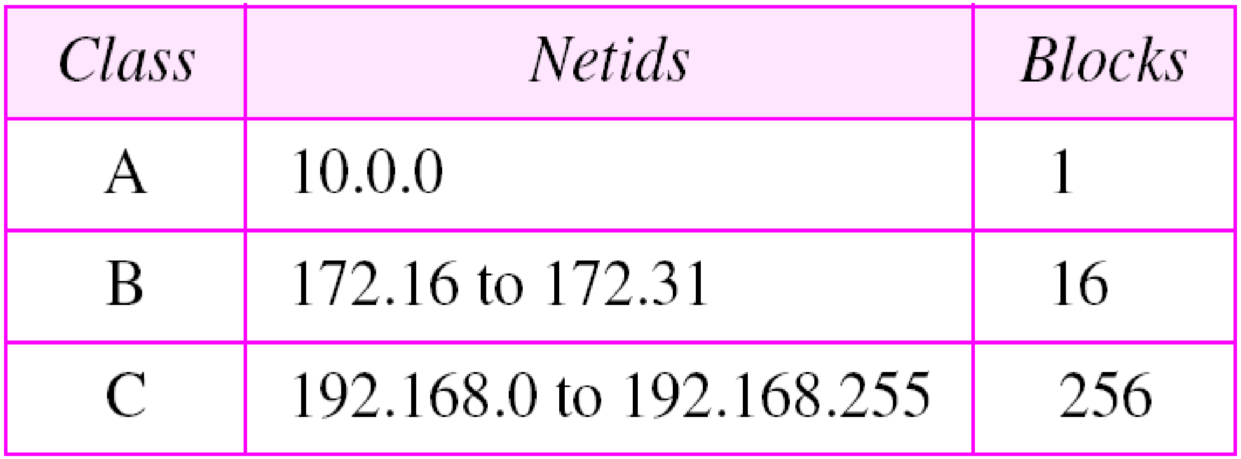
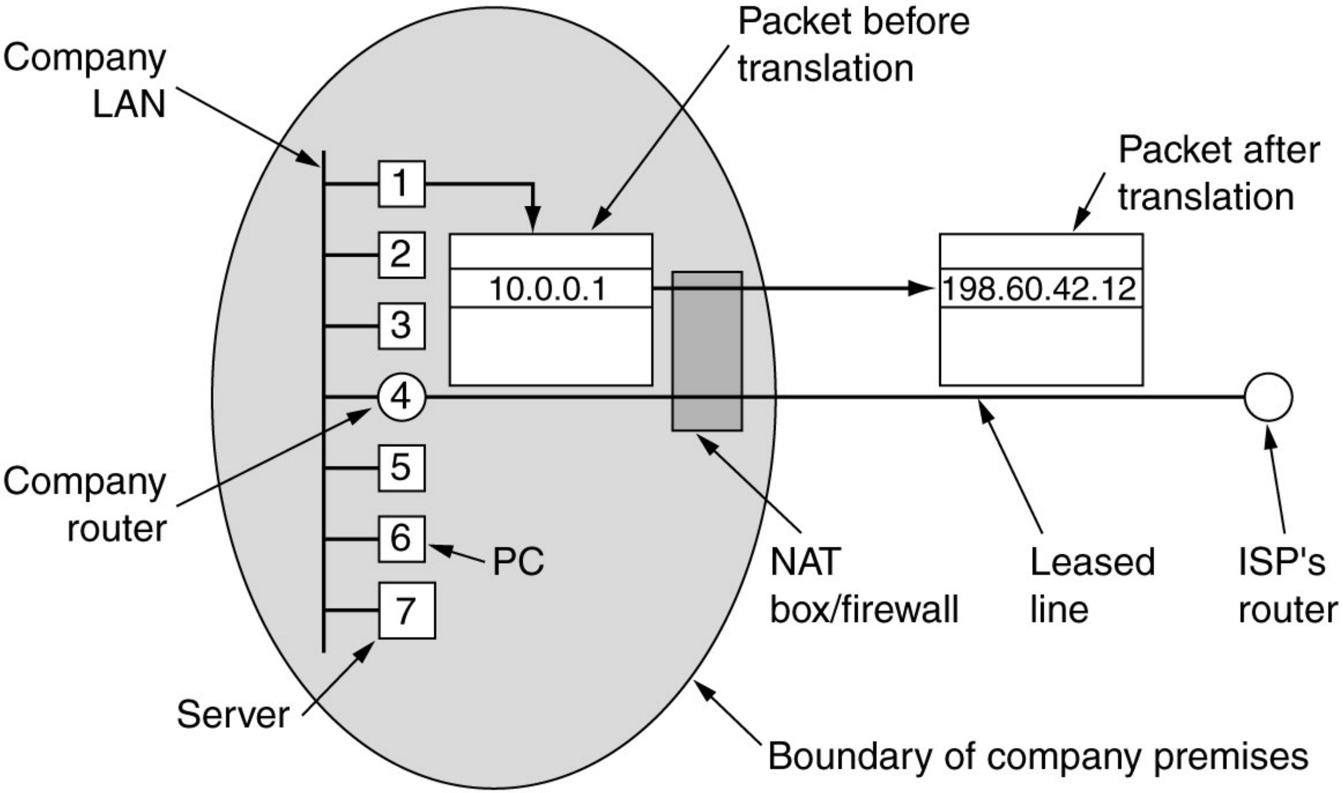
Addresses for **private networks**

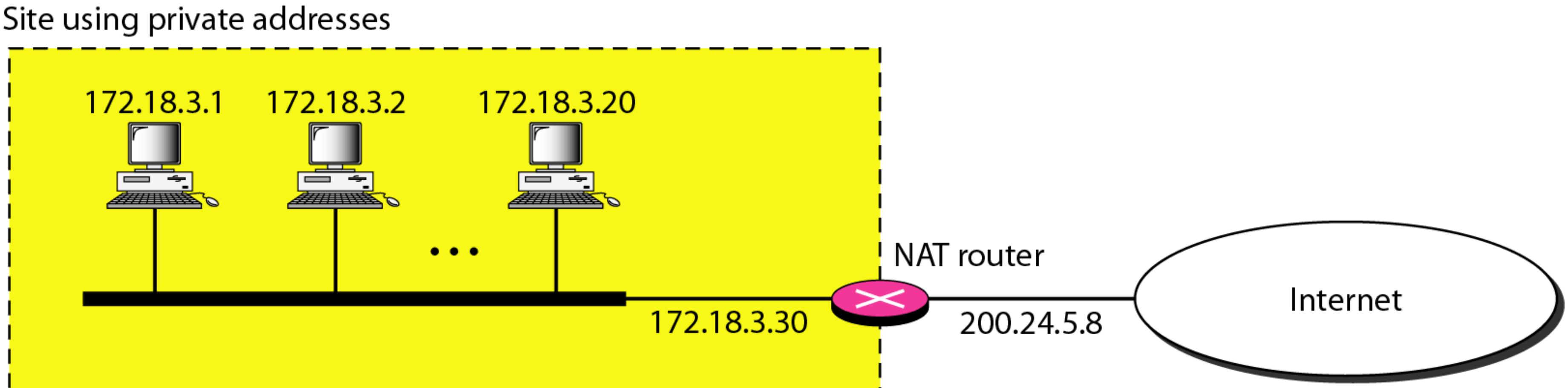


Class	*Netids*	*Blocks*
A	10.0.0	1
B	172.16 to 172.31	16
C	192.168.0 to 192.168.255	256

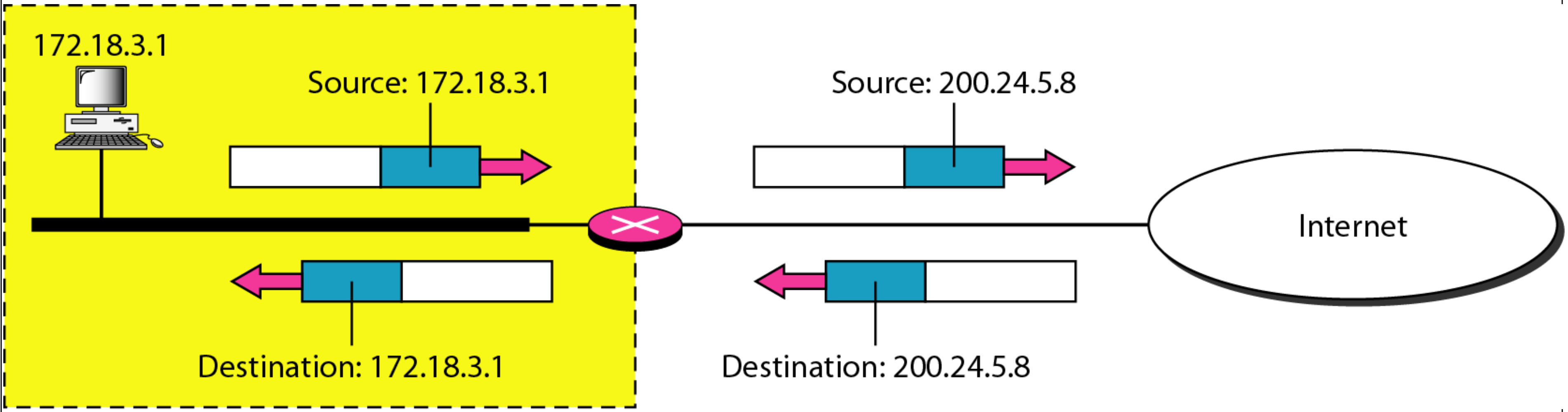
NAT – Network Address Translation



A NAT implementation



Addresses in a NAT



ICMP V4 -Introduction

- The IP protocol has no error-reporting or error correcting mechanism.
- What happens if something goes wrong? What happens if a router must discard a datagram because it cannot find a router to the final destination, or
- Because the time-to-live field has a zero value?
- These are examples of situations where an error has occurred and the IP protocol has no built-in mechanism to notify the original host.
- **The solution is ICMP protocol**

ICMP V4 -MESSAGES

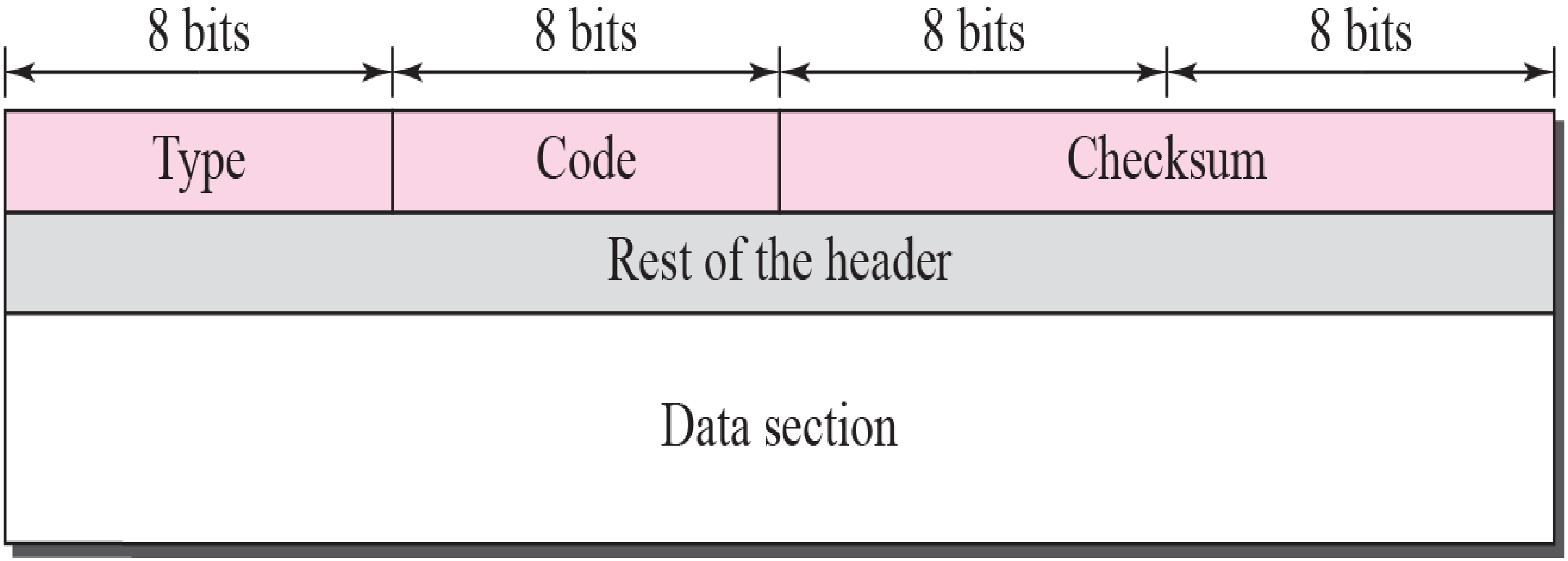
❑ICMP messages are divided into two broad categories:

1. **error-reporting messages**
2. **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, help a host or a network manager get specific information from a router or another host. Also, hosts can discover and learn about routers on their network and routers can help a node redirect its messages.

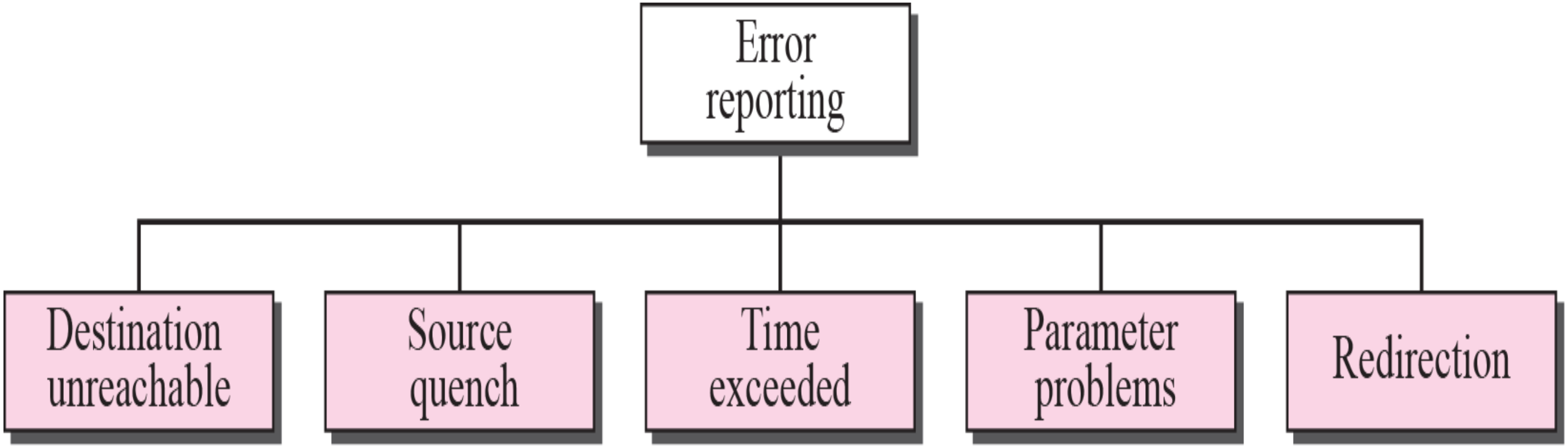
General format of ICMP messages or ICMP header



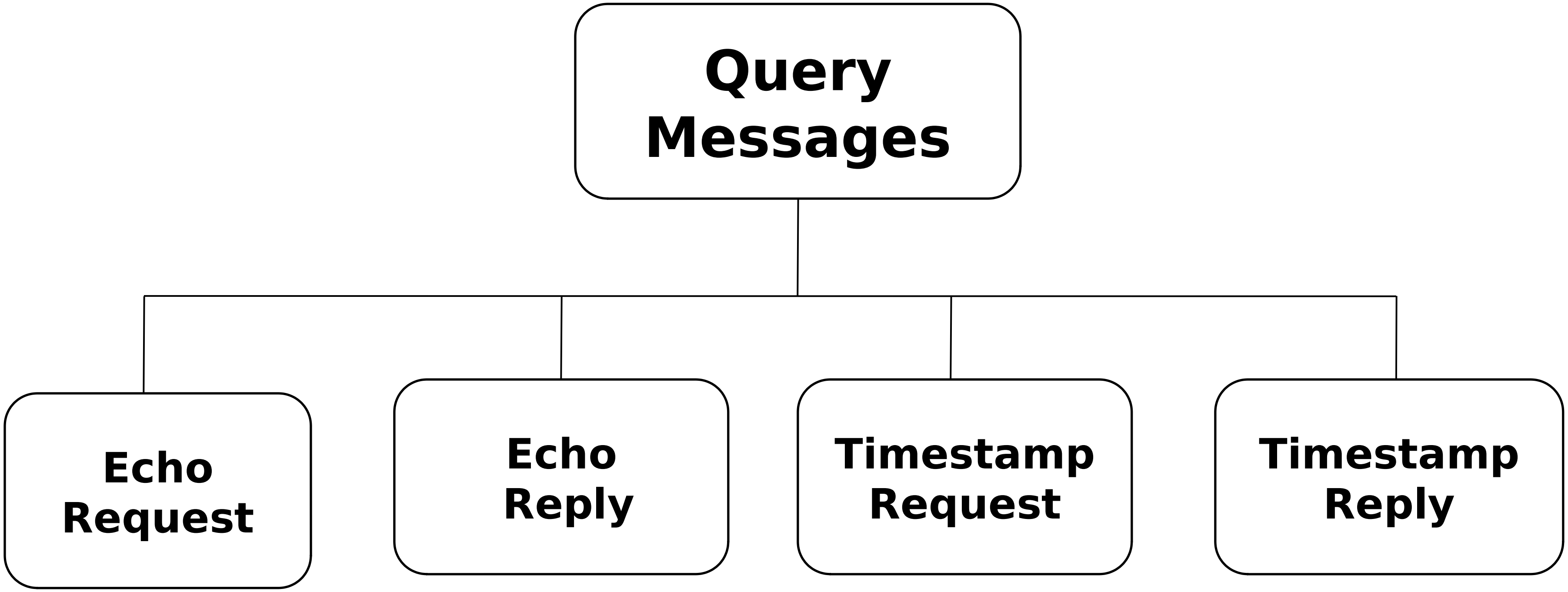
Basic ICMP Header

- Headers are 32 bits in length; all contain same three fields
  - type - 8 bit message type code
    - Thirteen message type are defined
  - code - 8 bit;
    - indicating why message is being sent
  - checksum - standard internet checksum
    - for purpose of calculation the checksum field is set to zero

Error-reporting messages



Query Messages



Query Messages

Echo Request

Echo Reply

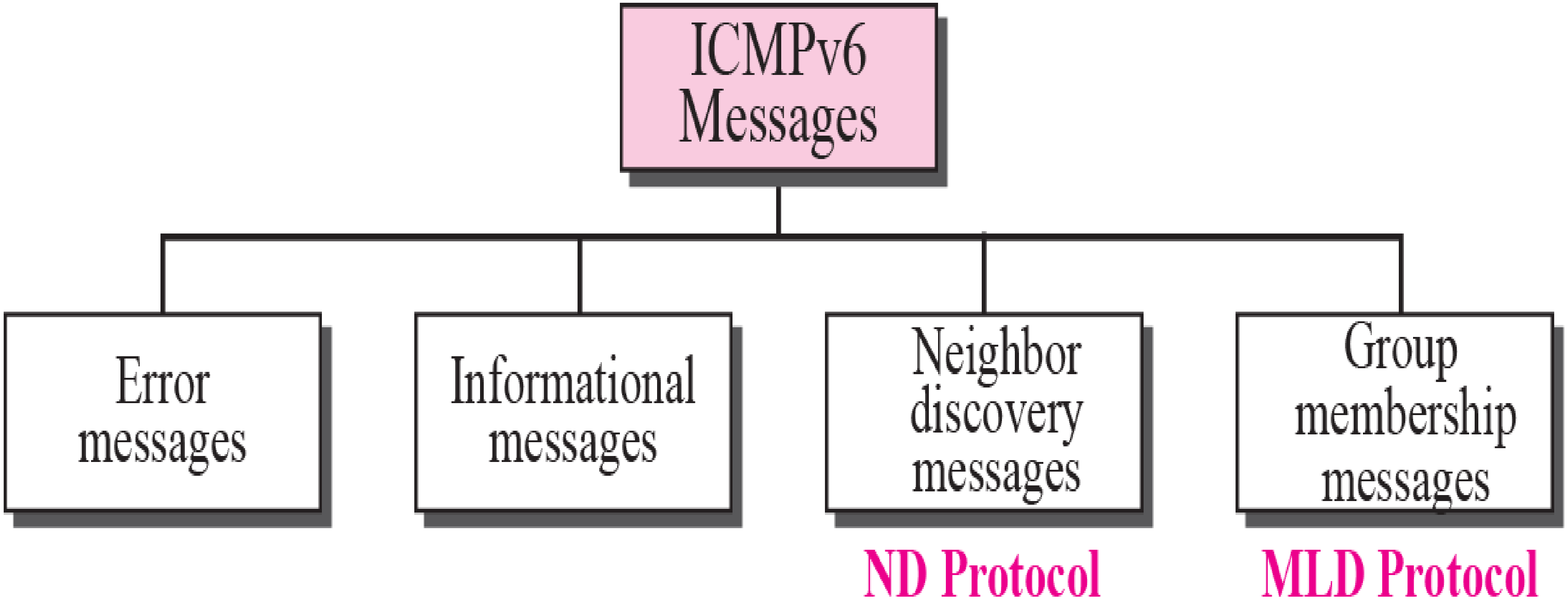
Timestamp Request

Timestamp Reply

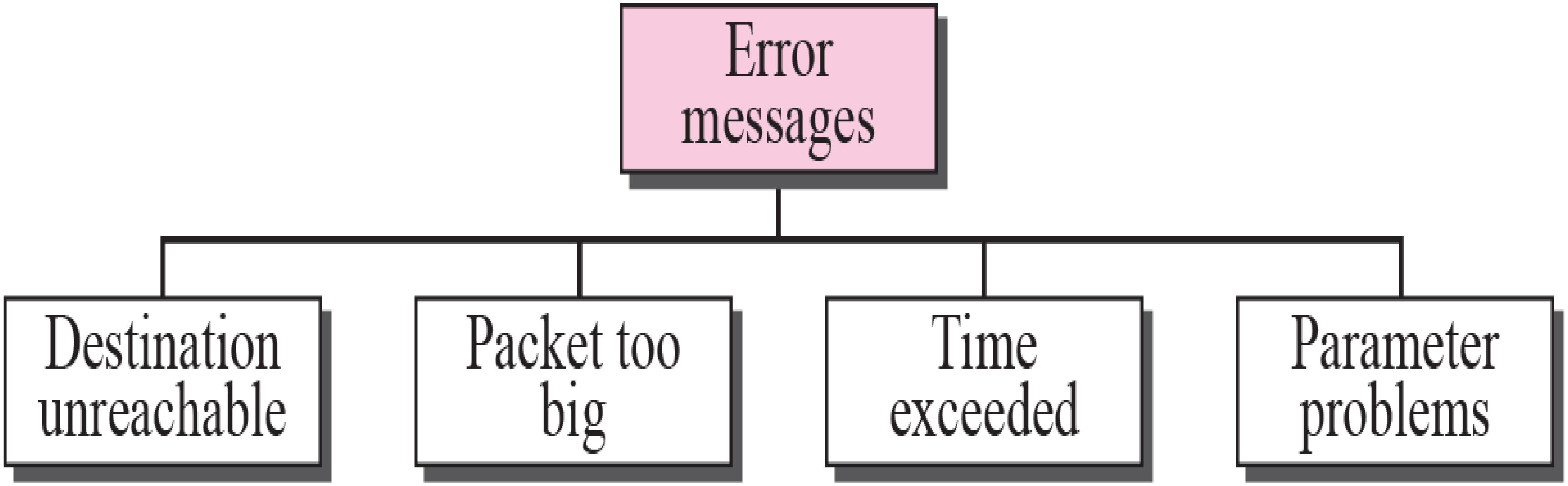
ICMP V6- INTRODUCTION

- ❑Another protocol that has been modified in **version 6** of the TCP/IP protocol suite is ICMP.
- ❑This new version, Internet Control Message Protocol version 6 (ICMPv6), follows the same strategy and purposes of version 4.
- ❑ICMPv6, however, is more complicated than ICMPv4: some protocols that were independent in version 4 are now part of ICMPv6 and
- ❑some new messages have been added to make it more useful.

Taxonomy of ICMPv6 messages



Error-reporting messages



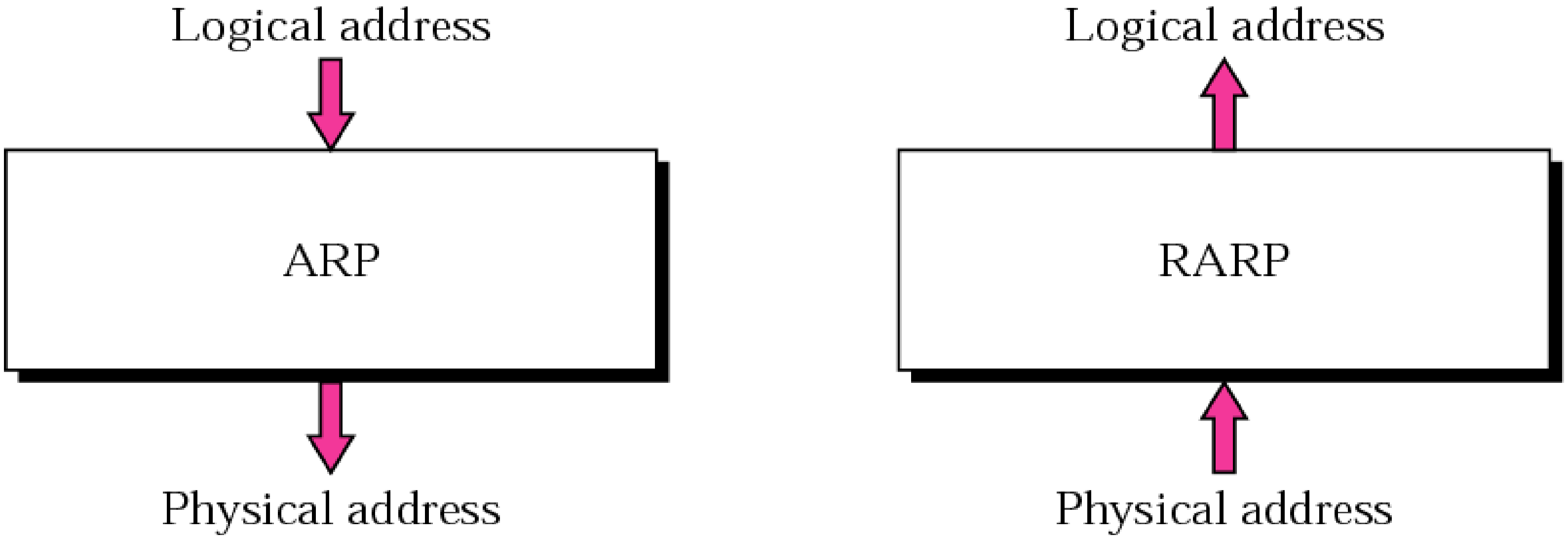
Informational Messages

- ❑Two of the ICMPv6 messages can be categorized as informational messages: echo request and echo reply messages.
- ❑The echo request and echo response messages are designed to check if two devices in the Internet can communicate with each other.
- ❑ A host or router can send an echo request message to another host; the receiving computer or router can reply using the echo response message.

Neighbor-Discovery Messages

- The most important issue is the definition of two new protocols that clearly define the functionality of these group messages:
    1. Neighbor-Discovery (ND) protocol
    2. Inverse-Neighbor-Discovery (IND) protocol.
- These two protocols are used by nodes (hosts or routers) on the same link (network).

ARP and RARP


Logical address
ARP
Physical address
Logical address
RARP
Physical address

ARP (Address Resolution Protocol)

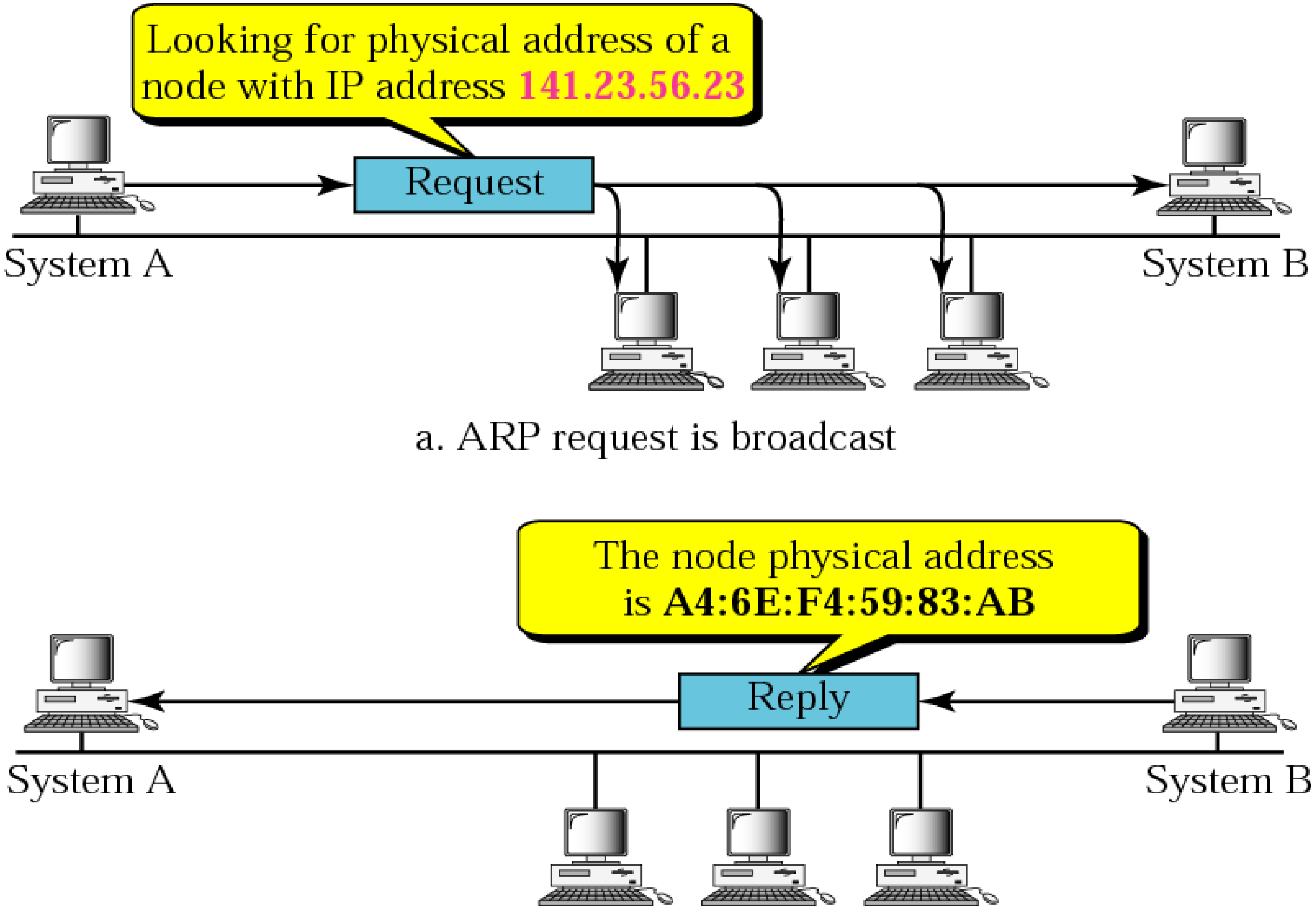
ARP associates an IP address with its physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address that is usually imprinted on the NIC.

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. These can be done using either static or dynamic mapping.

Logical address to physical address translation can be done statically (not practical) or dynamically (with ARP).

ARP operation



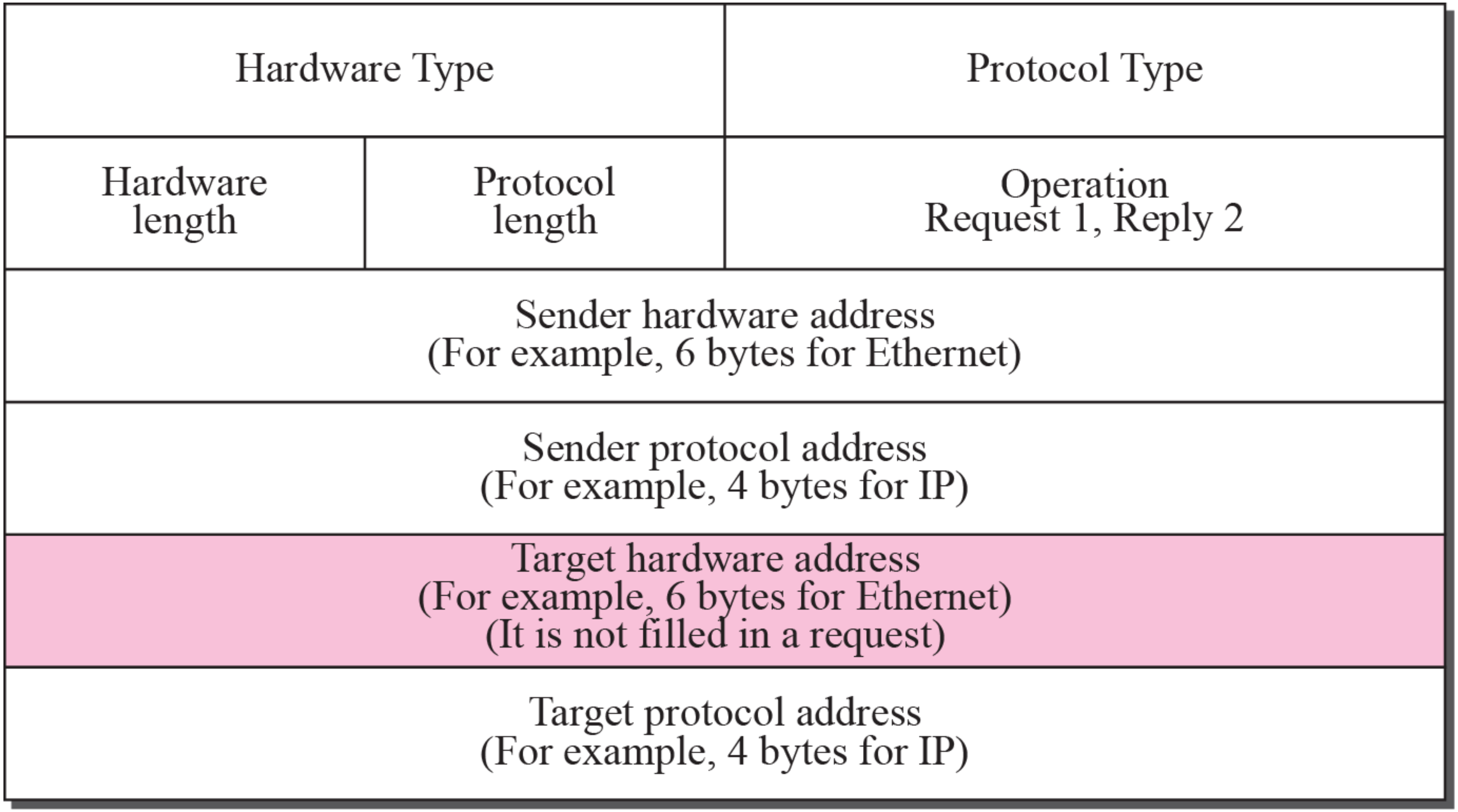
Looking for physical address of a node with IP address **141.23.56.23**

a. ARP request is broadcast

The node physical address is **A4:6E:F4:59:83:AB**

b. ARP reply is unicast

ARP packet



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)		

Note

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

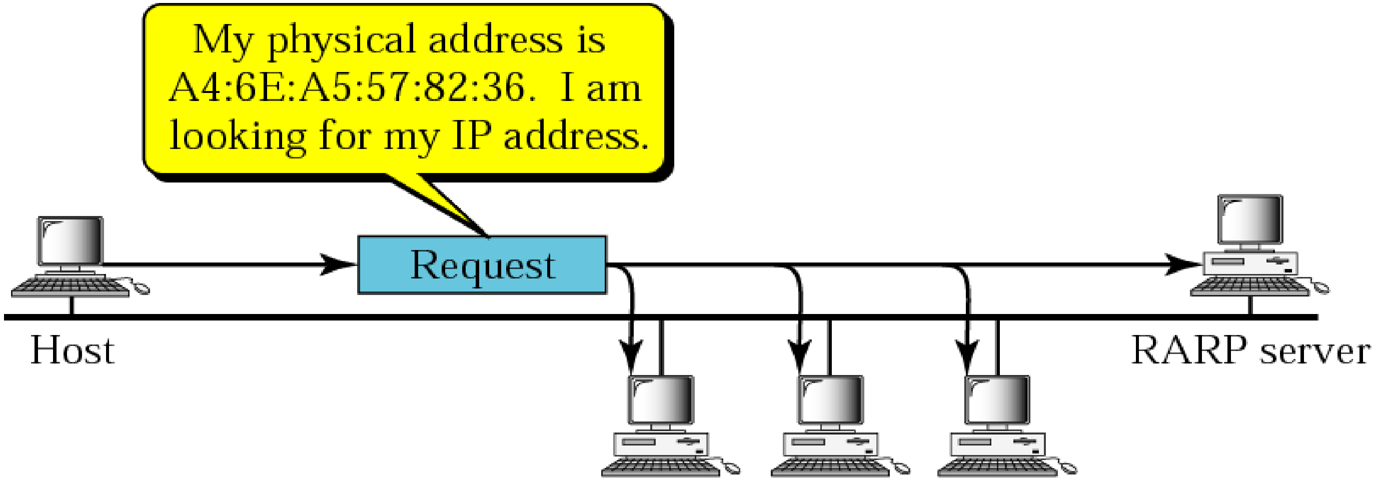
RARP (Reverse Address resolution Protoco

RARP finds the logical address for a machine that only knows its physical address. RARP requests are broadcast, RARP replies are unicast.

This if often encountered on thin-client workstations. No disk, so when machine is booted, it needs to know its IP address (don’t want to burn the IP address into the ROM).

If a thin client workstation needs to know its IP address, it probably also needs to know its subnet mask, router address, DNS address, etc.So we need something more than RARP. BOOTP, and now DHCP have replaced RARP.

RARP operation



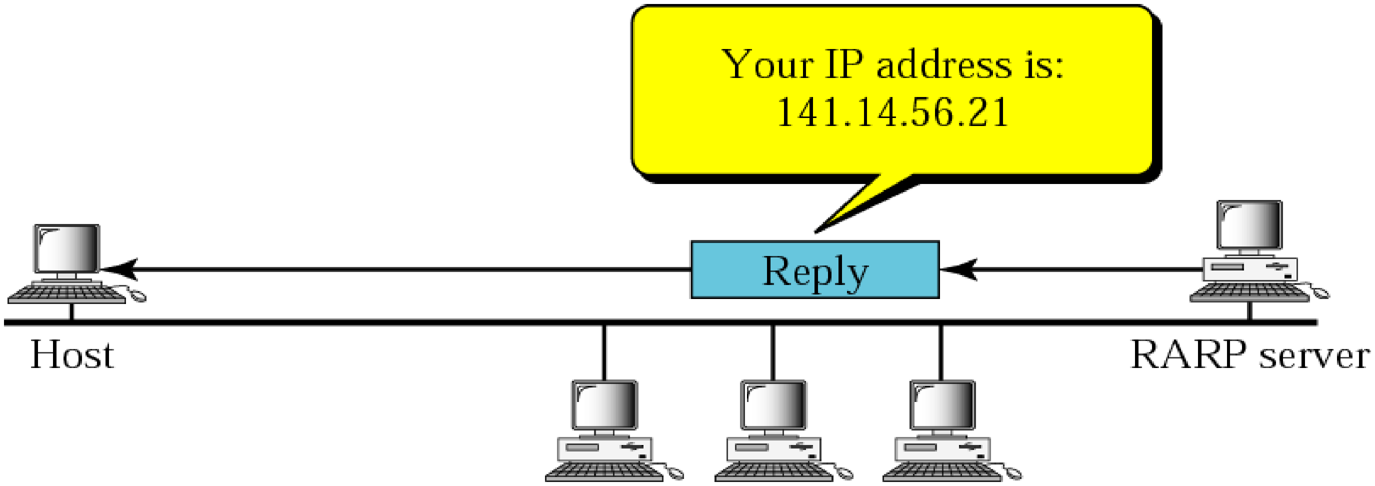
My physical address is A4:6E:A5:57:82:36. I am looking for my IP address.

Request

Host

RARP server

a. RARP request is broadcast



Your IP address is: 141.14.56.21

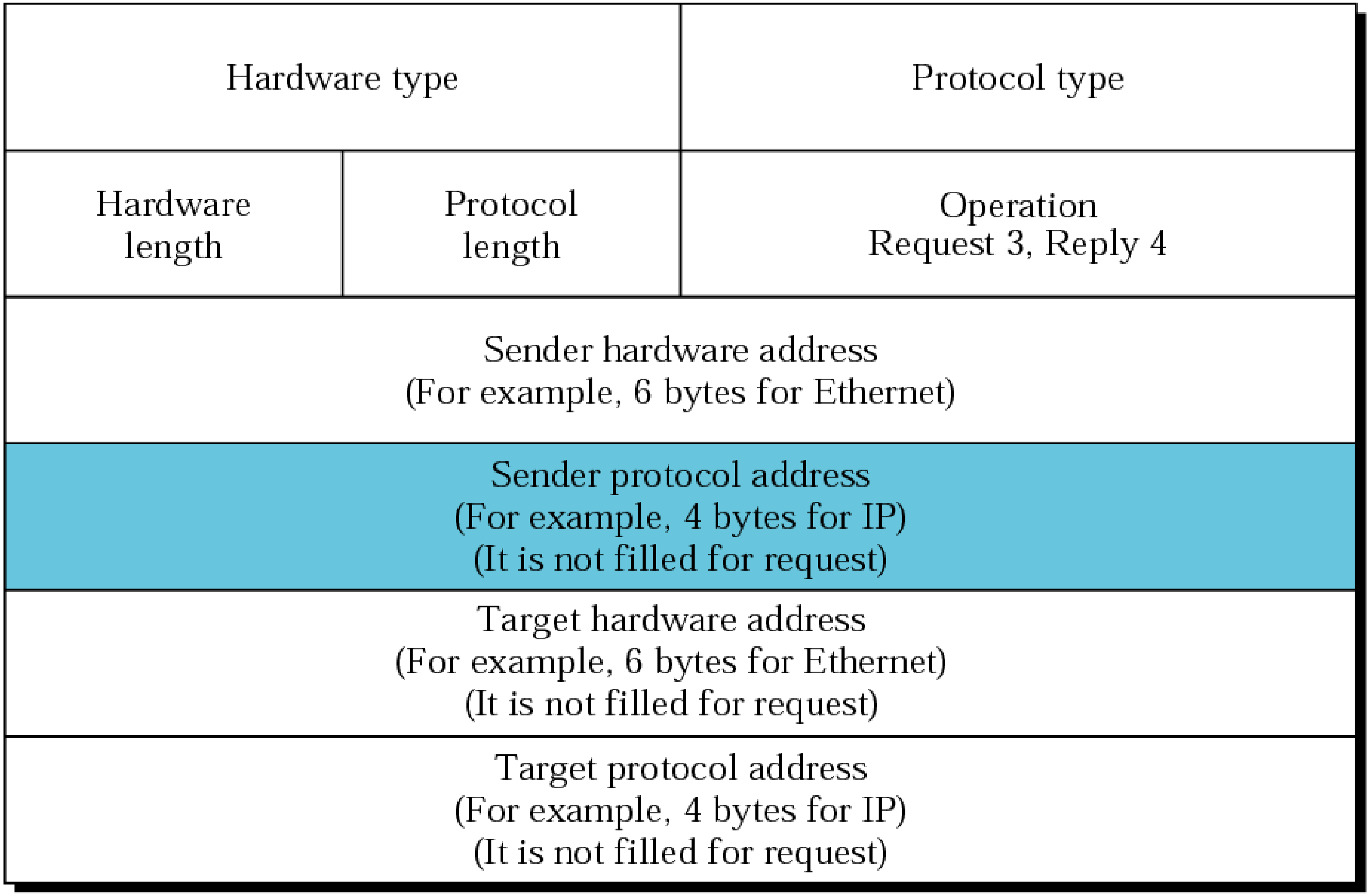
Reply

Host

RARP server

b. RARP reply is unicast

RARP packet



Hardware type		Protocol type
Hardware length	Protocol length	Operation Request 3, Reply 4
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP) (It is not filled for request)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled for request)		
Target protocol address (For example, 4 bytes for IP) (It is not filled for request)		