Data Communications and Networking Fourth Edition

Forouzan

# Chapter 21

# Network Layer: Address Mapping, Error Reporting, and Multicasting



Copyright © The McGraw-Hill Companies, Inc. Permission required for reproduction or display.

- IP was designed as a best-effort delivery protocol, but it lacks some features such as flow control and error control. It is a host-to-host protocol using logical addressing.
- To make IP more responsive to some requirements in today's intemetworking, we need the help of other protocols.
- We need protocols to create a mapping between physical and logical addresses.IP packets use logical (host-to-host) addresses. These packets, however, need to be encapsulatedin a frame, which needs physical addresses (node-to-node).Address Resolution Protocol, is designed for this purpose.

- We sometimes need reverse mapping-mapping a physical address to a logical address. For example, when booting a diskless network or leasing an IP address to a host. Three protocol are designed for this purpose: RARP, BOOTp, and DHCP.
- Lack of flow and error control in the Internet Protocol has resulted in another protocol, ICMP, that provides alerts. It reports congestion and some types of errors in the network or destination host.
- IP was originally designed for unicast delivery, one source to one destination. As the Internet has evolved, the need for multicast delivery, one source to many destinations, has increased tremendously. IGMP gives IP a multicast capability.

# 21-1 ADDRESS MAPPING

***The delivery of a packet to a host or a router requires two levels of addressing: logical and physical. We need to be able to map a logical address to its corresponding physical address and vice versa. This can be done by using either static or dynamic mapping.***

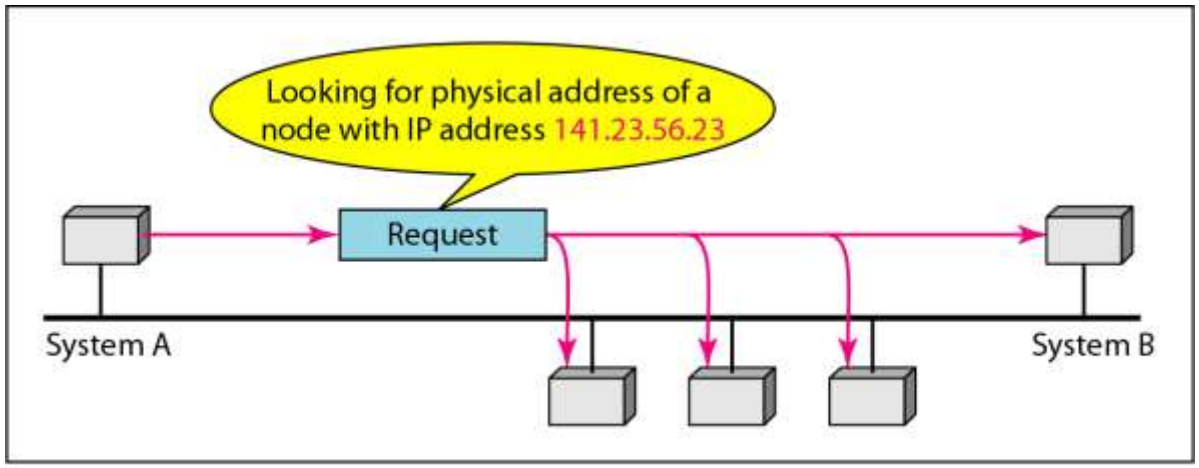
***Topics discussed in this section:***

**Mapping Logical to Physical Address**
**Mapping Physical to Logical Address**

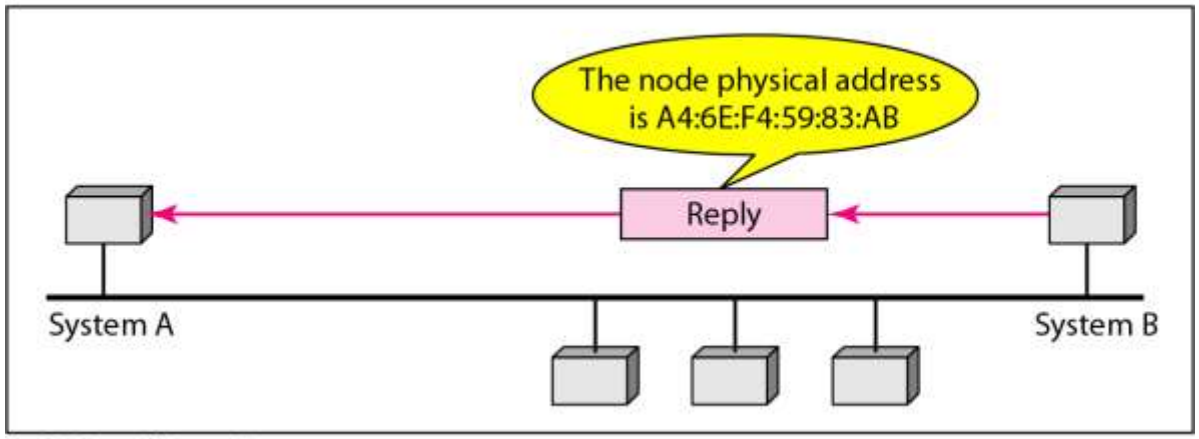
- Anytime a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver.
- But the IP datagram must be encapsulated in a frame to be able to pass through the physical network. This means that the sender needs the physical address of the receiver.
- 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.
- 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.
- The packet is unicast directly to the inquirer by using the physical address received in the query packet.

# Figure 21.1 *ARP operation*

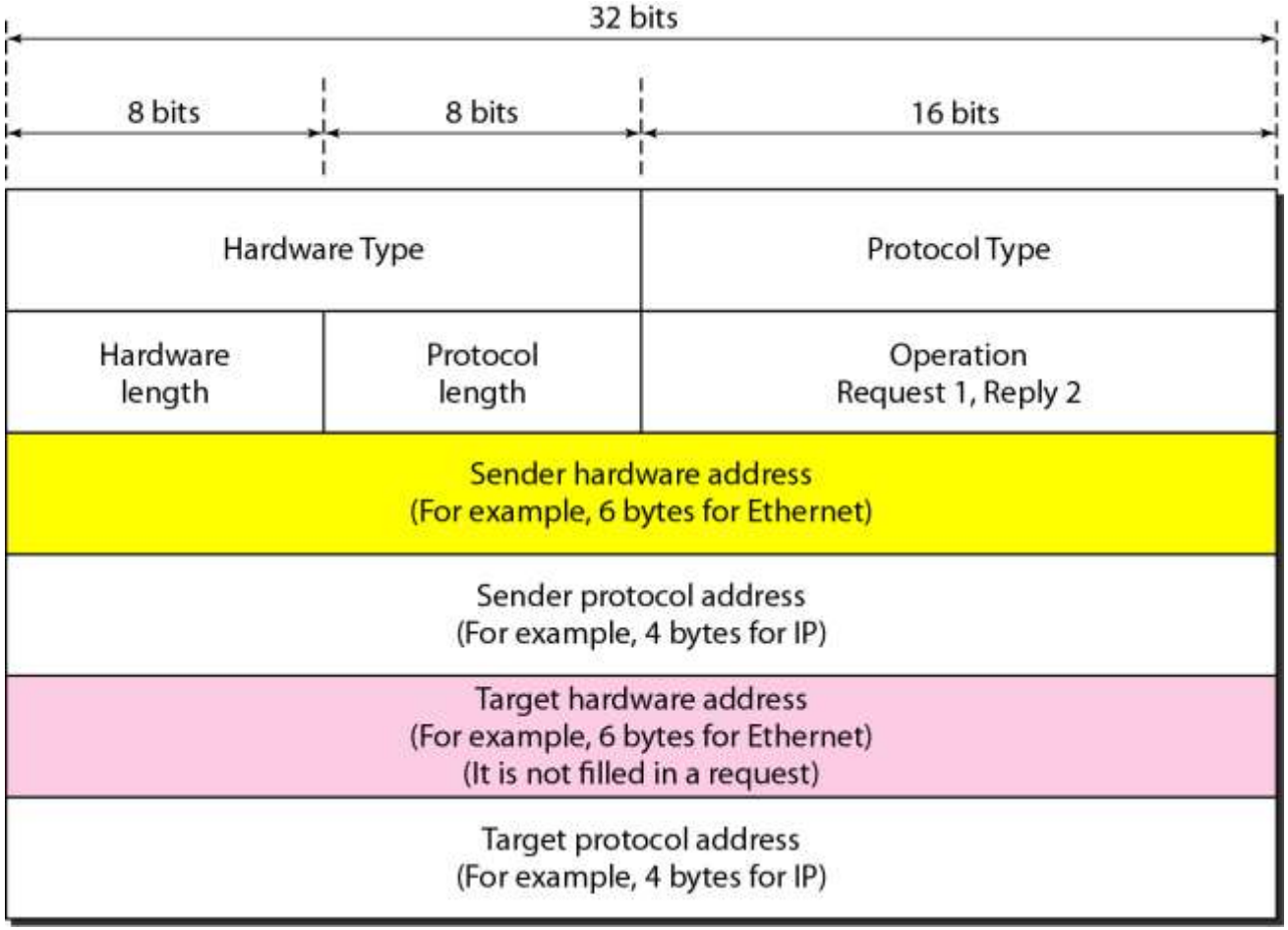



a. ARP request is broadcast




b. ARP reply is unicast

## Figure 21.2 *ARP packet*



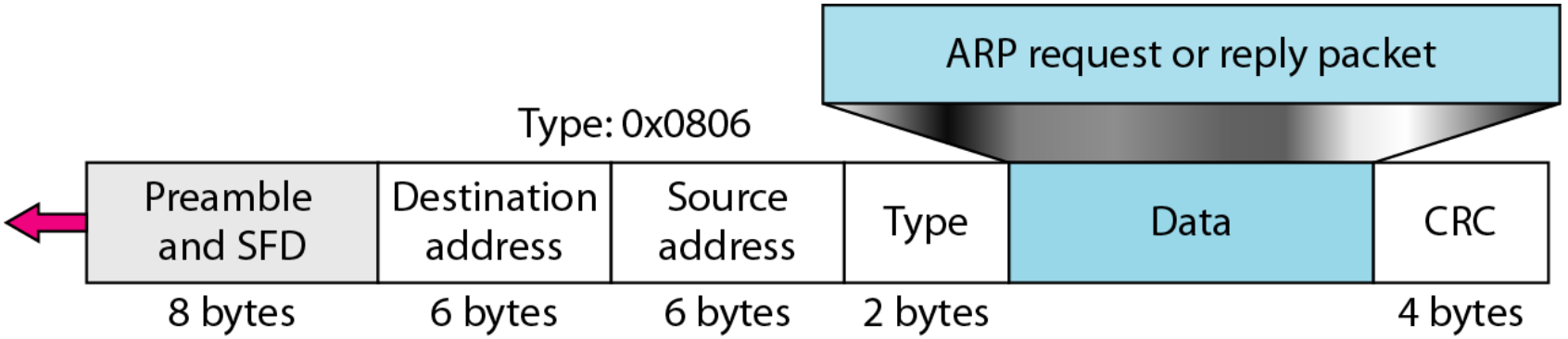
- Hardware type- This is a 16-bit field defining the type of the network on which ARP is running. Each LAN has been assigned an integer based on its type. For example, Ethernet is given type 1. ARP can be used on any physical network.
- Protocol type-This is a 16-bit field defining the protocol. For example, the value of this field for the IPv4 protocol is 080016, ARP can be used with any higher-level protocol.
- Hardware length- This is an 8-bit field defining the length of the physical address in bytes. For example, for Ethernet the value is 6.
- Protocol length-This is an 8-bit field defining the length of the logical address in bytes. For example, for the IPv4 protocol the value is 4.

- Operation-This is a 16-bit field defining the type of packet. Two packet types are defined: ARP request and ARP reply
- Sender hardware address- This is a variable-length field defining the physical
- address of the sender-For example, for Ethernet this field is 6 bytes long.
- Sender protocol address-This is a variable-length field defining the logical (for example, IP) address of the sender. For the IP protocol, this field is 4 bytes long.
- Target hardware address-This is a variable-length field defining the physical address of the target. For example, for Ethernet this field is 6 bytes long. For an ARP request message, this field is alIOs because the sender does not know the physical address of the target.
- Target protocol address-This is a variable-length field defining the logical (for example, IP) address of the target. For the IPv4 protocol, this field is 4 bytes long.

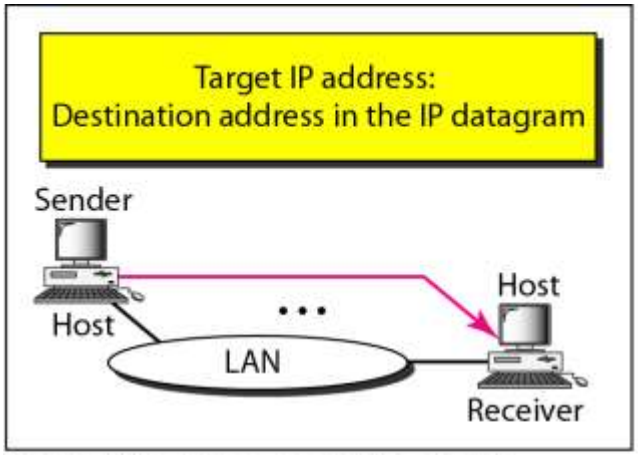
## *Encapsulation*

- An ARP packet is encapsulated directly into a data link frame. For example, in Fig an ARP packet is encapsulated in an Ethernet frame.
- Note that the type field indicates that the data carried by the frame are an ARP packet.

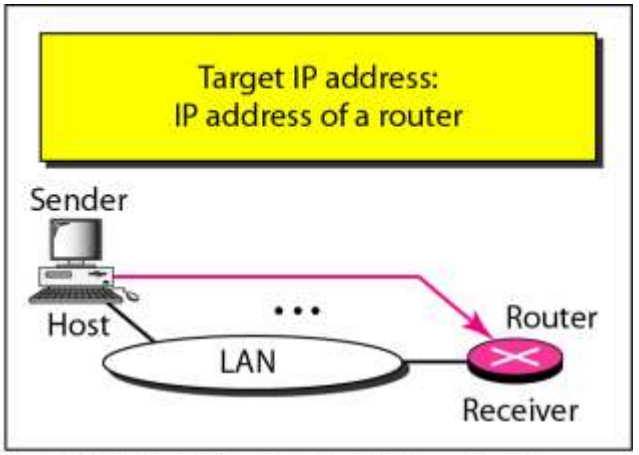
## Figure 21.3 *Encapsulation of ARP packet*



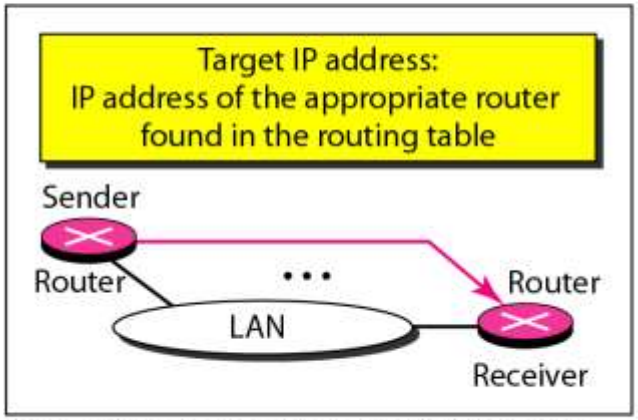
# Figure 21.4 *Four cases using ARP*



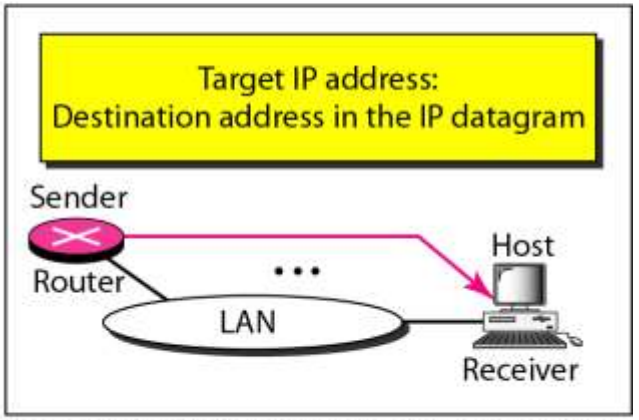

Case 1. A host has a packet to send to another host on the same network.




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.**

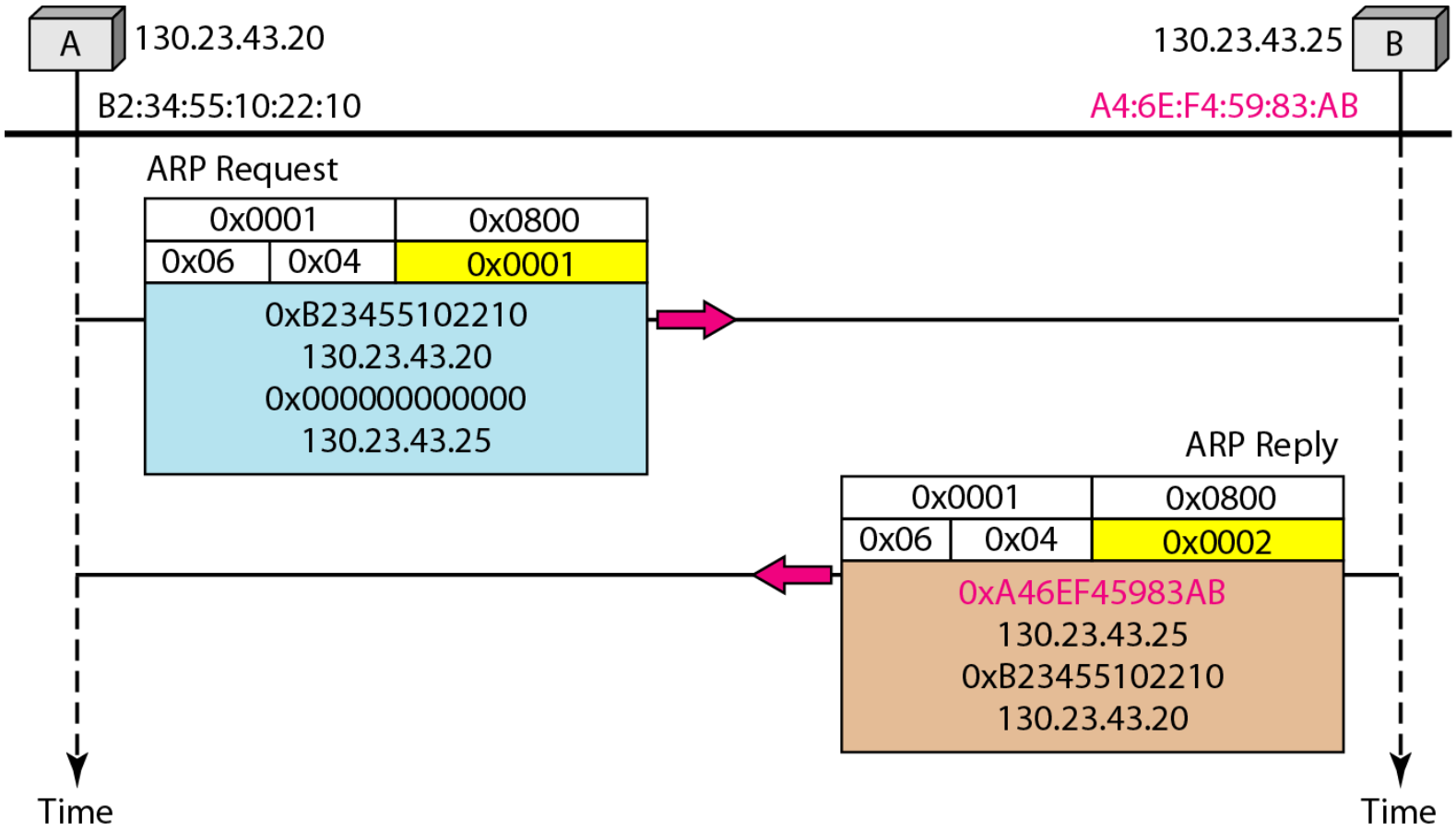
# Example 21.1

*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

*Figure 21.5 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.*

## Figure 21.5 *Example 21.1, an ARP request and reply*



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:

1. A diskless 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.

## **Reverse Address Resolution Protocol** (RARP)

- Finds the logical address for a machine that knows only its physical address.
- To create an IP datagram, a host or a router needs to know its own IP address or addresses. The IP address of a machine is usually read from its configuration file stored on a disk file.
- The machine can get its physical address (by reading its NIC, for example), which is unique locally. It can then use the physical address to get the logical address by using the RARP protocol.
- 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.
- There is a serious problem with RARP: Broadcasting is done at the data link layer. The physical broadcast address, allis 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

# 16.1 BOOTP

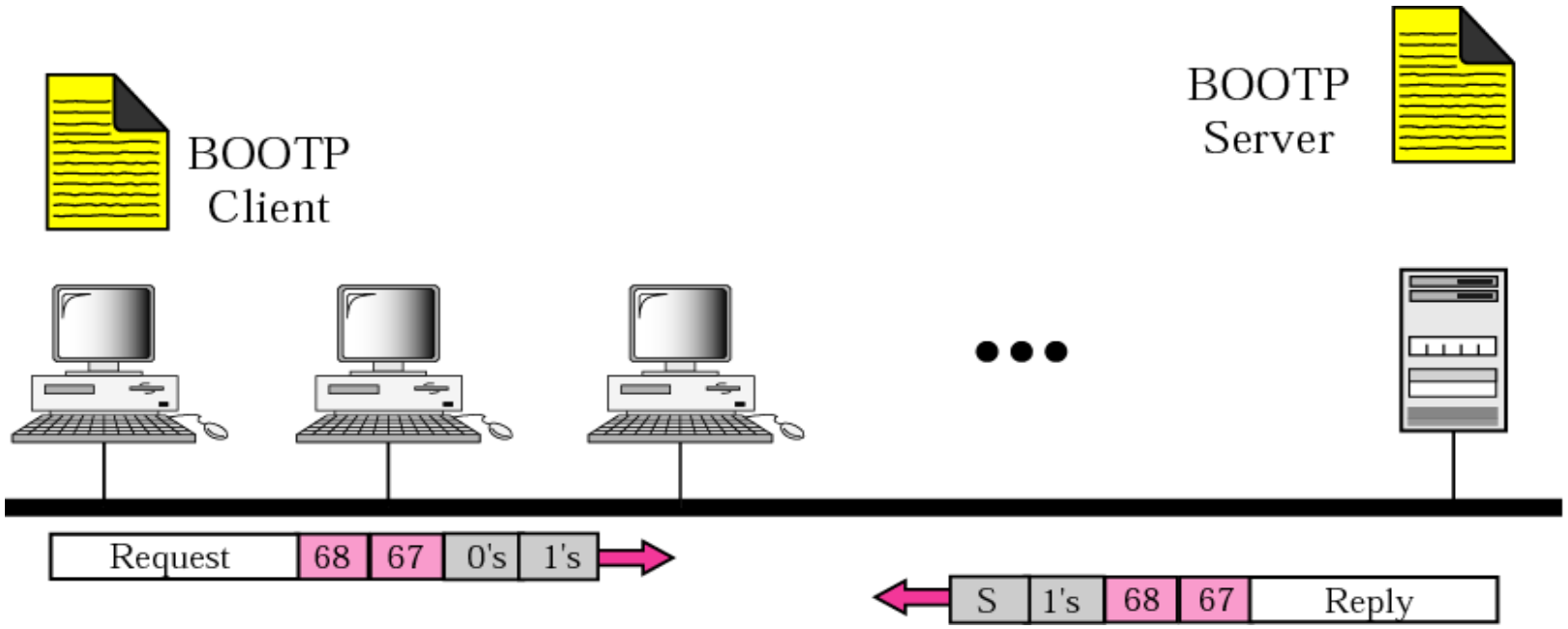
*The Bootstrap Protocol (BOOTP) is a client/server protocol that configures a diskless computer or a computer that is booted for the first time. BOOTP provides the*

- *IP address*
- *net mask*
- *the address of a default router*
- *the address of a name server.*

*BOOTP is static. When a client workstation asks for the above info, it is retrieved from a fixed table. Every time the client asks for the info, it gets the same results.*

# *Client and server on the same network*

**The BOOTP server can be on the same network as the BOOTP client or on different networks.**

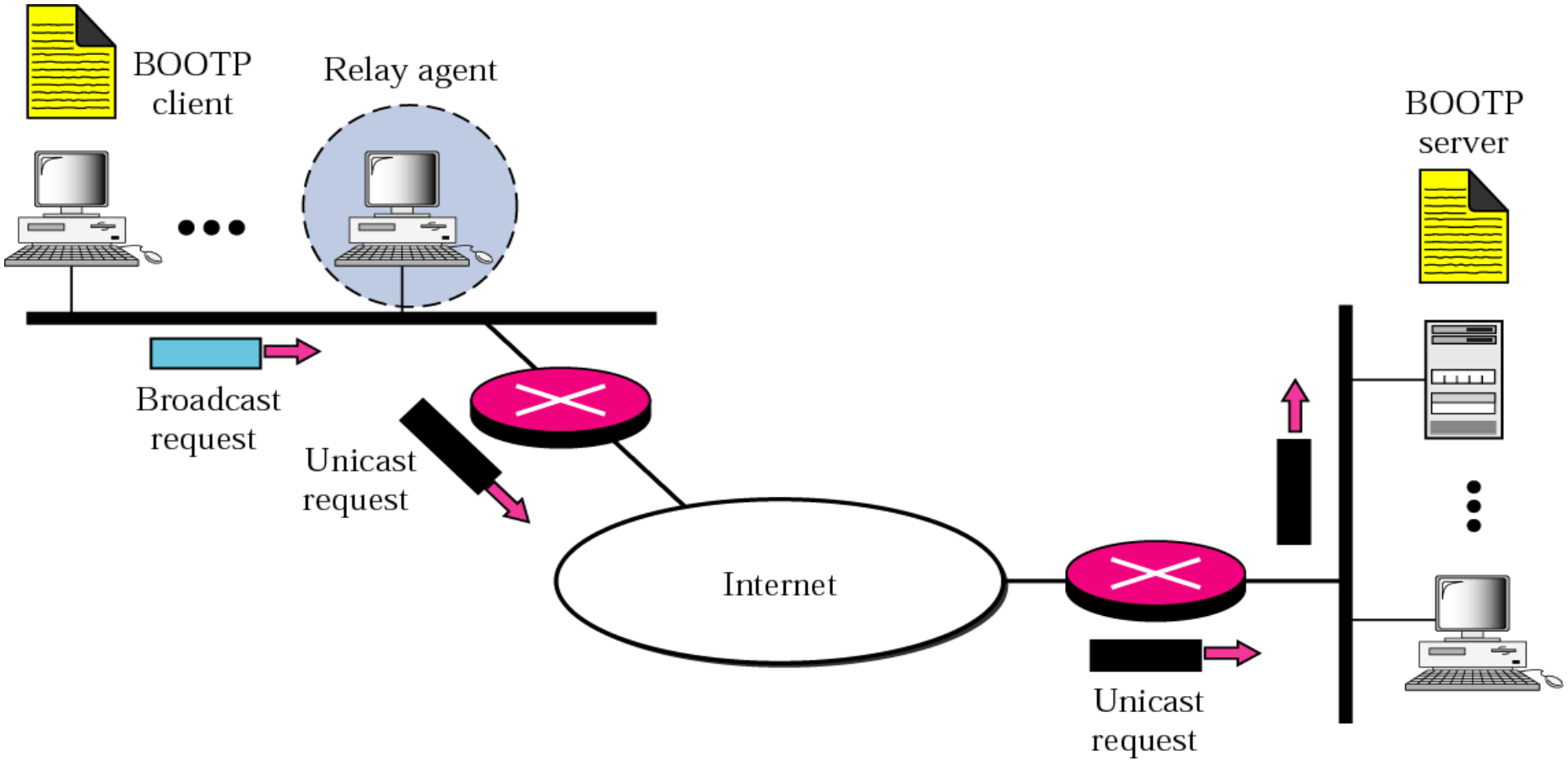



**BOOTP places its packet inside a UDP packet (note that BOOTP is an application layer program).**

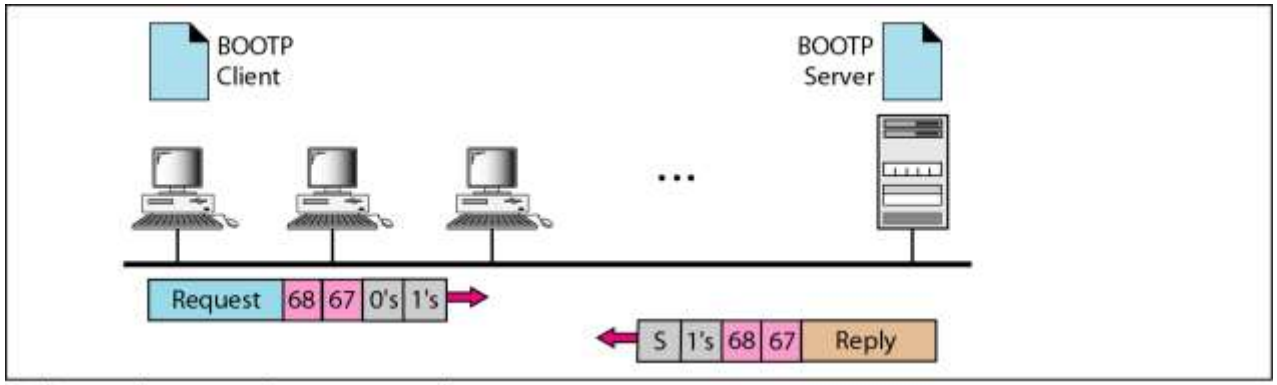
- The BOOTP server issues a passive open command on UDP port number 67 and waits for a client.
- A booted client issues an active open command on port number 68. The message is encapsulated in a UDP user datagram and then in an IP packet. In the IP packet the source address is all 0s and the destination address is all 1s.
- Server responds with a UDP datagram source port 67 and destination port 68. Can also bypass ARP since server also knows the MAC address of the client.

# *Client and server on two different networks*

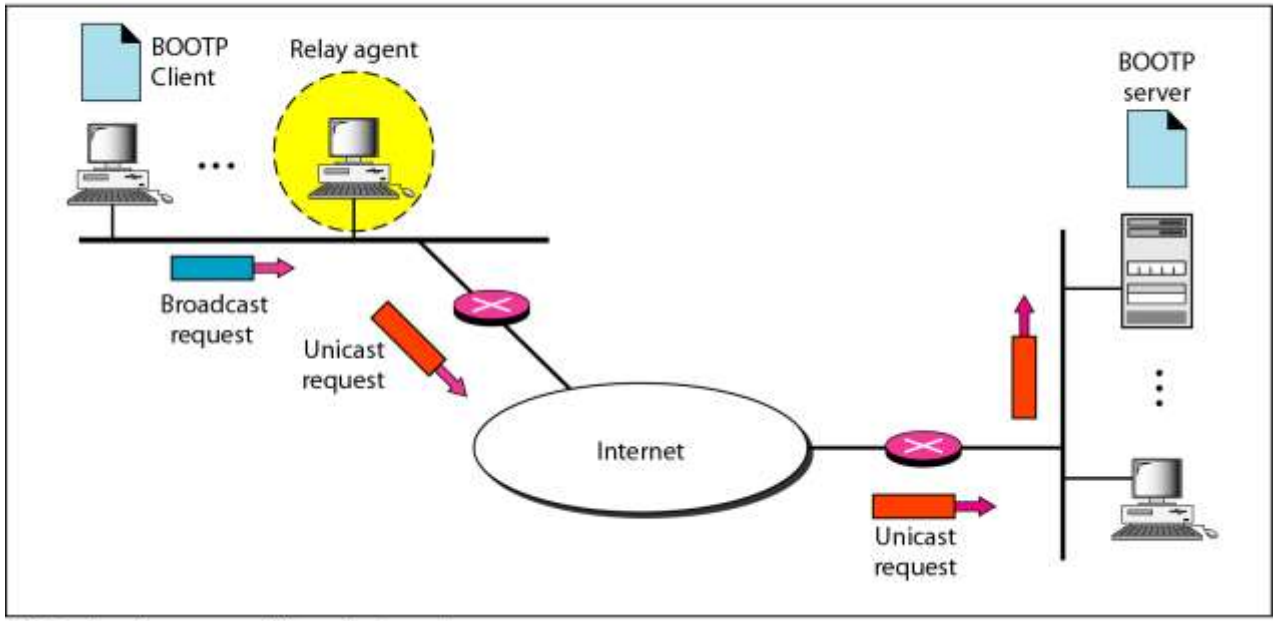
**When client and server are on different networks, we need a relay agent, because client does not know IP address of server, and a limited broadcast address gets dumped by the local router. Relay agent knows the IP addr of the server.**



## Figure 21.7 *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

# 16.2 DHCP

*The Dynamic Host Configuration Protocol (DHCP) provides static and dynamic address allocation that can be manual or automatic.*

*The topics discussed in this section include:*

*Static Address Allocation*
*Dynamic Address Allocation*
*Manual and Automatic Configuration*
*Packet Format*
*Transition States*
*Exchanging Messages*

# *DHCP basics*

Bootp is static, but DHCP is dynamic (but it can also be static).

DHCP has a pool of available addresses. When a request arrives, DHCP pulls out the next available address and assigns it to the client for a negotiable time period.

When a request comes in from a client, the DHCP server first consults the static table.

DHCP is great when devices and IP addresses change.

The DHCP packet format is almost identical to the BOOTP packet format (in order to be compatible with BOOTP).

Only difference is 1-bit flag.

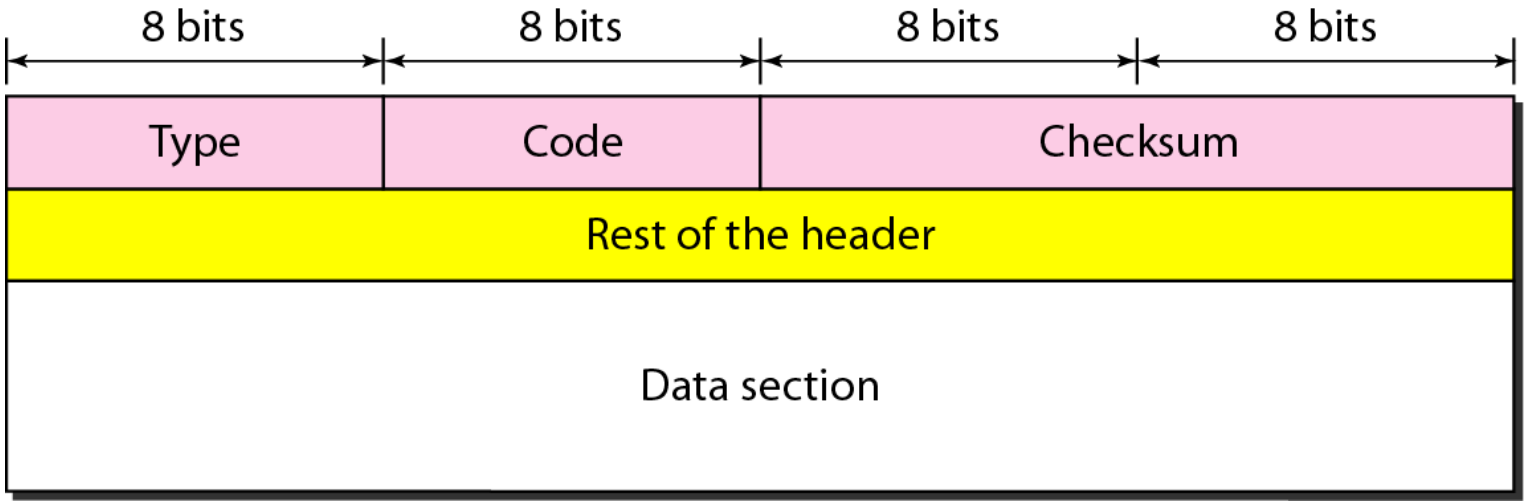
*Note*

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

# 21-2 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.***

## Figure 21.8 *General format of ICMP messages*

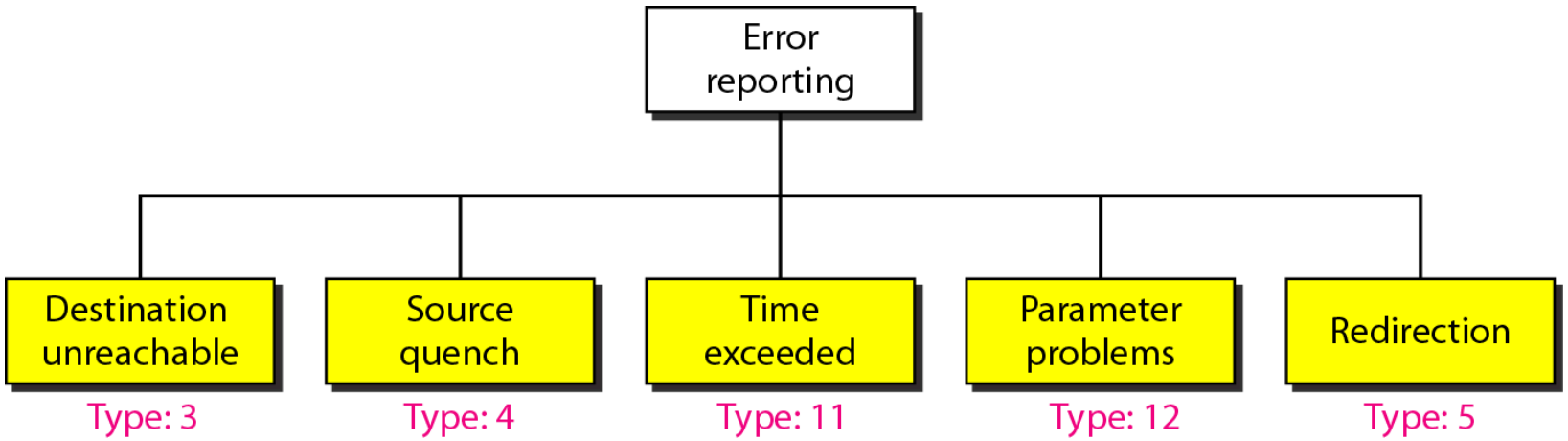


- An ICMP message has an 8-byte header and variable size data section.
- Two types of messages:
  - Error reporting messages
  - Query messages
- The code field specifies the reason for the particular message type.
- The last common field is the checksum field.
- The rest of the header is specific for 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.**

## Figure 21.9 *Error-reporting messages*



- The source-quench message in ICMP was designed to add a kind of flow control to the IP. When a router or host discards a datagram due to congestion, it sends a source-quench message to the sender of the datagram. This message has two purposes. First, it informs the source that the datagram has been discarded. Second, it warns the source that there is congestion somewhere in the path and that the source should slow down (quench) the sending process.
- when the datagram is discarded, a time-exceeded message must be sent by the router to the original source. Second, a time-exceeded message is also generated when not all fragments that make up a message arrive at the destination host within a certain time limit.

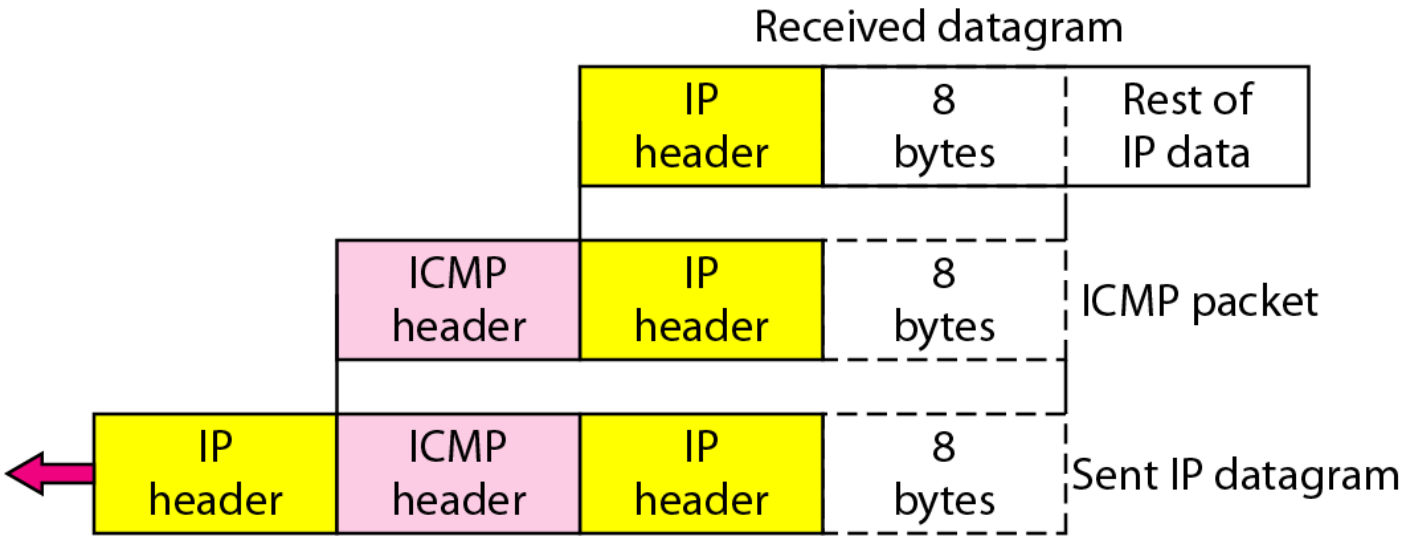
- Any ambiguity in the header part of a datagram can Create serious problems as the datagram travels through the Internet. If a router or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards the datagram and sends a parameter-problem message back to the source.
- 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.

Note

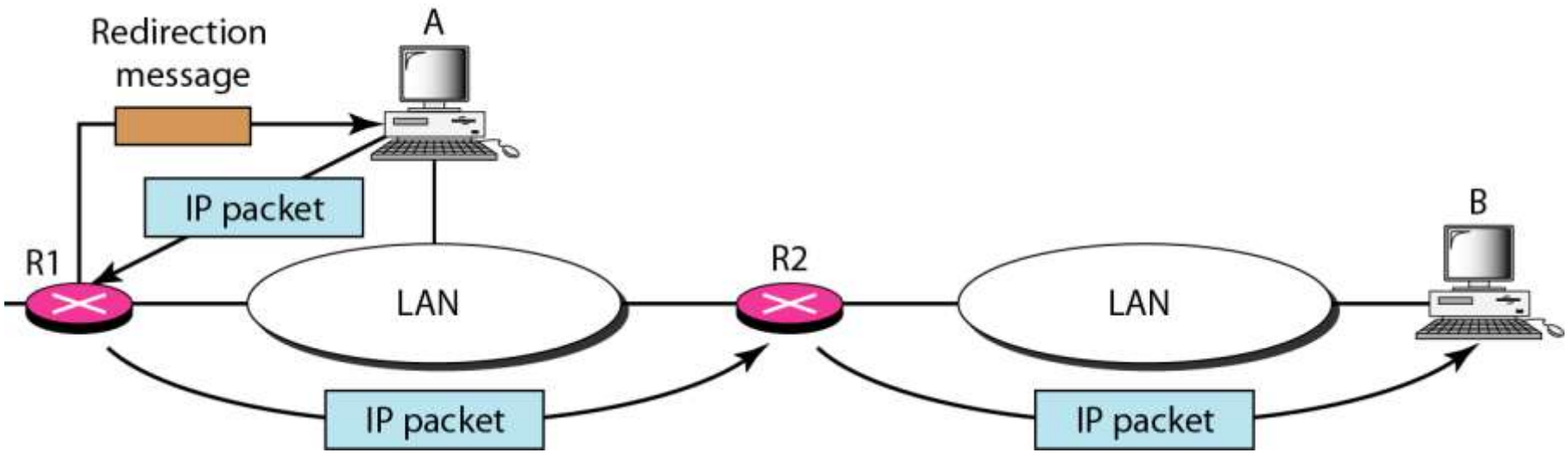
**Important points about ICMP error messages:**

- 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.

## Figure 21.10 *Contents of data field for the error messages*

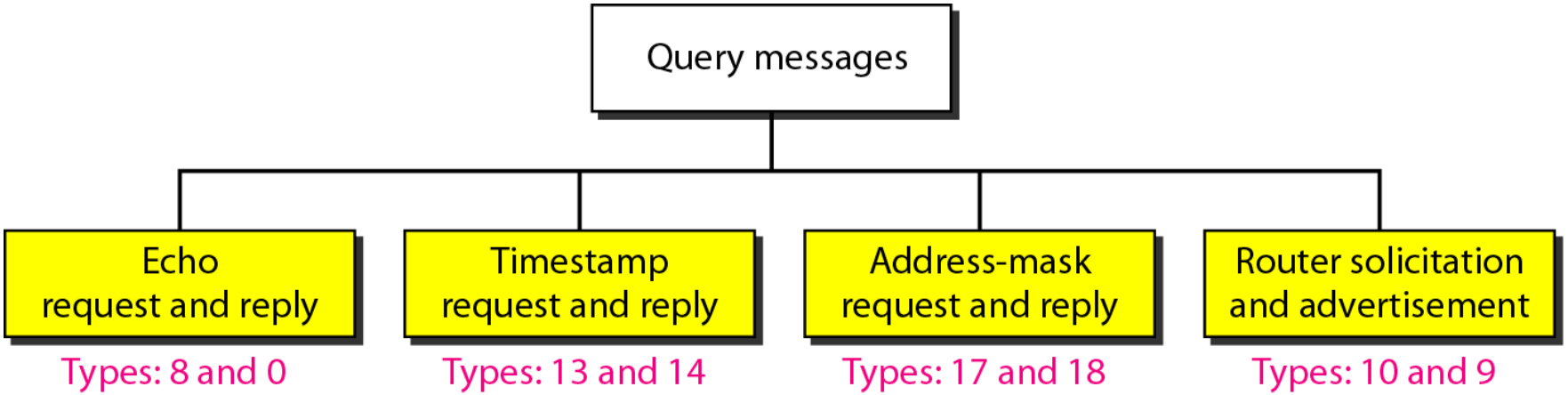


## Figure 21.11 *Redirection concept*



- In addition to error reporting, ICMP can diagnose some network problems. This is accomplished through the query messages, a group of four different pairs of messages
- A query message is encapsulated in an IP packet, which in turn is encapsulated in a data link layer frame.
- However, in this case, no bytes of the original IP are included in the message.

## Figure 21.12 *Query messages*



# *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.
- ICMP messages are encapsulated in IP datagrams, the receipt of an echo-reply message by the machine that sent the echo request is proof that the IP protocols in the sender and receiver are communicating with each other using the IP datagram.
- Also, it is proof that the intermediate routers are receiving, processing, and forwarding IP datagrams.
- Today, most systems provide a version of the *ping command* that can create a series (instead of just one) of echo-request and echo-reply messages, providing statistical information

*Timestamp Request and Reply*

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

*Address-Mask Request and Reply*

- 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. This can be applied to its full IP address to get its subnet address.

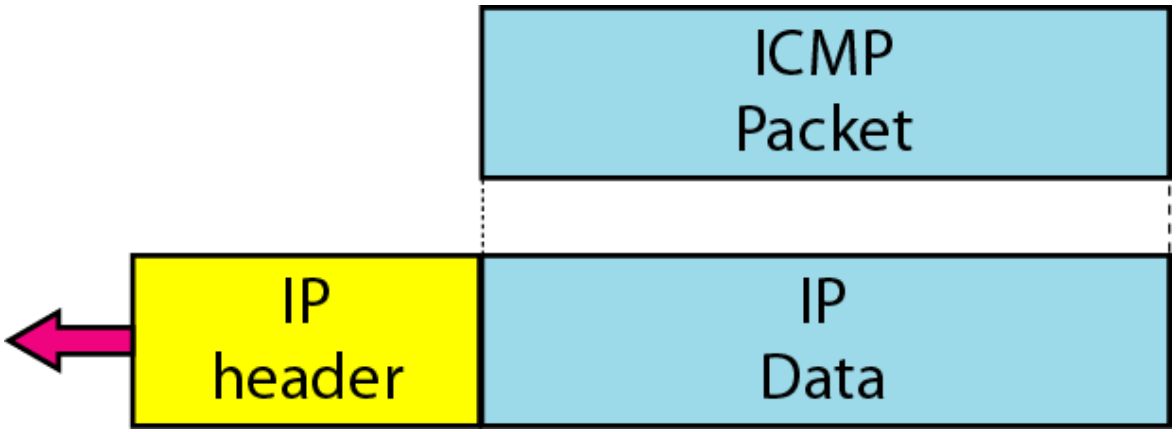
*Router Solicitation and Advertisement*

- The router-solicitation and router-advertisement messages are used to find the routers information.
- 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.
- A router can also periodically send router-advertisement messages even if no host has solicited.

*Checksum*

- In ICMP the checksum is calculated over the entire message (header and data).

## Figure 21.13 *Encapsulation of ICMP query messages*



# 21-3 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.***

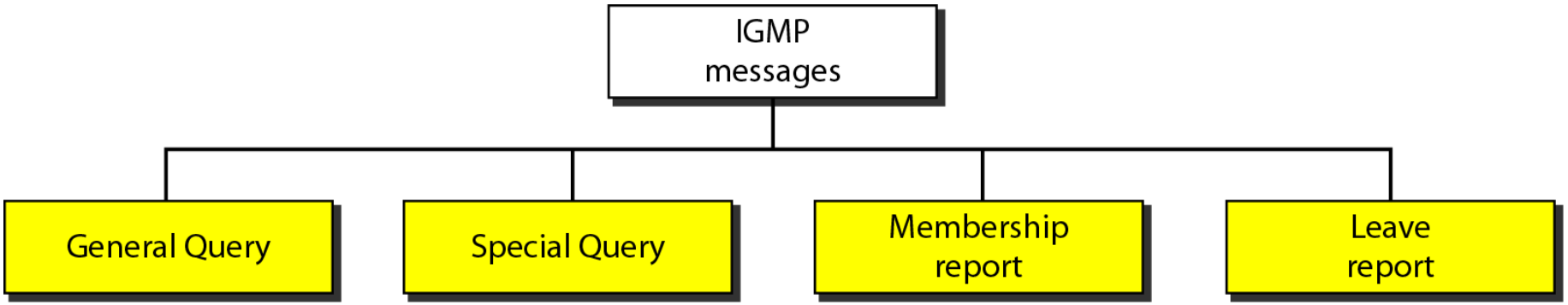
***Topics discussed in this section:***

**Group Management**
**IGMP Messages and IGMP Operation**
**Encapsulation**
**Netstat Utility**

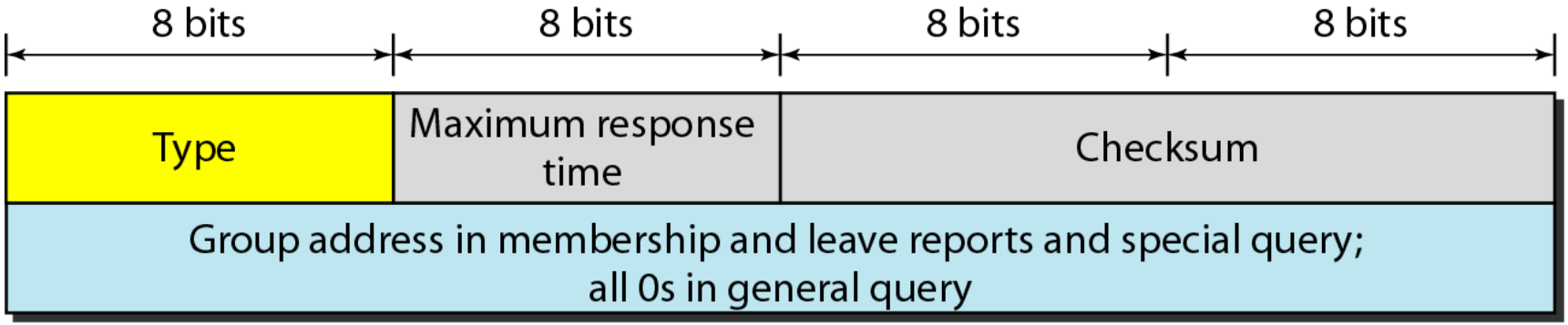
# Group Management

- IGMP is not a multicasting routing protocol; it is a protocol that manages group membership.
- In any network, there are one or more multicast routers that distribute multicast packets to hosts or other routers.
- The IGMP protocol gives the multicast routers information about the membership status of hosts (routers) connected to the network.
- A multicast router may receive thousands of multicast packets every day for different groups. If a router has no knowledge about the membership status of the hosts, it must broadcast all these packets. This creates a lot of traffic and consumes bandwidth.
- A better solution is to keep a list of groups in the network for which there is at least one loyal member. IGMP helps the multicast router create and update this list.

## Figure 21.16 *IGMP message types*



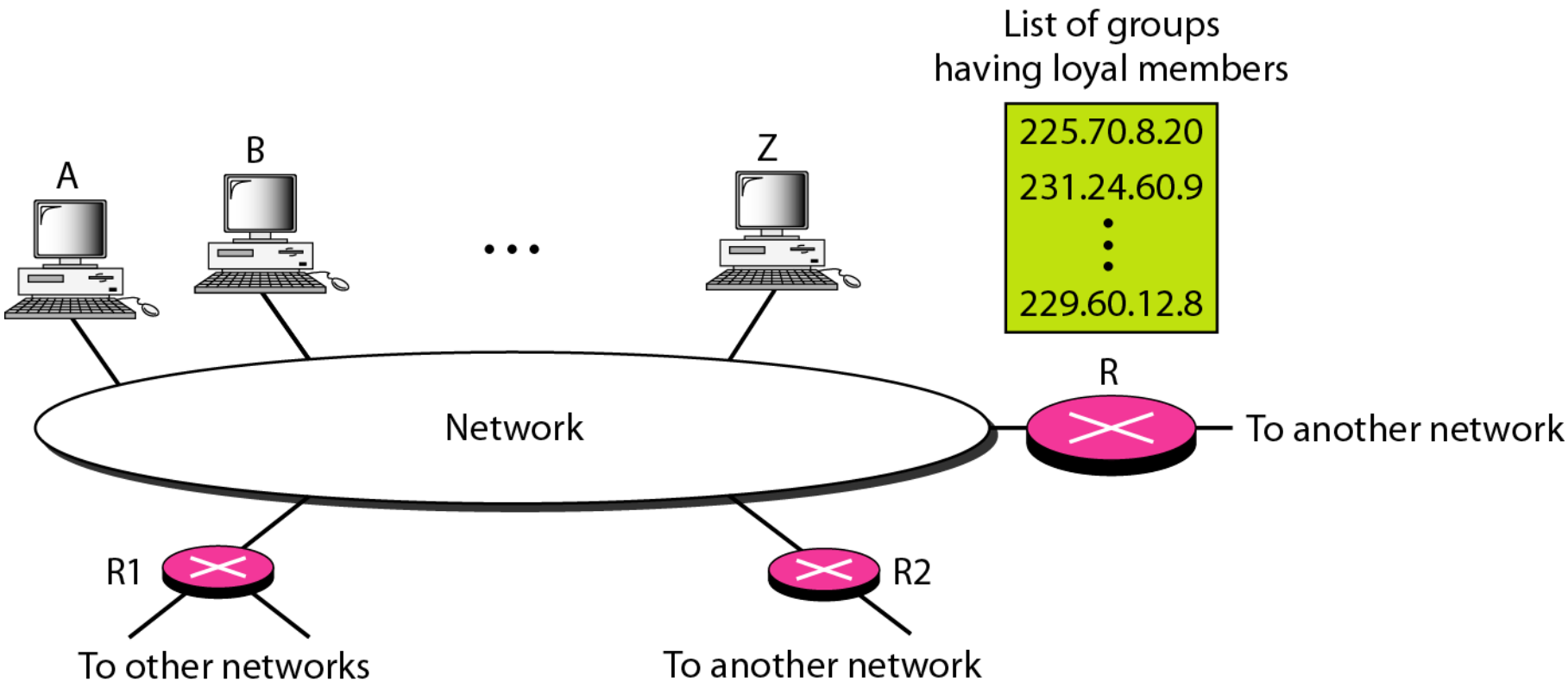
## Figure 21.17 *IGMP message format*



## Table 21.1 *IGMP type field*

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

## Figure 21.18 *IGMP operation*



*Note*

**In IGMP, a membership report is sent twice, one after the other.**

*Note*

**The general query message does not define a particular group.**

# Example 21.6

*Imagine there are three hosts in a network, as shown in Figure 21.19. A query message was received at time 0; the random delay time (in tenths of seconds) for each group is shown next to the group address. Show the sequence of report messages.*

## Solution

*The events occur in this sequence:*

*a. Time 12: The timer for 228.42.0.0 in host A expires, and a membership report is sent, which is received by the router and every host including host B which cancels its timer for 228.42.0.0.*

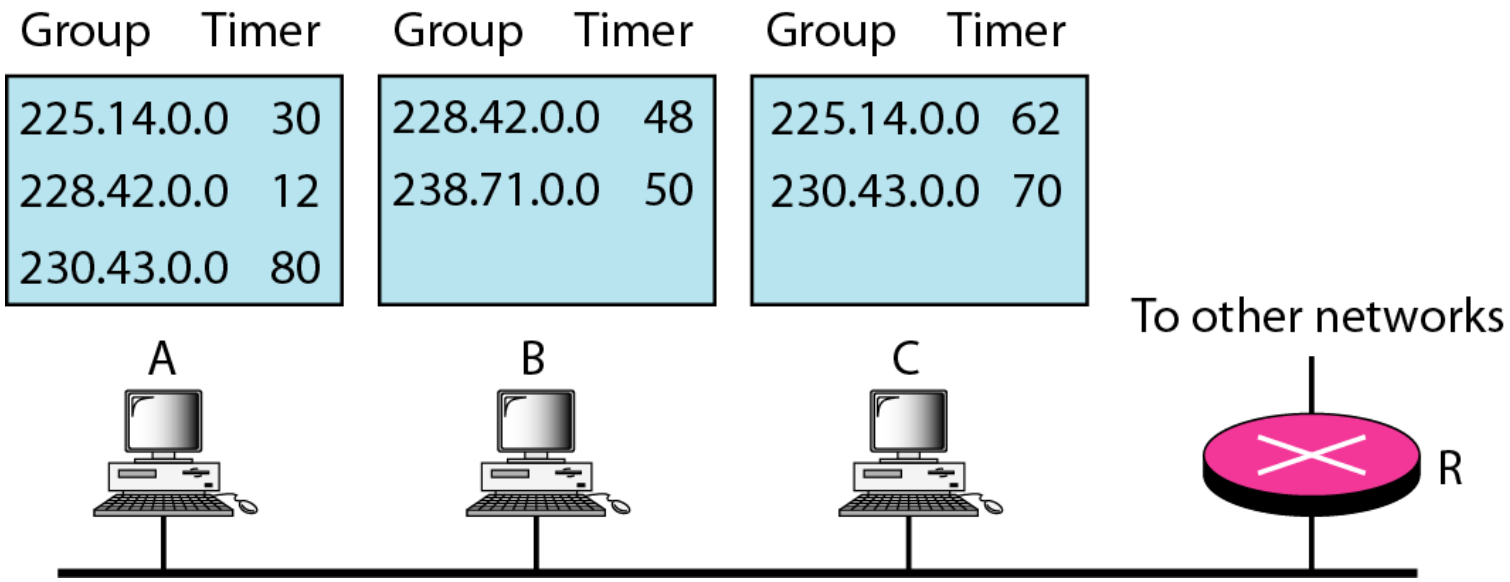
# Example 21.6 (continued)

**b.** ***Time 30:*** *The timer for 225.14.0.0 in host A expires, and a membership report is sent which is received by the router and every host including host C which cancels its timer for 225.14.0.0.*

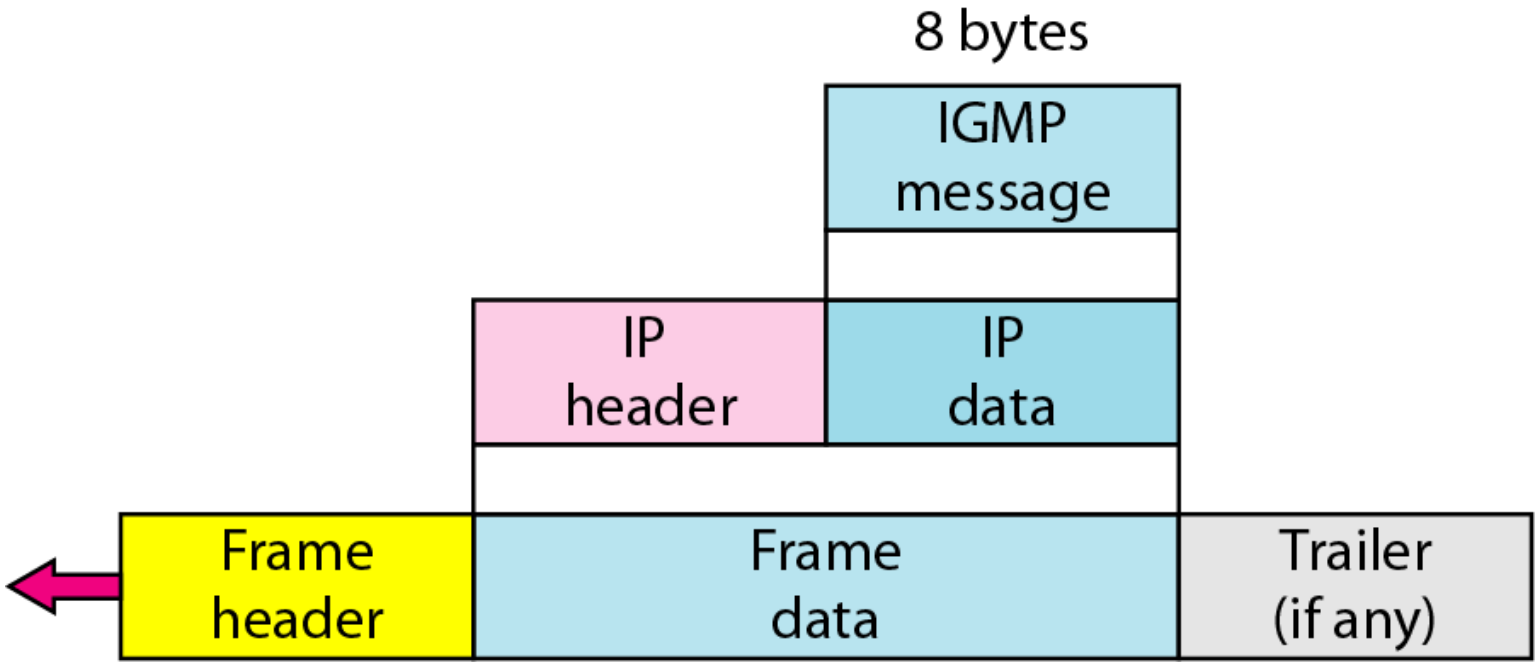
**c.** ***Time 50:*** *The timer for 238.71.0.0 in host B expires, and a membership report is sent, which is received by the router and every host.*

**d.** ***Time 70:*** *The timer for 230.43.0.0 in host C expires, and a membership report is sent, which is received by the router and every host including host A which cancels its timer for 230.43.0.0.*

## Figure 21.19 *Example 21.6*



## Figure 21.20 *Encapsulation of IGMP packet*



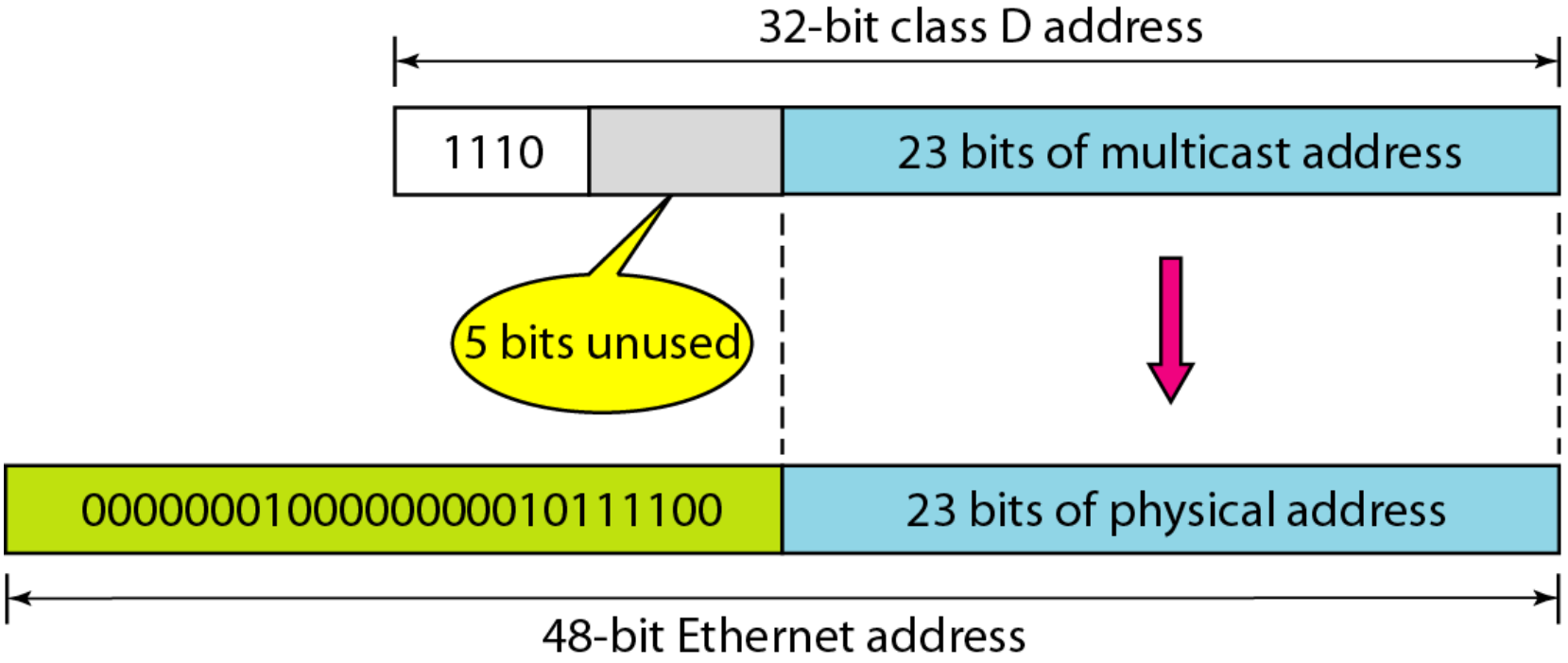
*Note*

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

**Table 21.2** ***Destination IP addresses***

| *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 |

## Figure 21.21 *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 21.7

*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. This can be done by changing the rightmost 3 bytes to hexadecimal and then subtracting 8 from the leftmost digit if it is greater than or equal to 8. In our example, the result is 2B:0E:07.*

# Example 21.7 (continued)

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

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

# Example 21.8

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

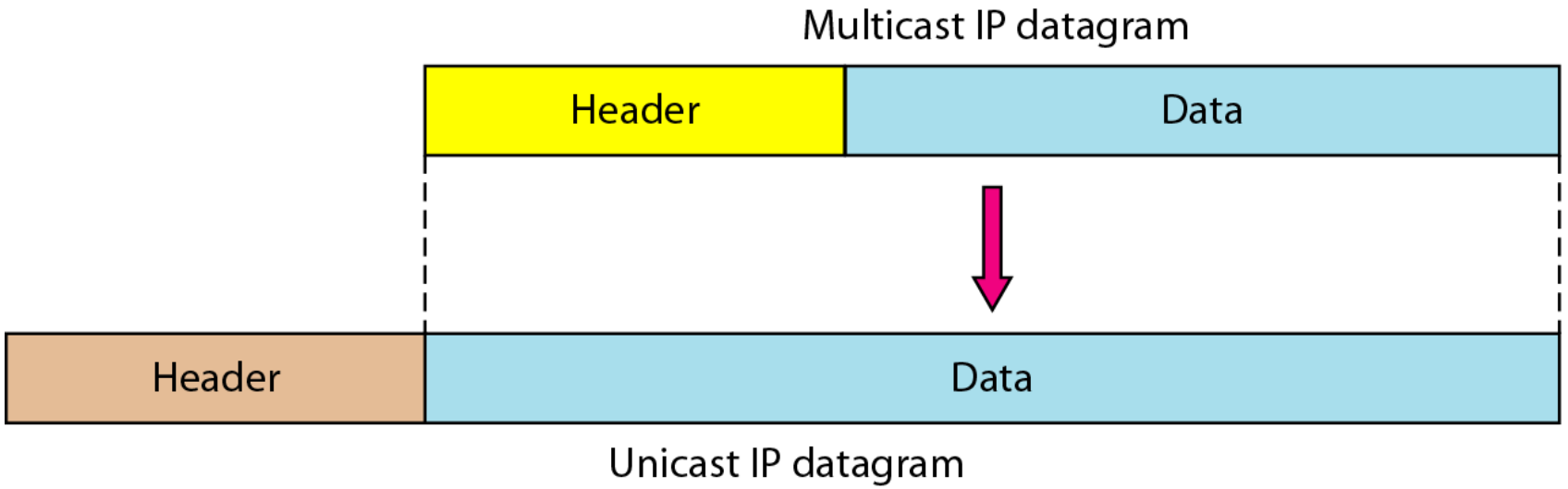
*Solution*

*a. The rightmost 3 bytes in hexadecimal is D4:18:09. We need to subtract 8 from the leftmost digit, resulting in 54:18:09.*

*b. We add the result of part a to the Ethernet multicast starting address. The result is*

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

## Figure 21.22 *Tunneling*



# Example 21.9

*We use netstat (see next slide) 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 21.9 (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 |

# 21-4 ICMPv6

*We discussed IPv6 in Chapter 20. Another 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.*

***Topics discussed in this section:***

**Error Reporting**

**Query**

## Figure 21.23 *Comparison of network layers in version 4 and version 6*

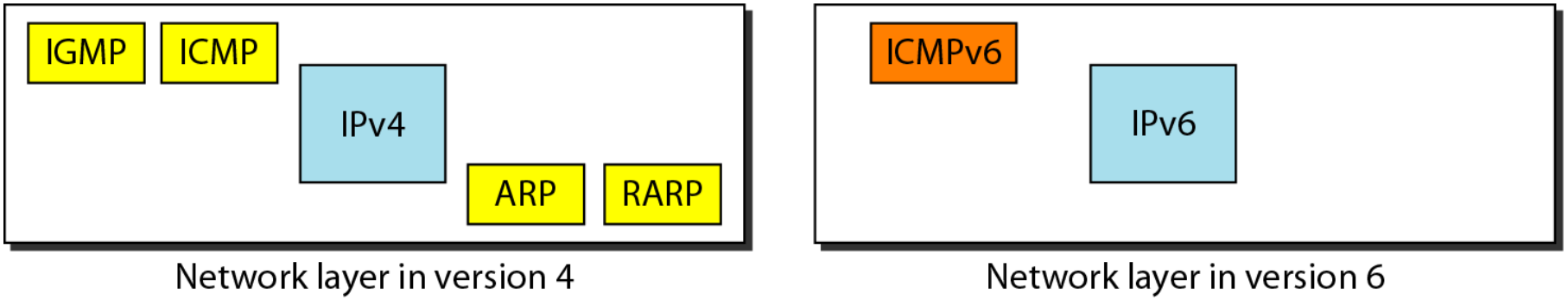


**Table 21.3** ***Comparison of error-reporting messages in ICMPv4 and ICMPv6***

| *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 |

**Table 21.4** *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 |