CN (IT-3001)

Network Layer: Protocols Associated to Network Layer

Prof. Amit Jha

School of Electronics Engineering (SOEE)

KIIT Deemed to be University

Objectives

- The objective of this module is to discus following concepts…
  1. NAT
  2. DHCP
  3. ARP
  4. ICMP
  5. IPv6

To be discussed….

- Network Address Translation (NAT)
- Methods to allocate the IP address
  - Static
  - Dynamic→ DHCP
- Address Mapping
  - From logical address to physical address
  - From Physical address to logical address
- Error reporting
  - ICMP…… Unicast application
  - IGMP……Multicast application

Special addresses from the set of IP Addresses

- The following groups has special IP addresses for special purpose:
- ***This-host Address:*** The only address in the block **0.0.0.0**/32 is called *this-host* address. It is used whenever a host needs to send an IP datagram but it does not know its own address to use as the source address.
- ***Limited-broadcast Address:*** The only address in the block **255.255.255.255/32** is called *limited-broadcast* address. It is used whenever a router or a host needs to send an IP datagram to all devices on a network. The routers in a network, however, block the packet having this address as the destination; the packet can not travel outside the network.
- ***Loopback Address:*** The block **127.0.0.0/8** (available ranges are: 127.0.0.0/8 to 127.255.255.255/8) is called the *loopback* address. A packet with one of the addresses in this block as the destination address never leaves the host; it will remain in the host. Any address in this block is used to test a piece of software in the machine. For e.g., we can write a client and server program in which one of the addresses in the block is used as the server address. We can test the programs using the same host to see if they work before running them on different computers. Typically, we use 127.0.0.1/8 as loop back IP address. Thus, 16, 777, 215 IP wasted.
- ***Private Address:*** Four blocks are assigned as private addresses as shown in table below. The significance of this is discussed later in NAT.
- ***Multicast Address:*** The block **224.0.0.0/4** is reserved for multicast addresses to be discussed later on.

Network Address Translation (NAT)

- Let us say, you have been given an IP address by ISP. But now you want to use 5 hosts to connect to the Internet using only one IP address. How is this possible?

Network Address Translation (NAT)

- This is possible using the concept of NAT. So, to do this, it must be ensured that router must support NAT software.

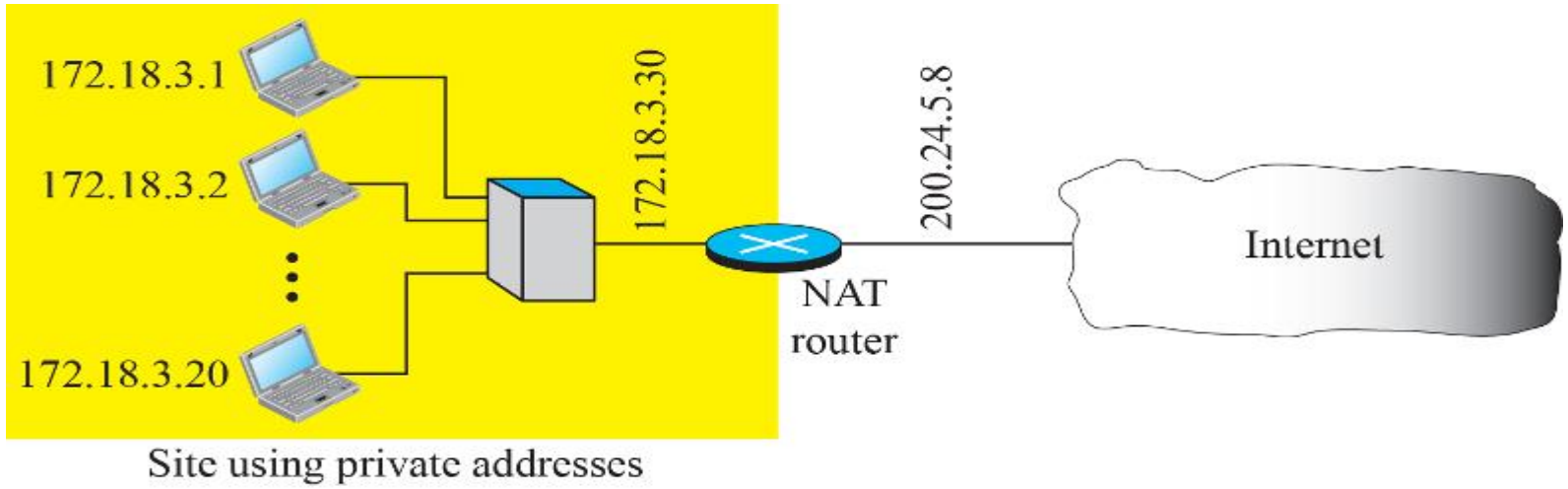
NAT: It enables a user to have a larger set of addresses internally and one address or a small set of addresses externally.

- To separate the addresses used inside the home or business and the ones used for the Internet, the Internet authorities have reserved three set of addresses as a private address which are unique inside the organization but not unique globally.
- *The list of private IP addresses are summarized below:*

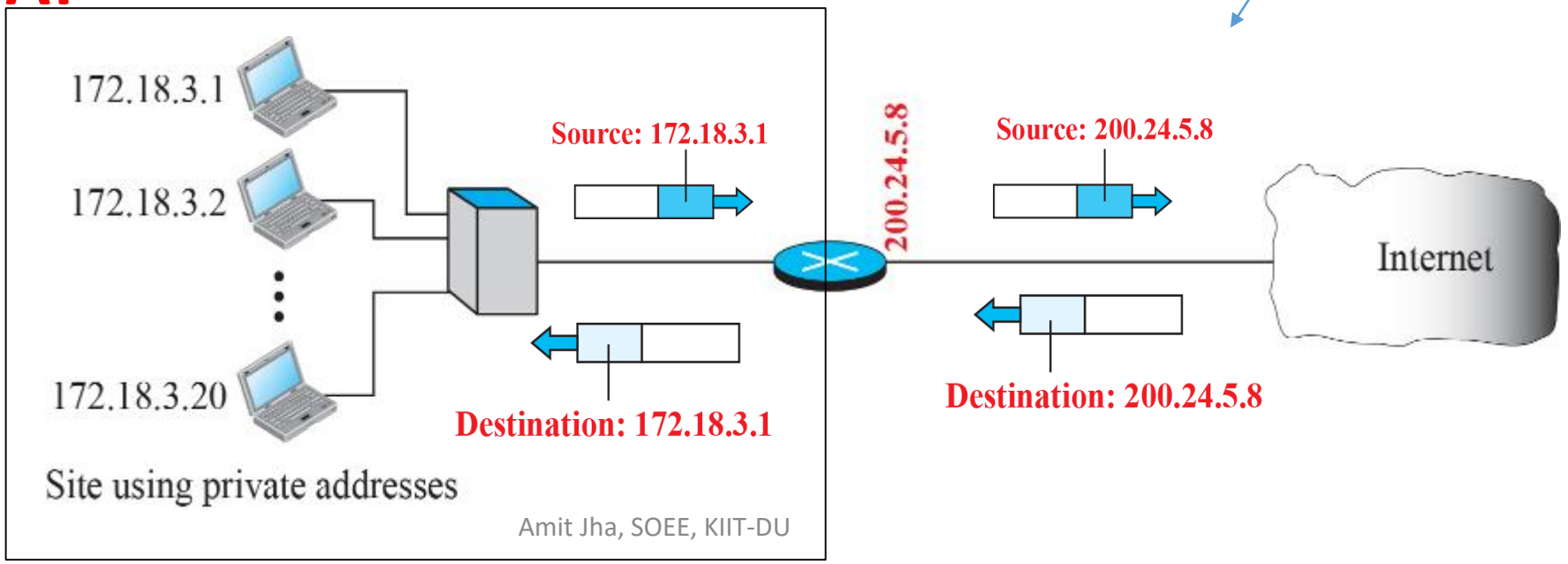
Short Representation	Range	Total
10.0.0.0/8	10.0.0.0 to 10.255.255.255	2^{24}
172.16.0.0/12	172.16.0.0 to 172.31.255.255	2^{20}
192.168.0.0/16	192.168.0.0 to 192.168.255.255	2^{16}

A NAT implementation

Note: *Private IP addresses are non routable.*



Address in a NAT



Time to Think

- **Question:** Who does provide the IP addresses to larger organizations?
- **Answer:** ICANN→ Internet Corporation for Assigned Names and Numbers.
- **Question:** Who does provide the IP addresses to smaller organizations?
- **Answer:** ISP→ Internet Service Provider
- **Question:** After assigning IP addresses to the organizations, who will manage these IP addresses?
  - **Answer:** Network administrator of the corresponding organization.
- **Question:**How does the network administrator distribute these IP addresses?
  - **Answer:** Two Methods→ 1) Static or 2) Dynamic

Dynamic Host Configuration Protocol (DHCP)

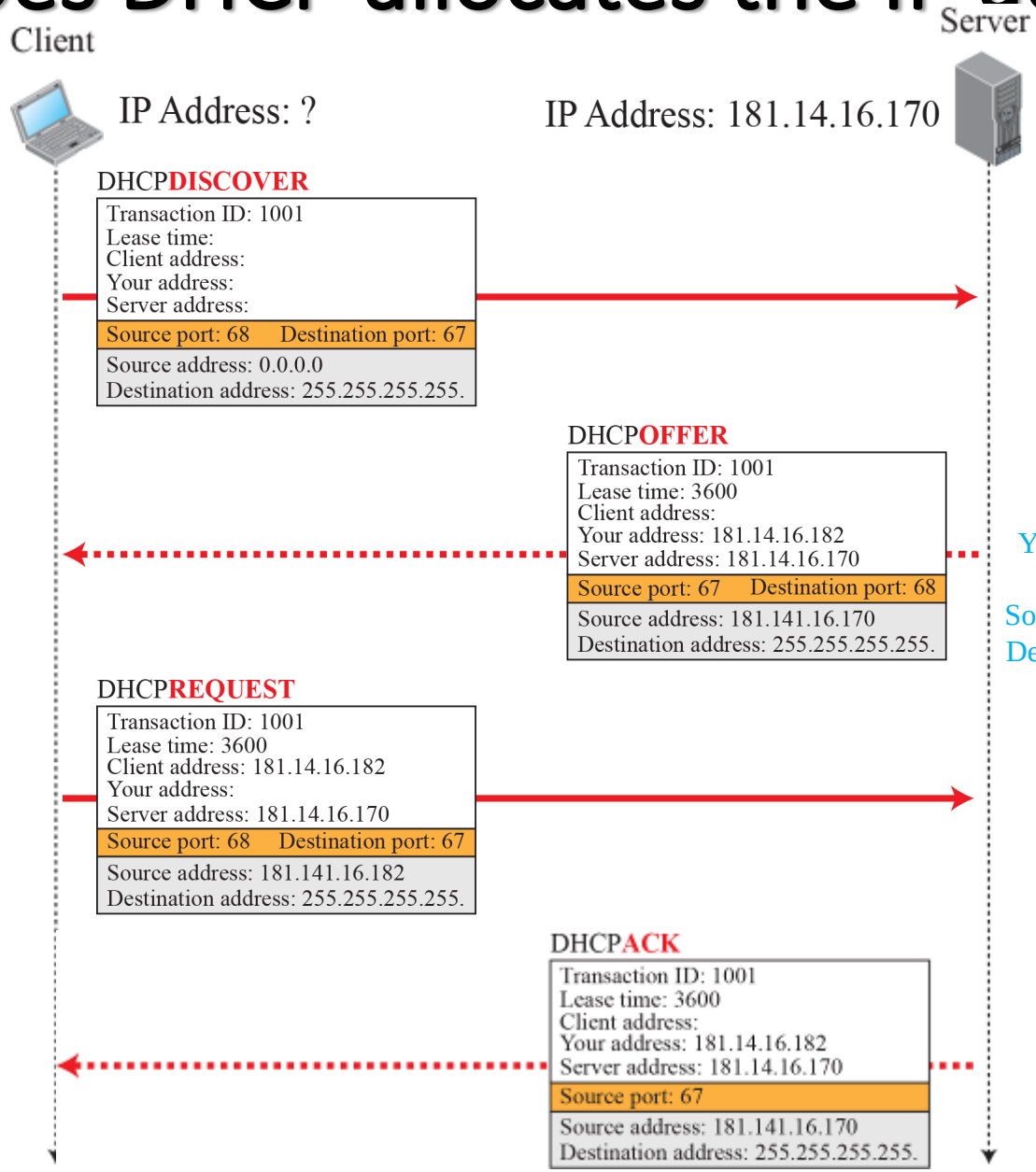
- This is used to dynamically assign the IP addresses in an organization.
- The Dynamic Host Configuration Protocol is used for this purpose.
- DHCP is an application layer program based on client-server paradigm which actually helps the TCP/IP at the Network layer.
- A network manager can configure DHCP to assign IP addresses dynamically which can be either permanent or temporary.
- It also allows an ISP with 1000 granted addresses to provide services to 4000 households, assuming not more than $1/4^{th}$ of customers use the Internet at the same time.
- The DHCP can be used to provide following piece of information to the host→ the computer address, prefix, the address of a router and the IP address of a name server.

How does DHCP allocates the IP address?

Transaction id→ Random

Source Address→ "this host"

Destination Address→ "broadcast"



Note:
Only partial information is given.

Legend

Application
UDP
IP

Your Address→ "Offered IP Address"

Source Address→ "DHCP Server IP Address"

Destination Address→ "Broadcast Address"

HYU: Answer the following Questions shortly.

12. What should be the transaction id in DHCPDISCOVER message?
13. Which of the available protocols of the transport layer have been utilized in the previous example?
14. Why does the DHCPOFFER message contains the Destination address as a broadcast address in spite of offering the IP address to the Host?
15. What is the need of DHCPREQUEST message as it knows the IP address offered to it on the reception of DHCPOFFER mesage?
16. Why does the DHCPREQUEST message contains the Destination address as a broadcast address in spite of offering the IP address to the Host?
17. What is the need of DHCPACK message?
18. Do we need DHCPNACK message, and if yes, then what case?
19. Why do we need two well known ports as we know for client, one can use ephemeral port?
20. As DHCP uses UDP, which is unreliable, thus how does DHCP provide error control?

Address Mapping

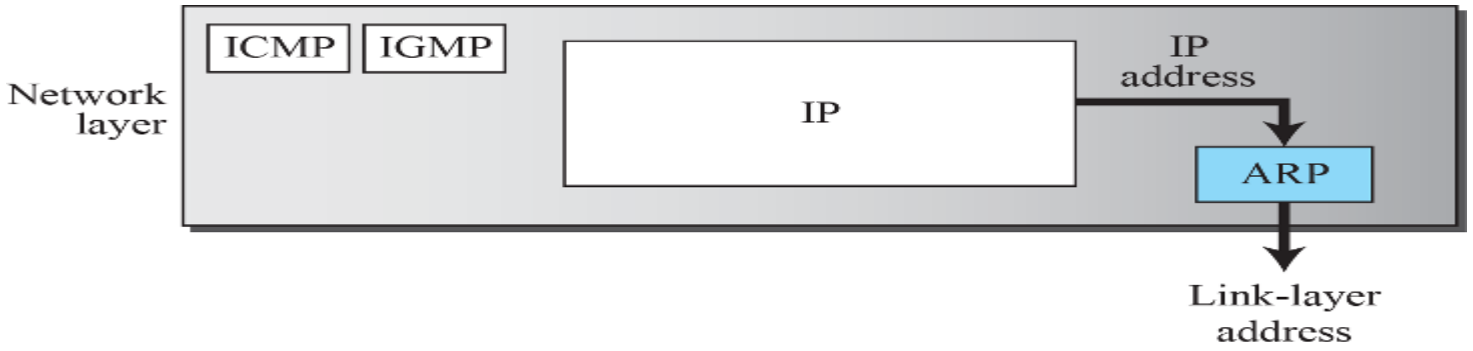
- **Motivation:** The hosts and routers are recognized at the network level by their logical (IP) addresses.
- However, packets pass through physical networks to reach these hosts and routers.
- At the physical level, the hosts and routers are recognized by their physical addresses.
- This means that delivery of a packet to a host or a router requires two levels of addressing: logical and physical.
- Thus, we need to be able to map a logical address to its corresponding physical address and vice versa. These can be done by using either static or dynamic mapping.

Static Address Mapping

- Static mapping involves in the creation of a table that associates a logical address with a physical address.
- But this method is not feasible because physical addresses may change in the following ways:
  - A machine could change its NIC, resulting in a new physical address.
  - In some LANs, such as Local Talk, the physical address changes every time the computer is turned on.
- To implement these changes, a static mapping table must be updated periodically. This overhead could affect network performance.
- In dynamic address mapping, each time a machine knows one of the two addresses (logical or physical), it can use **a protocol** to find the other one.

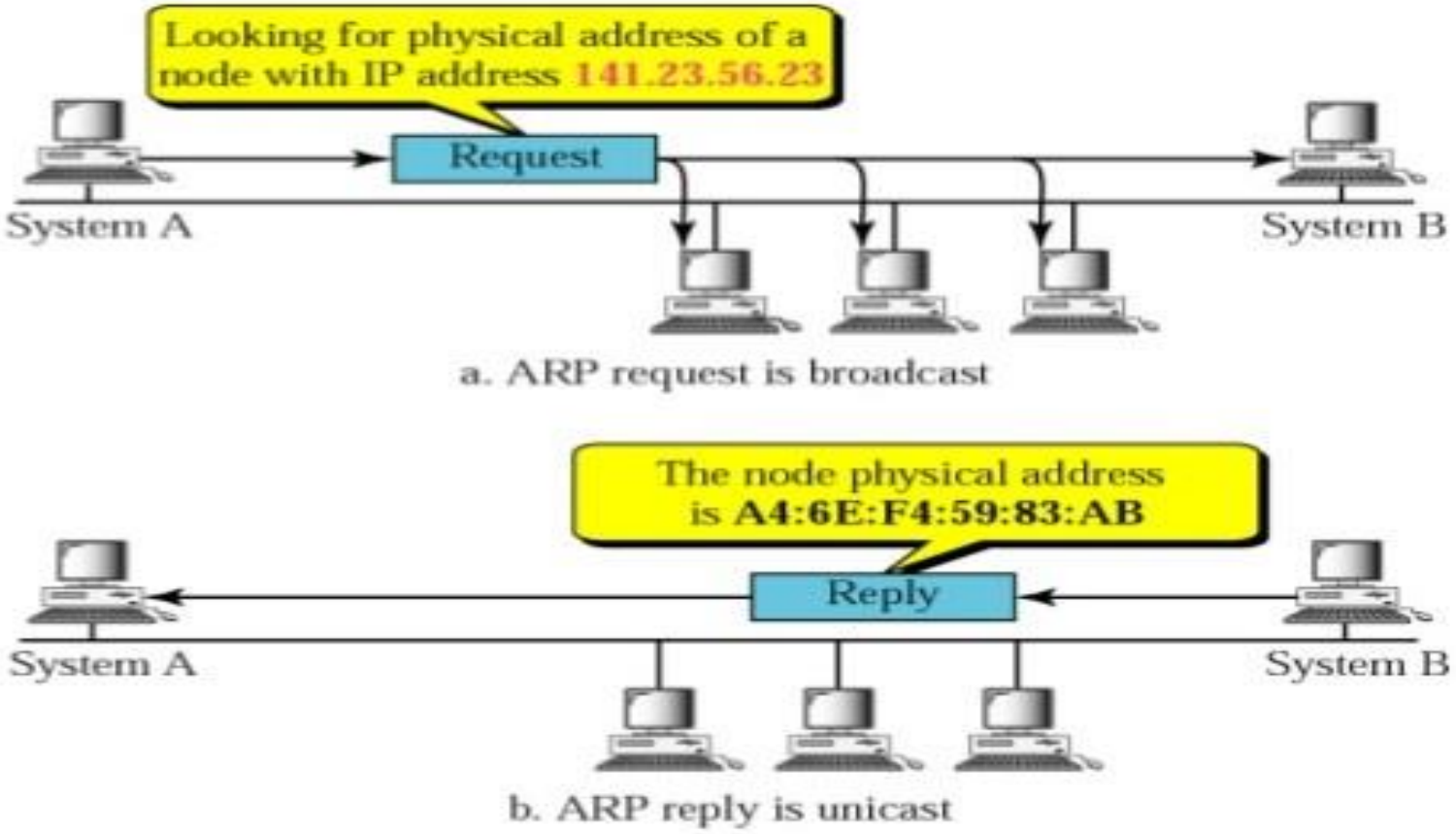
Mapping Logical to Physical Address: ARP

- ARP stands for Address Resolution Protocol.
- It is done by broadcasting ARP query packet containing physical and logical addresses of sender and only logical address of receiver.
- Every host or router on the network receives and processes the ARP query packet, but 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.



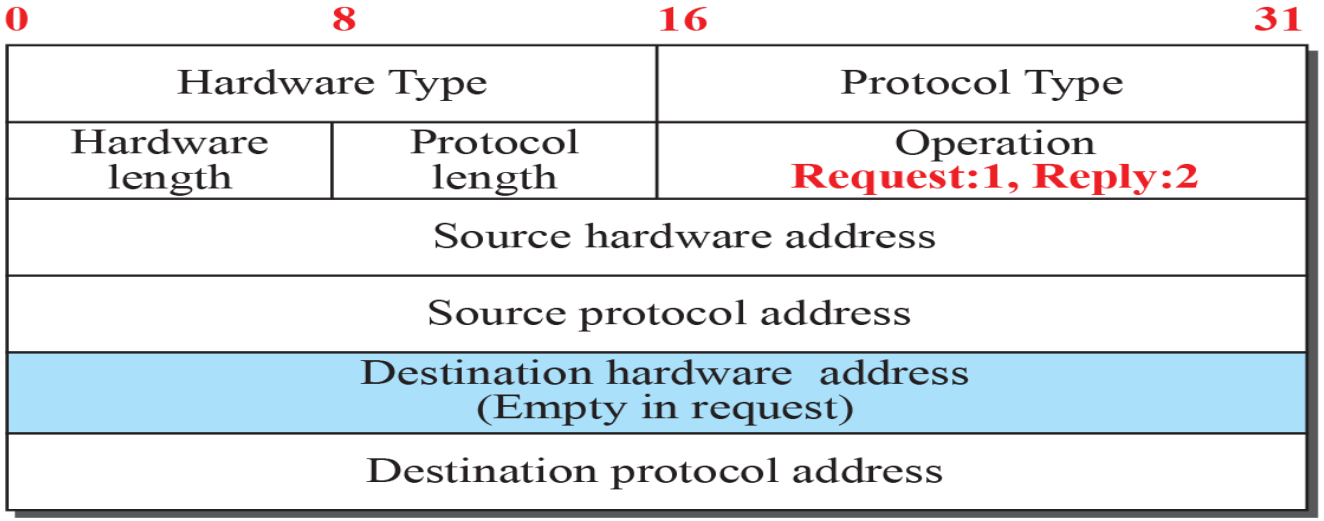
← **Position of ARP**

ARP Operation



Packet Format of ARP

- ***Hardware Type:*** It defines the type of link-layer protocol. For Ethernet, this value is 1.
- ***Protocol Type:*** It defines the network-layer protocol. For IPv4 protocol, this value is (0800)16.
- ***Hardware Length:*** It defines the length of the hardware address in bytes. For MAC address, the value is 6 bytes.
- ***Protocol Length:*** It defines the length of the protocol address in bytes. For IPv4 address, the value is 4 bytes.
- ***Source Hardware Address:*** It defines the link-layer address i.e., MAC address of the source.
- ***Source Protocol Address:*** It defines the Network-layer address i.e., IP address of the source.
- ***Destination Hardware Address:*** It defines the link-layer address i.e., MAC address of the destination.
- ***Destination Protocol Address:*** It defines the Network-layer address i.e., IP address of the destination.
- Operation: It defines the nature of ARP message. For request, value is 1; and for reply, value is 2.

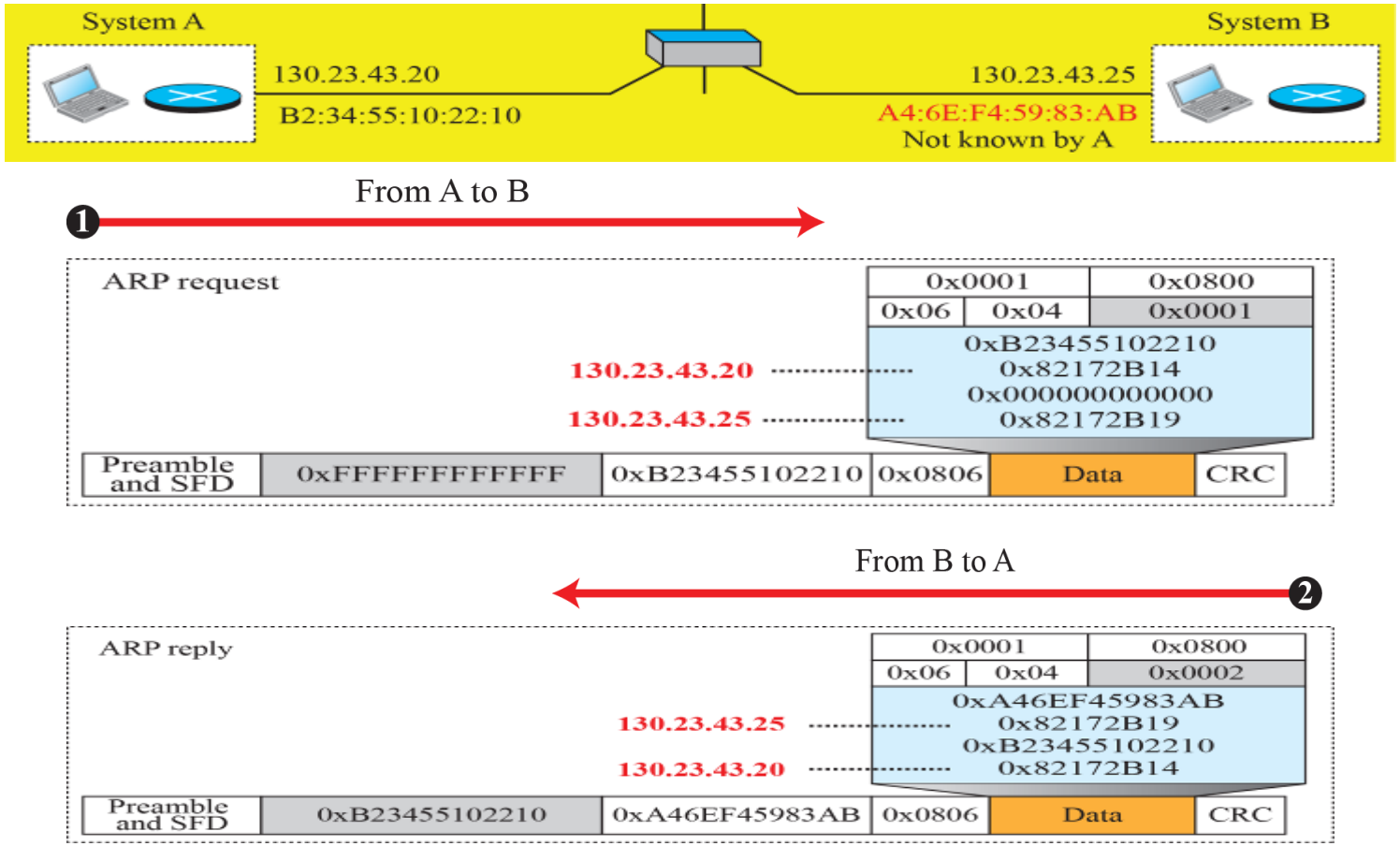


Hardware: LAN or WAN protocol

Protocol: Network-layer protocol

Example 4.17: A host with IP address N1= 130.23.43.20 and MAC address L1= B2: 34: 55: 10: 22:10 has a packet to send to another host with IP address N2= 130.23.43.25 and physical address L2 = A4: 6E: F4: 59: 83: AB (which is unknown to the first host). The two hosts are on the same network. Show the ARP request and reply packets encapsulated in Ethernet frames.

Solution:- Figure below shows the ARP request and reply packets. Note that the ARP data field in this case is 28 bytes, and that the individual addresses do not fit in the 4-byte boundary. That is why we do not show the regular 4-byte boundaries for these addresses. Also note that the IP addresses are shown in hexadecimal.



- For more details of ARP, you can refer Section 5.4, page no-421-427 of the Text Book.

Mapping Physical to Logical Address: RARP

- **Need:** There are occasions in which a host knows its physical address, but needs to know its logical address. This may happen in two cases:
  1. A disk less station is just booted. The station can find its physical address by checking its interface, but it does not know its IP address.
  2. An organization does not have enough IP addresses to assign to each station; it needs to assign IP addresses on demand. The station can send its physical address and ask for a short time lease.

Three protocols are used for finding out logical address from known physical address: RARP, BOOTP, DHCP.

Internet Control Message Protocol (ICMP)

- **Need:** The IP protocol is a best-effort delivery service i.e., it provides unreliable and connectionless datagram delivery.

  It was designed to make an efficient use of network resources.

However, it has ***two deficiencies:***

1. Lack of error control & 2. Lack of assistance mechanisms.

What happens if

- Something goes wrong?
- A router discards a datagram because TTL field has 0?
- Final destination host discards all fragments of a data gram because it has not received all fragments within a predetermined time?

- A host sometimes needs to determine if a router or another host is alive.
- And sometimes a network administrator needs information From another host or router

ICMP or ICMPv4: Types of Messages

- ICMP messages are divided into two broad categories: **error-reporting messages** and **query messages**.
- **Error Reporting:** ICMP does not correct errors, it simply reports error message to the original source. This is because the only information available in the datagram about the route is source and destination IP addresses.

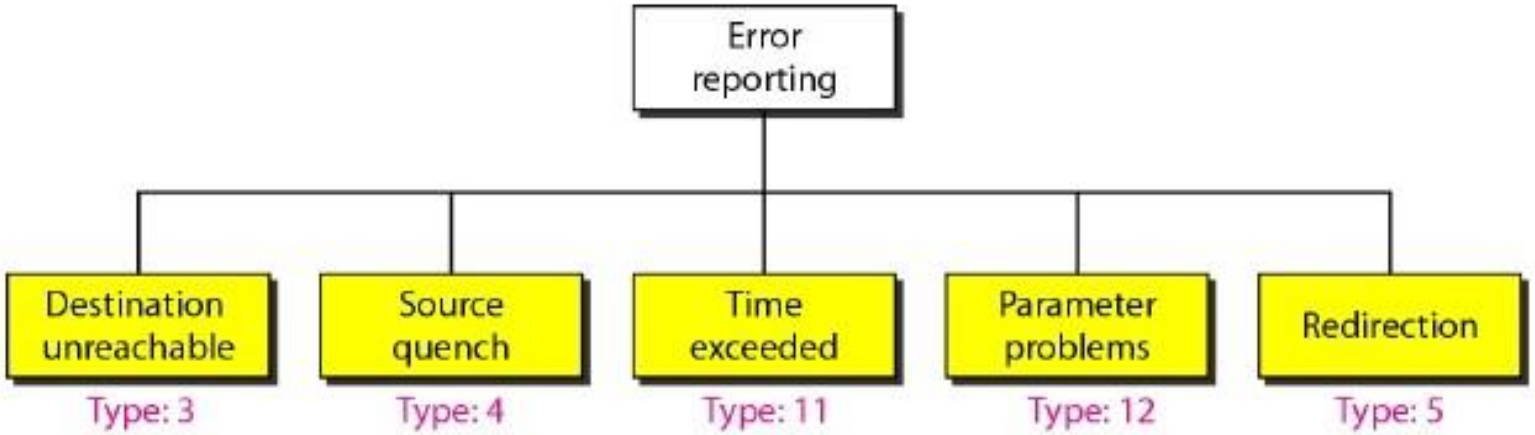


Fig: Error-Reporting Message

Cont....

- .

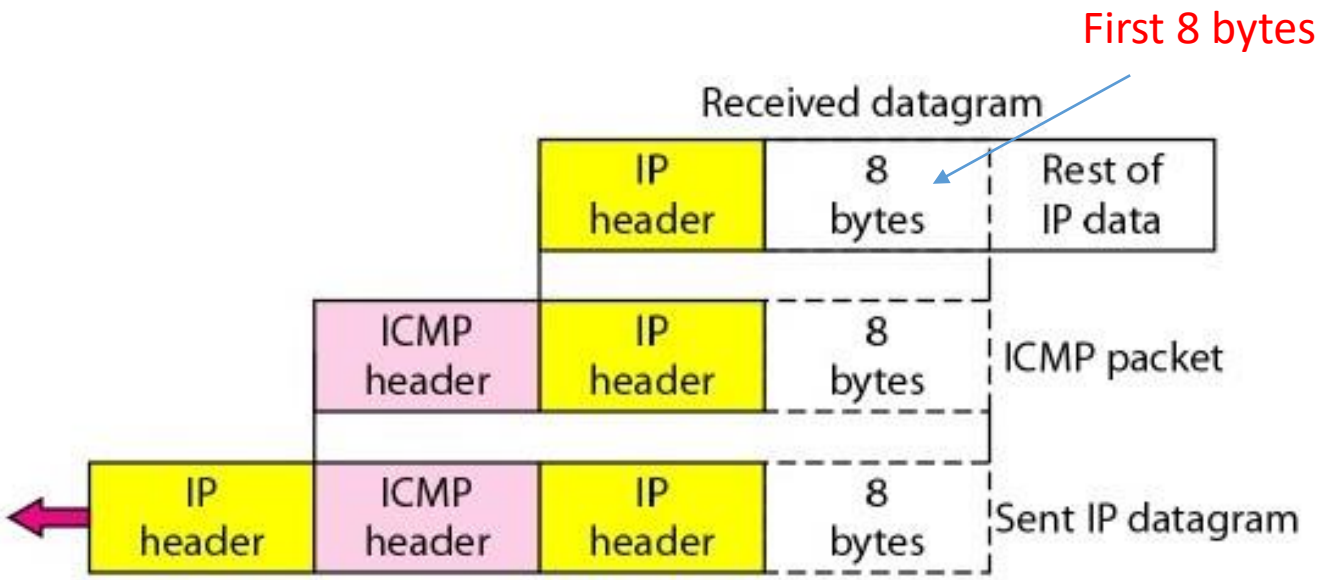


Fig: Contents of data field for the error messages

- **Note:** All error messages contain a data section that includes the IP header of the original datagram plus the first 8 bytes of data in that datagram.
- The original datagram header is added to give the original source, which receives the error message, information about the datagram itself. The 8 bytes of data are included because the first 8 bytes provide information about the port numbers (**UDP and TCP**) and sequence number (**TCP**). This information is needed so the source can inform the protocols (TCP or UDP) about the error.

Types of ICMP Error Reporting Message

1. ***Destination Unreachable:*** This message is created when a router can not route a datagram or a host can not deliver a datagram.
2. ***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.
3. ***Time Exceeded:*** This message is created when datagram can not reach to the destination because of either congestion or travelling in a loop or cycle endlessly.

Cont…

4. ***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.

5. ***Redirection:*** The hosts usually use static routing and its routing table has a limited number of entries. It usually knows the IP address of only one router, the default router. For this reason, the host may send a datagram, which is destined for another network, to the wrong router. In this case, the router that receives the datagram will forward the datagram to the correct router. However, to update the routing table of the host, it sends a redirection message to the host.

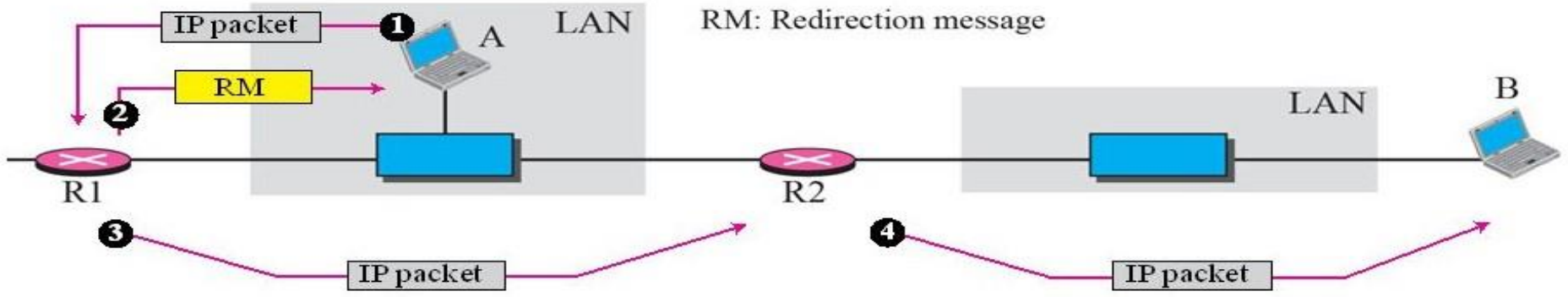
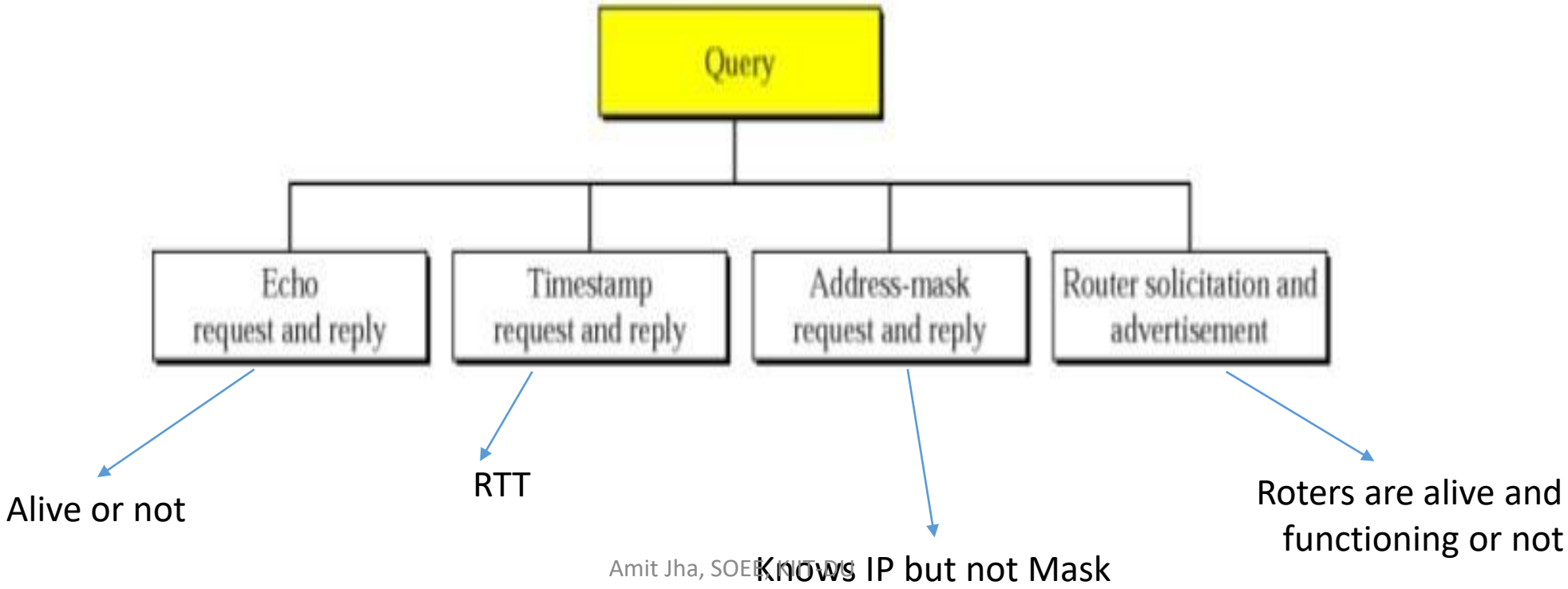


Fig: Redirection concept

Types of ICMP Query Message

- In addition to error reporting, ICMP can diagnose some network problems using the ***query messages***.



Cont…

1. ***Echo Request and Reply:*** The combination of echo-request and echo reply messages determines whether two systems (hosts or routers) can communicate with each other at IP level or not. ***Ping*** command can create a series (instead of just one) of echo-request and echo reply messages, providing statistical information.
2. ***Time stamp Request and Reply:*** This is used to determine the round-trip time needed for an IP datagram to travel between two hosts or routers.
3. ***Address-Mask Request and Reply:*** This message is sent to the corresponding LAN when a host knows its IP address but does not know its mask.

Cont…

4. *Router Solicitation and Advertisement:* When a host wants to communicate with a host on other network, it must know the address of routers connected to its own network. Also, the host must know if the routers are alive and functioning. The router-solicitation and router-advertisement messages can help in this situation. A host can broadcast(or multicast) a router-solicitation message. The router or routers that receive the solicitation message broadcast not only their own routing information but also information of other routers it is aware of, using the router-advertisement message.

HYU 21: Explore the use of *ping* and *tracert* from the point of network administrator.

Q. Will ICMP help if we want to send error report and query (network management) to more than one routers i.e. group management?

Q. Will ICMP help if we want to send error report and query (network management) to more than one routers i.e. group management?

Ans: No, it won't work. This is because ICMP was designed for unicast application. For multicast application we need to use Internet Group Management Protocol (IGMP)

Note: IGMP is not in syllabus. If you wish then you can refer to Forouzan, P.N 630, 4th edition.

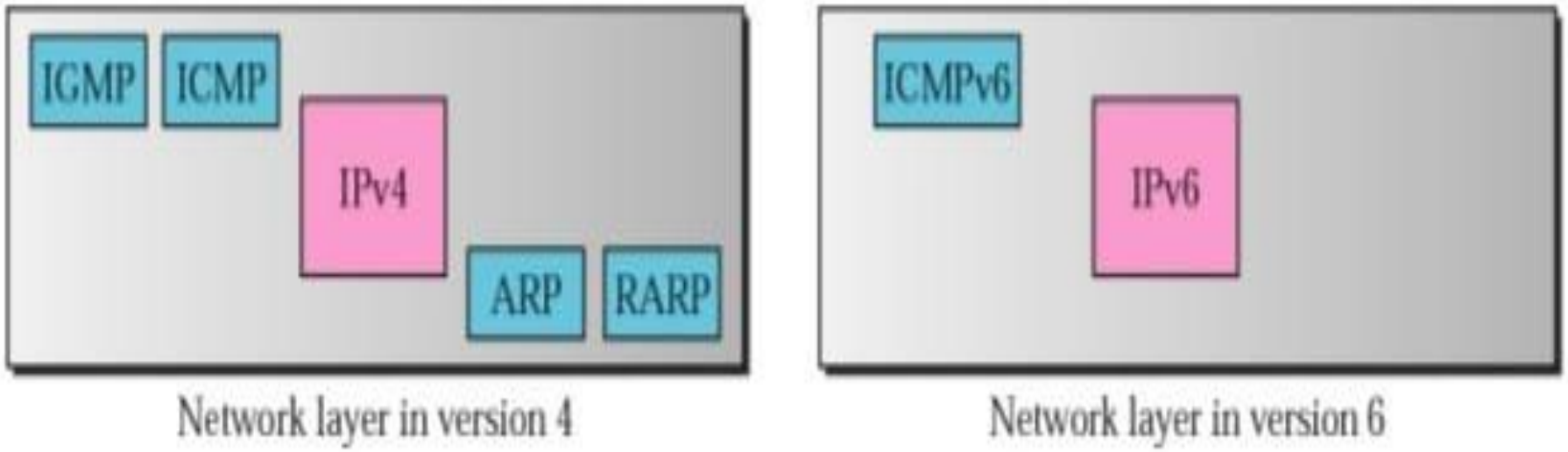
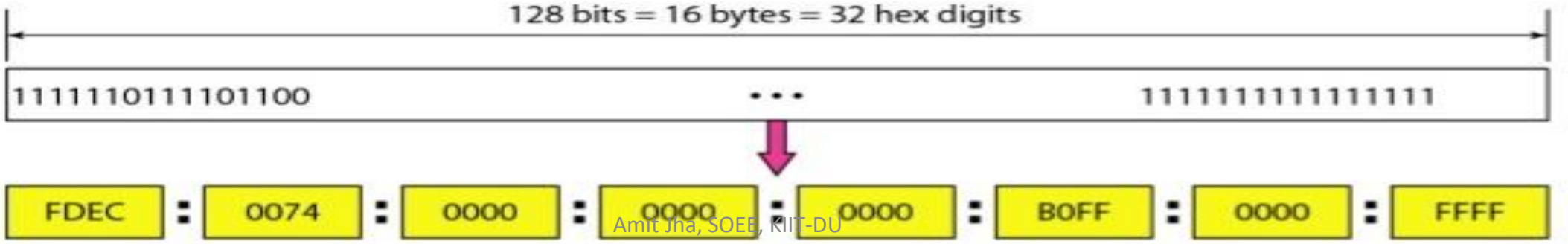


Fig: Comparison of network layers in version 4 and version 6.

- **In IPv6, ICMPv4 has been modified as ICMPv6 to make it more suitable for IPv6.**
- **ICMPv6 not in syllabus. If you wish then you can refer to Forouzan P.N 638, 4th edition.**

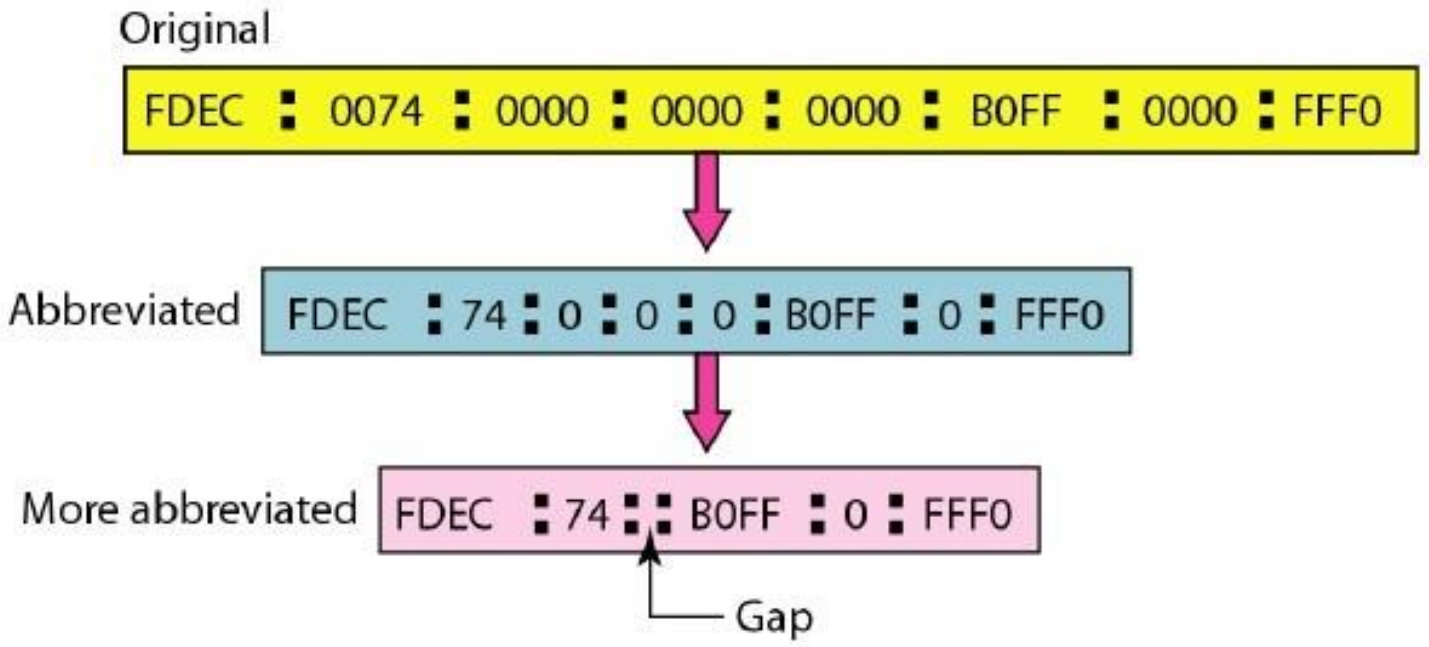
Internet Protocol version 6 (IPv6)

- **Need/Motivation:**
  - Despite all short-term solutions, such as **classless addressing**, Dynamic Host Configuration Protocol (**DHCP**), and **NAT**, address depletion is still a long-term problem for the Internet.
  - For real-time audio and video transmission, minimum delay strategies and reservation of resources are required in transmission which were not provided in the IPv4 design.
  - The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.
- **IPv6 Address Structure:** An IPv6 address is 16 bytes or 128 bits long.
  This format is known as colon hexadecimal notation.



Abbreviation of IPv6

- Although the IP address, even in hexadecimal format, is very long, many of the digits are zeroes. In this case, we can abbreviate the address.

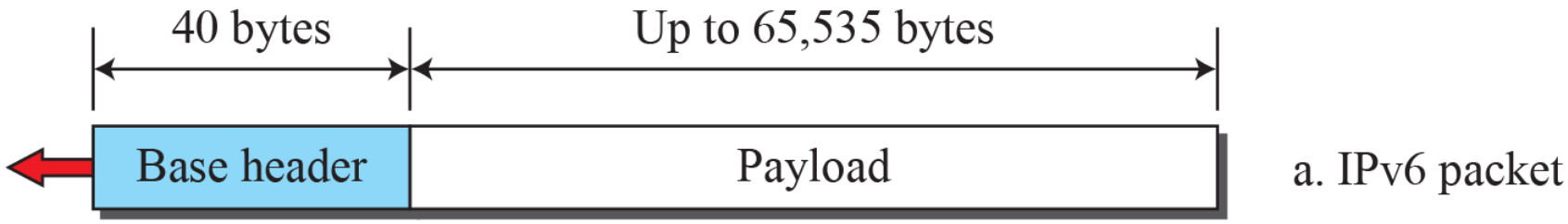


Advantages of IPv6 over IPv4

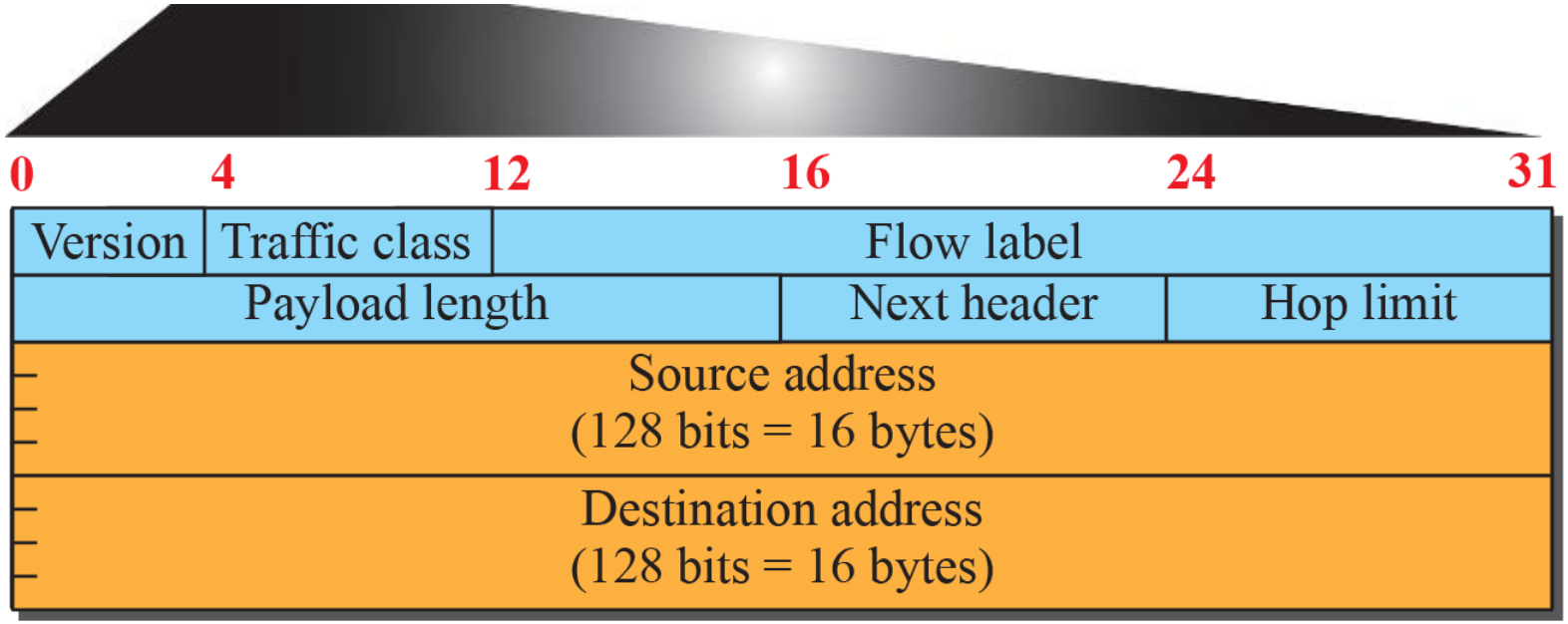
1. **Larger Address Space:** 128 bits long, so 2^{96} increase in the address space.
2. **Better Header Format:** Options are separated from the base header. So, speed up in the routing process as options do not need to be checked by the routers most of the time.
3. **New Options:** This field allows more functionalities in IPv6.
4. **Allowance for Extension:** Designed to allow extension of the protocol if desired.
5. **Support for Resource Allocation:** Flow control is added
6. **Support for More Security:** The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Packet Format of IPv6

- Each packet is composed of a mandatory base **header of 40 bytes** (fixed size) followed by the payload.
- The **payload consists of two parts**: optional extension headers and **data f**rom an upper layer.



a. IPv6 packet



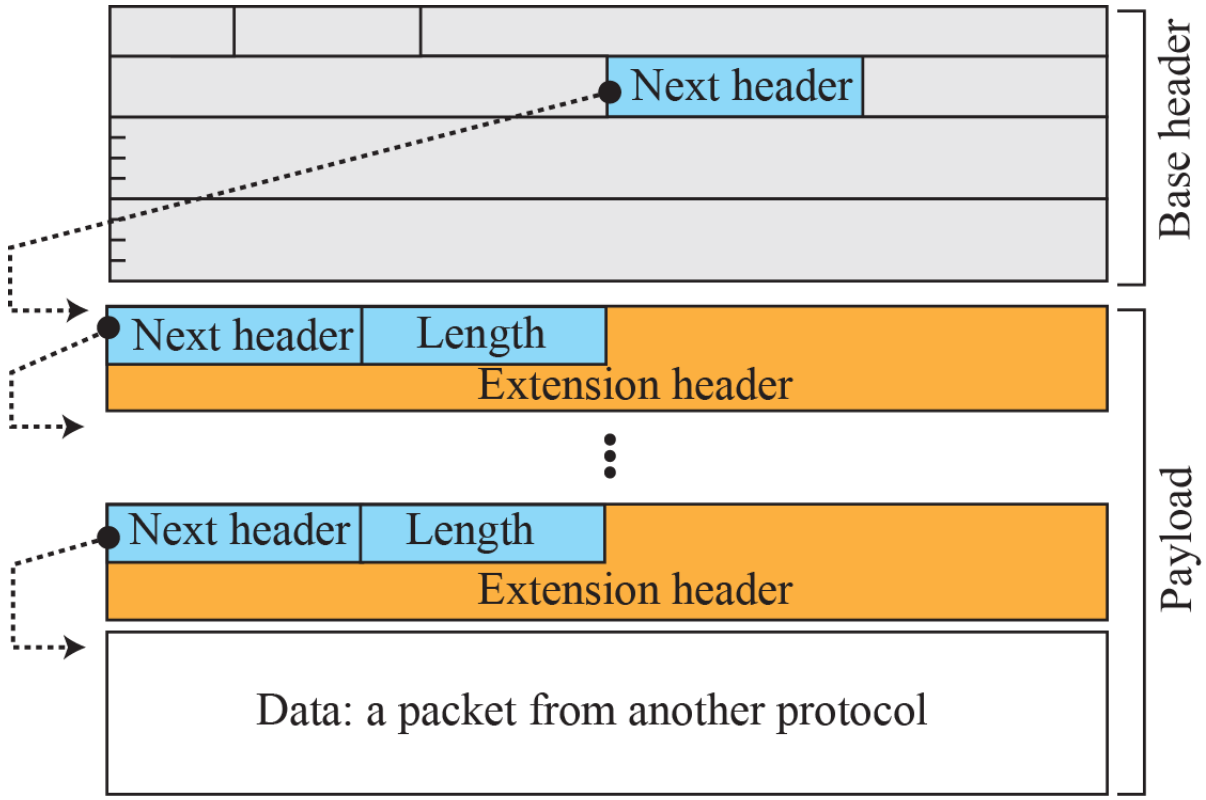
b. Base header

IPv6 Base Header

- The IPv6 packet, or datagram is shown in diagram below.
- *Version: To define IPv4 or IPv6*
- *Traffic Class or Priority:* identify priority among datagrams
- *Flow Label:* Used for flow control
- *Payload Length:* It defines the size of the IP datagram excluding the header.
- *Next Header:* It defines the type of first extension header (if present) or the type of the data that follows the base header in the datagram. This field is similar to protocol field of IPv4 header.
- *Hop Limit:* It serves the same purpose as the TTL field in IPv4 header.

Note: The size of IPv6 base header is 40 bytes.

Structure of Payload in IPv6 Datagram:



Some next-header codes

00: Hop-by-hop option
02: ICMPv6
06: TCP
17: UDP
43: Source-routing option
44: Fragmentation option
50: Encrypted security payload
51:Authentication header
59: Null (no next header)
60: Destination option

Significance of Extension Header

Comparison Between IPv4 and IPv6 Headers

Comparison
1. The header length field is eliminated in IPv6 because the length of the header is fixed in this version.
2. The service type field is eliminated in IPv6. The priority and flow label fields together take over the function of the service type field.
3. The total length field is eliminated in IPv6 and replaced by the payload length field.
4. The identification, flag, and offset fields are eliminated from the base header in IPv6. They are included in the fragmentation extension header.
5. The TTL field is called hop limit in IPv6.
6. The protocol field is replaced by the next header field.
7. The header checksum is eliminated because the checksum is provided by upper-layer protocols; it is therefore not needed at this level.
8. The option fields in IPv4 are implemented as extension headers in IPv6.