

4.3 Protocols - ARP, RARP, ICMP, IGMP



Types of Addresses in Internet

- Media Access Control (MAC) addresses in the network access layer
 - Associated w/ network interface card (NIC)
 - 48 bits or 64 bits
- IP addresses for the network layer
 - 32 bits for IPv4, and 128 bits for IPv6
 - E.g., 123.4.56.7
- IP addresses + ports for the transport layer
 - E.g., 123.4.56.7:80
- Domain names for the application/human layer
 - E.g., www.google.com

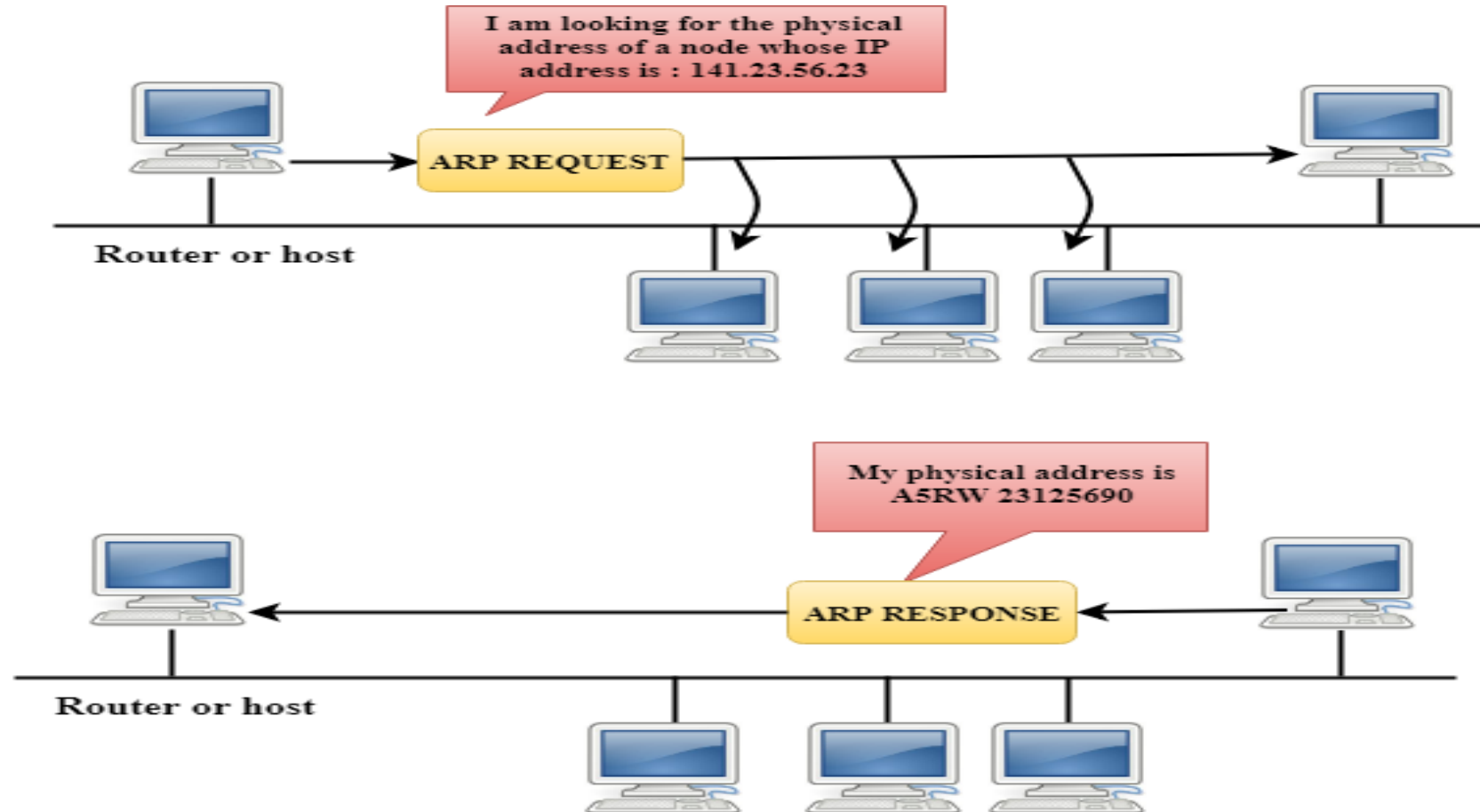
ARP - Address Resolution Protocol.

- ARP - It is used to associate an IP address with the MAC address.
- Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the MAC address for communication on a local area network. MAC address can be changed easily.
- For example, if the NIC on a particular machine fails, the MAC address changes but IP address does not change. ARP is used to find the MAC address of the node when an internet address is known

How ARP works?

- If the host wants to know the physical address of another host on its network, **then it sends an ARP query packet that includes the IP address and broadcast it over the network.**
- Every host on the network receives and processes the ARP packet, but **only the intended recipient recognizes the IP address and sends back the physical address.**
- The **host holding the datagram adds the physical address to the cache memory and to the datagram header, then sends back to the sender.**

How ARP works?



How ARP works?

- The device will first look at its internet list, called the ARP cache to check whether an IP address contains a matching MAC address or not.
- It will check the ARP cache in command prompt by using a command **arp-a**.

How ARP works?

- If ARP cache is empty, then device broadcast the message to the entire network asking each device for a matching MAC address.
- The device that has the matching IP address will then respond back to the sender with its MAC address
- Once the MAC address is received by the device, then the communication can take place between two devices.
- If the device receives the MAC address, then the MAC address gets stored in the ARP cache. We can check the ARP cache in command prompt by using a command `arp -a`.

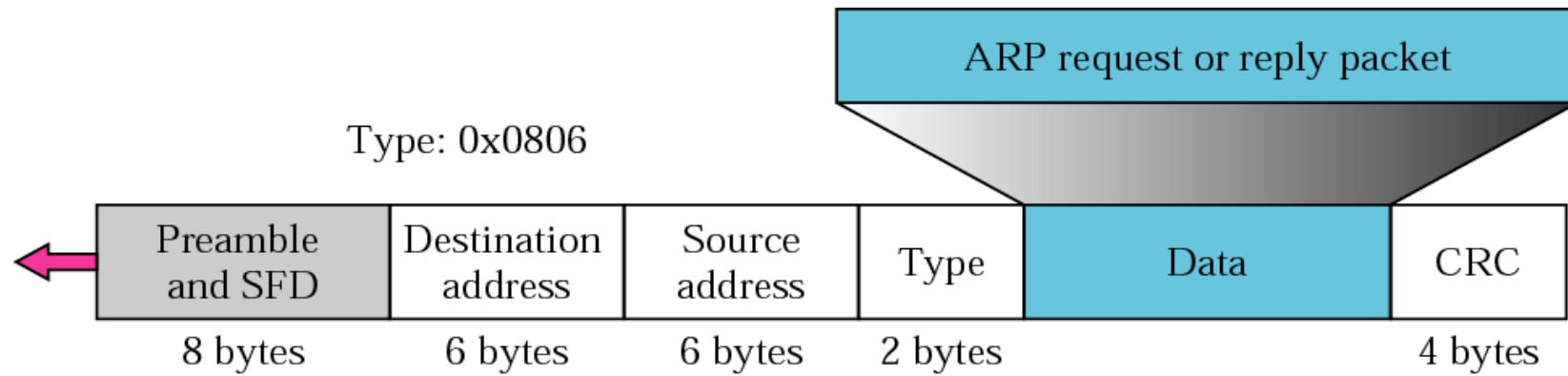
```
Command Prompt

C:\Users\admin>arp -a

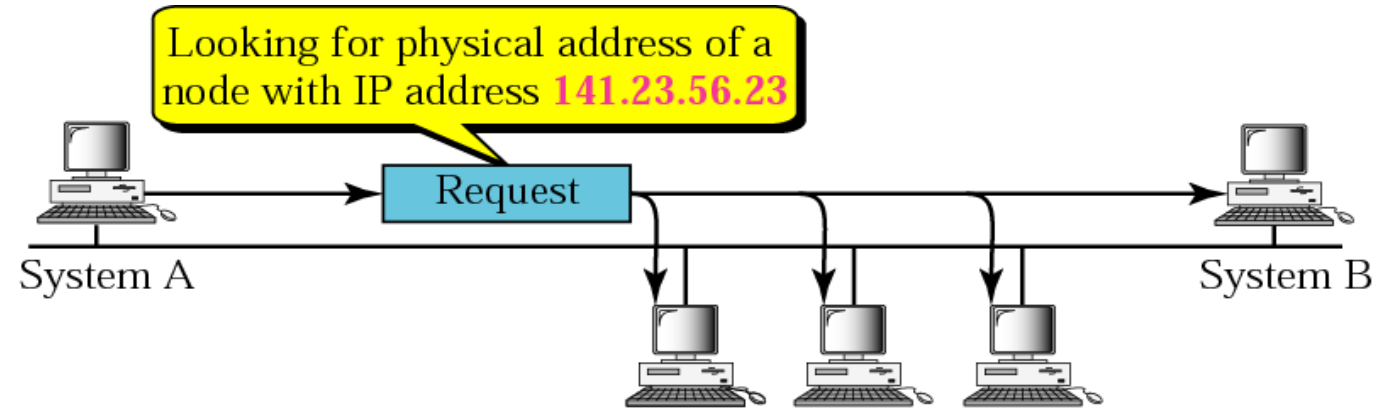
Interface: 192.168.1.10 --- 0x3
Internet Address      Physical Address      Type
192.168.1.1           74-da-da-db-f7-67    dynamic
192.168.1.11          fc-aa-14-ee-cc-c2    dynamic
192.168.1.14          18-60-24-bd-3d-1d    dynamic
192.168.1.32          1c-1b-0d-bd-d2-7e    dynamic
192.168.1.41          58-20-b1-40-b7-74    dynamic
192.168.1.55          fc-aa-14-a5-67-7a    dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

There are two types of ARP entries:

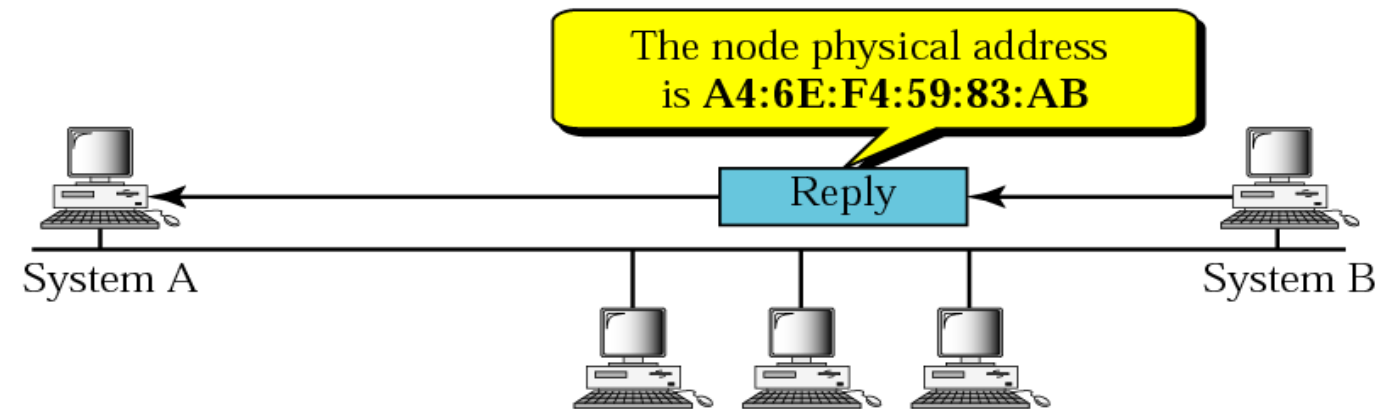
- Dynamic entry:** It is an entry which is created automatically when the sender broadcast its message to the entire network. Dynamic entries are not permanent, and they are removed periodically.
- Static entry:** It is an entry where someone manually enters the IP to MAC address association by using the ARP command utility.



The ARP packet is encapsulated within an Ethernet packet.
Note: Type field for Ethernet is x0806



a. ARP request is broadcast



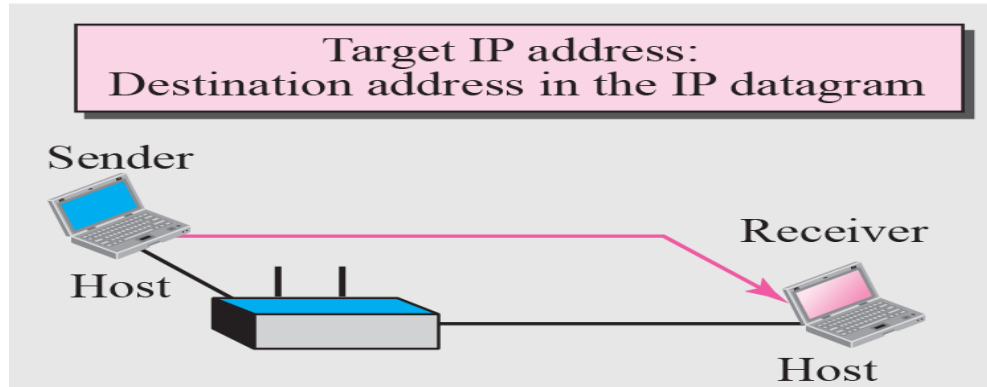
b. ARP reply is unicast



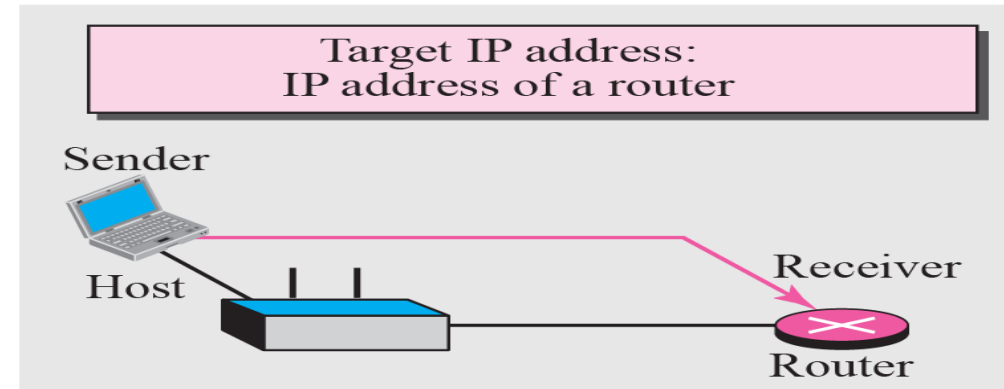
Figure 8.5 *Four cases using ARP*

11 TCP/IP
Protocol
Suite

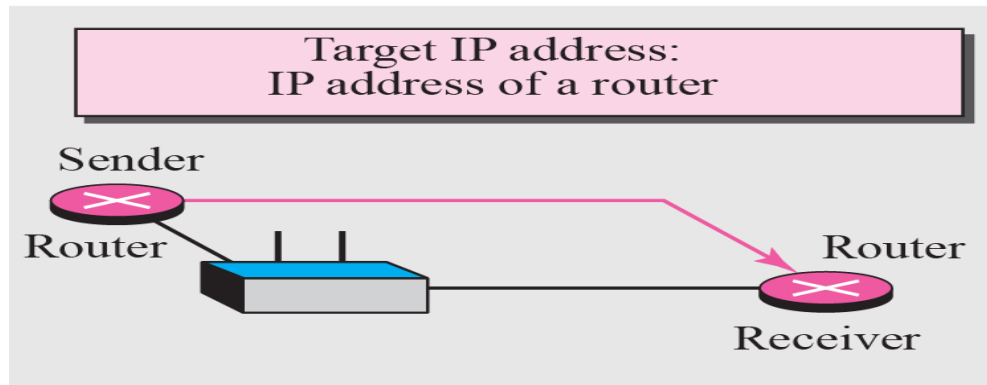
Case 1: A host has a packet to send to a host on the same network.



Case 2: A host has a packet to send to a host on another network.



Case 3: A router has a packet to send to a host on another network.



Case 4: A router has a packet to send to a host on the same network.

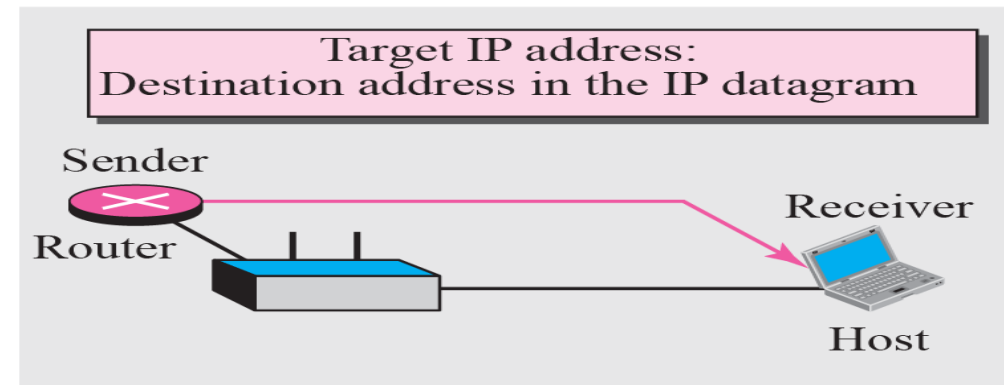
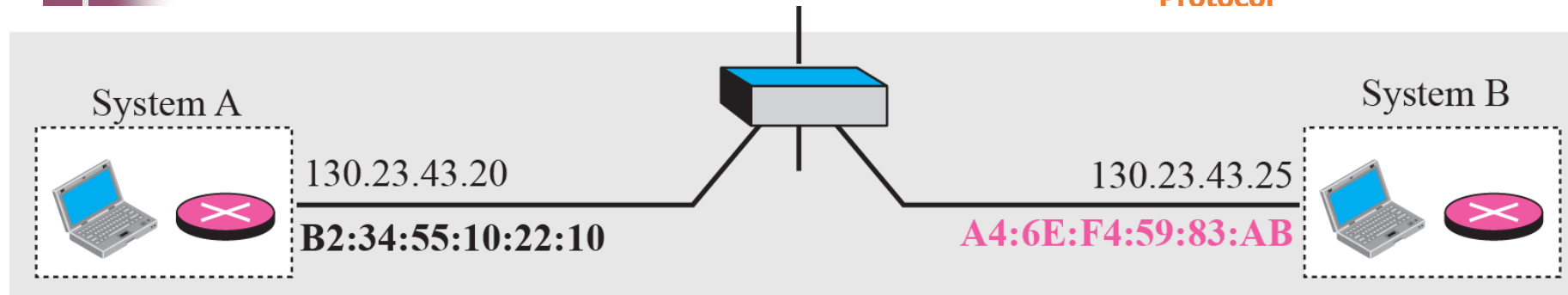
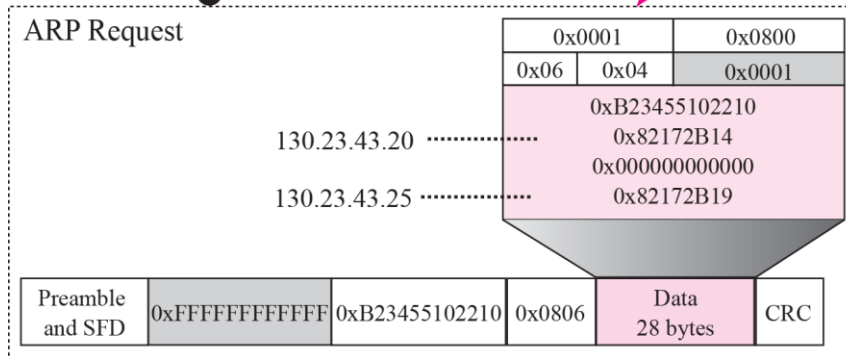


Figure 8.6 *Example 8.1*

12 TCP/IP
Protocol

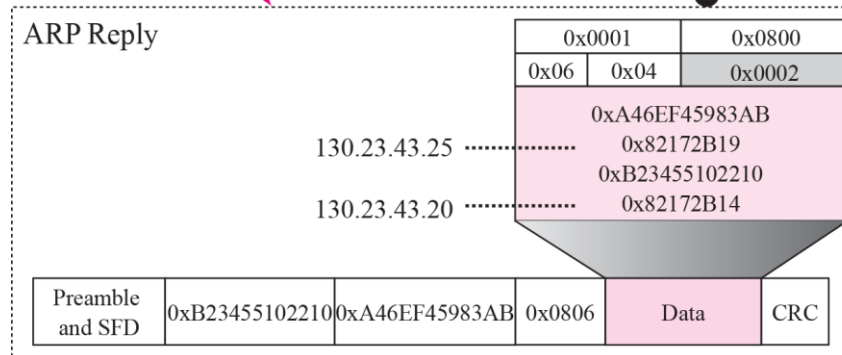


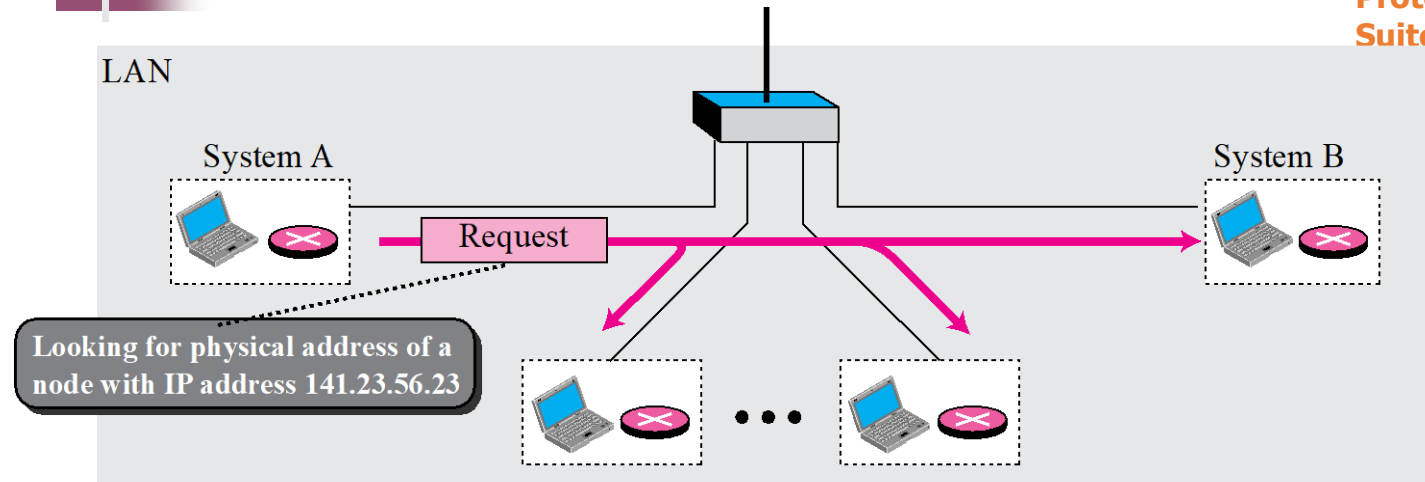
1 From A to B



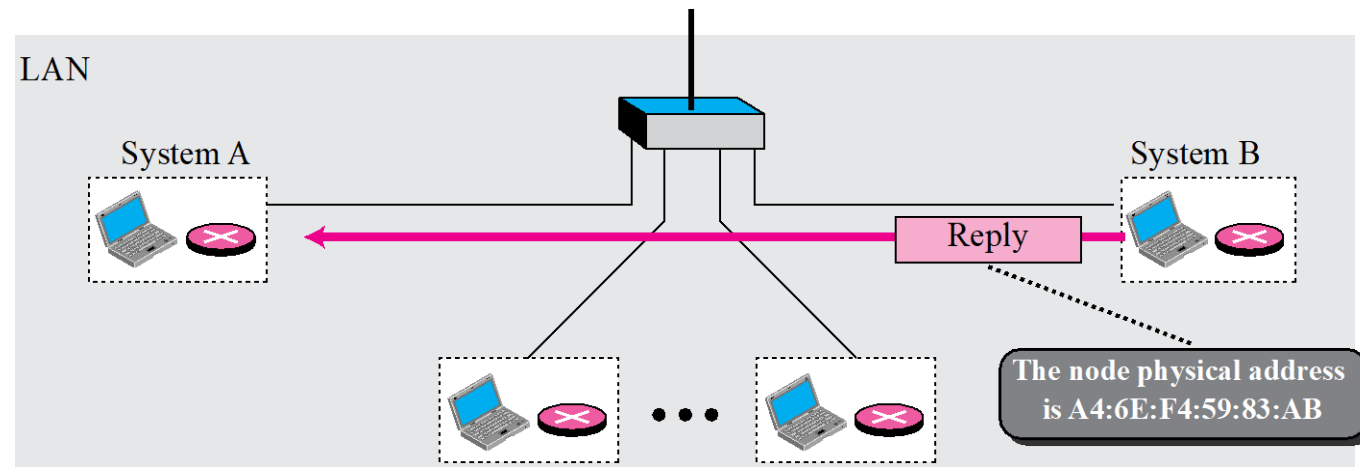
From B to A

2





a. ARP request is multicast



b. ARP reply is unicast

ARP Cache

- ▶ For every outgoing packet sending ARP request and waiting for responses is inefficient
- ▶ Requires more bandwidth
- ▶ Consumes Time
- ▶ ARP cache maintained at each node
- ▶ Size limit = 512 entries (timer)



The Cache Table

- If ARP just resolved an IP address, chances are a few moments later someone is going to ask to resolve the same IP address
- When ARP returns a MAC address, it is placed in a cache. When the next request comes in for the same IP address, look first in the cache

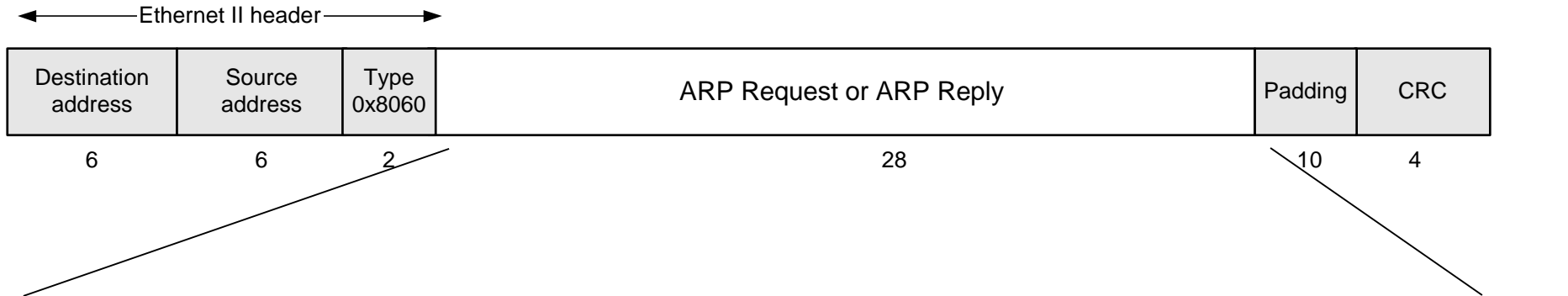
Cache Table

- Each host maintains a table of IP to MAC addresses
- Message types:
 - ARP request
 - ARP reply
 - ARP announcement

ARP Cache Problems

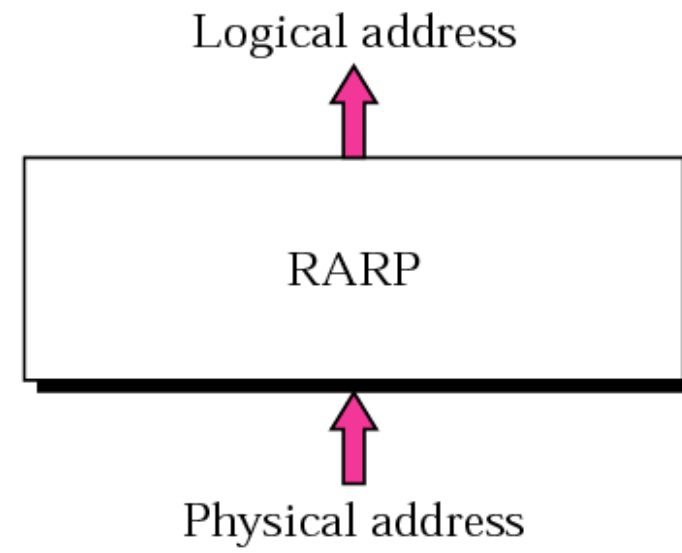
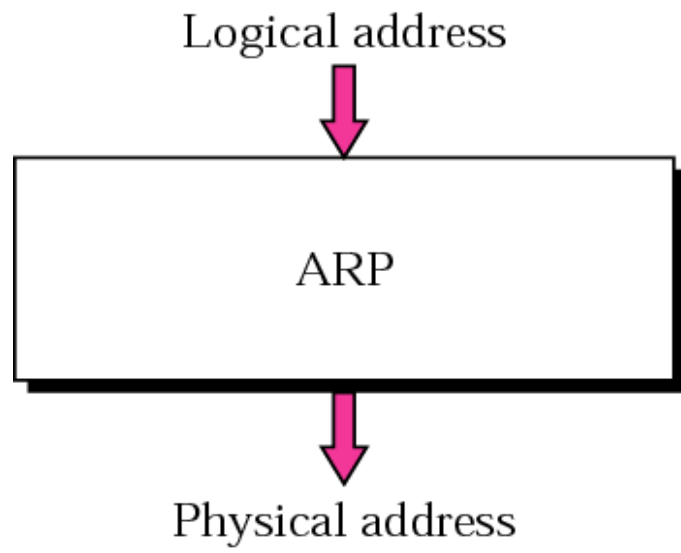
- Cache space may be limited
- Hosts move or change IP addresses
- Solution?
- Drop (invalidate) cache entries after “a while” (20 minutes is normal)

ARP Packet Format



Hardware type (2 bytes)		Protocol type (2 bytes)	
Hardware address length (1 byte)	Protocol address length (1 byte)	Operation code (2 bytes) Request = 1 : Reply = 2	
Source hardware address*			
Source protocol address*			
Target hardware address*			
Target protocol address*			

* Note: The length of the address fields is determined by the corresponding address length fields



RARP - Reverse Address Resolution Protocol.

- If the host wants to know its IP address, then it broadcast the RARP query packet that contains its physical address to the entire network.
- A RARP server on the network recognizes the RARP packet and responds back with the host IP address.
- The protocol which is used to obtain the IP address from a server is known as **Reverse Address Resolution Protocol**.
- The message format of the RARP protocol is similar to the ARP protocol.
- Like ARP frame, RARP frame is sent from one machine to another encapsulated in the data portion of a frame.

7.3 RARP

RARP finds the logical address for a machine that only knows its physical address.

The topics discussed in this section include:

Packet Format

Encapsulation

RARP Server

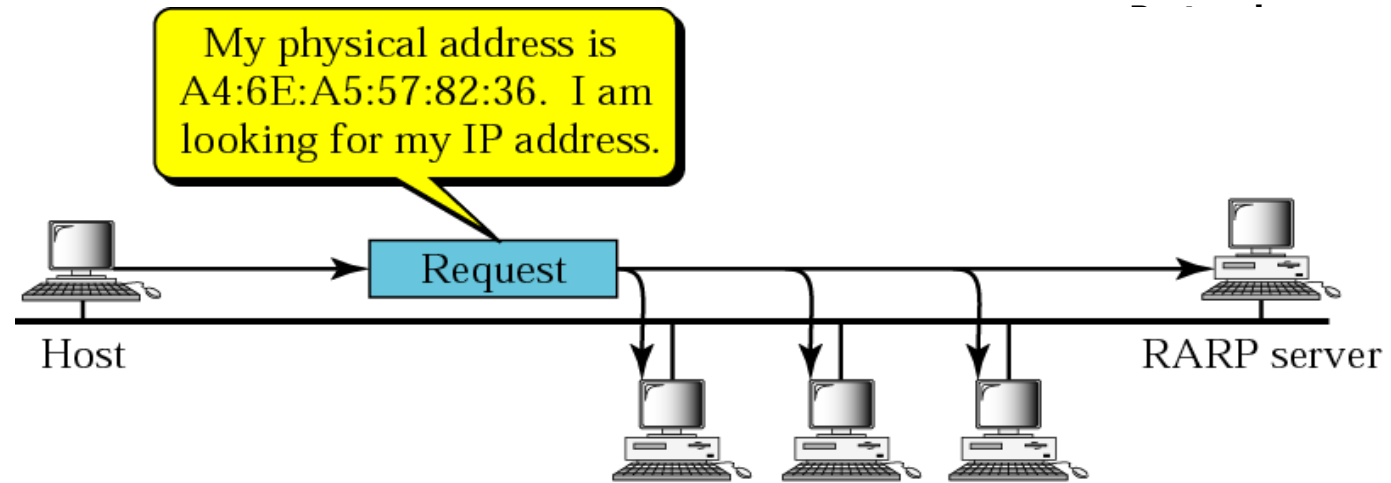
Alternative Solutions to RARP



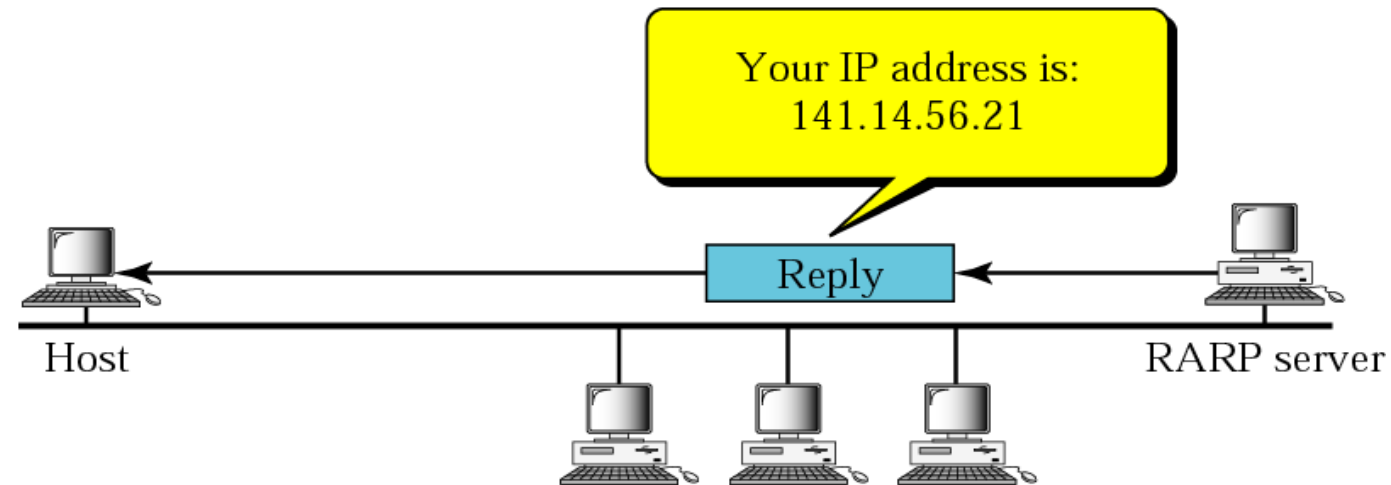
Note:

*The RARP request packets are broadcast;
the RARP reply packets are unicast.*

Figure 7.10 *RARP operation*



a. RARP request is broadcast



b. RARP reply is unicast

Figure 7.11 *RARP packet*

24

**TCP/IP
Protocol
Suite**

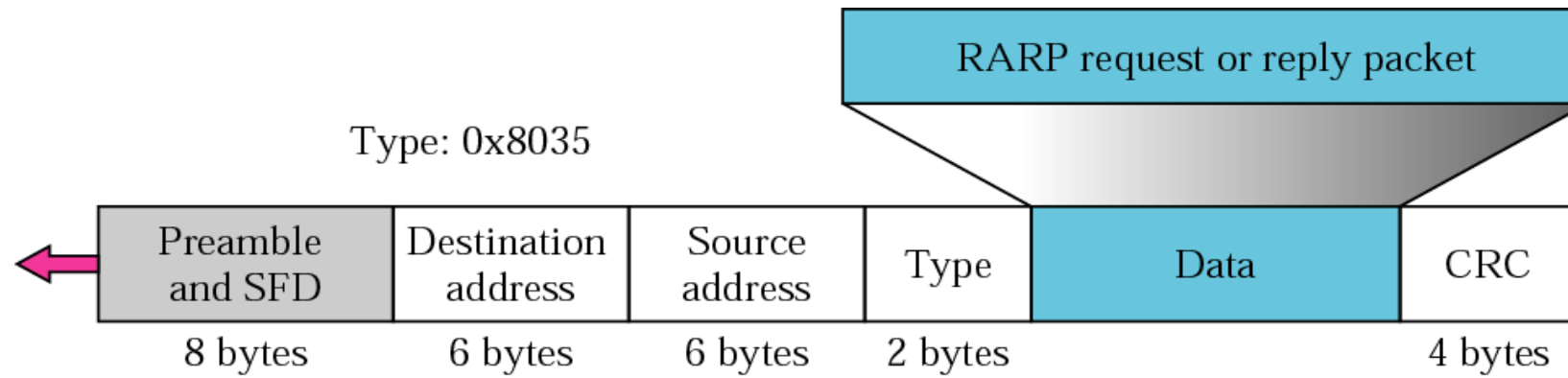
Hardware type		Protocol type
Hardware length	Protocol length	Operation Request 3, Reply 4
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP) (It is not filled for request)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled for request)		
Target protocol address (For example, 4 bytes for IP) (It is not filled for request)		



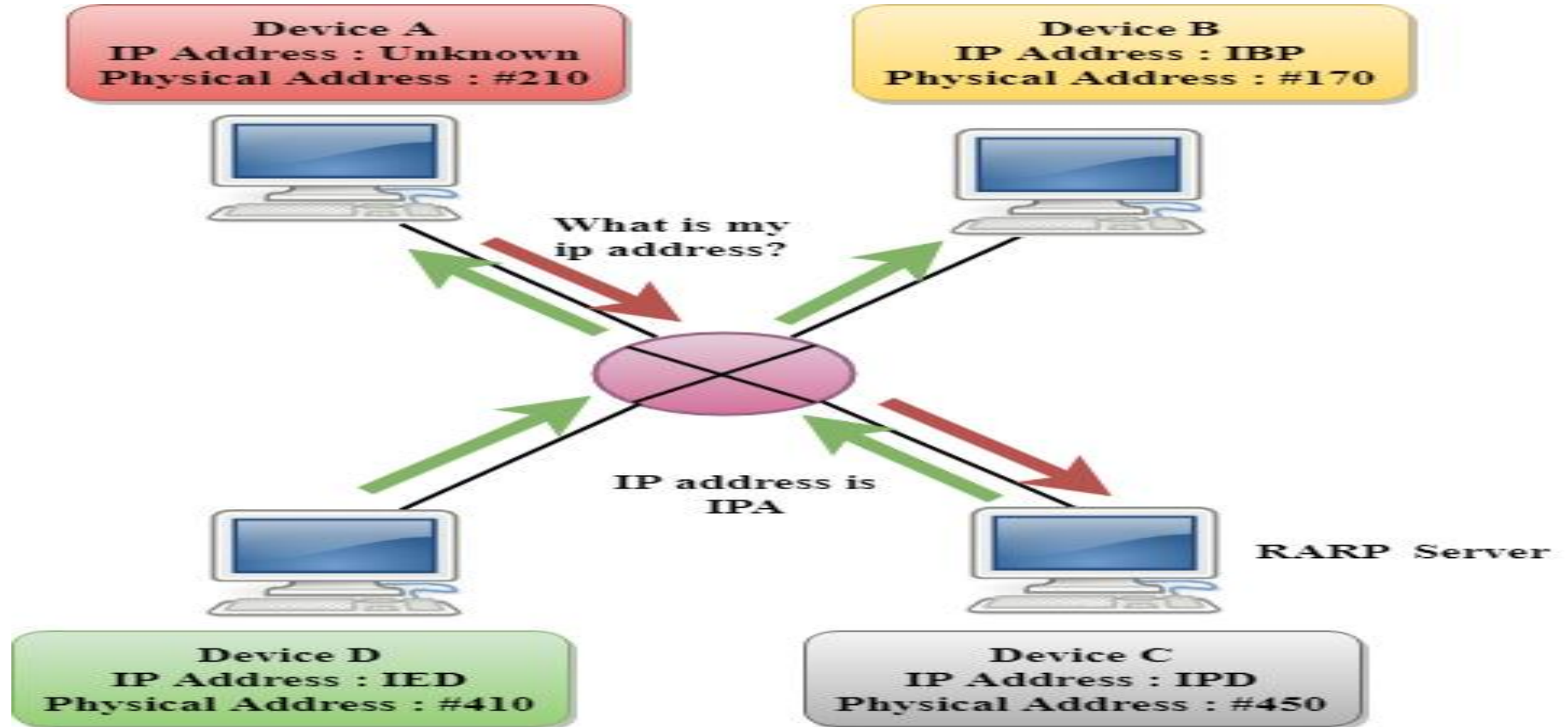
Figure 7.12 *Encapsulation of RARP packet*

25

**TCP/IP
Protocol
Suite**

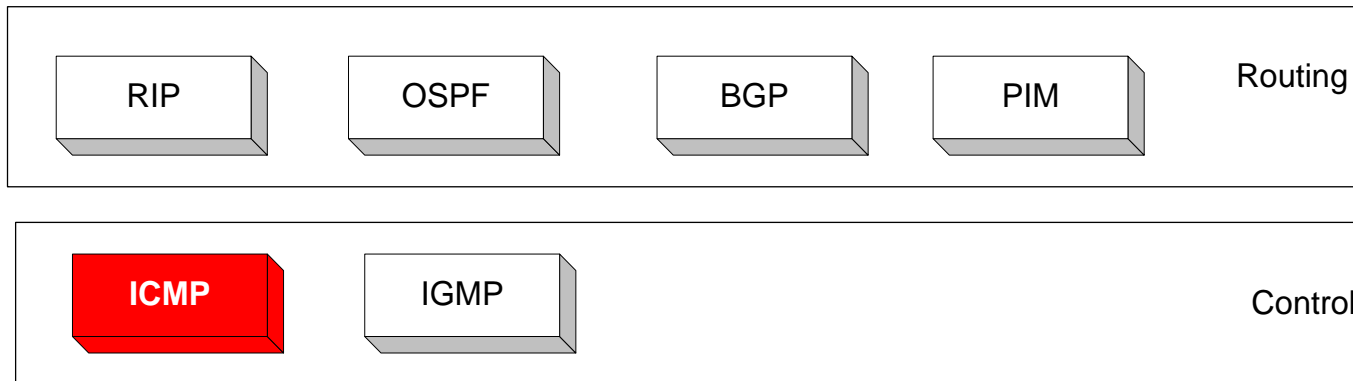


RARP



Overview

- The IP (Internet Protocol) relies on several other protocols to perform necessary control and routing functions:
 - Control functions (ICMP)
 - Multicast signaling (IGMP)
 - Setting up routing tables (RIP, OSPF, BGP, PIM, ...)



Internet Control Message Protocol (ICMP)

Relates to Lab 2:

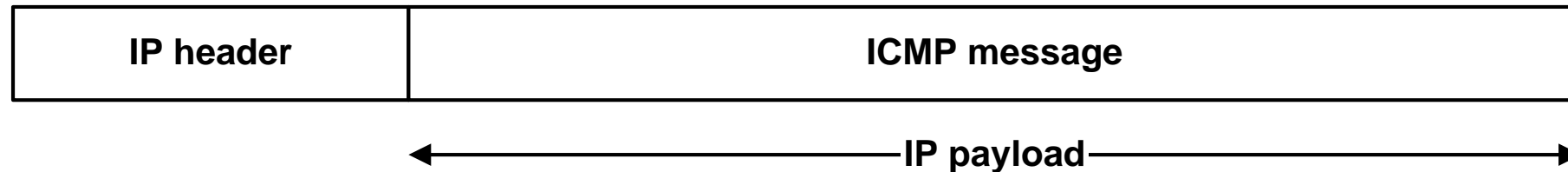
A short module on the Internet Control Message Protocol (ICMP).

ICMP - Internet Control Message Protocol.

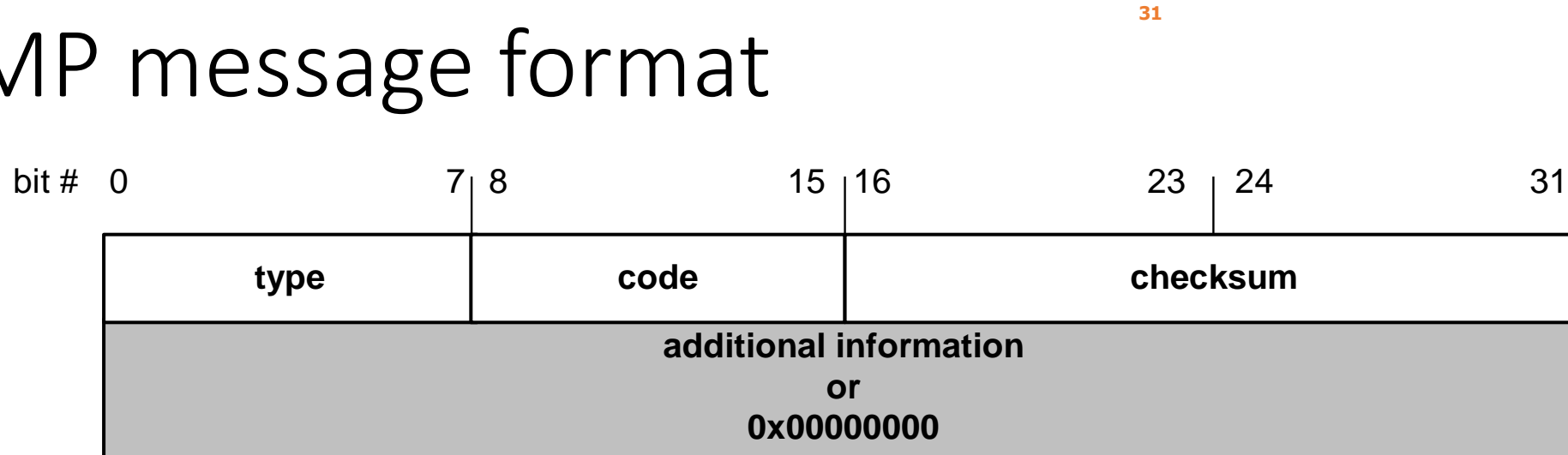
- The ICMP is used by hosts and routers to send the notifications of IP datagram problems back to the sender.
- It uses echo test/reply to check whether the destination is reachable and responding.
- ICMP handles both control and error messages, but its main function is to report the error but not to correct them.
- An IP datagram contains the addresses of both source and destination, but it does not know the address of the previous router through which it has been passed. Due to this reason, ICMP can only send the messages to the source, but not to the immediate routers.
- ICMP protocol communicates the error messages to the sender. ICMP messages cause the errors to be returned back to the user processes.
- ICMP messages are transmitted within IP datagram.

Overview

- The **Internet Control Message Protocol (ICMP)** is a helper protocol that supports IP with facility for
 - Error reporting
 - Simple queries
- ICMP messages are encapsulated as IP datagrams:



ICMP message format



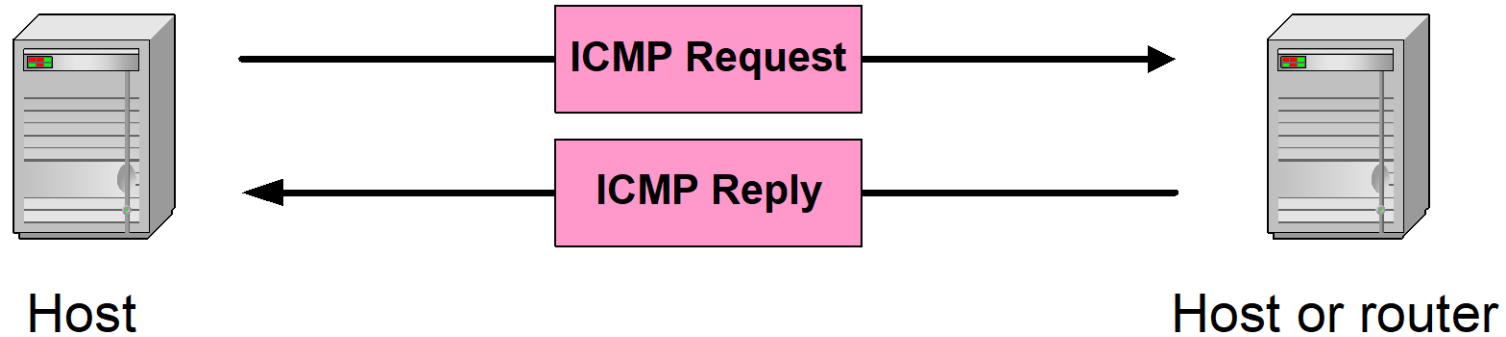
4 byte header:

- **Type (1 byte):** type of ICMP message
- **Code (1 byte):** subtype of ICMP message
- **Checksum (2 bytes):** similar to IP header checksum.
Checksum is calculated over entire ICMP message

If there is no additional data, there are 4 bytes set to zero.

→ each ICMP messages is at least 8 bytes long


ICMP Query message



ICMP query:

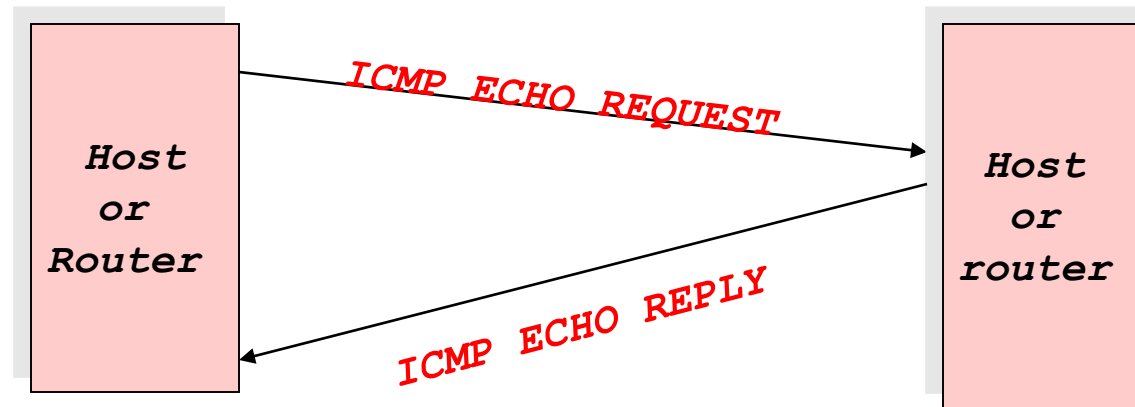
- **Request** sent by host to a router or host
- **Reply** sent back to querying host

Example of ICMP Queries

Type/Code:	Description	
8/0	Echo Request	 The ping command uses Echo Request/ Echo Reply
0/0	Echo Reply	
13/0	Timestamp Request	
14/0	Timestamp Reply	
10/0	Router Solicitation	
9/0	Router Advertisement	

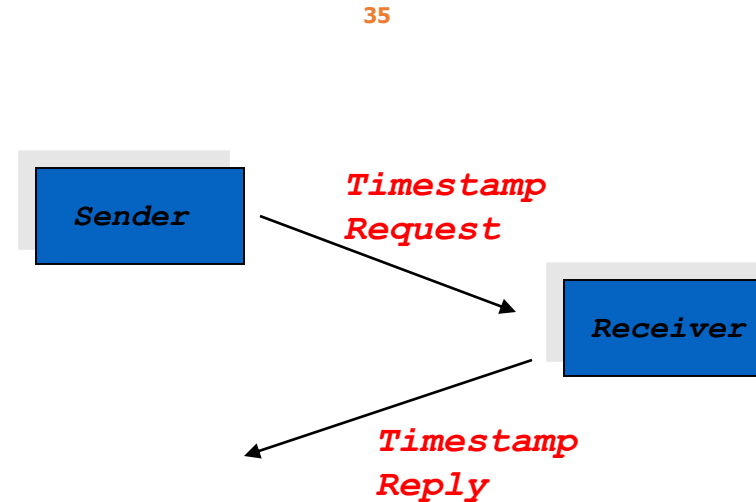
Example of a Query: Echo Request and Reply

- Ping's are handled directly by the kernel
- Each Ping is translated into an **ICMP Echo Request**
- The Ping'ed host responds with an **ICMP Echo Reply**



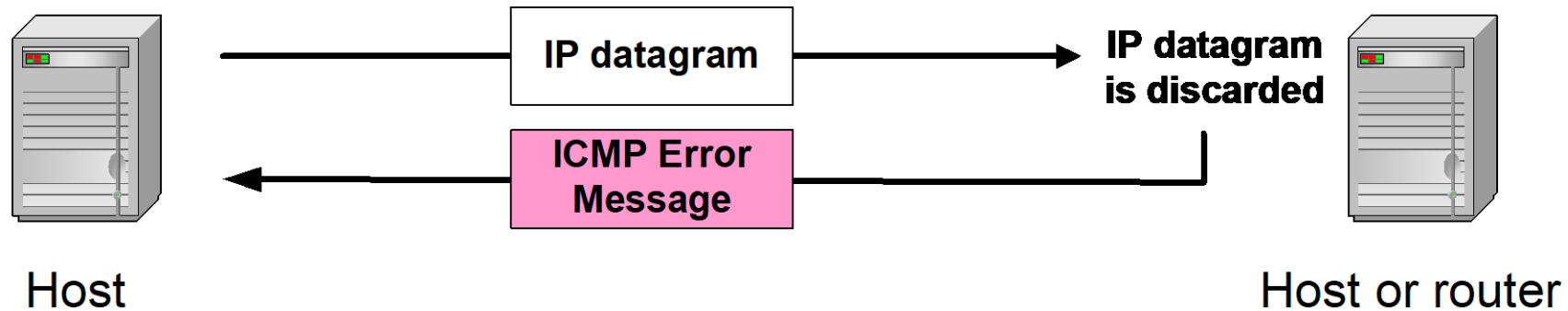
Example of a Query: ICMP Timestamp

- A system (host or router) asks another system for the current time.
- Time is measured in milliseconds after midnight UTC (Universal Coordinated Time) of the current day
- Sender sends a **request**, receiver responds with **reply**



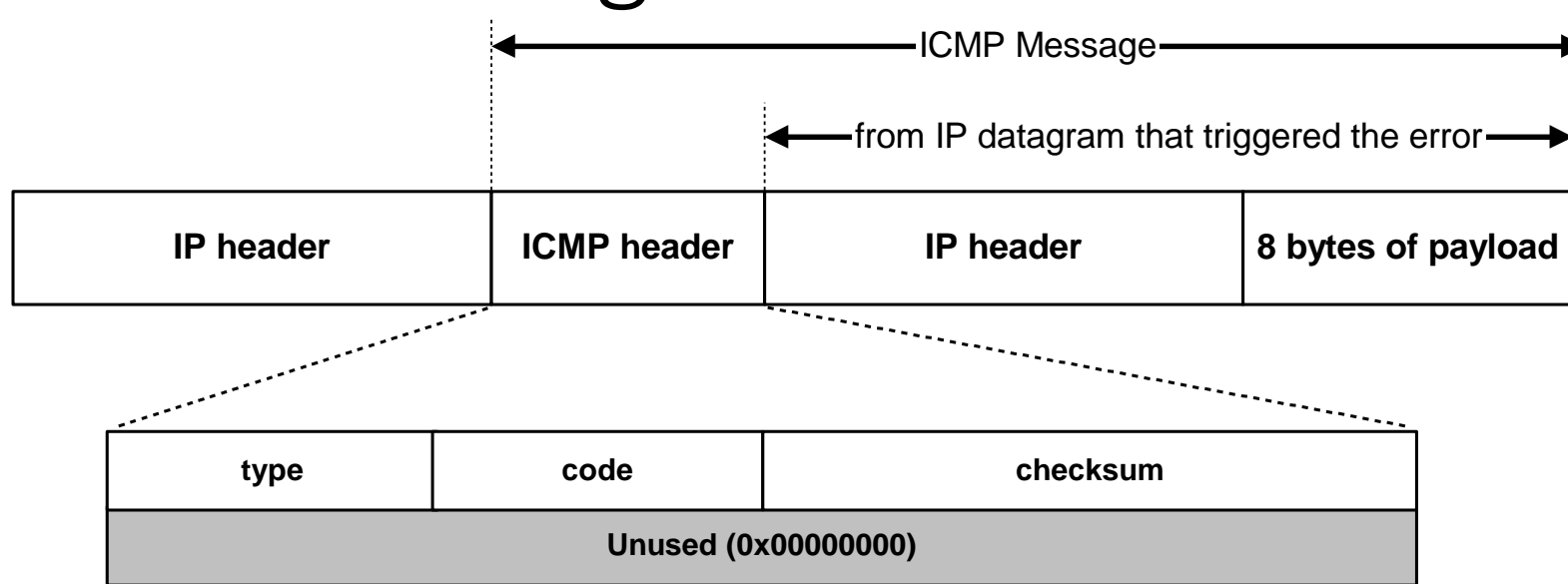
Type (= 17 or 18)	Code (=0)	Checksum
identifier		sequence number
32-bit sender timestamp		
32-bit receive timestamp		
32-bit transmit timestamp		

ICMP Error message



- **ICMP error messages report error conditions**
- **Typically sent when a datagram is discarded**
- **Error message is often passed from ICMP to the application program**

ICMP Error message



- **ICMP error messages include the complete IP header and the first 8 bytes of the payload (typically: UDP, TCP)**

Frequent ICMP Error message

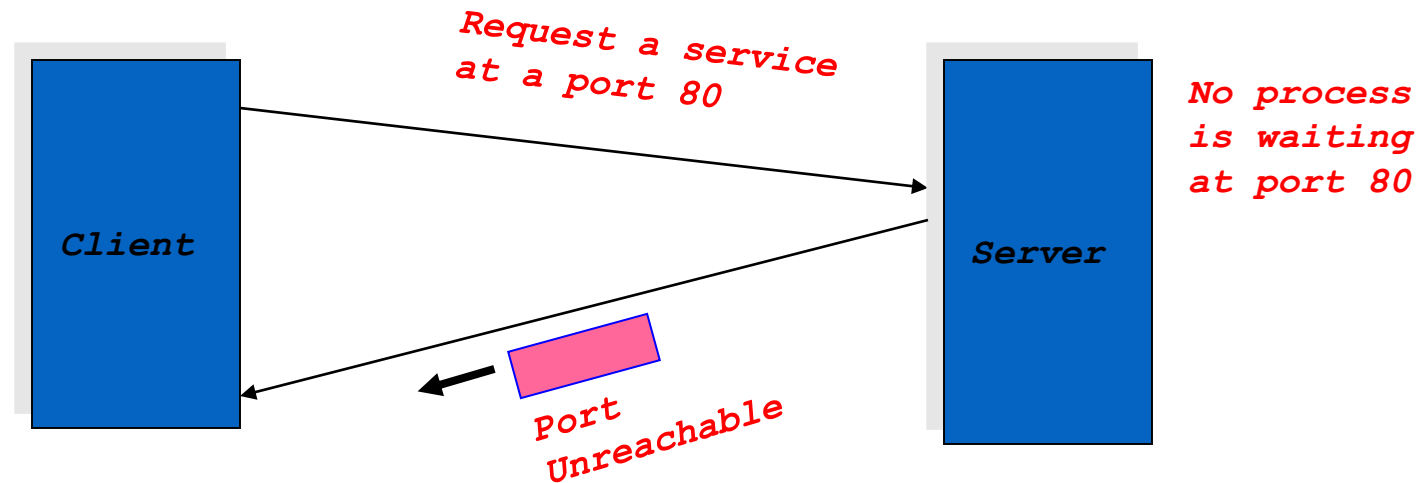
Type	Code	Description	
3	0–15	Destination unreachable	Notification that an IP datagram could not be forwarded and was dropped. The code field contains an explanation.
5	0–3	Redirect	Informs about an alternative route for the datagram and should result in a routing table update. The code field explains the reason for the route change.
11	0, 1	Time exceeded	Sent when the TTL field has reached zero (Code 0) or when there is a timeout for the reassembly of segments (Code 1)
12	0, 1	Parameter problem	Sent when the IP header is invalid (Code 0) or when an IP header option is missing (Code 1)

Some subtypes of the “Destination Unreachable”

Code	Description	Reason for Sending
0	Network Unreachable	No routing table entry is available for the destination network.
1	Host Unreachable	Destination host should be directly reachable, but does not respond to ARP Requests.
2	Protocol Unreachable	The protocol in the protocol field of the IP header is not supported at the destination.
3	Port Unreachable	The transport protocol at the destination host cannot pass the datagram to an application.
4	Fragmentation Needed and DF Bit Set	IP datagram must be fragmented, but the DF bit in the IP header is set.

Example: ICMP Port Unreachable⁴⁰

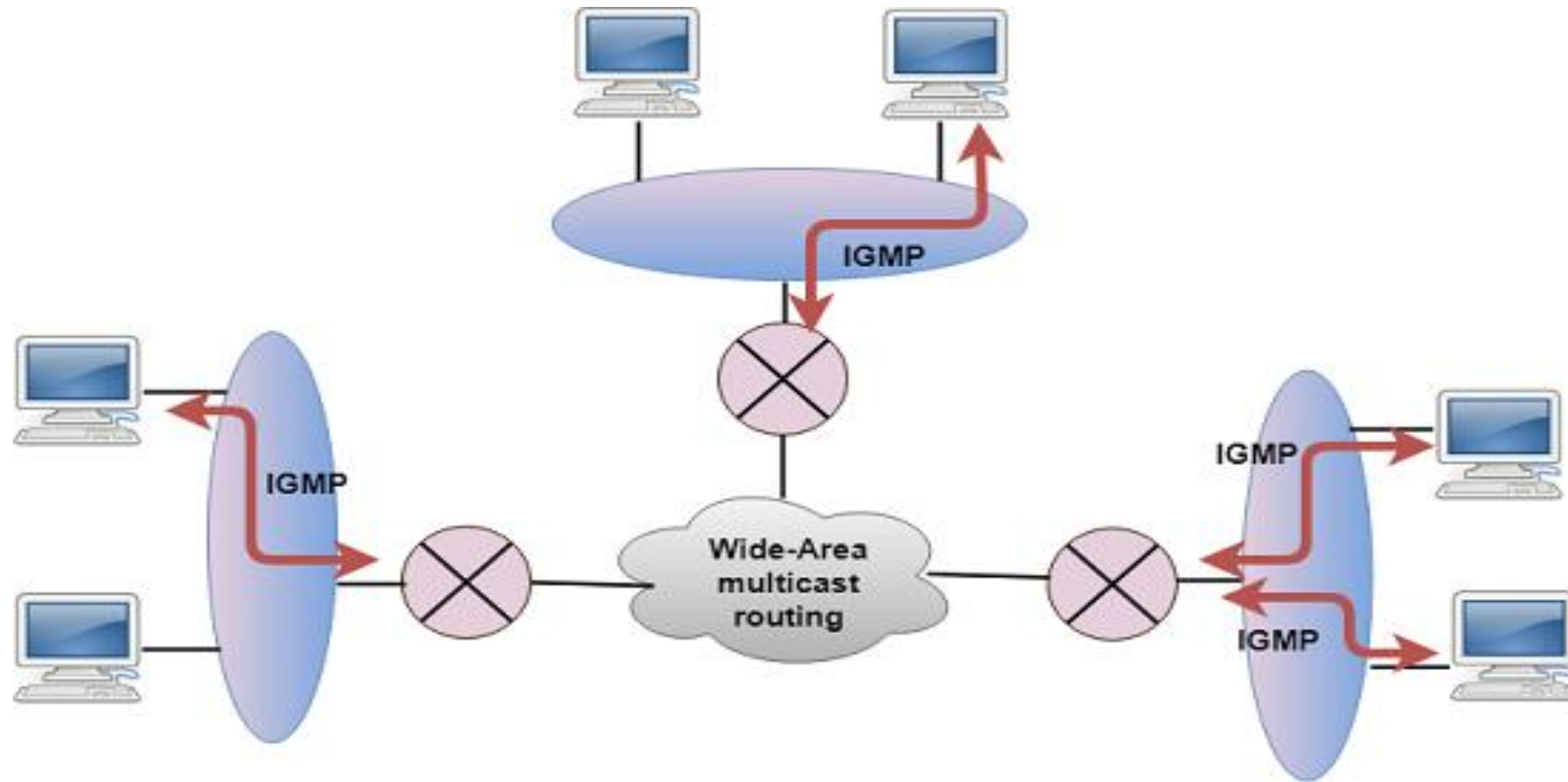
- RFC 792: If, in the destination host, the IP module cannot deliver the datagram because the indicated protocol module or process port is not active, the destination host may send a destination unreachable message to the source host.
- Scenario:



IGMP - Internet Group Message Protocol.

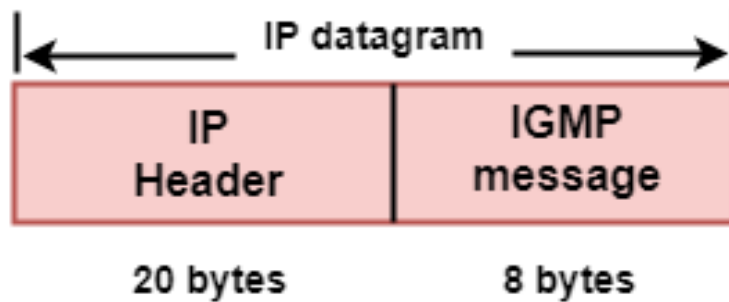
- The IP protocol supports two types of communication:
 - **Unicasting:** It is a communication between one sender and one receiver. Therefore, we can say that it is one-to-one communication.
 - **Multicasting:** Sometimes the sender wants to send the same message to a large number of receivers simultaneously. This process is known as multicasting which has one-to-many communication.
- The IGMP protocol is used by the hosts and router to support multicasting.
- The IGMP protocol is used by the hosts and router to identify the hosts in a LAN that are the members of a group.

IGMP



IGMP

- IGMP is a part of the IP layer, and IGMP has a fixed-size message.
- The IGMP message is encapsulated within an IP datagram.



IGMP Format

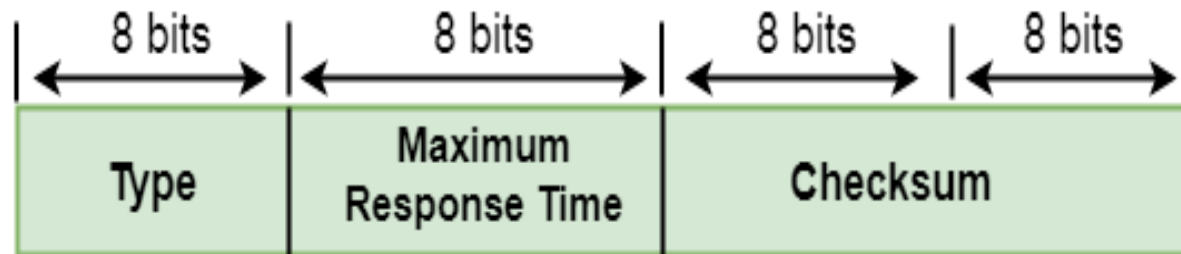
Type: There are three types of IGMP message: Membership Query, Membership Report and Leave Report.

Maximum Response Time: It determines the maximum time the host can send the Membership Report message in response to the Membership Query message.

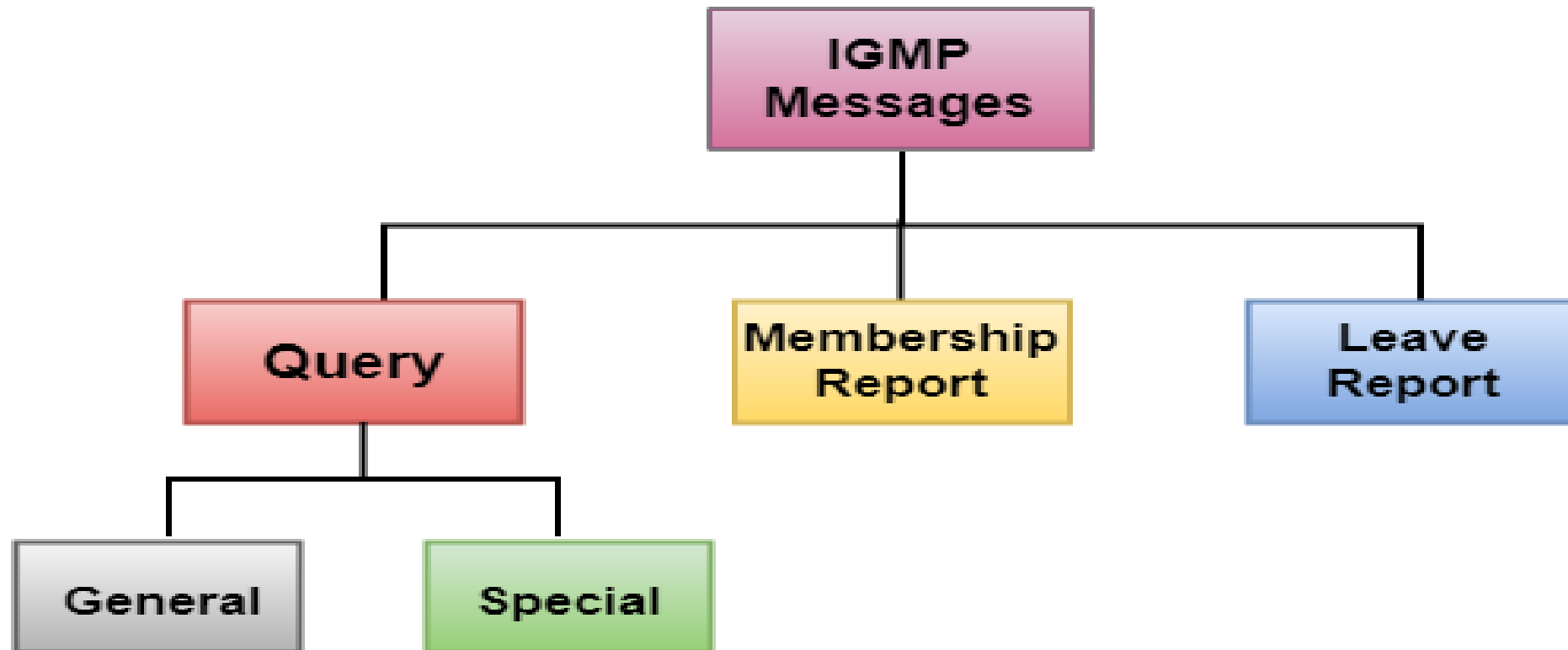
Checksum: It determines the entire payload of the IP datagram in which IGMP message is encapsulated.

Group Address: The behavior of this field depends on the type of the message sent.

- **For Membership Query**, the group address is set to zero for General Query and set to multicast group address for a specific query.
- **For Membership Report**, the group address is set to the multicast group address.
- **For Leave Group**, it is set to the multicast group address.



IGMP Messages



References

- <https://www.javatpoint.com/network-layer-protocols>