Network Layer: Address Mapping, Error Reporting, and Multicasting

Mr.K.K.RAJKUMAR/Communication Networks/19EC501

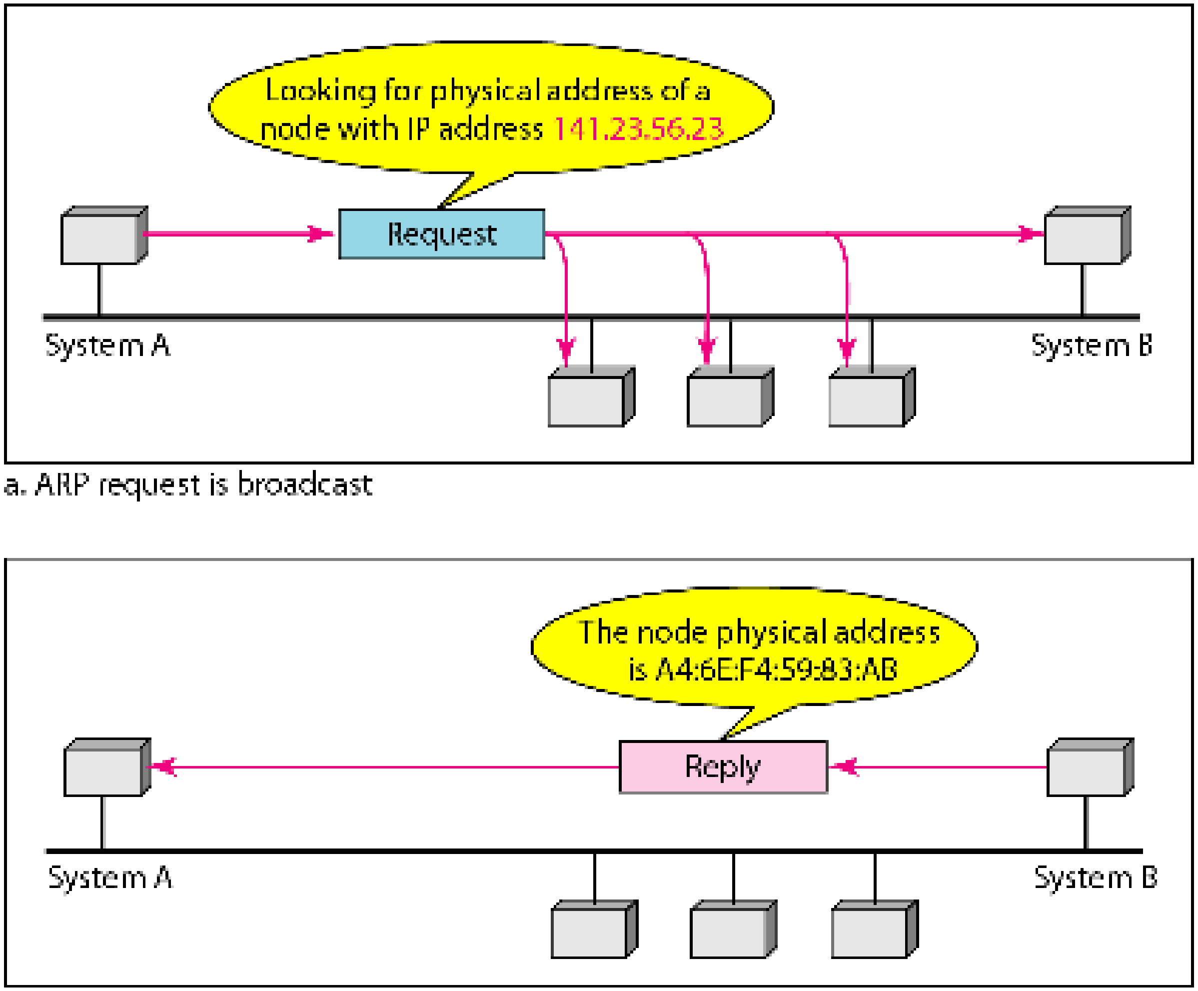
21-1 ADDRESS MAPPING

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

Figure 21.1 *ARP operation*



a. ARP request is broadcast

b. ARP reply is unicast

Figure 21.2 *ARP packet*

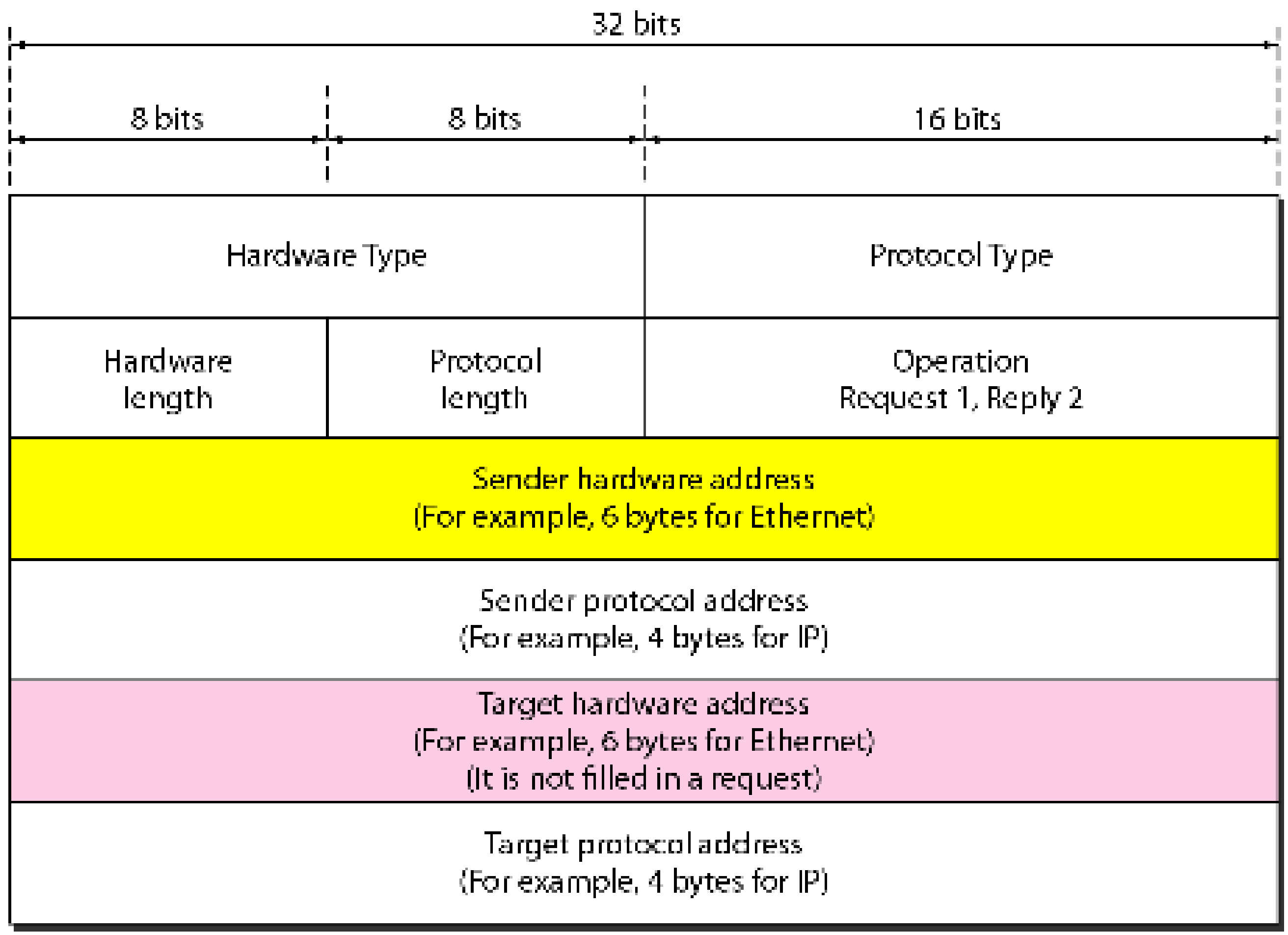


Figure 21.3 *Encapsulation of ARP packet*

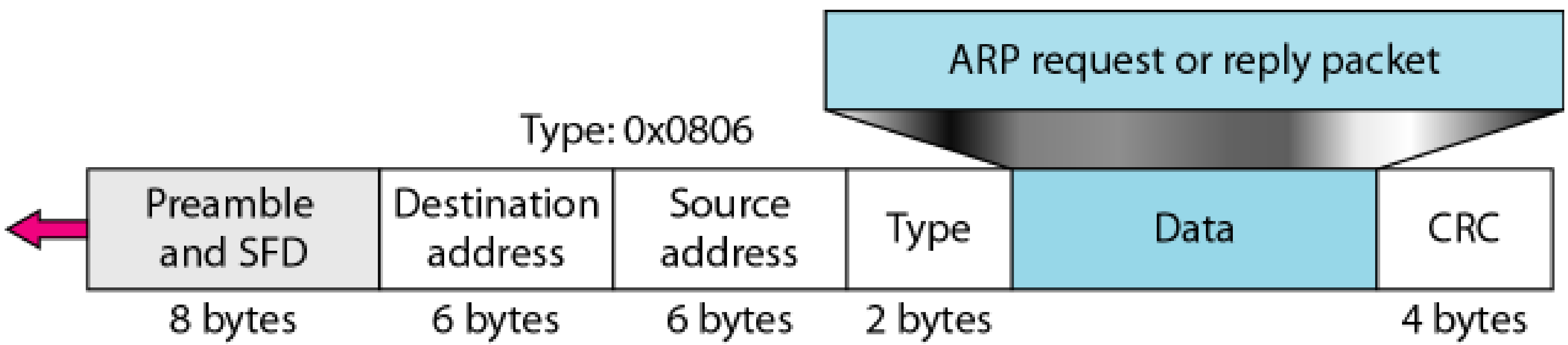
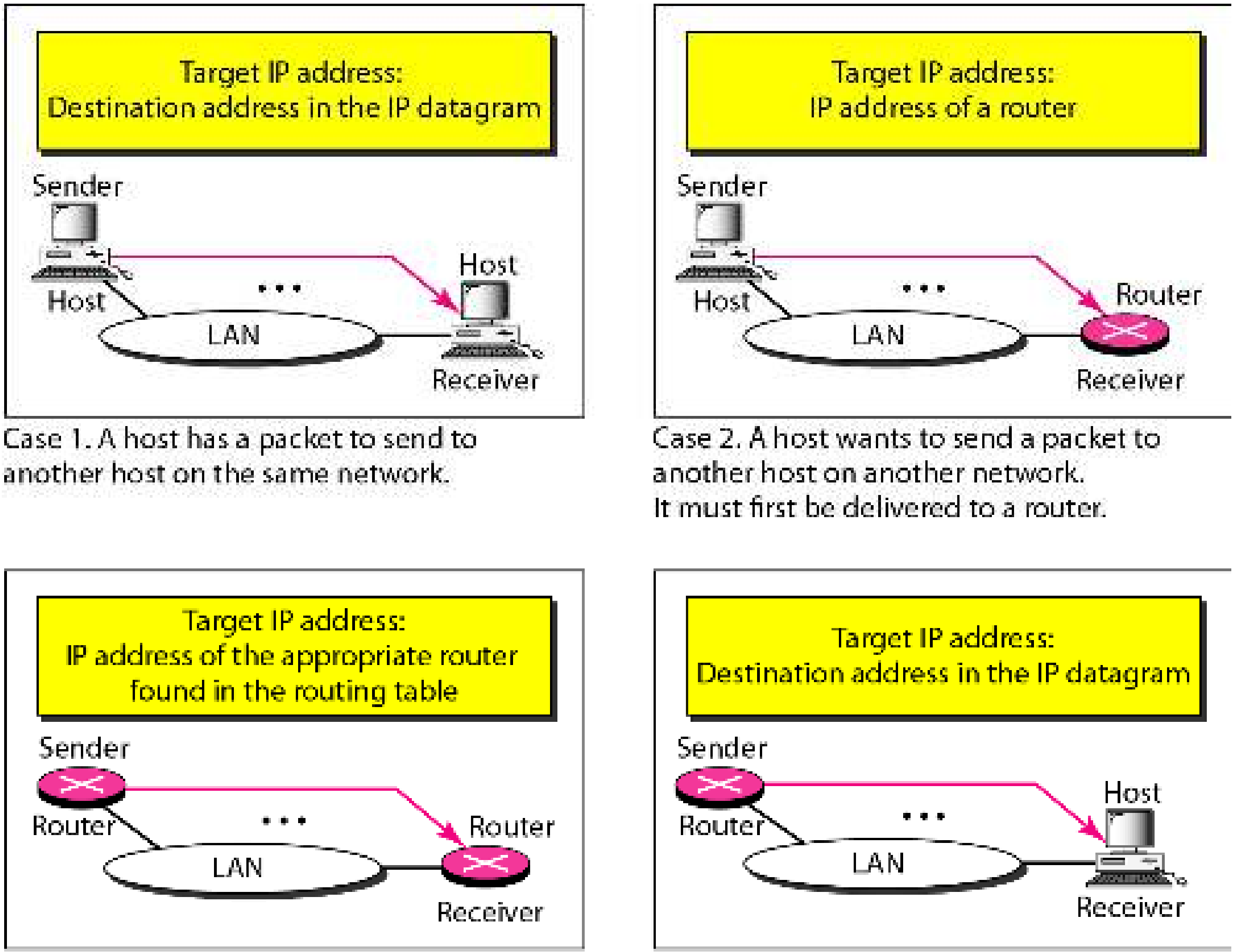


Figure 21.4 *Four cases using ARP*



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*

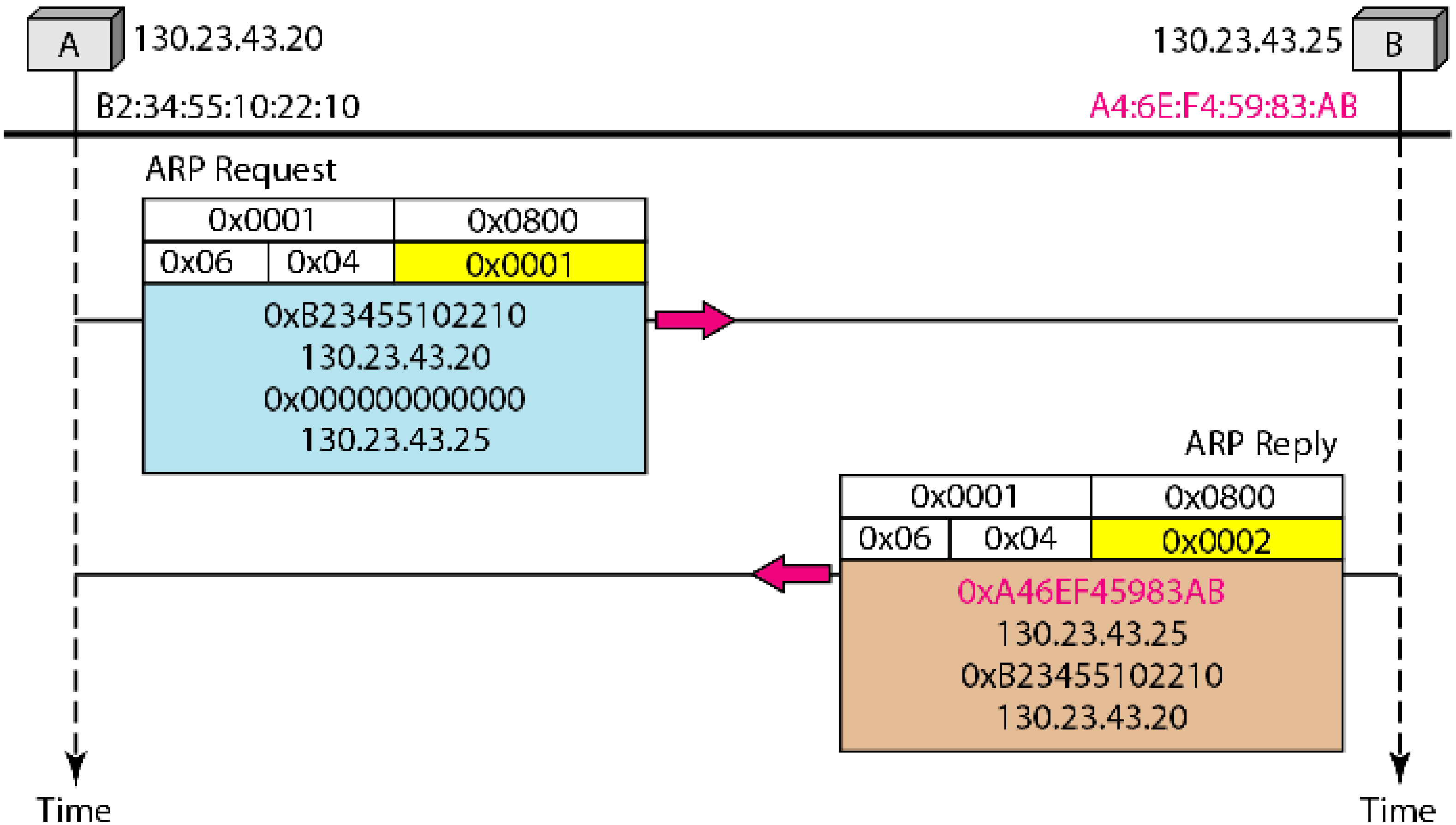


Figure 21.6 *Proxy ARP*

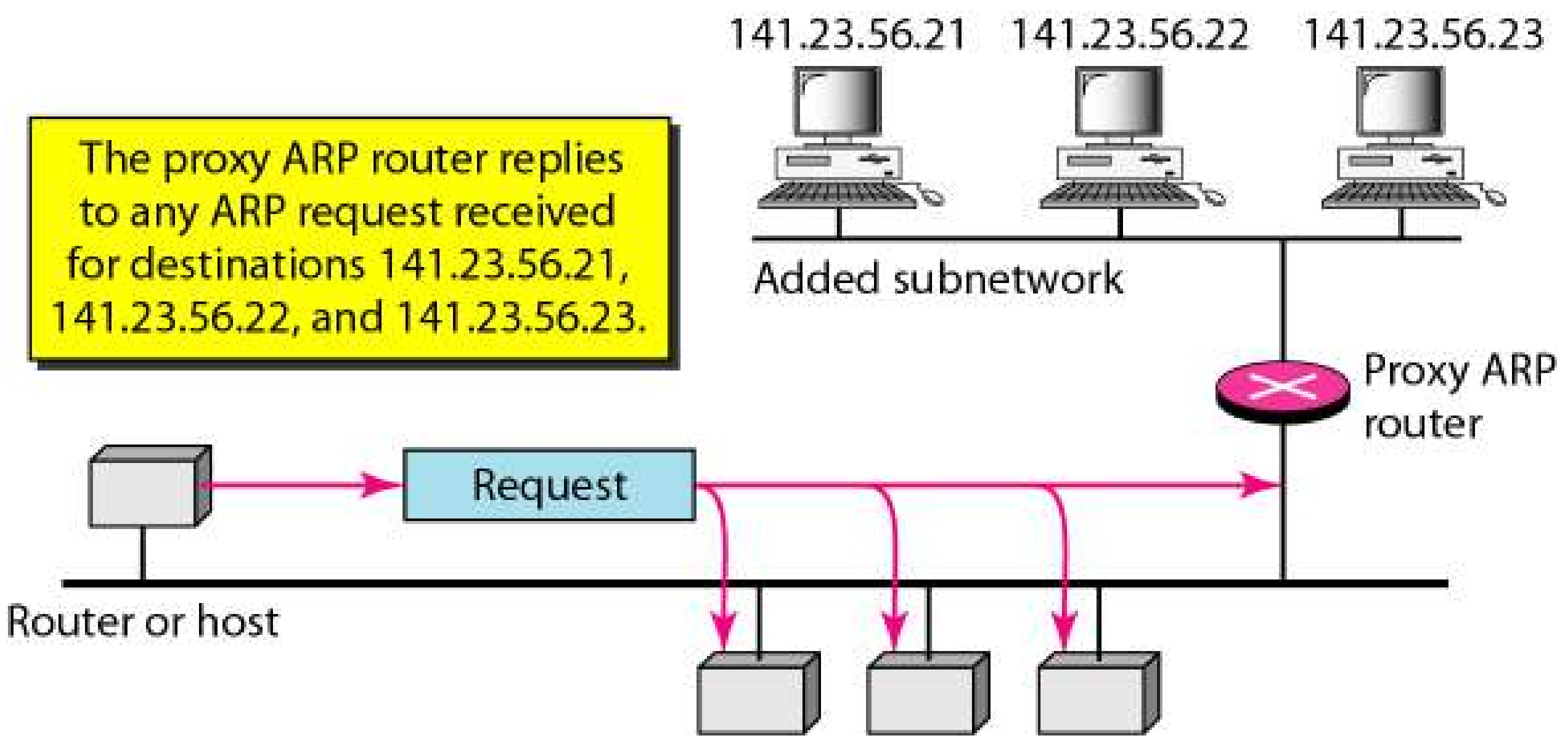
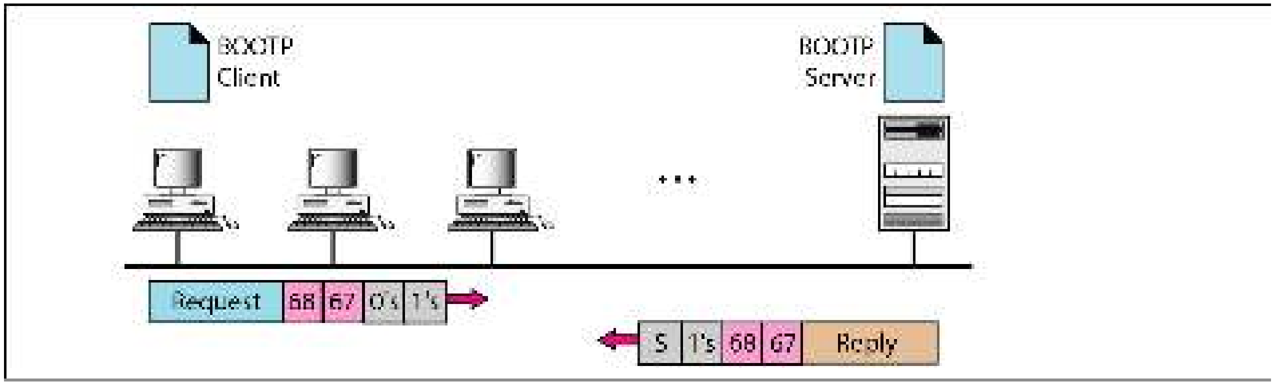
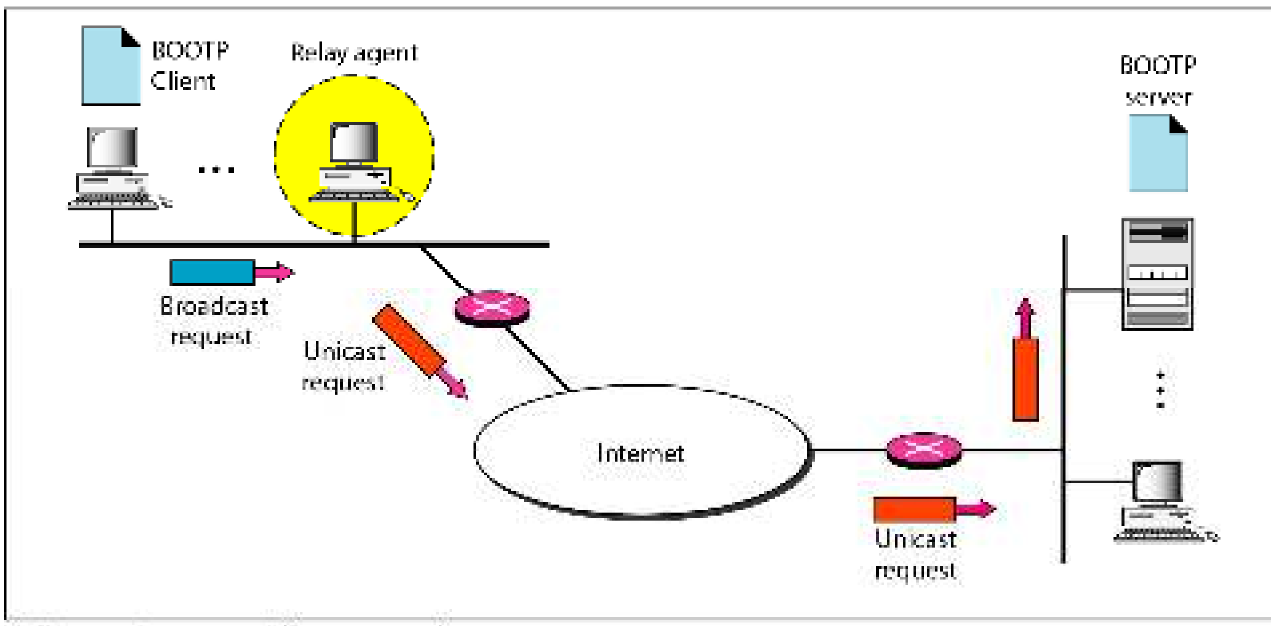


Figure 21.7 *BOOTP client and server on the same and different networks*



a. Client and server on the same network



b. Client and server on different networks

Note

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

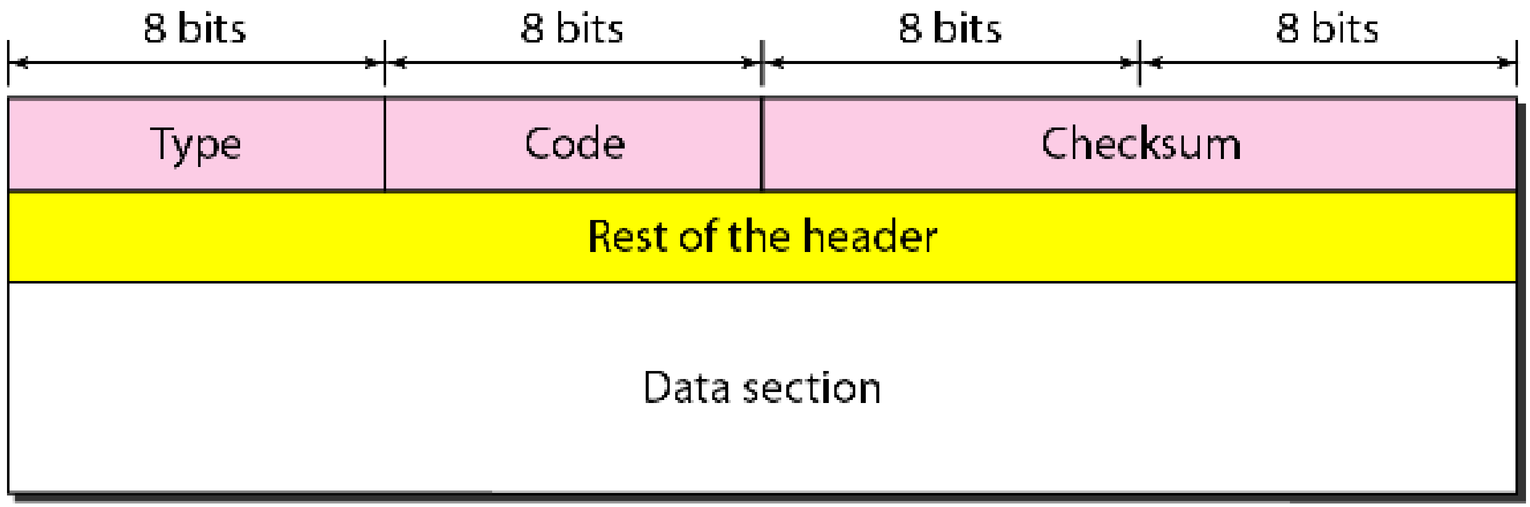
21-2 ICMP

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.

Topics discussed in this section:

Types of Messages
Message Format
Error Reporting and Query
Debugging Tools

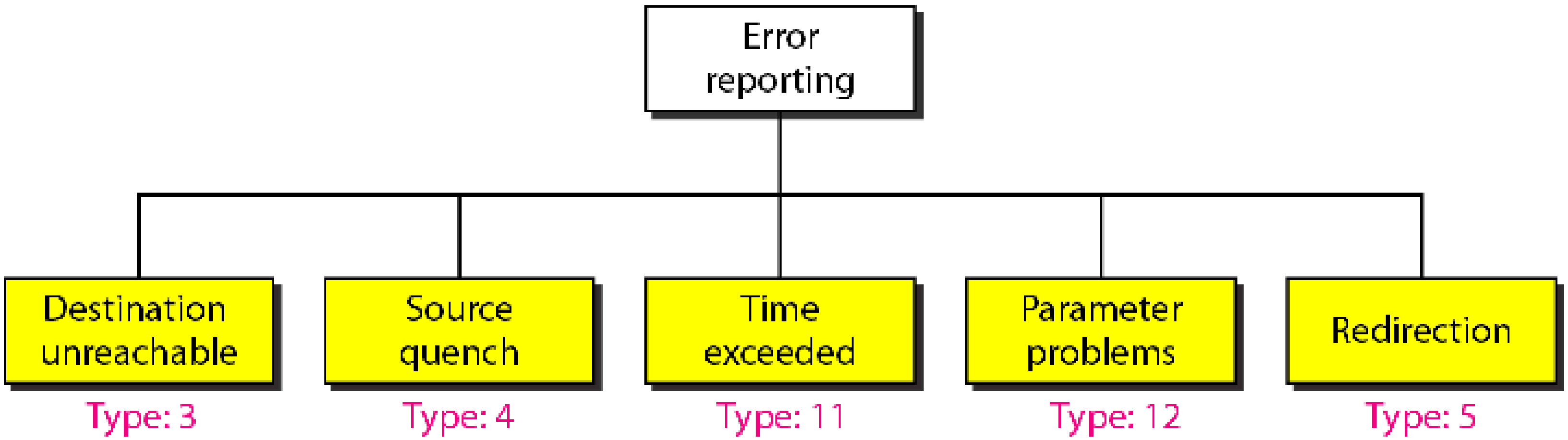
Figure 21.8 *General format of ICMP messages*



Note

ICMP always reports error messages to the original source.

Figure 21.9 *Error-reporting messages*



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*

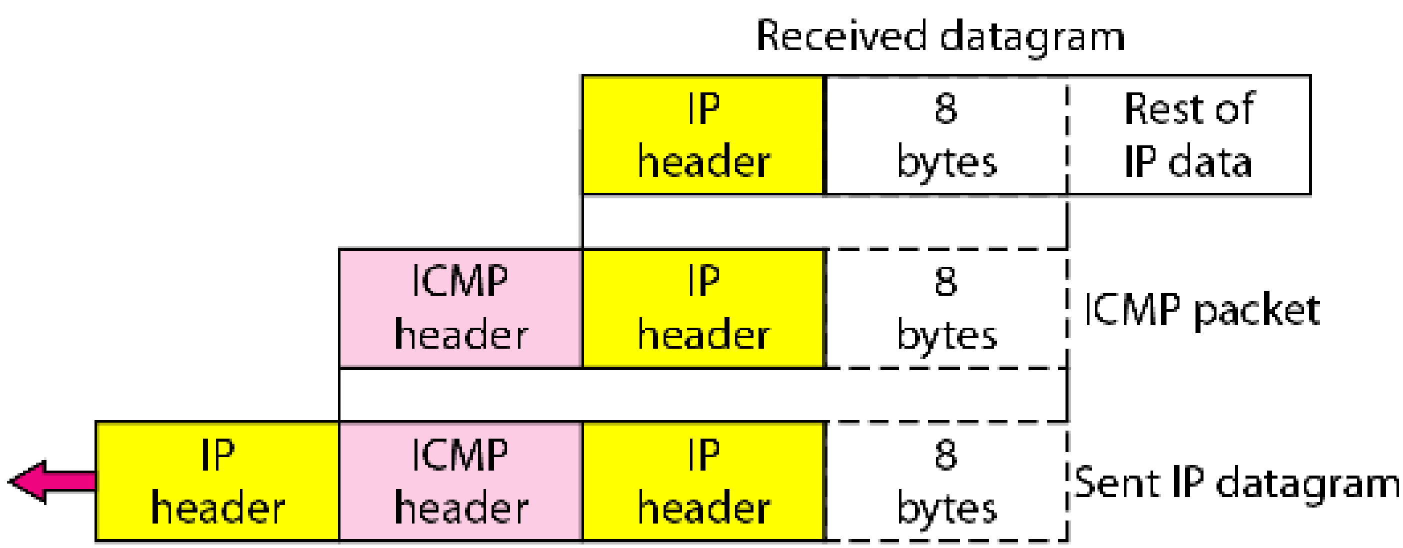


Figure 21.11 *Redirection concept*

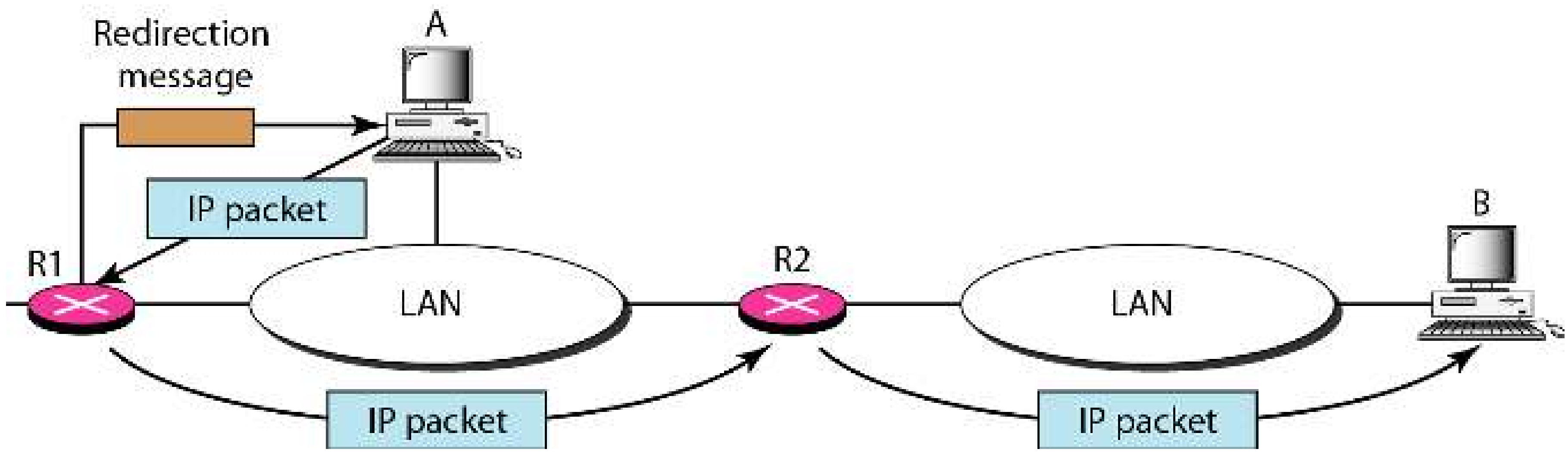


Figure 21.12 *Query messages*

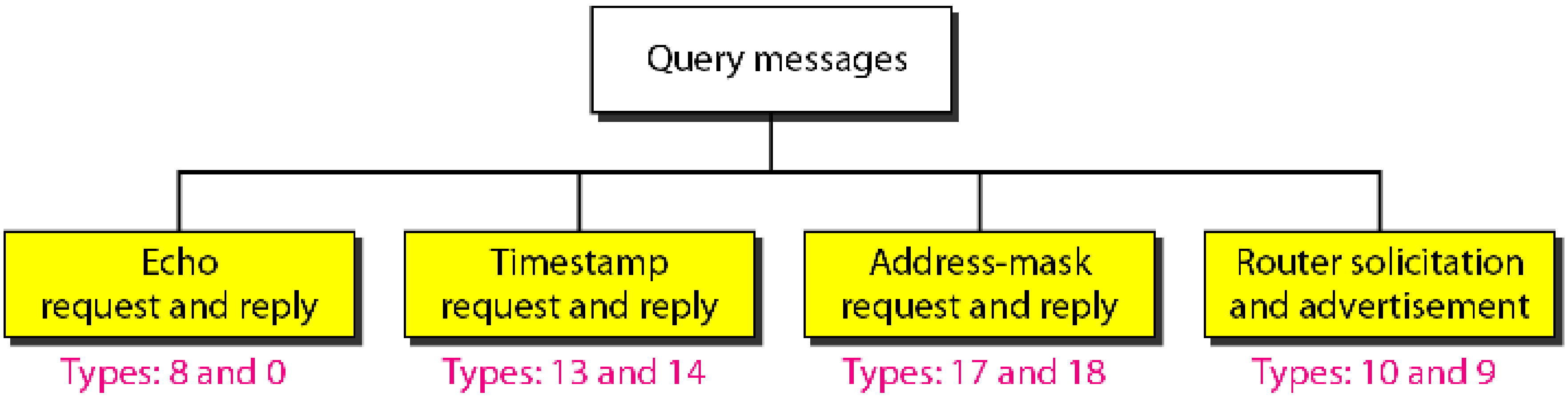
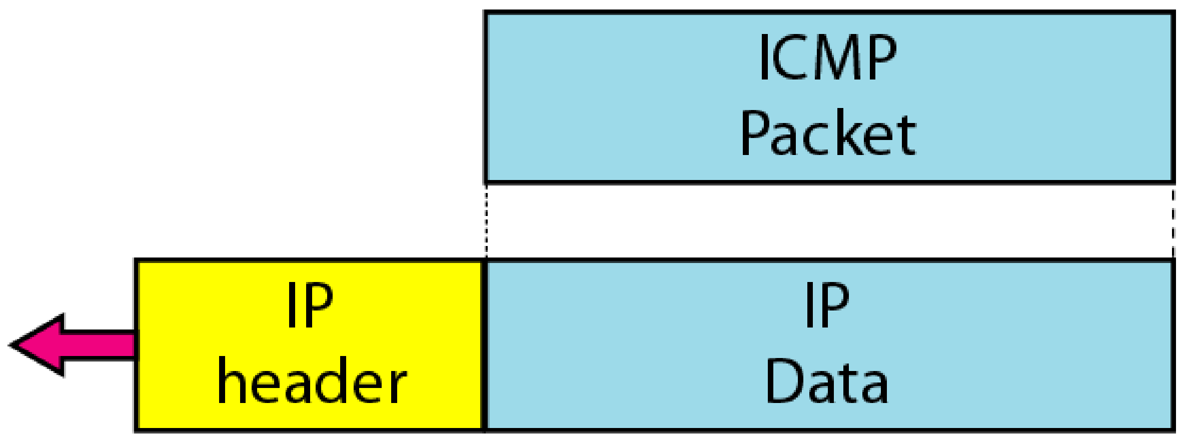


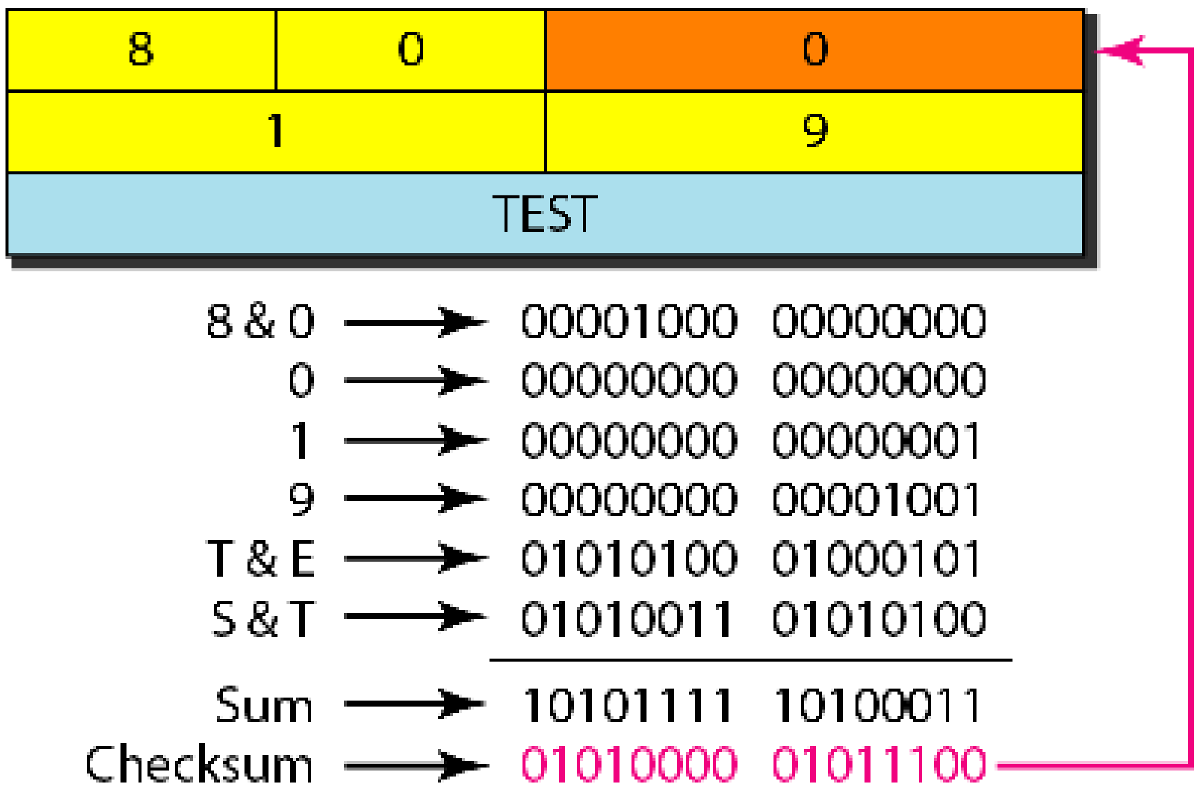
Figure 21.13 *Encapsulation of ICMP query messages*



Example 21.2

Figure 21.14 shows an example of checksum calculation for a simple echo-request message. We randomly chose the identifier to be 1 and the sequence number to be 9. The message is divided into 16-bit (2-byte) words. The words are added and the sum is complemented. Now the sender can put this value in the checksum field.

Figure 21.14 *Example of checksum calculation*



Example 21.3

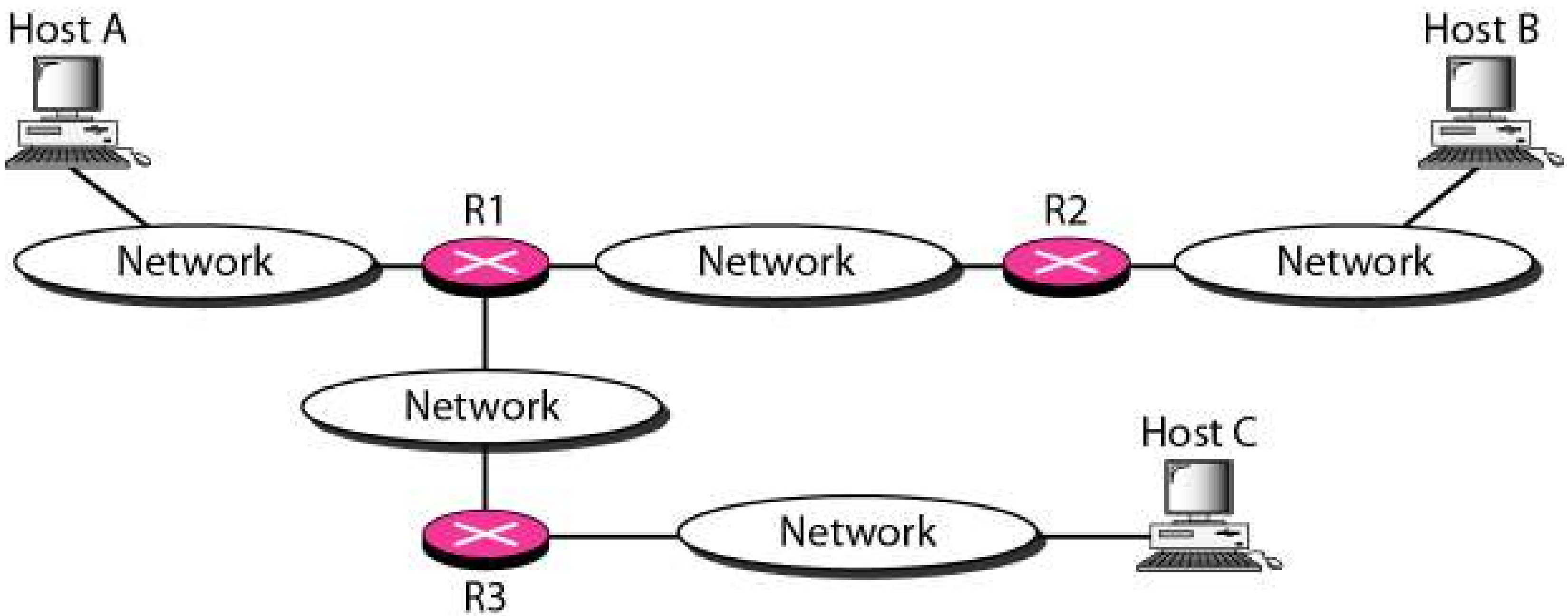
We use the ping program to test the server fhda.edu. The result is shown on the next slide. The ping program sends messages with sequence numbers starting from 0. For each probe it gives us the RTT time. The TTL (time to live) field in the IP datagram that encapsulates an ICMP message has been set to 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 21.3 (continued)

```
$ 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
```

Figure 21.15 *The traceroute program operation*



Example 21.4

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 21.4 (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 21.5

In this example, we trace a longer route, the route to xerox.com (see next slide). 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.

Example 21.5 (continued)

```
$ 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
```

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

Figure 21.16 *IGMP message types*

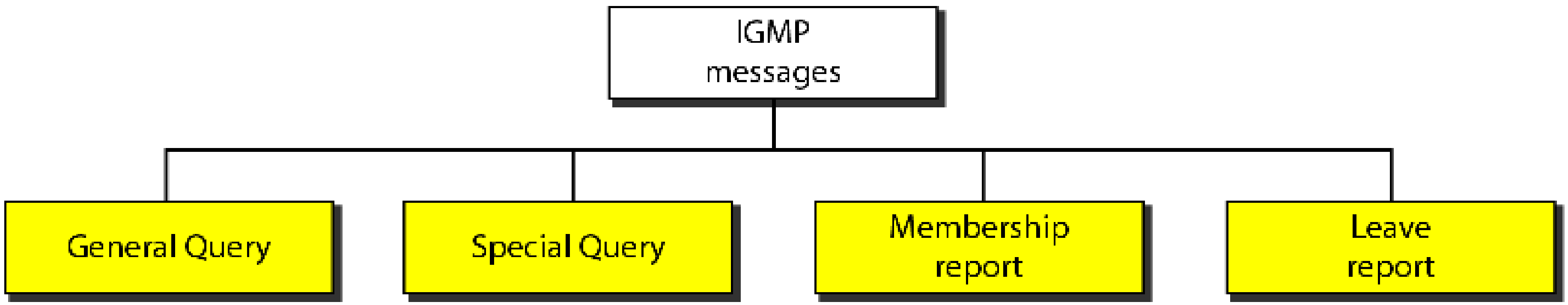


Figure 21.17 *IGMP message format*

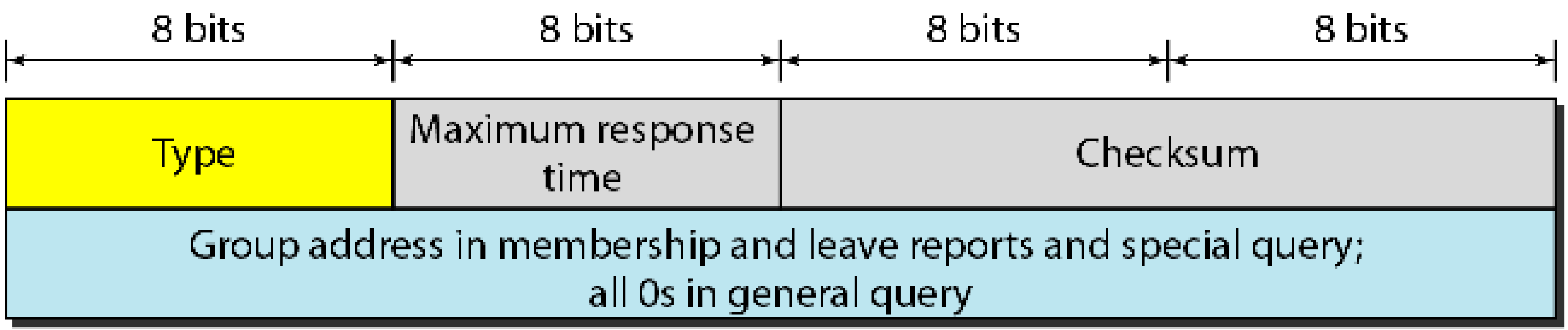
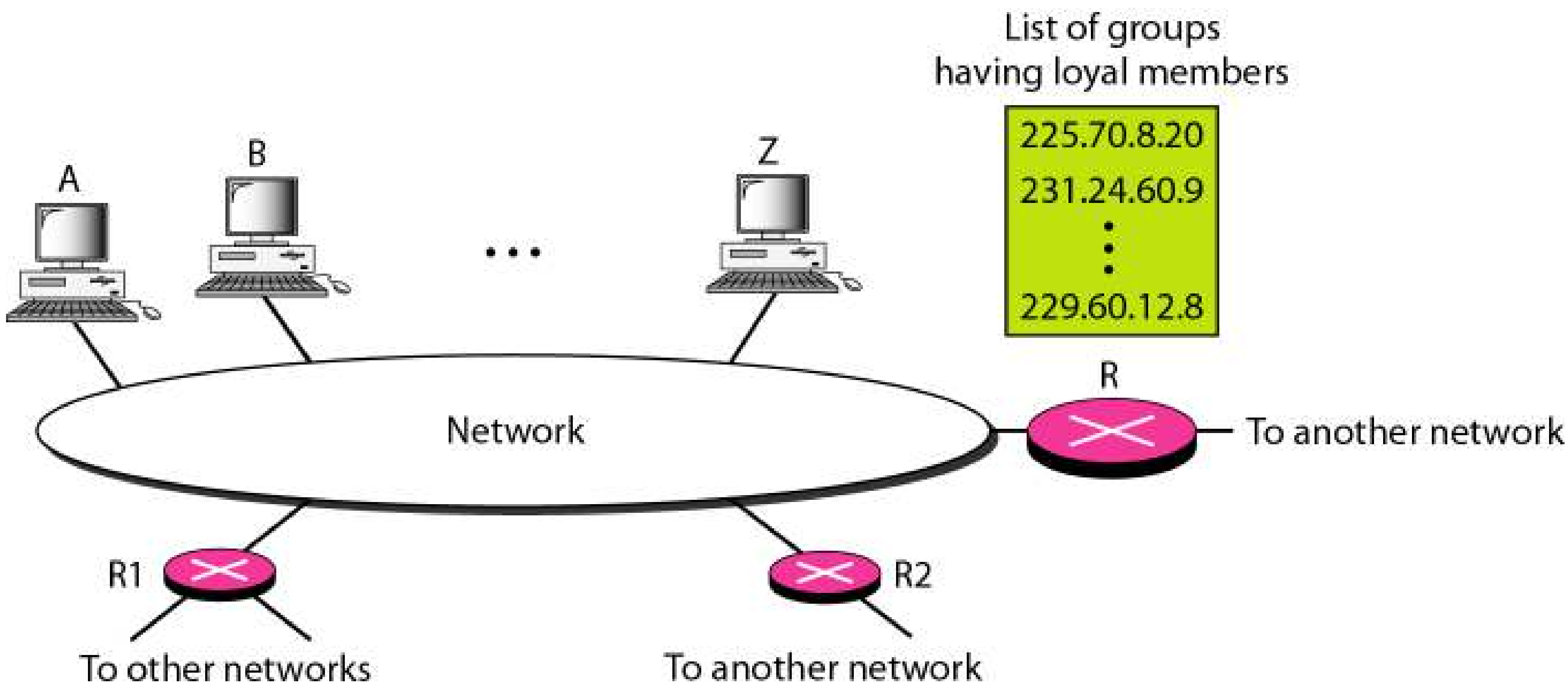


Table 21.1 ***IGMP type field***

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*

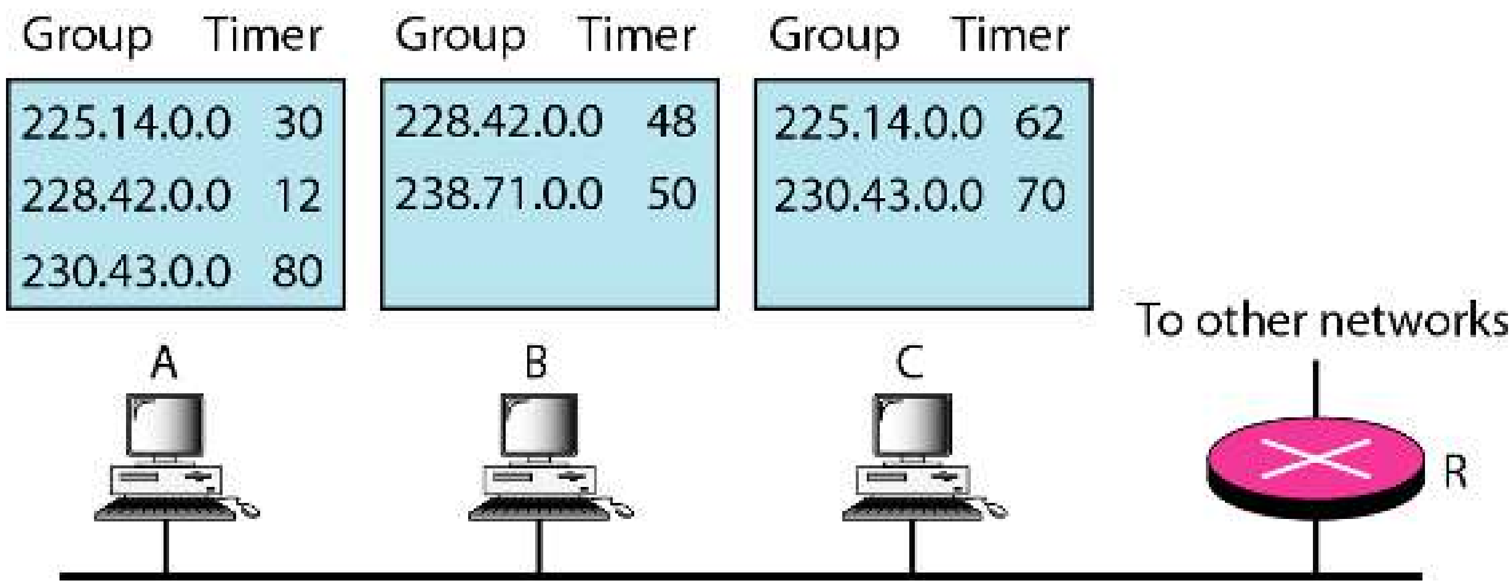
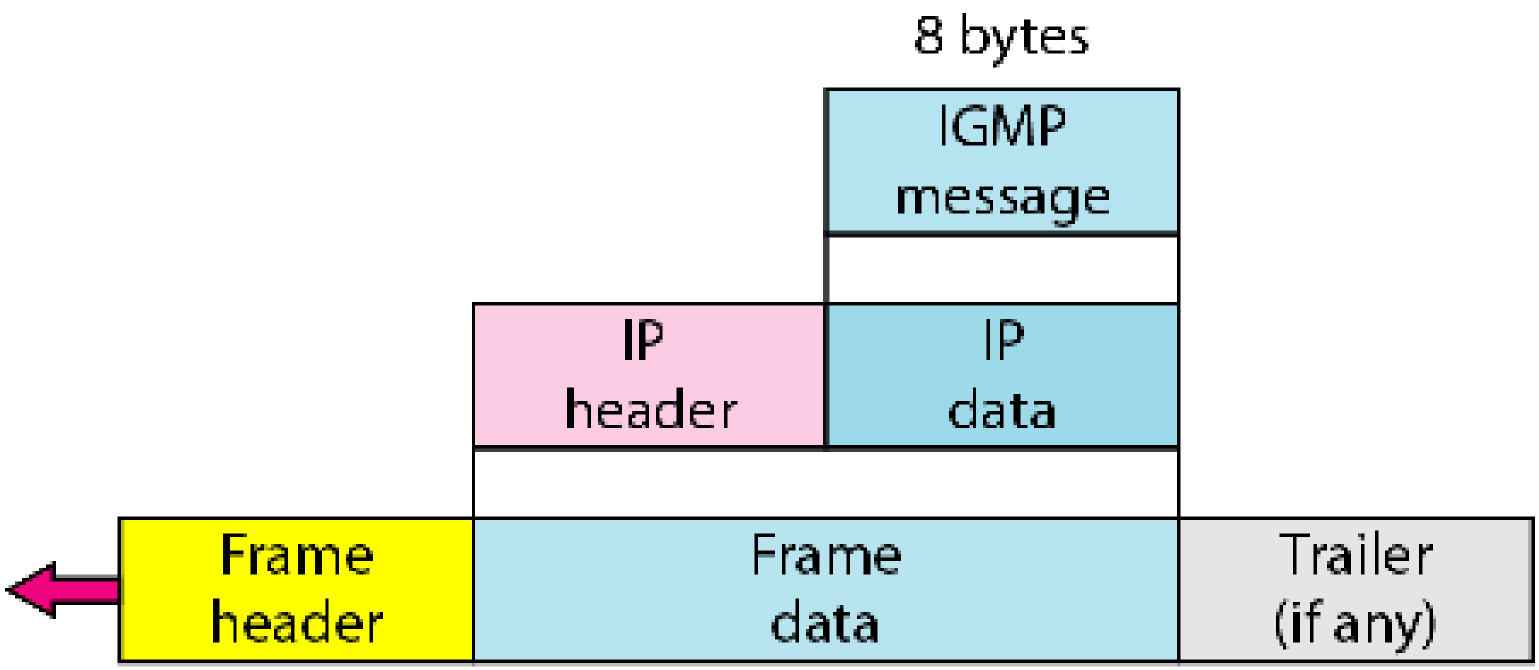


Figure 21.20 *Encapsulation of IGMP packet*



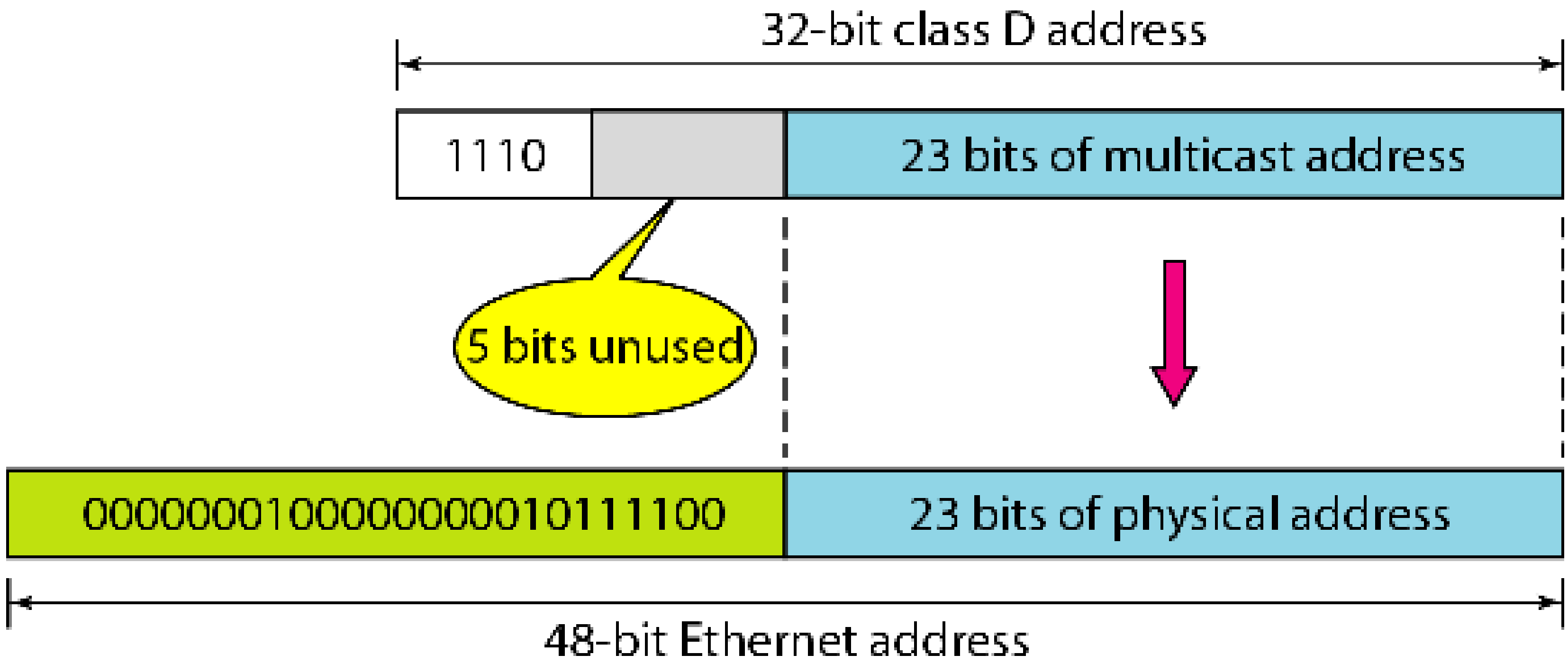
Note

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.

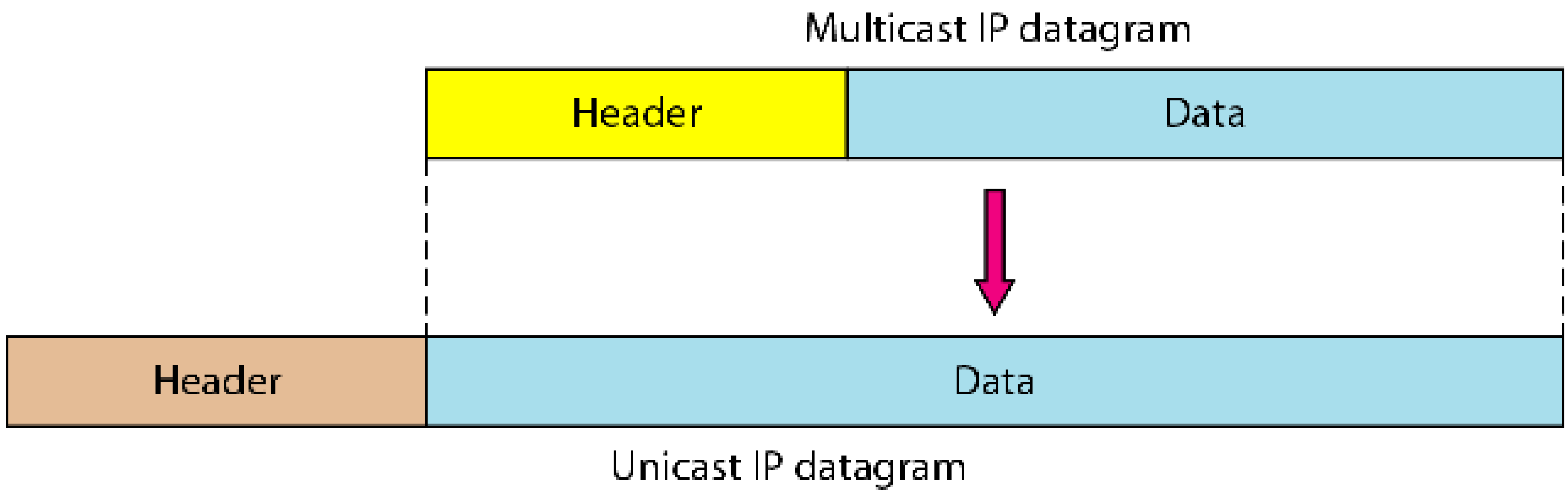
Solution

***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

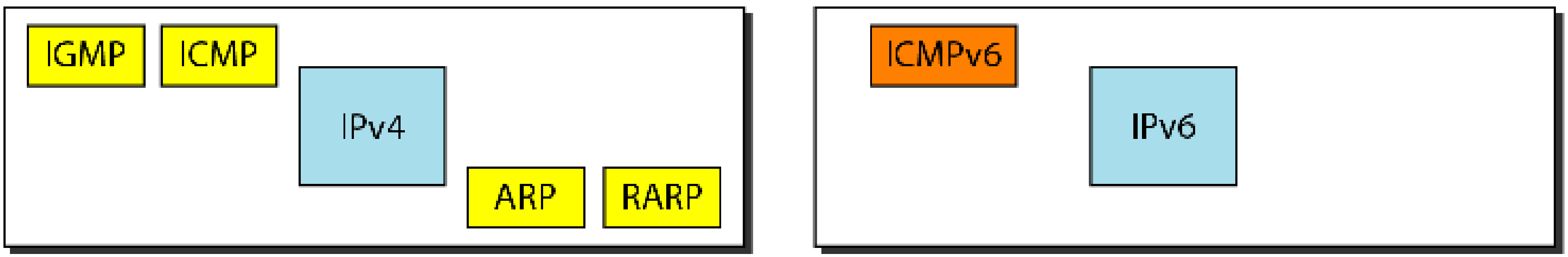
21-4 ICMPv6

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*



Network layer in version 4

Network layer in 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