Network Layer: Protocols

Address Mapping

- *A packet starting from a host may pass through several different physical networks before reaching the destination host.*
- *Hosts and routers are recognized at the network level by their logical (IP) addresses.*
- *At the physical level, the host and routers are recognized by their physical (MAC) addresses.*

- *The delivery of a packet to a host or a router requires two levels of addressing: logical and physical.*

- *We need to be able to map a logical address to its corresponding physical address and vice versa.*

- *This can be done by using either static or dynamic mapping.*

Address Mapping

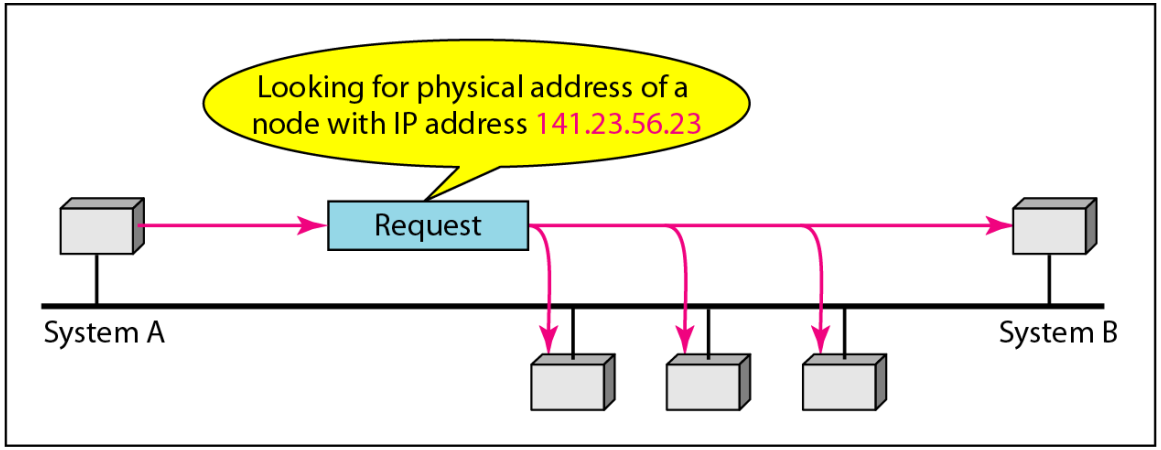
- ***Static mapping*** involves in the creation of a table that associates a logical address with a physical address.
- This table is stored in each machine on the network.
- Each machine that knows, for example, the IP address of another machine but not its physical address can look it up in the table.
- This has some limitations because physical addresses may change

- In ***dynamic mapping*** each time a machine knows one of the two addresses (logical or physical), it can use a protocol to find the other one.

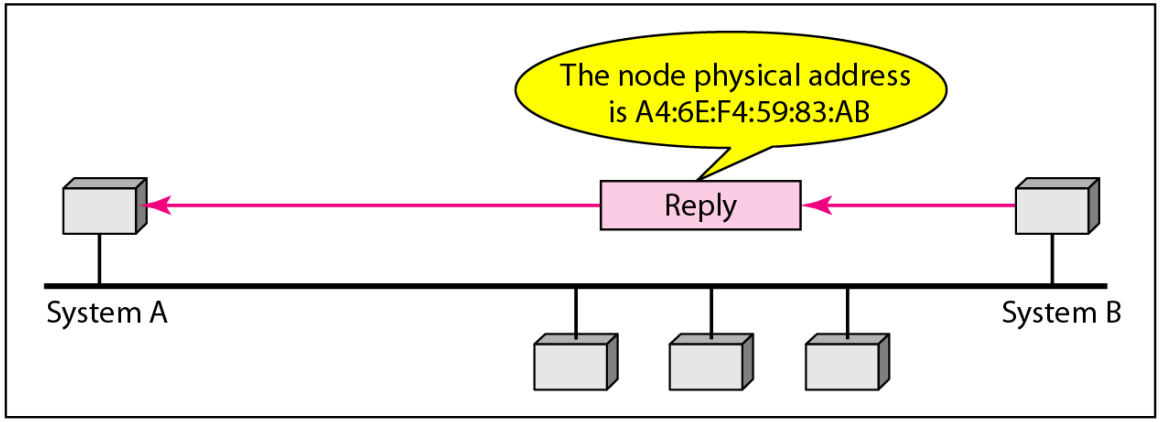
Mapping Logical to Physical Address: **ARP**

- Anytime a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver.
- The logical (IP) address is obtained from the *DNS* if the sender is the host or it is found in a routing table if the sender is a router.
- But the IP datagram must be encapsulated in a frame to be able to pass through the physical network.
- This means that the sender needs the physical address of the receiver.
- The host or the router sends an ***ARP query packet.***
  - The packet includes the *physical and IP addresses of the sender and the IP address of the receiver.*
  - Because the sender does not know the physical address of the receiver, the query is broadcast over the network

ARP operation



a. ARP request is broadcast



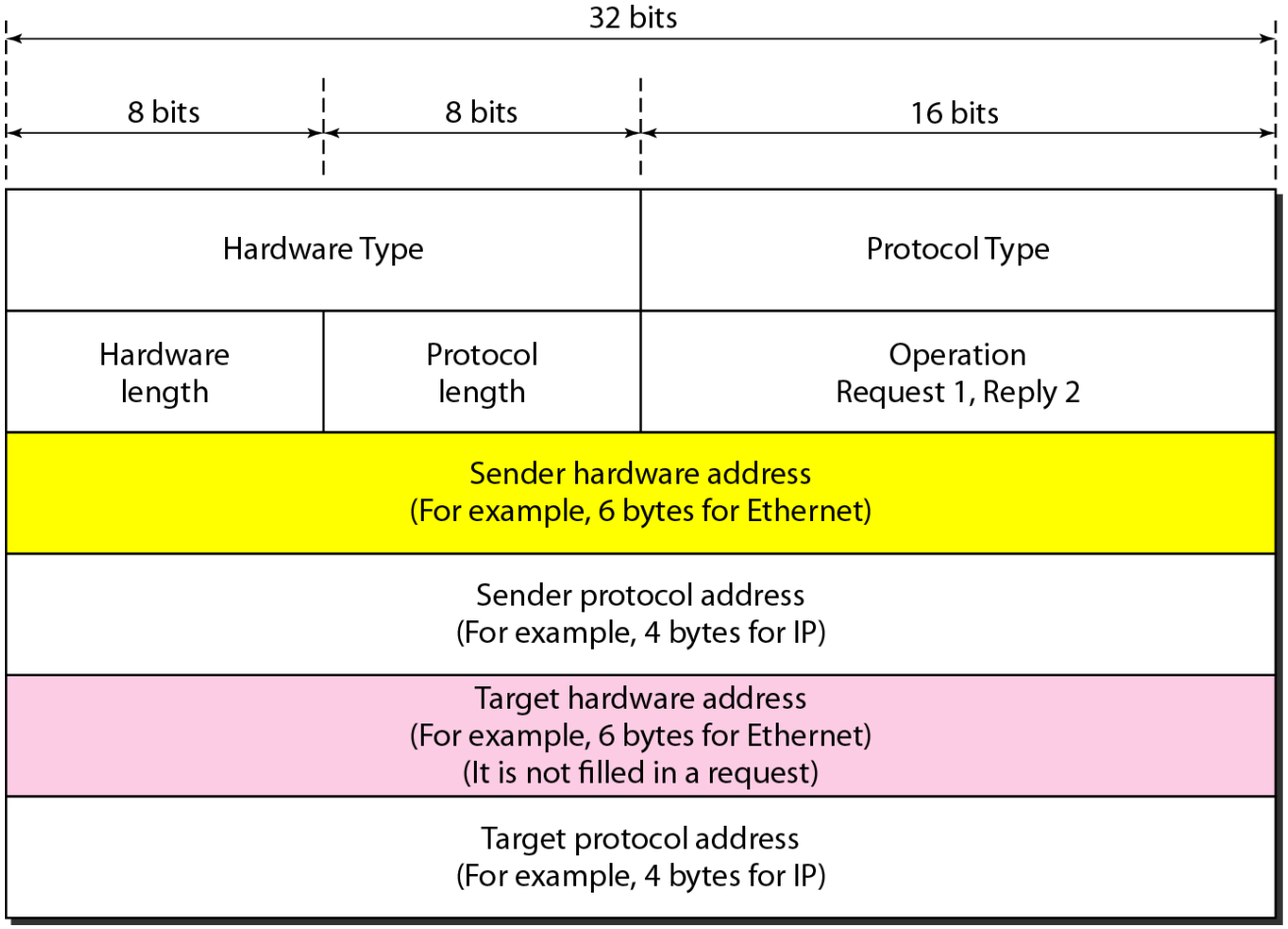
b. ARP reply is unicast

- **The response packet contains the *recipient's IP and physical addresses*.**

Cache Memory

- Use of ARP protocol by the sender for every IP packet is inefficient
- Instead if the host itself store the mapped information in cache memory and use that it will speed up sending the packets.
- Before sending an ARP request, the system first checks its cache to see if it can find the mapping.

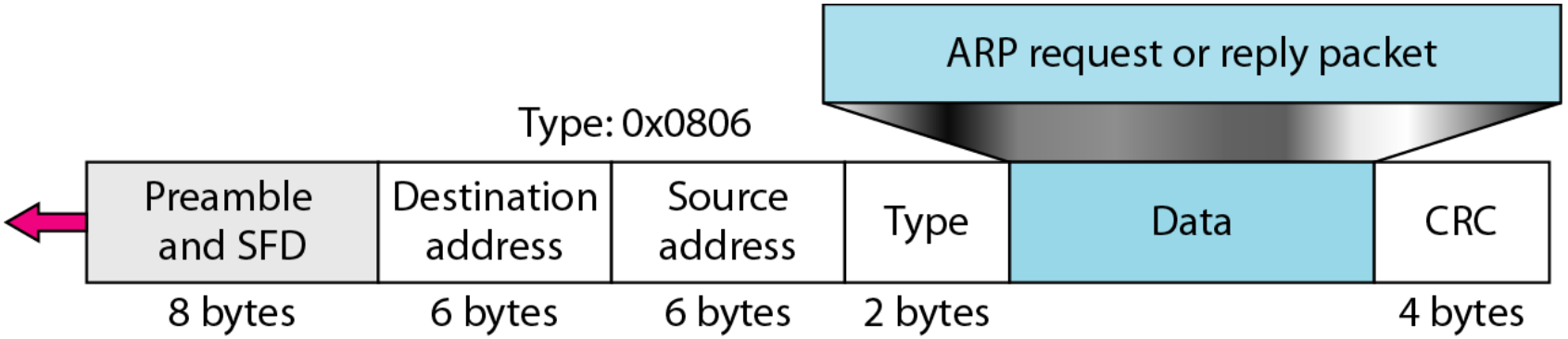
ARP packet


32 bits
8 bits
8 bits
16 bits
Hardware Type
Protocol Type
Hardware length
Protocol length
Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)
Sender protocol address (For example, 4 bytes for IP)
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)
Target protocol address (For example, 4 bytes for IP)

ARP packet fields

- **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.
  - **Example:** Ethernet is given type 1
- **Protocol type:**
  - This is a 16-bit field defining the protocol.
  - **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.
  - **Example:** for Ethernet the value is 6.
- **Protocol length:**
  - This is an 8-bit field defining the length of the logical address in bytes.
  - 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).

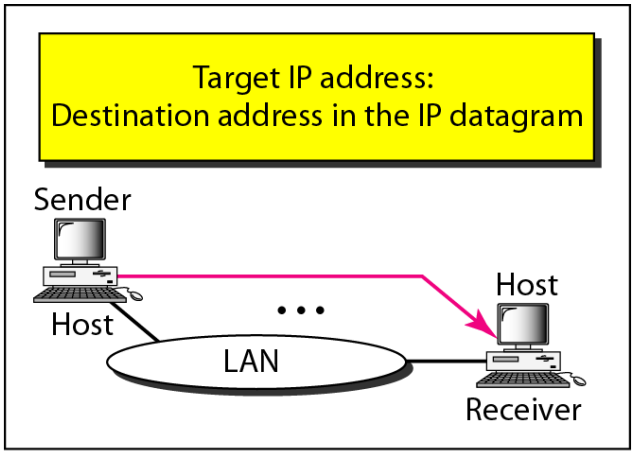
Encapsulation of ARP packet



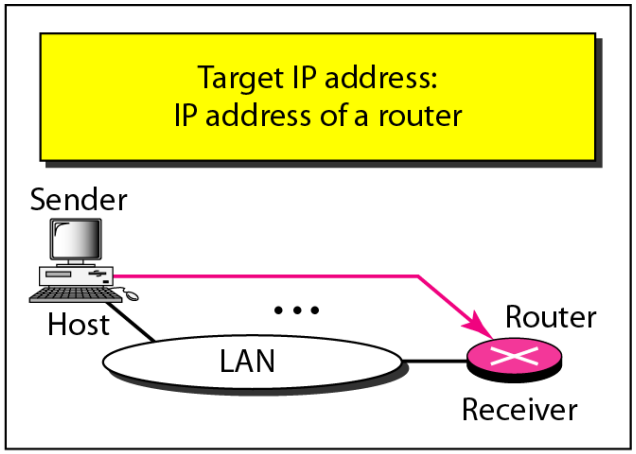
ARP operation

- **Steps:**
  - Sender knows the IP address of the receiver (using DNS)
  - IP asks ARP to create an ARP request message
  - The target physical address field is filled with 0s.
  - The message is passed to the data link layer
    - Physical address of the sender as the source address and the
    - ***Physical broadcast address as the destination address.***
  - Every host or router receives the frame.
  - All machines except the one targeted drop the packet.
  - The target machine recognizes its IP address.
  - The target machine replies with an ARP reply message
  - The sender receives the reply message.
  - The IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.

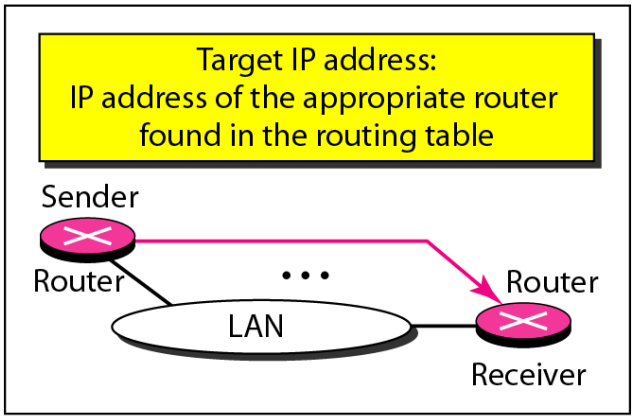
Four cases using ARP



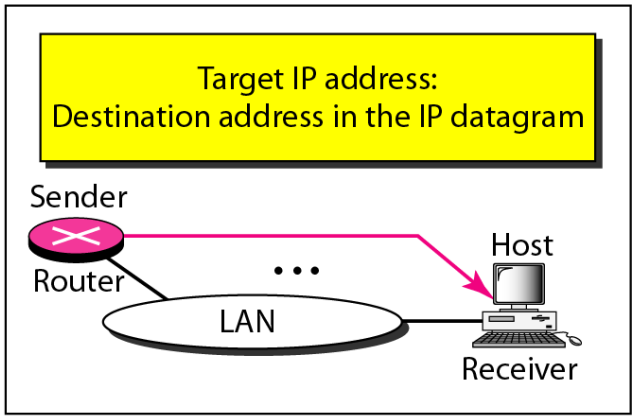
Case 1. A host has a packet to send to another host on the same network.



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



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



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

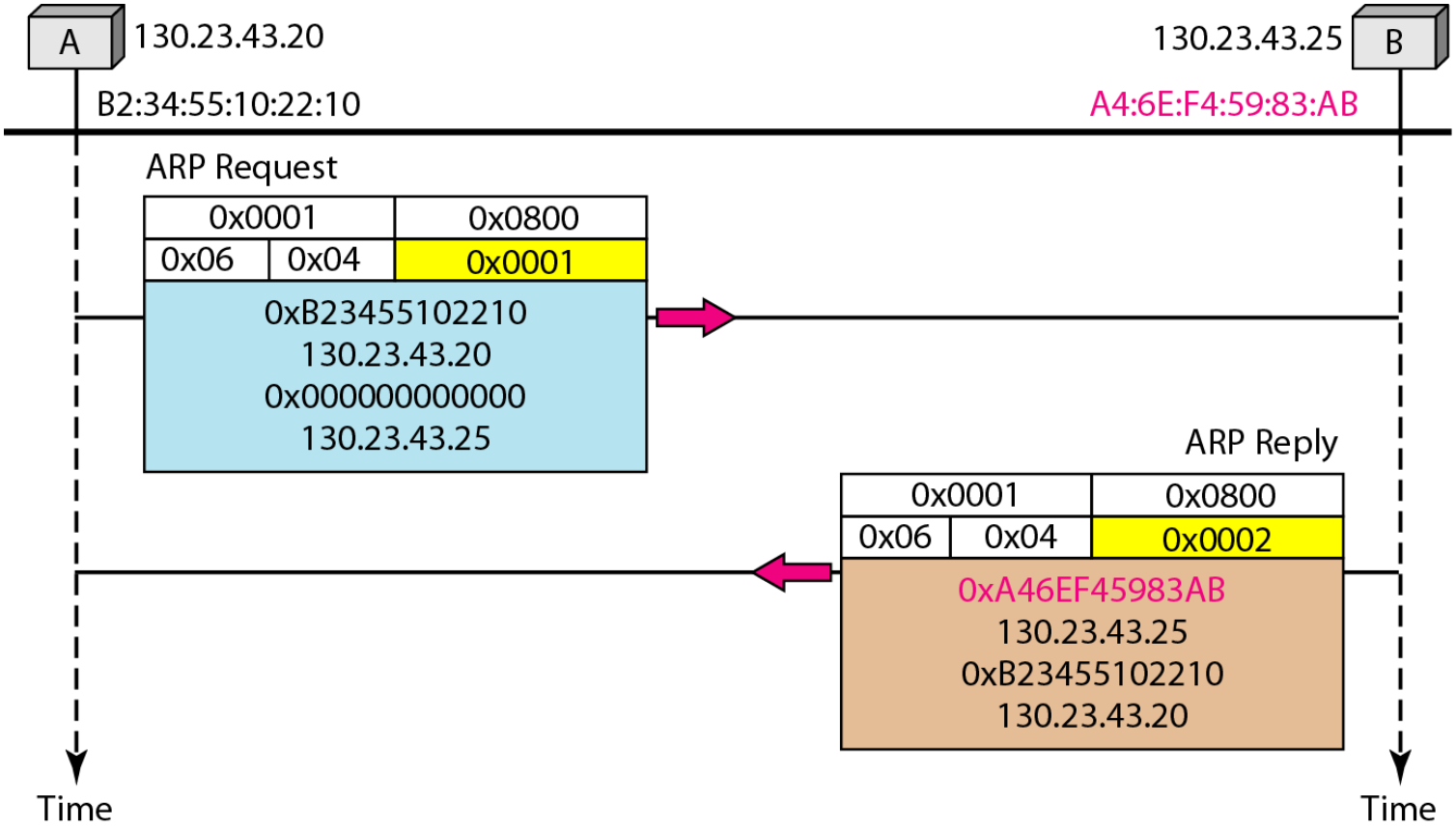
Note

An ARP request is broadcast;
an ARP reply is unicast.

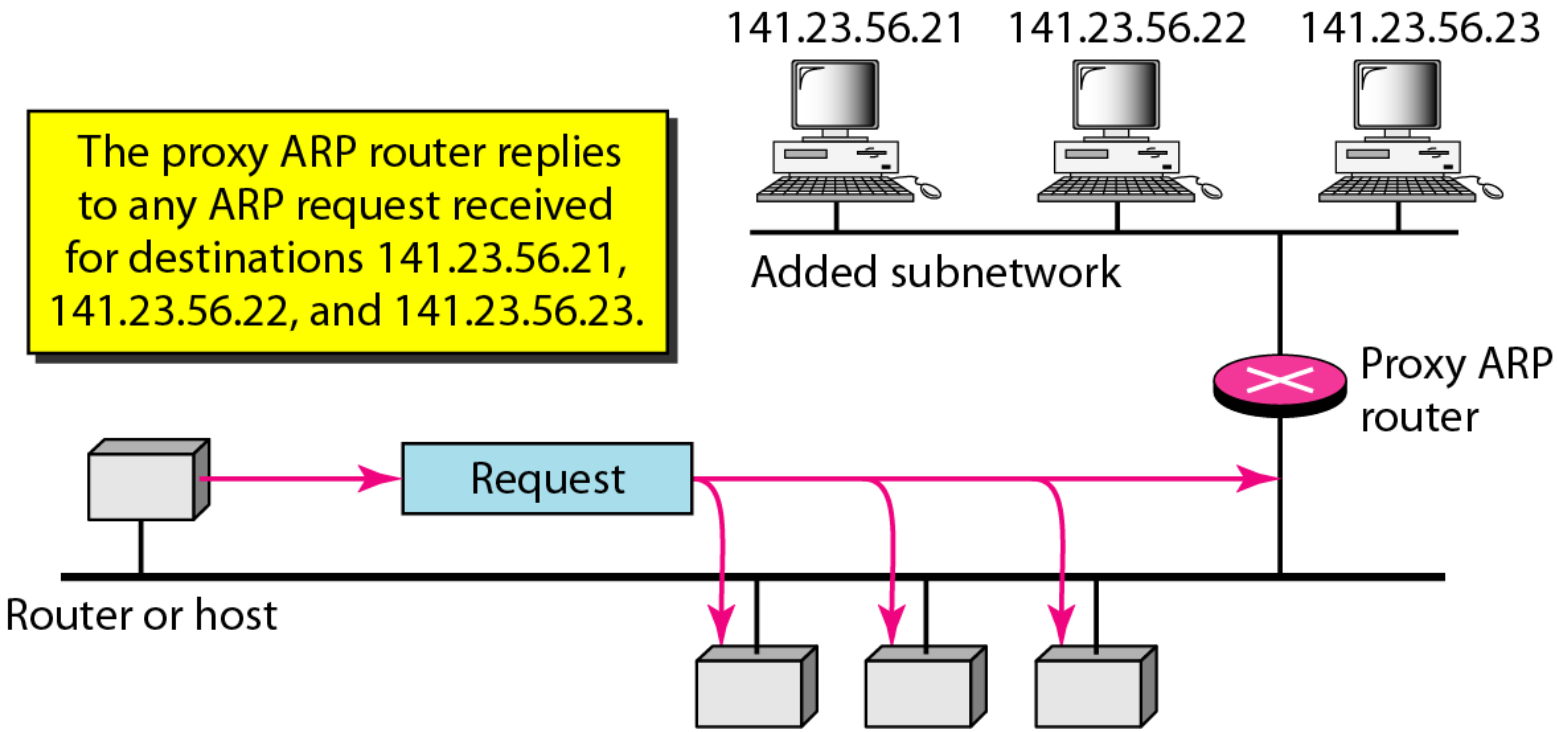
Example

A host with IP address 130.23.43.20 and physical address B2:34:55:10:22:10 has a packet to send to another host with IP address 130.23.43.25 and physical address A4:6E:F4:59:83:AB. The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.

Solution



Proxy ARP



- ARP request looking for the IP address of one of these hosts, the router sends an ARP reply announcing its own hardware (physical) address.
- After the router receives the actual IP packet, it sends the packet to the appropriate host or router.

Mapping Physical to Logical Address: RARP, BOOTP, and DHCP

- There are occasions in which a host knows its physical address, but needs to know its logical address.
- This may happen in two cases:
  - 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.
  - 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.

RARP

- Reverse Address Resolution Protocol (RARP) finds the logical address for a machine that knows only its physical address.
- A RARP request is created and broadcast on the local network.
- Another machine on the local network that knows all the IP addresses will respond with a RARP reply.
- The requesting machine must be running a RARP client program;
- The responding machine must be running a RARP server program.

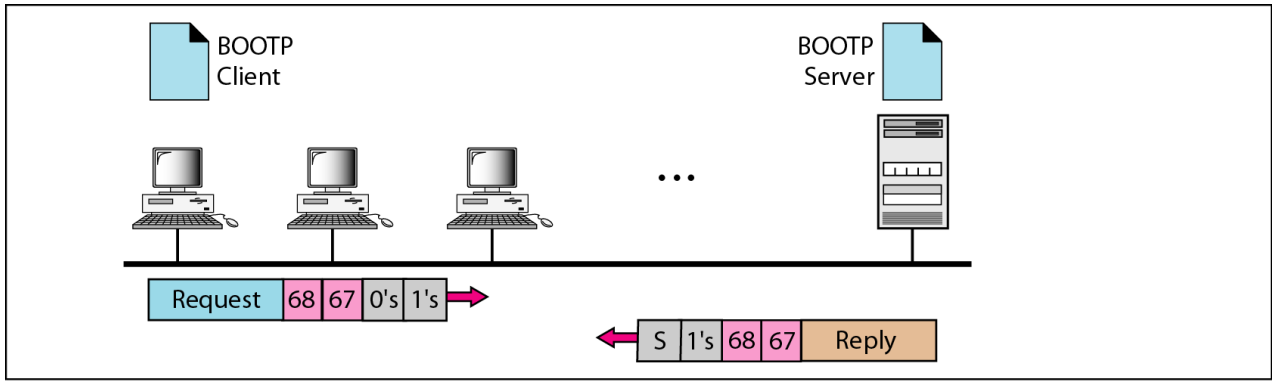
RARP : Problem

- Broadcasting is done at the data link layer.
- The physical broadcast address, all is in the case of Ethernet, does not pass the boundaries of a network.
- This means that if an administrator has several networks or several subnets
  - It needs to assign a RARP server for each network or subnet.
- This is the reason that RARP is almost obsolete.
- Two protocols, BOOTP and DHCP, are replacing RARP.

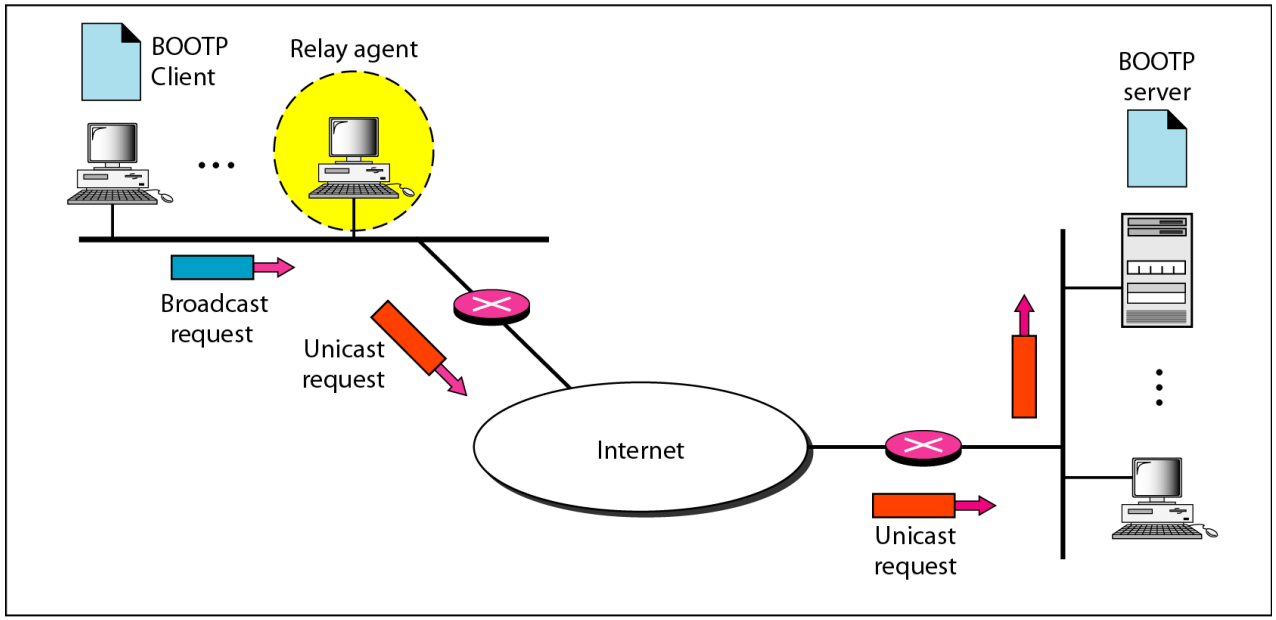
BOOTP

- The Bootstrap Protocol (BOOTP) is a client/server protocol designed to provide physical address to logical address mapping.
- BOOTP is an *application layer protocol.*
- The administrator may put the client and the server on the same network or on different networks.
- BOOTP messages are encapsulated in a UDP packet, and the UDP packet itself is encapsulated in an IP packet.
-

BOOTP client and server on the same and different networks



a. Client and server on the same network



b. Client and server on different networks

Note

DHCP provides static and dynamic address allocation that can be manual or automatic.

DHCP

- BOOTP can not handle
  - if a host moves from one physical network to another
  - if a host wants a temporary IP address
- Reason: BOOTP is a static configuration protocol.
- The Dynamic Host Configuration Protocol (DHCP) has been devised to provide static and dynamic address allocation that can be manual or automatic.

DHCP

- Dynamic Address Allocation
- DHCP has a second database
- This second database makes DHCP dynamic.
  - When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available (unused) IP addresses and assigns an IP address for a negotiable period of time.
- DHCP provides temporary IP addresses for a limited time as lease.
- When the lease expires, the client must either stop using the IP address or renew the lease.
- The server has the option to agree or disagree with the renewal.
- If the server disagrees, the client stops using the address.

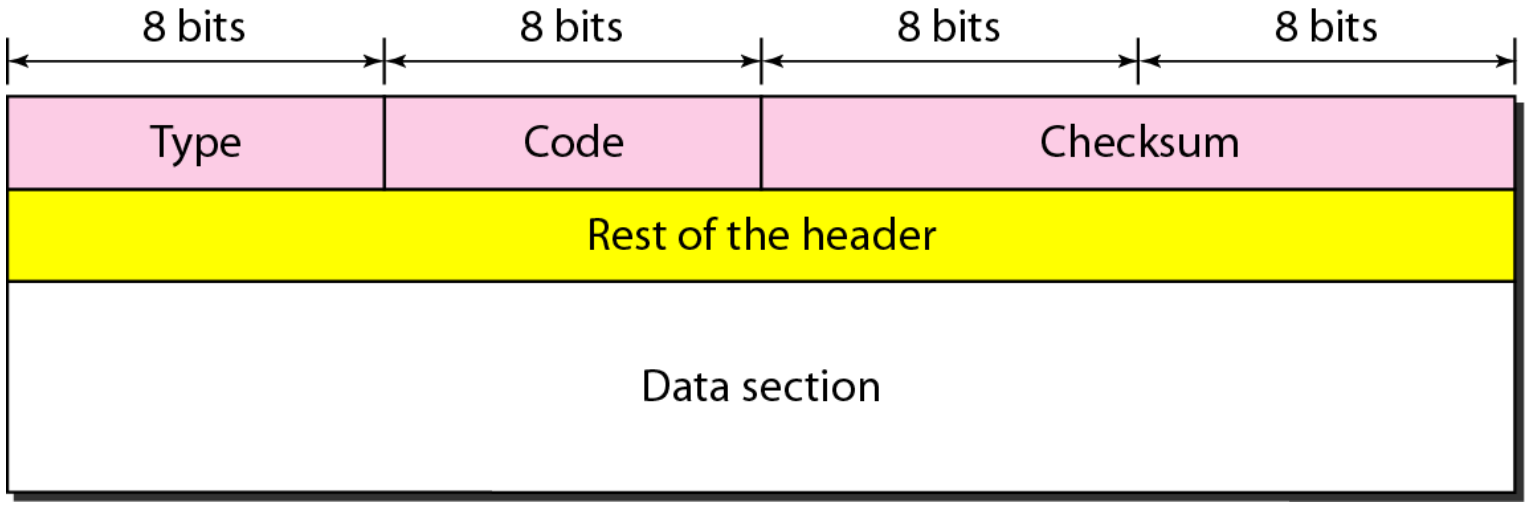
ICMP

- *The IP protocol has no error-reporting or error-correcting mechanism.*
- *The IP protocol also lacks a mechanism for host and management queries.*
- *The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies.*
- *It is a companion to the IP protocol.*
- *We will look into*
    - **Types of Messages**
    - **Message Format**
    - **Error Reporting and Query**
    - **Debugging Tools**

Types of Messages

- ICMP messages are divided into two broad categories:
  - Error-reporting messages:
    - Report problems that a router or a host (destination) may encounter when it processes an IP packet.
  - Query messages:
    - Which occur in pairs, help a host or a network manager get specific information from a router or another host.

General format of ICMP messages



- **An ICMP message has an 8-byte header and a variable-size data section.**

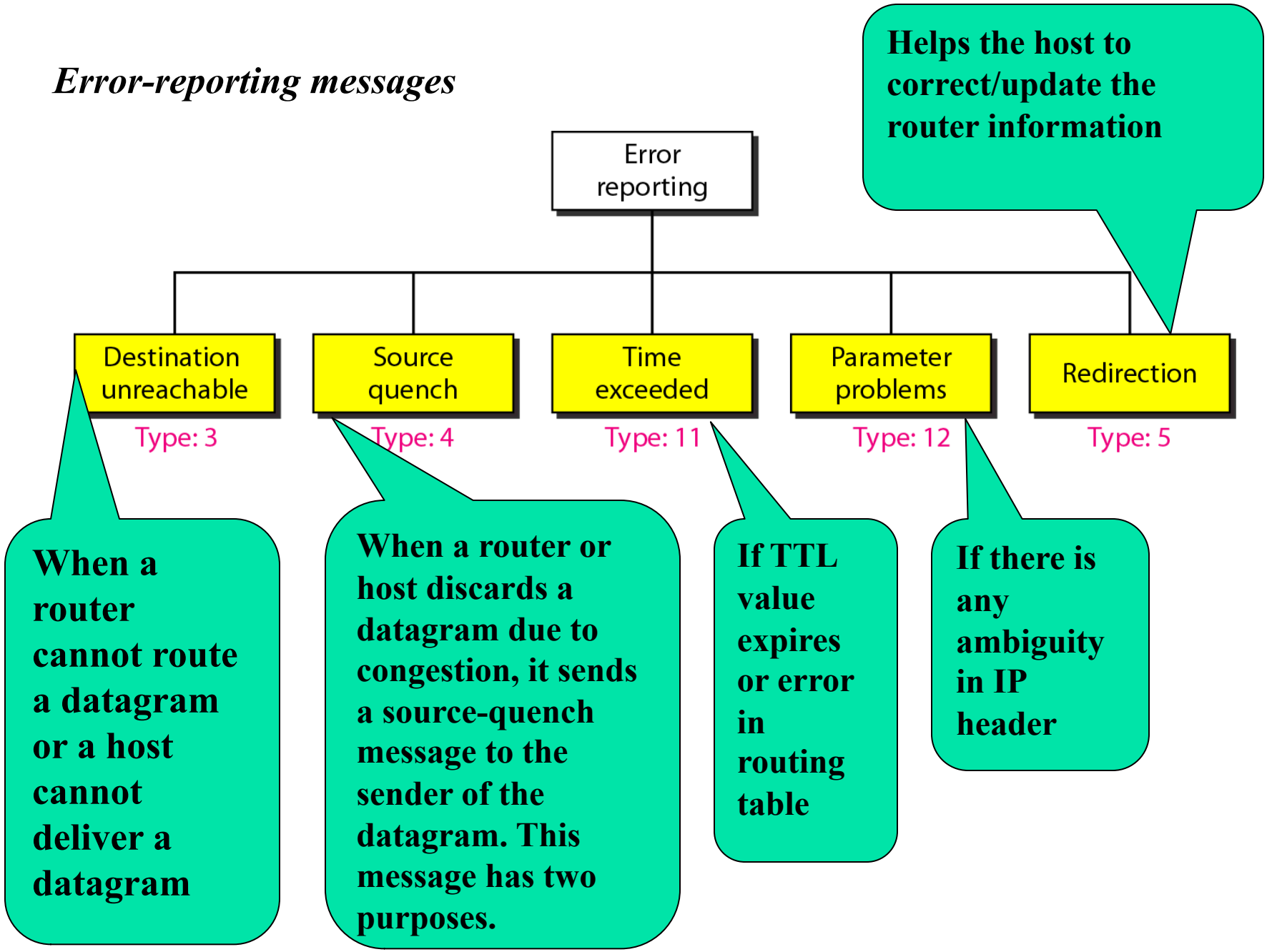
ICMP message

- **Type (8 bits):** Type of ICMP message
- **Code (8 bits):** specifies the reason for the particular message type
- The ***rest of the header*** is specific for each message type.
- The **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.

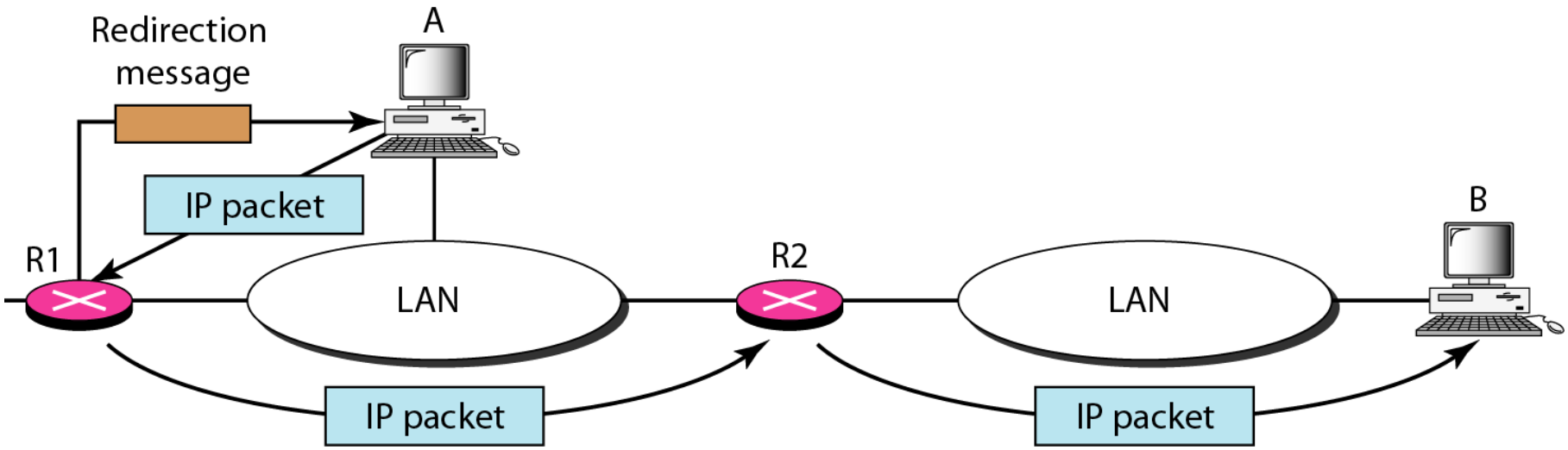
Note

- **ICMP always reports error messages to the original source.**
- **ICMP does not correct errors-it simply reports them.**
- **Error correction is left to the higher-level protocols.**

Error-reporting messages



Redirection concept



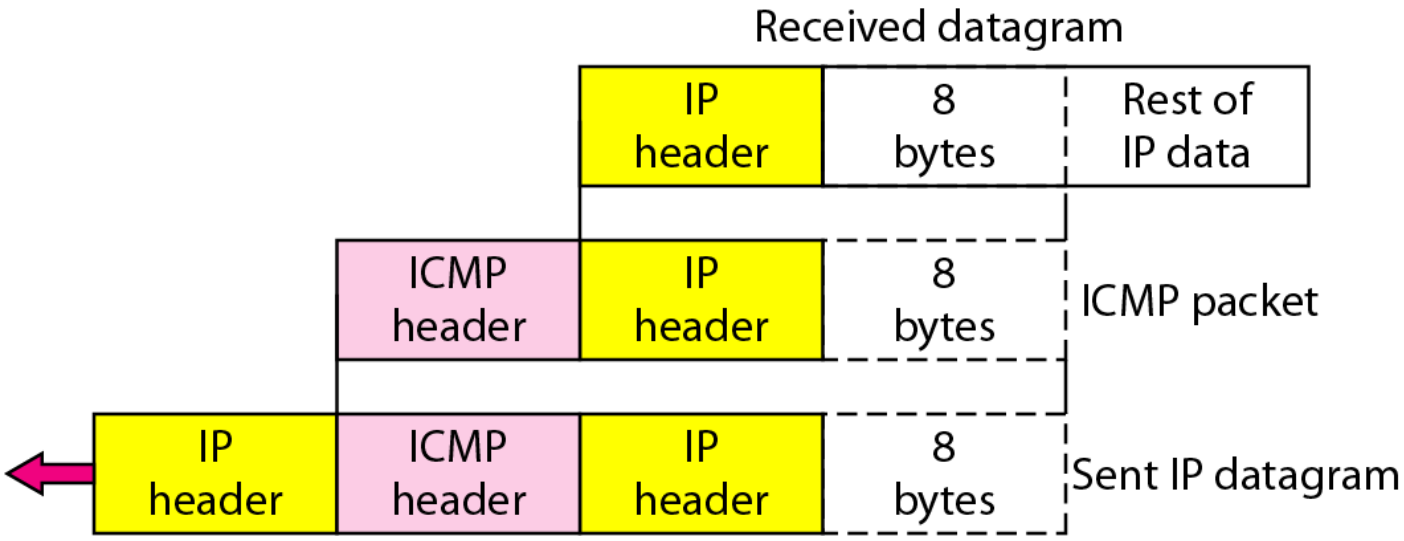
Note

Important points about ICMP error messages:

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

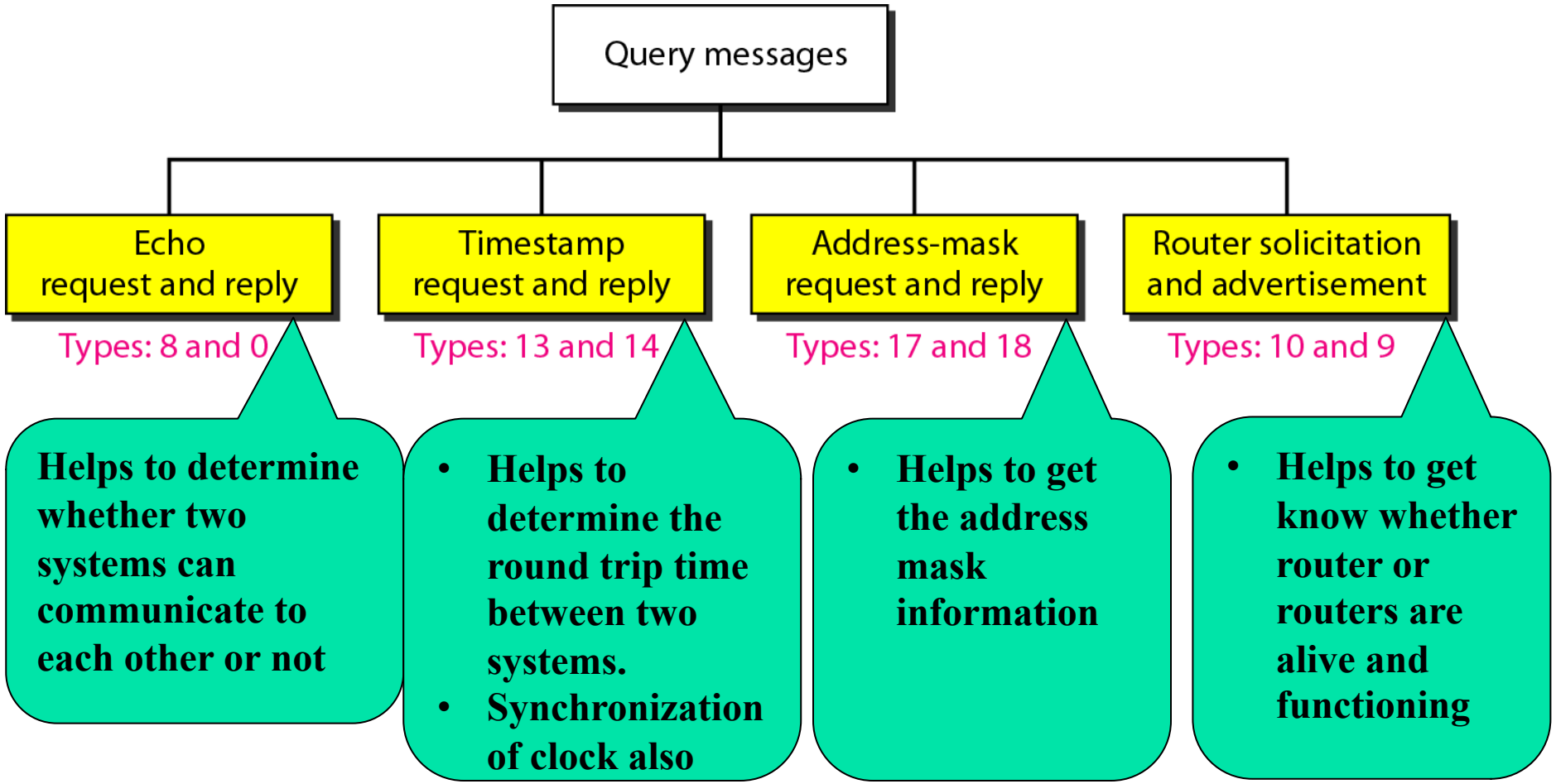
Contents of data field for the error messages

- 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.

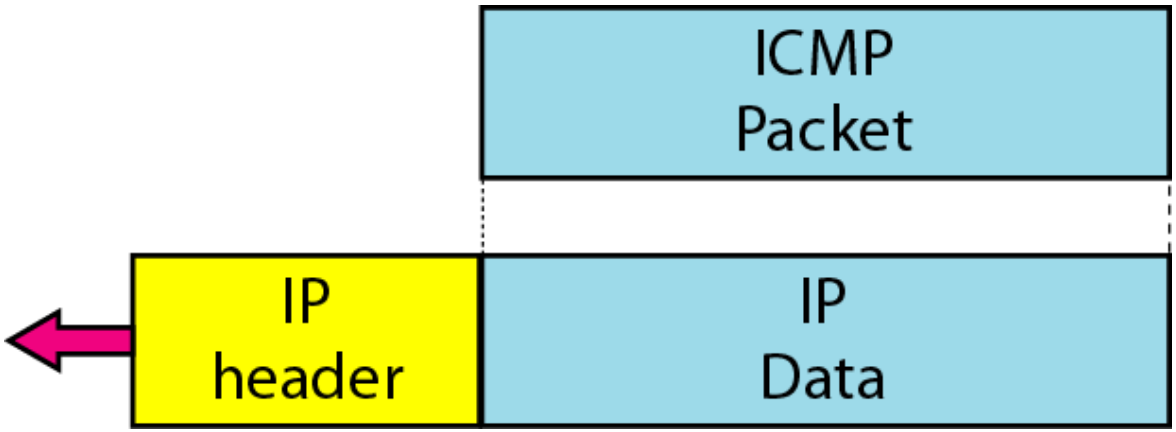


- The first 8 bytes provide information about the port numbers (UDP and TCP) and sequence number (TCP).

Query messages



Encapsulation of ICMP query messages



Example

- **We use the ping program to test the server *www.fhda.edu*. The result is shown on the next slide.**

- **The ping program sends messages with sequence numbers starting from 0. For each probe it gives us the RTT time.**

- **The TTL (time to live) field in the IP datagram that encapsulates an ICMP message has been set to 62.**

- **At the beginning, ping defines the number of data bytes as 56 and the total number of bytes as 84.**

- **It is obvious that if we add 8 bytes of ICMP header and 20 bytes of IP header to 56, the result is 84.**

- **However, note that in each probe ping defines the number of bytes as 64.**

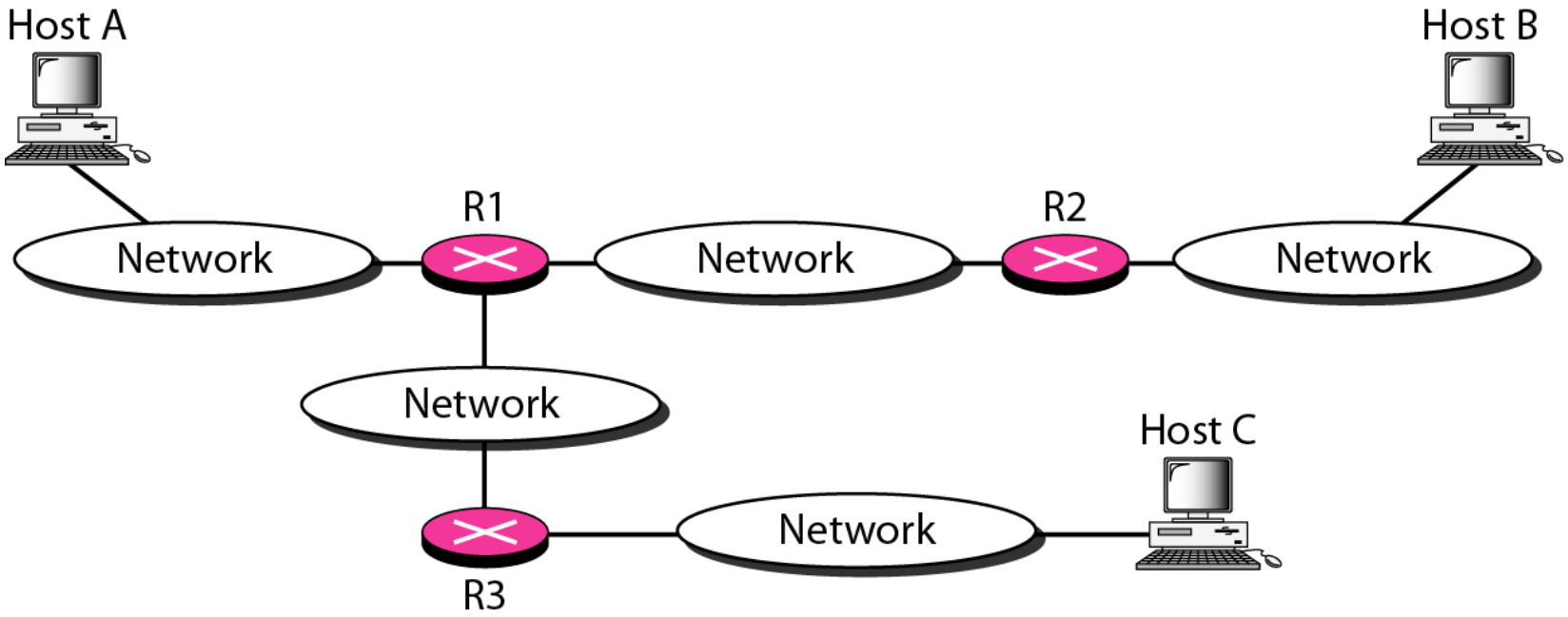
- **This is the total number of bytes in the ICMP packet (56 + 8).**

Example

```
$ ping fhda.edu
PING fhda.edu (153.18.8.1)    56 (84)  bytes of data.
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=0     ttl=62     time=1.91 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=1     ttl=62     time=2.04 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=2     ttl=62     time=1.90 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=3     ttl=62     time=1.97 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=4     ttl=62     time=1.93 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=5     ttl=62     time=2.00 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=6     ttl=62     time=1.94 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=7     ttl=62     time=1.94 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=8     ttl=62     time=1.97 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=9     ttl=62     time=1.89 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=10    ttl=62     time=1.98 ms

--- fhda.edu ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10103ms
      rtt min/avg/max = 1.899/1.955/2.041 ms
```

The *traceroute* program operation



Example

We use the traceroute program to find the route from the computer voyager.deanza.edu to the server fhda.edu. The following shows the result:

```
$ traceroute fhda.edu
traceroute to fhda.edu    (153.18.8.1), 30 hops max, 38 byte packets
 1  Dcore.fhda.edu        (153.18.31.254)    0.995 ms    0.899 ms    0.878 ms
 2  Dbackup.fhda.edu      (153.18.251.4)     1.039 ms    1.064 ms    1.083 ms
 3  tiptoe.fhda.edu       (153.18.8.1)       1.797 ms    1.642 ms    1.757 ms
```

- ***The unnumbered line after the command shows that the destination is 153.18.8.1.***
- ***The packet contains 38 bytes: 20 bytes of IP header, 8 bytes of UDP header, and 10 bytes of application data.***
- ***The application data are used by traceroute to keep track of the packets.***

Example (continued)

- ***The first line shows the first router visited. The router is named Dcore.fhda.edu with IP address 153.18.31.254.***
  - The first round-trip time was 0.995 ms, the second was 0.899 ms, and the third was 0.878 ms.
- ***The second line shows the second router visited.***
  - The router is named Dbackup.fhda.edu with IP address 153.18.251.4.
  - The three round-trip times are also shown.
- ***The third line shows the destination host.***
  - We know that this is the destination host because there are no more lines.
  - The destination host is the server fhda.edu, but it is named tiptoe.fhda.edu with the IP address 153.18.8.1.
  - The three round-trip times are also shown.

Example

- ***In this example, we trace a longer route, the route to xerox.com***
- ***Here there are 17 hops between source and destination.***
- ***Note that some round-trip times look unusual.***
- ***It could be that a router was too busy to process the packet immediately.***

$ traceroute xerox.com

traceroute to xerox.com (13.1.64.93), 30 hops max, 38 byte packets

1	Dcore.fhda.edu	(153.18.31.254)	0.622 ms	0.891 ms	0.875 ms
2	Ddmz.fhda.edu	(153.18.251.40)	2.132 ms	2.266 ms	2.094 ms
3	Cinic.fhda.edu	(153.18.253.126)	2.110 ms	2.145 ms	1.763 ms
4	cenic.net	(137.164.32.140)	3.069 ms	2.875 ms	2.930 ms
5	cenic.net	(137.164.22.31)	4.205 ms	4.870 ms	4.197 ms
	. . . .	. . . .	. . .	. . . .	. . .
14	snfc21.pbi.net	(151.164.191.49)	7.656 ms	7.129 ms	6.866 ms
15	sbcglobal.net	(151.164.243.58)	7.844 ms	7.545 ms	7.353 ms
16	pacbell.net	(209.232.138.114)	9.857 ms	9.535 ms	9.603 ms
17	209.233.48.223	(209.233.48.223)	10.634 ms	10.771 ms	10.592 ms
18	alpha.Xerox.COM	(13.1.64.93)	11.172 ms	11.048 ms	10.922 ms

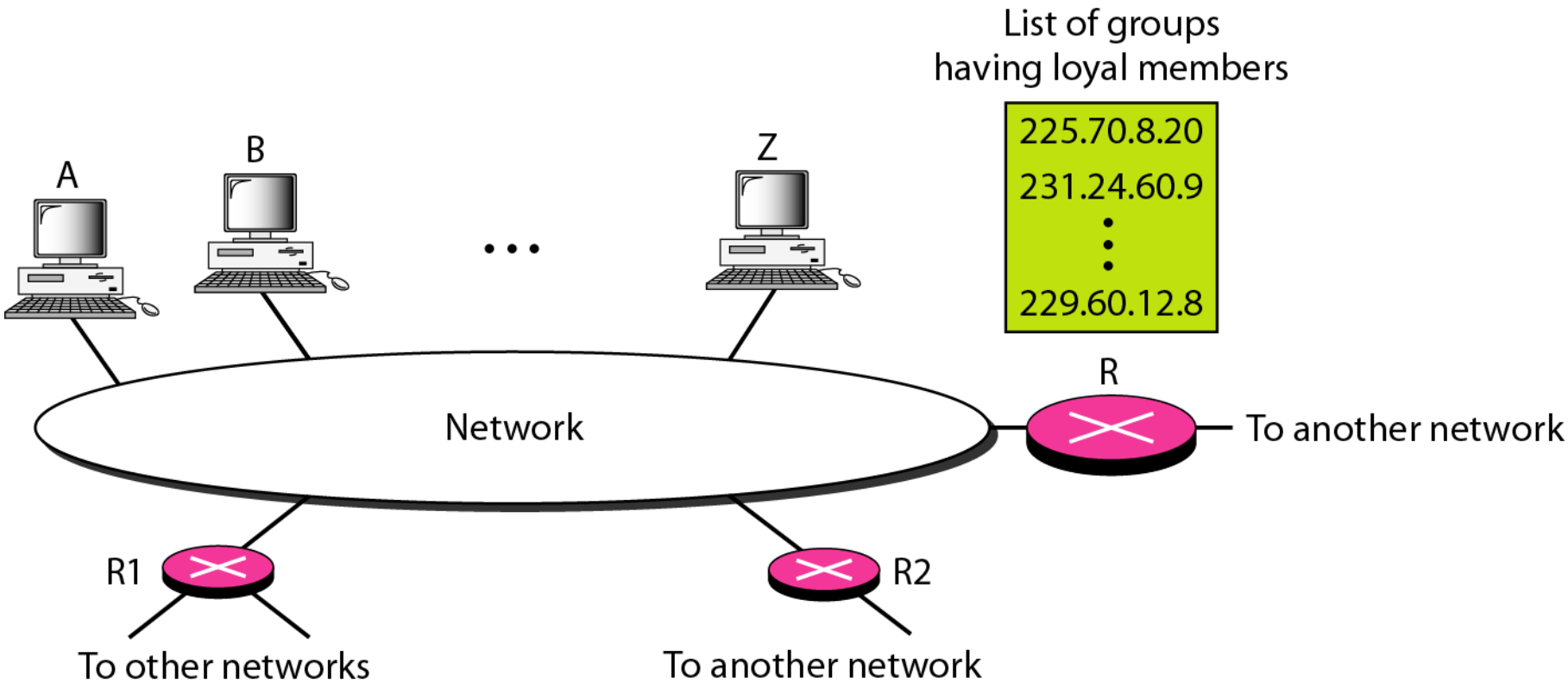
IGMP

- The IP protocol can be involved in two types of communication: ***unicasting and multicasting*.**
- The *Internet Group Management Protocol (IGMP)* is one of the necessary, but not sufficient, protocols that is involved in multicasting.
- IGMP is a companion to the IP protocol.
- Now we will look into:
    - **Group Management**
    - **IGMP Messages and IGMP Operation**
    - **Encapsulation**
    - **Netstat Utility**

IGMP

- IGMP operates locally
- A multicast router connected to a network have a list of multicast addresses of the groups with at least one loyal member in the network.
- For each group, there is one router that distributes the multicast packets destined for the group.

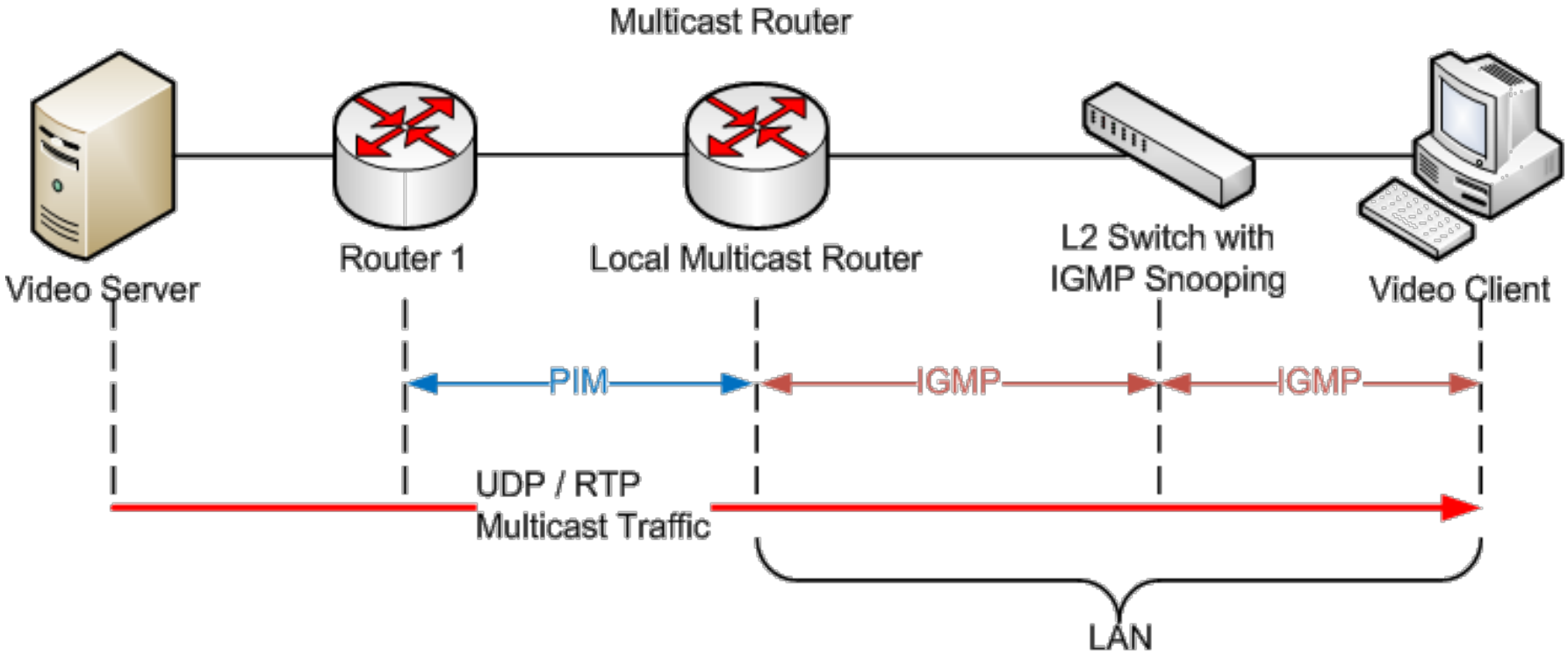
IGMP operation



How multicast works?

- Multicast server application configures with layer 3 addresses as (*Class D*)
- Multiclass application installed on all the hosts
- Indicate router that they want to receive multicast traffic group.(IGMP)
- Multicast routing protocol forward to multicast server
- Calculate layer 2 multicast MAC address (IGMP Snooping/CGMP)

How multicast works?



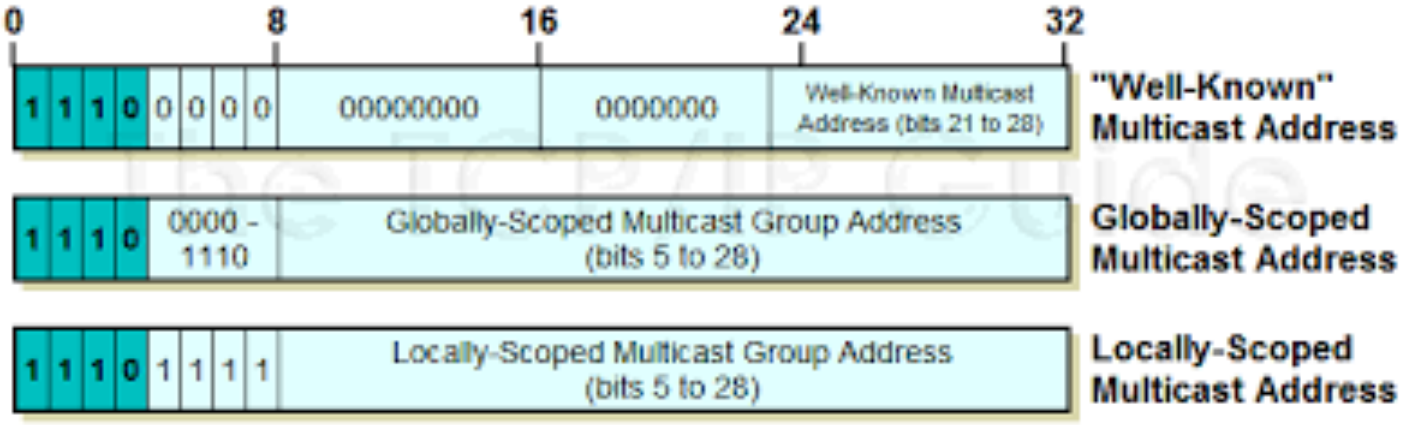
Multicast IP Addresses

- The Internet Assigned Members Authority (IANA) has assigned **Class D** address to multicast

1	1	1	0	28 bits (Multicast Group ID)

- Address range: 224.0.0.0 to 239.255.255.255
- The class D address range is used only for the group address or destination address of IP multicast traffic
- The source address for multicast datagram is always the unicast source address

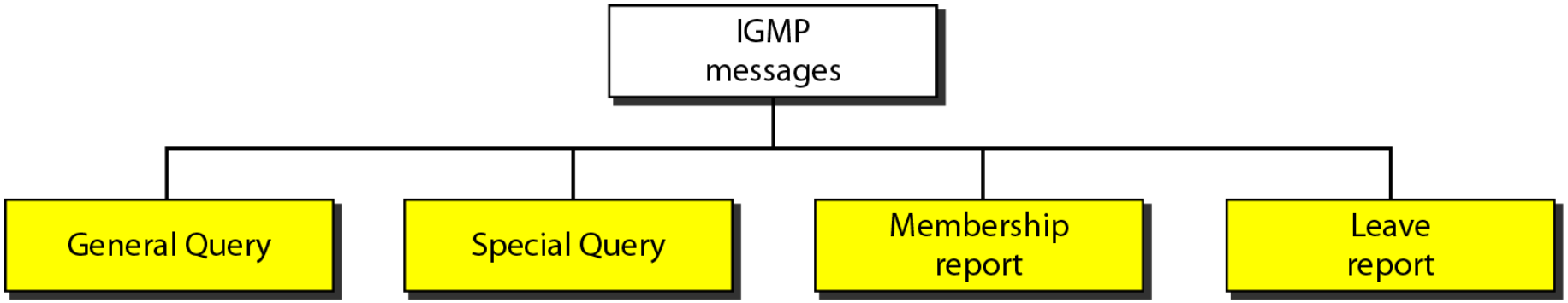
Multicast IP Addresses



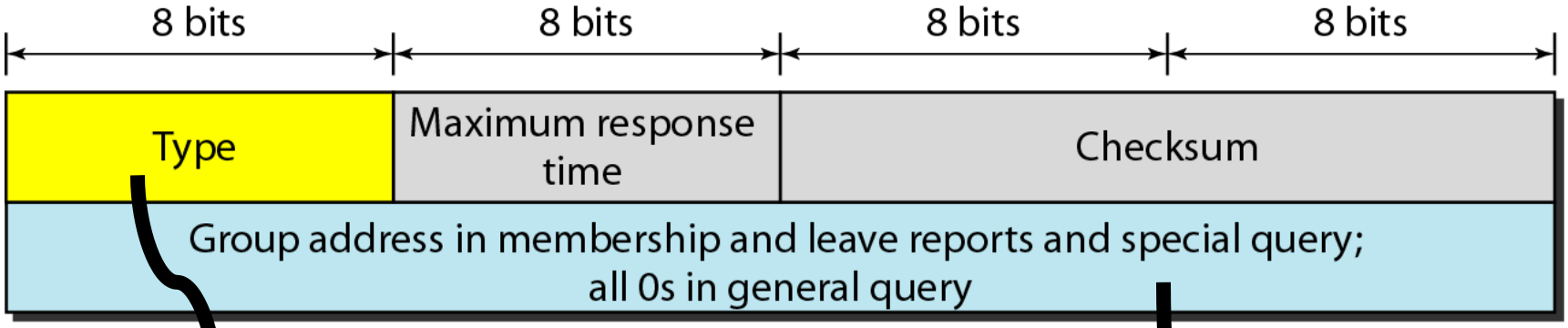
224.0.0.0 to 239.255.255.255

Addresses	Use
224.0.0.0 - 224.0.0.255	Local Multicast (not forwarded by L3 devices)
224.0.1.0 - 224.0.1.255	Routed Multicast (forwarded by L3 devices)
232.0.0.0 - 232.255.255.255	Source Specific Applications
233.0.0.0 - 233.255.255.255	GLOP Addressing
239.0.0.0 - 239.255.255.255	Private addressing

IGMP message types



IGMP message format



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

Type	*IP Destination Address*
Query	224.0.0.1 All systems on this subnet
Membership report	The multicast address of the group
Leave report	224.0.0.2 All routers on this subnet

Note

The general query message does not define a particular group.

IGMP : Version 1

- IGMP version 1 is the first version
- Hosts announce to a router that they want to receive the multicast traffic from a specific group.
- It is a simple protocol that uses only two messages:
  - Membership report
  - Membership query

IGMP : Version 1

- When a hos wants to join a multicast group, it will send a *membership report* to the interested group address
- When the multicast enabled router receives this message
  - It will start forwarding the requested multicast traffic on the interface in which IGMP membership report received

IGMP: Version 1

- The router will periodically send a membership query to destination 224.0.0.1 (all hosts multicast group address)
- Hosts that receive this message will respond with membership report
- Receiving the membership report router renewed the the membership
- When the router receieves no response from the hosts it will remove the entry once the timer expires

IGMP: Version 2

- Enhanced version of Version 1
- New features are:
  - Leave group message
    - Hosts can send leave message to router to show its willingness for a multicast traffic
  - Group specific membership query:
    - Router can able to send a membership query for a specific group address
    - When a router receives a leave group message, it will use this query to check if there are still any hosts interested in receiving the multicast traffic

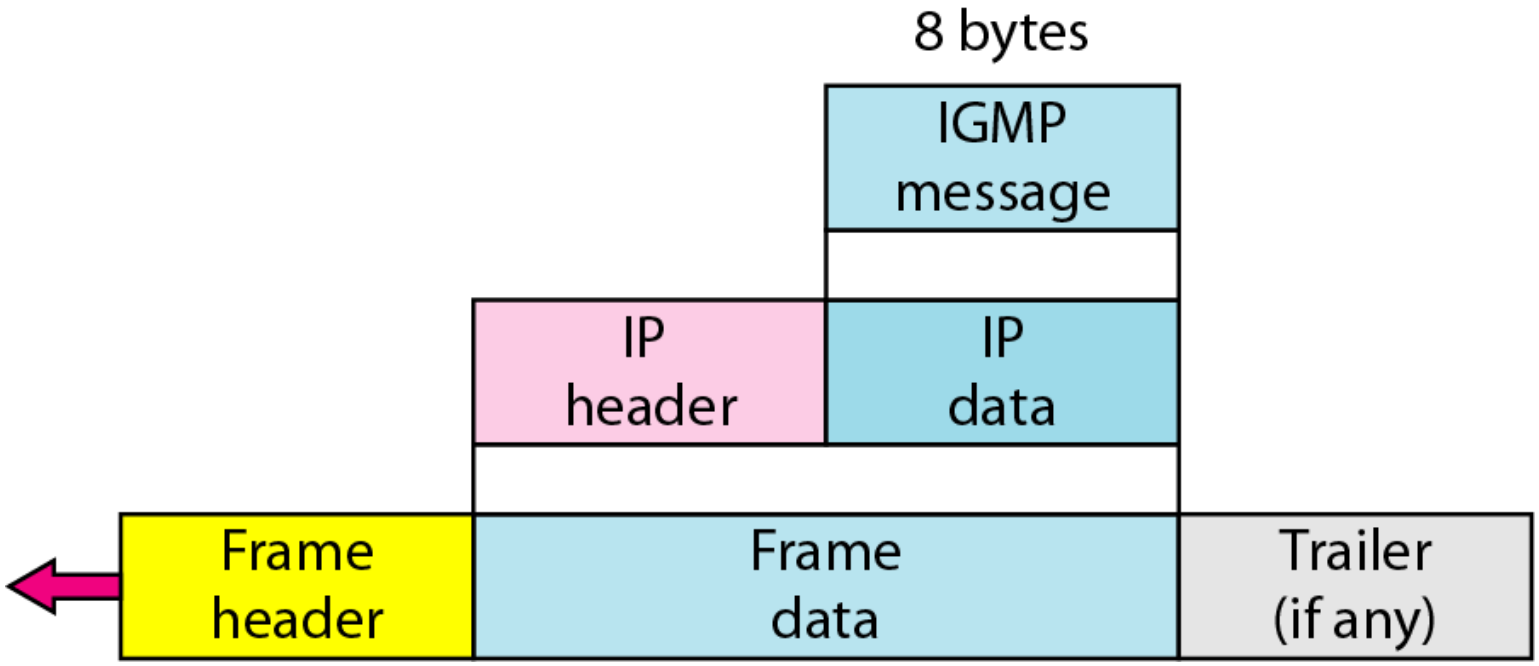
IGMP: Version 2

- MRT (Maximum Response Time):
  - It specifies how much time hosts have to respond to the query
- Querier election process:
  - When there are two routers in the same subnet then only one of them should send query messages
  - The router with lowest IP address becomes the querier

IGMP: Version 3

- Support for source filtering
- With source filtering, we can join multicast groups but only from a specified source addresses
- It uses the Source Specific Multicast (SSM) address: 232.0.0.0 – 232.255.255.255

Encapsulation of IGMP packet



Note

The IP packet that carries an IGMP packet has a value of 1 in its TTL field.

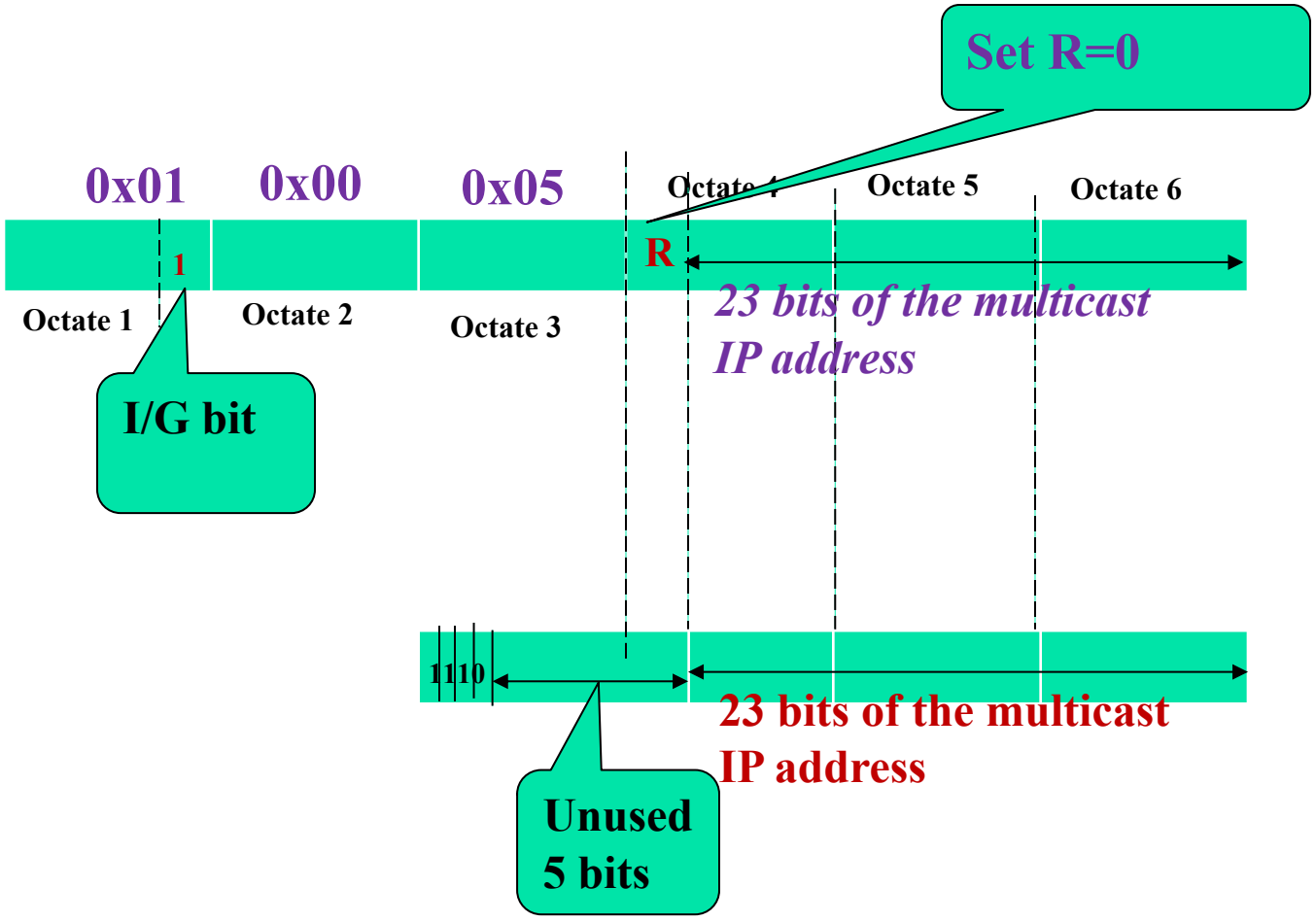
Mapping class D to Ethernet physical address

- At the network layer, the IGMP message is encapsulated in an IP packet and is treated as an IP packet.
- However, because the IP packet has a multicast IP address
  - The ARP protocol cannot find the corresponding MAC (physical) address to forward the packet at the data link layer.
- This requires to convert the an IP multicast address into an Layer 2 address.

Mapping class D to Ethernet physical address

- Most LANs support physical multicast addressing.
  - Ethernet is one of them.
- To convert an IP multicast address into an Ethernet address,
  - The multicast router extracts the least significant 23 bits of a class D IP address
  - Inserts them into a multicast Ethernet physical address

Mapping class D to Ethernet physical address



Note

An Ethernet multicast physical address is in the range

01:00:5E:00:00:00 to 01:00:5E:7F:FF:FF.

Example

Change the multicast IP address 230.43.14.7 to an Ethernet multicast physical address.

Solution

We can do this in two steps:

a. We write the rightmost 23 bits of the IP address in hexadecimal.

b. The result is 2B:0E:07.

c. We add the result of part to the starting Ethernet multicast address, which is 01:00:5E:00:00:00.

d. The result is

01:00:5E:2B:0E:07

Example

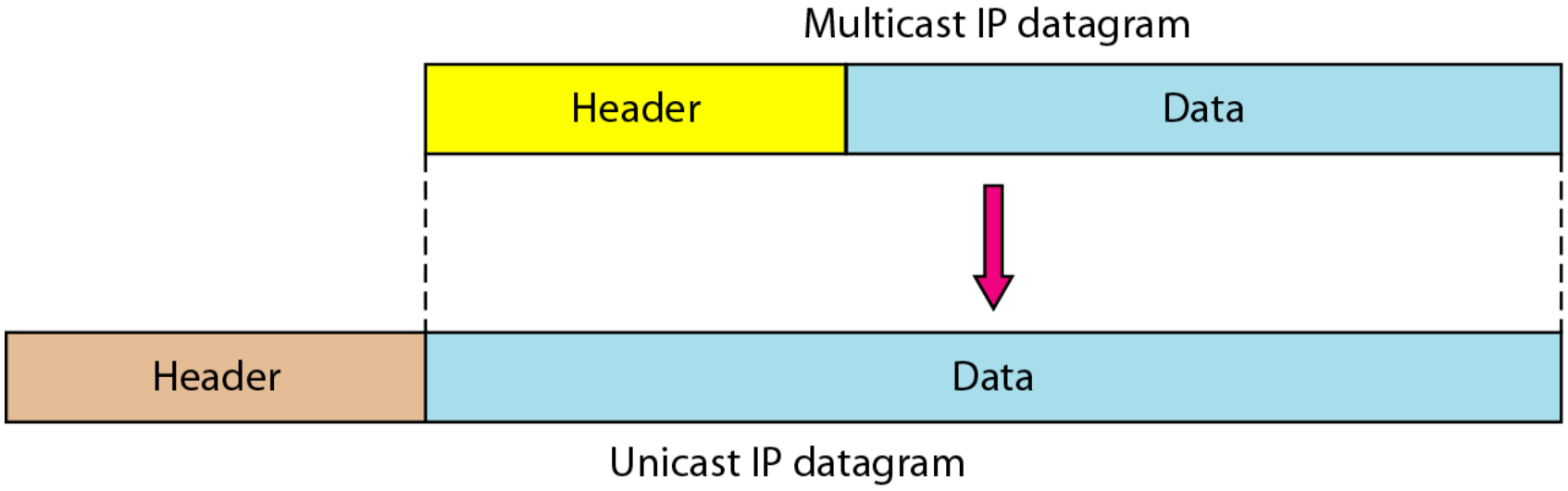
Change the multicast IP address 238.212.24.9 to an Ethernet multicast address.

Solution:

01:00:5E:54:18:09

Tunneling

- Most WANs do not support physical multicast addressing.
- To send a multicast packet through these networks, a process called *tunneling* is used.
- In tunneling, the multicast packet is encapsulated in a unicast packet and sent through the network
- It emerges from the other side as a multicast packet



Example

- *We use netstat with three options: -n, -r, and -a.*
- *The -n option gives the numeric versions of IP addresses, the -r option gives the routing table, and the -a option gives all addresses (unicast and multicast).*
- *Note that we show only the fields relative to our discussion.*
- *"Gateway" defines the router, "Iface" defines the interface.*

Note that the multicast address is shown in color. Any packet with a multicast address from 224.0.0.0 to 239.255.255.255 is masked and delivered to the Ethernet interface.

Example (continued)

$ netstat -nra

Kernel IP routing table

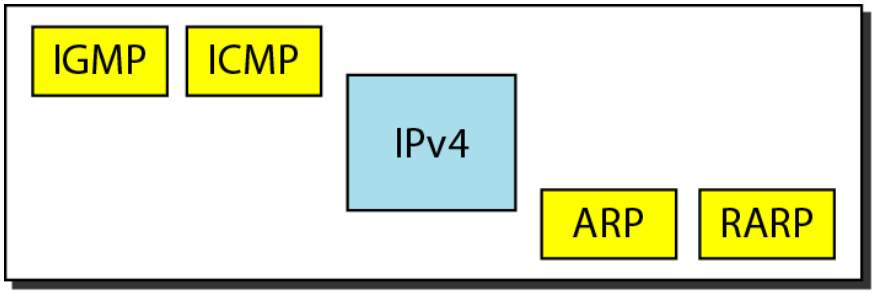
Destination	**Gateway**	**Mask**	**Flags**	**Iface**
153.18.16.0	0.0.0.0	255.255.240.0	U	eth0
169.254.0.0	0.0.0.0	255.255.0.0	U	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	lo
224.0.0.0	0.0.0.0	224.0.0.0	U	eth0
0.0.0.0	153.18.31.254	0.0.0.0	UG	eth0

ICMPv6

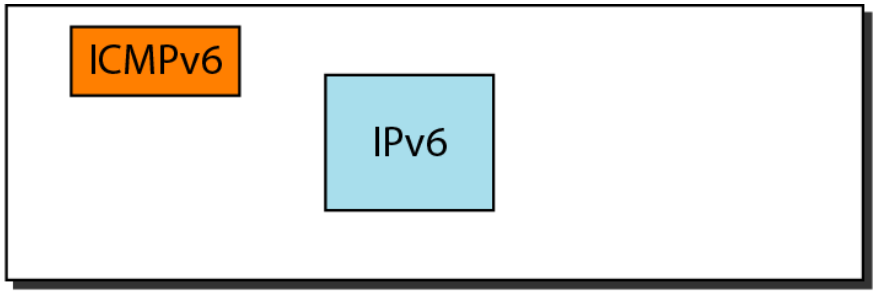
- ***Protocol that has been modified in version 6 of the TCP/IP protocol suite is ICMP (ICMPv6).***
- ***This new version follows the same strategy and purposes of version 4.***

Error Reporting
Query

Comparison of network layers in version 4 and version 6



Network layer in version 4



Network layer in version 6

Comparison of error-reporting messages in ICMPv4 and ICMPv6

Type of Message	*Version 4*	*Version 6*
Destination unreachable	Yes	Yes
Source quench	Yes	No
Packet too big	No	Yes
Time exceeded	Yes	Yes
Parameter problem	Yes	Yes
Redirection	Yes	Yes

Comparison of query messages in ICMPv4 and ICMPv6

Type of Message	*Version 4*	*Version 6*
Echo request and reply	Yes	Yes
Timestamp request and reply	Yes	No
Address-mask request and reply	Yes	No
Router solicitation and advertisement	Yes	Yes
Neighbor solicitation and advertisement	ARP	Yes
Group membership	IGMP	Yes