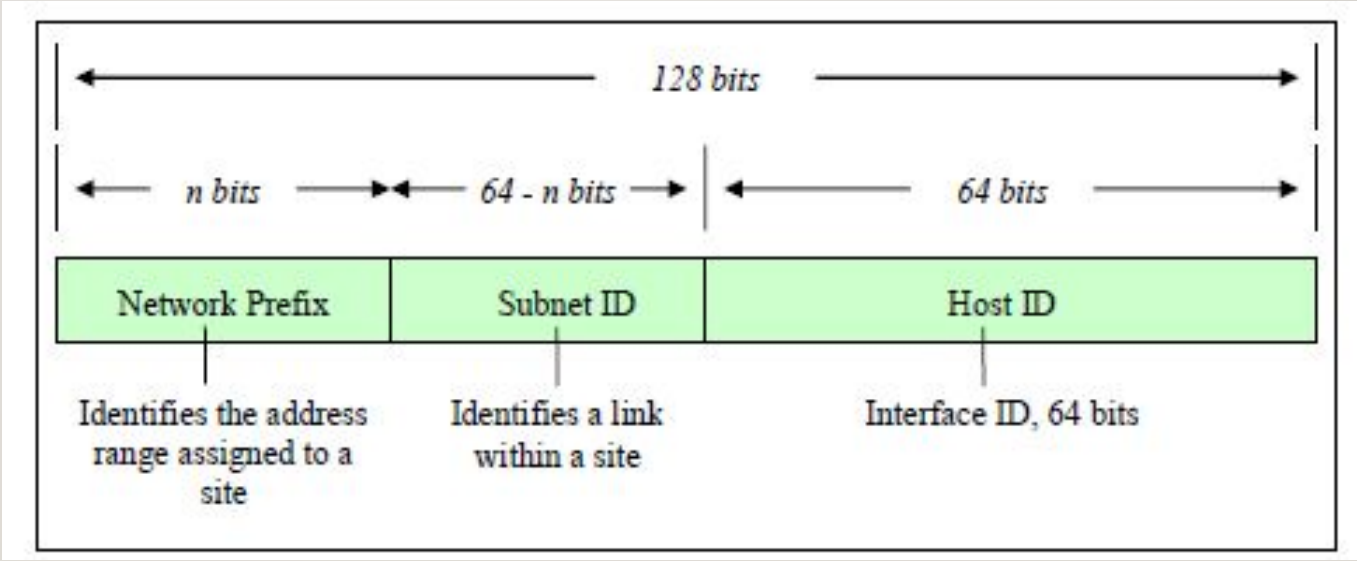
Block prefix	*CIDR*	*Block assignment*
0000 0000	0000::/8	Special addresses
001	2000::/3	Global unicast
1111 110	FC00::/7	Unique local unicast
1111 1110 10	FE80::/10	Link local addresses
1111 1111	FF00::/8	Multicast addresses

IPV6- ADDRESS SPACE ALLOCATION

- Global unicast addresses:
  - For one-to-one communication between two hosts in the Internet.
  - Size of this block is 2^{125} bits.
  - Address in this block is divided into global routing prefix, subnet identifier and interface identifier.
    - Global routing prefix: to route the packet through the internet to the organization site.
      - First 3 bits are fixed (001), rest of the 45 bits can define up to 2^{45} sites.
    - Subnet identifier: define a subnet in an organization; can have up to 2^{16}= 65536 subnets.
    - Interface identifier: similar to host id in IPV4.

IPV6 - ADDRESS SPACE ALLOCATION

- Global unicast addresses:



IPV6- ADDRESS SPACE ALLOCATION

- Other assigned blocks
  - IPV6 uses two large blocks for private addressing (unique local unicast and link local block) and one large block for multicasting.

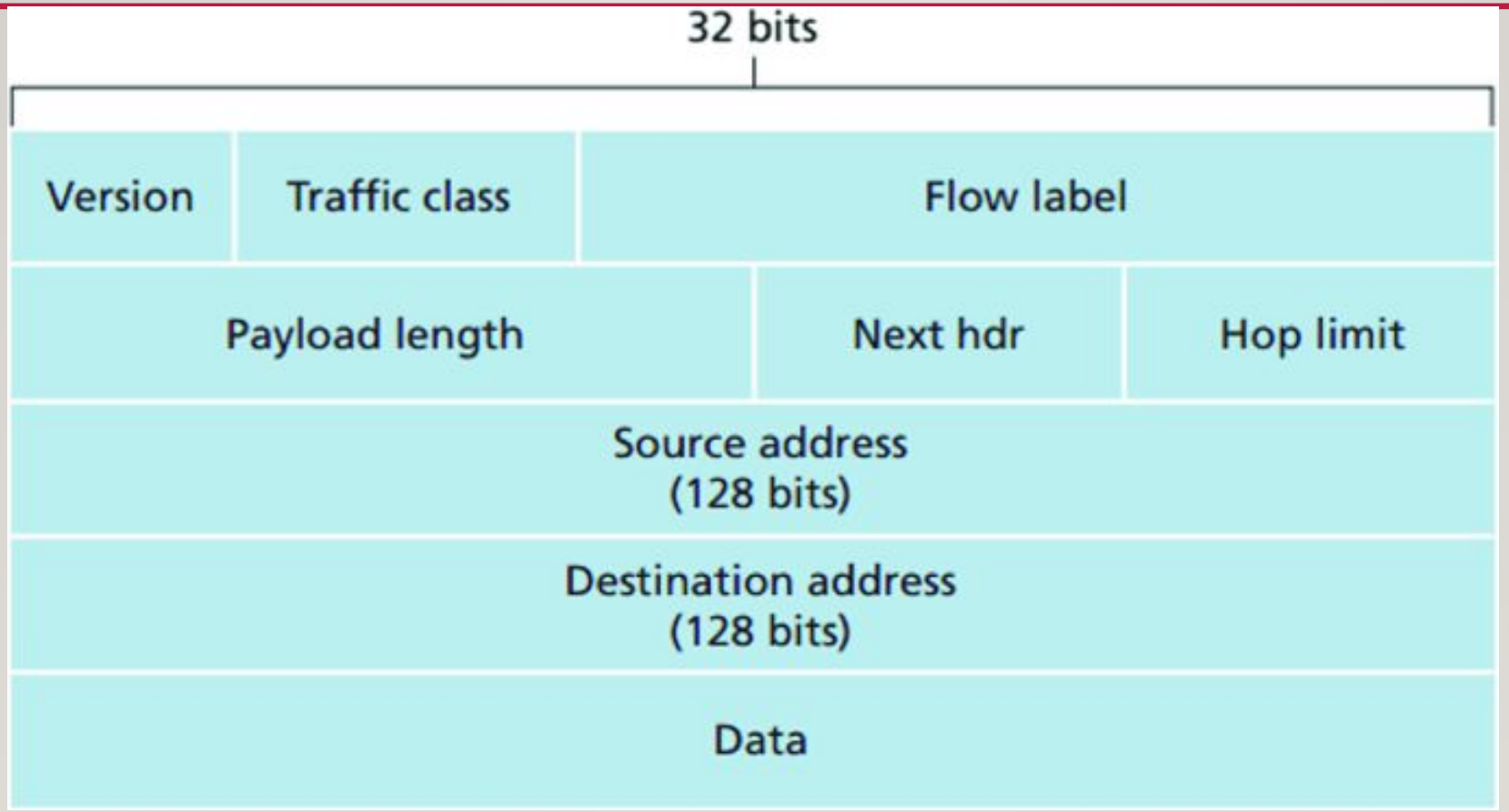
~~IPV6- ADDRESS SPACE ALLOCATION~~

- During the transition from IPV4 to IPV6, hosts can use their IPV4 addresses embedded in IPV6 addresses.
- Two formats for this:
  - Compatible address: address of 96 zero bits followed by 32 IPV4 address.
  - Mapped address: used when a computer already migrated to IPV6 wants to send a message to another computer using IPV6.

IPV6- DATAGRAM FORMAT

- Changes in IPV6 protocol:
  - Better header format: Options are separated from the base header and inserted (when needed) between the base header and data.
  - New options: for additional functionalities.
  - Allowance for extension: designed to allow the extension of the protocol if required by new technologies or applications.
  - Support for resource allocation: instead of type of service field, traffic class and flow label fields have been added to enable the source to request special handling of the packet.
  - Support for more security: Encryption and authentication options in IPV6 provide confidentiality and integrity of the packet.

IPV6- DATAGRAM FORMAT



IPV6- DATAGRAM FORMAT

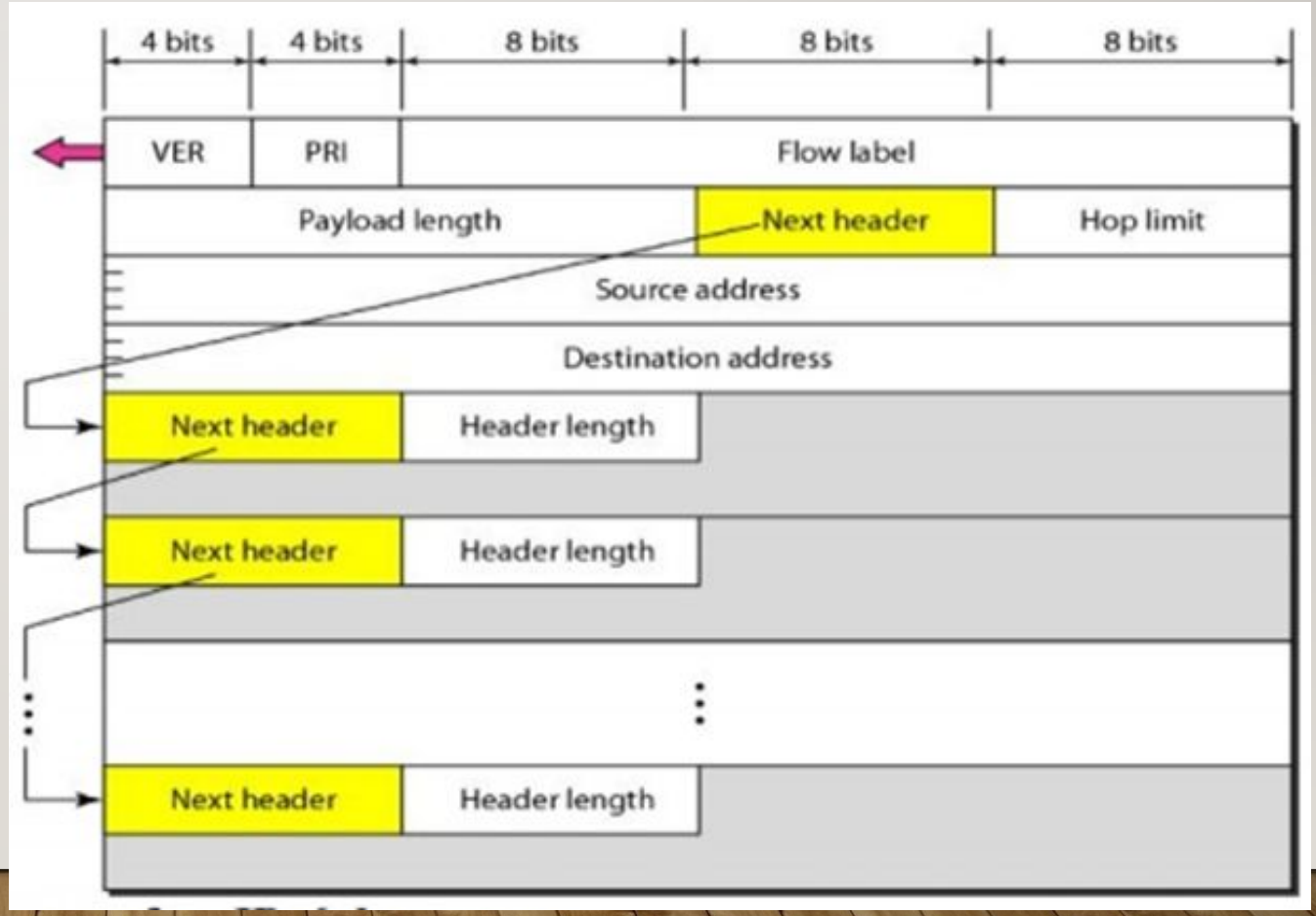
- Version: 4- bit field with value 6.
- Traffic Class: 8- bit field; distinguish different payloads with different delivery requirements. It replaces the type of service field in IPv4 (PRIORITY)
- Flow label: 20-bit field; handles flow of data.
- Payload length: 16- bit field; defines the length of the IP datagram excluding the header.
  - Length of the base header is fixed (40byes)

IPV6- DATAGRAM FORMAT

- Next header: 8-bit field defining the type of the first extension header (if present) or the type of the data that follows the base header in the datagram; similar to protocol field in IPV4.
- Hop limit: 8-bit field; same as TTL field in IPV4.
- Source and Destination addresses: 16- byte; defines the source and destination of the datagram.
- Payload: has a different format and meaning.

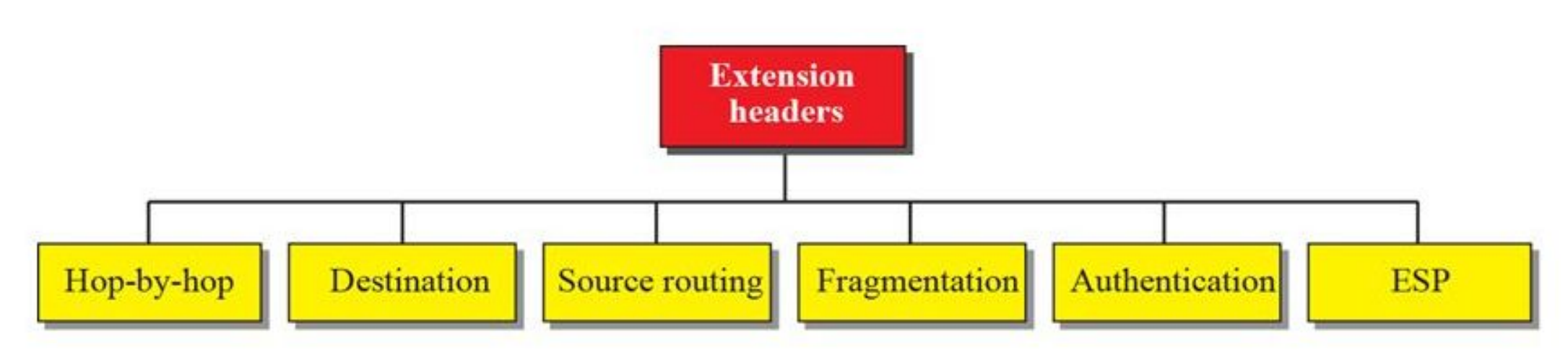
IPV6- DATAGRAM FORMAT

- Payload: has a different format and meaning.
- Payload means a combination of zero or more extension headers followed by the data from other protocols.
- Each extension header has two mandatory fields: next header and length followed by information related to the particular option.



IPV6- DATAGRAM FORMAT

- Extension header:
  - IPV6 packet base header and some extension headers.
  - The length of the base header is fixed at 40 bytes.
  - Maximum 6 extension headers.



IPV6- DATAGRAM FORMAT

- Extension header:
  - Hop by hop option: used when source needs to pass information to all routers visited by the datagram.
  - Destination option: used when the source needs to pass information to the destination only. Intermediate routers are not permitted access to this information.
  - Source Routing: combines the concepts of the strict source route and loose source route options in IPV4.

IPV6- DATAGRAM FORMAT

- Extension header:
  - Fragmentation: IPV6 datagrams can be fragmented only by the source, not by the routers. Reassembly takes place at the destination. The fragmentation of the packets at the router is not allowed to speed up the processing of packets in the router.
  - Authentication: it validates the message sender and ensures the integrity of data.
  - ESP(Encrypted Security Payload): provides confidentiality and guards against eavesdropping.