Computer Networks

By

Lt Col Ishtiaq Kiani

(10 Sep 12 to 12 Jan 13)

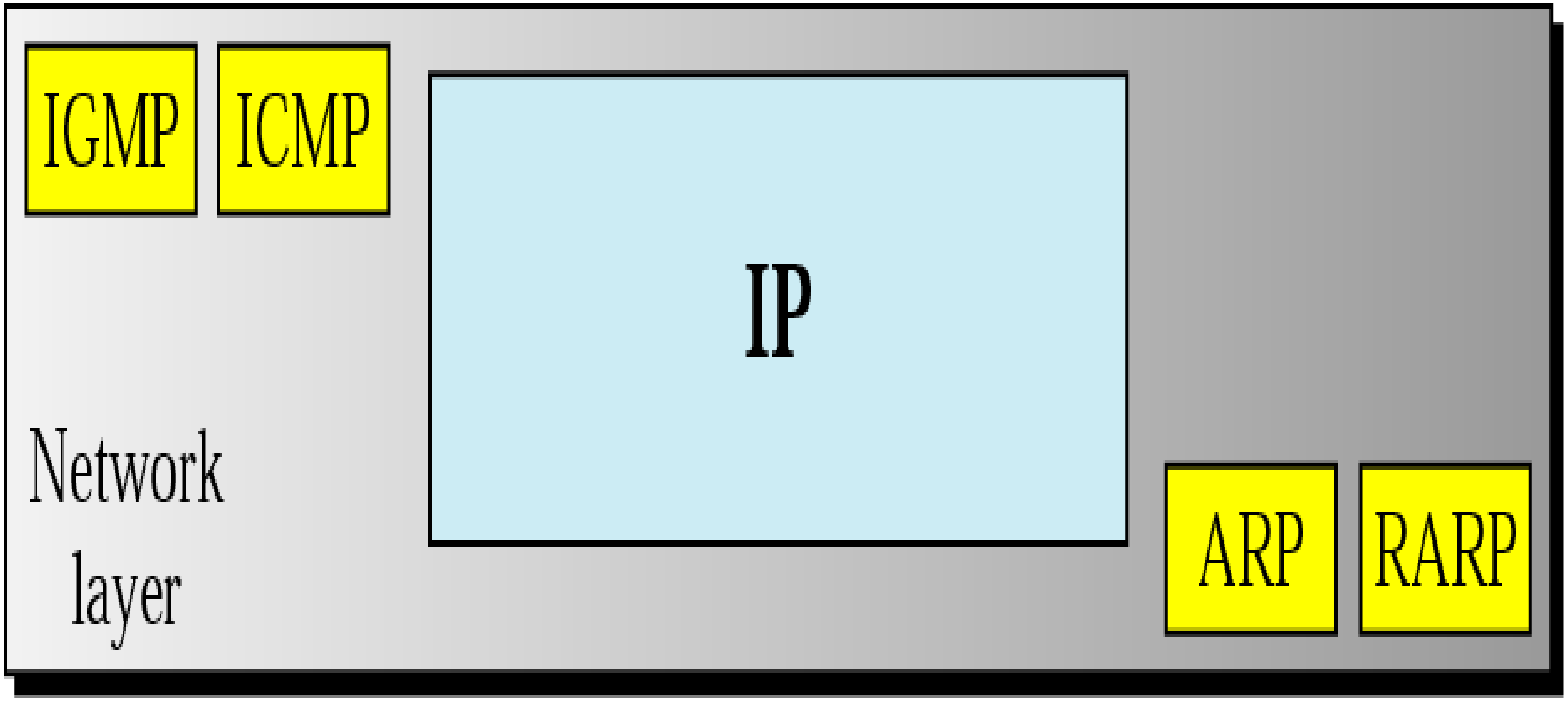
PART 4

Network Layer

Chapter 21
Network Layer – Address Mapping, Error Reporting and Multicasting

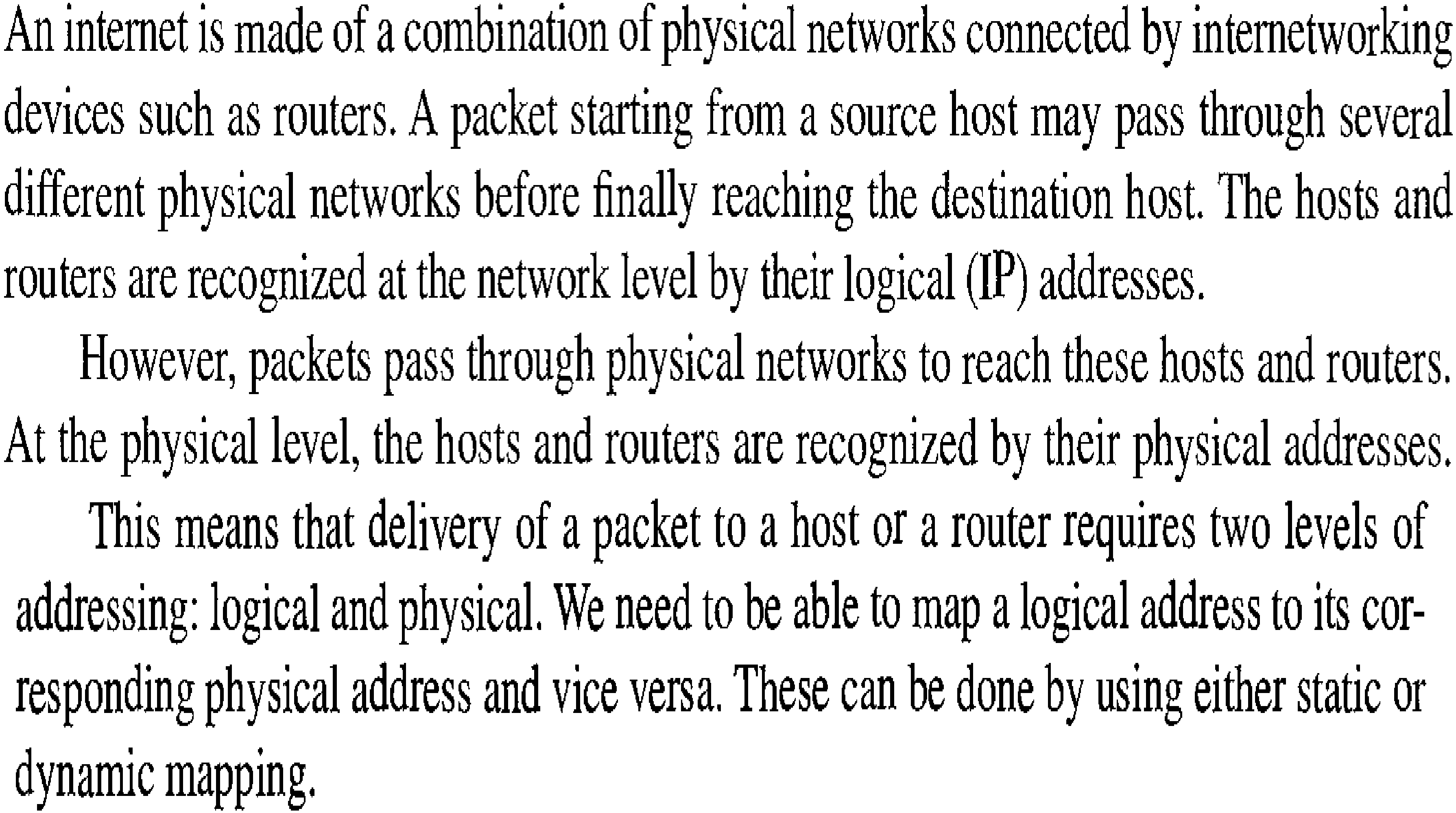
- **Address Mapping**
- **ICMP**
- **IGMP**
- **ICMPv6**

Network Layer Protocols



Address Mapping

Need of Mapping



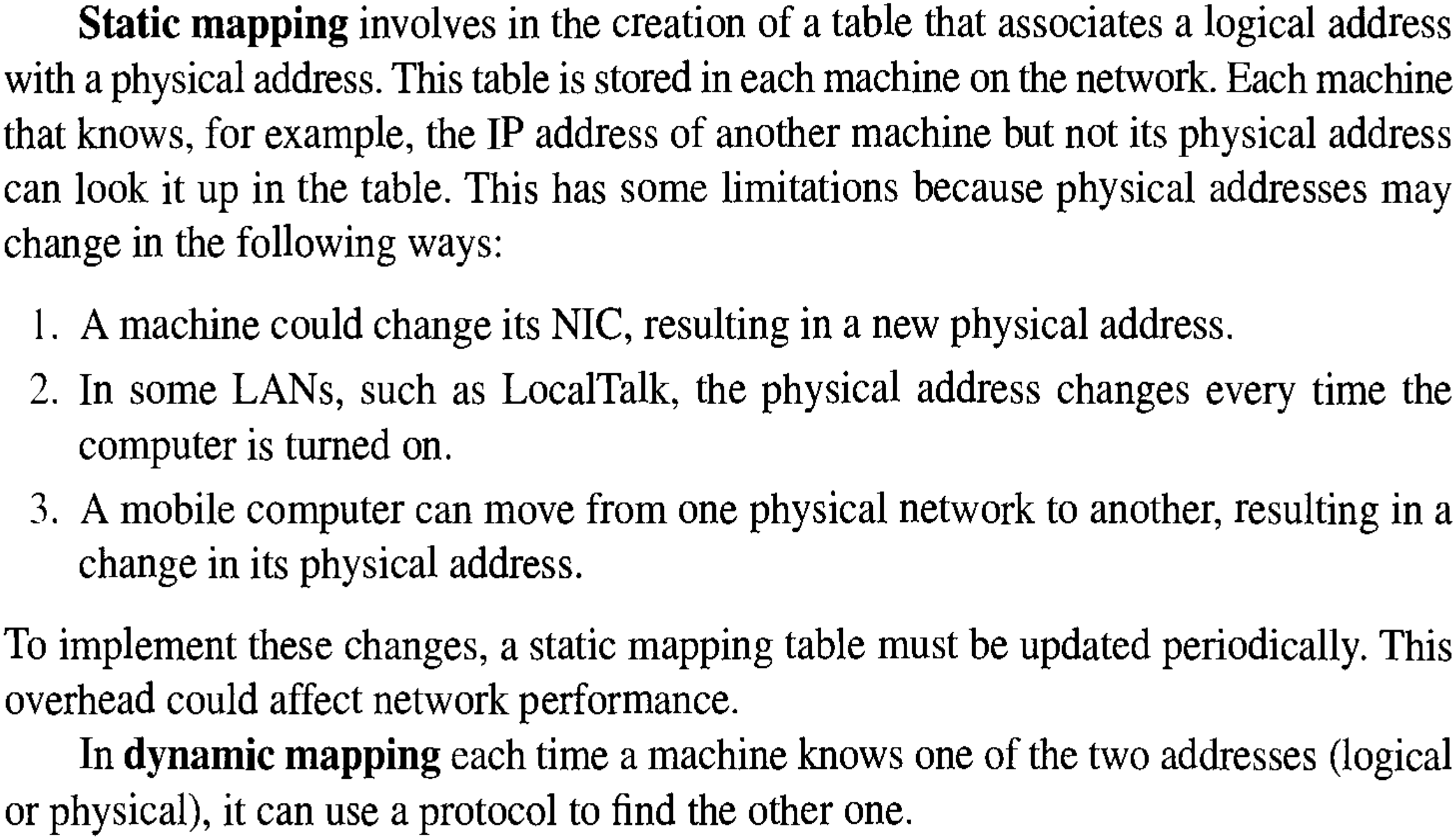
An internet is made of a combination of physical networks connected by internetworking devices such as routers. A packet starting from a source host may pass through several different physical networks before finally reaching the destination host. The hosts and routers are recognized at the network level by their logical (IP) addresses.

However, packets pass through physical networks to reach these hosts and routers. At the physical level, the hosts and routers are recognized by their physical addresses.

This means that 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. These can be done by using either static or dynamic mapping.

Address Mapping

Static 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 the following ways:

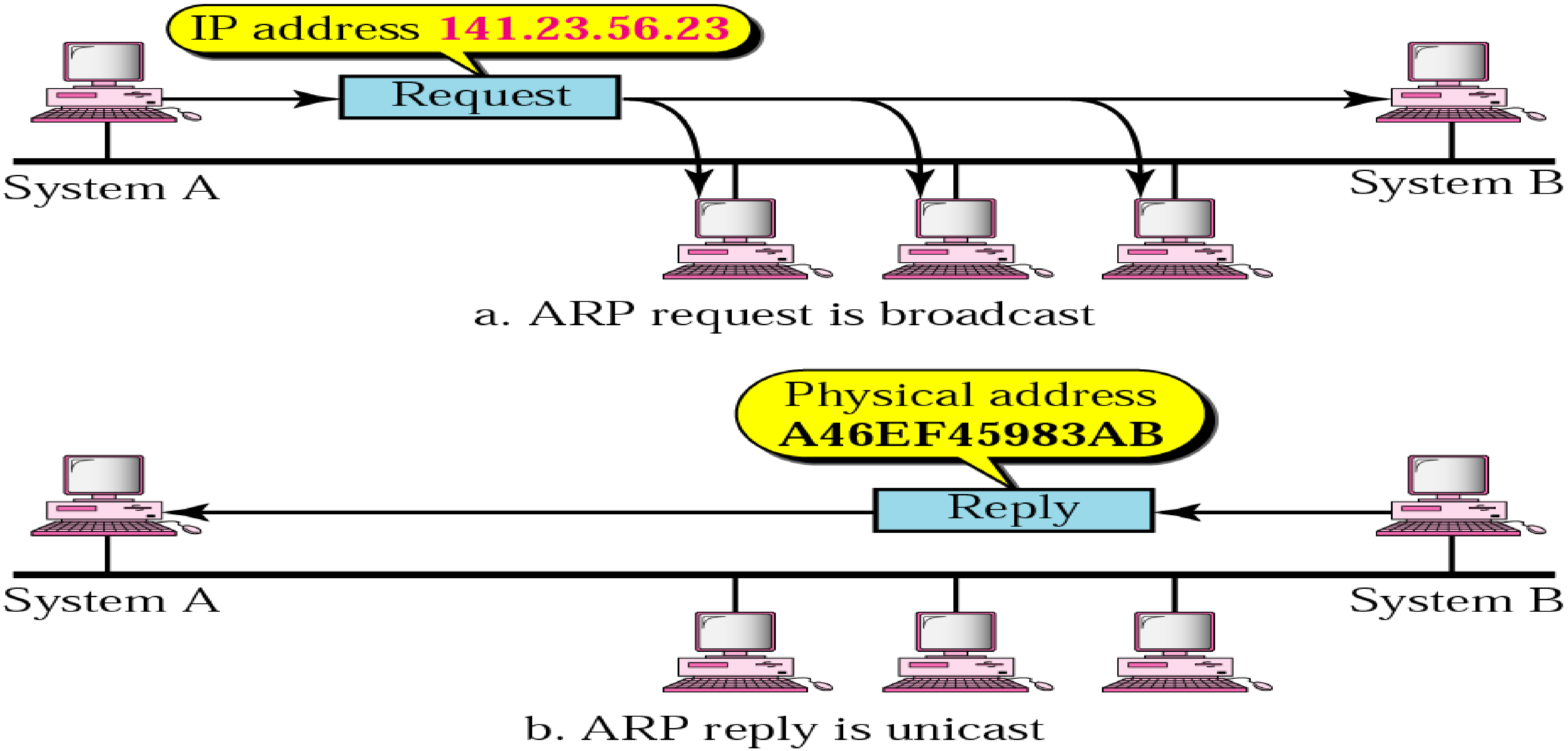
1. A machine could change its NIC, resulting in a new physical address.
2. In some LANs, such as LocalTalk, the physical address changes every time the computer is turned on.
3. A mobile computer can move from one physical network to another, resulting in a change in its physical address.

To implement these changes, a static mapping table must be updated periodically. This overhead could affect network performance.

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.

Address Mapping

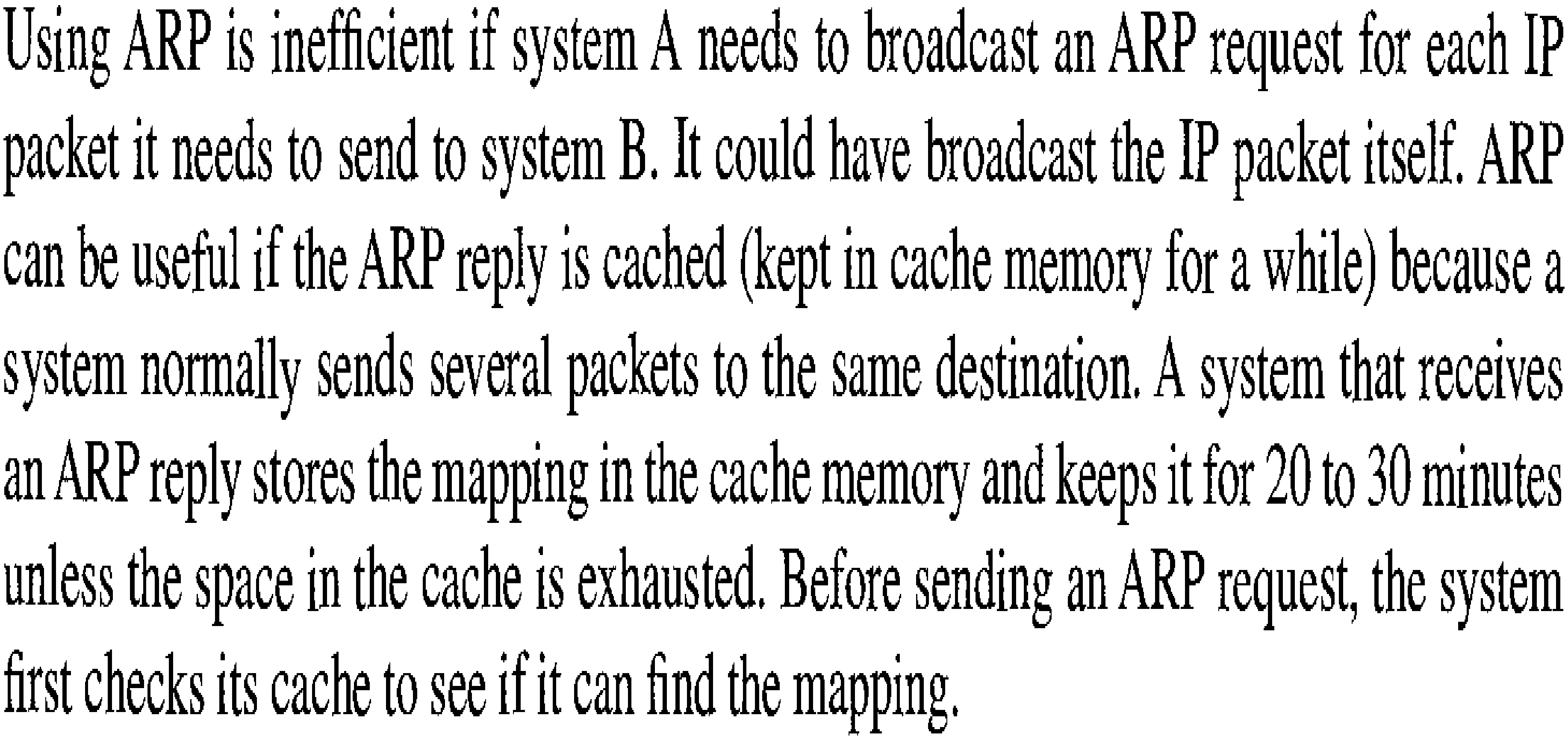
ARP – Mapping



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

Address Mapping

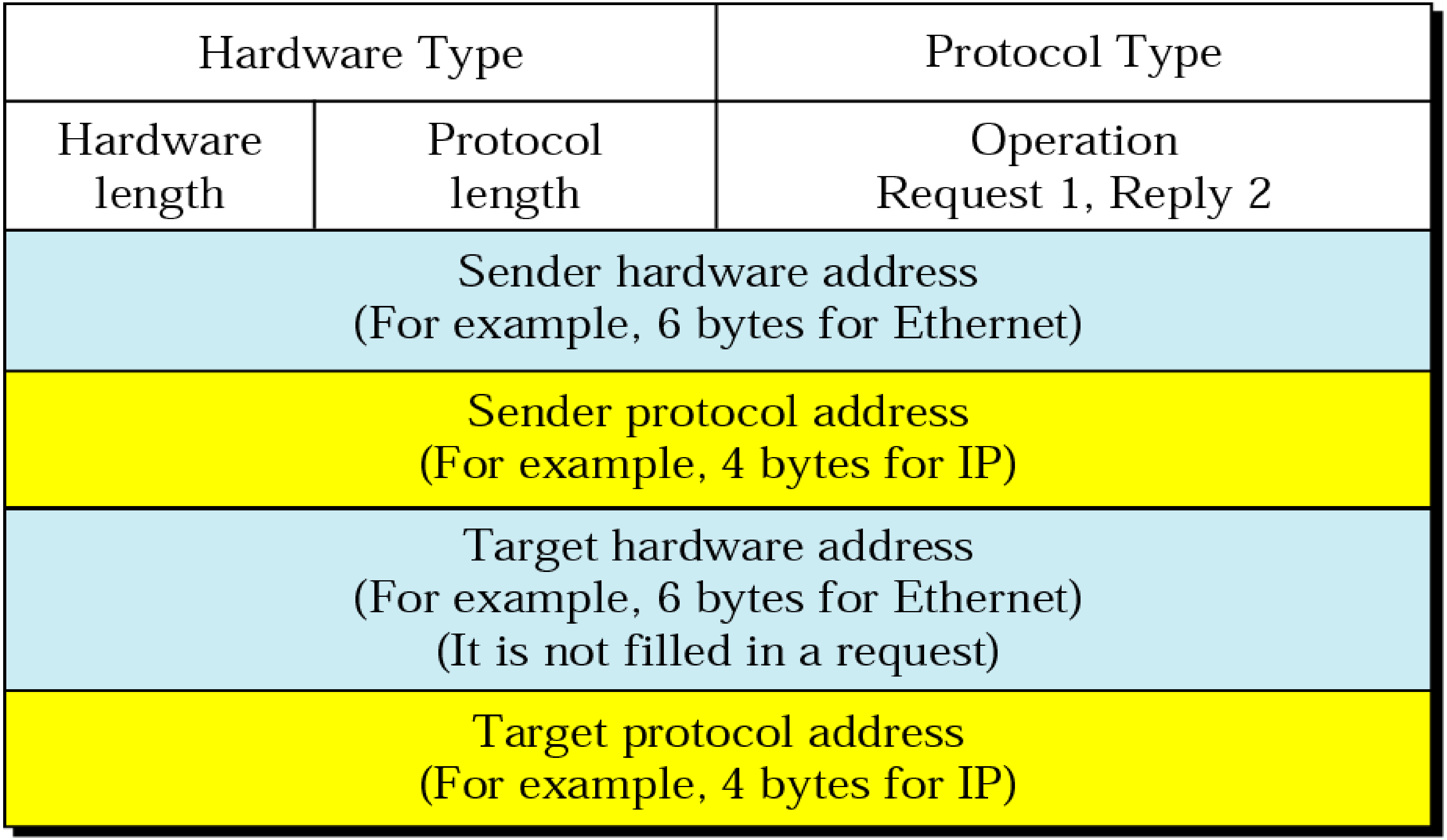
ARP – Cache Memory



Using ARP is inefficient if system A needs to broadcast an ARP request for each IP packet it needs to send to system B. It could have broadcast the IP packet itself. ARP can be useful if the ARP reply is cached (kept in cache memory for a while) because a system normally sends several packets to the same destination. A system that receives an ARP reply stores the mapping in the cache memory and keeps it for 20 to 30 minutes unless the space in the cache is exhausted. Before sending an ARP request, the system first checks its cache to see if it can find the mapping.

Address Mapping

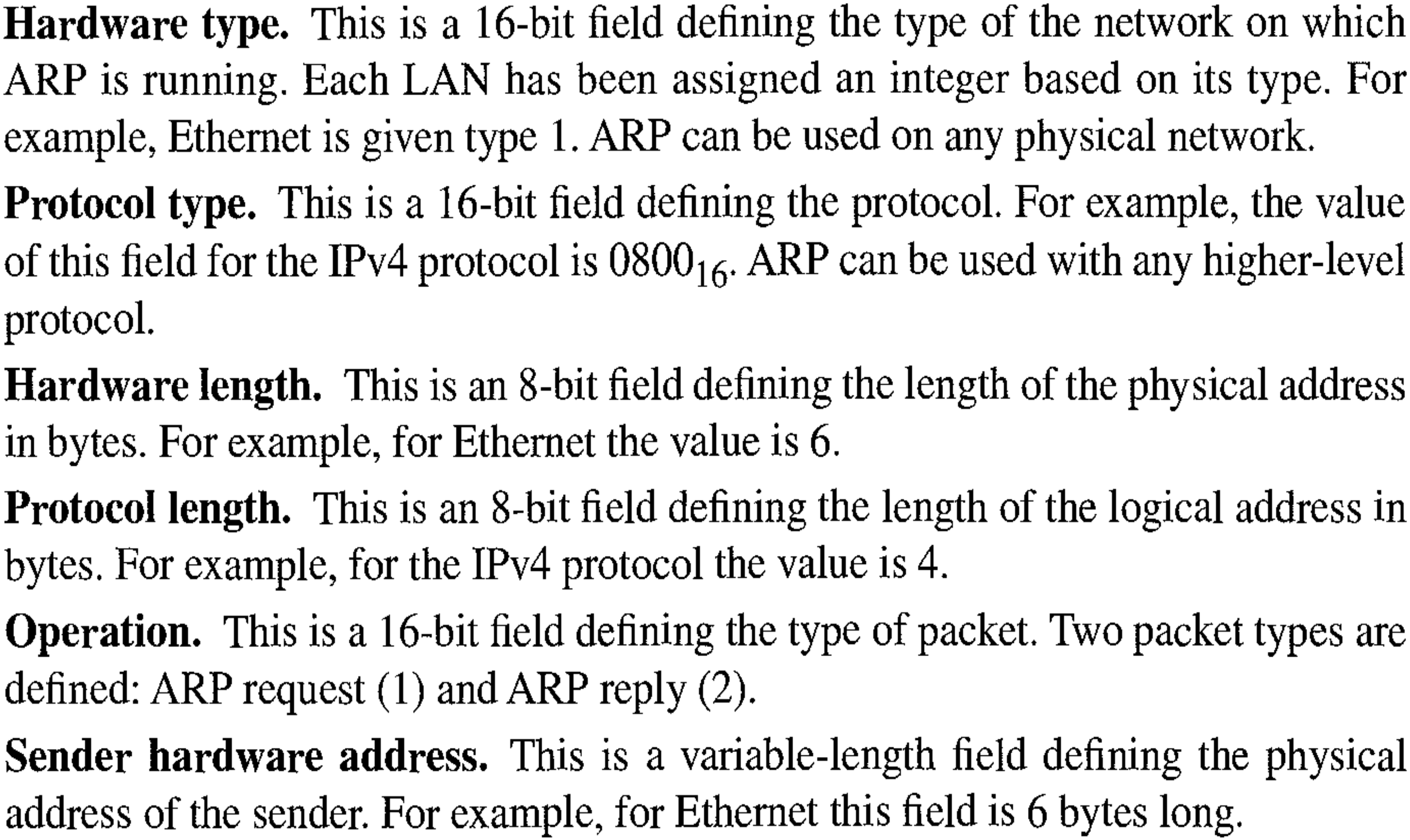
ARP – Packet Format



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)		

Address Mapping

ARP – Packet Format



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 0800_{16}. 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.

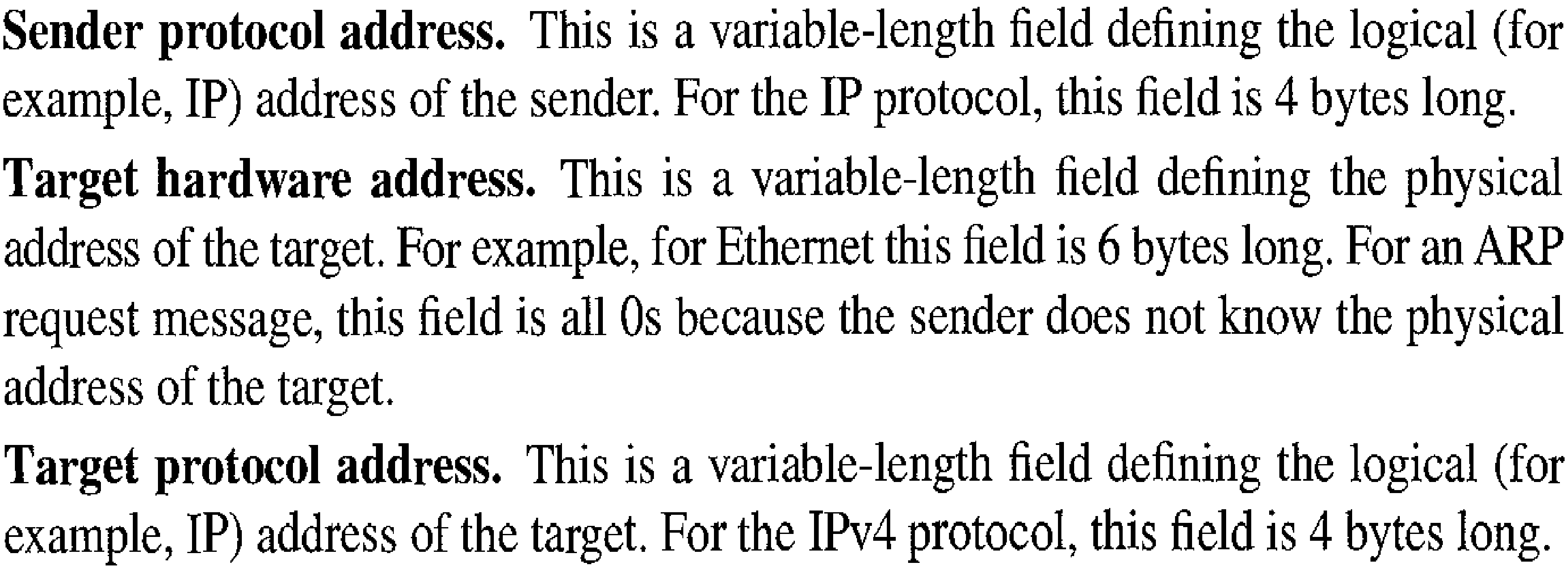
Protocol length. This is an 8-bit field defining the length of the logical address in bytes. For example, for the IPv4 protocol the value is 4.

Operation. This is a 16-bit field defining the type of packet. Two packet types are defined: ARP request (1) and ARP reply (2).

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.

Address Mapping

ARP – Packet Format



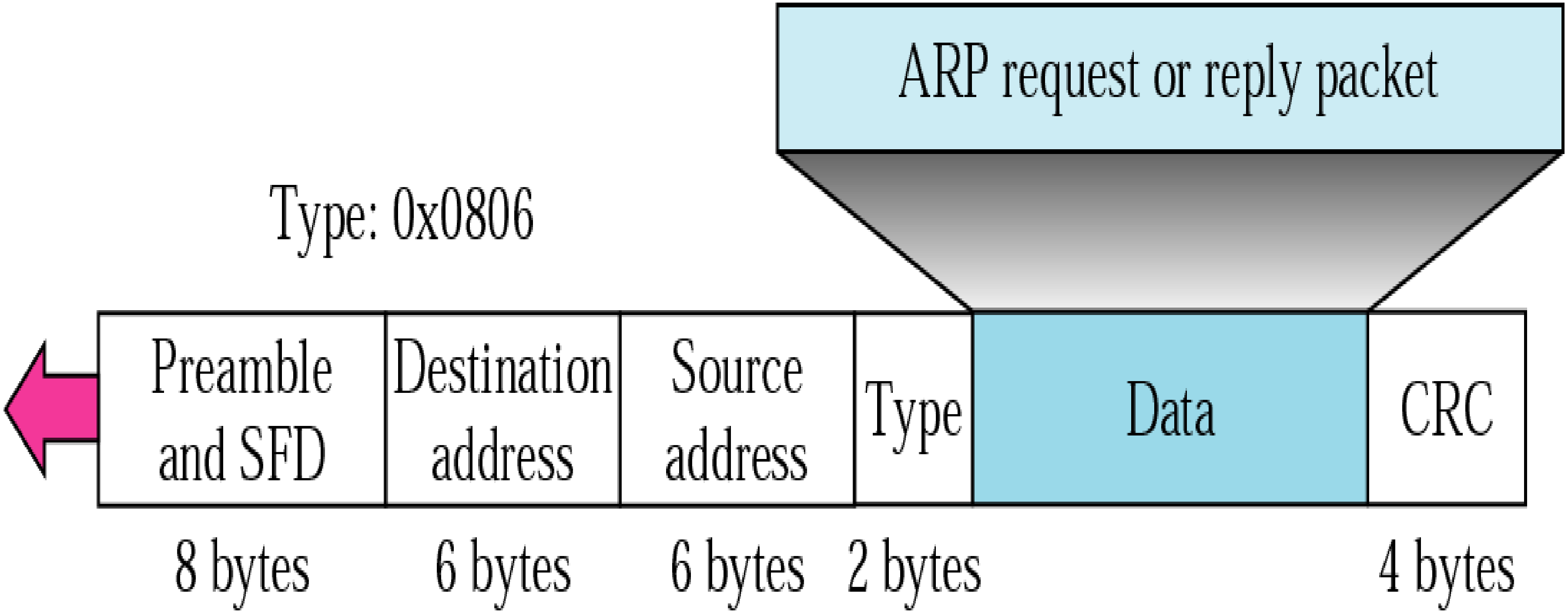
Sender protocol address. This is a variable-length field defining the logical (for example, IP) address of the sender. For the IP protocol, this field is 4 bytes long.

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 all 0s 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.

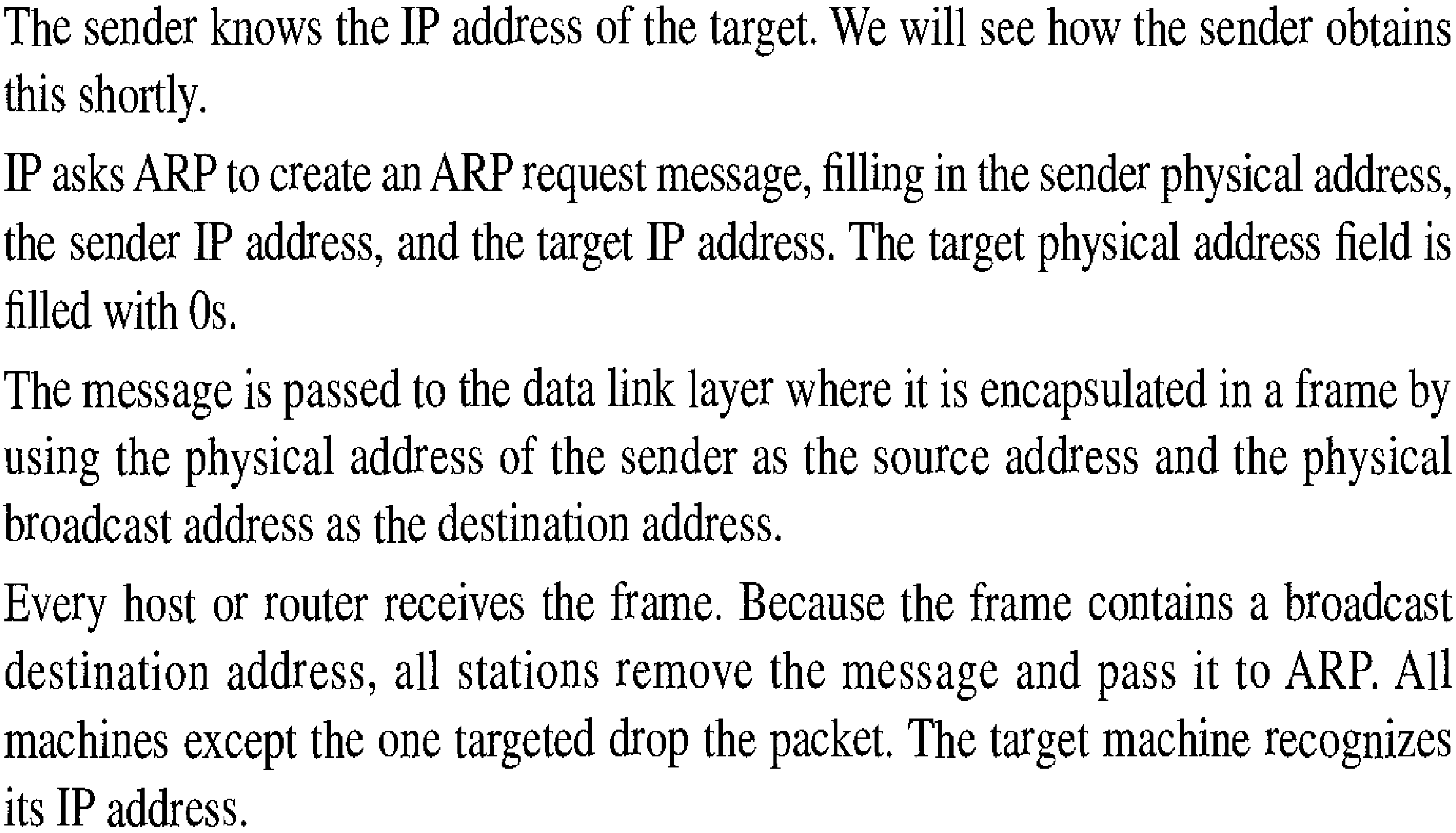
Address Mapping

ARP – Encapsulation



Address Mapping

ARP – Operation



The sender knows the IP address of the target. We will see how the sender obtains this shortly.

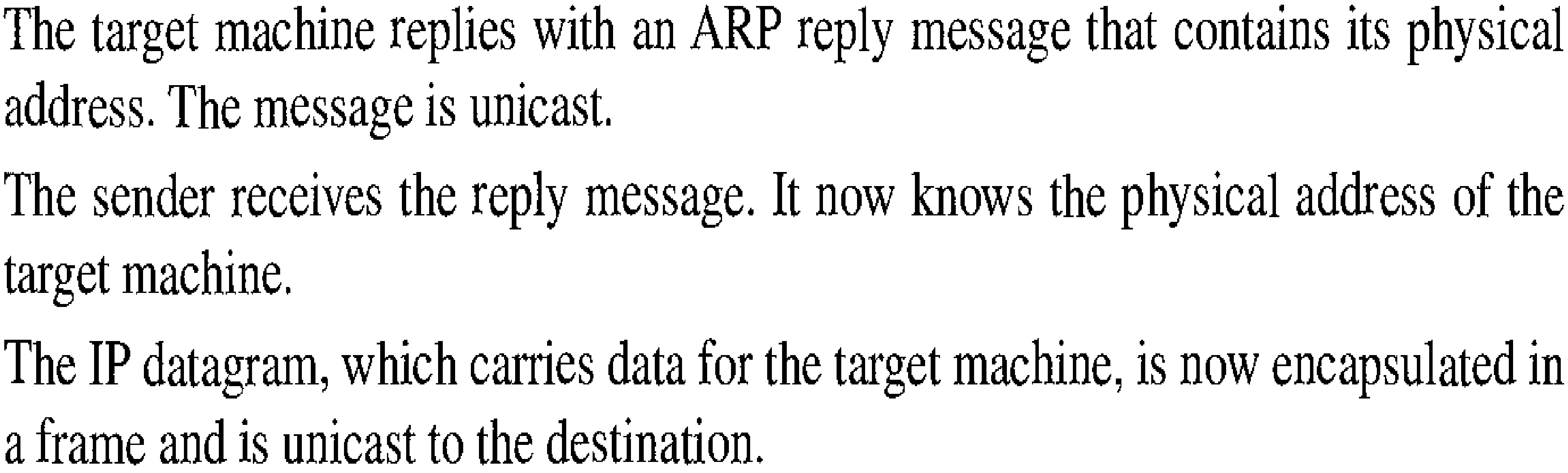
IP asks ARP to create an ARP request message, filling in the sender physical address, the sender IP address, and the target IP address. The target physical address field is filled with 0s.

The message is passed to the data link layer where it is encapsulated in a frame by using the 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. Because the frame contains a broadcast destination address, all stations remove the message and pass it to ARP. All machines except the one targeted drop the packet. The target machine recognizes its IP address.

Address Mapping

ARP – Operation



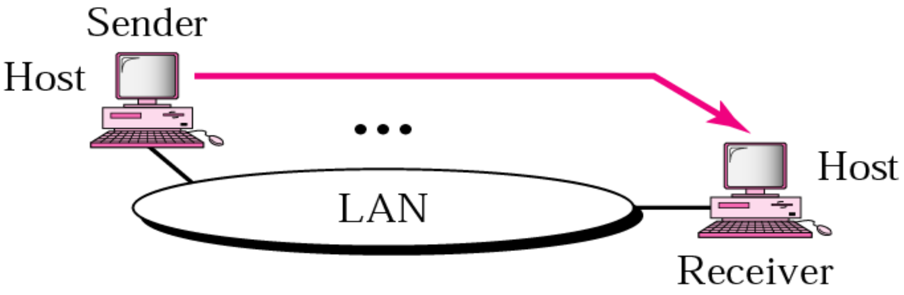
The target machine replies with an ARP reply message that contains its physical address. The message is unicast.

The sender receives the reply message. It now knows the physical address of the target machine.

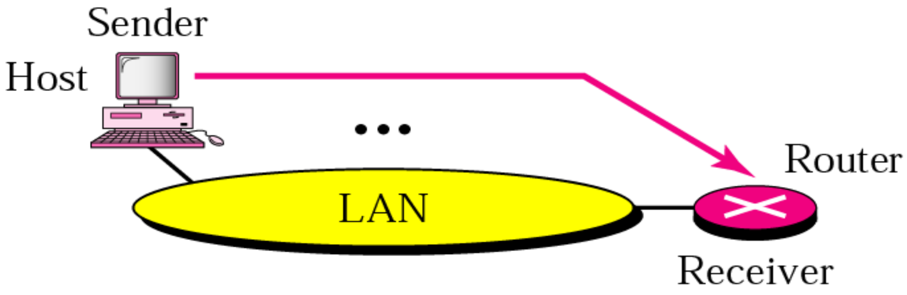
The IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.

Address Mapping

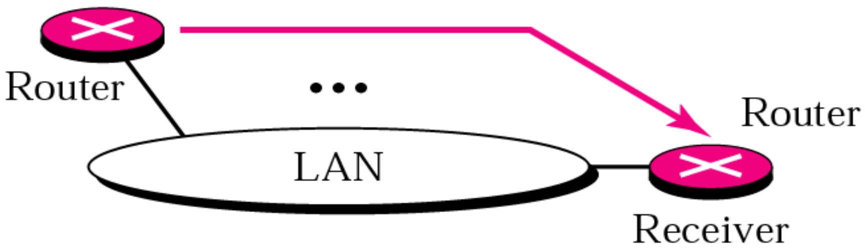
ARP – Four Cases



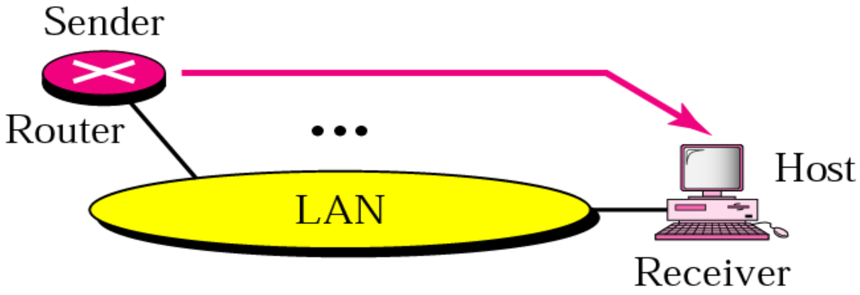
Case 1. A host has a packet to send to another host on the same network.



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

Address Mapping

ARP – Example

Example

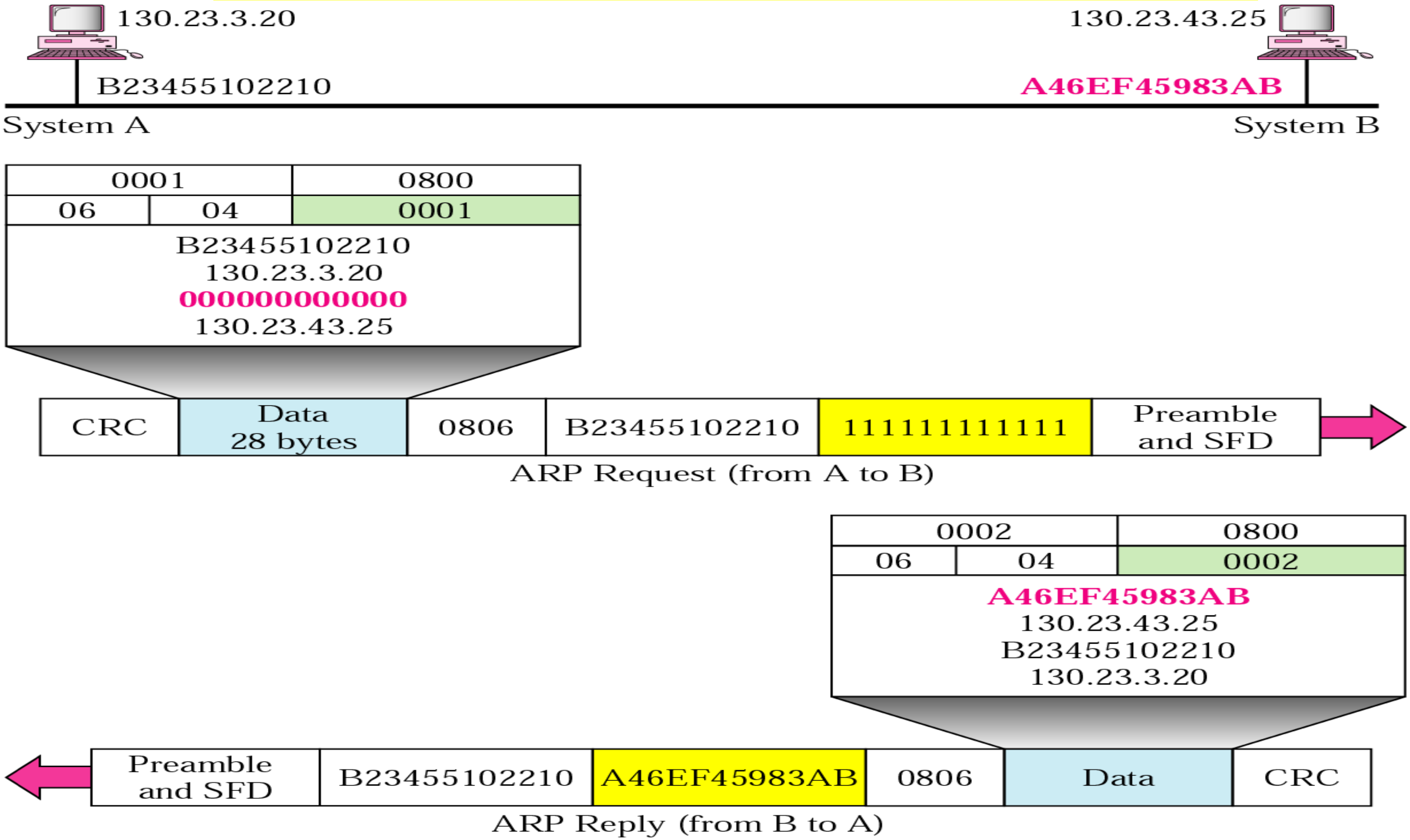
A host with IP address 130.23.3.20 and physical address B23455102210 has a packet to send to another host with IP address 130.23.43.25 and physical address A46EF45983AB. The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.

Solution

Figure 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. Note that we use hexadecimal for every field except the IP addresses.

Address Mapping

ARP – Example



130.23.3.20

B23455102210

System A

130.23.43.25

A46EF45983AB

System B

0001 | 0800

06 | 04 | 0001

B23455102210

130.23.3.20

000000000000

130.23.43.25

CRC | Data 28 bytes | 0806 | B23455102210 | 111111111111 | Preamble and SFD

ARP Request (from A to B)

0002 | 0800

06 | 04 | 0002

A46EF45983AB

130.23.43.25

B23455102210

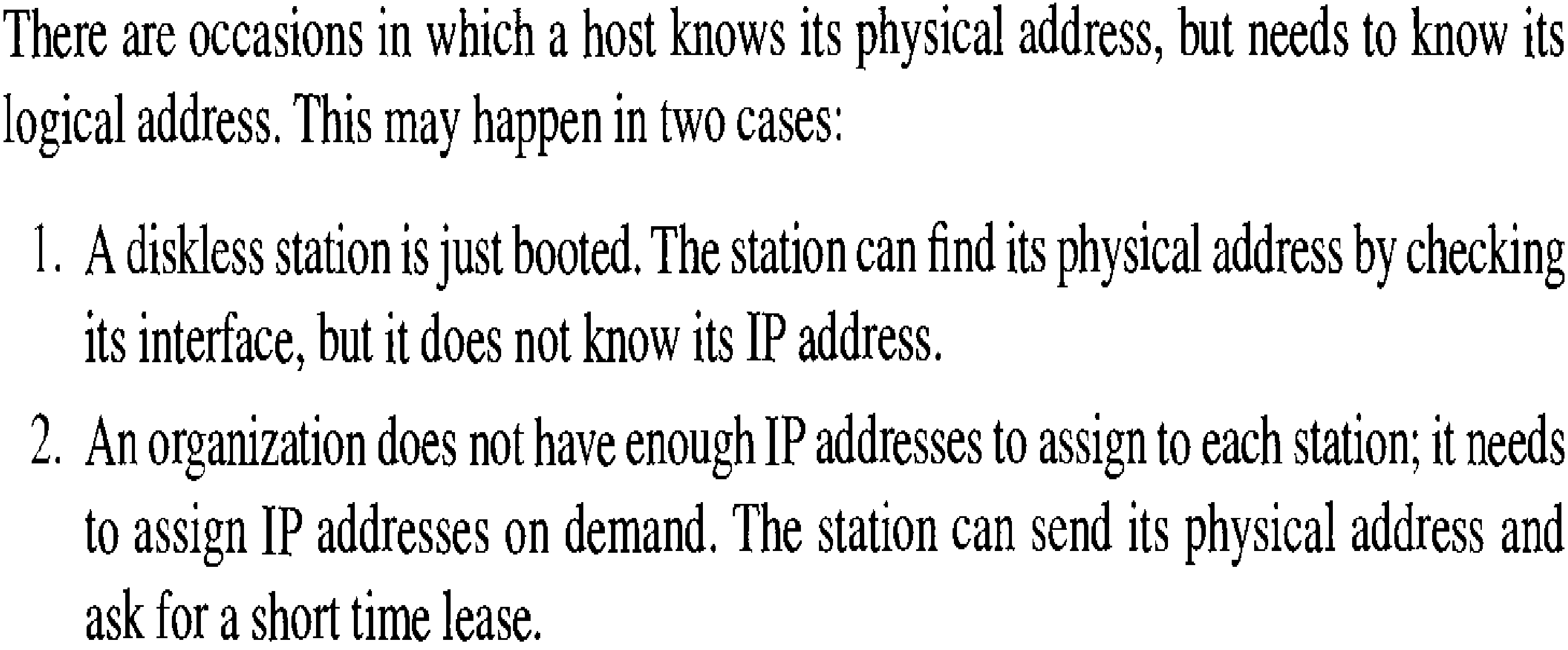
130.23.3.20

Preamble and SFD | B23455102210 | A46EF45983AB | 0806 | Data | CRC

ARP Reply (from B to A)

Address Mapping

Mapping Physical to Logical Addresses

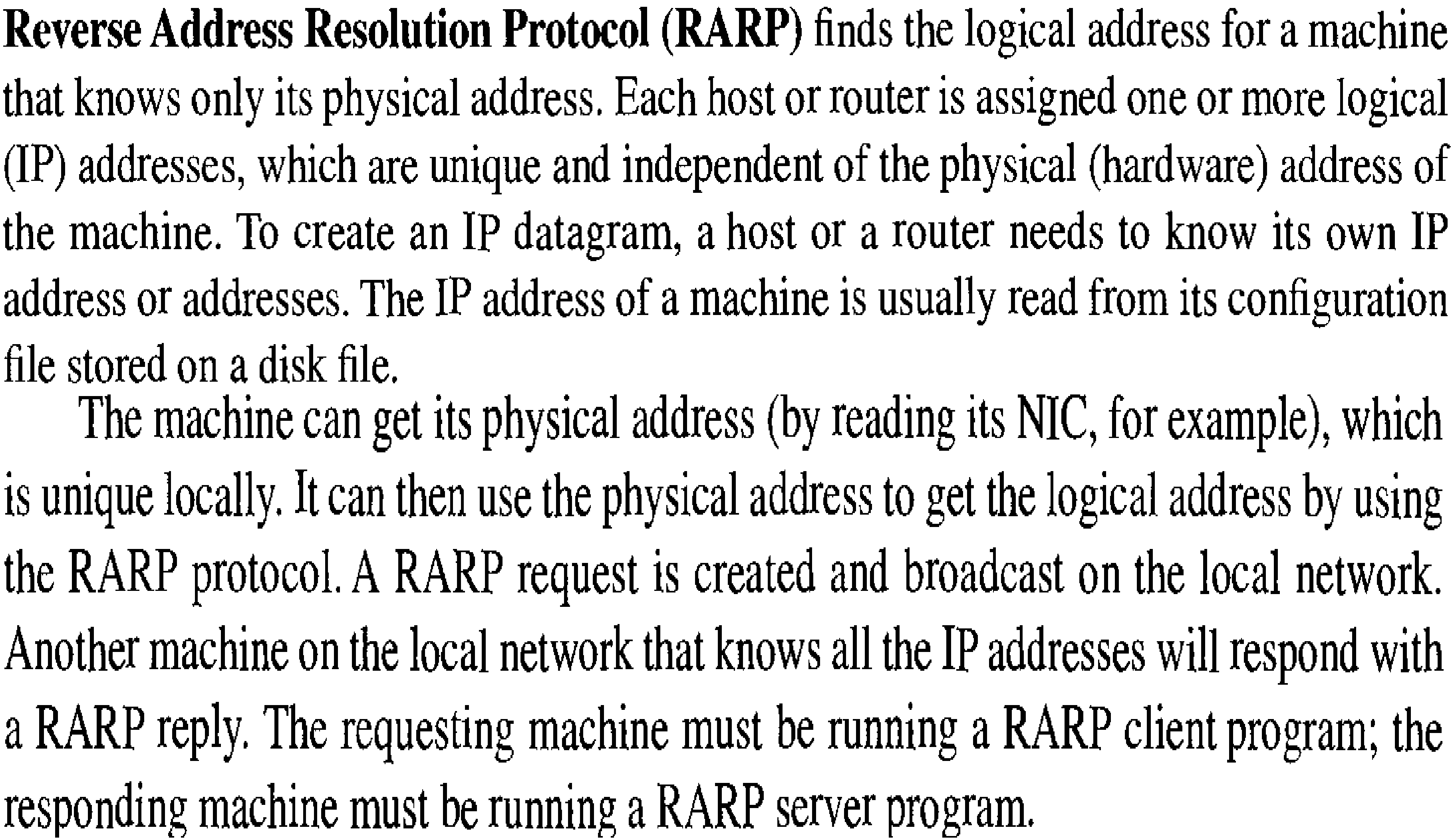


There are occasions in which a host knows its physical address, but needs to know its logical address. This may happen in two cases:

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.

Address Mapping

Mapping Physical to Logical Addresses



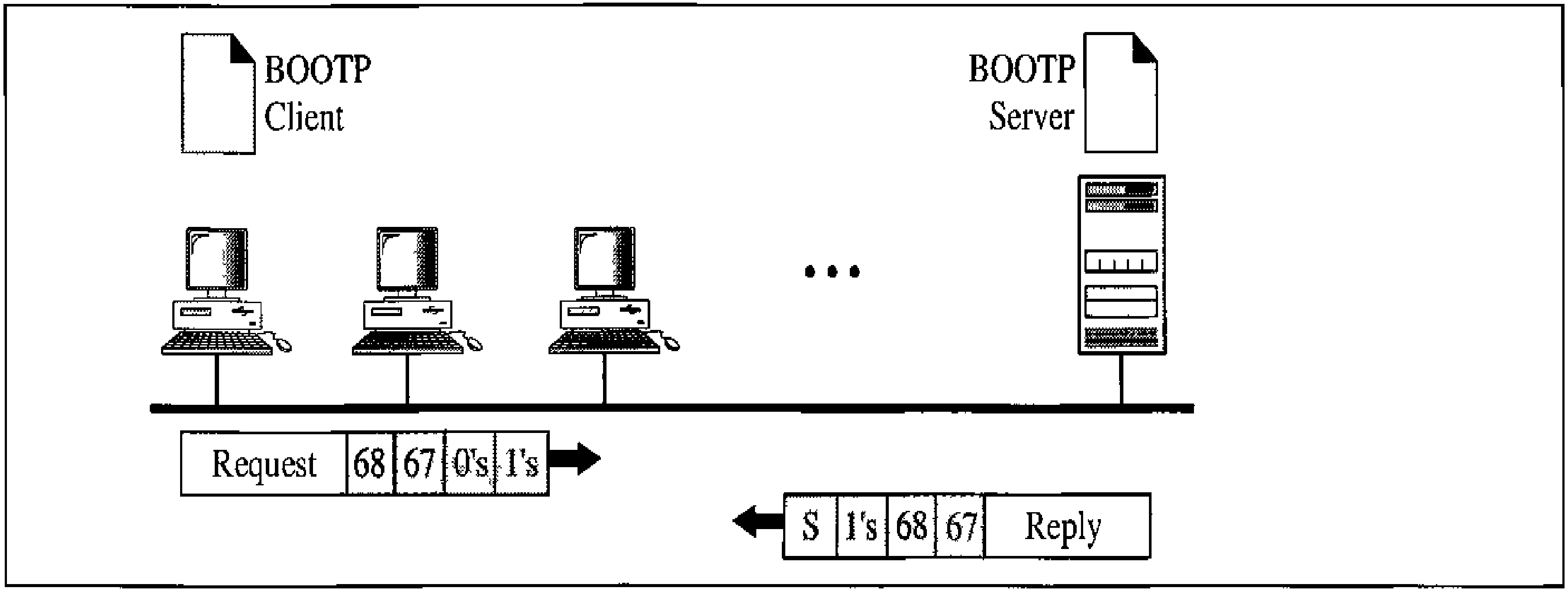
Reverse Address Resolution Protocol (RARP) finds the logical address for a machine that knows only its physical address. Each host or router is assigned one or more logical (IP) addresses, which are unique and independent of the physical (hardware) address of the machine. To create an IP datagram, a 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.

Address Mapping

Mapping Physical to Logical Addresses

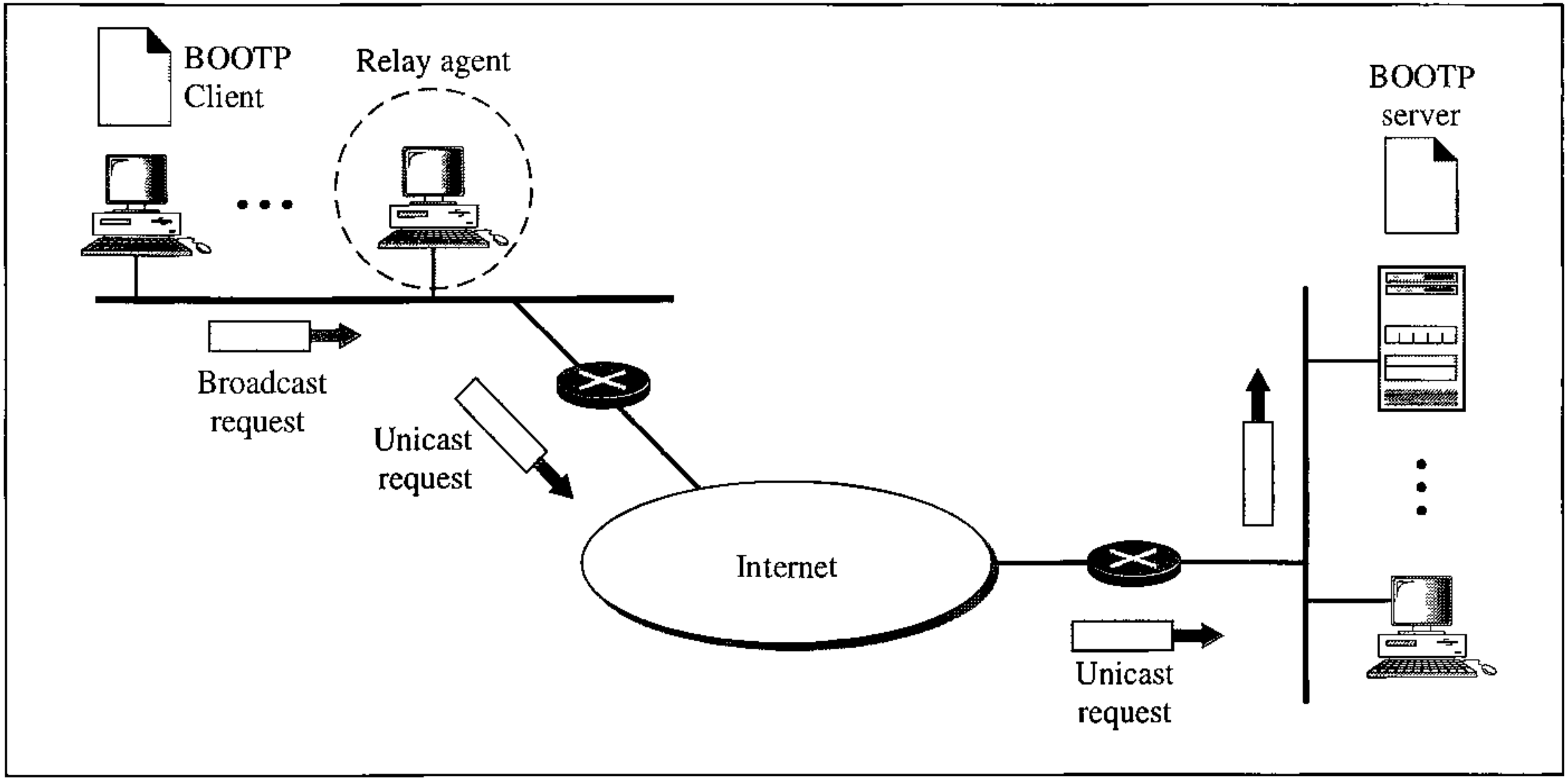
The **Bootstrap Protocol (BOOTP)** is a client/server protocol designed to provide physical address to logical address mapping. BOOTP is an application layer protocol. The administrator may put the client and the server on the same network or on different networks,



a. Client and server on the same network

Address Mapping

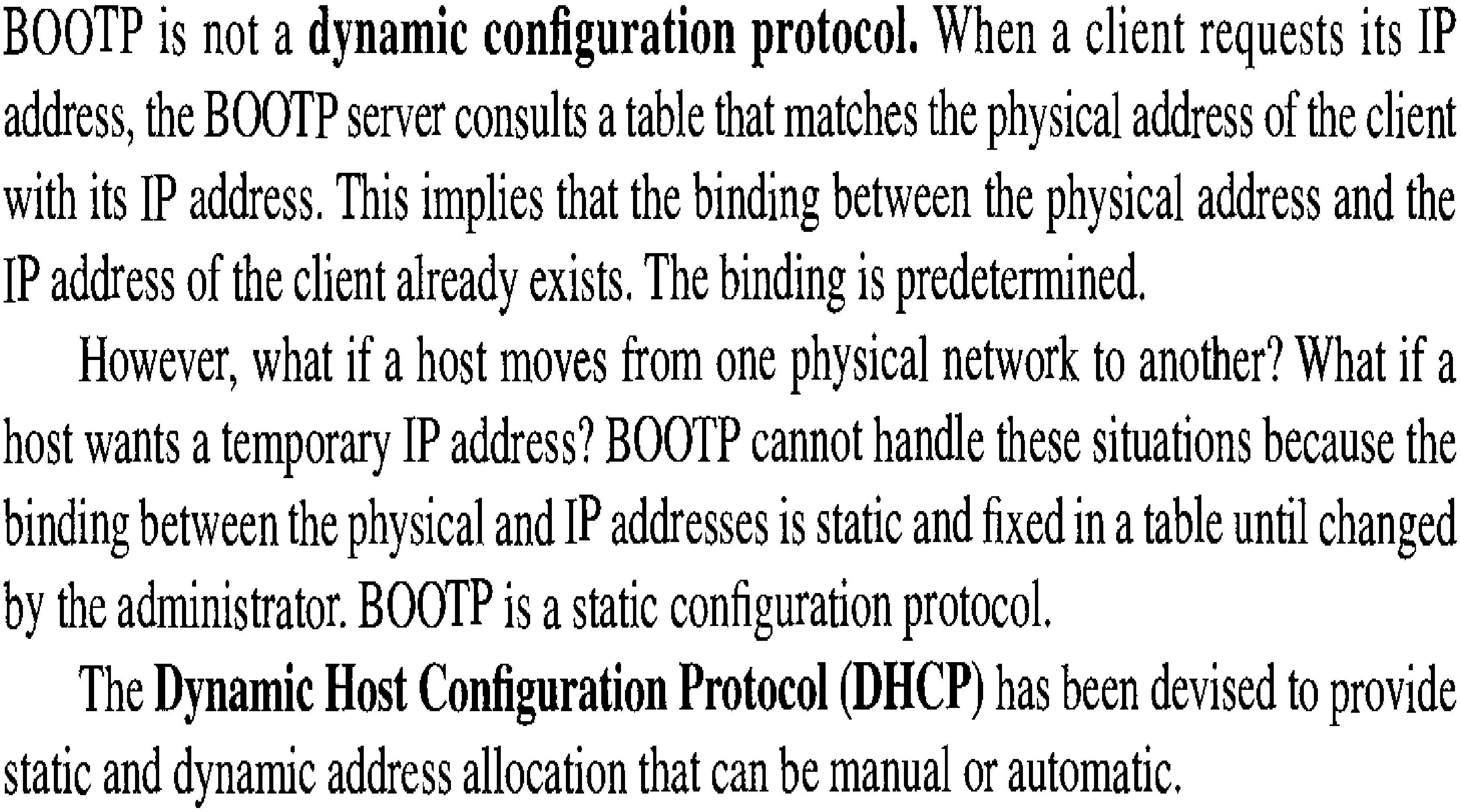
Mapping Physical to Logical Addresses



b. Client and server on different networks

Address Mapping

Mapping Physical to Logical Addresses



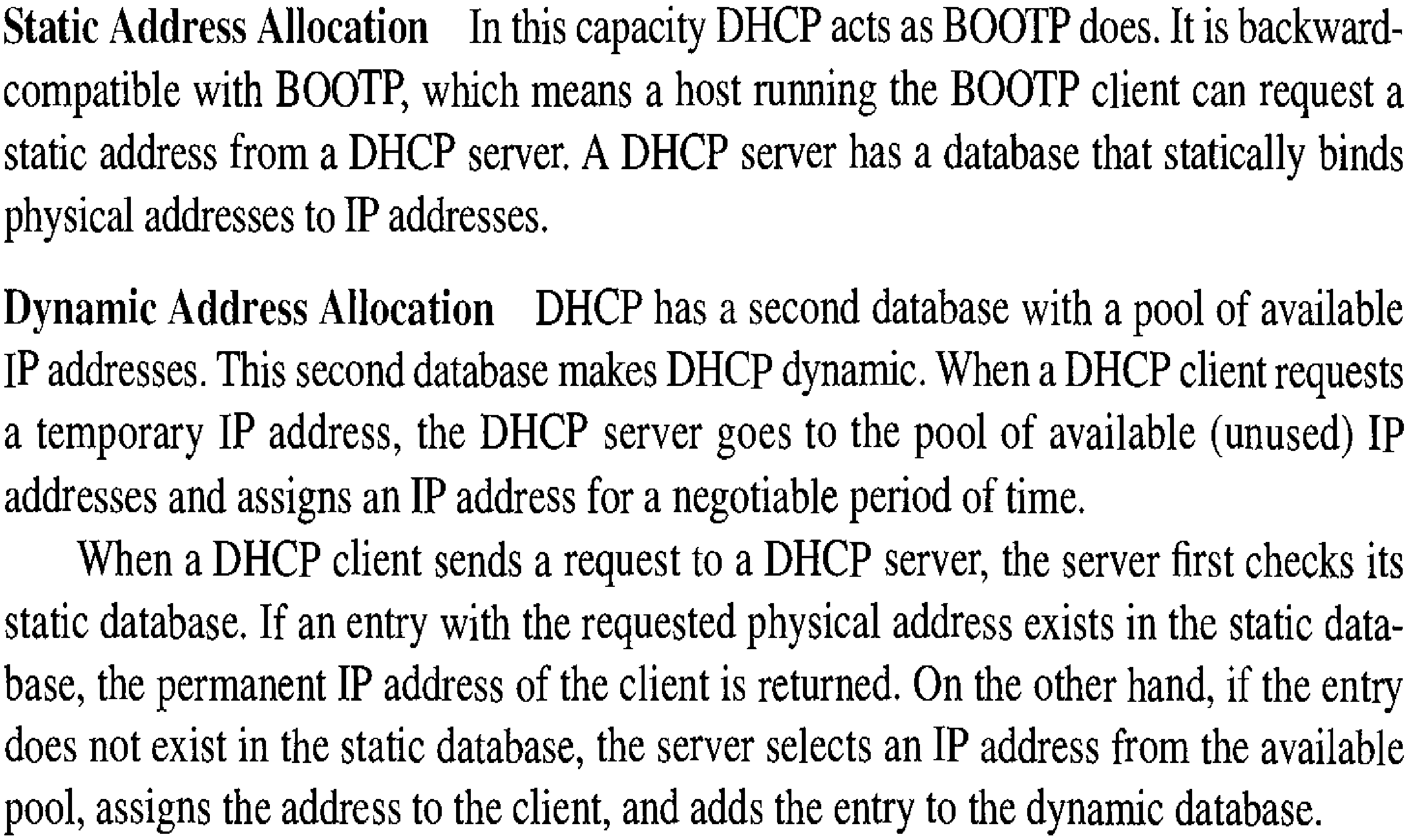
BOOTP is not a **dynamic configuration protocol.** When a client requests its IP address, the BOOTP server consults a table that matches the physical address of the client with its IP address. This implies that the binding between the physical address and the IP address of the client already exists. The binding is predetermined.

However, what if a host moves from one physical network to another? What if a host wants a temporary IP address? BOOTP cannot handle these situations because the binding between the physical and IP addresses is static and fixed in a table until changed by the administrator. 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.

Address Mapping

Mapping Physical to Logical Addresses



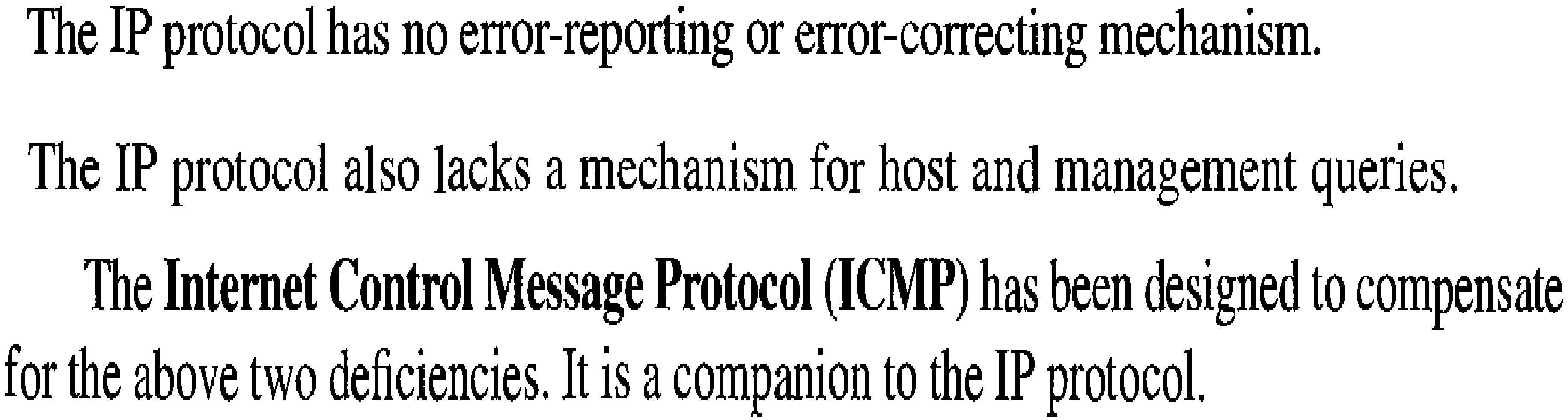
Static Address Allocation In this capacity DHCP acts as BOOTP does. It is backward-compatible with BOOTP, which means a host running the BOOTP client can request a static address from a DHCP server. A DHCP server has a database that statically binds physical addresses to IP addresses.

Dynamic Address Allocation DHCP has a second database with a pool of available IP addresses. 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.

When a DHCP client sends a request to a DHCP server, the server first checks its static database. If an entry with the requested physical address exists in the static database, the permanent IP address of the client is returned. On the other hand, if the entry does not exist in the static database, the server selects an IP address from the available pool, assigns the address to the client, and adds the entry to the dynamic database.

ICMP

Purpose



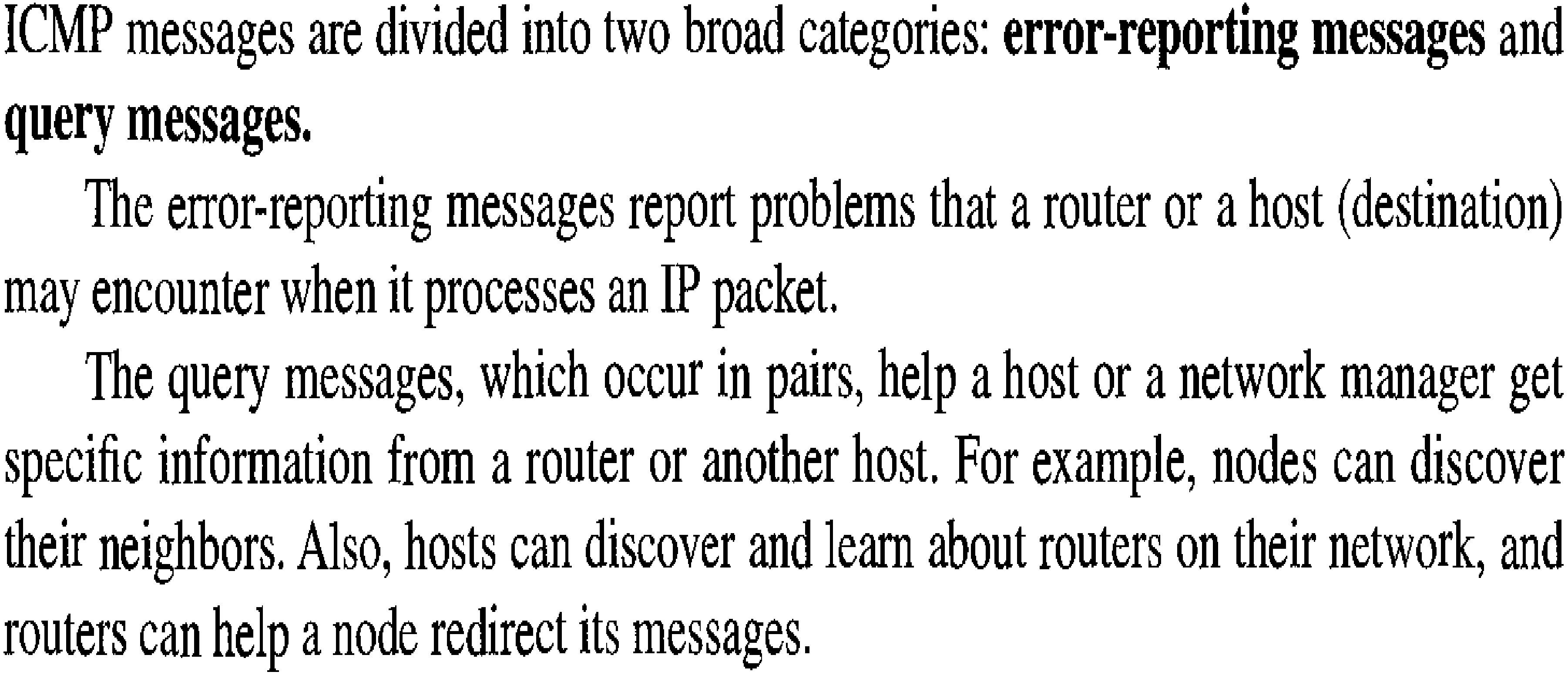
The IP protocol has no error-reporting or error-correcting mechanism.

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.

ICMP

Type of Messages



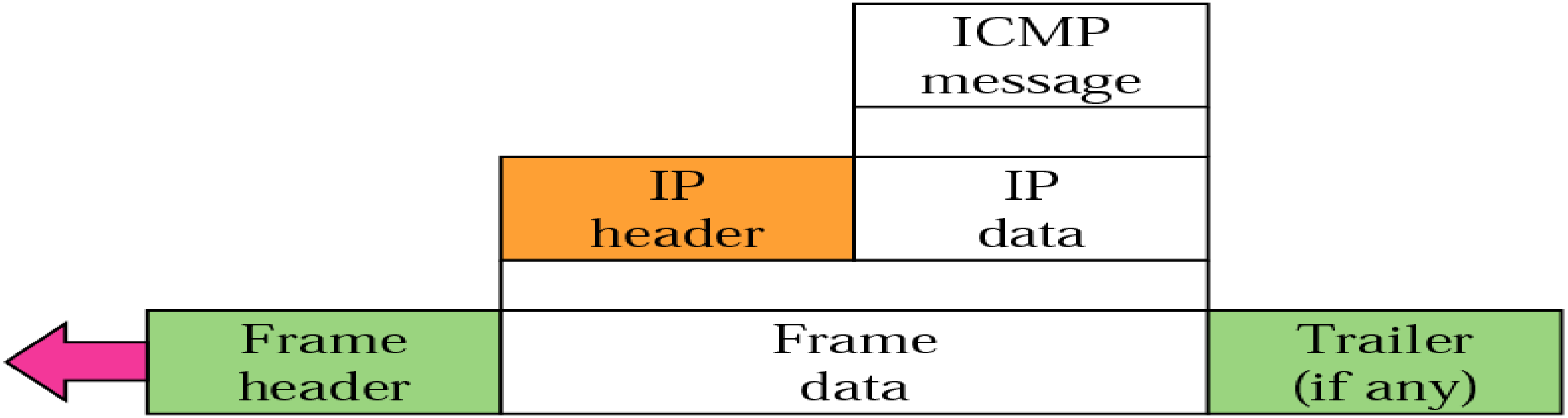
ICMP messages are divided into two broad categories: **error-reporting messages** and **query messages.**

The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.

The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host. For example, nodes can discover their neighbors. Also, hosts can discover and learn about routers on their network, and routers can help a node redirect its messages.

ICMP

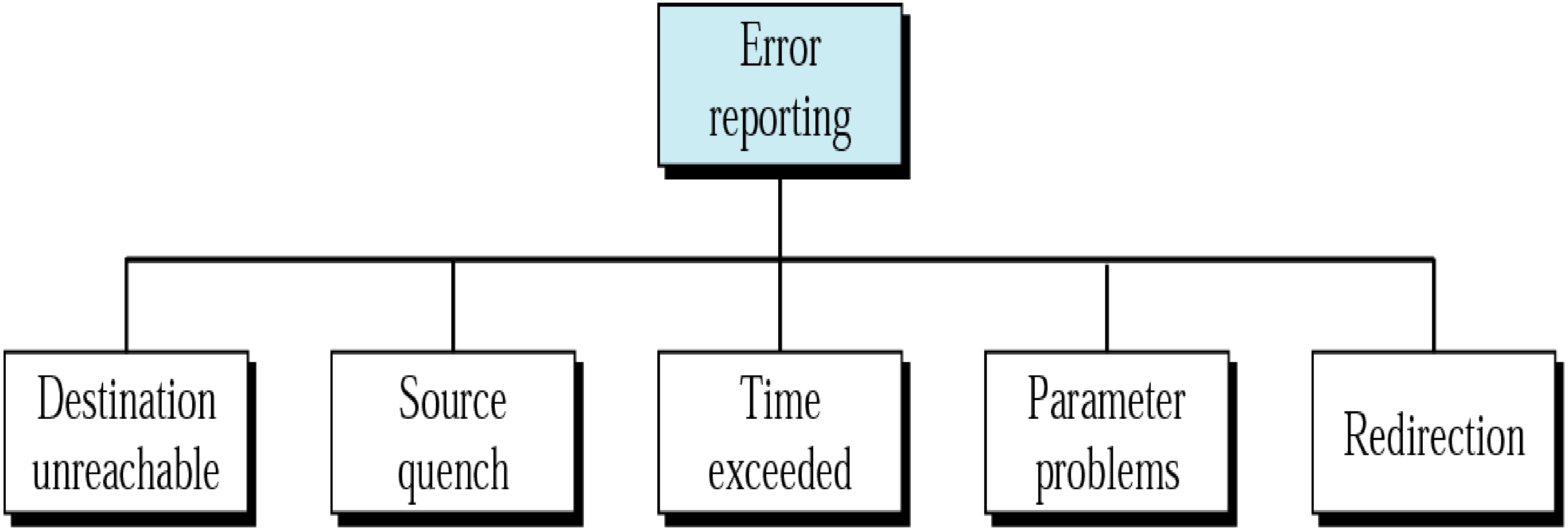
ICMP Encapsulation & Format



8 bits	8 bits	8 bits	8 bits
Type	Code	Checksum	
Rest of the header			
Data section			

ICMP

Error Reporting



ICMP always reports error messages to the original source.

ICMP

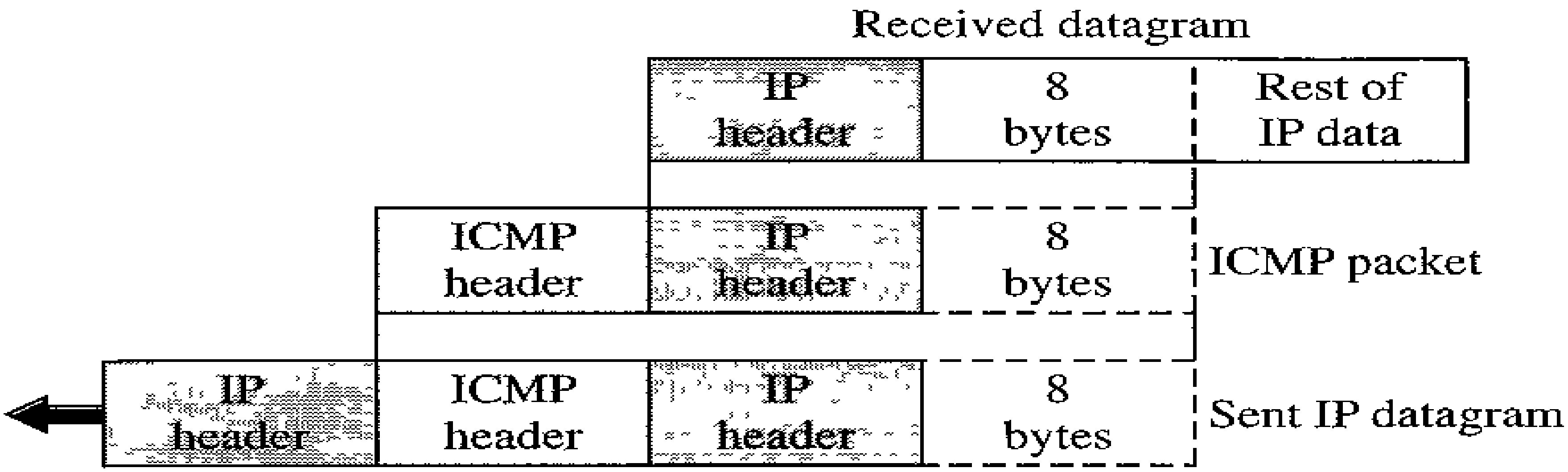
Error Reporting

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.

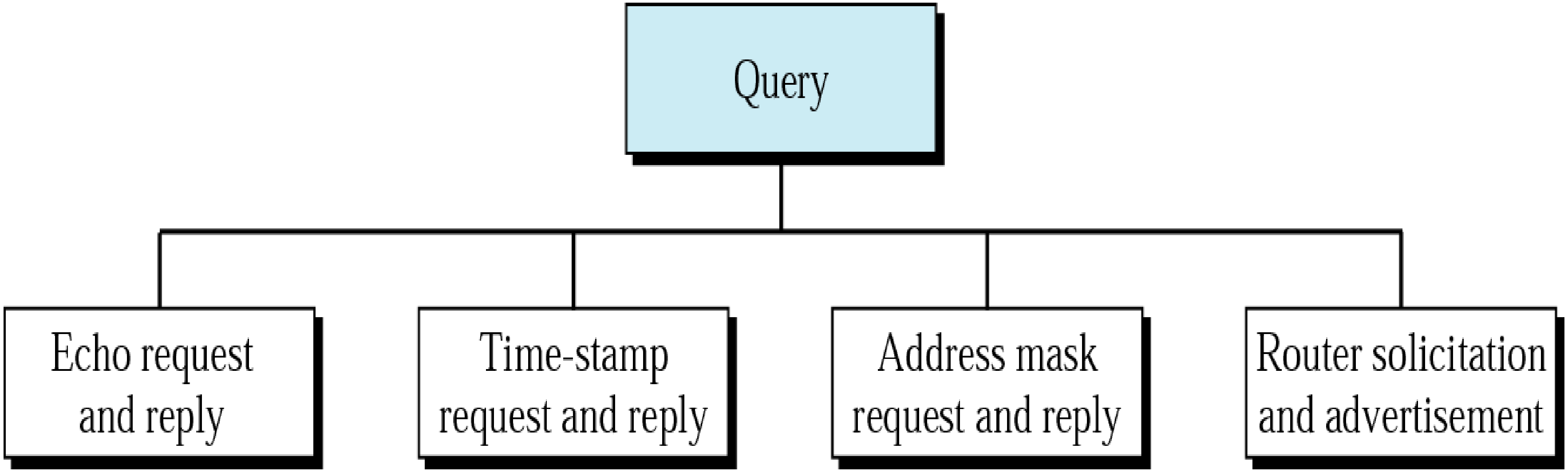
No ICMP error message will be generated for a datagram having a multicast address.

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.



ICMP

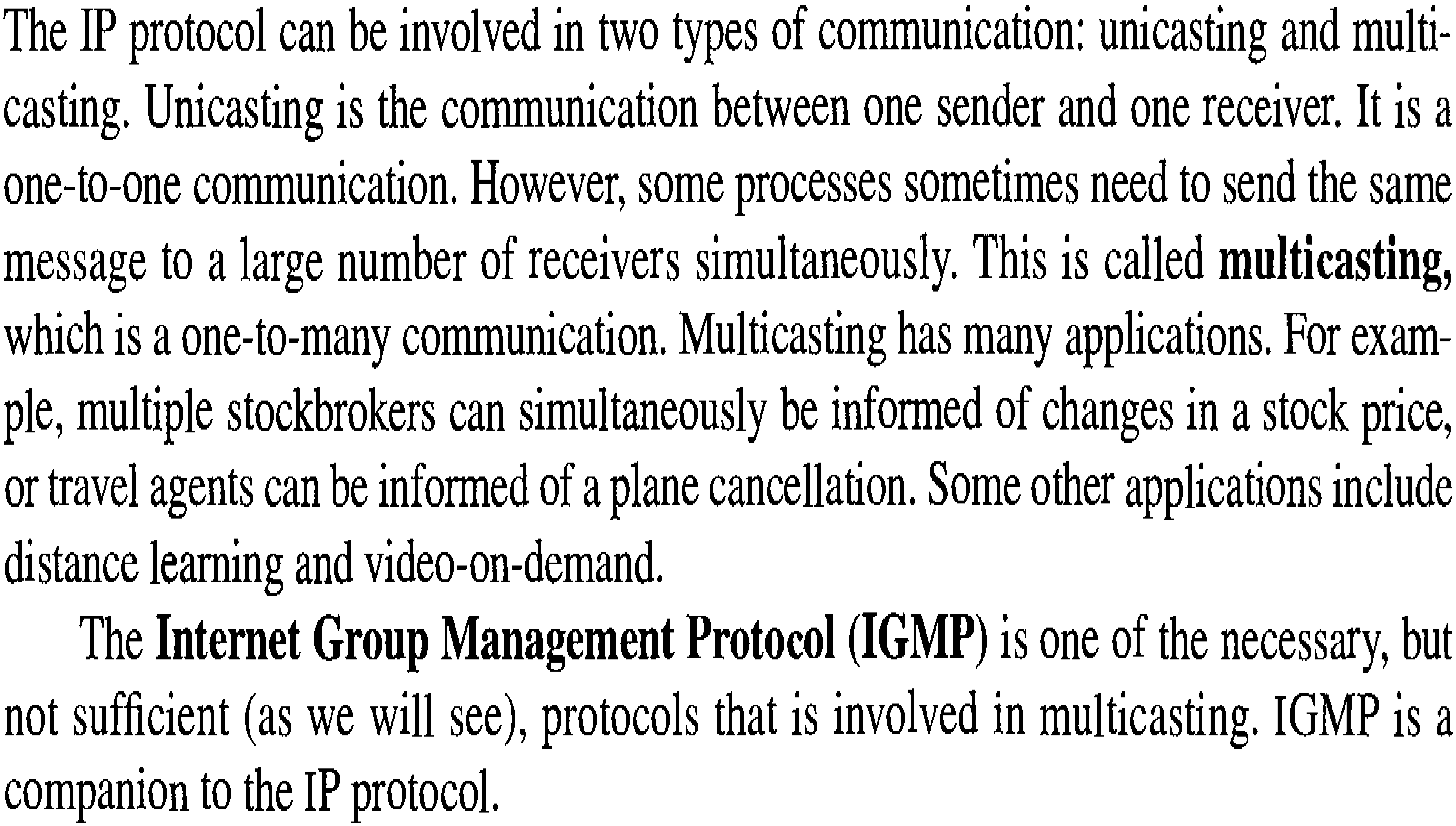
Query Message


Query
Echo request and reply
Time-stamp request and reply
Address mask request and reply
Router solicitation and advertisement

There is no flow control or congestion control mechanism in IP.

IGMP

Purpose

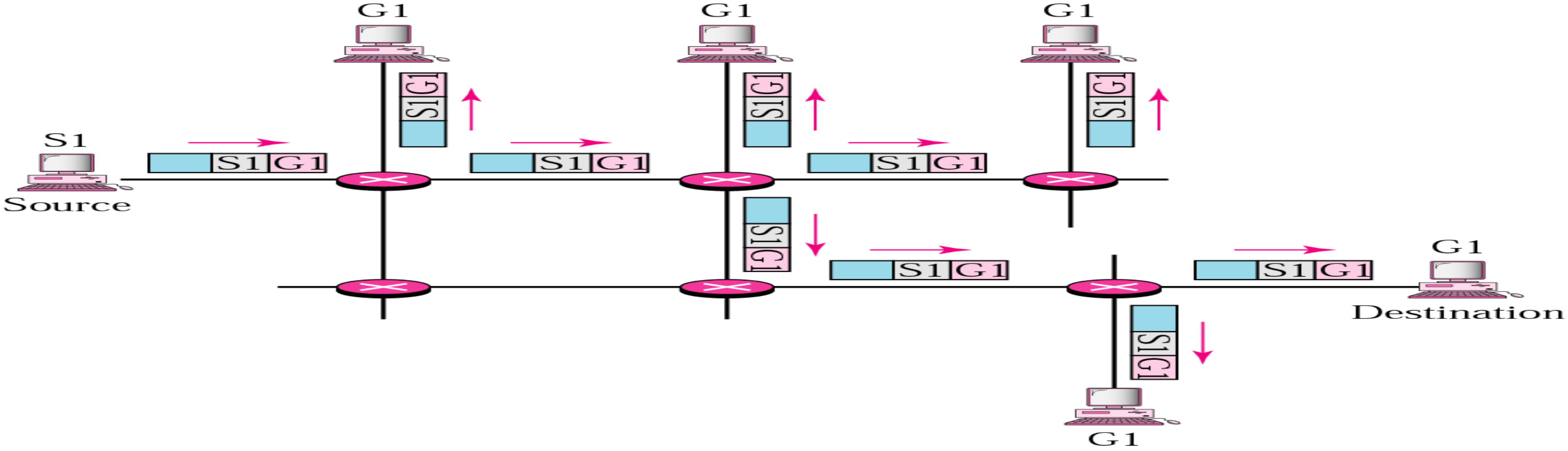


The IP protocol can be involved in two types of communication: unicasting and multicasting. Unicasting is the communication between one sender and one receiver. It is a one-to-one communication. However, some processes sometimes need to send the same message to a large number of receivers simultaneously. This is called **multicasting,** which is a one-to-many communication. Multicasting has many applications. For example, multiple stockbrokers can simultaneously be informed of changes in a stock price, or travel agents can be informed of a plane cancellation. Some other applications include distance learning and video-on-demand.

The **Internet Group Management Protocol (IGMP)** is one of the necessary, but not sufficient (as we will see), protocols that is involved in multicasting. IGMP is a companion to the IP protocol.

IGMP

Multicasting

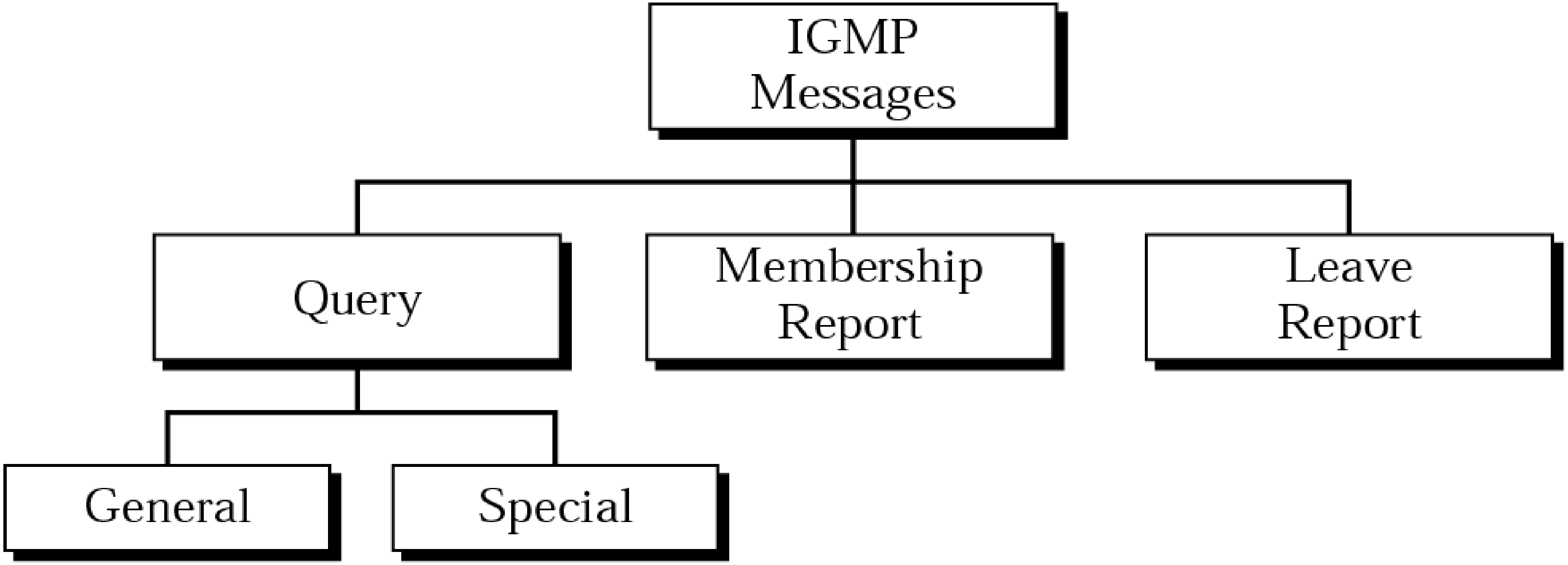


In multicast routing, the router may forward the received packet through several of its ports.

IGMP is a group management protocol. It helps a multicast router create and update a list of loyal members related to each router interface.

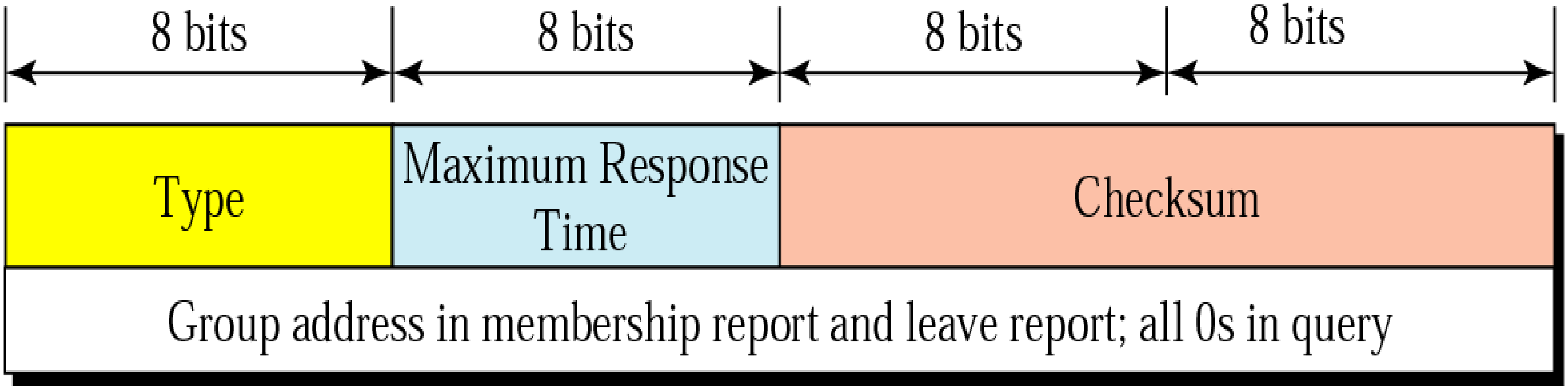
IGMP

Message Type



IGMP

Message Format



8 bits | 8 bits | 8 bits | 8 bits

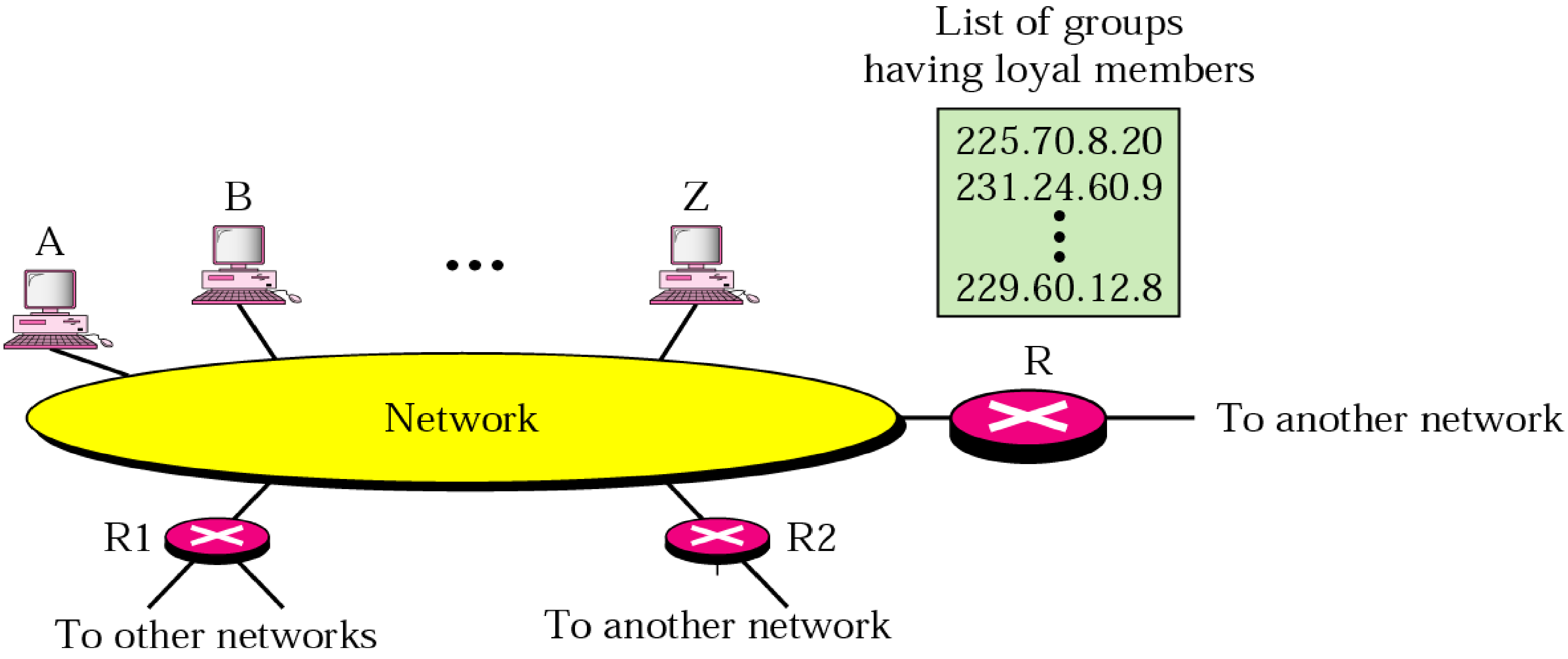
Type | Maximum Response Time | Checksum

Group address in membership report and leave report; all 0s in query

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

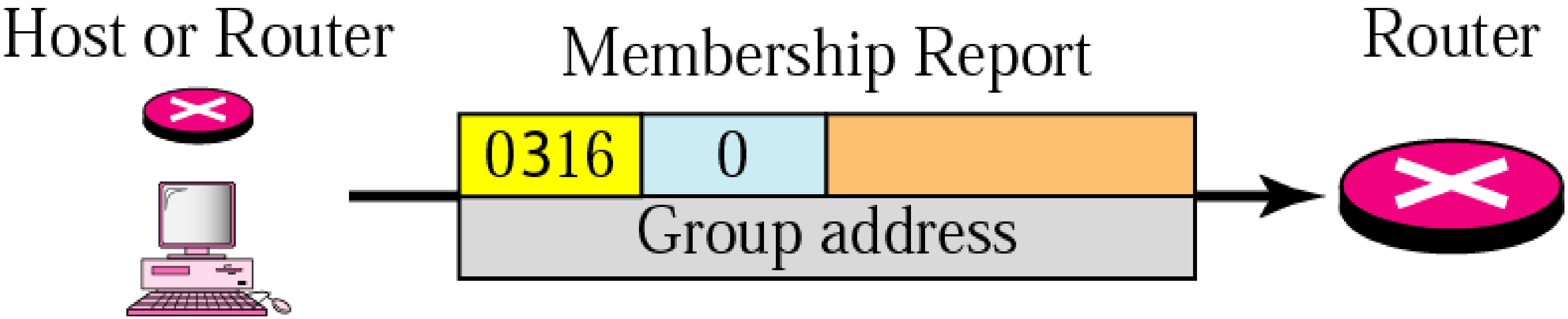
IGMP

Operation



IGMP

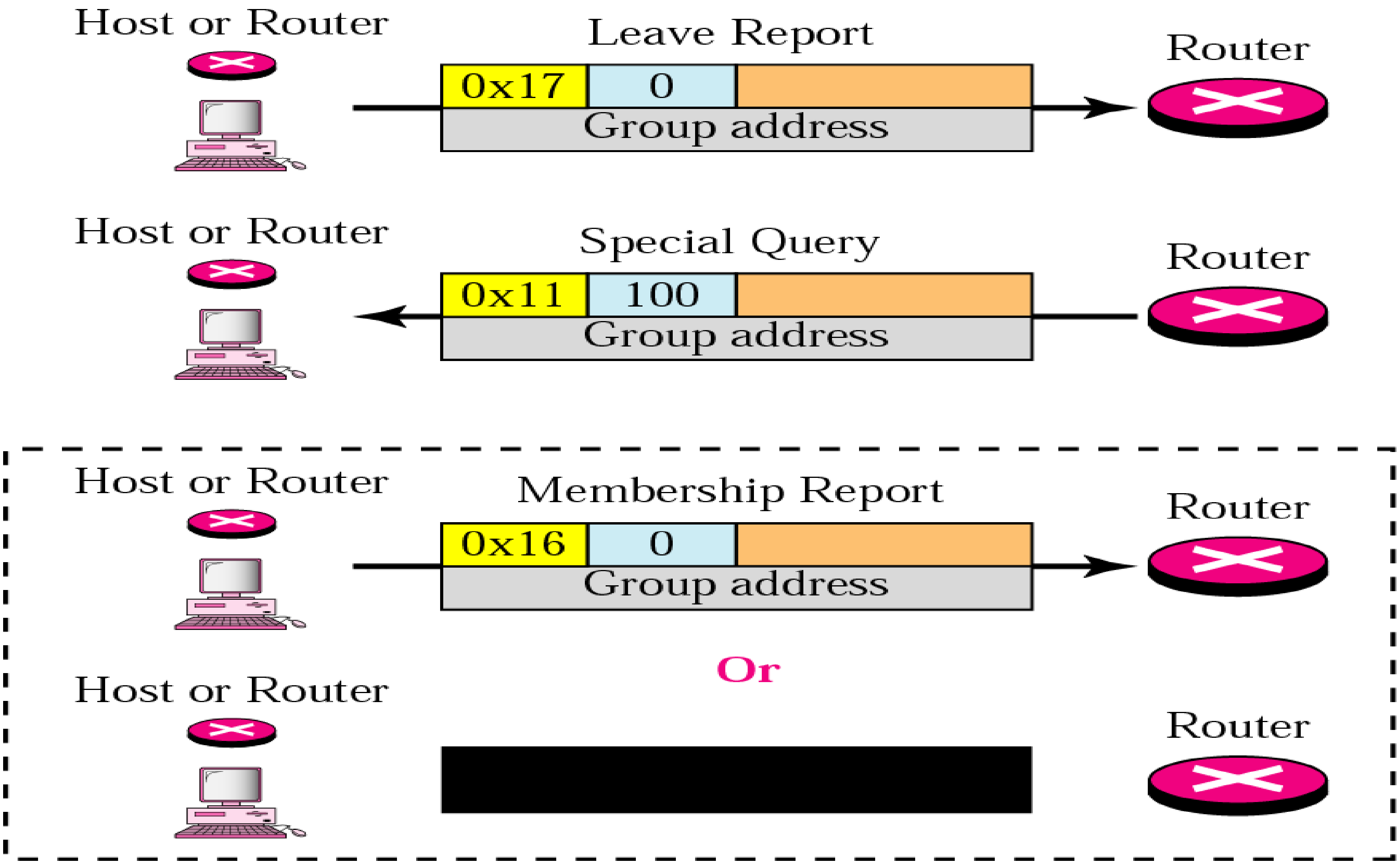
Membership Report



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

IGMP

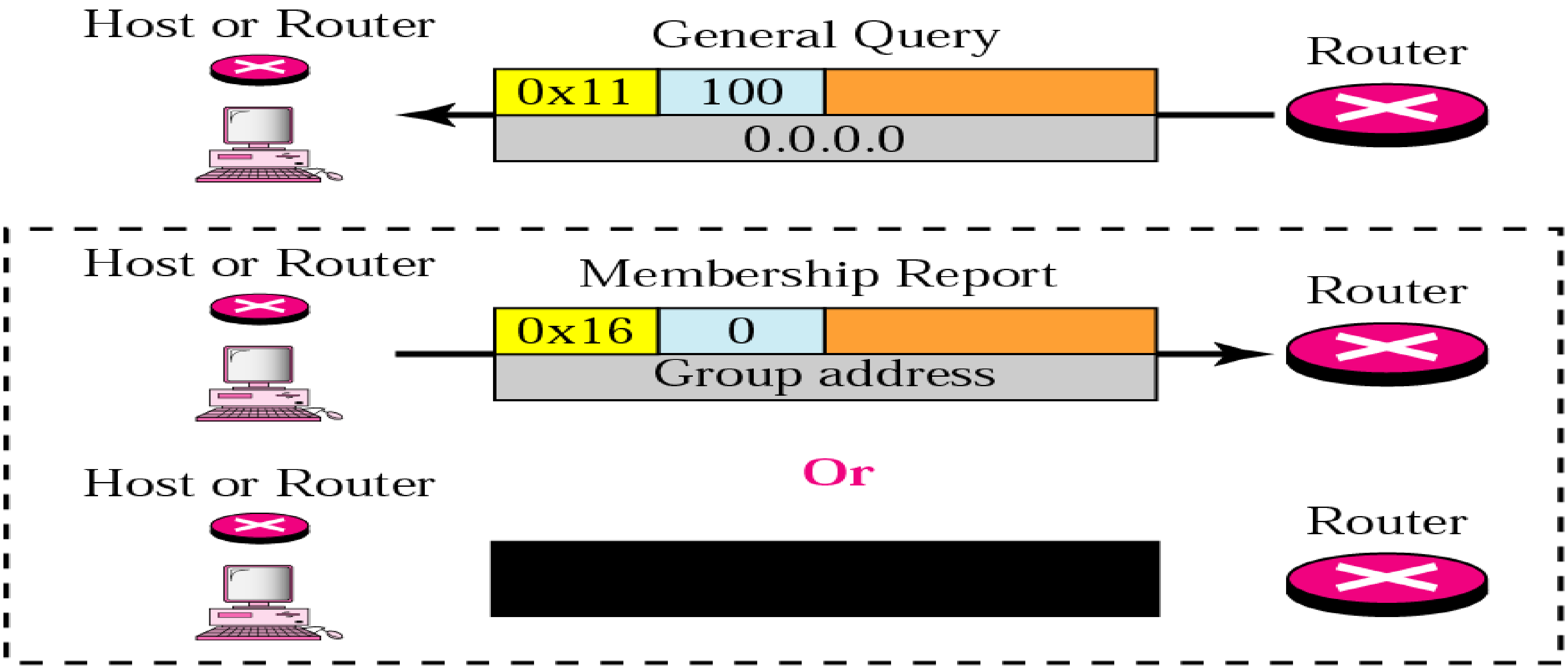
Leave Report



[redacted]

IGMP

General Query Message



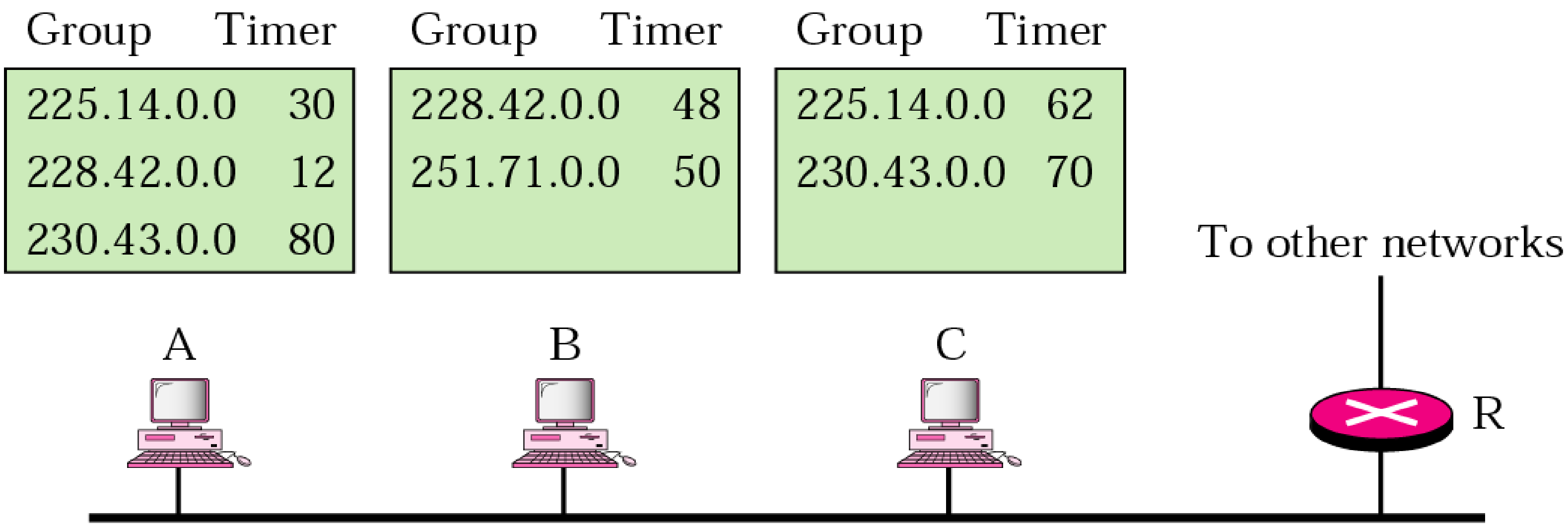
[redacted]

The general query message does not define a particular group.

IGMP

Example

Imagine there are three hosts in a network, as shown in Figure 21.30 (below). 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.



Group	Timer
225.14.0.0	30
228.42.0.0	12
230.43.0.0	80

Group	Timer
228.42.0.0	48
251.71.0.0	50

Group	Timer
225.14.0.0	62
230.43.0.0	70

IGMP

Solution

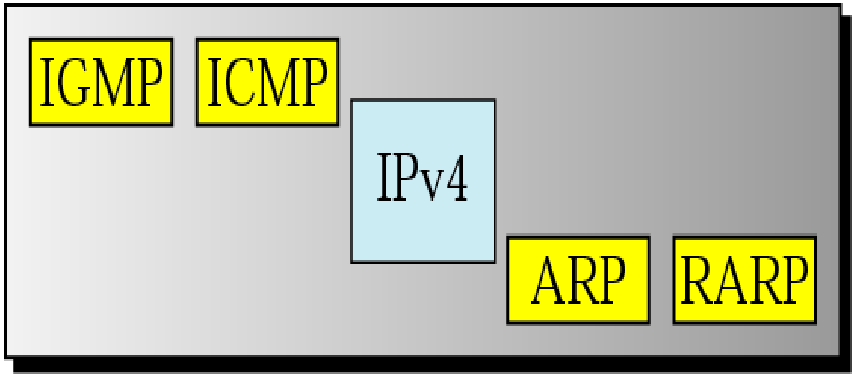
The events occur in this sequence:

1. 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.
2. 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.
3. Time 50. The timer for 251.71.0.0 in host B expires and a membership report is sent, which is received by the router and every host.
4. 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.

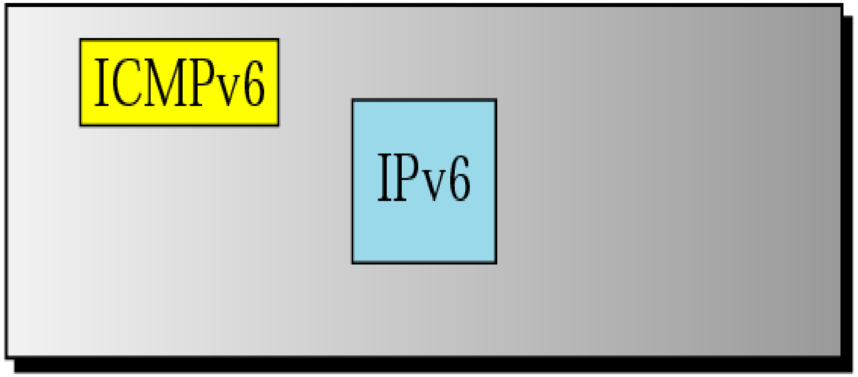
ICMPv6

Need & Comparison

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. ICMPv4 has been modified to make it more suitable for IPv6. In addition, some protocols that were independent in version 4 are now part of **Internetworking Control Message Protocol (ICMPv6).** Figure compares the network layer of version 4 to version 6.



Network layer in version 4



Network layer in version 6