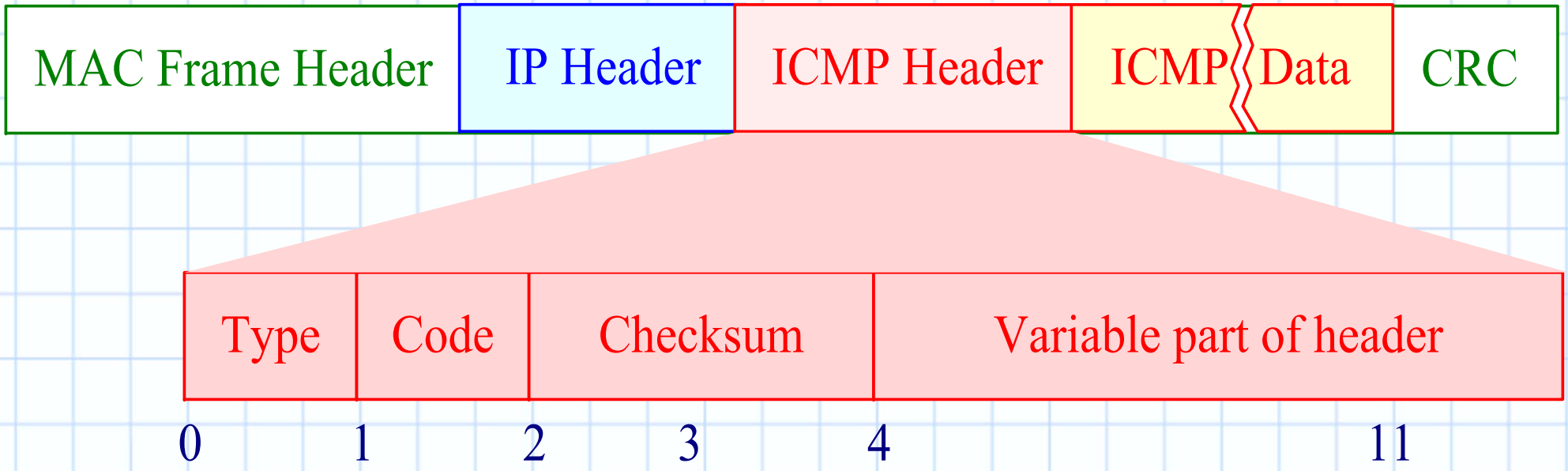
Internet Control Message Protocol

Internet Control Message Protocol

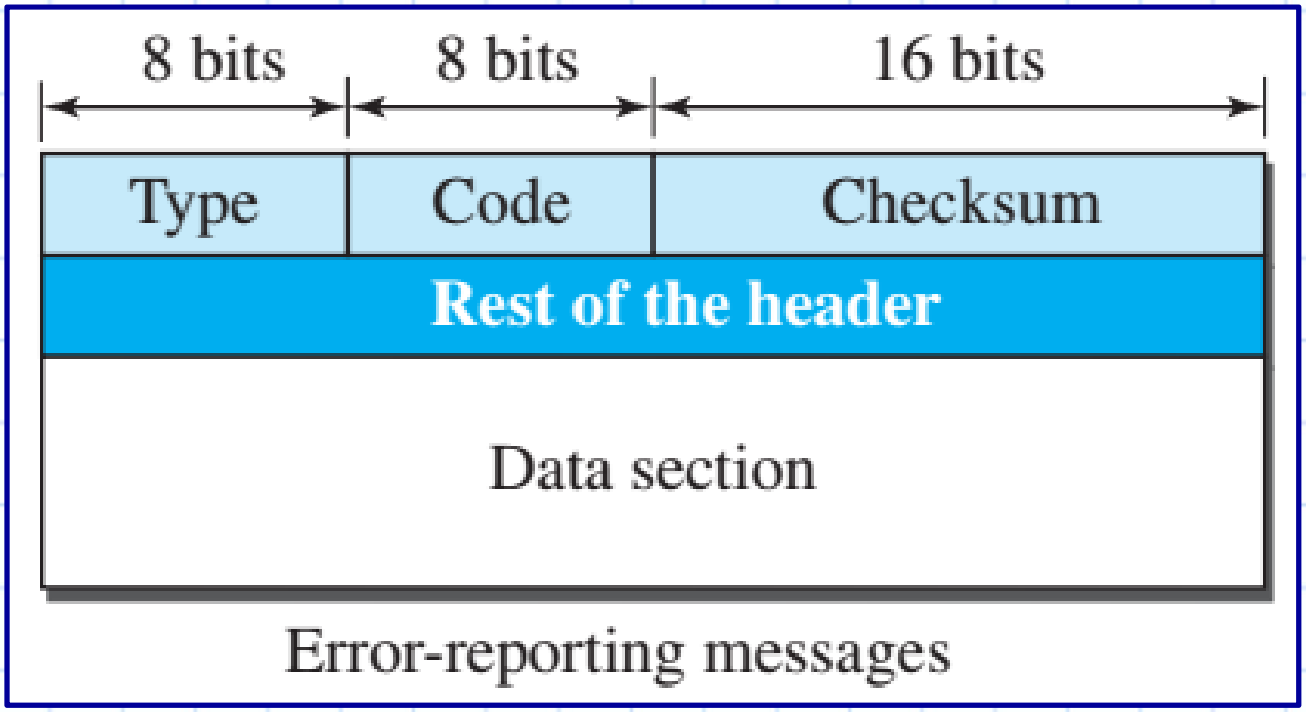
- ICMP is a service protocol that is part of IP.
- Signals abnormal events in networks.
- ICMP packets are wrapped into an IP datagram.
- Offers flow control and error-detection.
- Provides a facility to communicate with a source if there is a problem.
- Provides a mechanism for determining if a destination can not be reached.
- Tests intermediate networks along the way to the destination.
- PING is an ICMP message that tries to locate other station on the internet to see if they are active or to see if a path is up.

ICMP v4 Packet format and encapsulation



- Message Type indicates which ICMP message is present
- Message Code qualifies this for meaning specific to the type of message.

Error-reporting messages

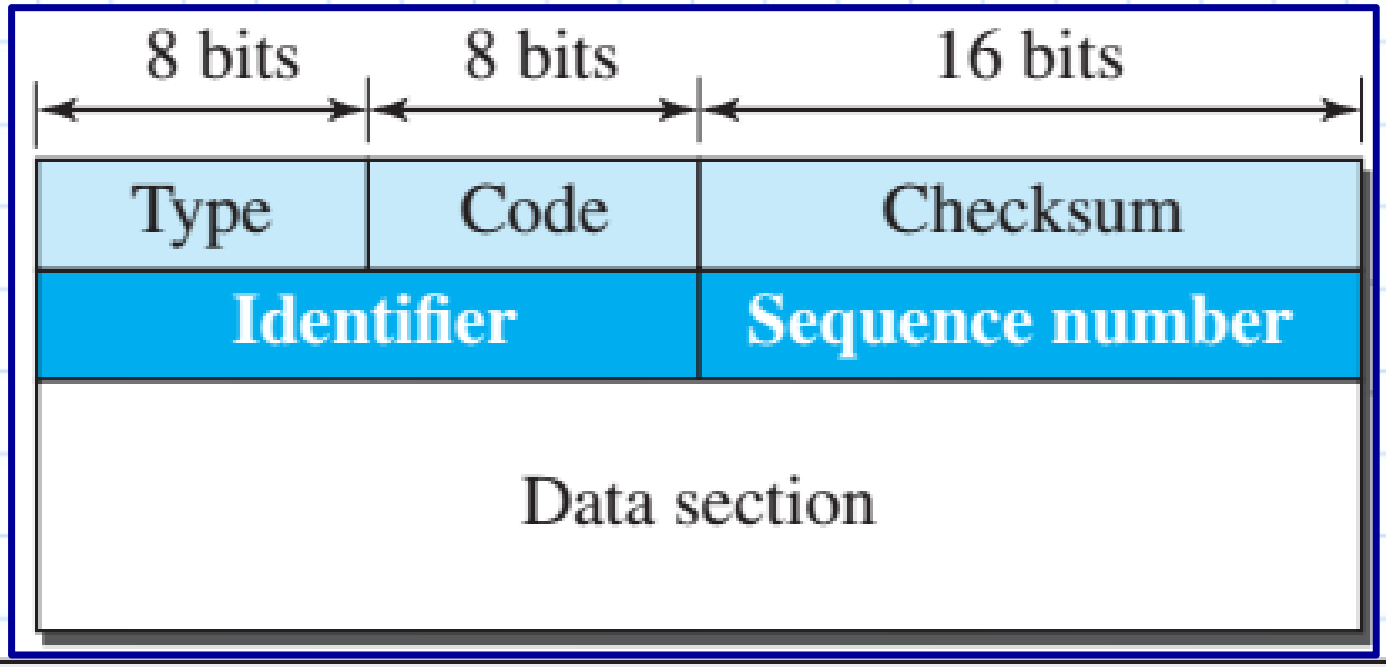


Error-reporting messages

Type and code values

03: Destination unreachable (codes 0 to 15)
04: Source quench (only code 0)
05: Redirection (codes 0 to 3)
11: Time exceeded (codes 0 and 1)
12: Parameter problem (codes 0 and 1)

Query messages

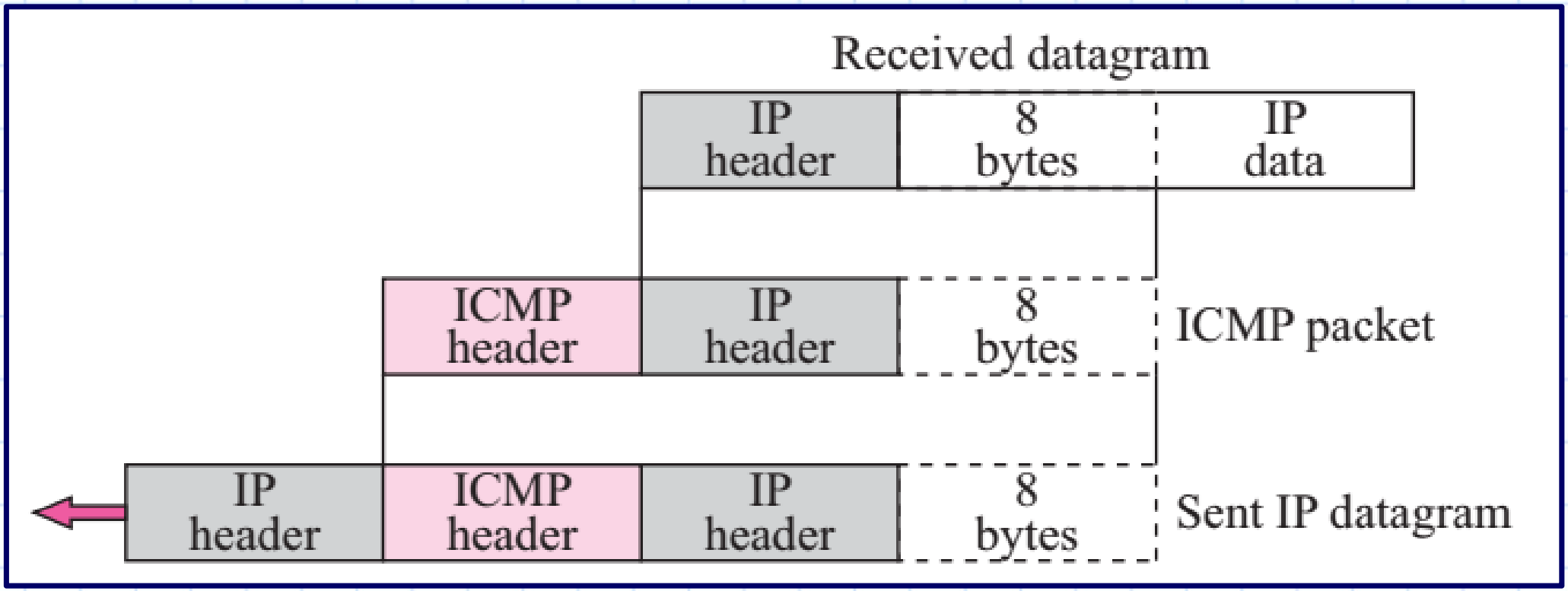


Type and code values

08 and 00: Echo request and reply (only code 0)

13 and 14: Timestamp request and reply (only code 0)

Contents of data field for the error messages

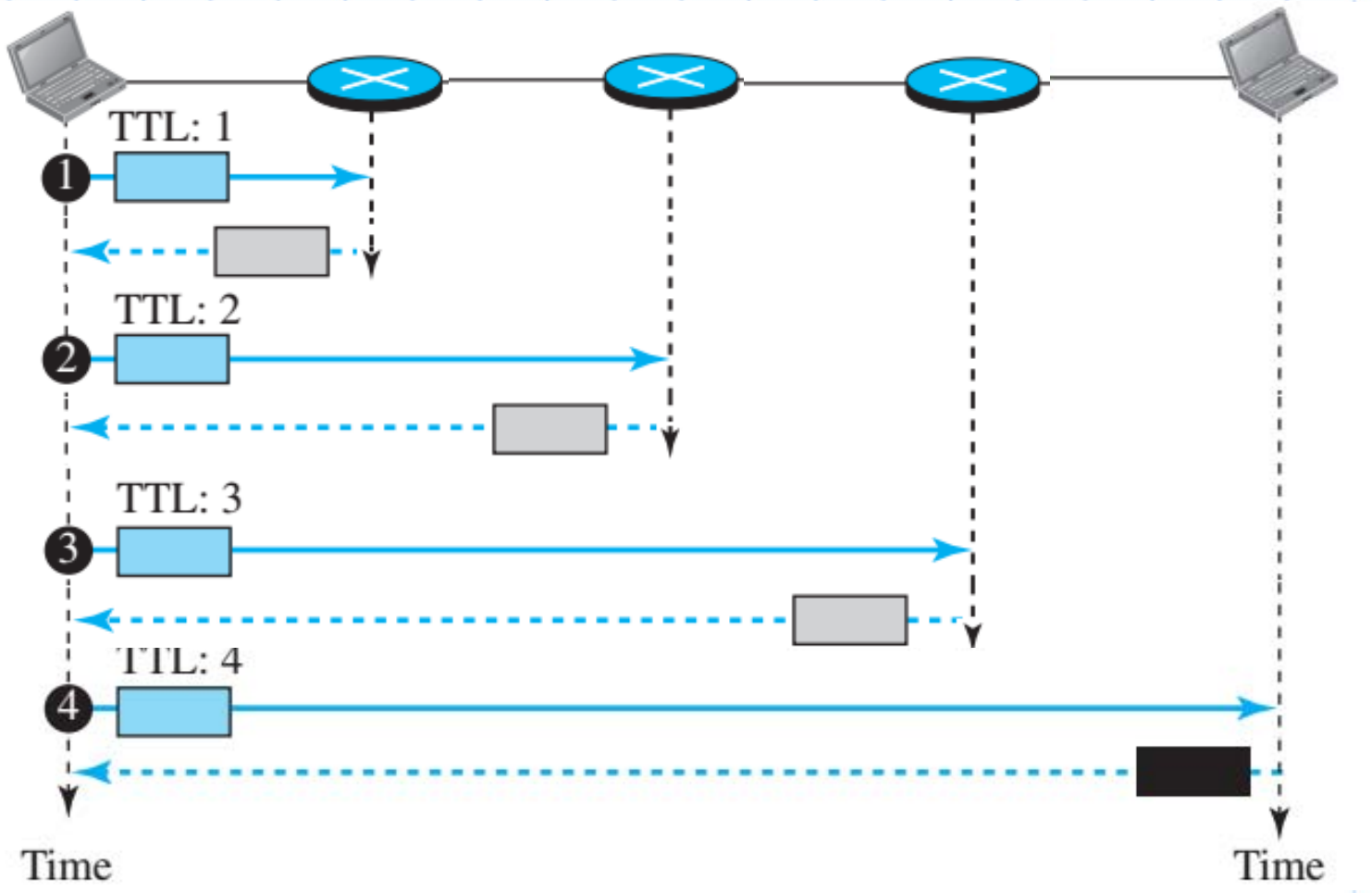


Important points about ICMP error messages

No ICMP error message will be generated

- in response to a datagram carrying an ICMP error message.
- for a fragmented datagram that is not the first fragment.
- for a datagram having a multicast address.
- for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

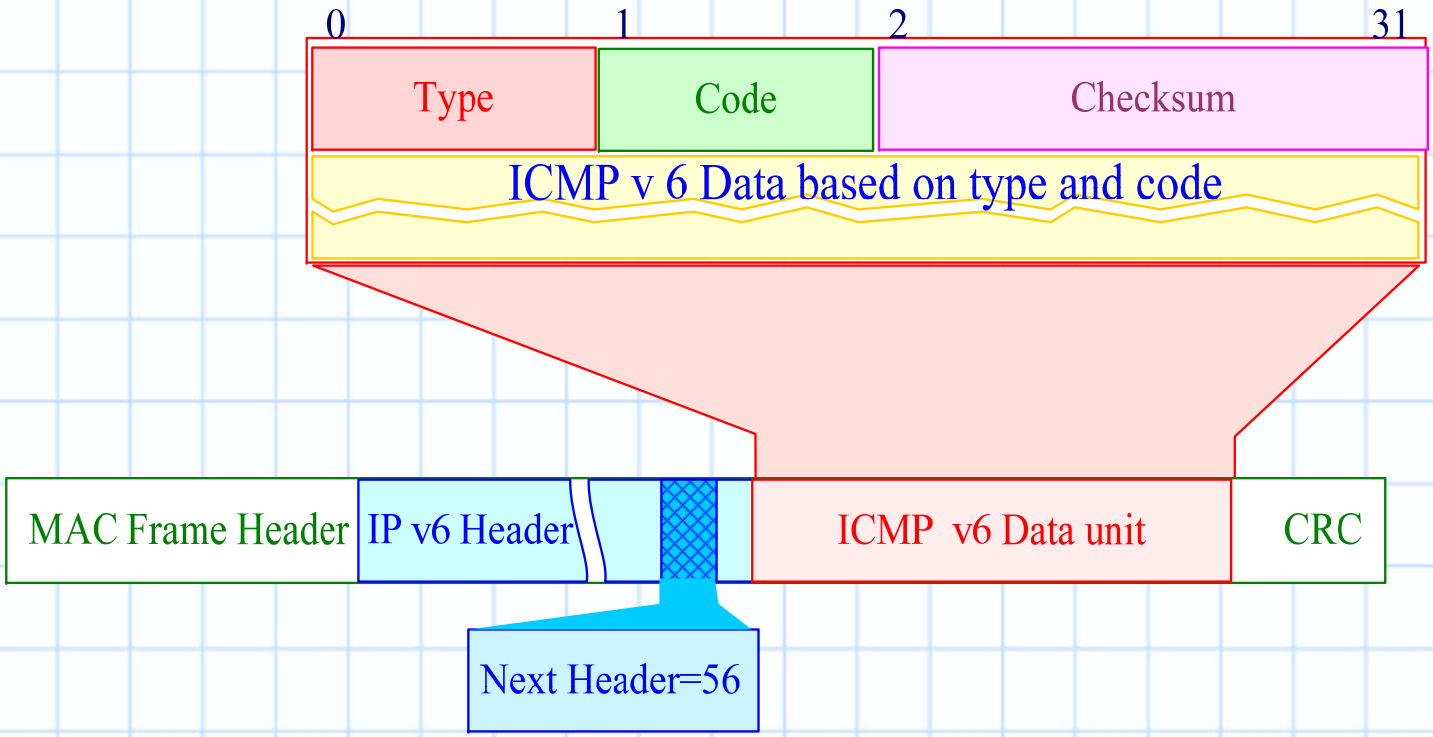
Use of ICMPv4 in traceroute



Important Note about ICMP error messages

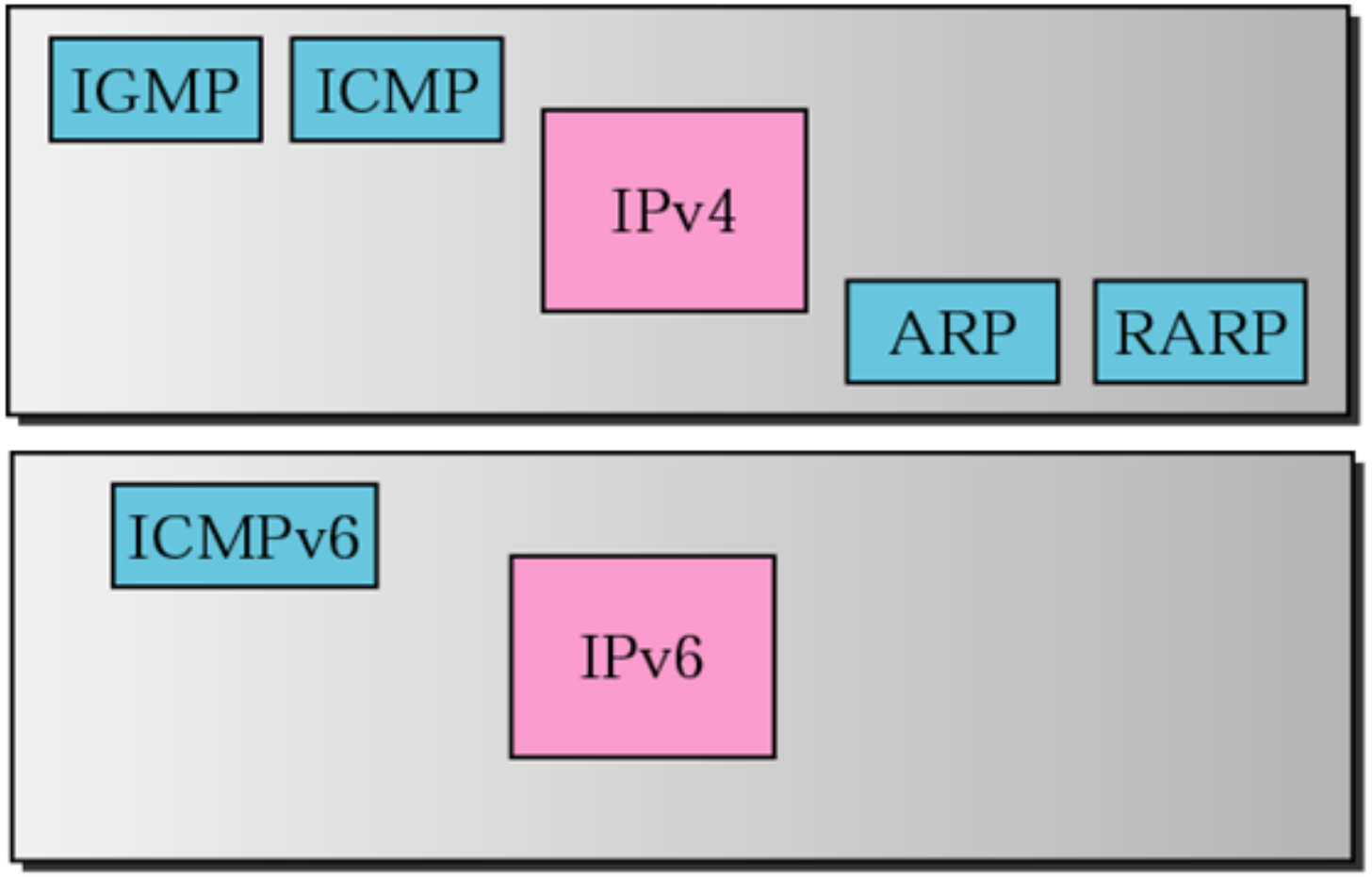
Note that all error messages contain a data section that includes the IP header of the original datagram plus the first 8 bytes of data in that datagram. The original datagram header is added to give the original source, which receives the error message, information about the datagram itself. The 8 bytes of data are included because the first 8 bytes provide information about the port numbers (UDP and TCP) and sequence number (TCP).

ICMP Version 6 Protocol



ICMP redirects can modify a router's routing table, so sometimes hackers try to subvert routers by issuing forged ICMP redirects in order to perform a denial of service attack.

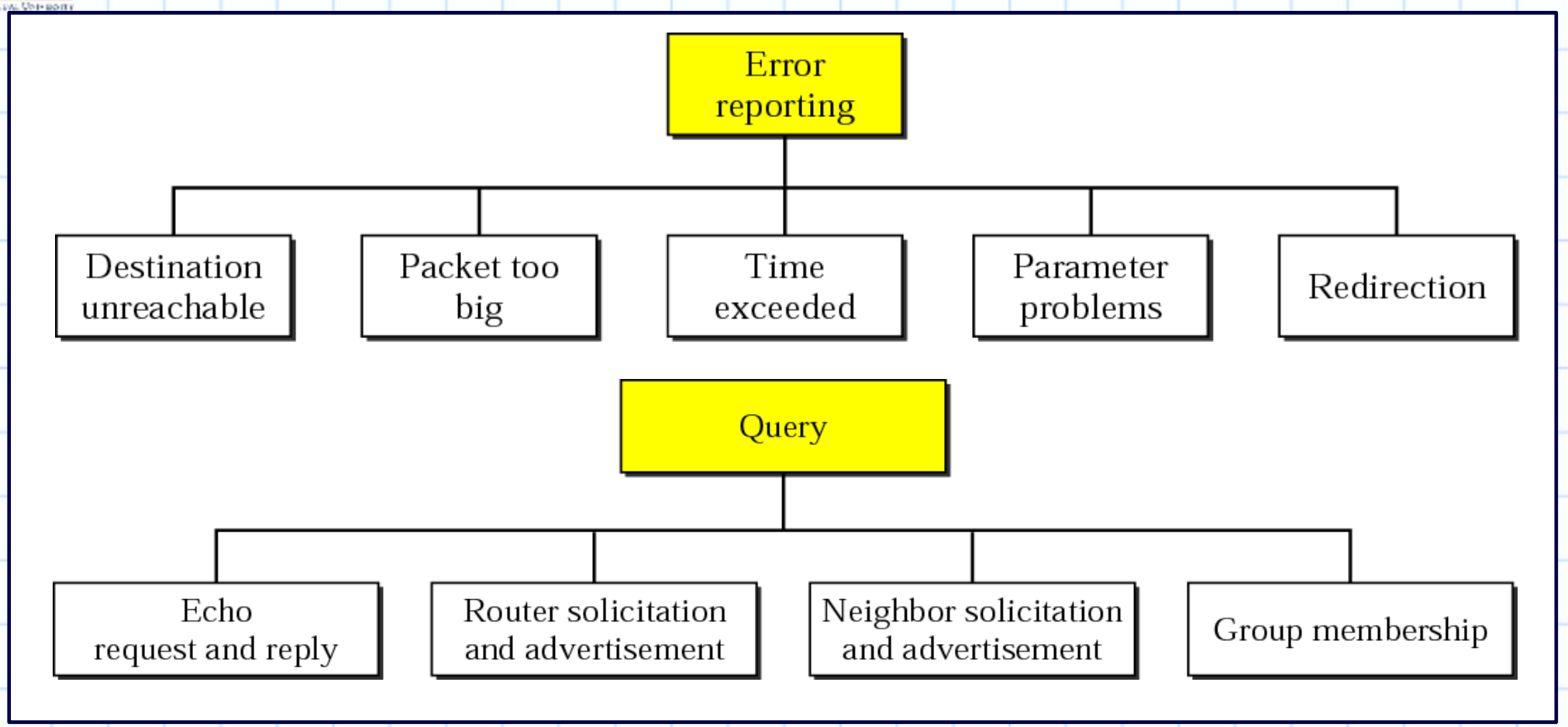
Network Layer in v4 & v6



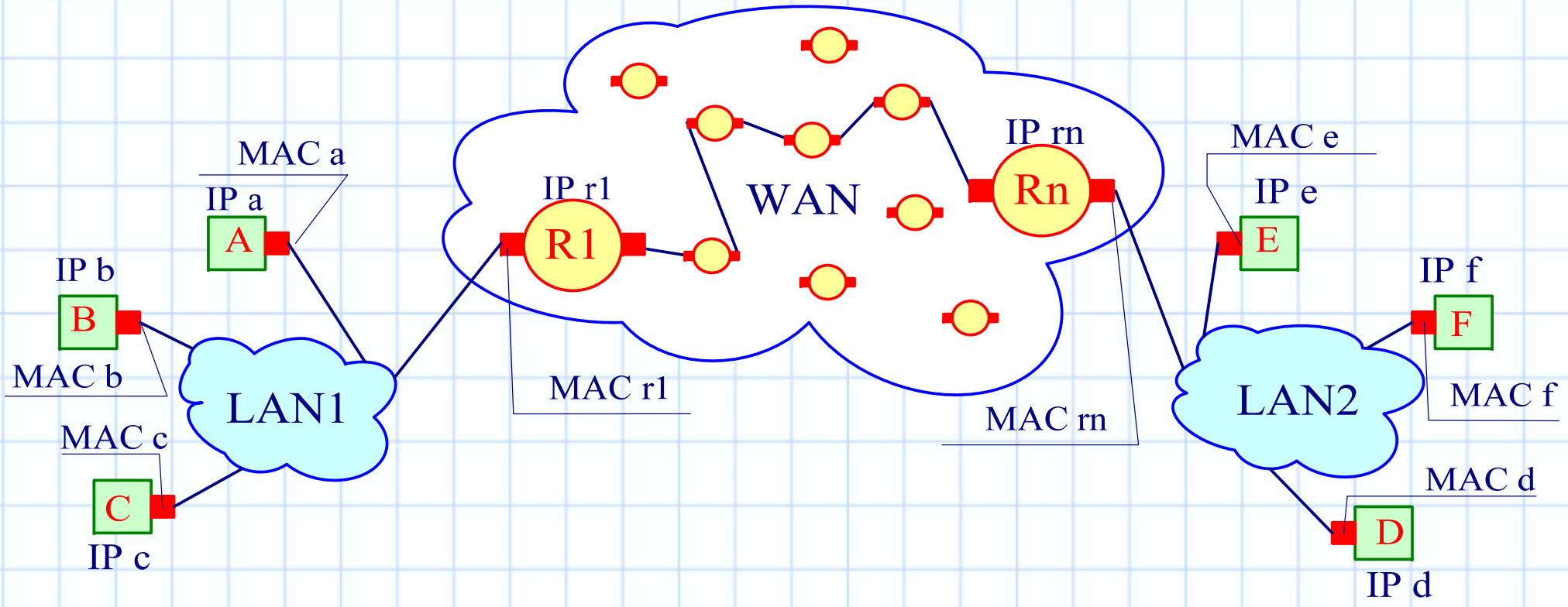
ICMPv6

- An integral part of IPv6 and MUST be fully implement by every IPv6 node (RFC 2463)
- Next Header value= 58
- Report delivery or forwarding errors
- Provide simple echo service for troubleshooting
- Neighbor Discovery (ND): 5 ICMP messages
- Multicast Listener Discovery (MLD): 3 ICMP messages

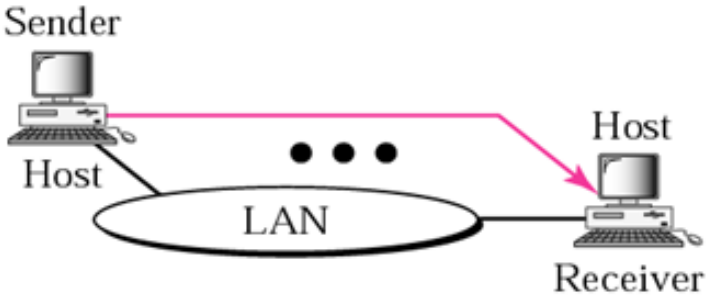
ICMPv6 Messages



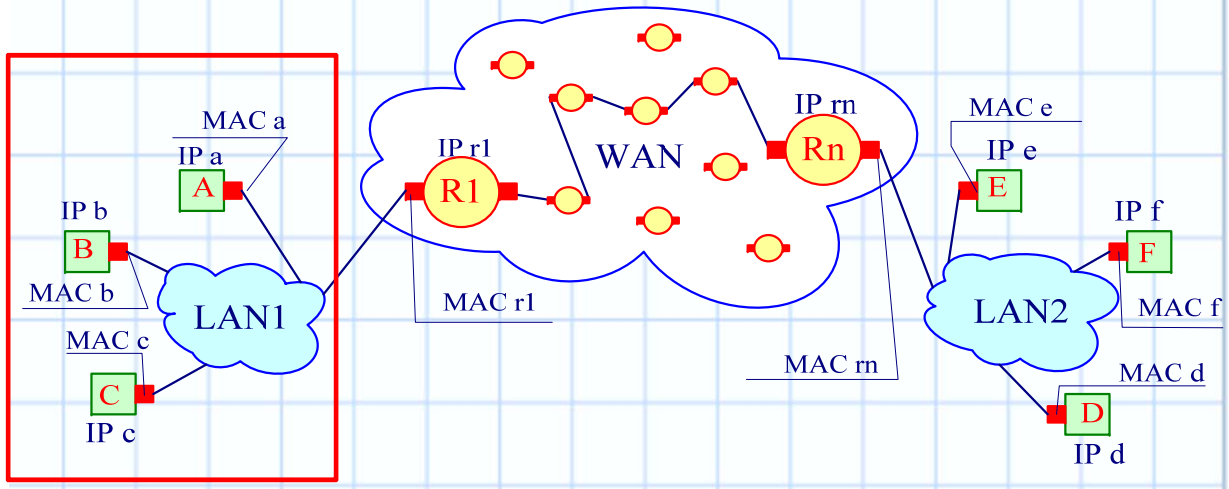
Address Resolution Protocol



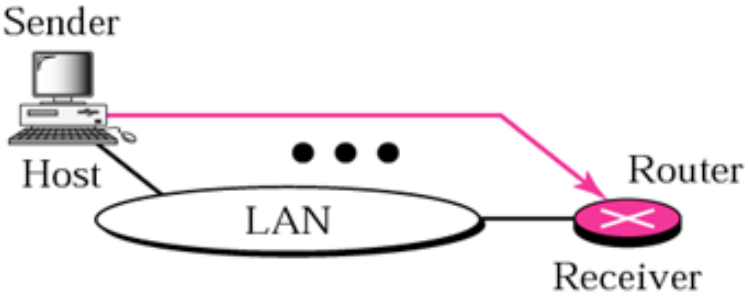
Target IP address:
Destination address in the IP datagram



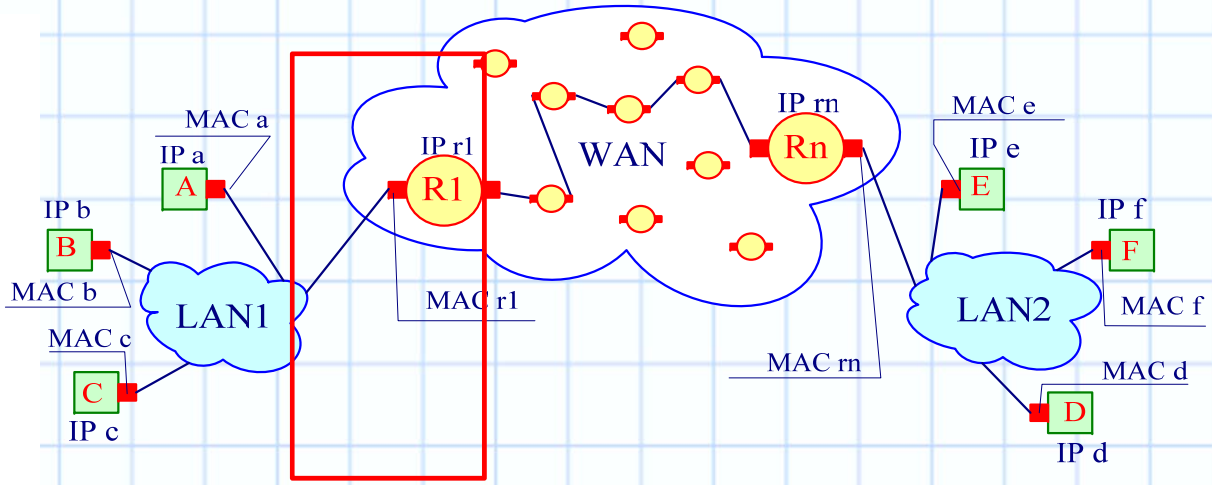
Case 1. A host has a packet to send to another host on the same network.



Target IP address:
IP address of a router

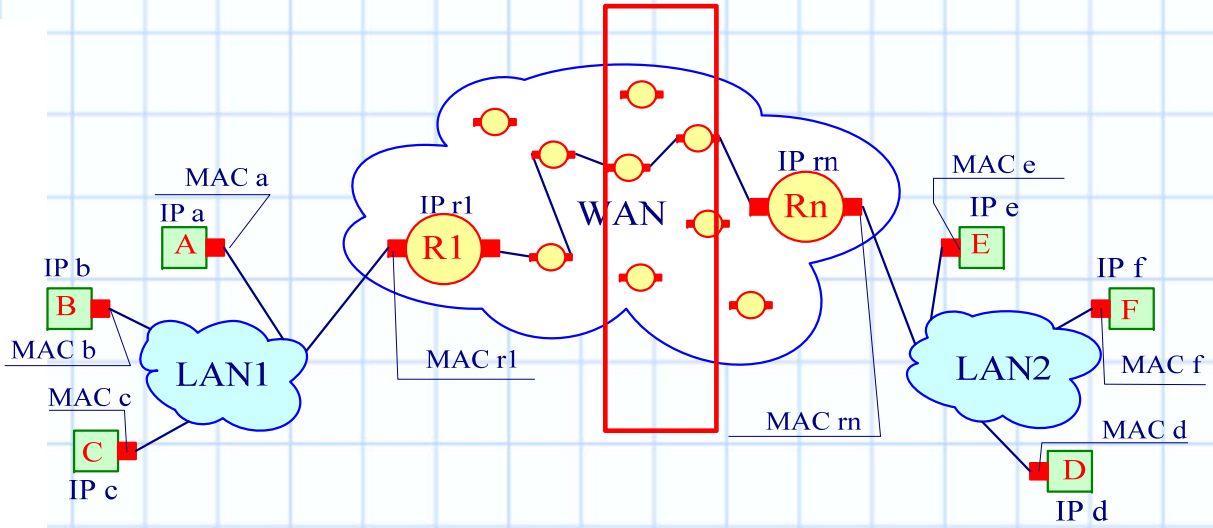


Case 2. A host wants to send a packet to another host on another network.
It must first be delivered to a router.

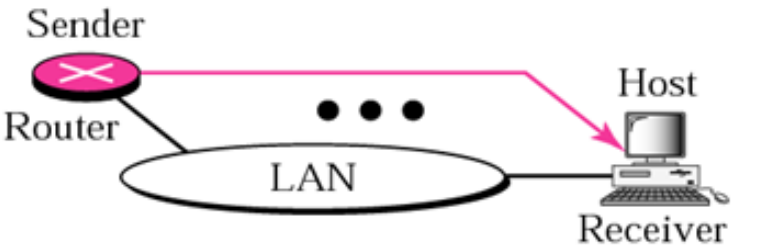


Target IP address:
IP address of the appropriate router
found in the routing table

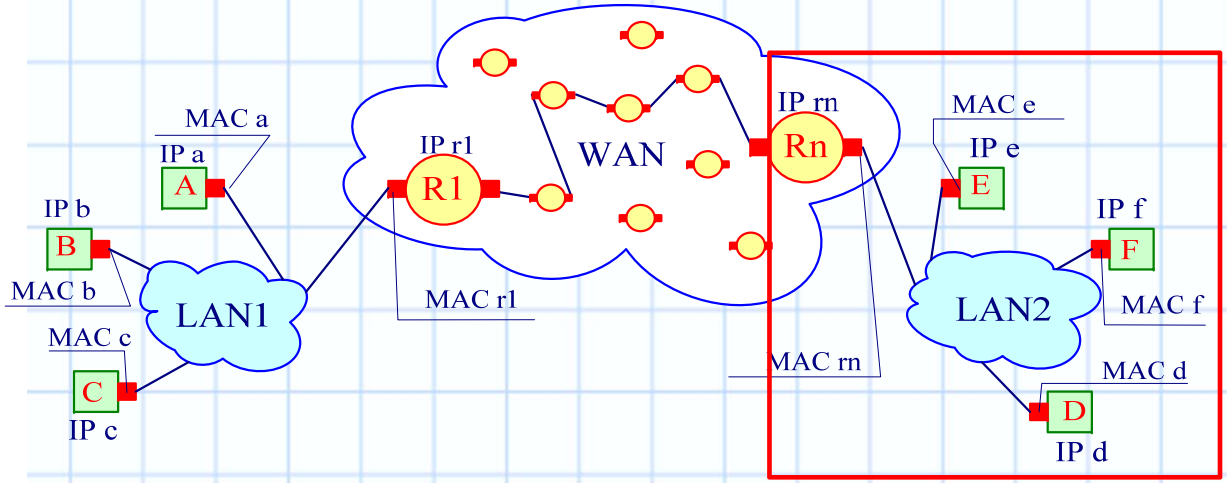
Case 3. A router receives a packet to be sent to a host on another network.
It must first be delivered to the appropriate router.



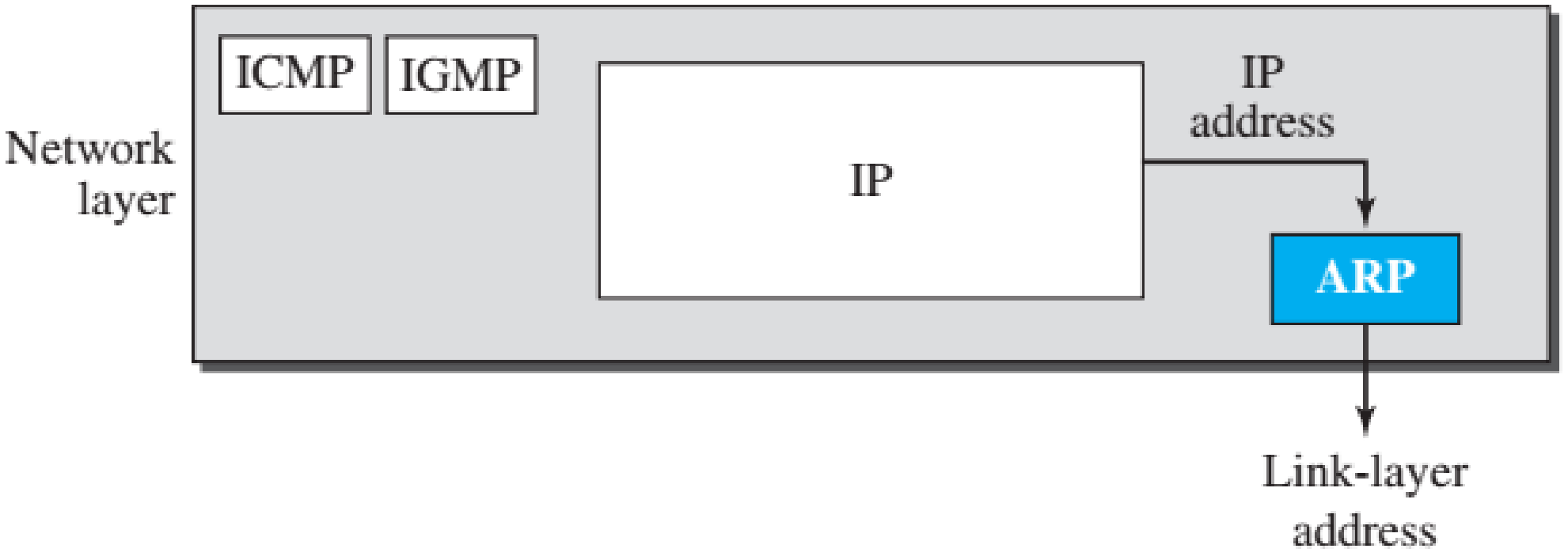
Target IP address:
Destination address in the IP datagram



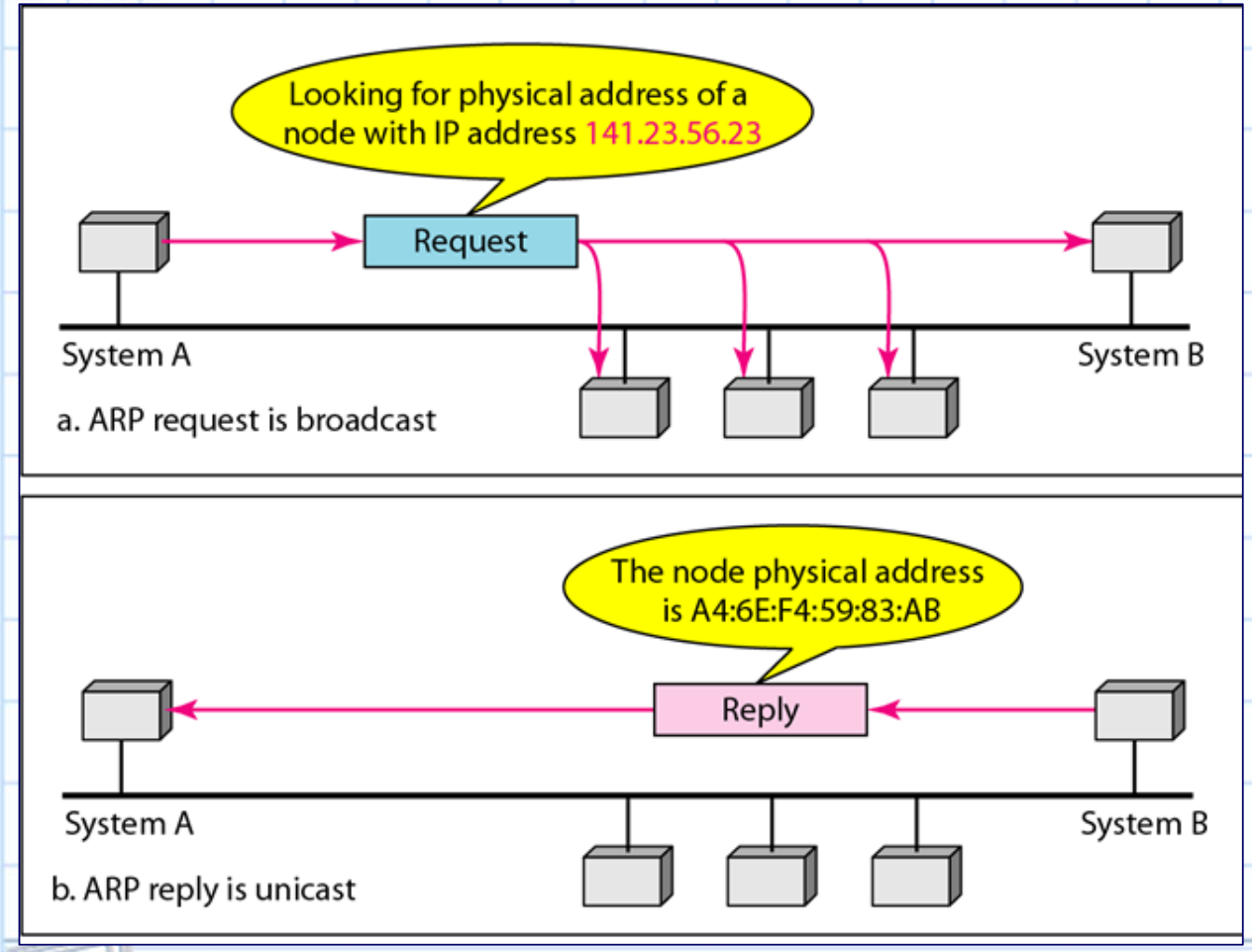
Case 4. A router receives a packet to be sent to a host on the same network.



Position of ARP in TCP/IP protocol suite



ARP operation



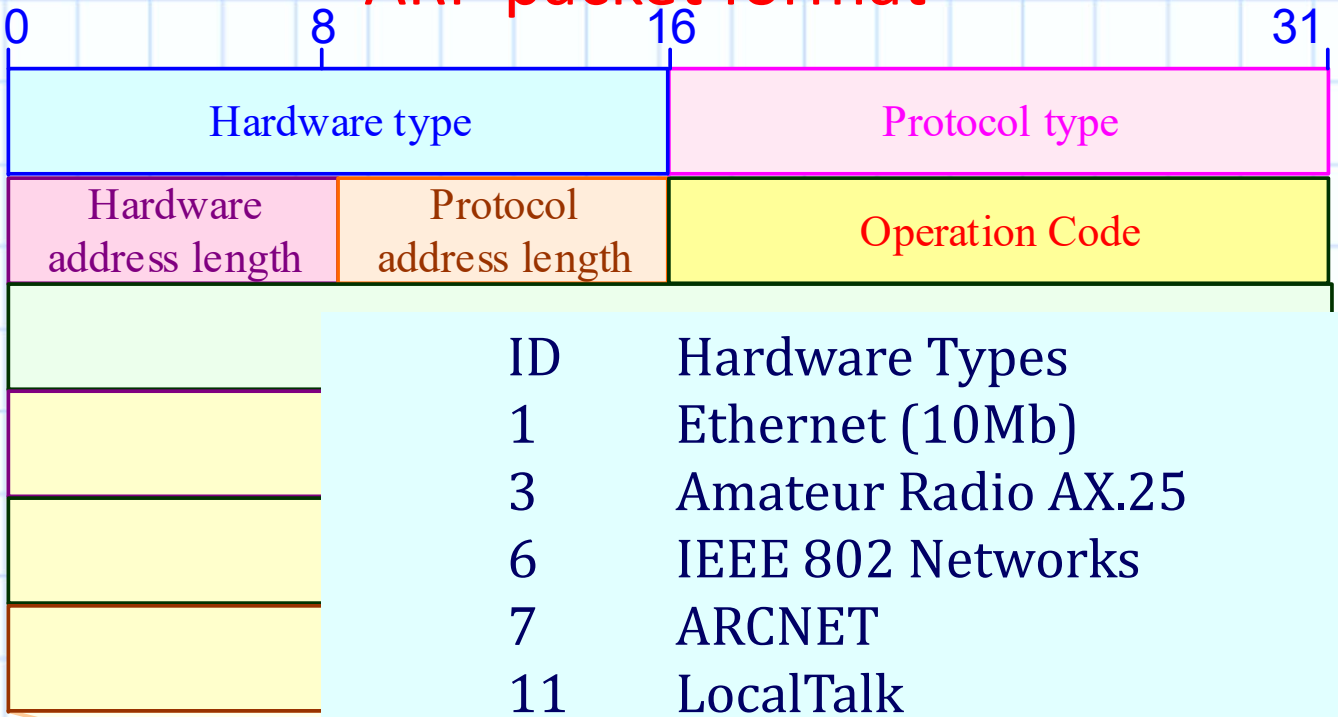
- Provides a dynamic mapping between 32-bit IP addresses and whatever type of address the data link uses.
- ARP module in each node has a table in its RAM called an ARP table

IP address	Physical address	TTL
IP b	MAC b	13:45:00
IP c	MAC c	13:52:00

Caching

If system A can broadcast a frame to find the link layer address of system B, why can't system A send the datagram for system B using a broadcast frame?

ARP packet format



ID	Hardware Types
1	Ethernet (10Mb)
3	Amateur Radio AX.25
6	IEEE 802 Networks
7	ARCNET
11	LocalTalk

Operation code

1= ARP request

2= ARP reply

3= RARP request

4= RARP reply

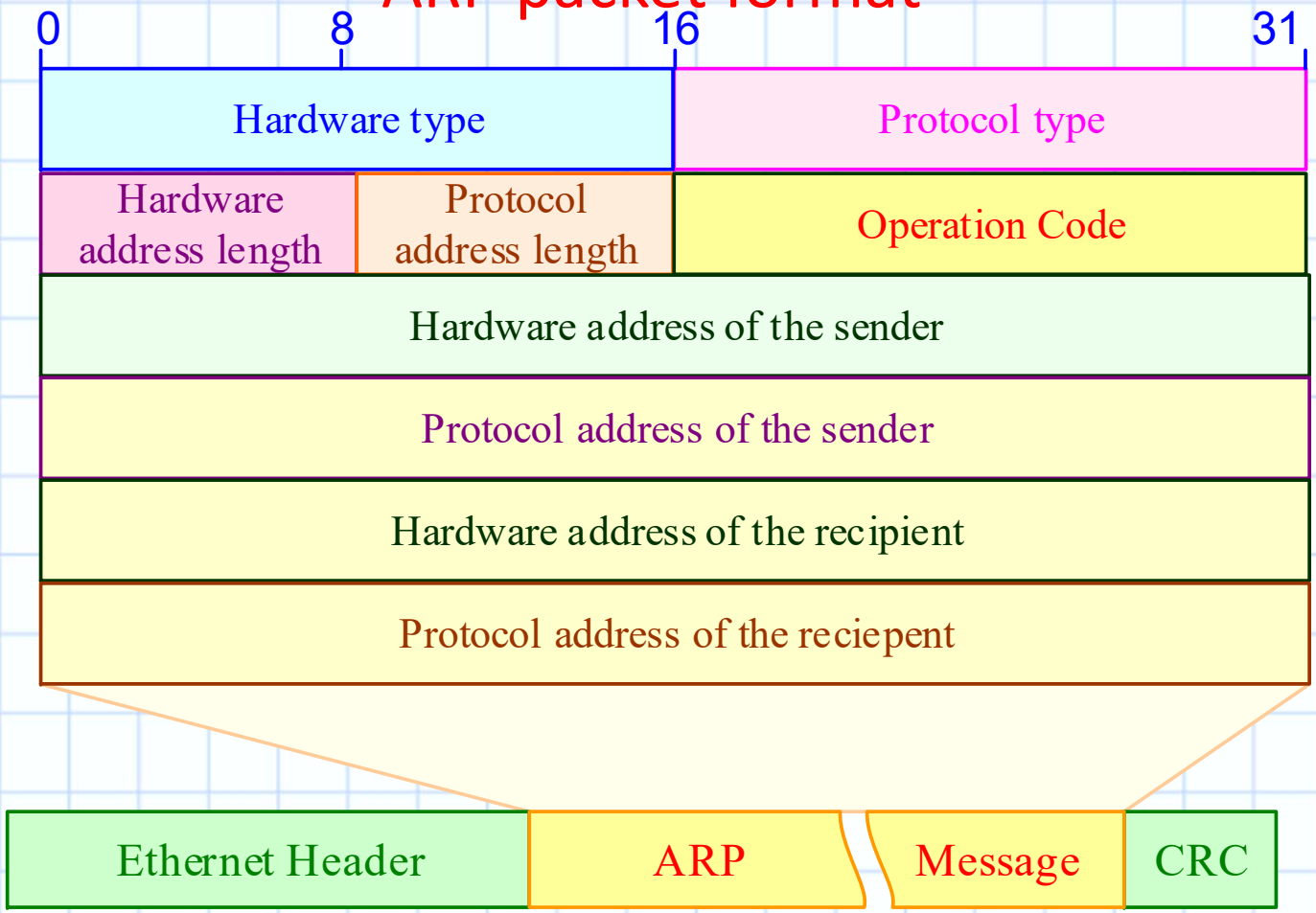
ion Mode (ATM)

Ethernet He

Recipient Hardware Add

Recipient IP Address: The

ARP packet format



ARP packet fields

- **Hardware type:** specifies the link protocol used on the LAN.
- **Protocol type:** specifies the network's protocol type.
- **Hardware address of the sender:** sets the length of a link address and the sender. By default, HS=6**.**
- **Protocol address of the sender:** sets the length of a network address. By default PS=4.
- **Operation code field:** specifies which operation is running.
- **Hardware Address Length:** the length of each hardware address in the datagram, given in bytes.
- **Protocol Address Length:** the length of the protocol address in the datagram, given in bytes.
- **Recipient Hardware Address:** The recipient hardware address is the hardware address of the recipient device.
- **Recipient IP Address:** The recipient IP address is the IP address of the recipient device.

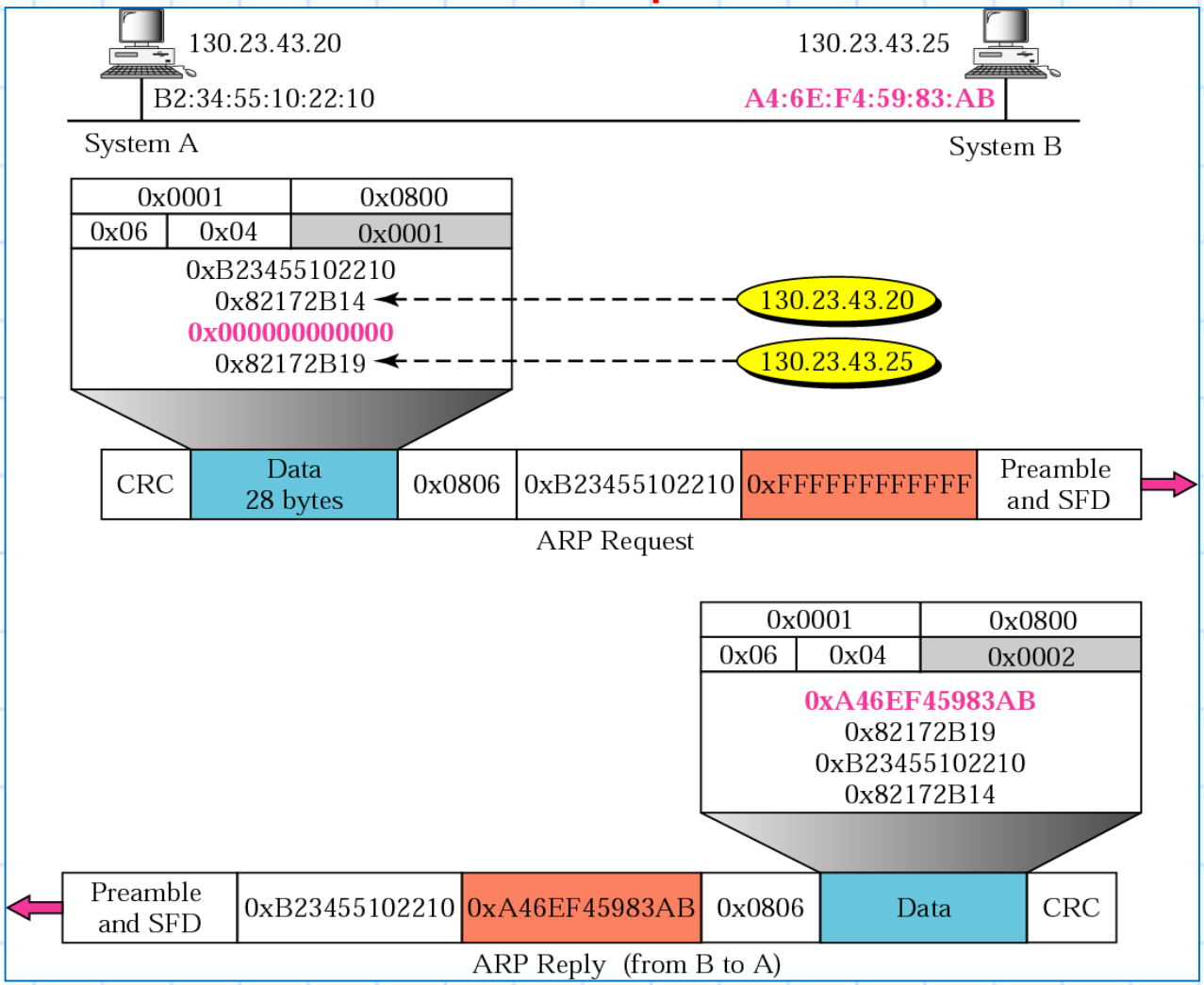
Example 1

- 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 (which is unknown to the first host). The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.

Solution

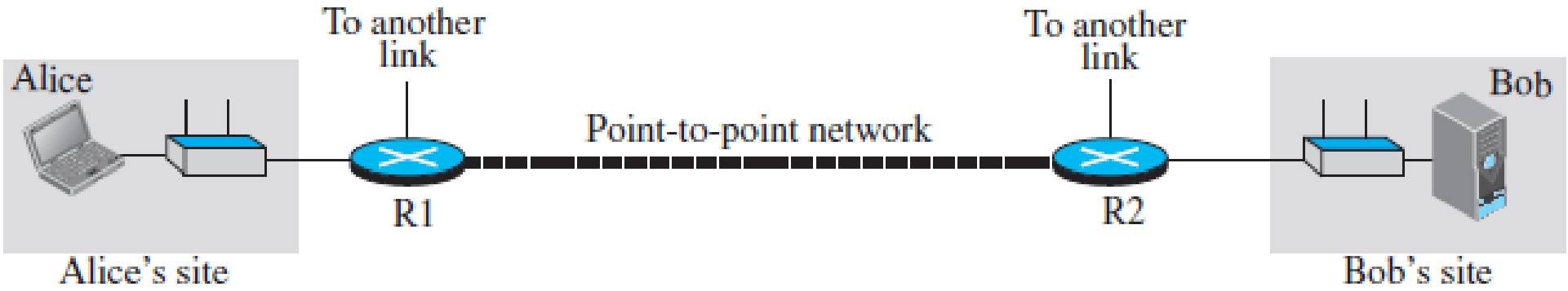
Note that the ARP data field in this case is 28 bytes, and that the individual addresses do not fit in the 4-byte boundary. That is why we do not show the regular 4-byte boundaries for these addresses. Also note that the IP addresses are shown in hexadecimal.

Example

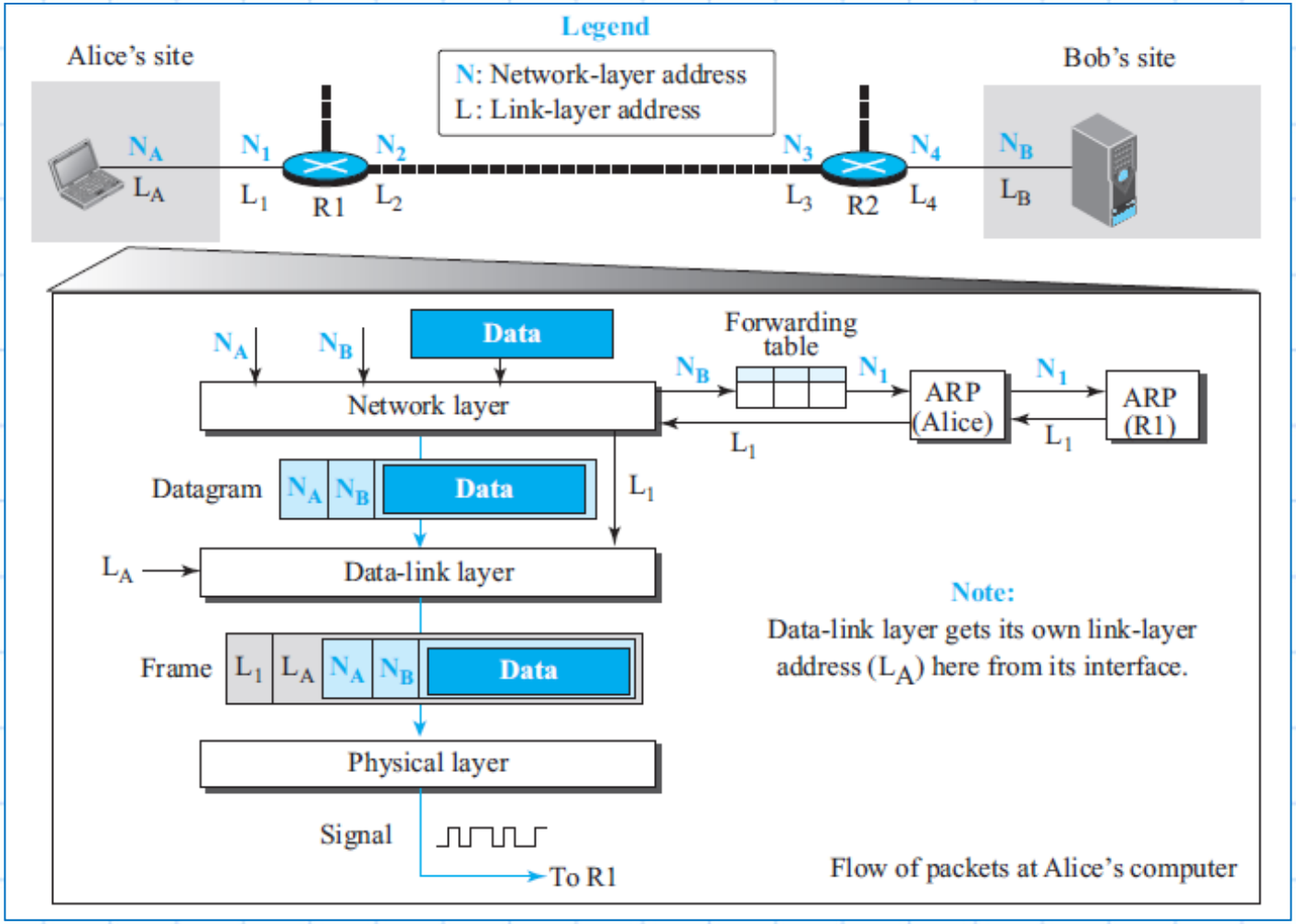

130.23.43.20
B2:34:55:10:22:10
System A
130.23.43.25
A4:6E:F4:59:83:AB
System B
0x0001
0x0800
0x06
0x04
0x0001
0xB23455102210
0x82172B14
0x000000000000
0x82172B19
130.23.43.20
130.23.43.25
CRC
Data
28 bytes
0x0806
0xB23455102210
0xFFFFFFFFFFFF
Preamble
and SFD
ARP Request
0x0001
0x0800
0x06
0x04
0x0002
0xA46EF45983AB
0x82172B19
0xB23455102210
0x82172B14
Preamble
and SFD
0xB23455102210
0xA46EF45983AB
0x0806
Data
CRC
ARP Reply (from B to A)

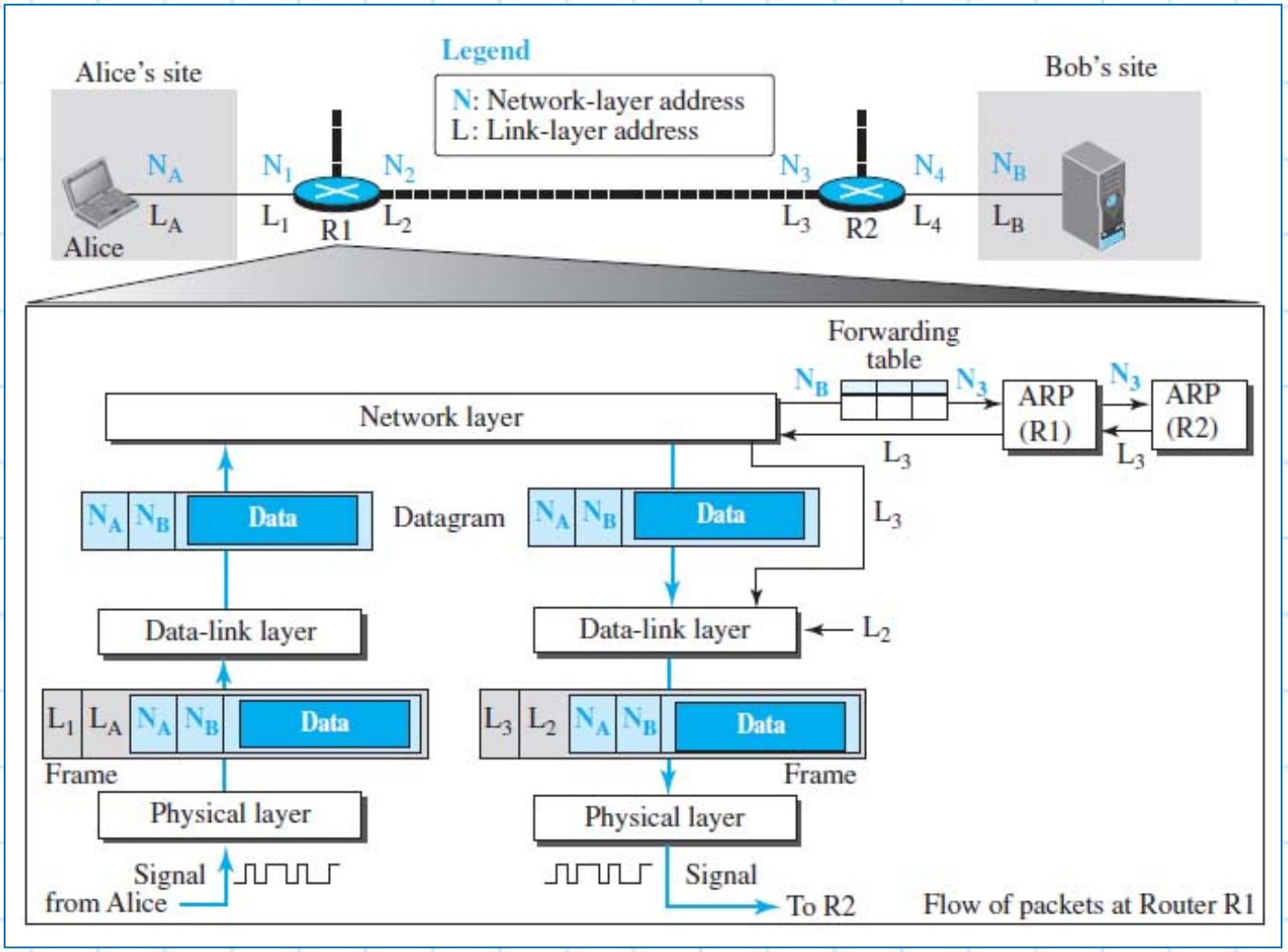
Example

- Assume Alice needs to send a datagram to Bob, who is three nodes away in the Internet. Assume that Alice knows the network-layer (IP) address of Bob. In other words, Alice's host is given the data to be sent, the IP address of Bob, and the IP address of Alice's host (each host needs to know its IP address).

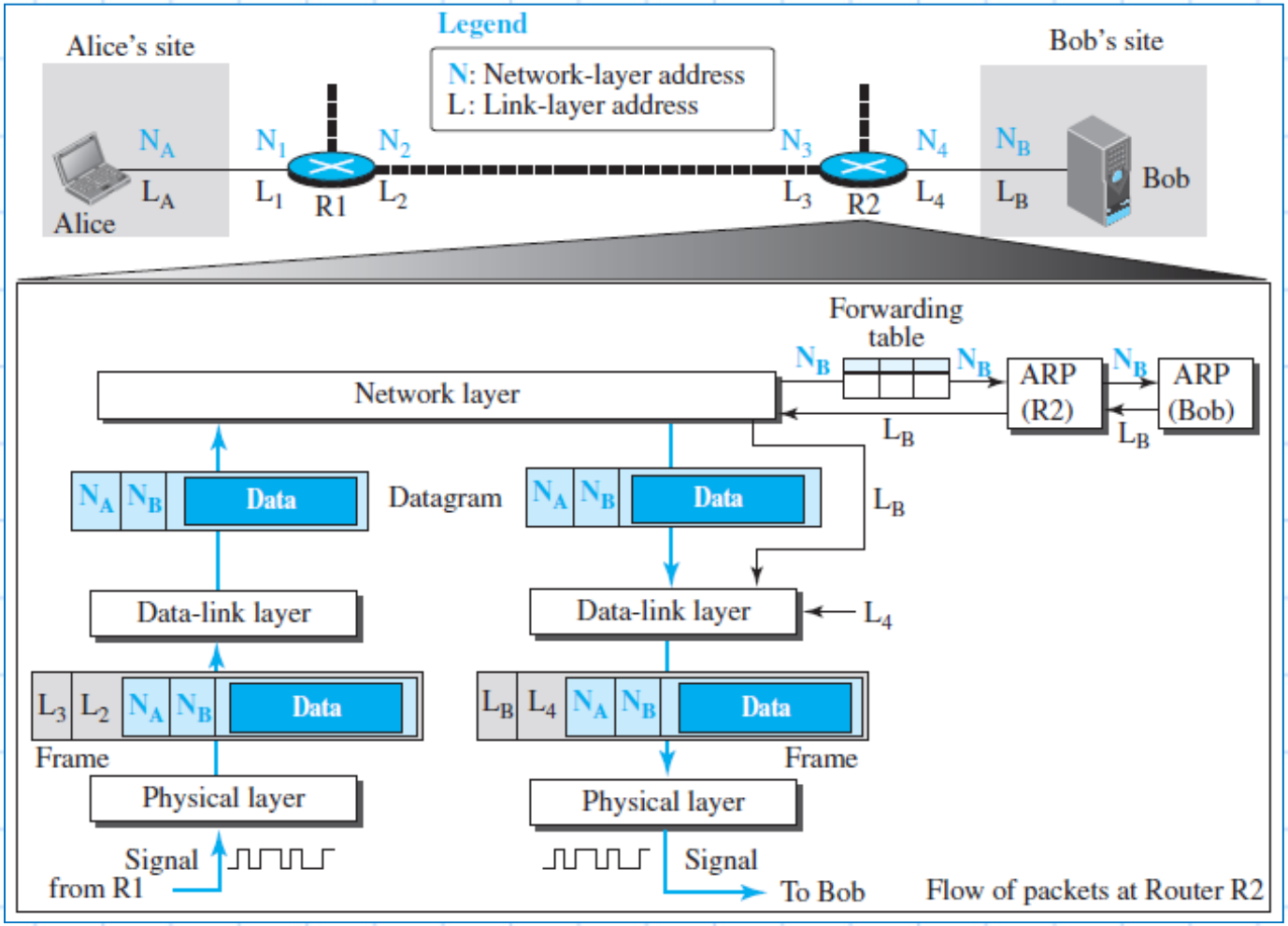


Example

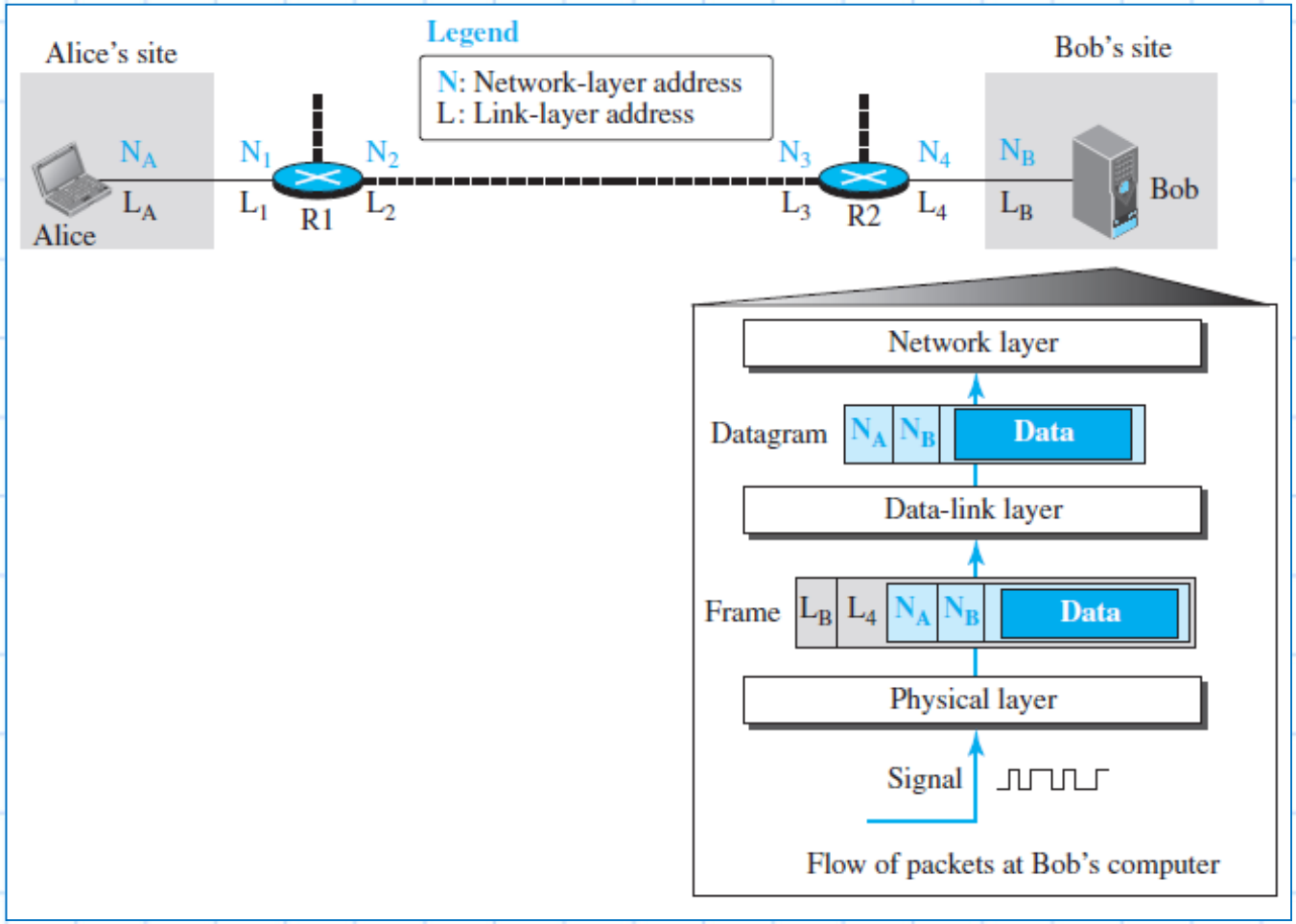

Legend
N: Network-layer address
L: Link-layer address
Alice's site
Bob's site
N_A
L_A
N_1
L_1
R1
N_2
L_2
N_3
L_3
R2
N_4
L_4
N_B
L_B
Data
Forwarding table
Network layer
ARP (Alice)
ARP (R1)
Datagram
Data-link layer
Frame
Physical layer
Signal
To R1
Note:
Data-link layer gets its own link-layer address (L_A) here from its interface.
Flow of packets at Alice's computer


Legend
N: Network-layer address
L: Link-layer address
Alice's site
Bob's site
Alice
R1
R2
Forwarding table
Network layer
ARP (R1)
ARP (R2)
Datagram
Data
Data-link layer
Frame
Physical layer
Signal from Alice
Signal
To R2
Flow of packets at Router R1

Example


Legend
N: Network-layer address
L: Link-layer address
Alice's site
Bob's site
Alice
Bob
R1
R2
Forwarding table
Network layer
ARP (R2)
ARP (Bob)
Datagram
Data
Data-link layer
Frame
Physical layer
Signal
from R1
To Bob
Flow of packets at Router R2

Example


Legend
N: Network-layer address
L: Link-layer address
Alice's site
Bob's site
N_A
L_A
Alice
N_1
L_1
R1
N_2
L_2
N_3
L_3
R2
N_4
L_4
N_B
L_B
Bob
Network layer
Datagram
N_A
N_B
Data
Data-link layer
Frame
L_B
L_4
N_A
N_B
Data
Physical layer
Signal
Flow of packets at Bob's computer