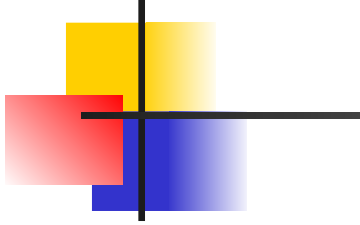
Network Layer: Address Mapping, Error Reporting, and Multicasting

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.

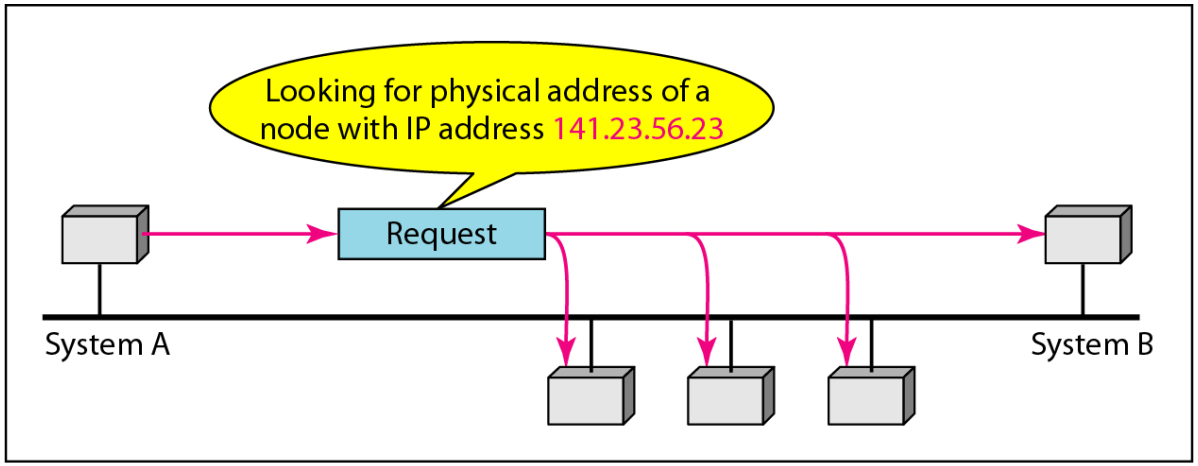
Mapping Logical to Physical Address
Mapping Physical to Logical Address



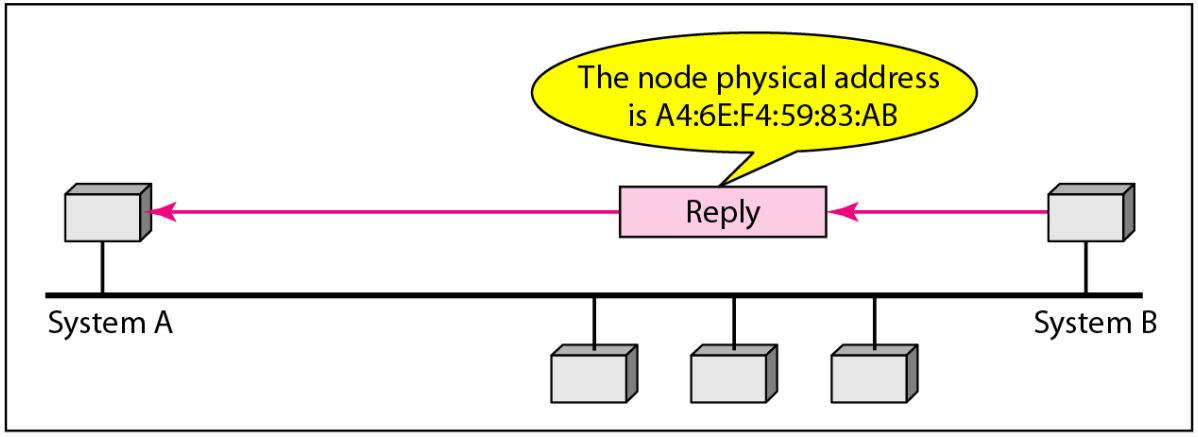
Mapping logical address to physical address

- ARP- Address Resolution Protocol
  - Cache Memory

Figure 21.1 *ARP operation*



a. ARP request is broadcast



b. ARP reply is unicast

Figure 21.2 *ARP packet*

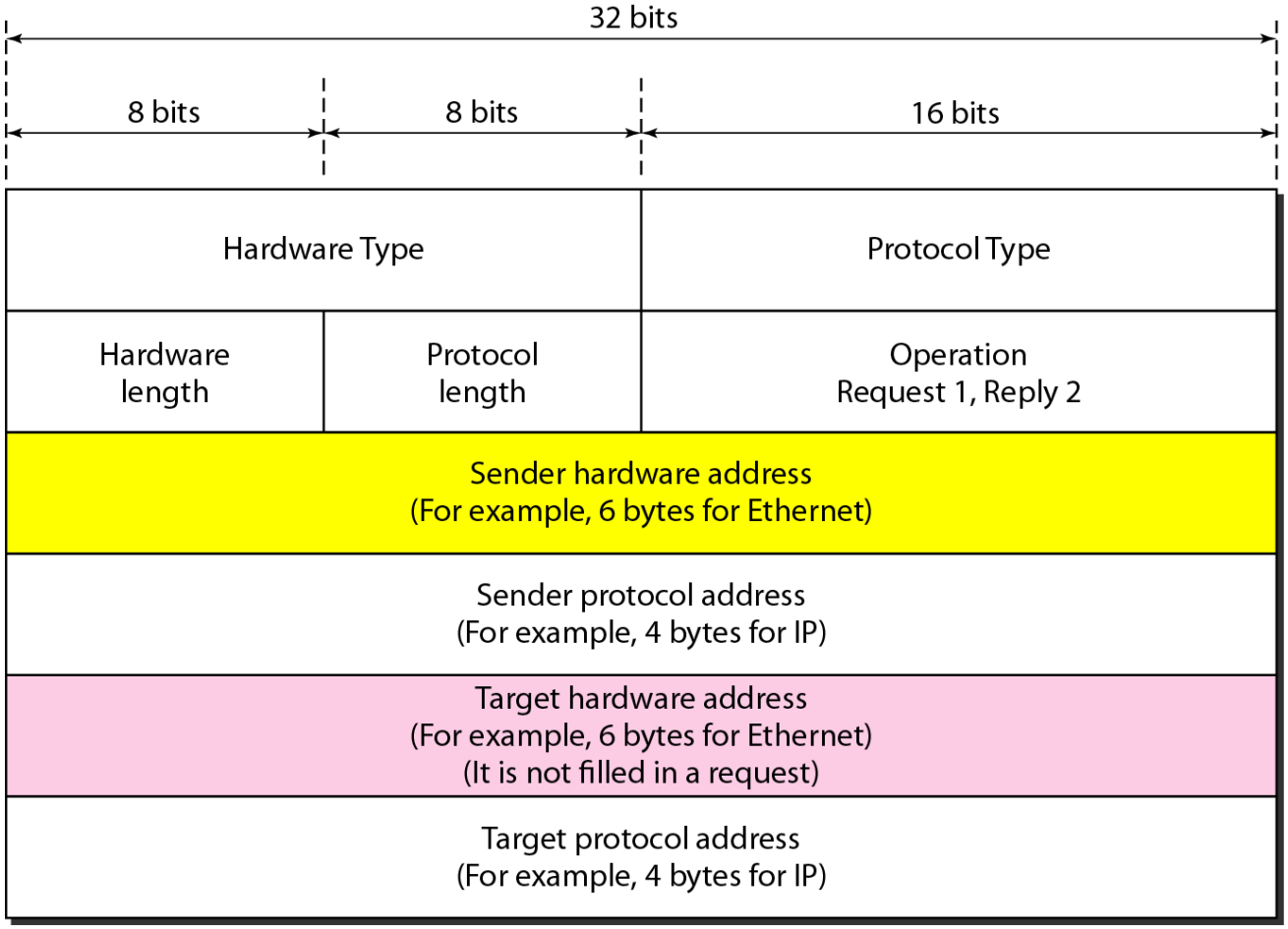


Figure 21.3 *Encapsulation of ARP packet*

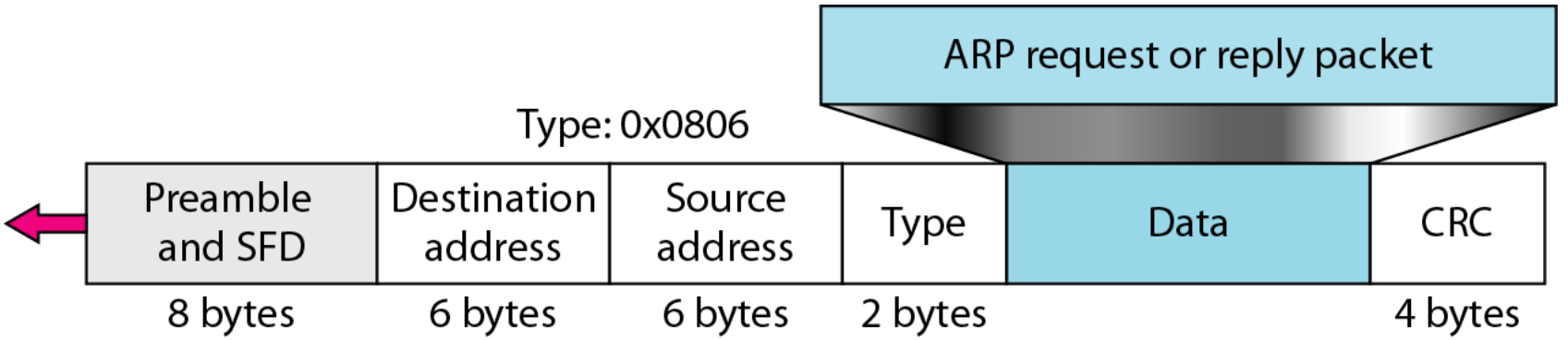
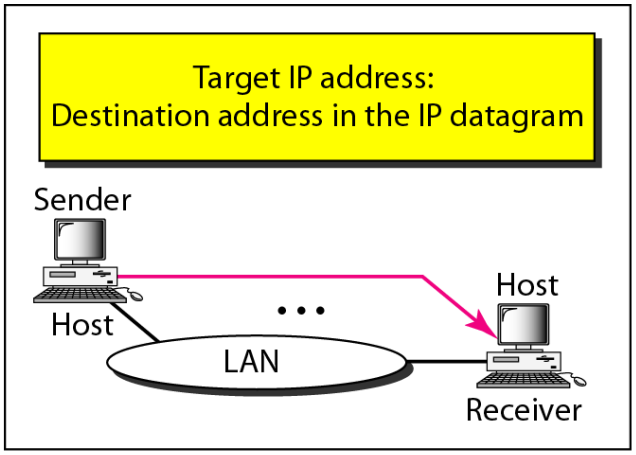
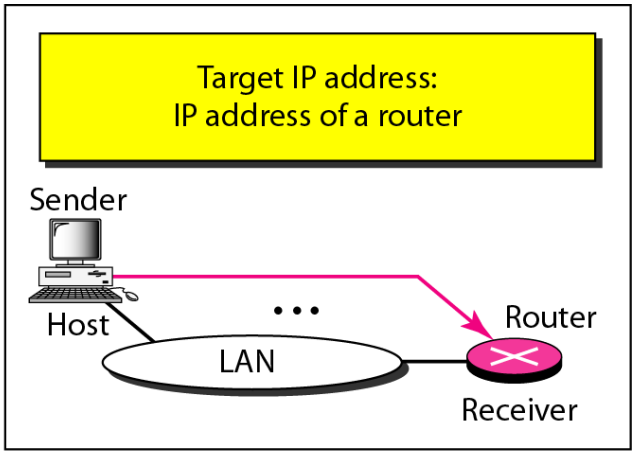


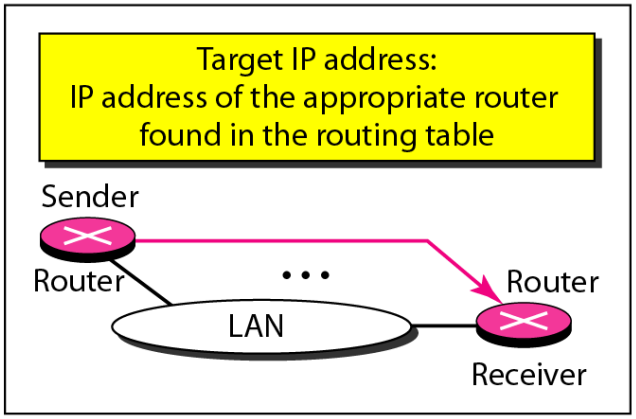
Figure 21.4 *Four cases using ARP*



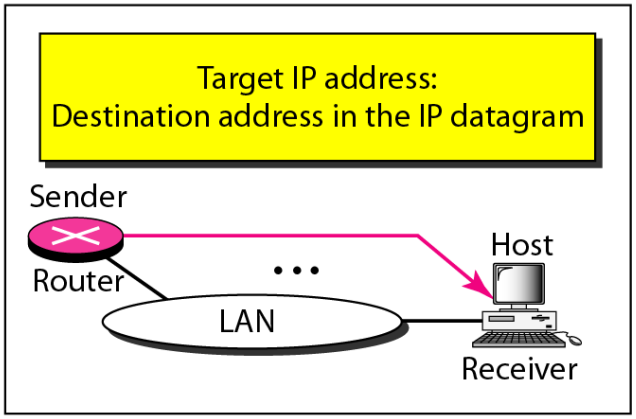
Case 1. A host has a packet to send to another host on the same network.



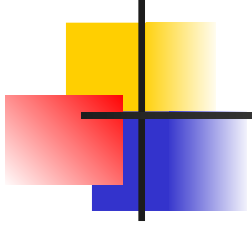
Case 2. A host wants to send a packet to another host on another network. It must first be delivered to a router.



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.



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*

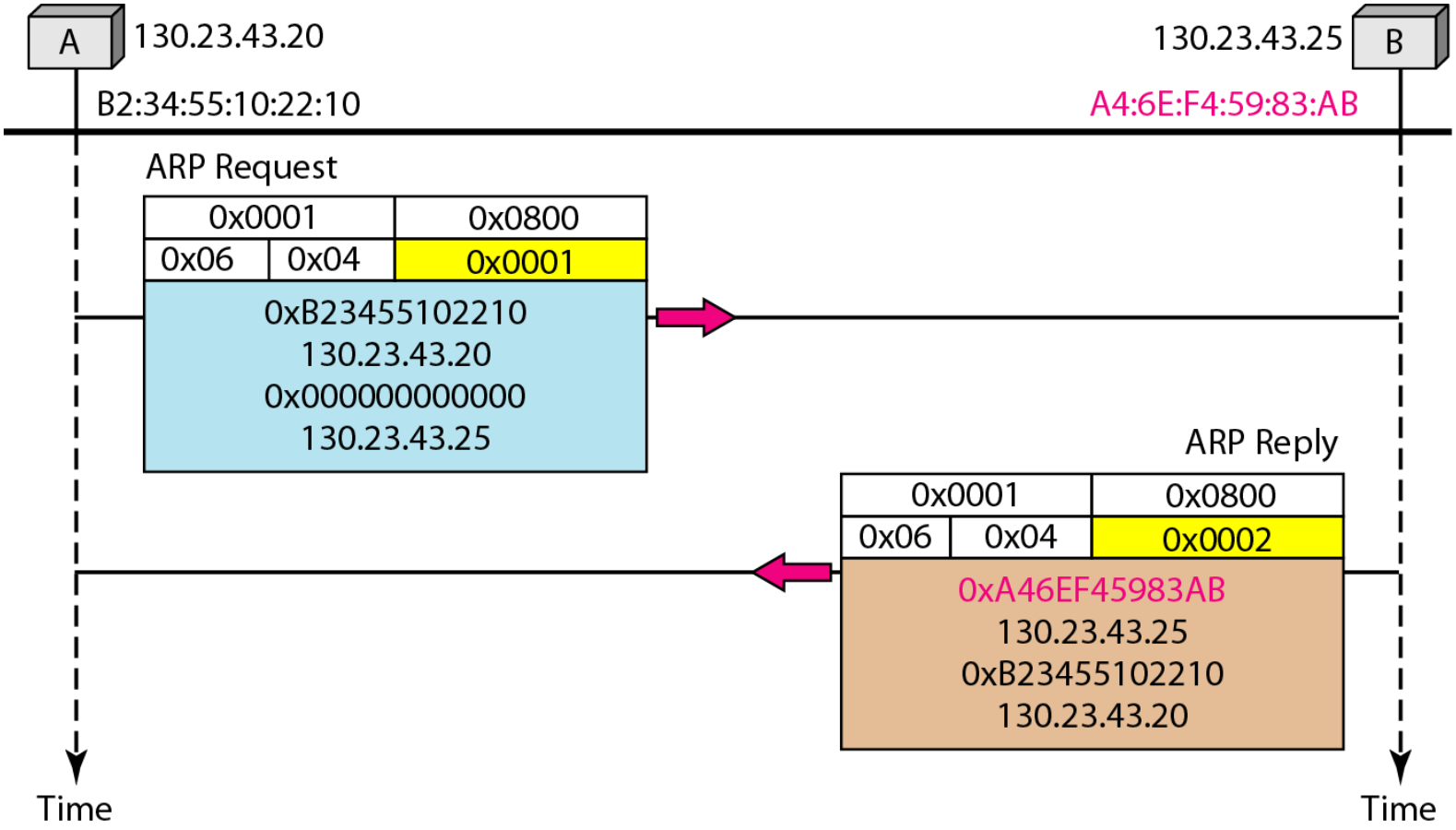
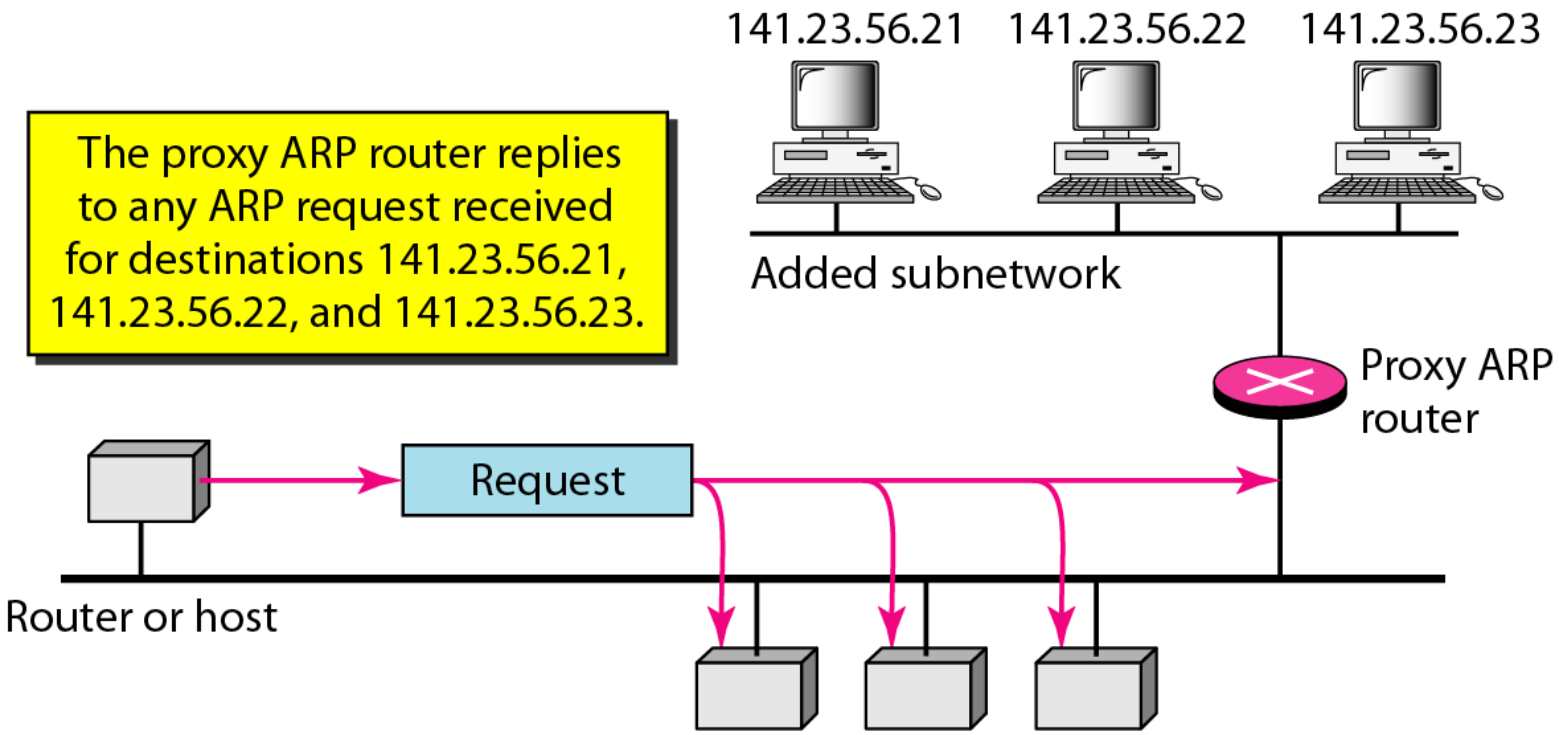


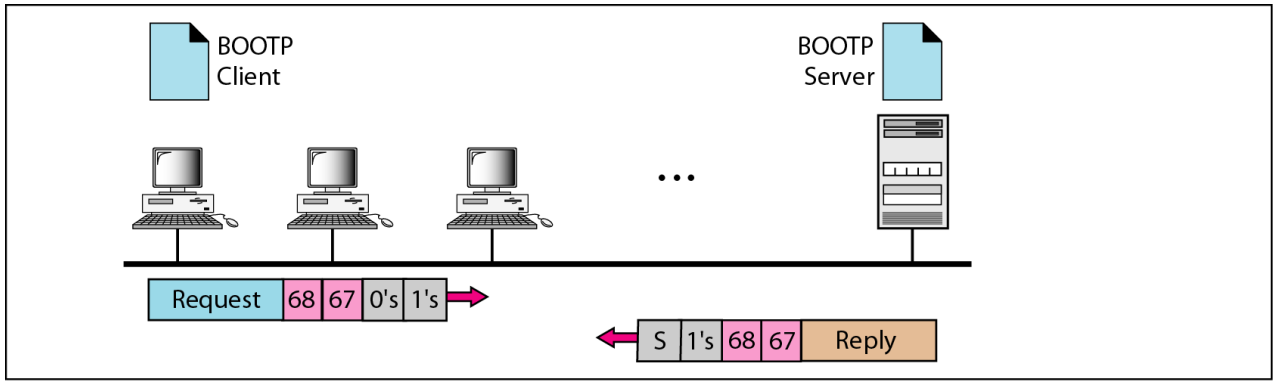
Figure 21.6 *Proxy ARP*



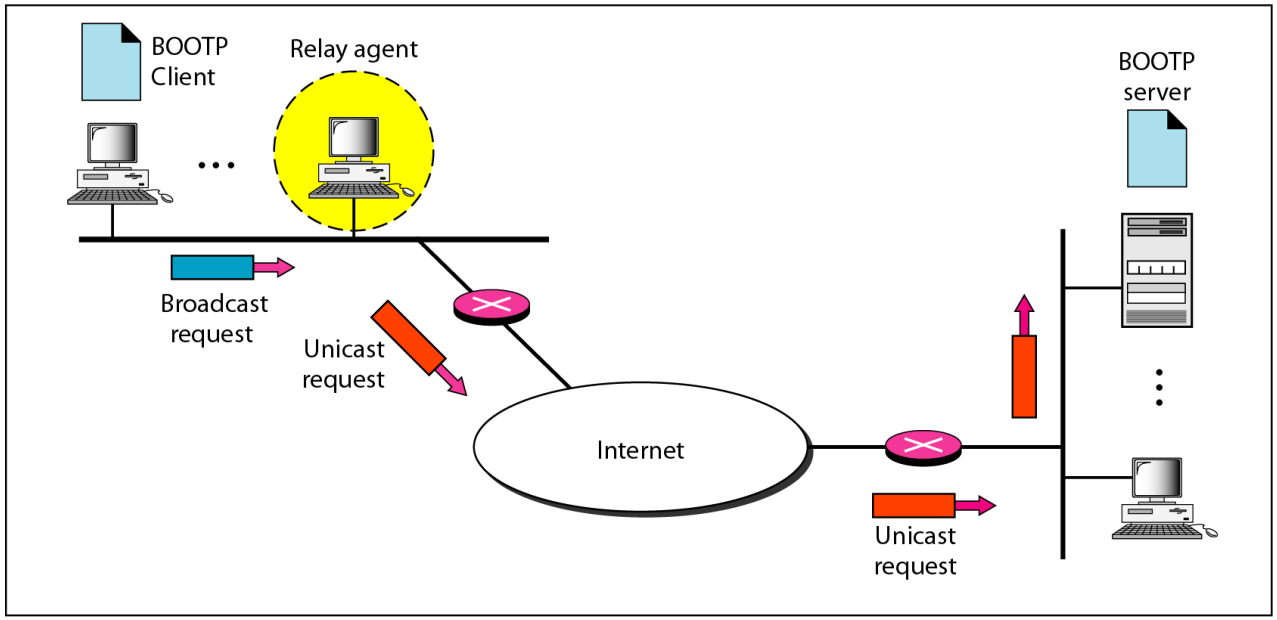
Mapping physical address to logical address

- RARP – Reverse ARP
- BOOTP
- DHCP

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



a. Client and server on the same network



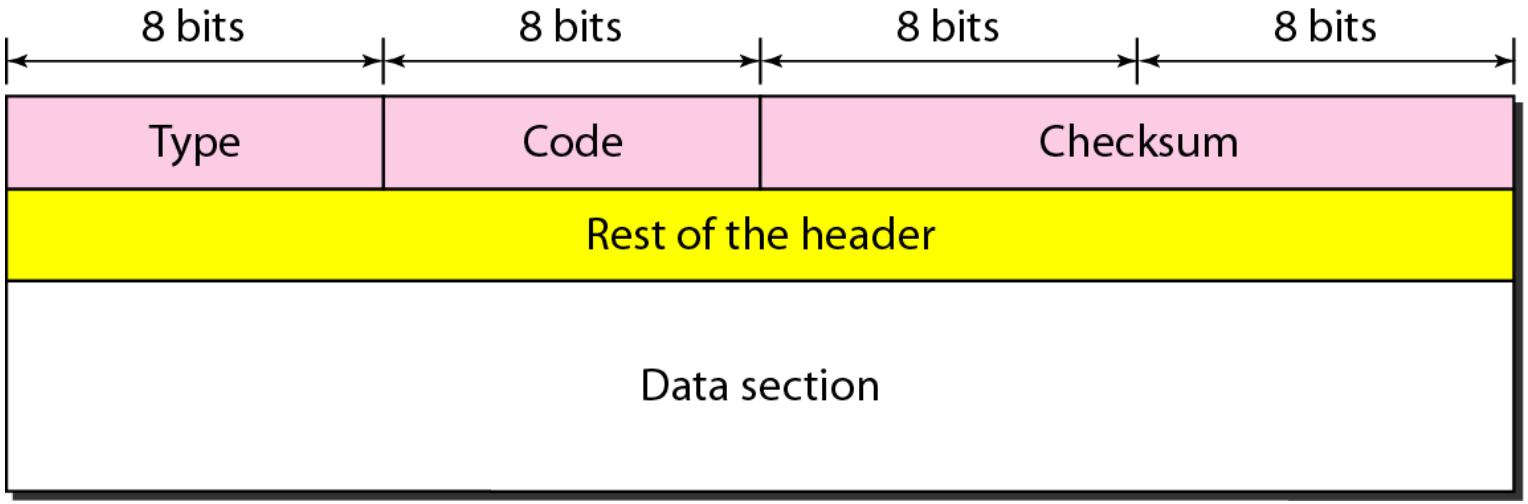
b. Client and server on different networks

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

21-2 ICMP

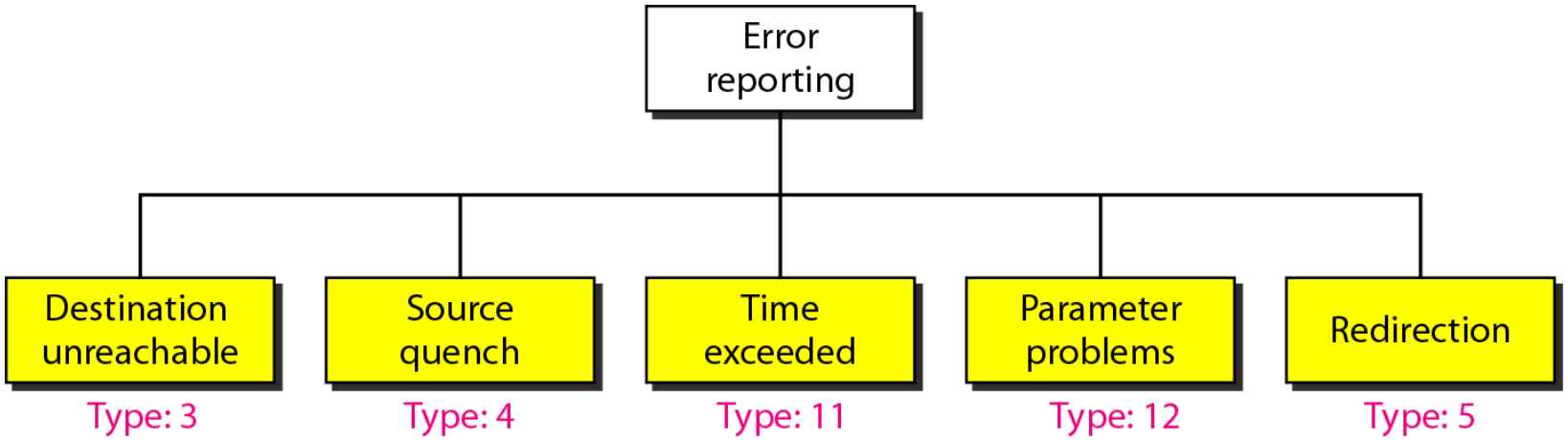
The IP protocol has no error-reporting or error-correcting mechanism. The IP protocol also lacks a mechanism for host and management queries. The ***Internet Control Message Protocol (ICMP)*** *has been designed to compensate for the above two deficiencies. It is a companion to the IP protocol.*

Figure 21.8 *General format of ICMP messages*



ICMP always reports error messages to the original source.

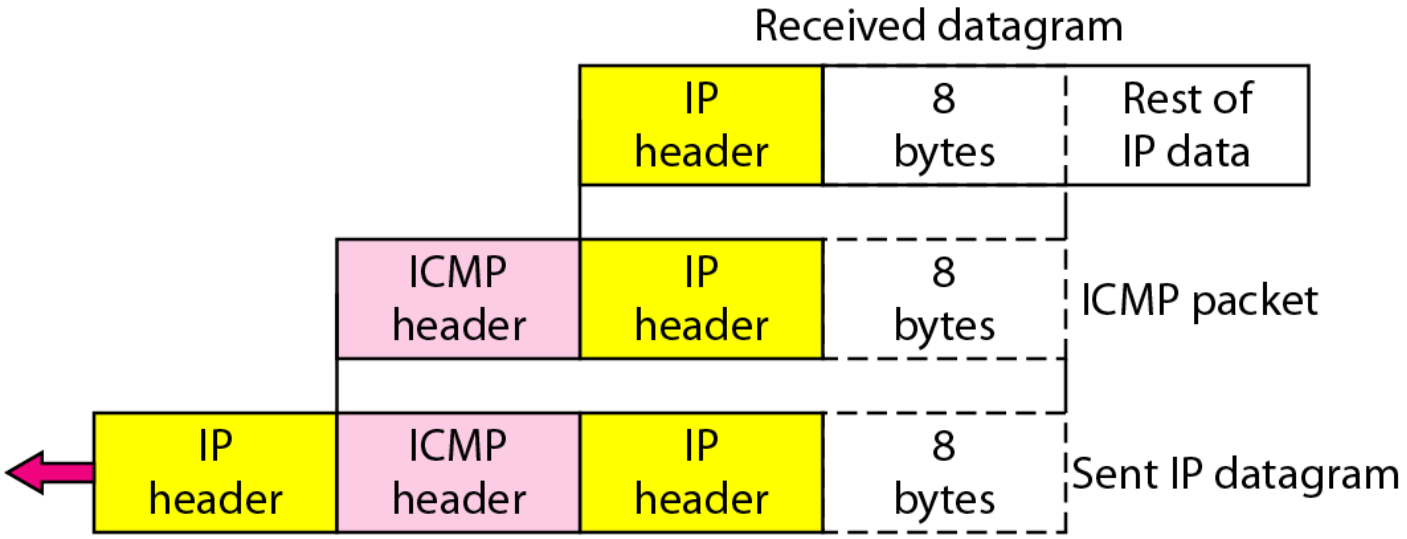
Figure 21.9 *Error-reporting messages*

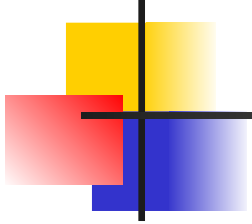


Important points about ICMP error messages:

- 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*





- Destination Unreachable
  When router cannot route/ host cannot deliver a datagram
- Source Quench
  Lack of flow control can cause congestion
- Time Exceeded
  TTL becomes zero
- Parameter Problem
  Some problem in the header of the datagram
- Redirection
  used when saved route changes in the host (because of updated route due to routing)

Figure 21.11 *Redirection concept*

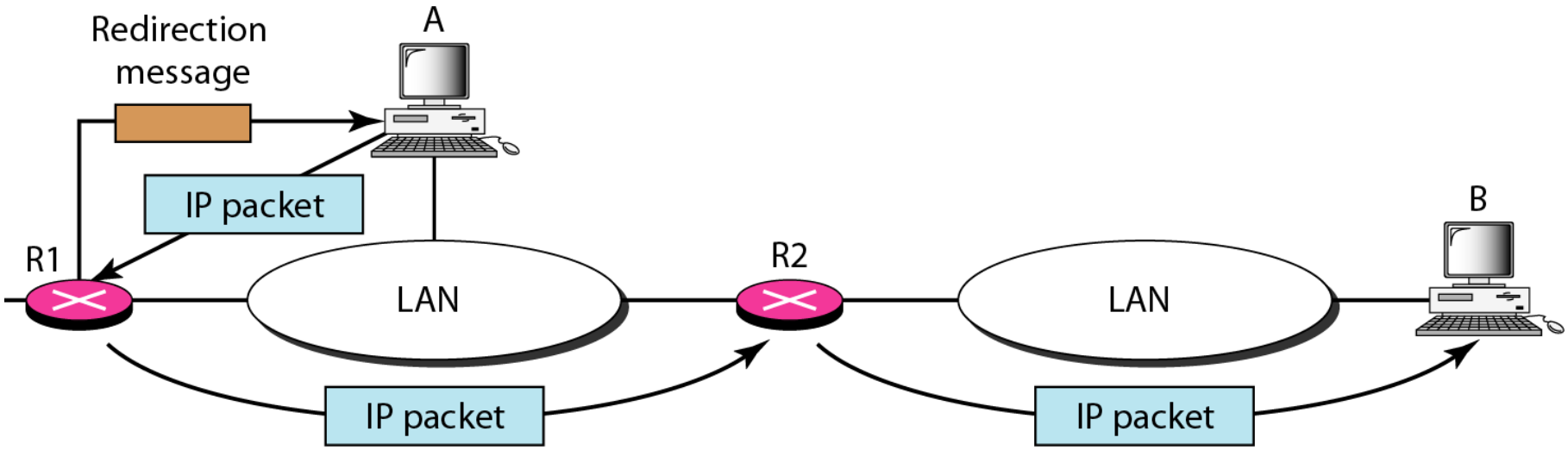
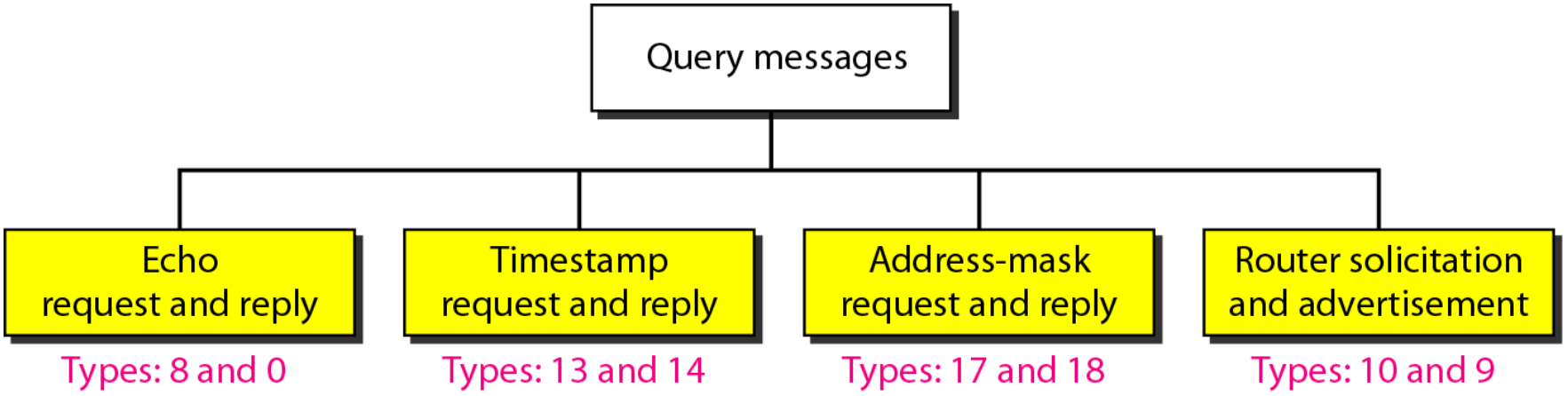
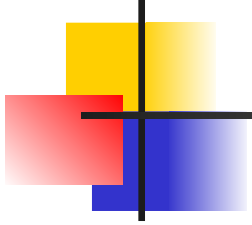


Figure 21.12 *Query messages*

- ICMP can also diagnose network problems





- Echo request and reply
  to diagnose and identify network problems, eg. Ping
- Timestamp request and reply
  to identify round trip time needed for a datagram
- Address-Mask request and reply
  for finding mask of its IP address from the router
- Router Solicitation and Advertisement
  - for finding whether a router is alive
  - it sends its information and also presence of all routers of which it is aware of

Figure 21.13 *Encapsulation of ICMP query messages*

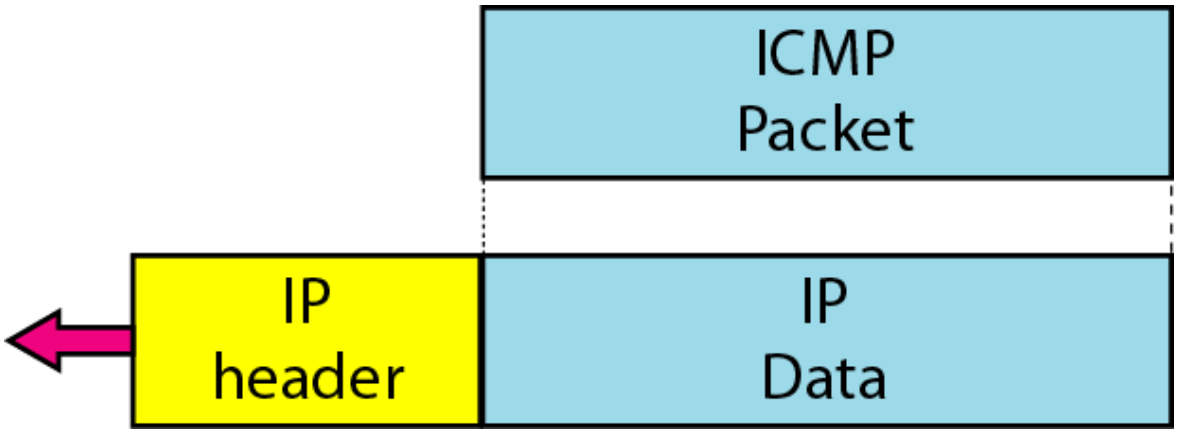
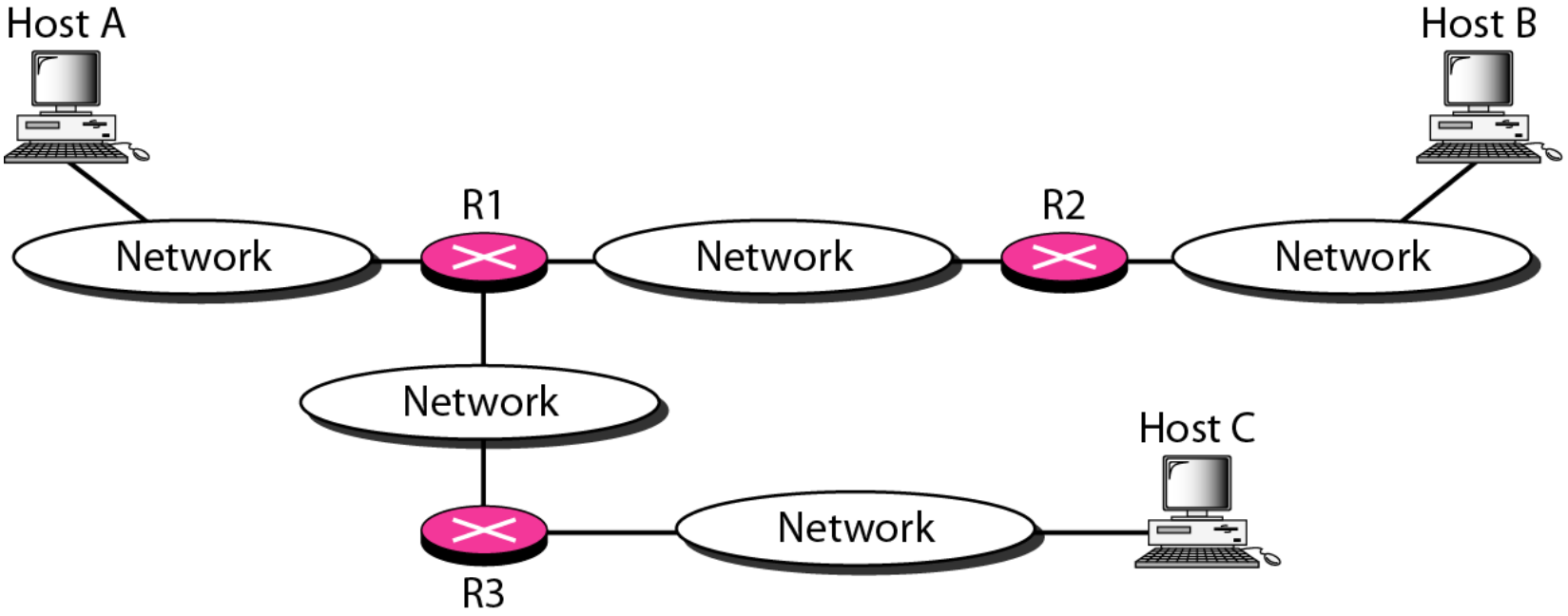


Figure 21.15 *The traceroute program operation*



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.

Group Management
IGMP Messages and IGMP Operation
Encapsulation
Netstat Utility

Figure 21.16 *IGMP message types*

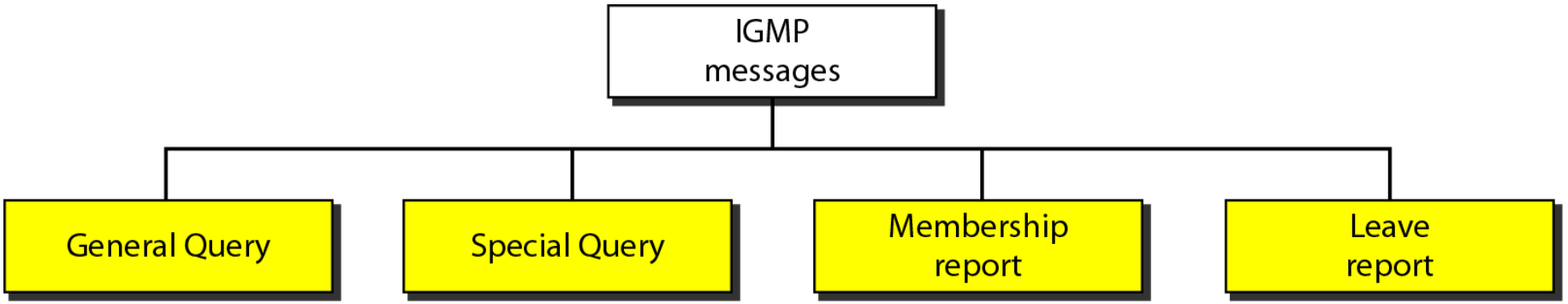


Figure 21.17 *IGMP message format*

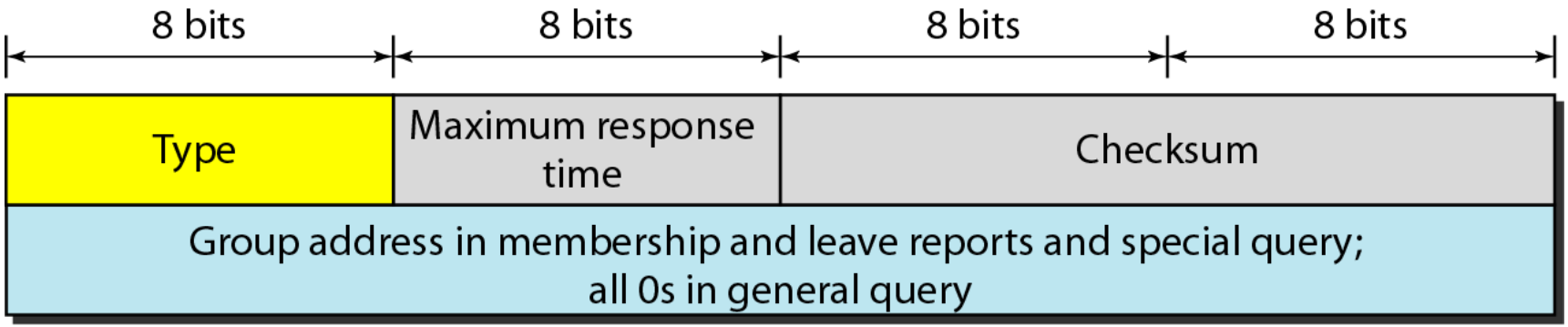
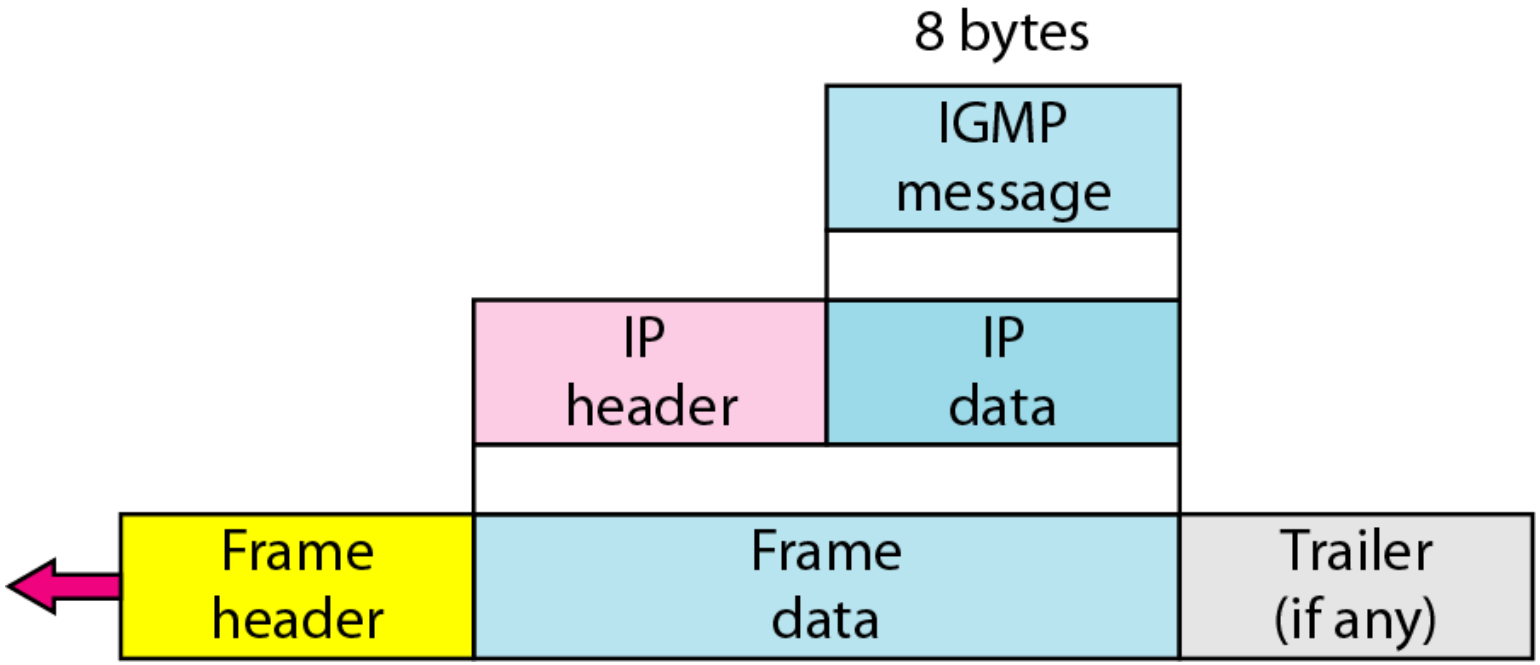


Figure 21.20 *Encapsulation of IGMP packet*



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.

Error Reporting
Query

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

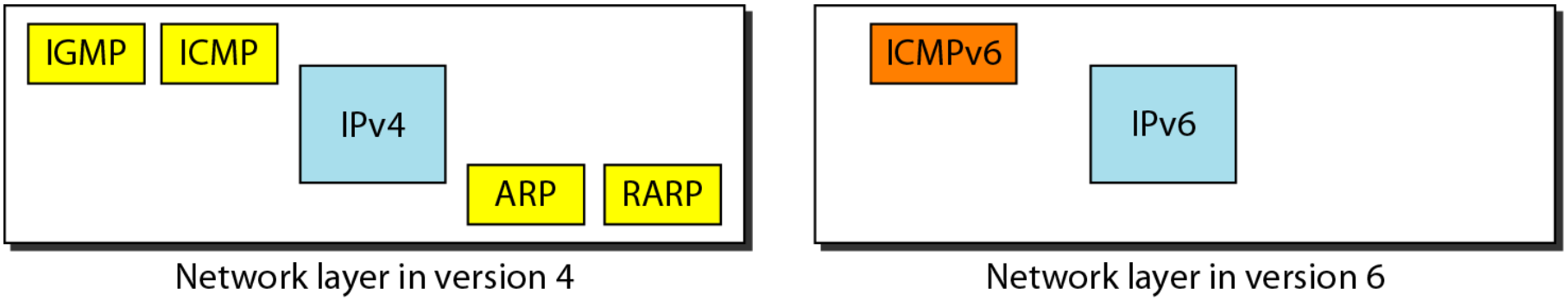


Table 21.3 ***Comparison of error-reporting messages in ICMPv4 and ICMPv6***

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