Chapter 1

Introduction

1.1

A BRIEF HISTORY

Time Line

The following is a list of important Internet events in chronological order:

1969. Four-node ARPANET established.

1970. ARPA hosts implement NCP.

1973. Development of TCP/IP suite begins.

1977. An internet tested using TCP/IP.

1978. UNIX distributed to academic sites.

1981. CSNET established.

1983. TCP/IP becomes the official protocol

1983. MILNET was born.

1986. NSFNET established.

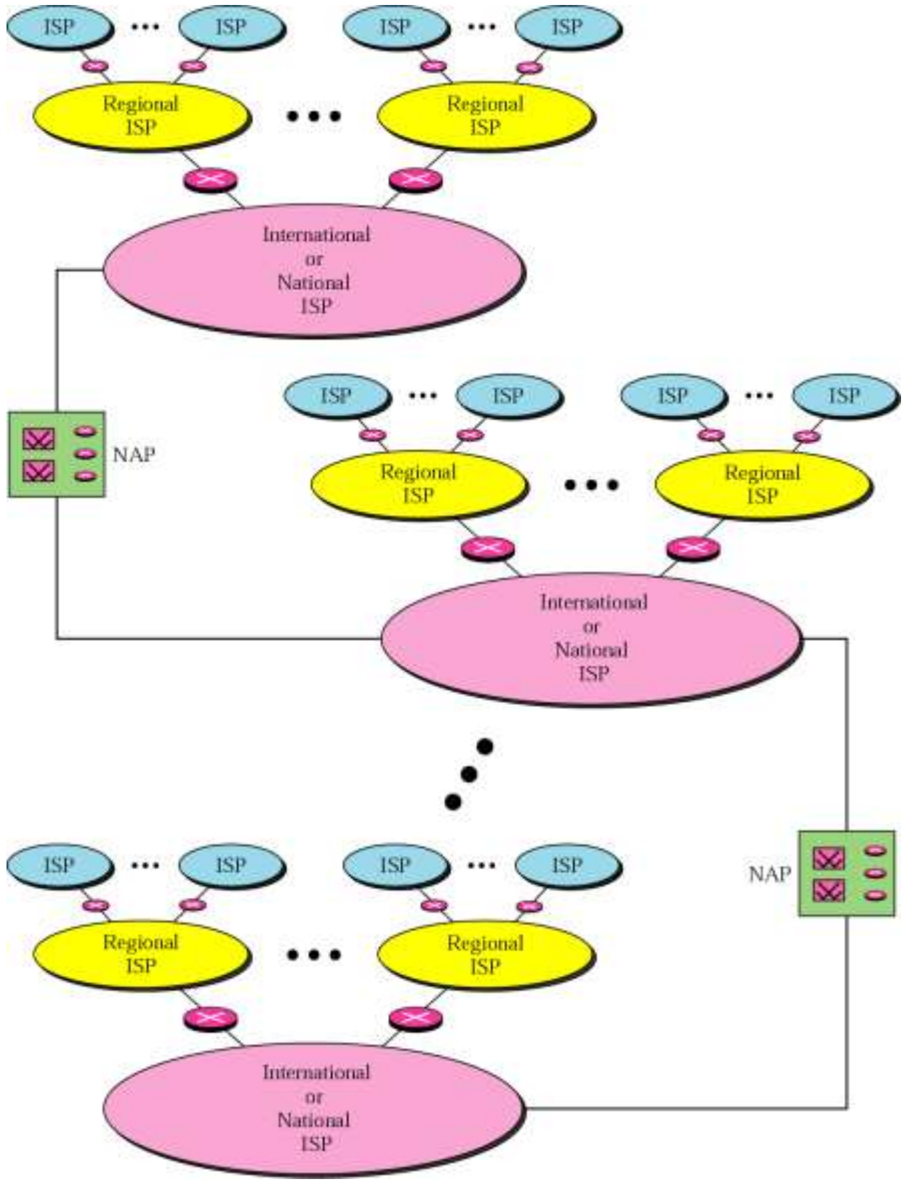
1990. ARPANET replaced by NSFNET.

1995. NSFNET became a research network.

1995. **ISPs** started.

Figure 1-1

Internet today



Cont…

- International ISPs :that connect nations together.
- Nationals ISPs :there are many nationals ISPs operating in north America :some of the most well-known are Sprintlink, PSINet ,UUNet technology ,AGIS.
- regional ISPs: are small ISPs that are connected to one or more national ISPs.
- Local ISPs: provide direct service to the end user .it can be connects to regional ISPs or directly to national ISPs.

1.2

PROTOCOLS AND STANDARDS

Protocols

- Is a set of rules that governs data communications . A protocol defines what is communicated , how its communicated, and when it is communicated.
- Key element of protocol:

1. syntax :refers to the structure or format of the data , meaning the order in which presented .
2. Semantics: refers the meaning of each sections of bits .
3. timing :refers to the two characteristics: when data should be sent and how fast it can be sent.

Figure 1.7 *Categories of topology*

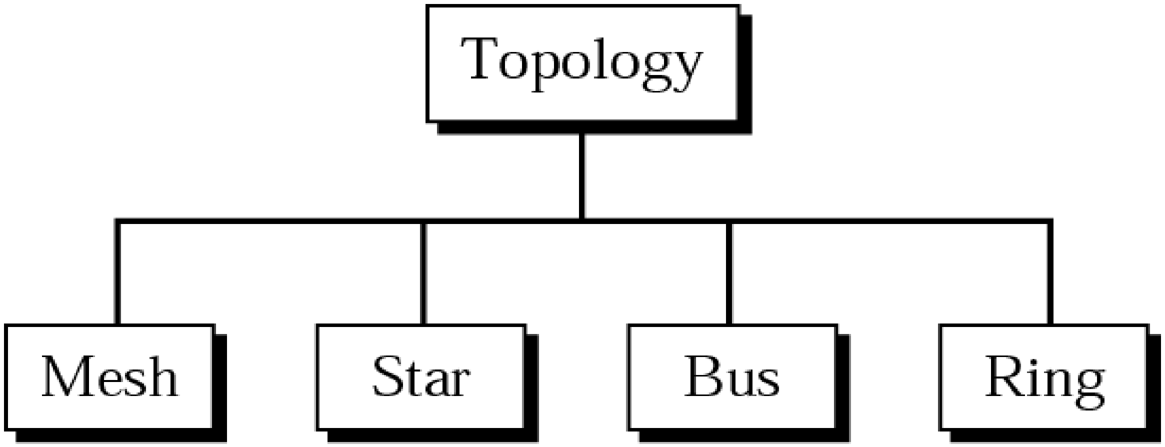
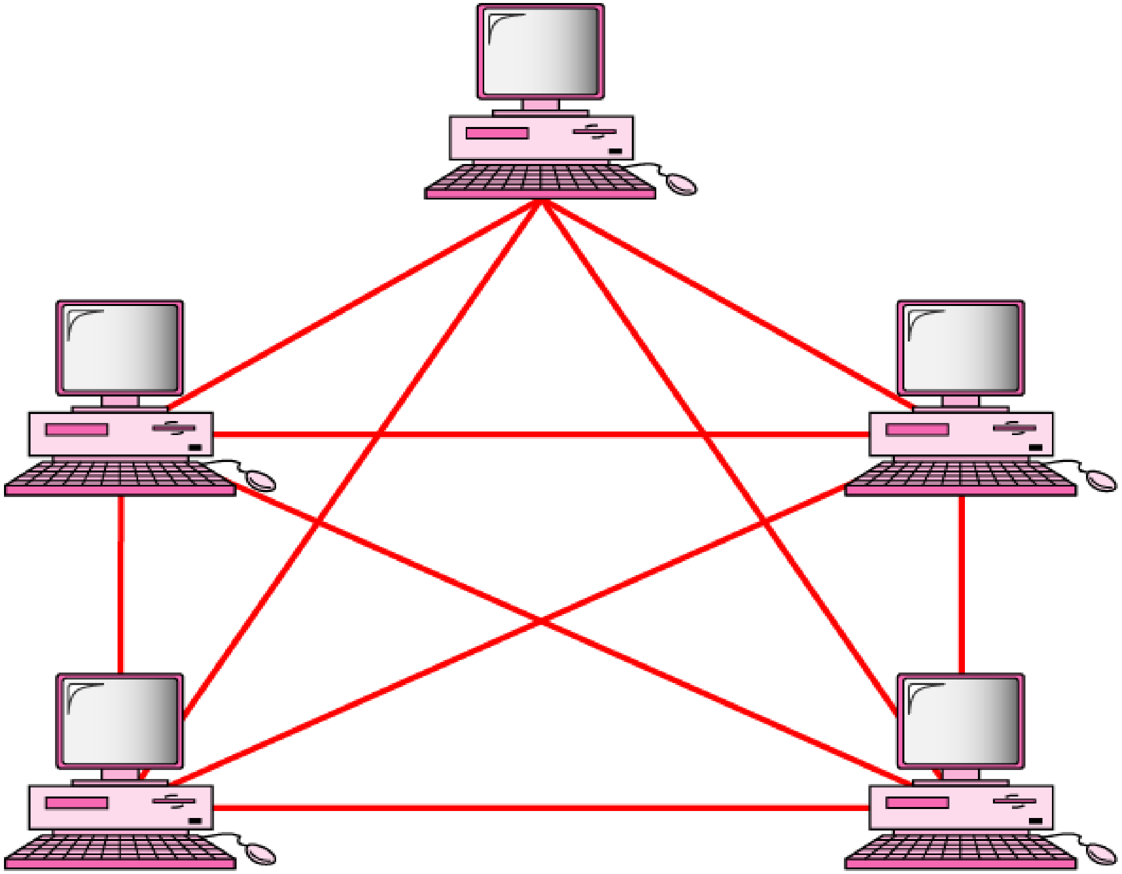


Figure 1.8 ***Fully connected mesh topology (for five devices)***



Mesh con…

- Every device has a dedicated point to point link to every other device.
- To find the number of physical links in a fully connected mesh network n(n-1)/2.

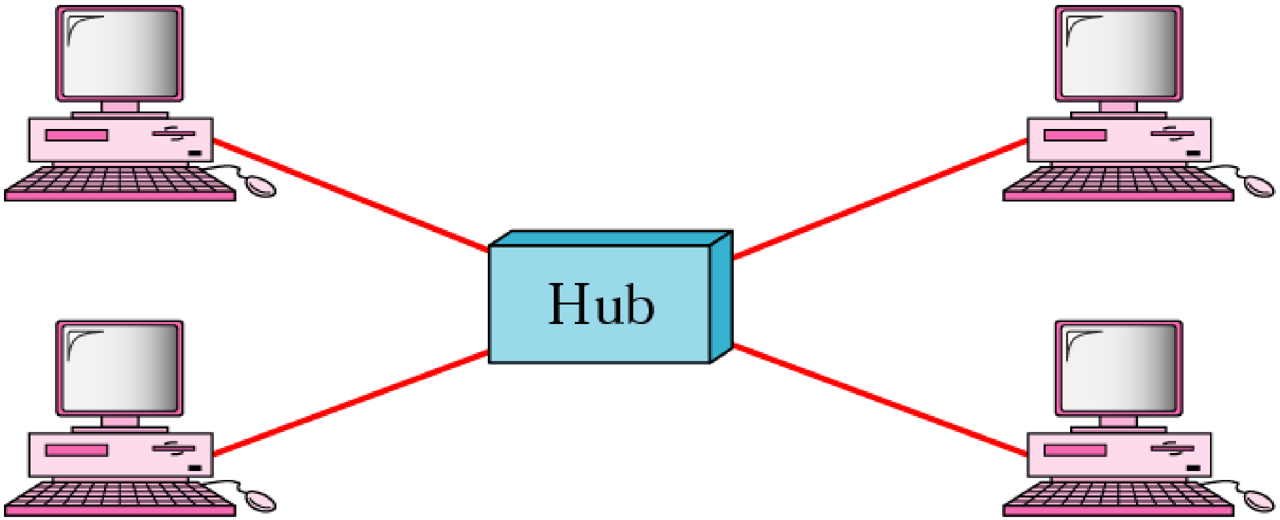
- **Advantage** :

1. the use of a dedicated link guarantees that each connections can carry its own data load
2. mesh topology is robust.
3. advantage of privacy and security.
4. point to point link make fault identification and isolation easy.

Disadvantages :

1. cabling and the number of I/O ports required .
2. the HW required to connect each link can be prohibitively expensive .

Figure 1.9 *Star topology*



Star topology

- each device has a dedicated point to point link only to a central controller.

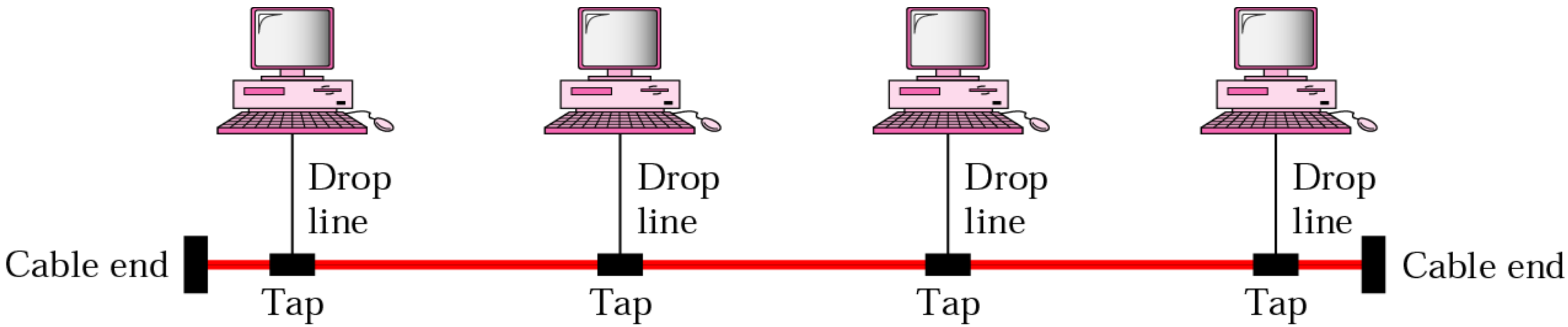
Advantages :

1. Less expensive than mesh topology .
2. Easy to install and reconfigure .
3. Robust .
4. Easy fault identification and isolation.

Disadvantages:

1. big disadvantage of star topology is dependency of the whole topology on one single point.
2. more cabling required .

Figure 1.10 *Bus topology*



Bus topology

- Its multipoint
- one long cable acts as link all the devices in the network.

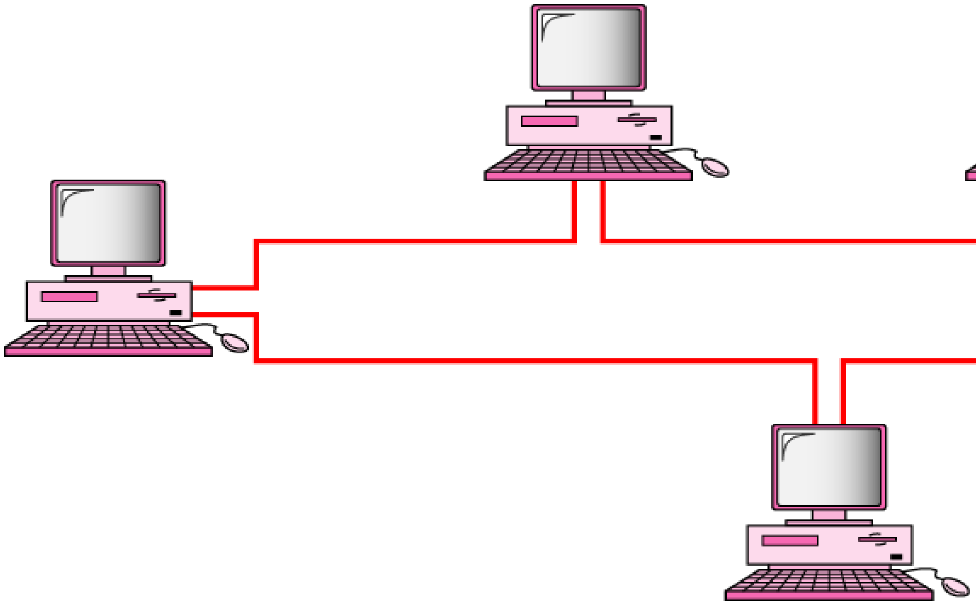
Advantage :

1. Easy of installations.
2. a bus use less cabling .

Disadvantages :

1. Difficult reconnections and fault isolation.
2. Difficult to add new devices.
3. Singles reflections at the taps can cause degradation in quality.
4. Fault or break on the bus cable stops all transmissions .

Figure 1.11 *Ring topology*



Ring topology

- Each device has a dedicated point to point connection with only the two devices on either side of it .

Advantages:

1. easy to install and reconfigure
2. fault isolations is simplified .

Disadvantages:

1. Media and traffic
2. Unidirectional
3. a break in the ring can disable the entire network.

Figure 1.12 *Categories of networks*

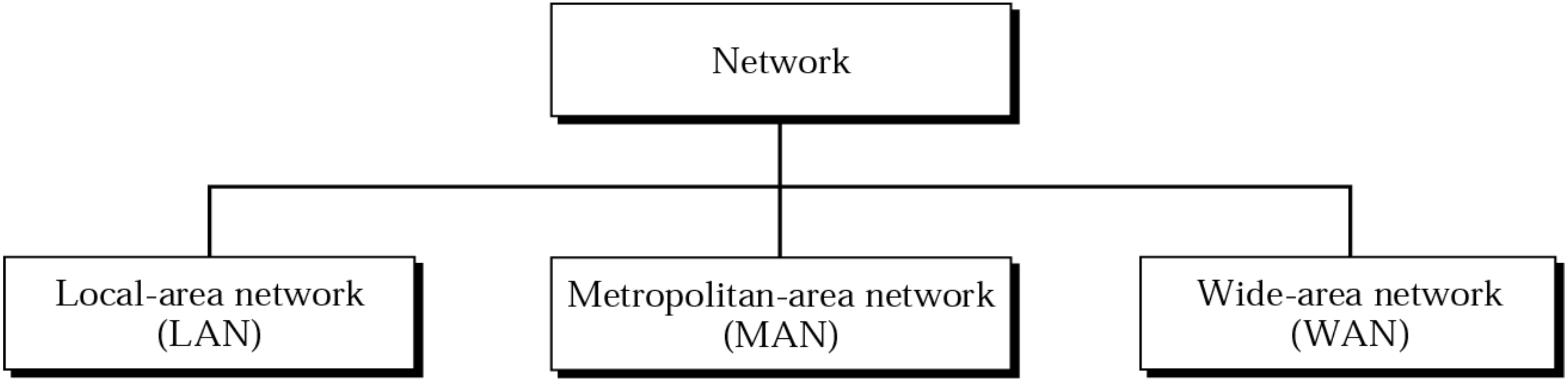
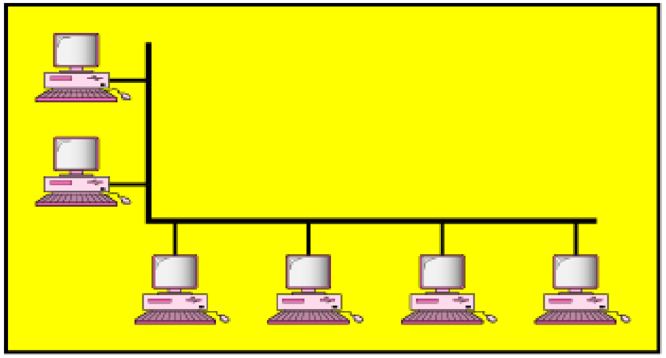
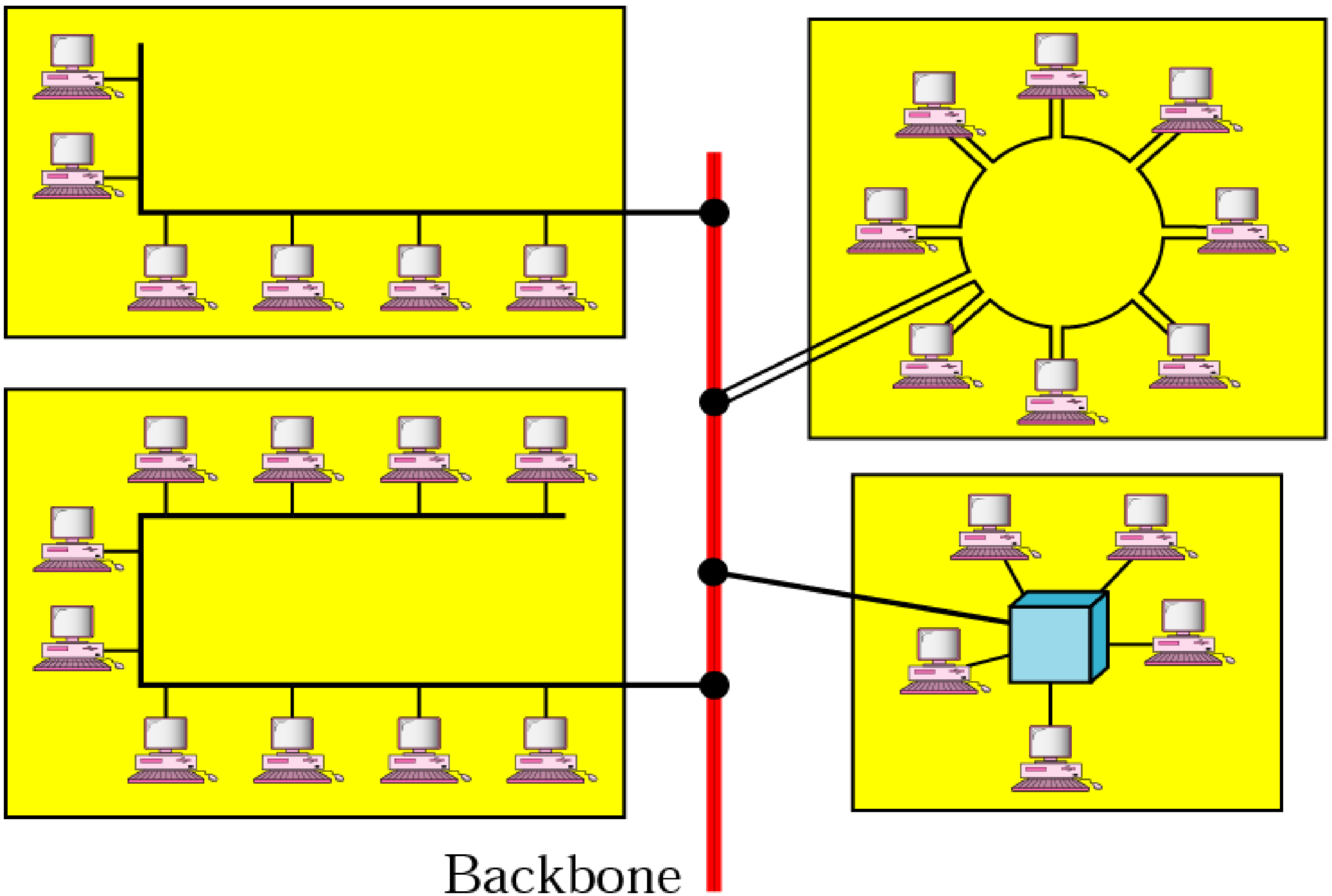


Figure 1.13 *LAN*



a. Single-building LAN

Figure 1.13 *LAN (Continued)*



b. Multiple-building LAN

Figure 1.14 *MAN*

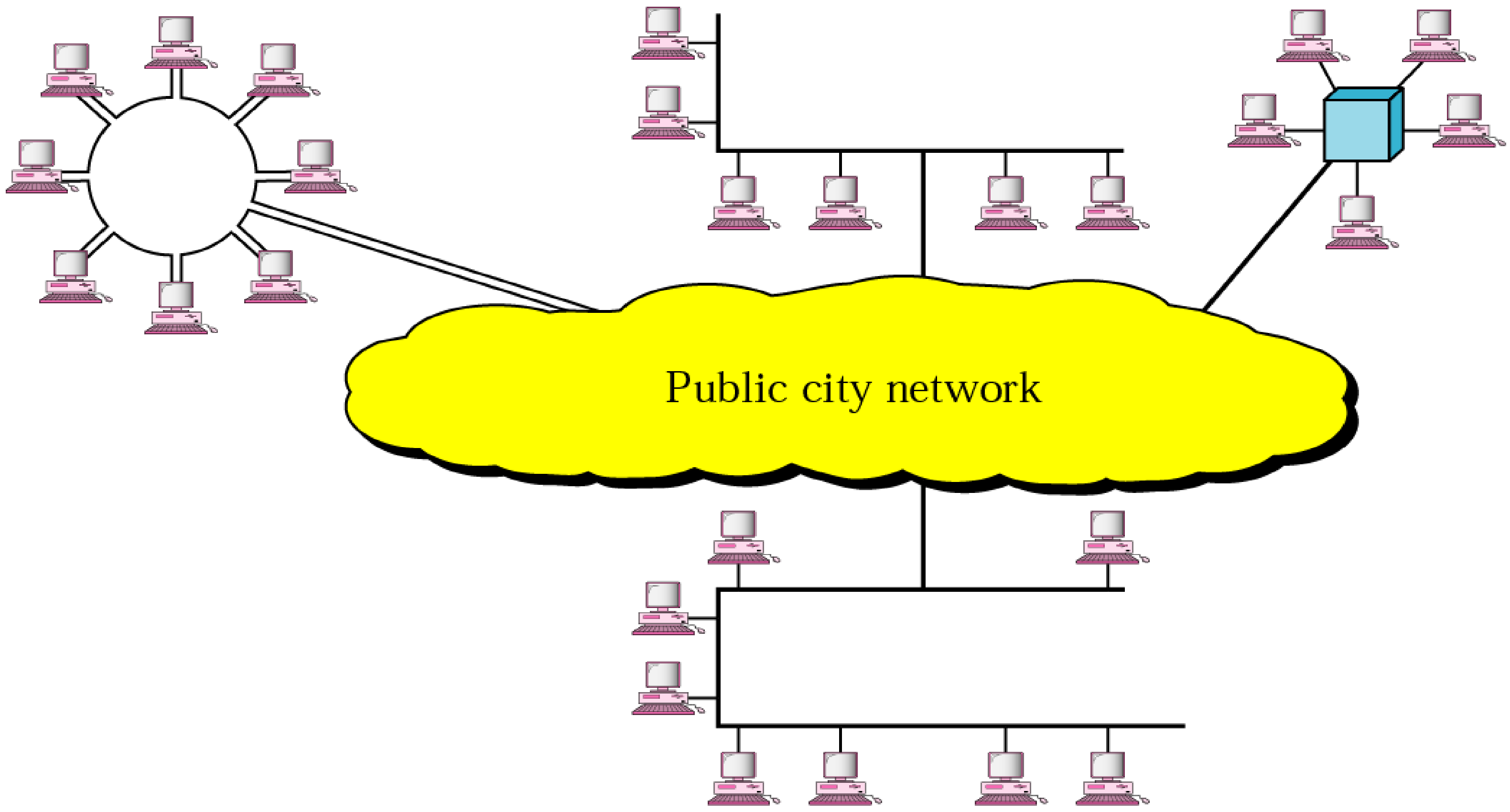
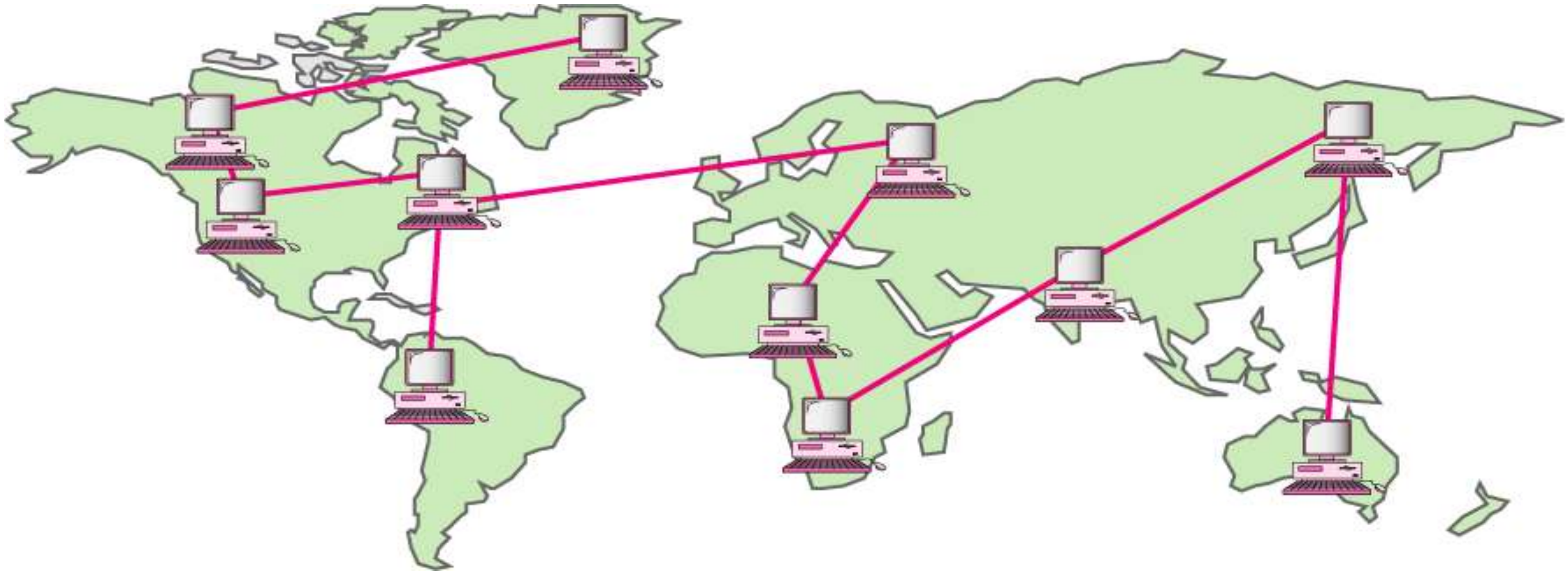


Figure 1.15 *WAN*



Data flow

- ***Simplex***
- ***Half-duplex***
- ***Full-duplex***

Figure 1.2 *Simplex: The communications is unidirectional*

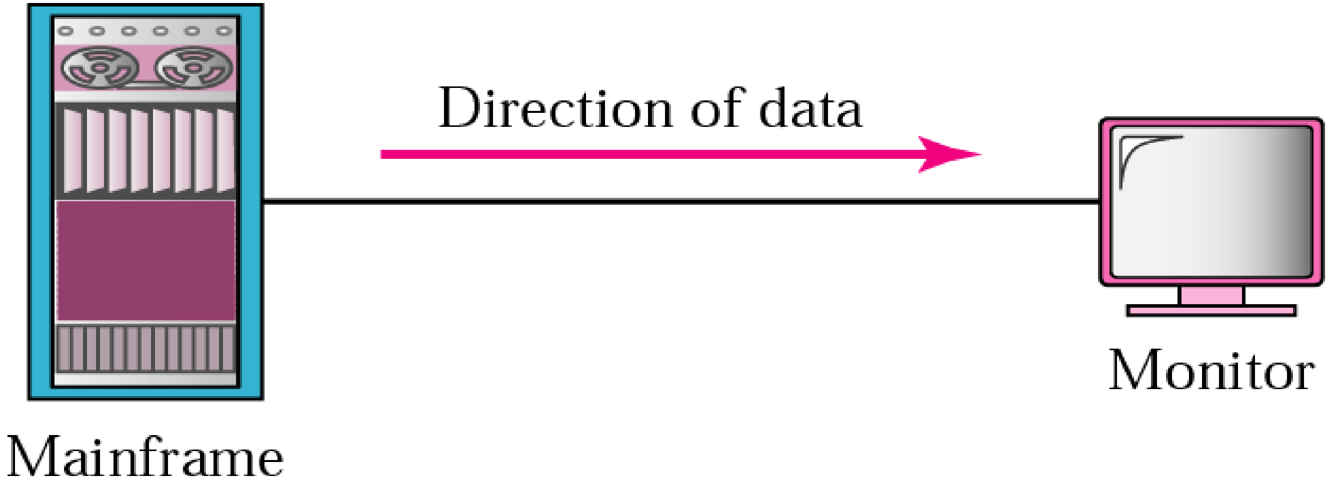


Figure 1.3 ***Half-duplex :each station can both transmit and receive but not at the same time***

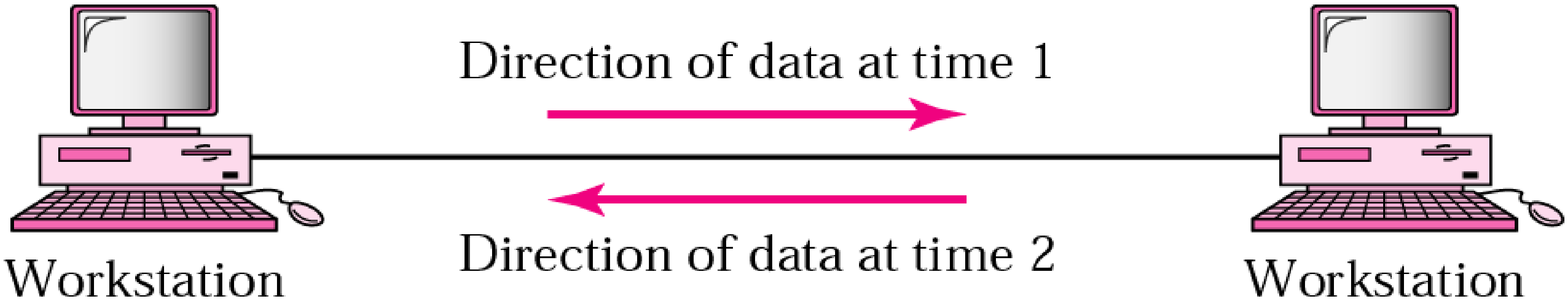
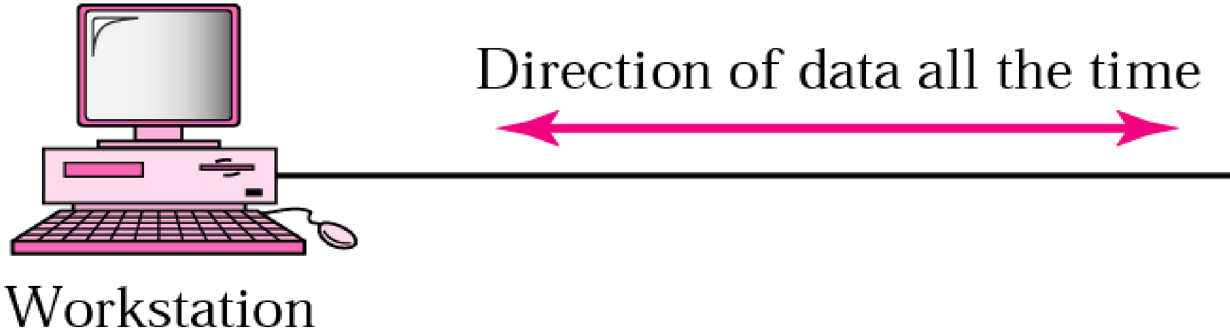


Figure 1.4 ***Full-duplex :both stations can transmit and receive simultaneously***



Chapter 4

IP Addresses: Classful Addressing

CONTENTS

4.1

INTRODUCTION

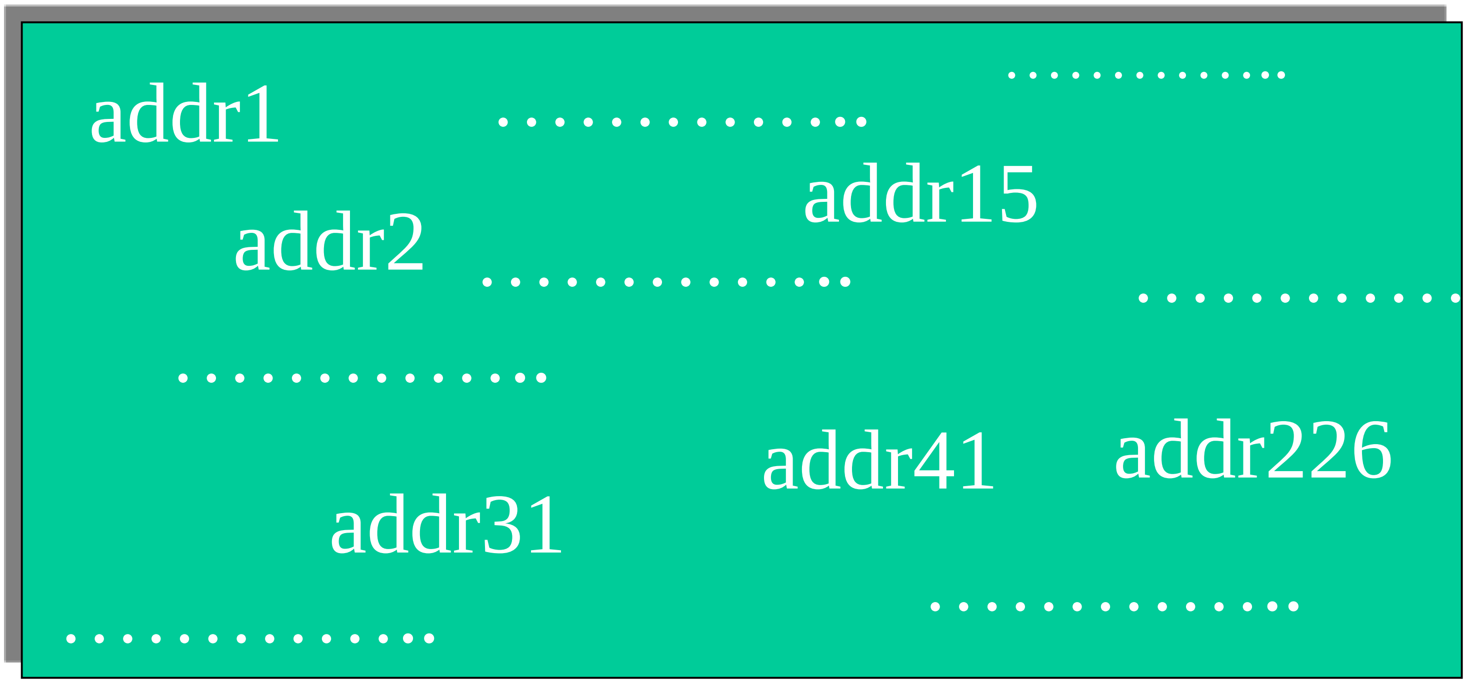
Note

An IP address is a 32-bit address.

Note

The IP addresses are unique.

Address Space



RULE:

If a protocol uses *N* bits to define an address, the address space is 2^N because each bit can have two different values (0 and 1) and *N* bits can have 2^N values.

Note

The address space of IPv4 is

2^{32}

or

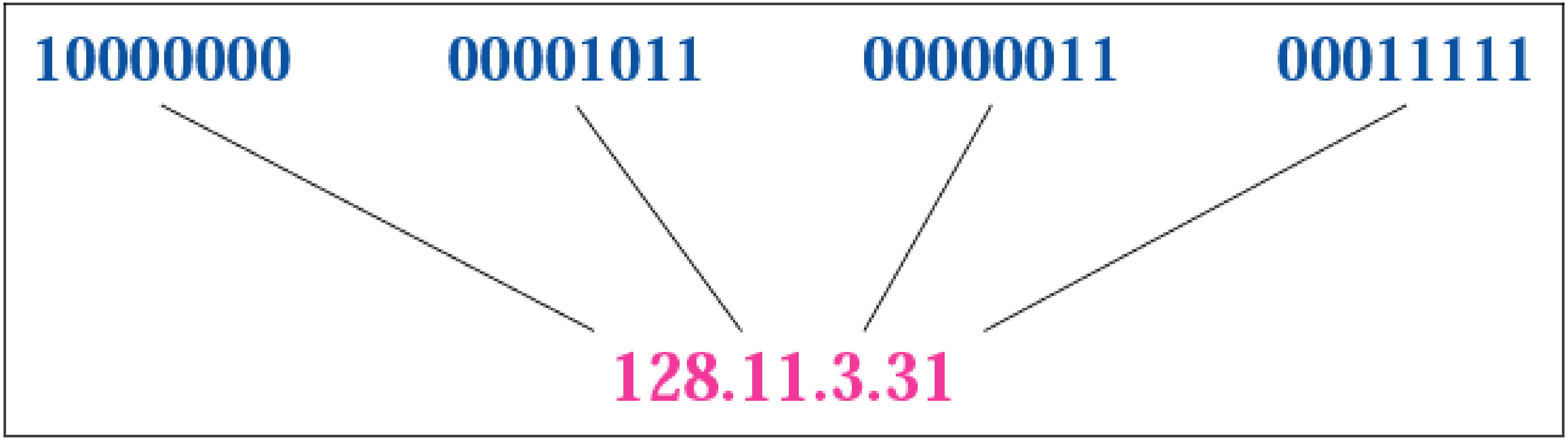
4,294,967,296.

Binary Notation

01110101 10010101 00011101 11101010

Figure 4-1

Dotted-decimal notation



Hexadecimal Notation

0111 0101 1001 0101 0001 1101 1110 1010

75 95 1D EA

0x75951DEA

Note

The binary, decimal, and hexadecimal number systems are reviewed in Appendix B.

Example 1

Change the following IP address from binary notation to dotted-decimal notation.

10000001 00001011 00001011 11101111

Solution

129.11.11.239

Example 2

Change the following IP address from dotted-decimal notation to binary notation.

111.56.45.78

Solution

01101111 00111000 00101101 01001110

Example 3

Find the error, if any, in the following IP address:

111.56.045.78

Solution

There are no leading zeroes in dotted-decimal notation (045).

Example 3 (continued)

Find the error, if any, in the following IP address:

75.45.301.14

Solution

In dotted-decimal notation, each number is less than or equal to 255; 301 is outside this range.

Example 4

Change the following IP addresses from binary notation to hexadecimal notation.

10000001 00001011 00001011 11101111

Solution

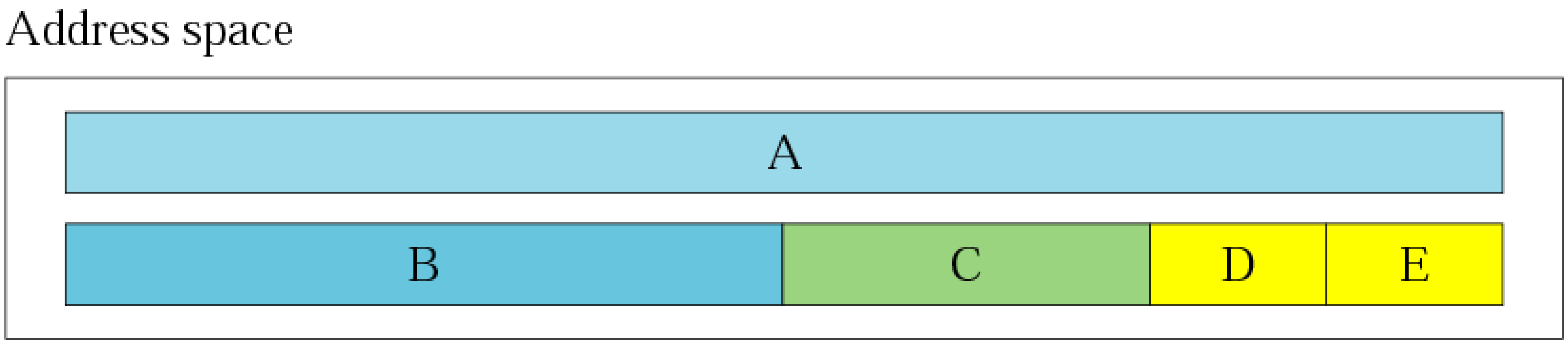
0X810B0BEF or $810B0BEF_{16}$

4.2

CLASSFUL ADDRESSING

Figure 4-2

Occupation of the address space



Note

In classful addressing, the address space is divided into five classes: A, B, C, D, and E.

Finding the class in binary notation

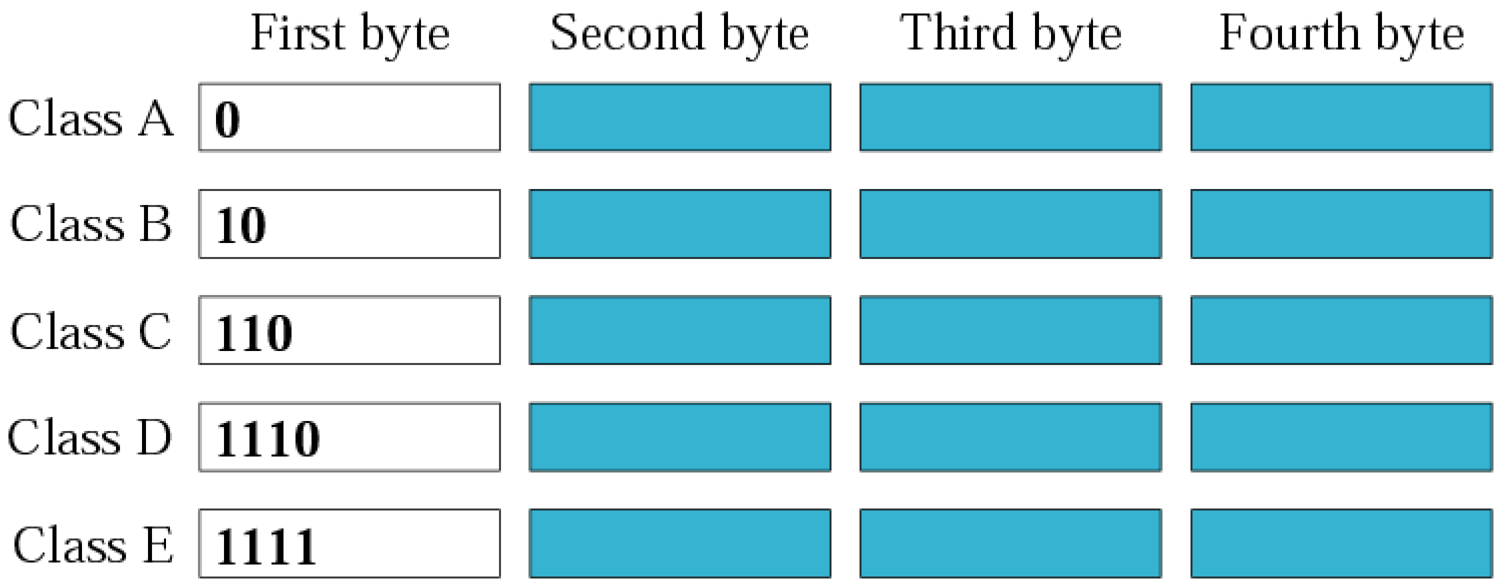
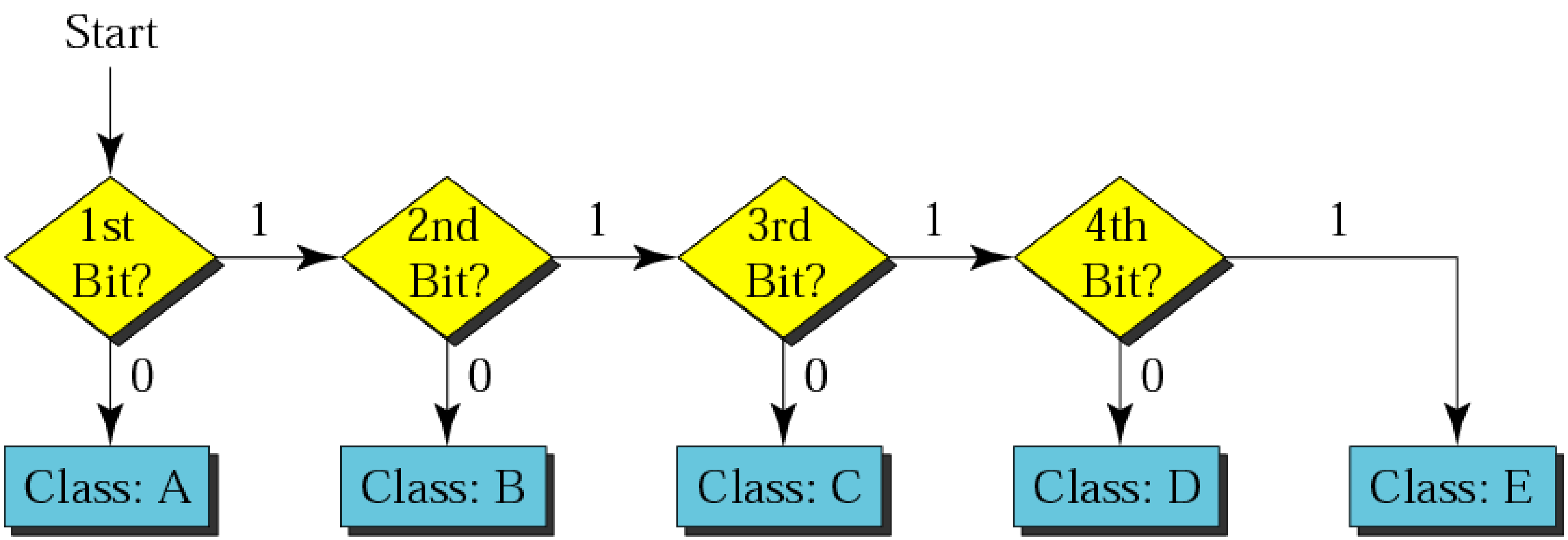


Figure 4-4

Finding the address class



Example 5

How can we prove that we have 2,147,483,648 addresses in class A?

Solution

In class A, only 1 bit defines the class. The remaining 31 bits are available for the address. With 31 bits, we can have 2^{31} or 2,147,483,648 addresses.

Example 6

Find the class of the address:

00000001 00001011 00001011 11101111

Solution

The first bit is 0. This is a class A address.

Example 6 (Continued)

Find the class of the address:

11000001 10000011 00011011 11111111

Solution

The first 2 bits are 1; the third bit is 0.
This is a class C address.

Figure 4-5

Finding the class in decimal notation

	First byte	Second byte	Third byte	Fourth byte
Class A	**0 to 127**			
Class B	**128 to 191**			
Class C	**192 to 223**			
Class D	**224 to 239**			
Class E	**240 to 255**			

Example 7

Find the class of the address:

227.12.14.87

Solution

The first byte is 227 (between 224 and 239); the class is D.

Example 7 (Continued)

Find the class of the address:

193.14.56.22

Solution

The first byte is 193 (between 192 and 223); the class is C.

Example 8

In Example 4 we showed that class A has 2^{31} (2,147,483,648) addresses. How can we prove this same fact using dotted-decimal notation?

Solution

The addresses in class A range from 0.0.0.0 to 127.255.255.255. We notice that we are dealing with base 256 numbers here.

Solution (Continued)

Each byte in the notation has a weight. The weights are as follows:

256^3 , 256^2, 256^1, 256^0

Last address: $127 \times 256^3 + 255 \times 256^2 + 255 \times 256^1 + 255 \times 256^0 = 2{,}147{,}483{,}647$

First address: $= 0$

If we subtract the first from the last and add 1, we get 2,147,483,648.

Figure 4-6

Netid and hostid

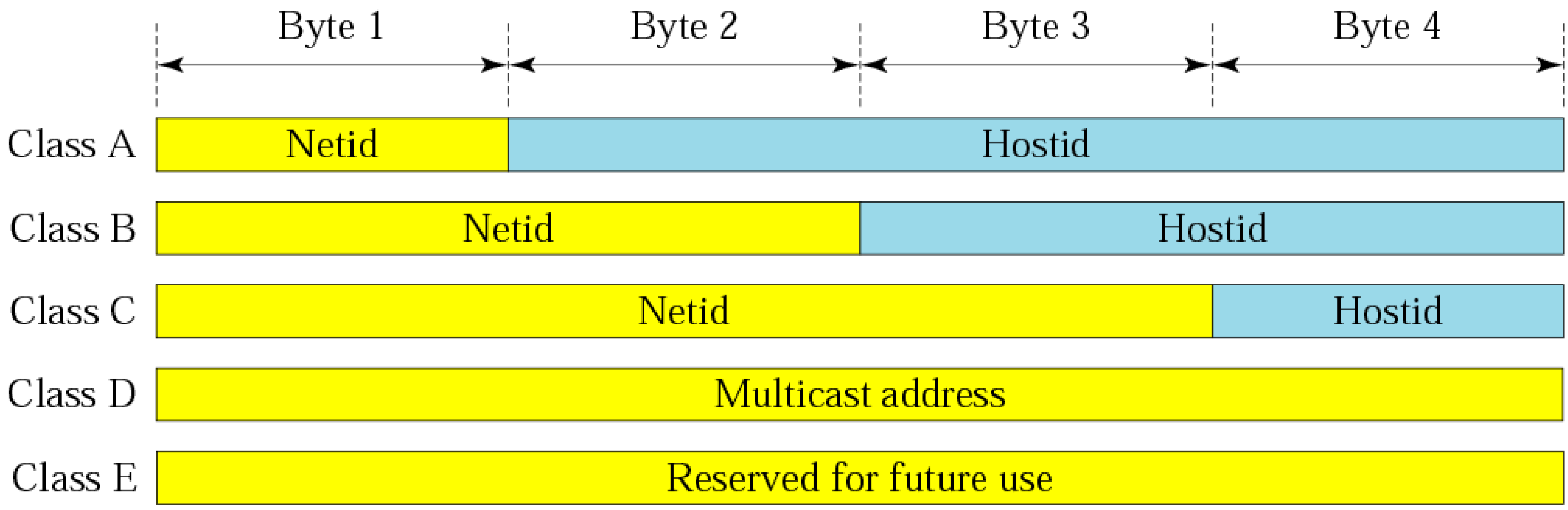
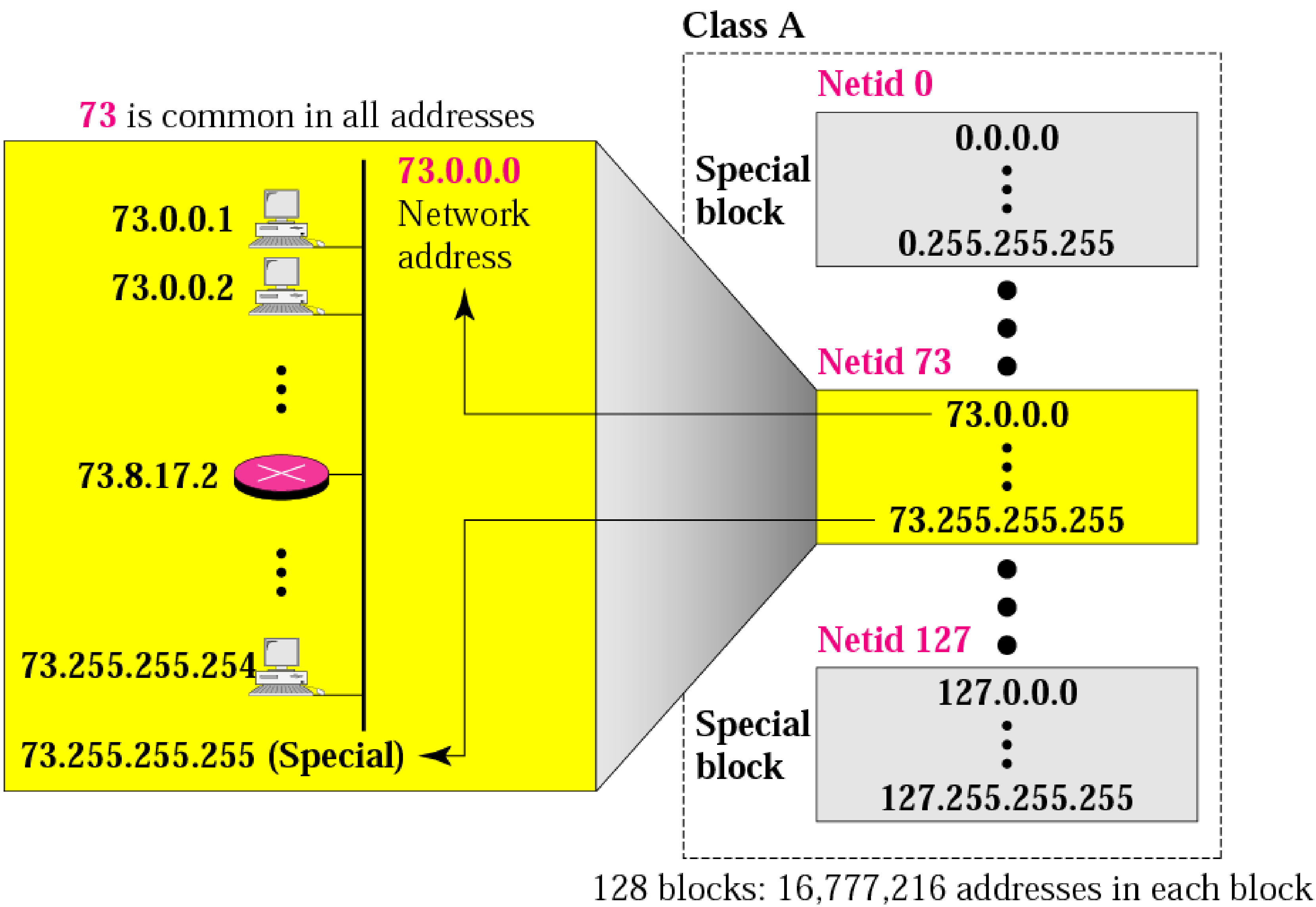


Figure 4-7

Blocks in class A

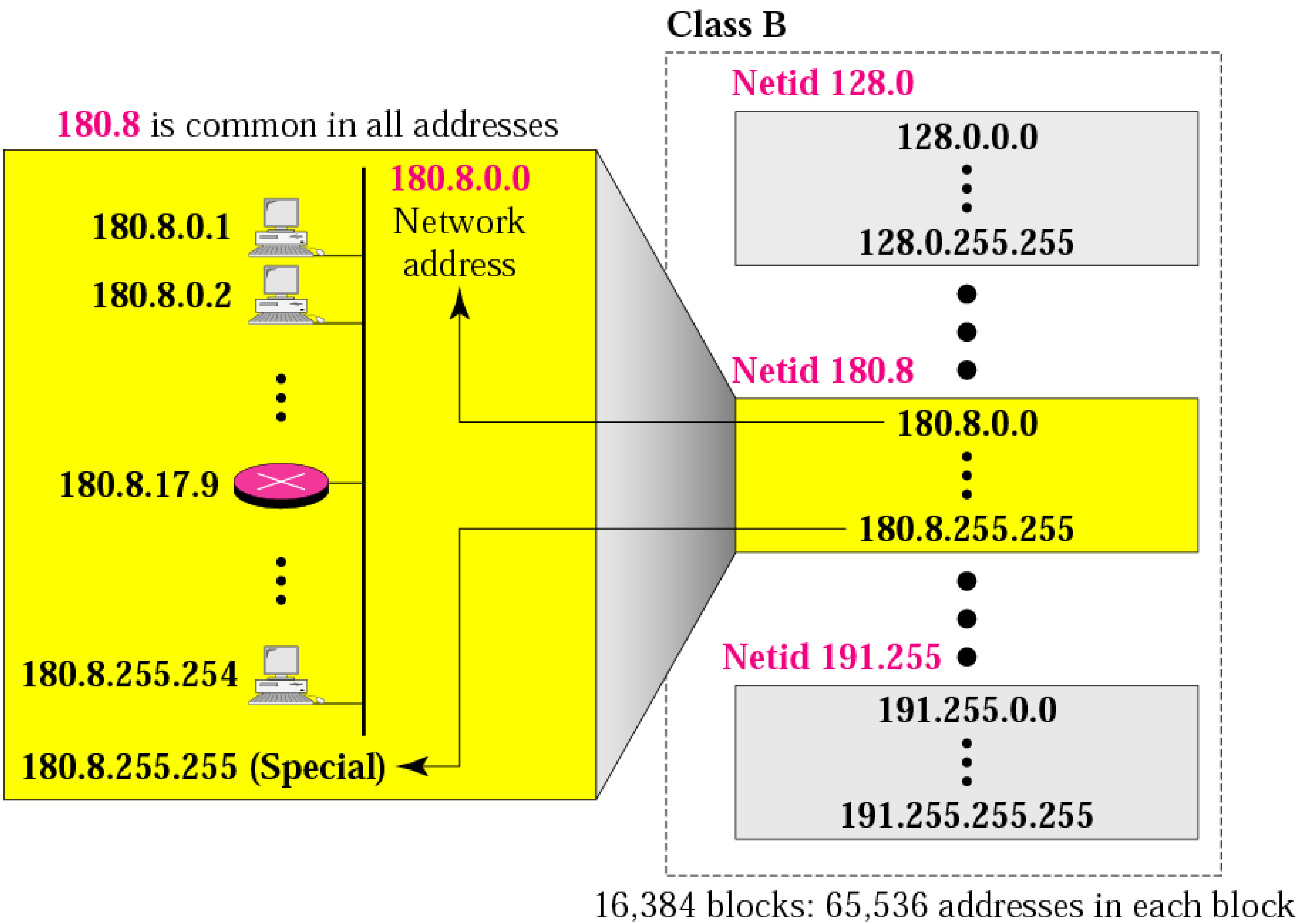


Note

Millions of class A addresses are wasted.

Figure 4-8

Blocks in class B

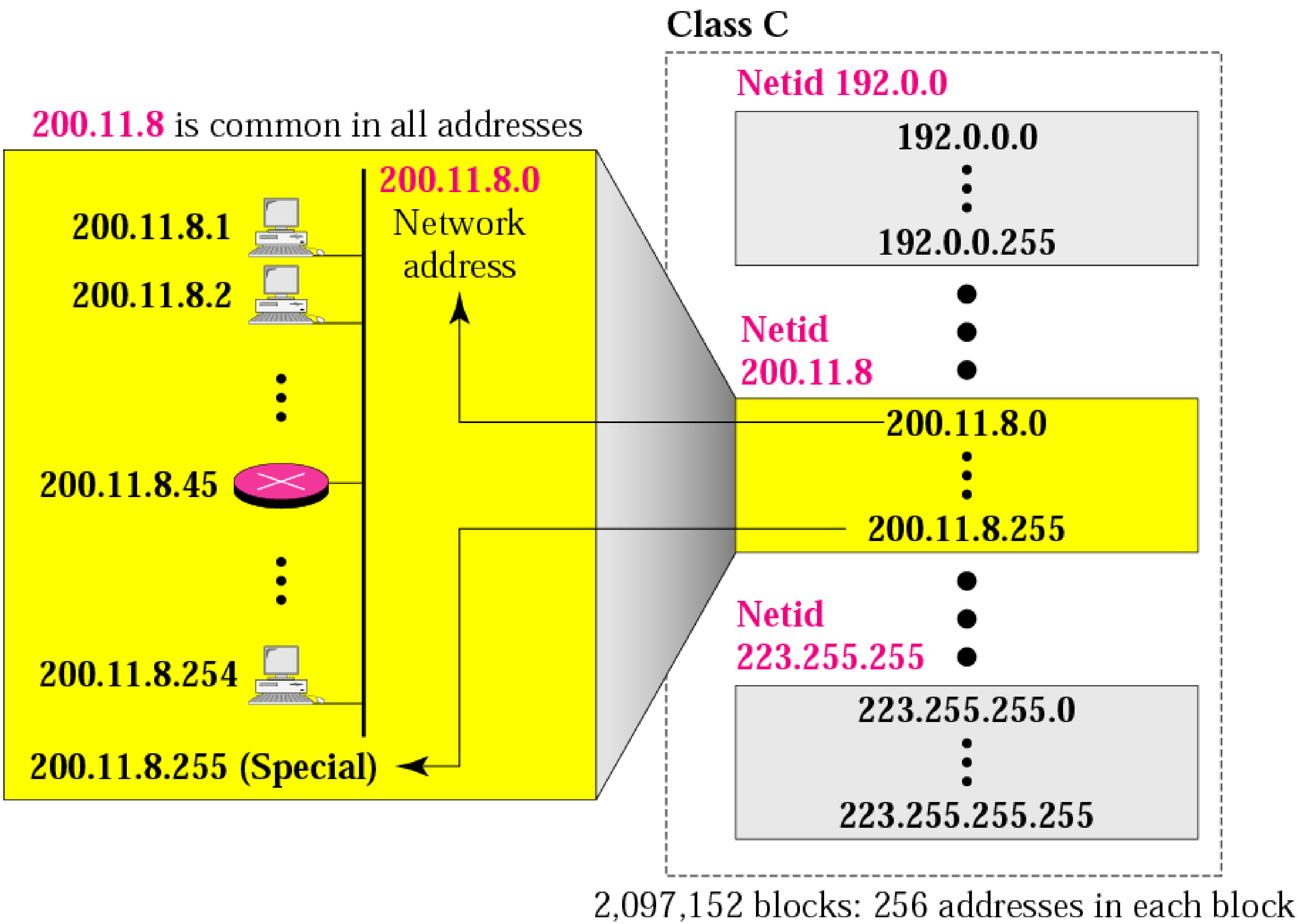


Note

Many class B addresses are wasted.

Figure 4-9

Blocks in class C



Note

The number of addresses in a class C block is smaller than the needs of most organizations.

Note

Class D addresses are used for multicasting; there is only one block in this class.

Note

Class E addresses are reserved for special purposes; most of the block is wasted.

Network Addresses

The network address is the first address.

The network address defines the network to the rest of the Internet.

Given the network address, we can find the class of the address, the block, and the range of the addresses in the block

Note

In classful addressing, the network address (the first address in the block) is the one that is assigned to the organization.

Example 9

Given the network address 17.0.0.0, find the class, the block, and the range of the addresses.

Solution

The class is A because the first byte is between 0 and 127. The block has a netid of 17. The addresses range from 17.0.0.0 to 17.255.255.255.

Example 10

Given the network address 132.21.0.0, find the class, the block, and the range of the addresses.

Solution

The class is B because the first byte is between 128 and 191. The block has a netid of 132.21. The addresses range from 132.21.0.0 to 132.21.255.255.

Example 11

Given the network address 220.34.76.0, find the class, the block, and the range of the addresses.

Solution

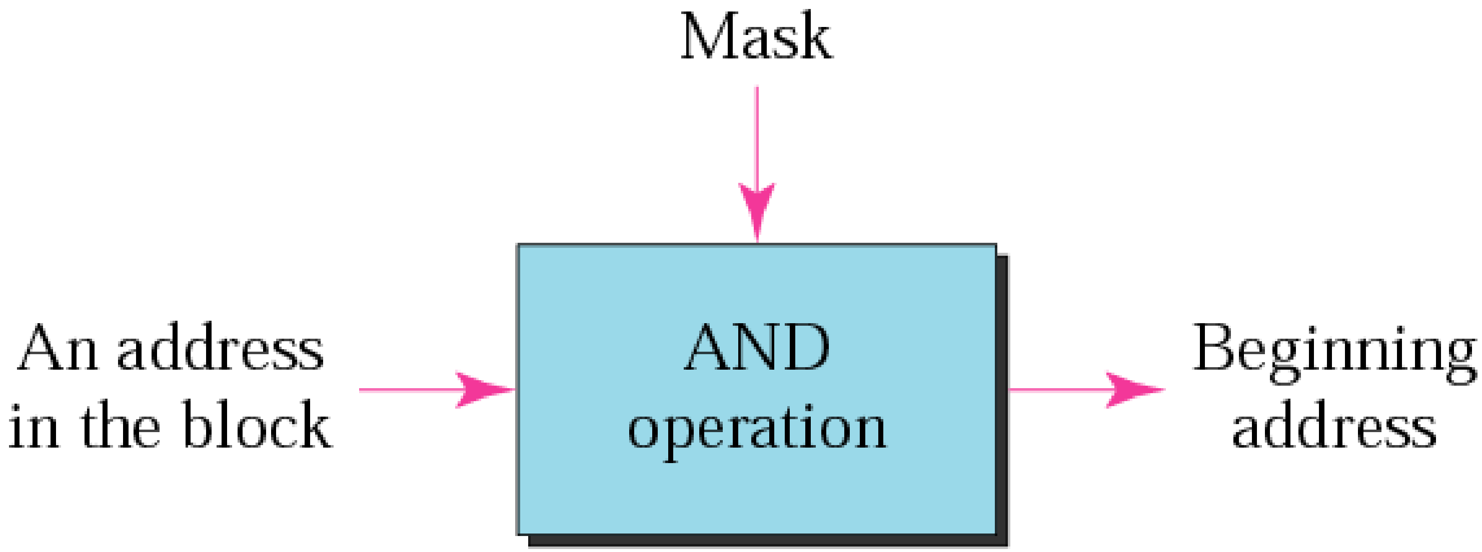
The class is C because the first byte is between 192 and 223. The block has a netid of 220.34.76. The addresses range from 220.34.76.0 to 220.34.76.255.

Mask

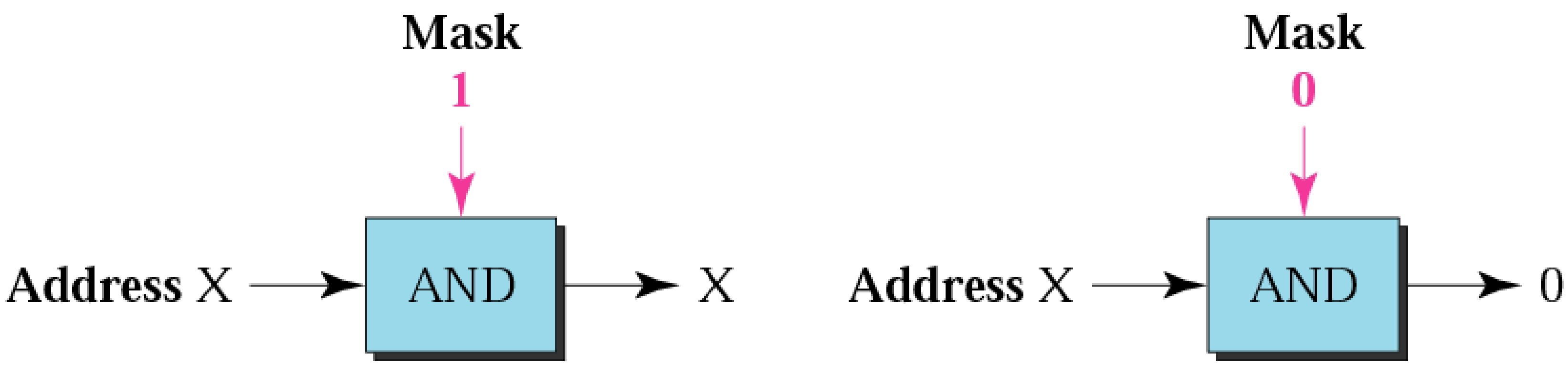
A mask is a 32-bit binary number that gives the first address in the block (the network address) when bitwise ANDed with an address in the block.

Figure 4-10

Masking concept



AND operation



Note

The network address is the beginning address of each block. It can be found by applying the default mask to any of the addresses in the block (including itself). It retains the netid of the block and sets the hostid to zero.

Example 12

Given the address 23.56.7.91 and the default class A mask, find the beginning address (network address).

Solution

The default mask is 255.0.0.0, which means that only the first byte is preserved and the other 3 bytes are set to 0s. The network address is 23.0.0.0.

Example 13

Given the address 132.6.17.85 and the default class B mask, find the beginning address (network address).

Solution

The default mask is 255.255.0.0, which means that the first 2 bytes are preserved and the other 2 bytes are set to 0s. The network address is 132.6.0.0.

Example 14

Given the address 201.180.56.5 and the class C default mask, find the beginning address (network address).

Solution

The default mask is 255.255.255.0, which means that the first 3 bytes are preserved and the last byte is set to 0. The network address is 201.180.56.0.

Note

We must not apply the default mask of one class to an address belonging to another class.

4.13

OTHER ISSUES

Figure 4-12

Multihomed devices

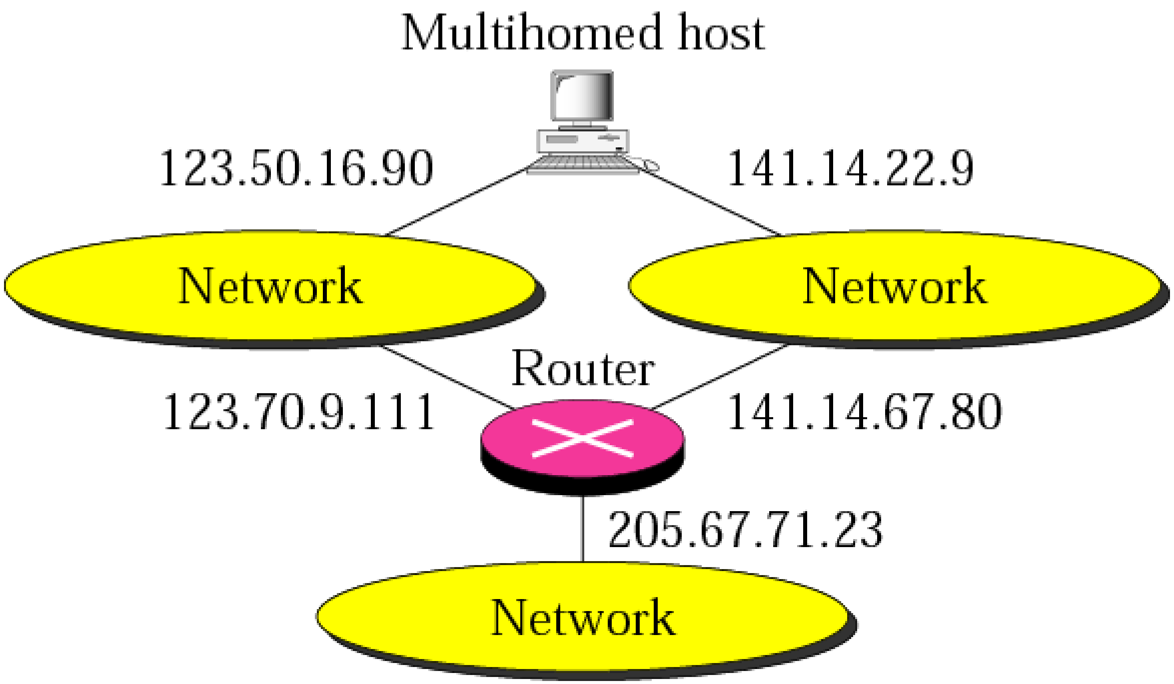


Figure 4-13

Network addresses

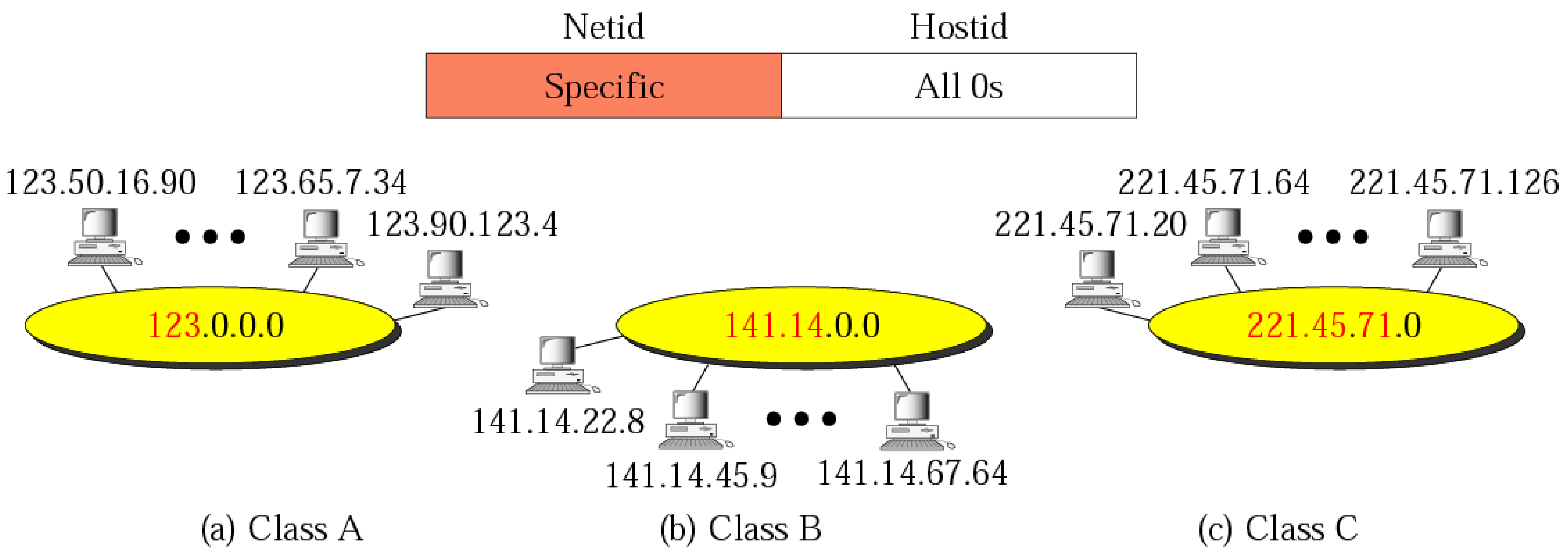
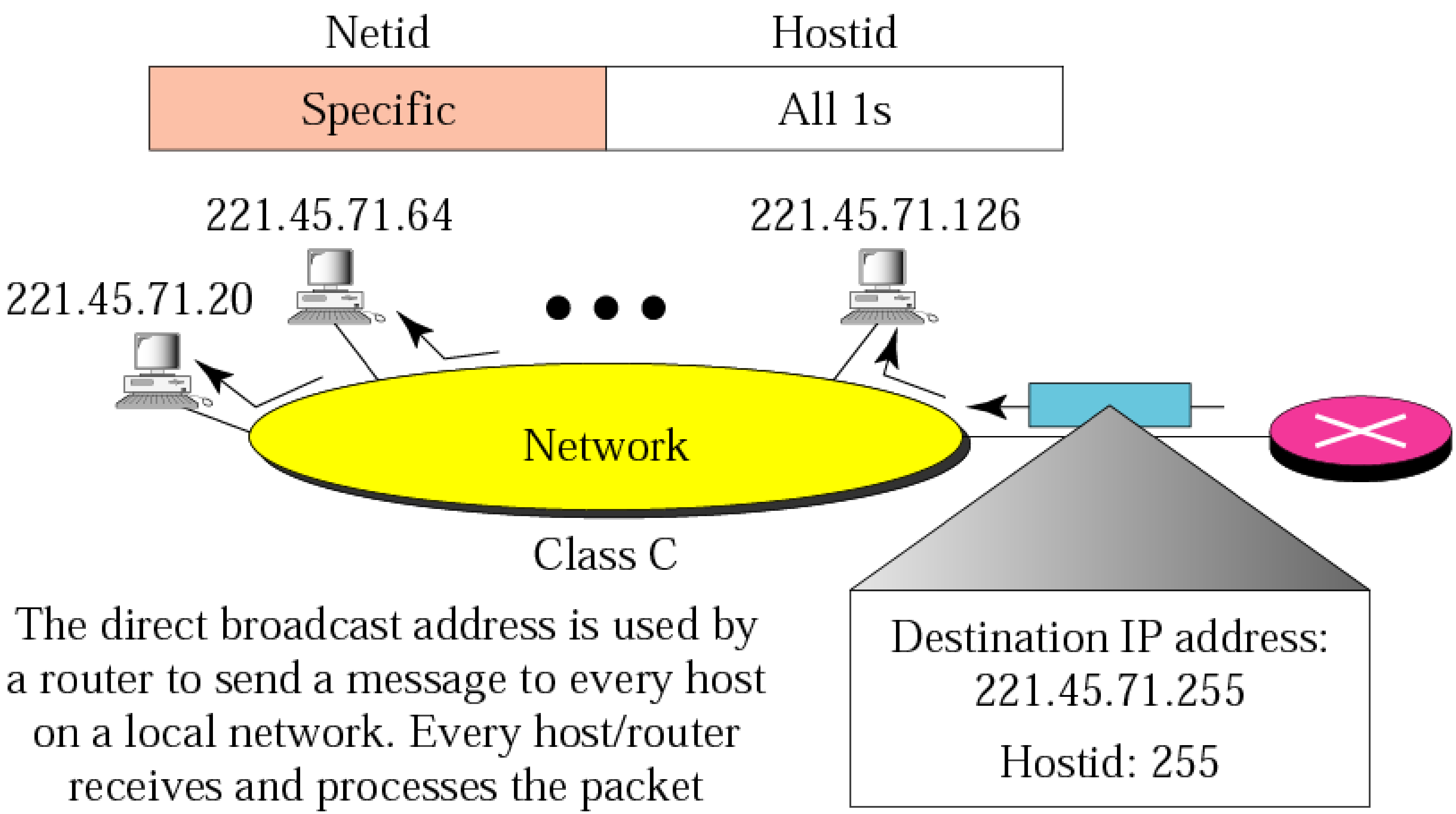


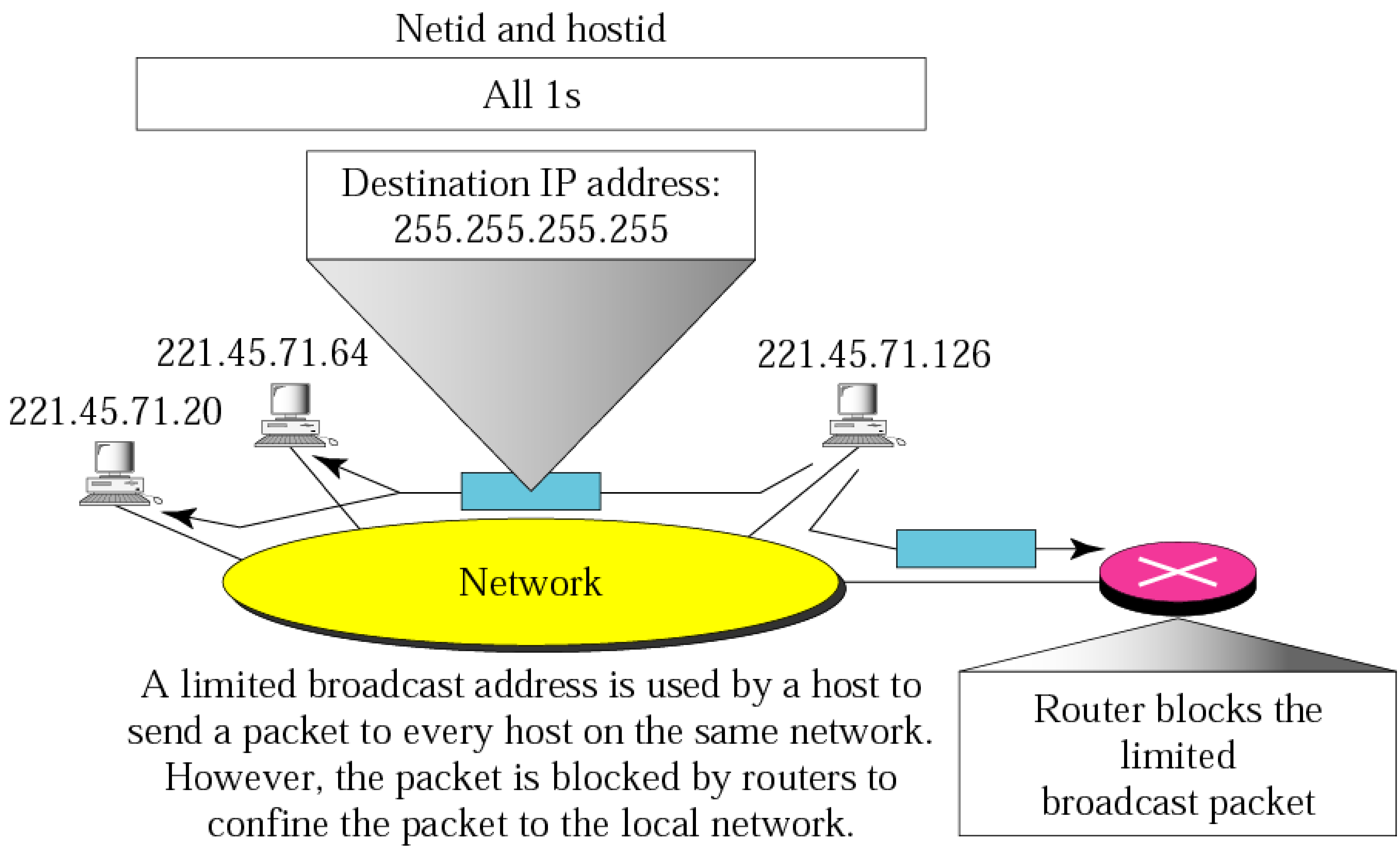
Figure 4-14

Example of direct broadcast address



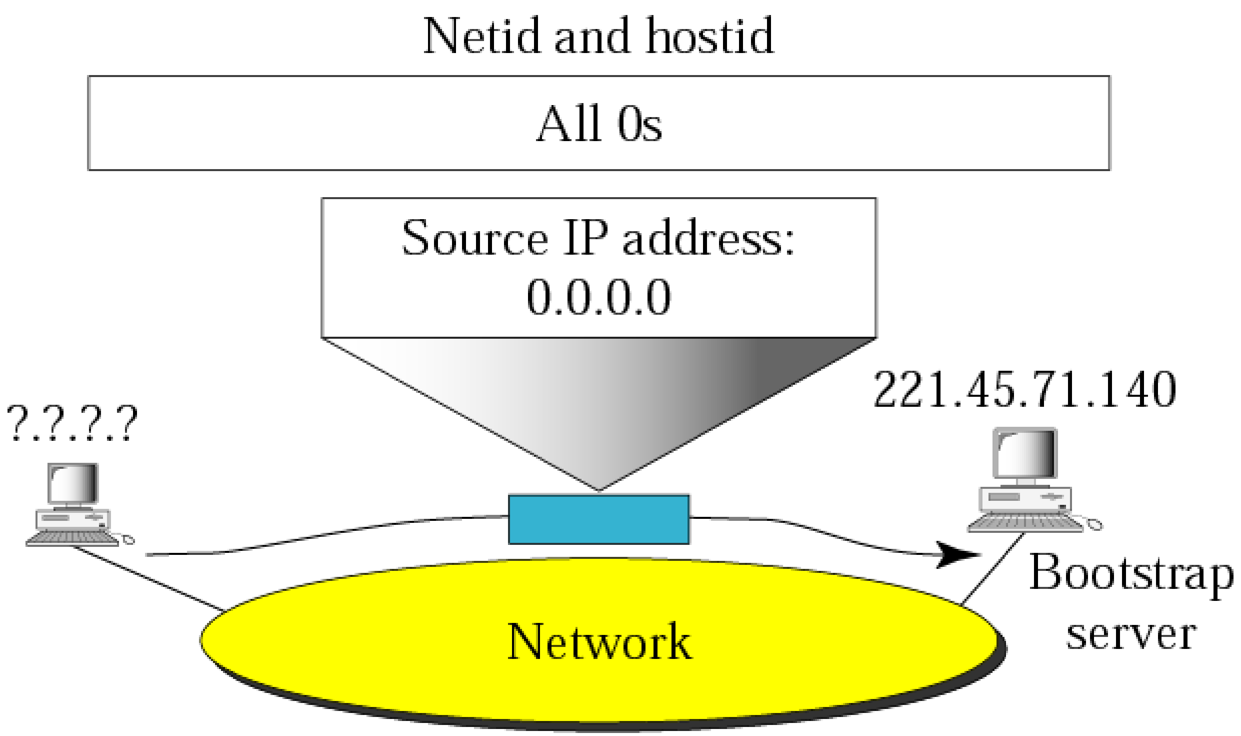
The direct broadcast address is used by a router to send a message to every host on a local network. Every host/router receives and processes the packet with a direct broadcast address.

Example of limited broadcast address



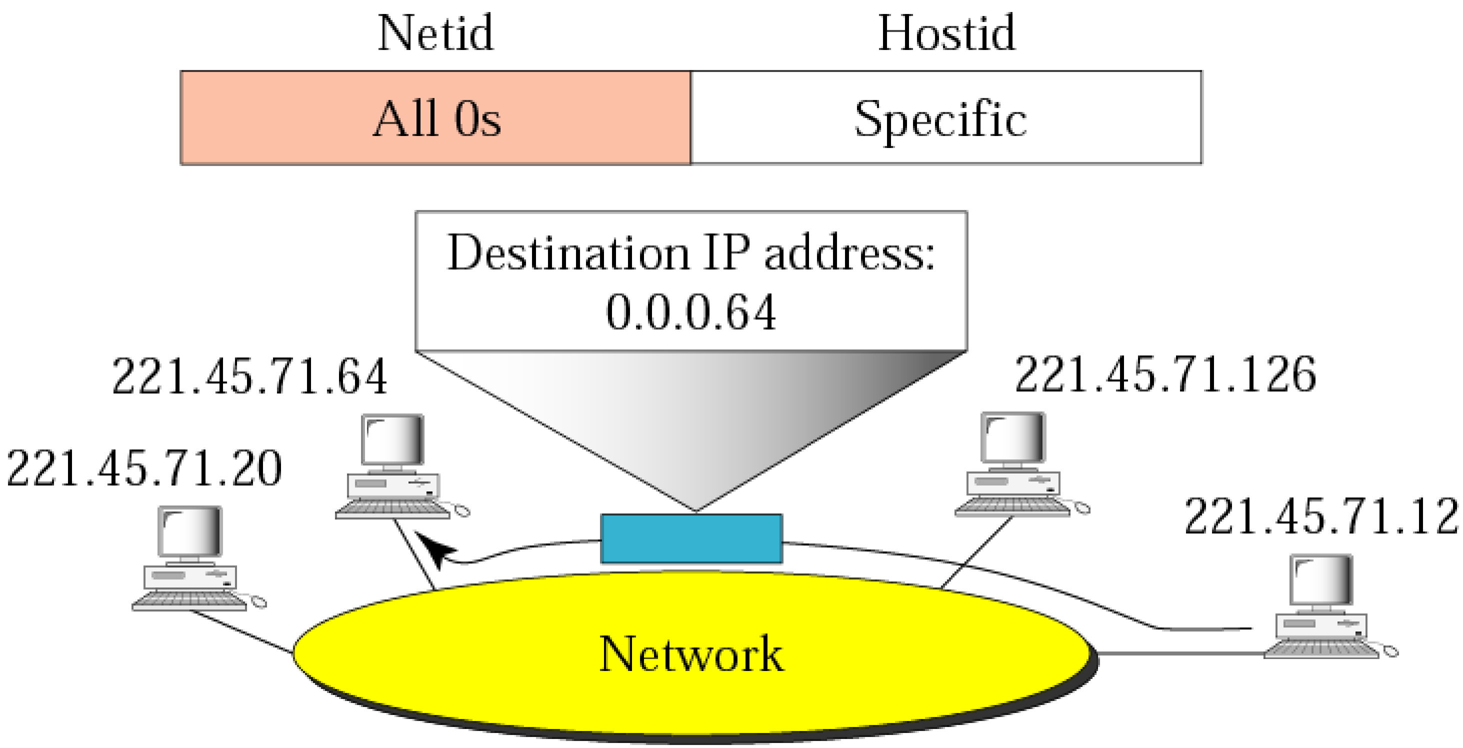
A limited broadcast address is used by a host to send a packet to every host on the same network. However, the packet is blocked by routers to confine the packet to the local network.

Example of *this* host on *this* address



A host that does not know its IP address uses the IP address 0.0.0.0 as the source address and 255.255.255.255 as the destination address to send a message to a bootstrap server.

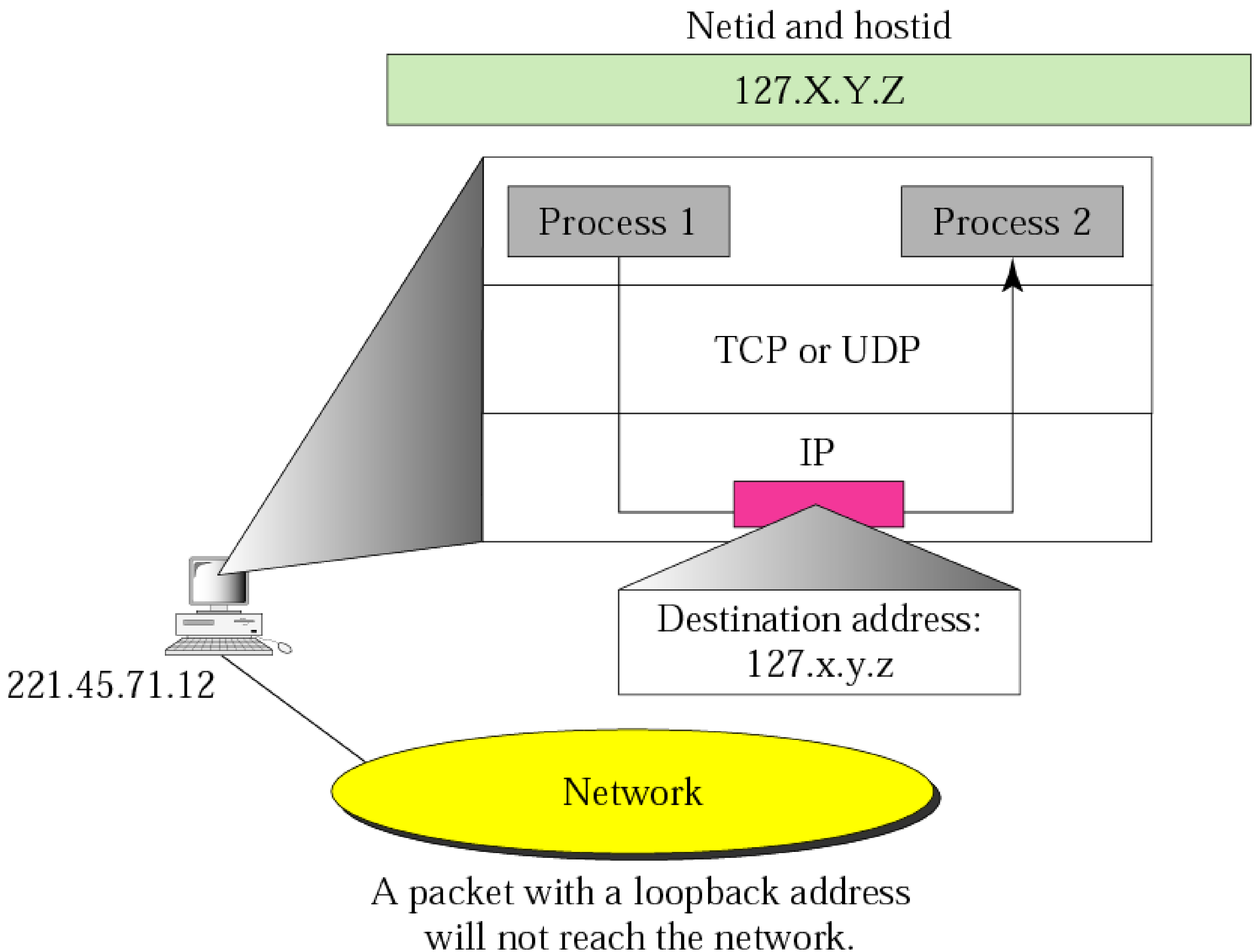
Example of specific host on *this* network



This address is used by a router or host
to send a message to a specific host on the same network.

Figure 4-18

Example of loopback address



Private Addresses

A number of blocks in each class are assigned for private use. They are not recognized globally. These blocks are depicted in Table 4.4

Unicast, Multicast, and Broadcast Addresses

Unicast communication is *one-to-one*.

Multicast communication is *one-to-many*.

Broadcast communication is *one-to-all*.

Note

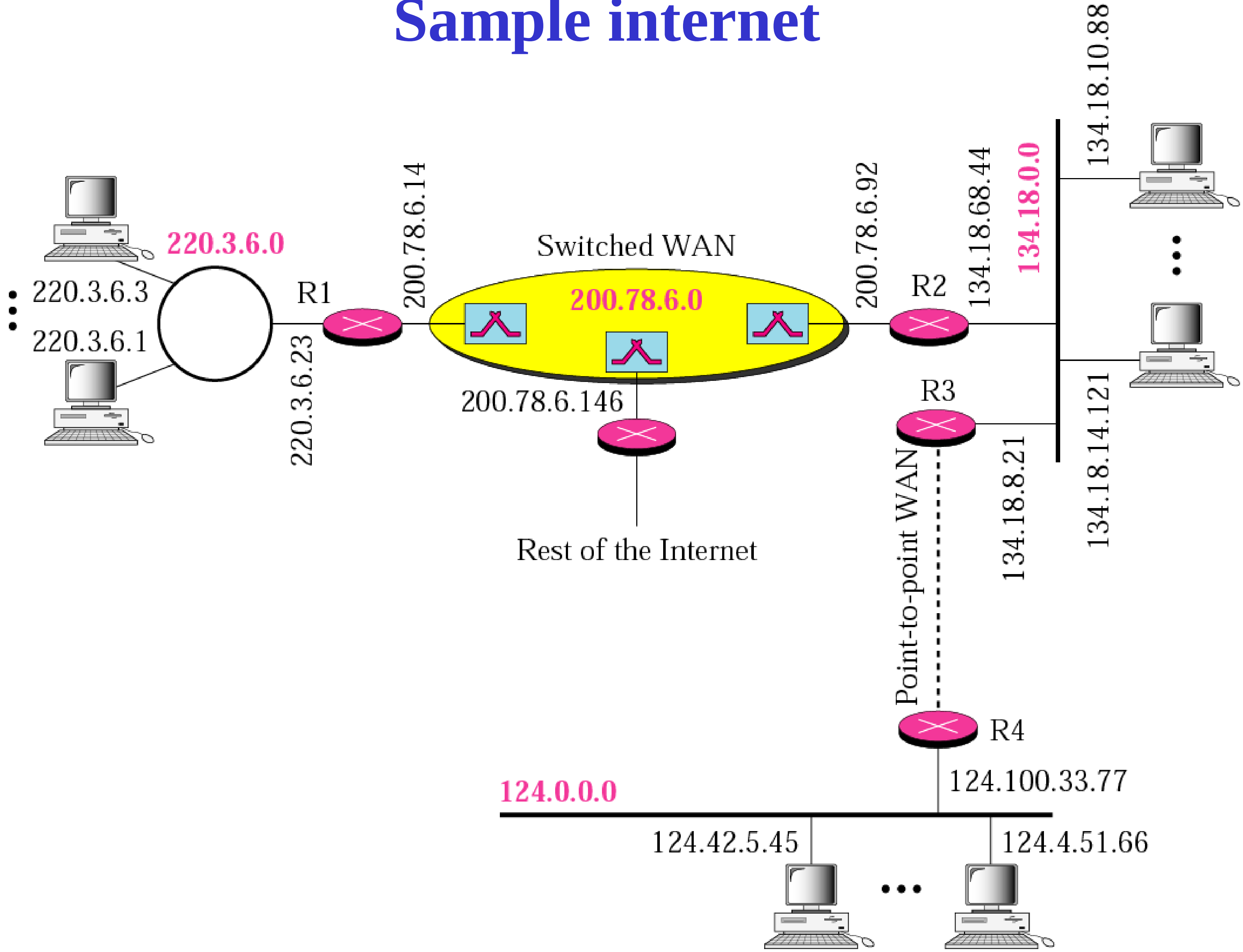
Multicast delivery will be discussed in depth in Chapter 14.

4.4

A SAMPLE INTERNET WITH CLASSFUL ADDRESSES

Figure 4-19

Sample internet



Chapter 2

The OSI Model and TCP/IP Protocol Suite

CONTENTS

- THE OSI MODEL
- LAYERS IN THE OSI MODEL
- TCP/IP PROTOCOL SUITE
- ADDRESSING
- TCP/IP VERSIONS

2.1

THE OSI MODEL

Note

ISO is the organization.
OSI is the model.

Figure 2-1

OSI Model

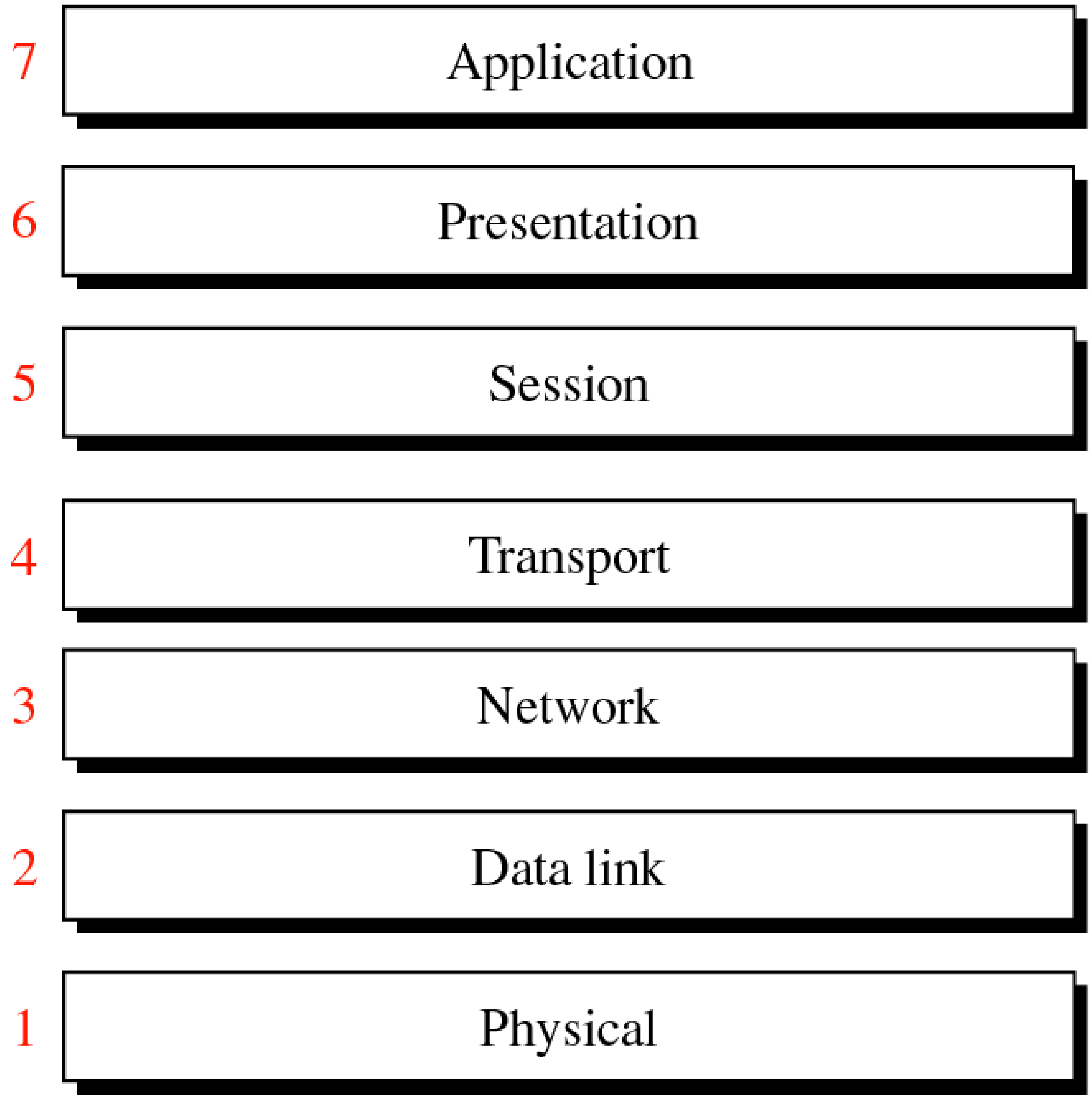
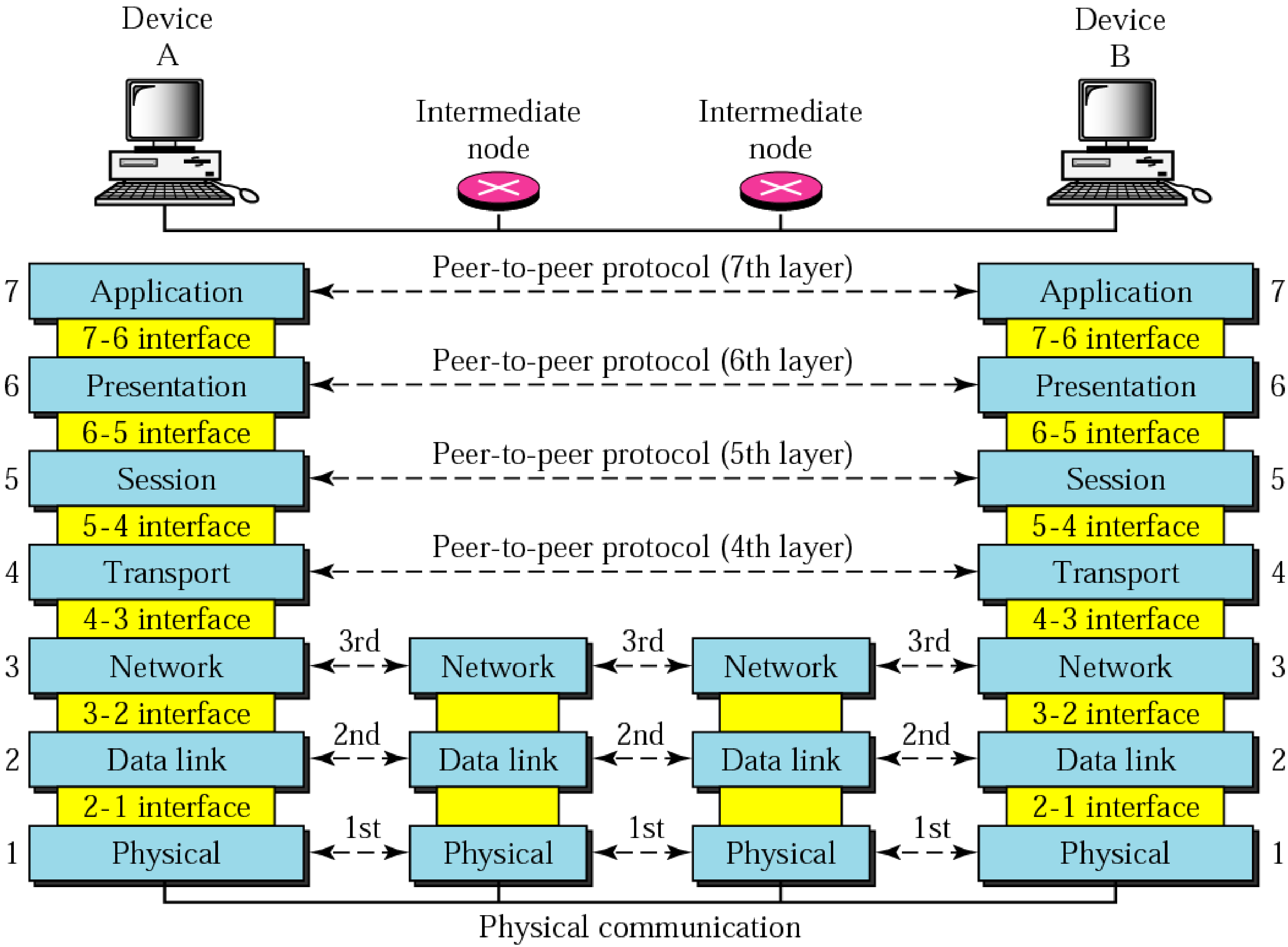


Figure 2-2

OSI layers

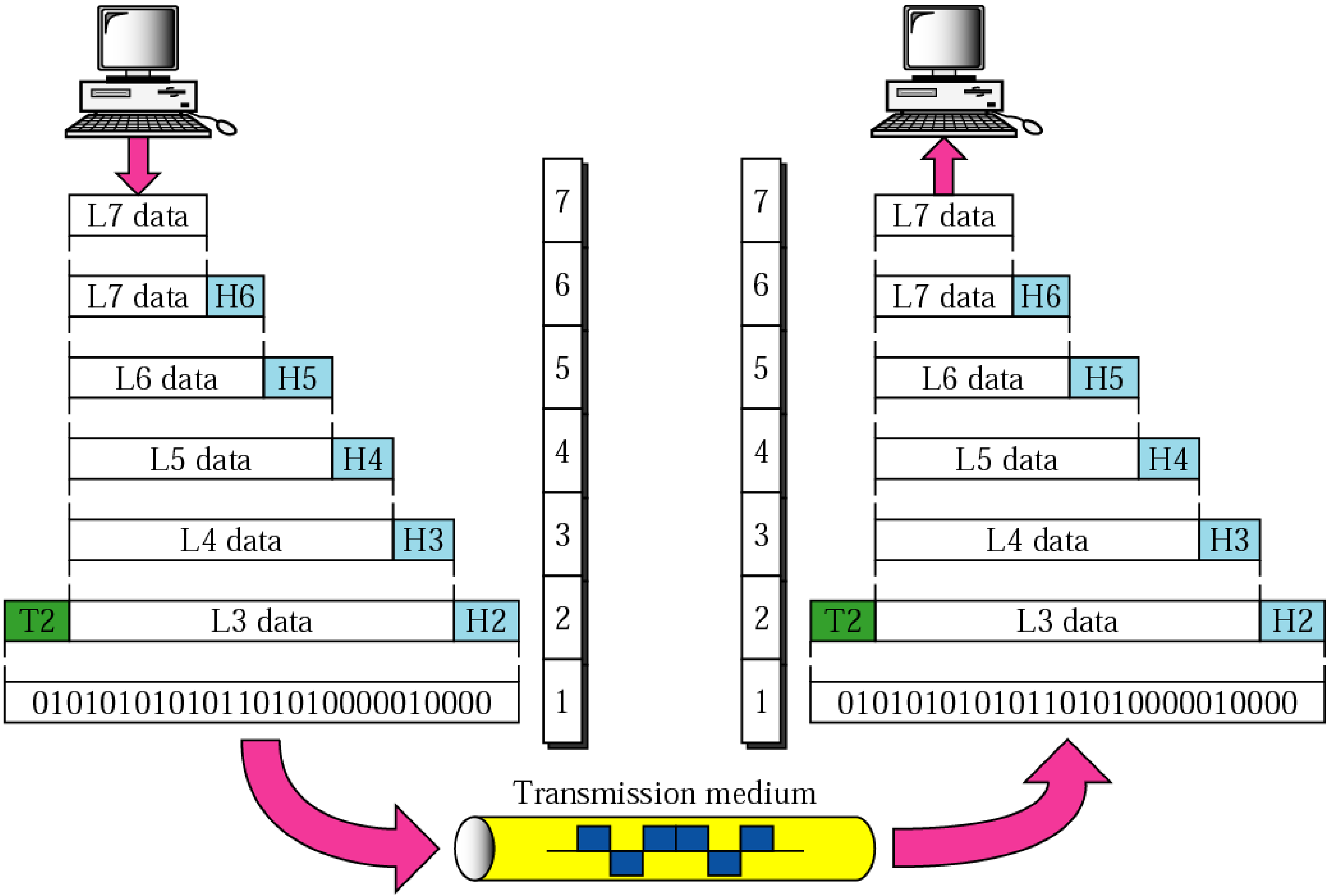


Note

Headers are added to the data at layers 6, 5, 4, 3, and 2. Trailers are usually added only at layer 2.

Figure 2-3

An exchange using the OSI model

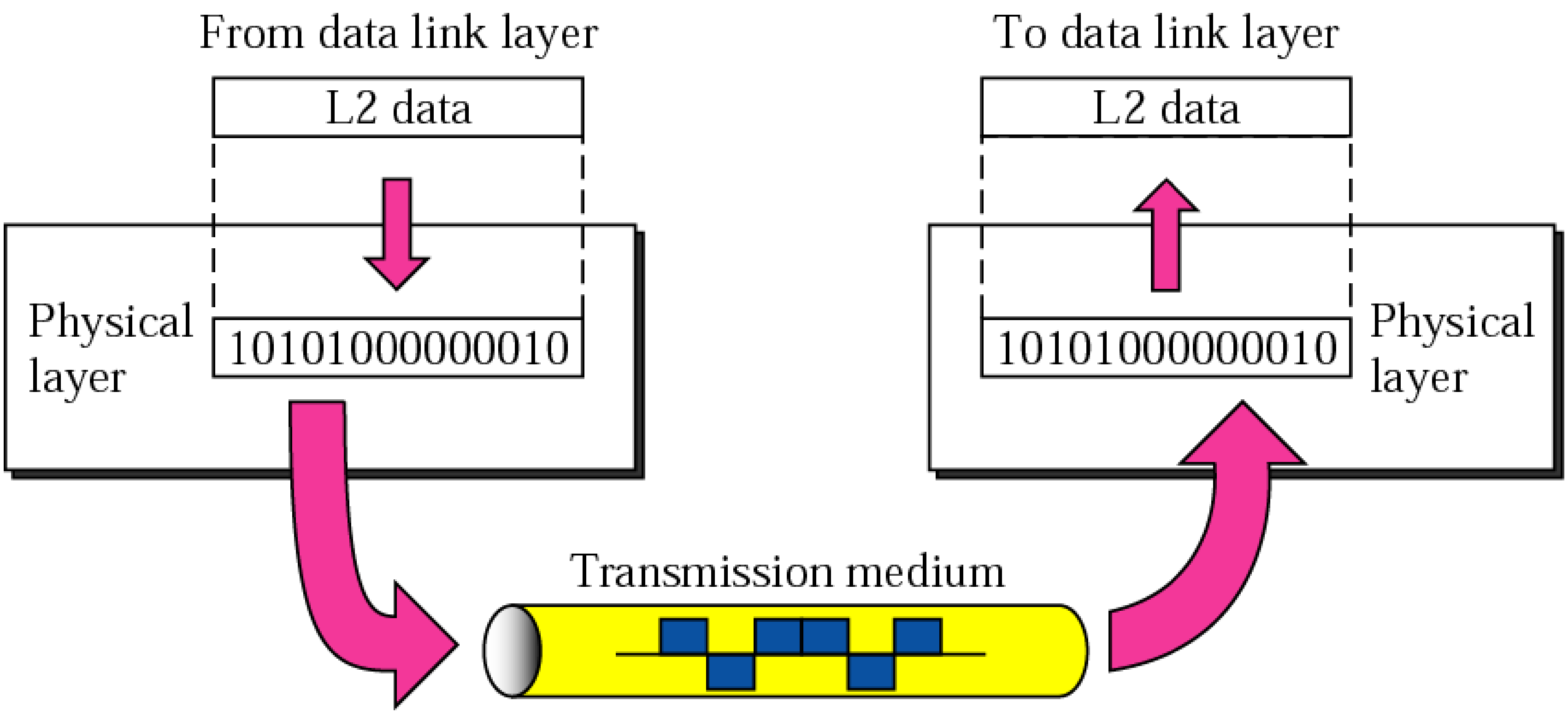


2.2

LAYERS IN THE OSI MODEL

Figure 2-4

Physical Layer

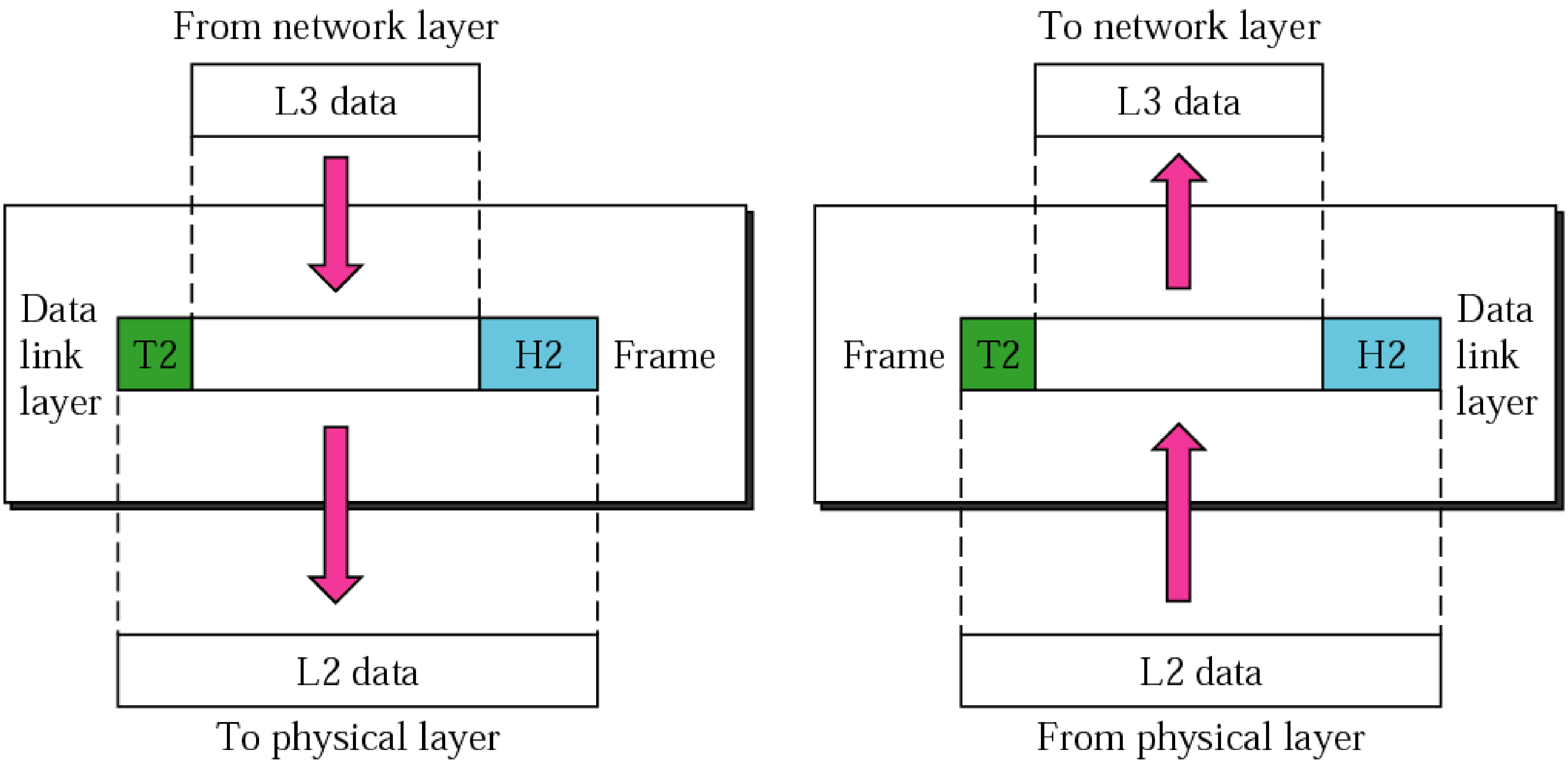


Physical layer

- responsible for movements of individual bits from one hop to the next
- The physical layer also concern with the following:

1. Physical characteristics of interface and medium.
2. Representation of bit: define the type of encoding.
3. Data rate :the number of bit sent each second .
4. Synchronization of bits: it must be synchronized at the bit level
5. Line configurations :concerned with the connection of devices to the media.
6. Physical topology: how device can connected to make a network.
7. Transmission mode: define the direction of transmission

Data Link Layer



Data link

- responsible for moving frame from one node to the next.
- Other responsibilities to the data link layer :

1. Framing .
2. Physical addressing .
3. Flow control.
4. Error control.

Node-to-node delivery

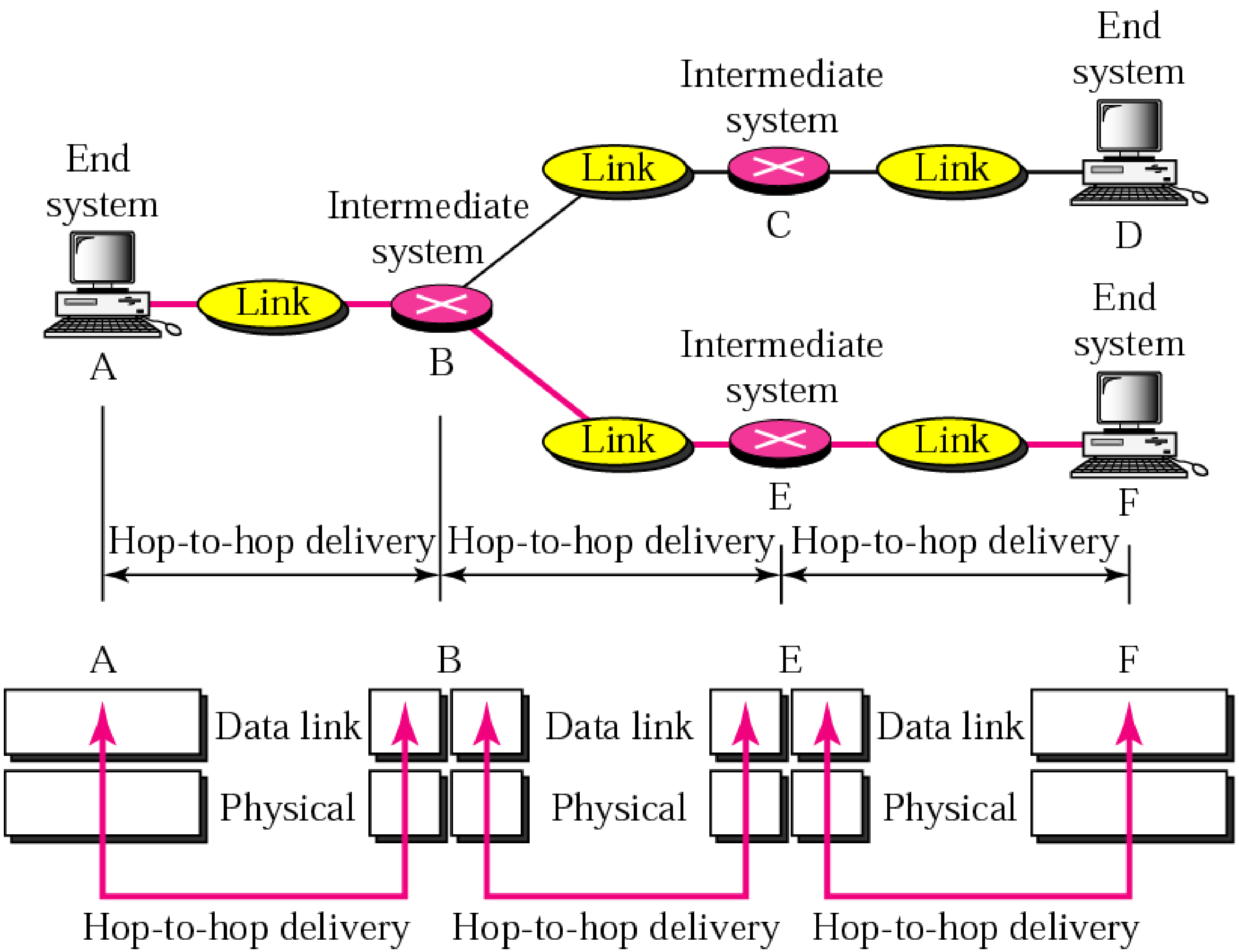
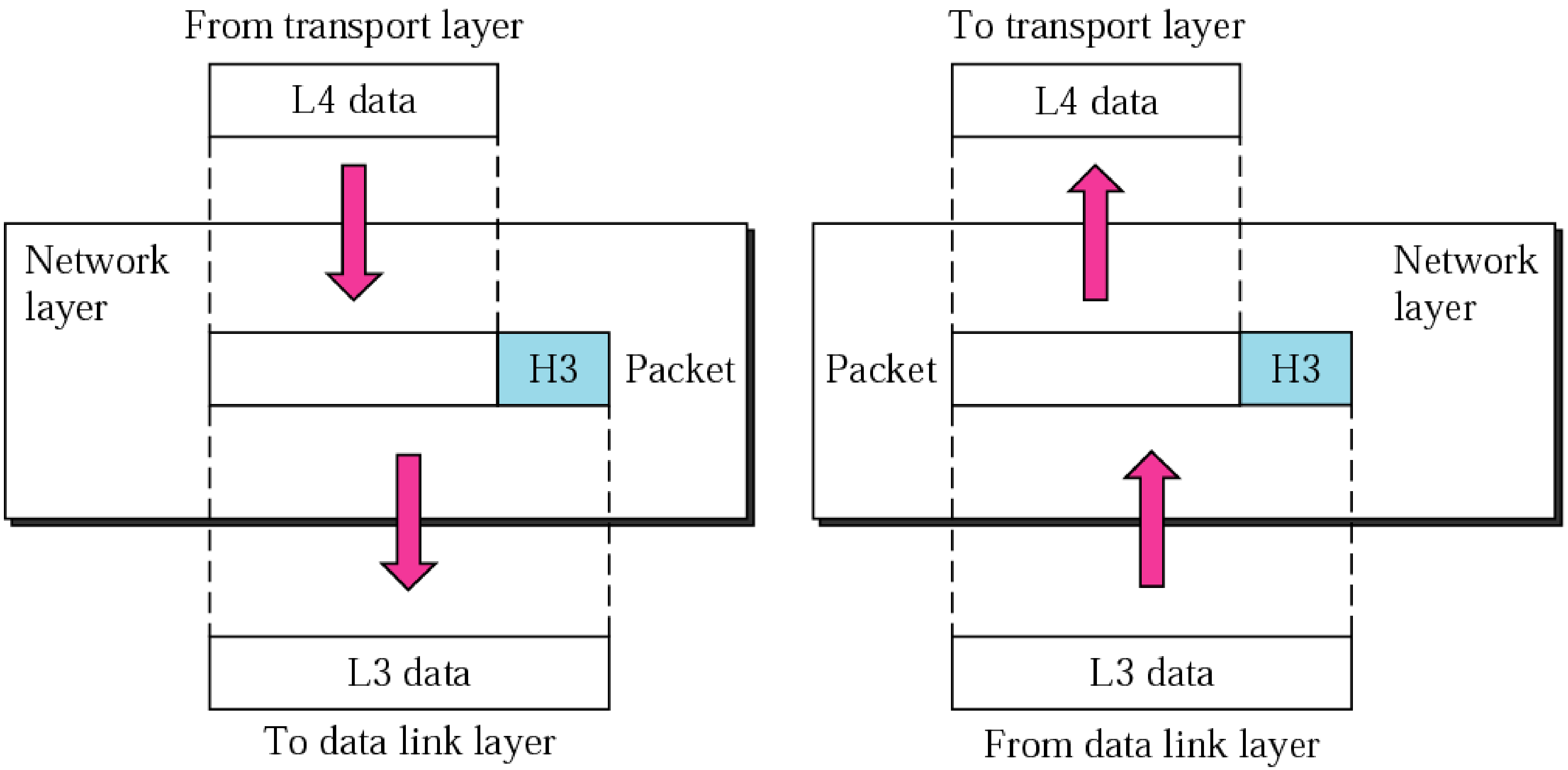


Figure 2-7

Network Layer



Network layer

- The network layer is responsible for the delivery of individual packets from the source host to the destination host.
- other responsibilities of the network layer include the following :

1. Logical addressing
2. routing

Figure 2-8

End-to-end delivery

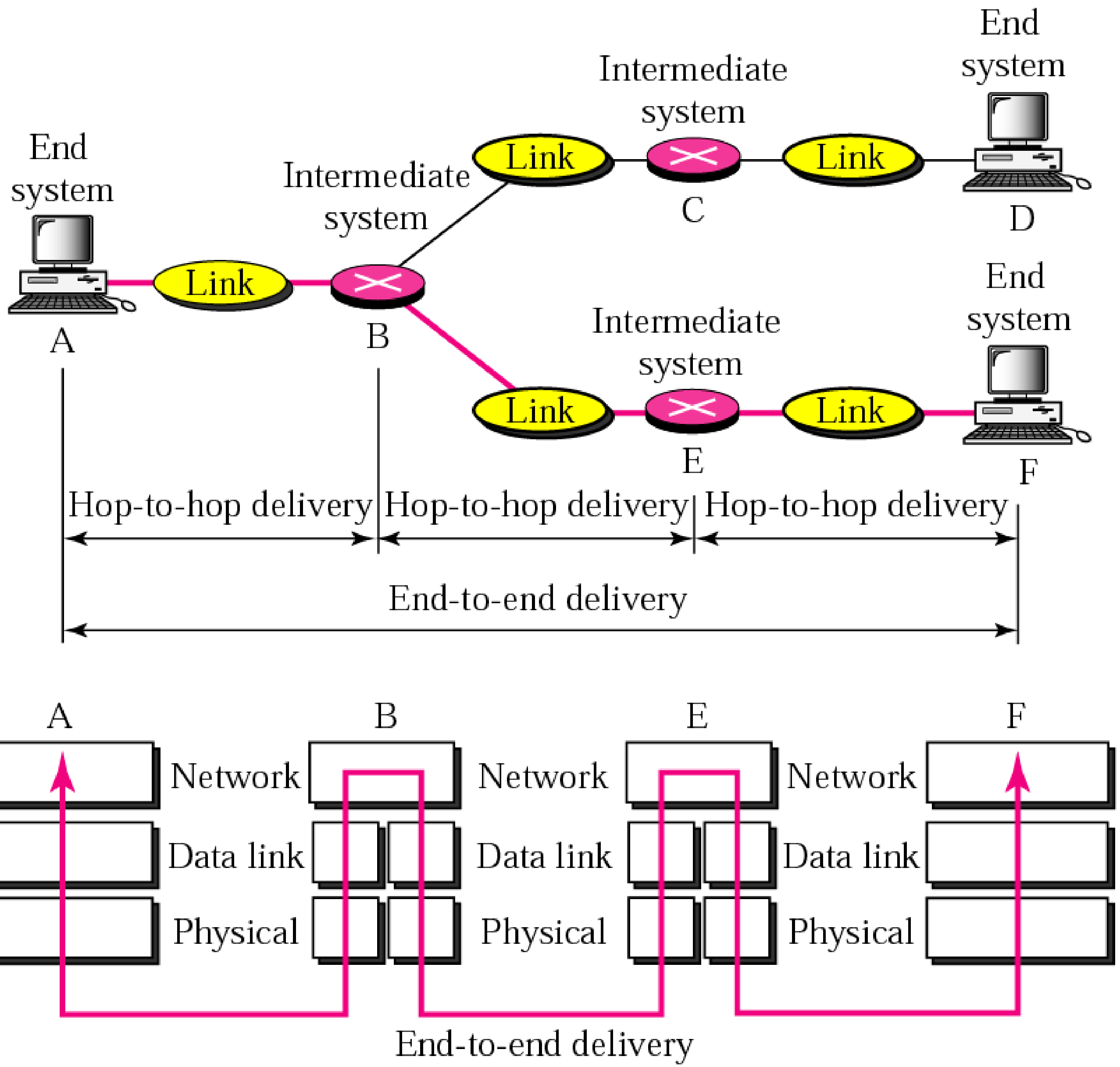
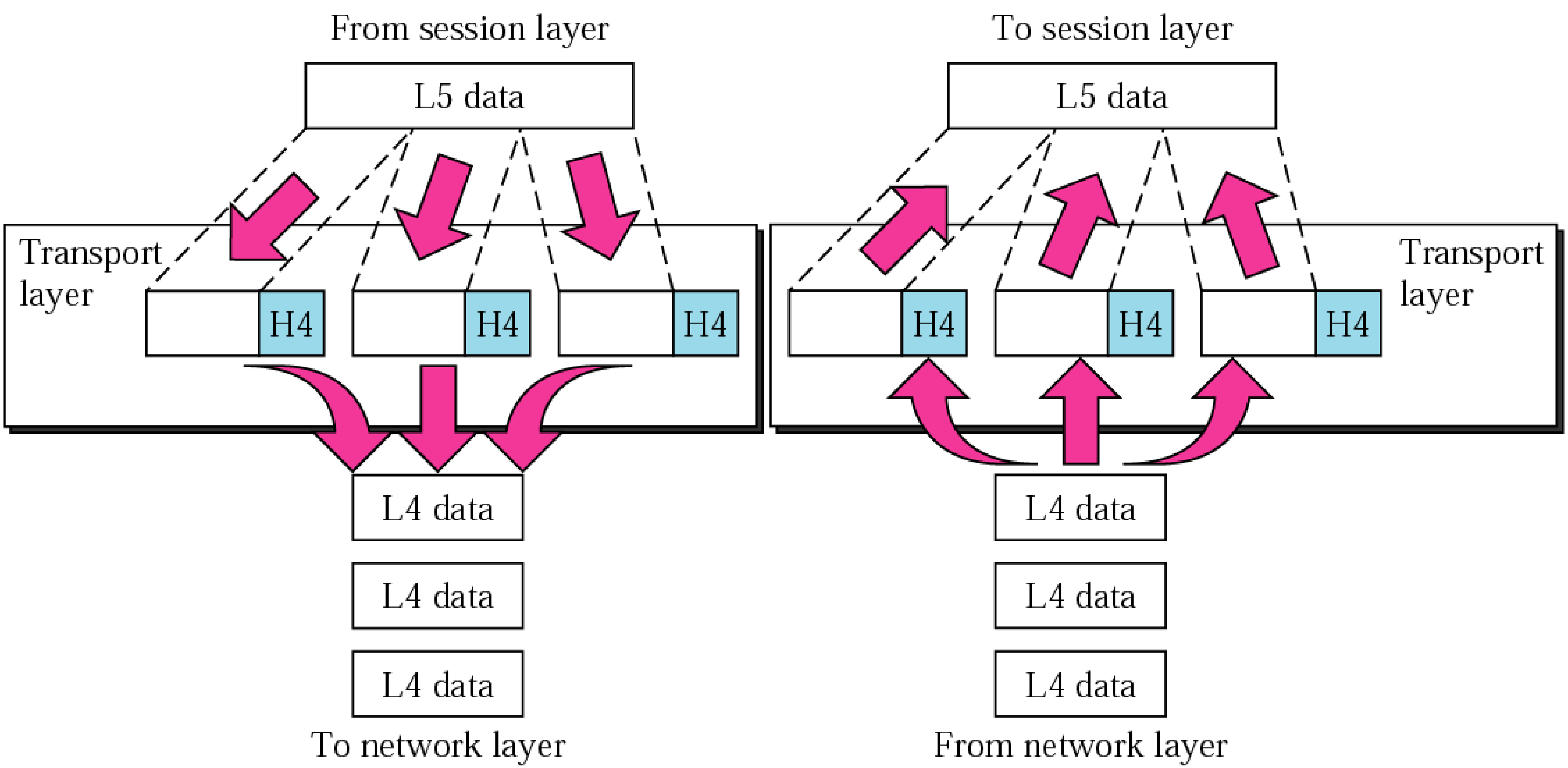


Figure 2-9

Transport Layer

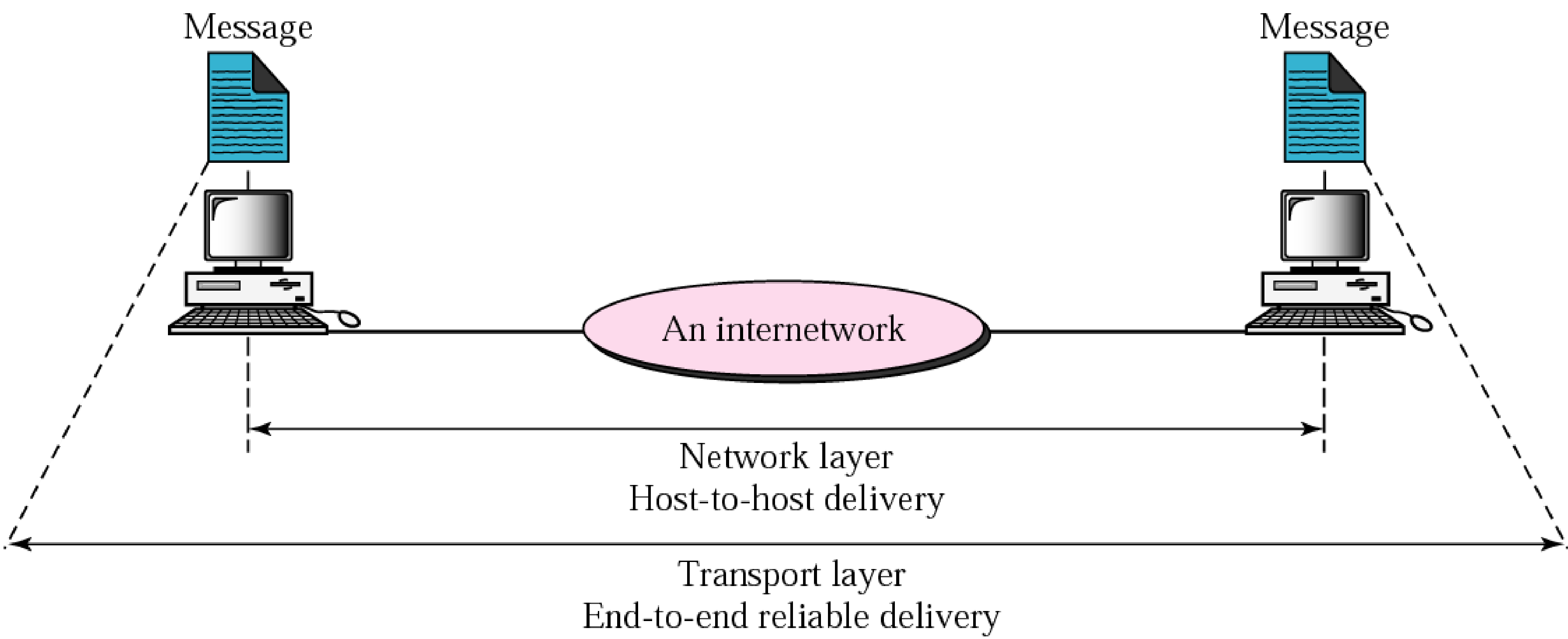


Transport layer

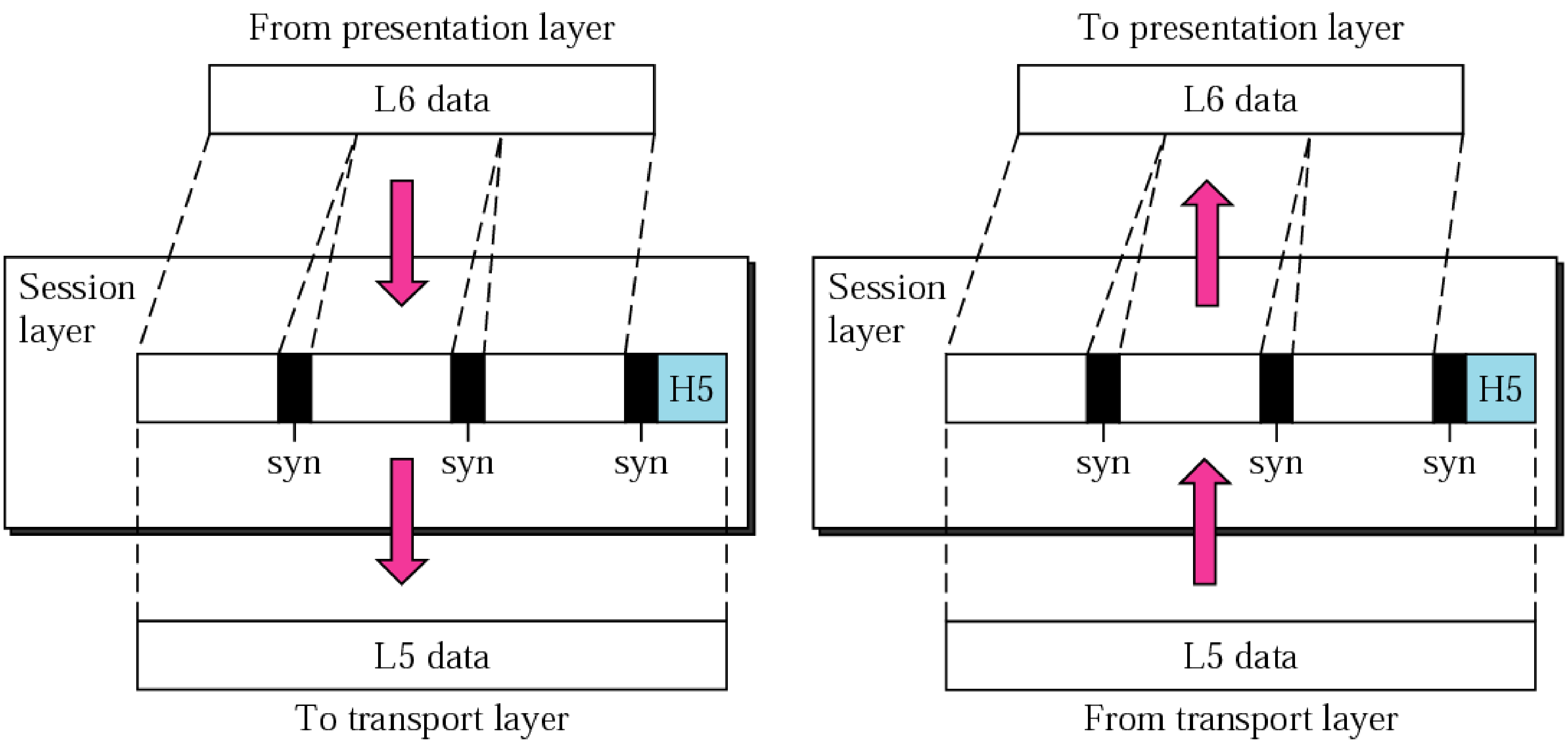
- the transport layer is responsible for the delivery of the message from one process to another .
- Other responsibilities of the transport layer:

1. Service- point addressing.
2. Segmentations and reassembly.
3. Connection control.
4. Flow control .
5. Error control.

Reliable end-to-end delivery of a message



Session Layer



Session layer

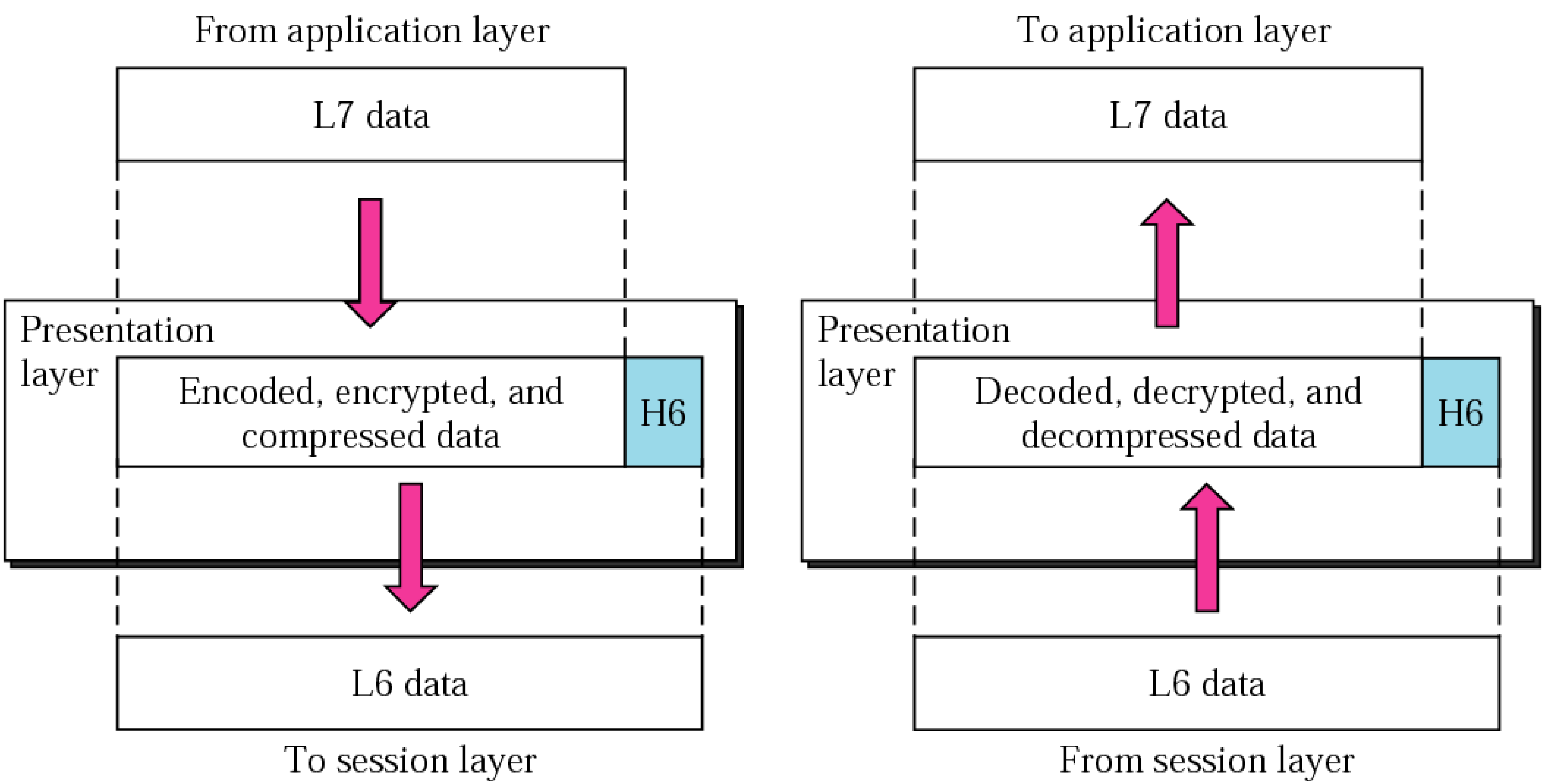
- The session layer is the network dialog controller
- It establishes, maintains and synchronizes the interaction between communicating system.

Specific responsibilities of the session layer:

1. dialog control :allows two system to enter a dialog .
2. synchronization point.

Figure 2-12

Presentation Layer



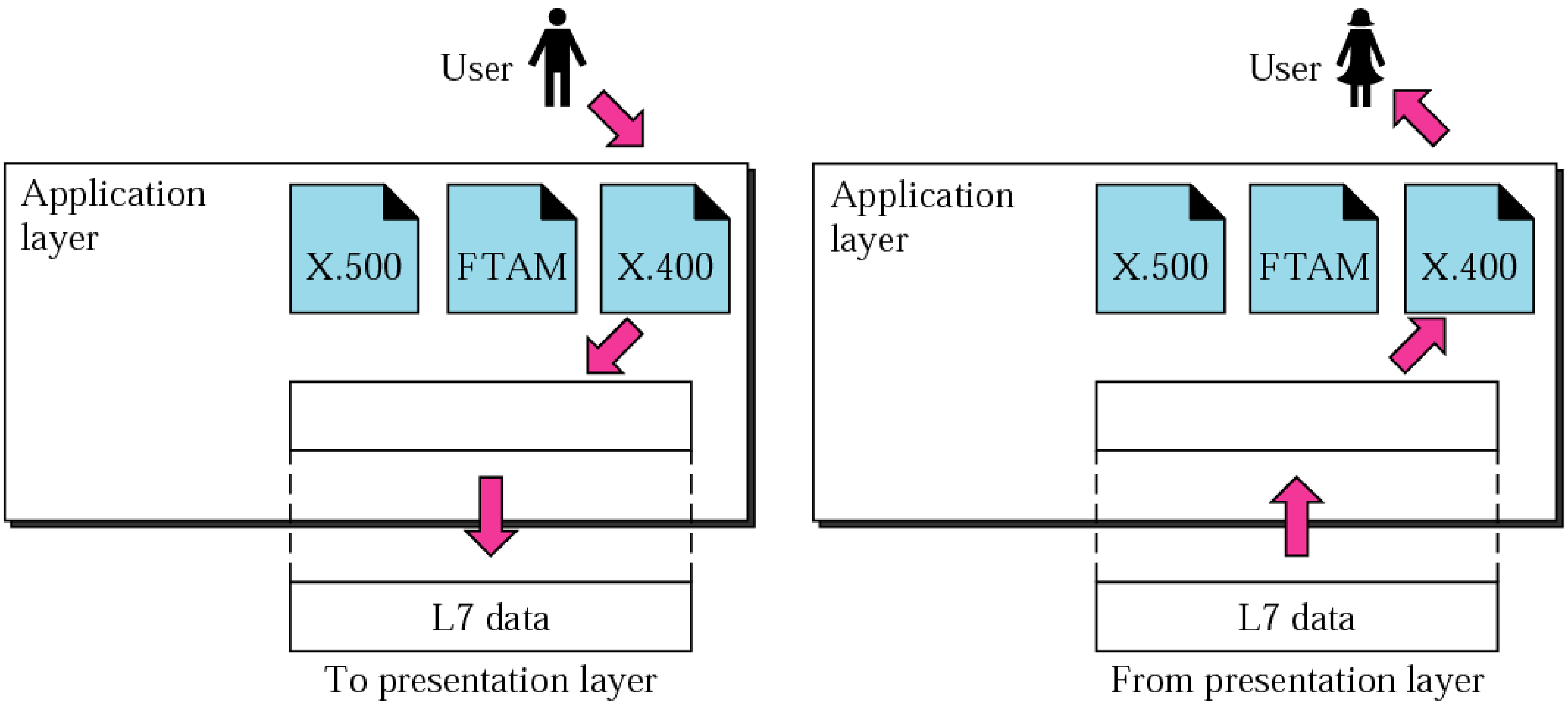
Presentation layer

- concerned with the syntax and semantics of the information exchanged between two systems.
- Specific responsibilities of the presentation layer:

1. Translation
2. Encryptions
3. Compression

Figure 2-13

Application Layer



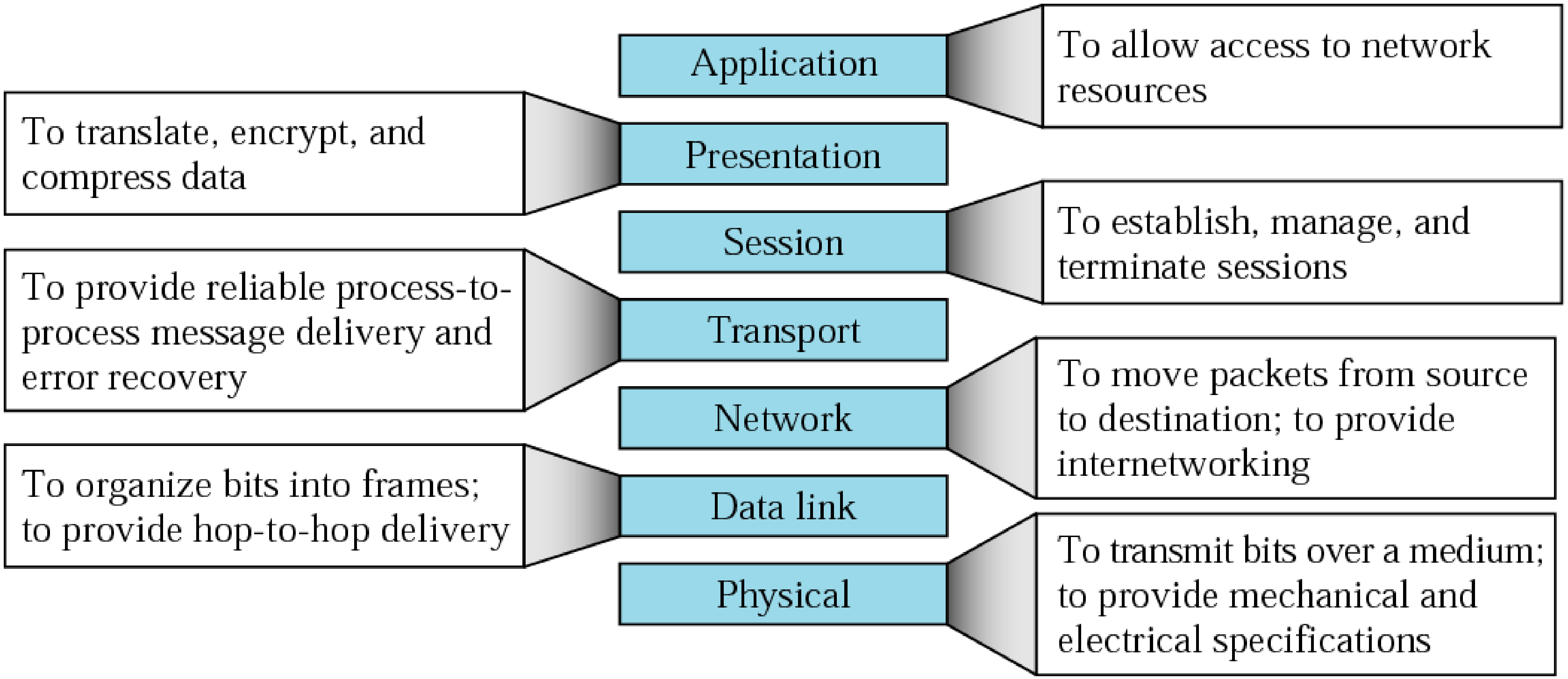
Application layer

- Enable the user ,whether human or software to access the network .
- Specific services provided by the application layer

1. network virtual terminal
2. File transfer ,access and management
3. Mail services
4. directory services

Figure 2-14

Summary of layers

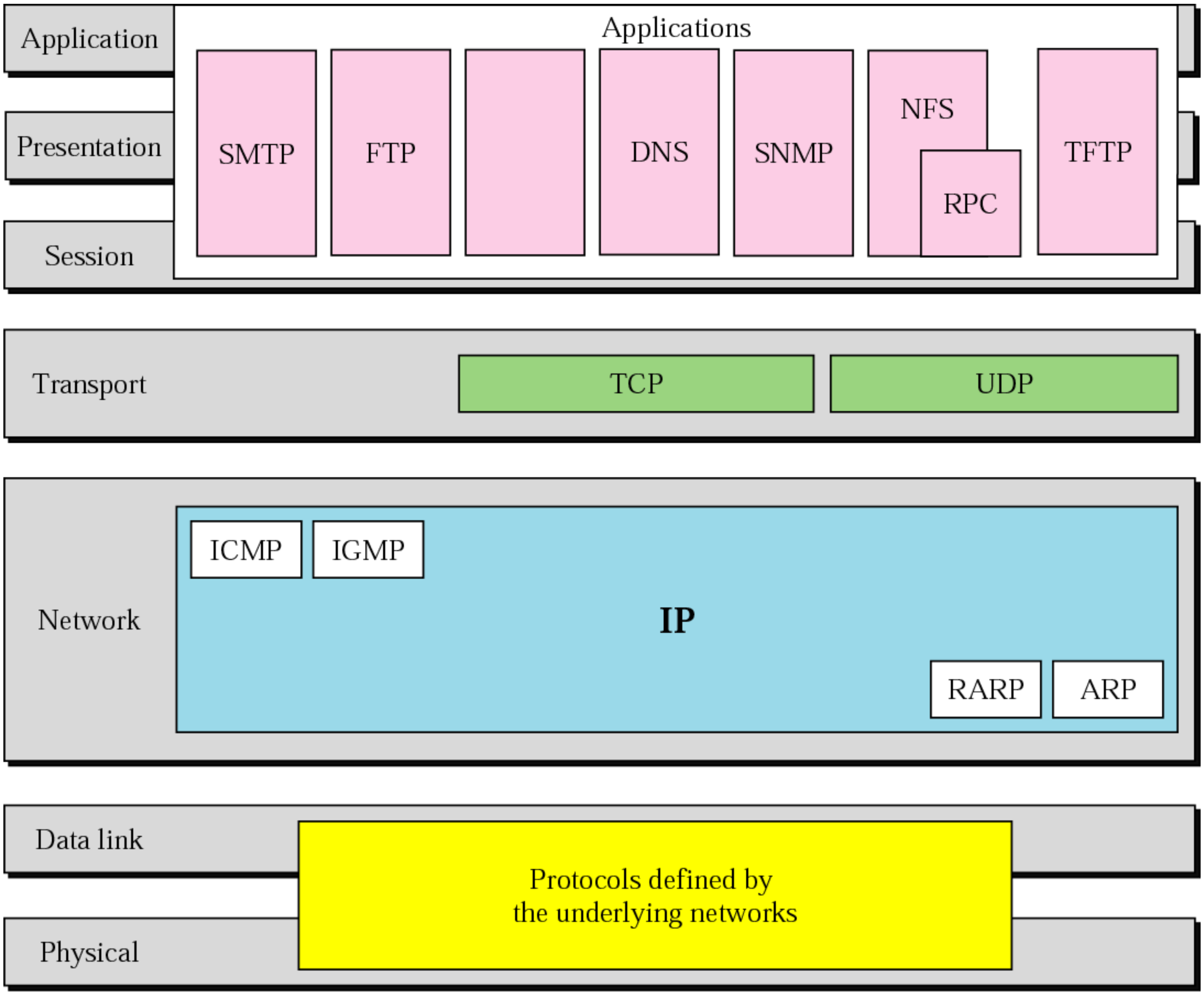


2.3

TCP/IP PROTOCOL SUITE

Figure 2-15

TCP/IP and OSI model



2.4

ADDRESSING

Addresses in TCP/IP

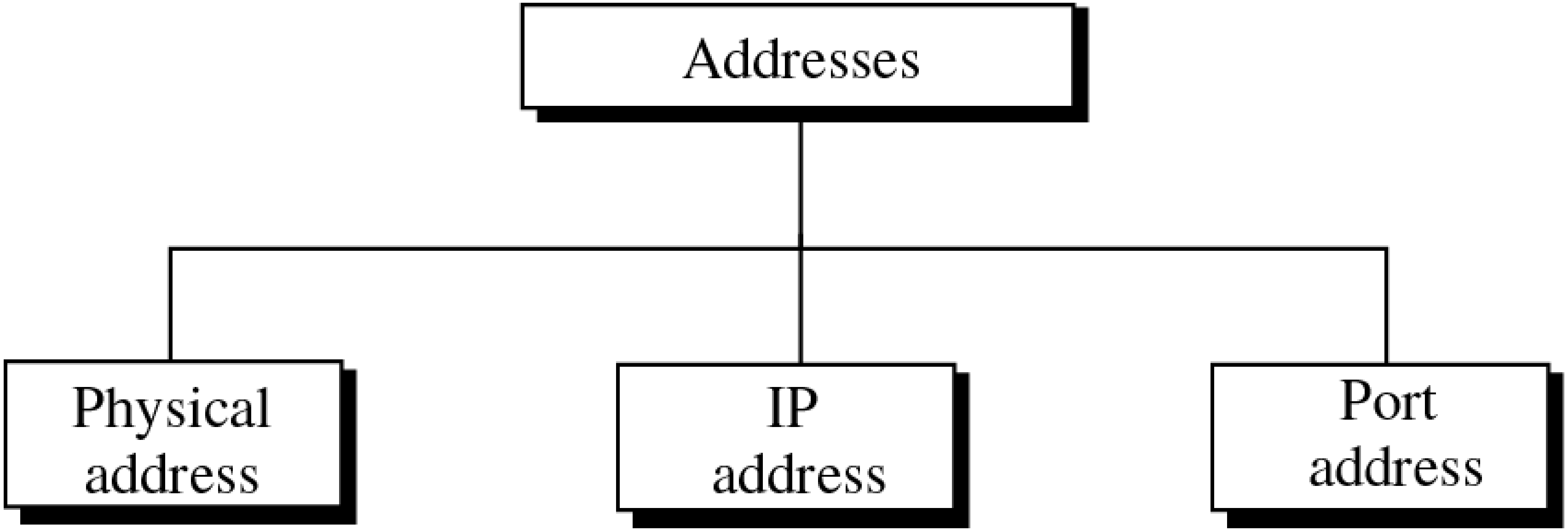
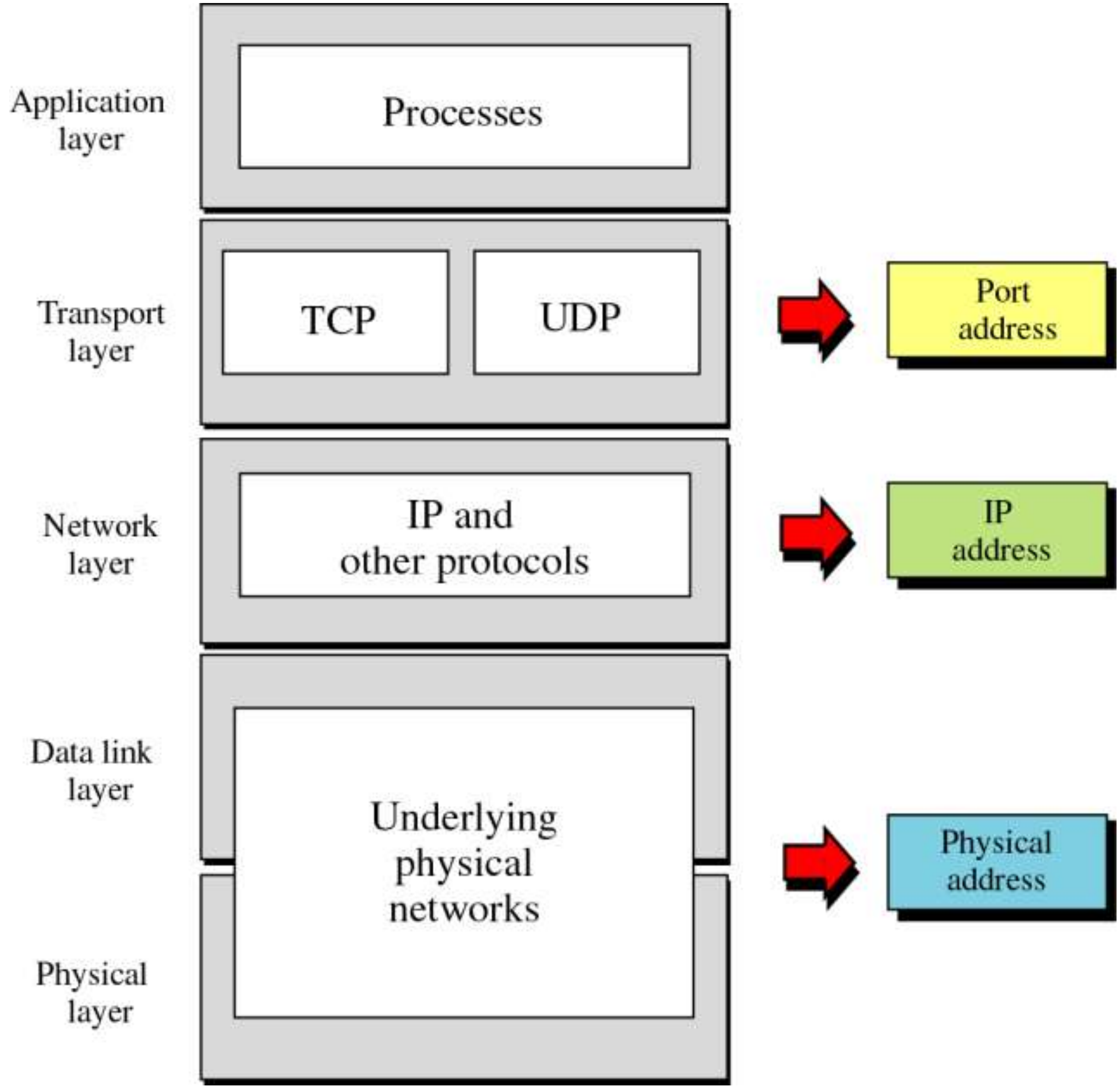
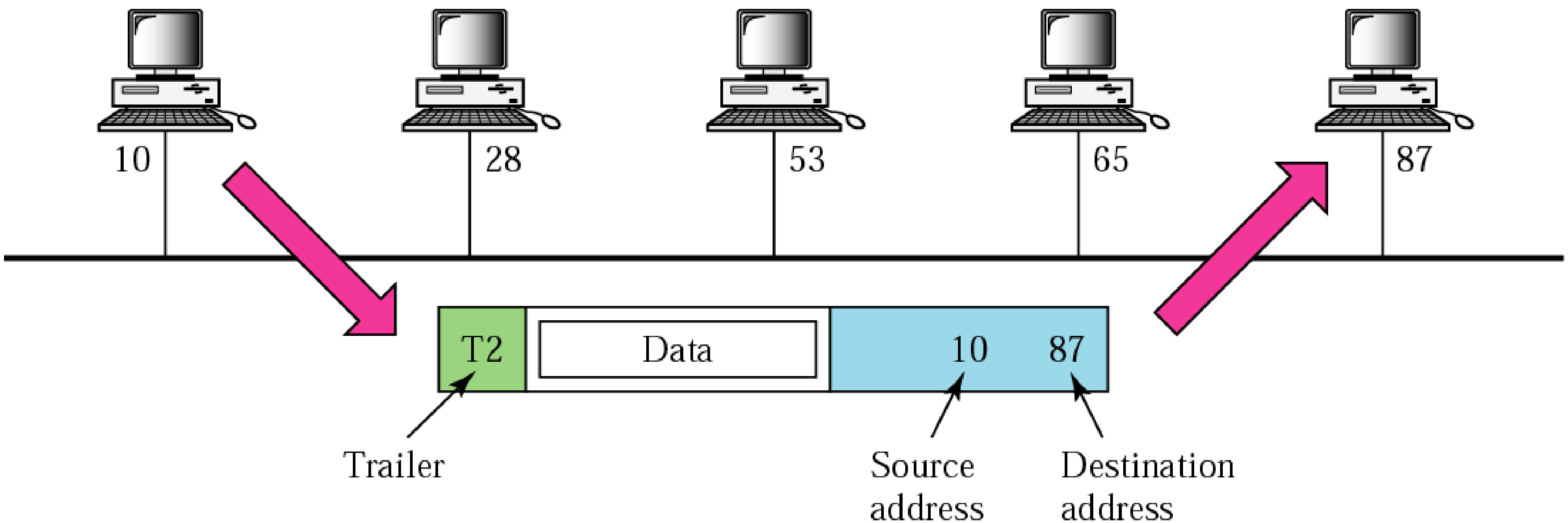


Figure 2-17



Relation-ship of layers and addresses in TCP/IP

Physical addresses



Example 2

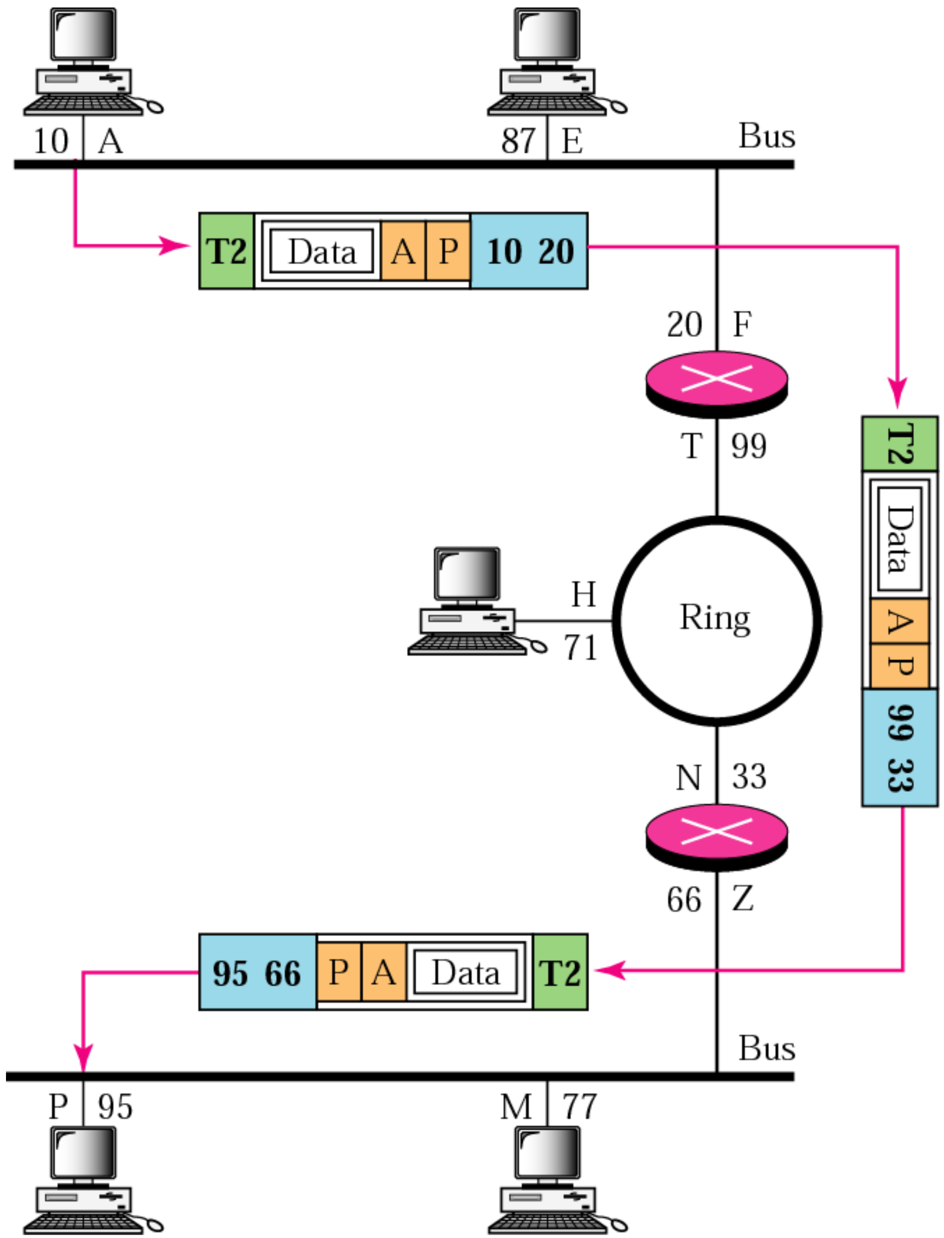
Most local area networks use a 48-bit (6 bytes) physical address written as 12 hexadecimal digits, with every 2 bytes separated by a hyphen as shown below:

07-01-02-01-2C-4B

A 6-byte (12 hexadecimal digits) physical address

Figure 2-19

IP addresses



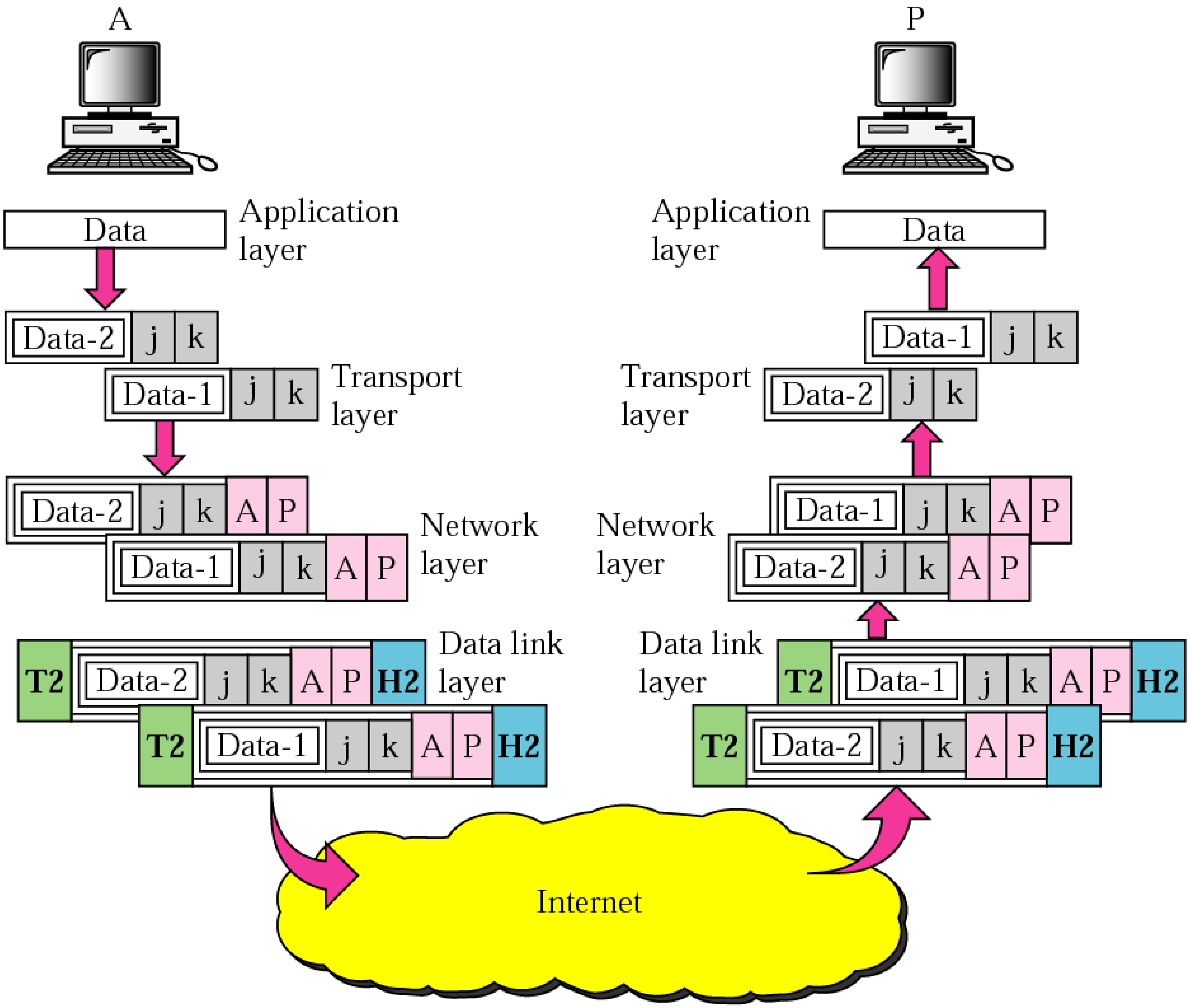
Example 4

As we will see in Chapter 4, an Internet address (in IPv4) is 32 bits in length, normally written as four decimal numbers, with each number representing 1 byte. The numbers are separated by a dot. Below is an example of such an address.

132.24.75.9

Figure 2-20

Port addresses



Example 6

As we will see in Chapters 11 and 12, a port address is a 16-bit address represented by one decimal number as shown below.

753	**A 16-bit port address**

2.5

TCP/IP VERSIONS

IP Versions:

- Version 4 (current)

The primary problem is that the Internet address is only 32 bits

- Version 6 (future)

Use 128bit addresses

Subnetting/Supernetting and Classless Addressing

CONTENTS

- SUBNETTING
- SUPERNETTING
- CLASSLESS ADDRSSING

5.1

SUBNETTING

Note

IP addresses are designed with two levels of hierarchy.

Figure 5-1

A network with two levels of hierarchy (not subnetted)

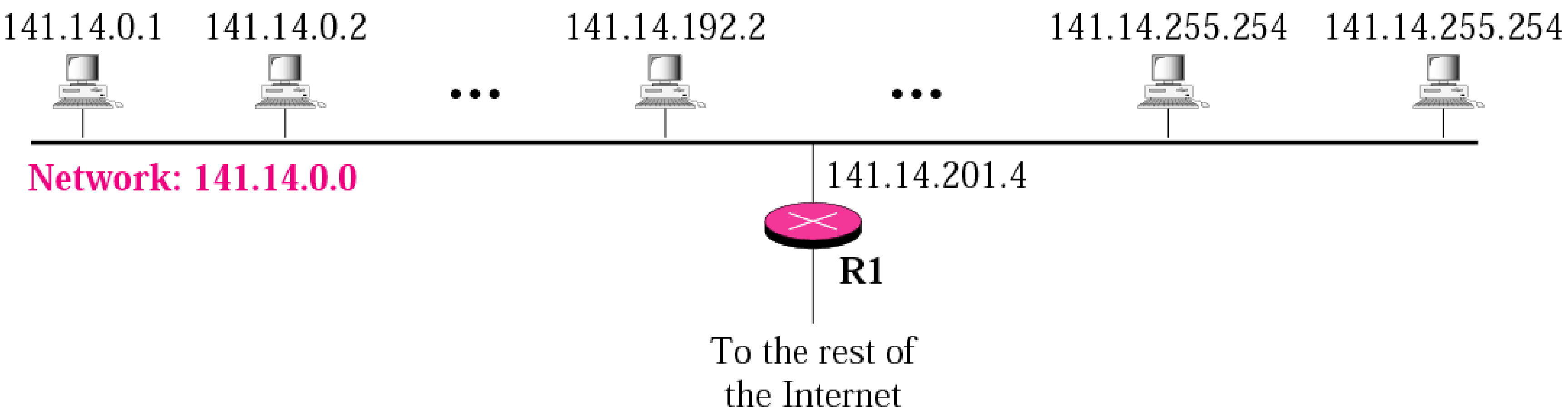


Figure 5-2

A network with three levels of hierarchy (subnetted)

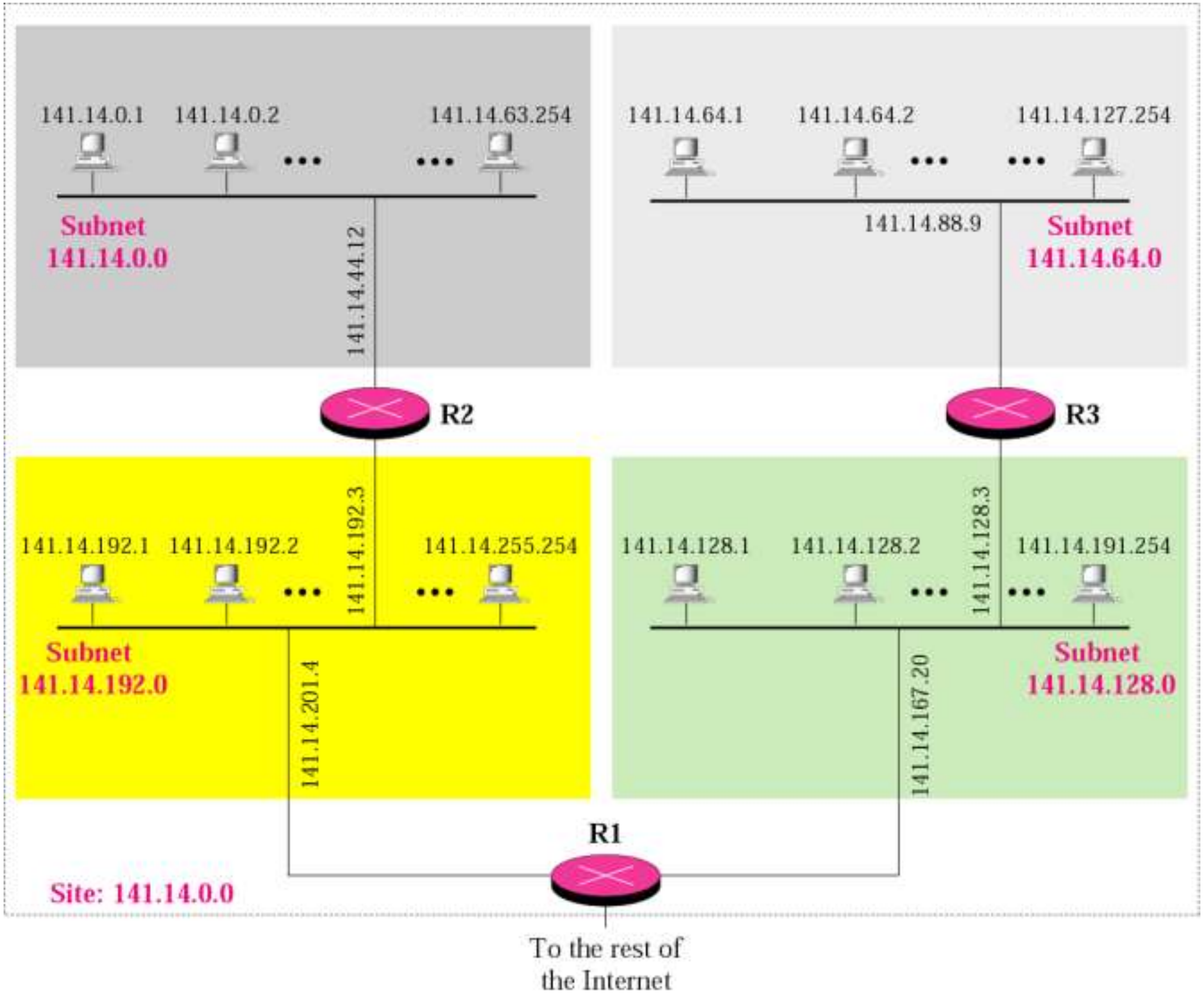
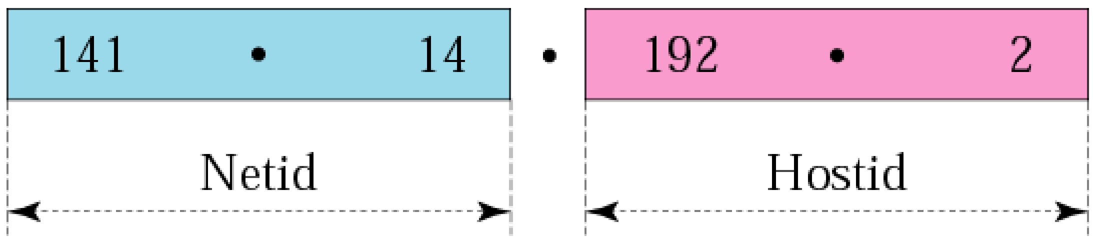
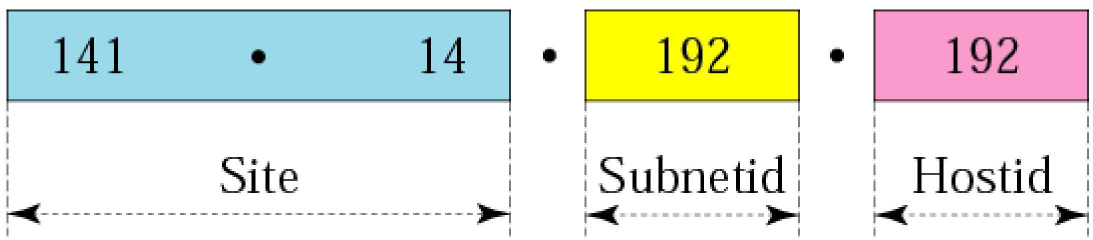


Figure 5-3

Addresses in a network with and without subnetting



a. Without subnetting



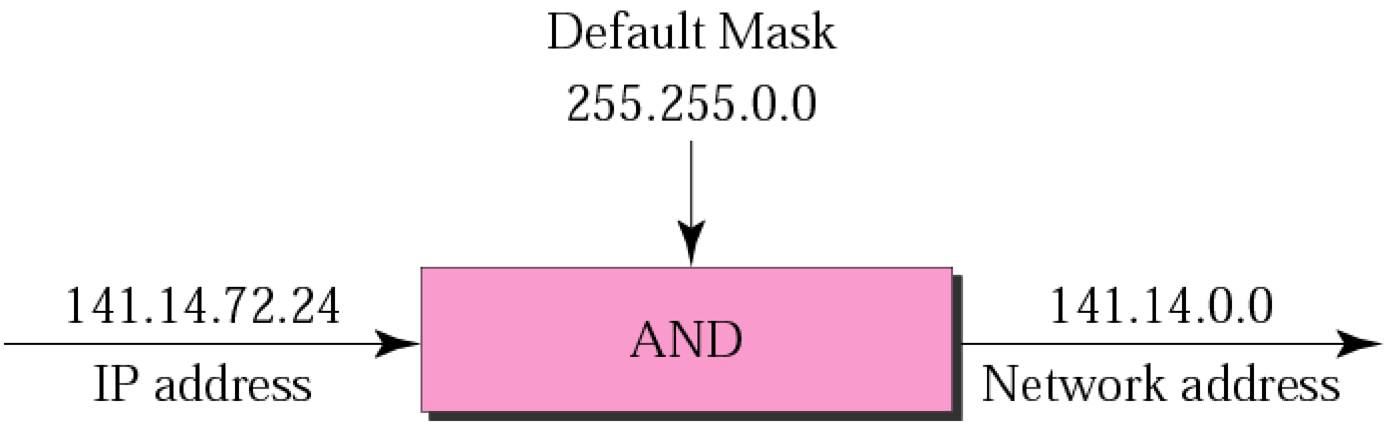
b. With subnetting

Figure 5-4

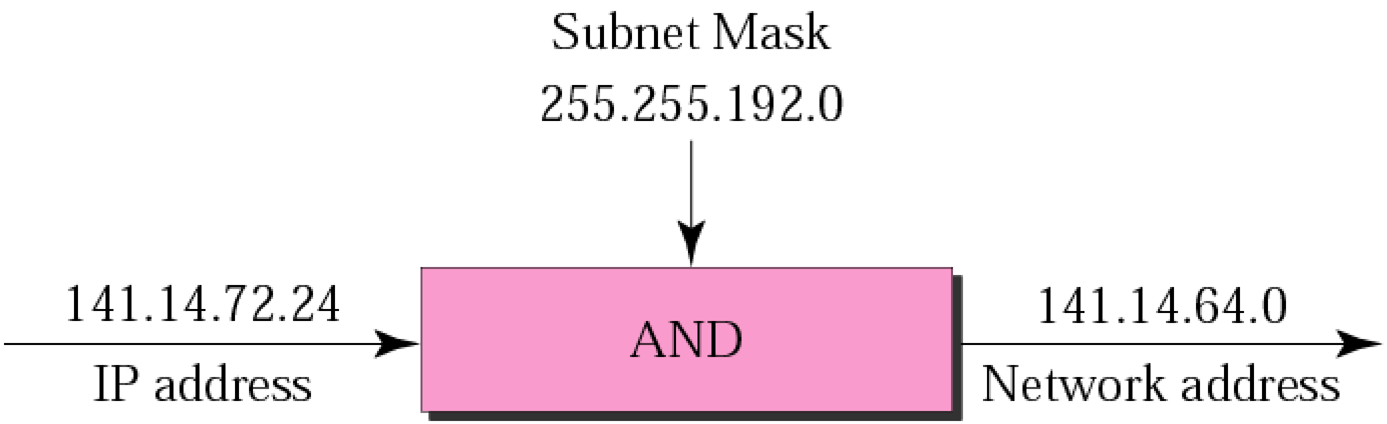
Hierarchy concept in a telephone number

Figure 5-5

Default mask and subnet mask



a. Without subnetting



b. With subnetting

Finding the Subnet Address

Given an IP address, we can find the subnet address the same way we found the network address in the previous chapter. We apply the mask to the address. We can do this in two ways: straight or short-cut.

Straight Method

In the straight method, we use binary notation for both the address and the mask and then apply the AND operation to find the subnet address.

Example 1

What is the subnetwork address if the destination address is 200.45.34.56 and the subnet mask is 255.255.240.0?

Solution

11001000 00101101 00100010 00111000

11111111 11111111 1111**0000** **00000000**

11001000 00101101 0010**0000** **00000000**

The subnetwork address is **200.45.32.0**.

Short-Cut Method

** If the byte in the mask is 255, copy the byte in the address.

** If the byte in the mask is 0, replace the byte in the address with 0.

** If the byte in the mask is neither 255 nor 0, we write the mask and the address in binary and apply the AND operation.

Example 2

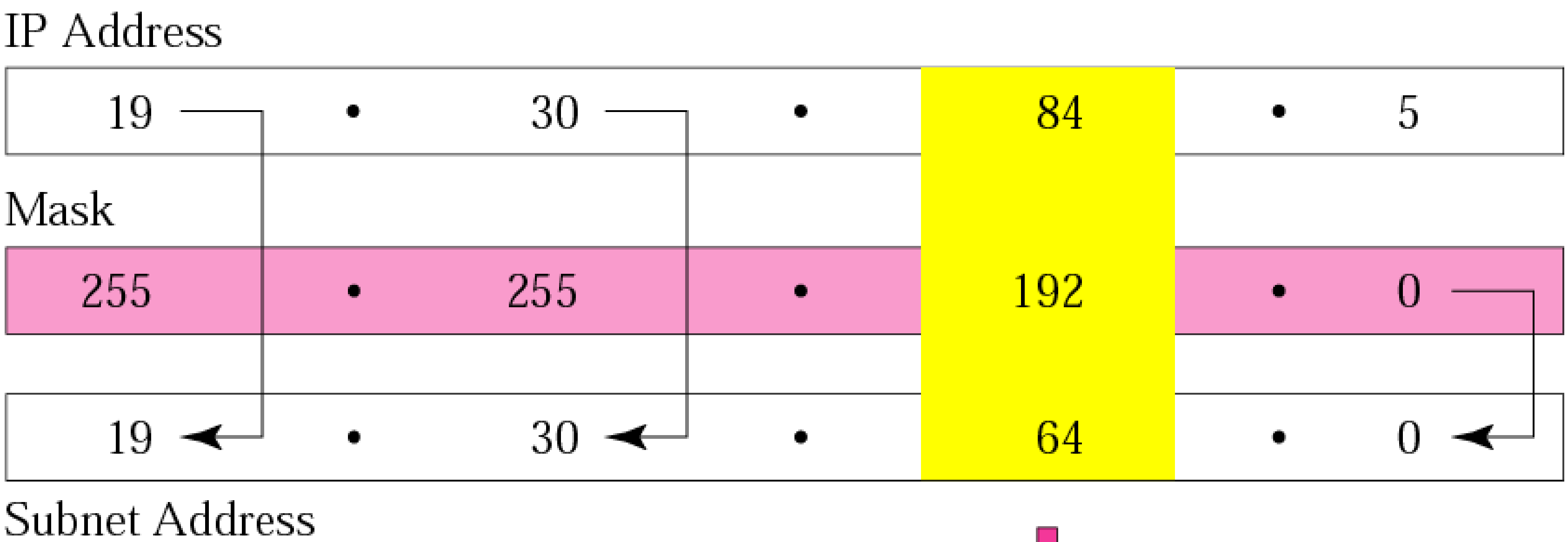
What is the subnetwork address if the destination address is 19.30.80.5 and the mask is 255.255.192.0?

Solution

See Figure 5.6

Figure 5-6

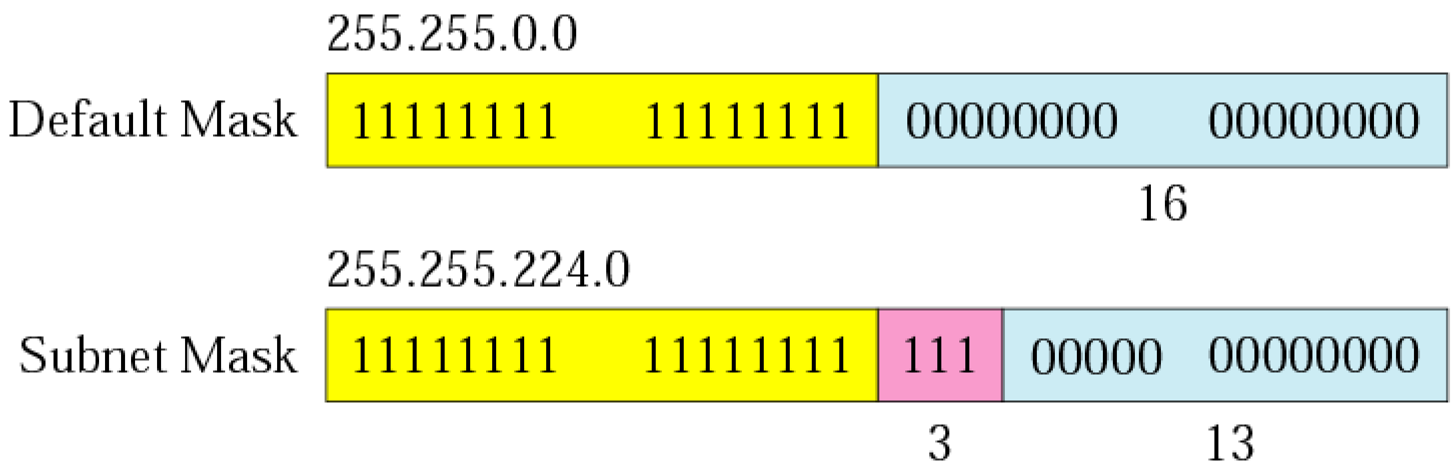
Example 2



84	0	1	0	1	0	1	0	0
192	1	1	0	0	0	0	0	0
64	0	1	0	0	0	0	0	0

Figure 5-7

Comparison of a default mask and a subnet mask



Note

The number of subnets must be a power of 2.

Example 3

A company is granted the site address 201.70.64.0 (class C). The company needs six subnets. Design the subnets.

Solution

The number of 1s in the default mask is 24 (class C).

Solution (Continued)

The company needs six subnets. This number 6 is not a power of 2. The next number that is a power of 2 is 8 (2^3). We need 3 more 1s in the subnet mask. The total number of 1s in the subnet mask is 27 (24 + 3).

The total number of 0s is 5 (32 – 27). The mask is

Solution (Continued)

<u>11111111 11111111 11111111</u> <u>111</u>00000

or

255.255.255.224

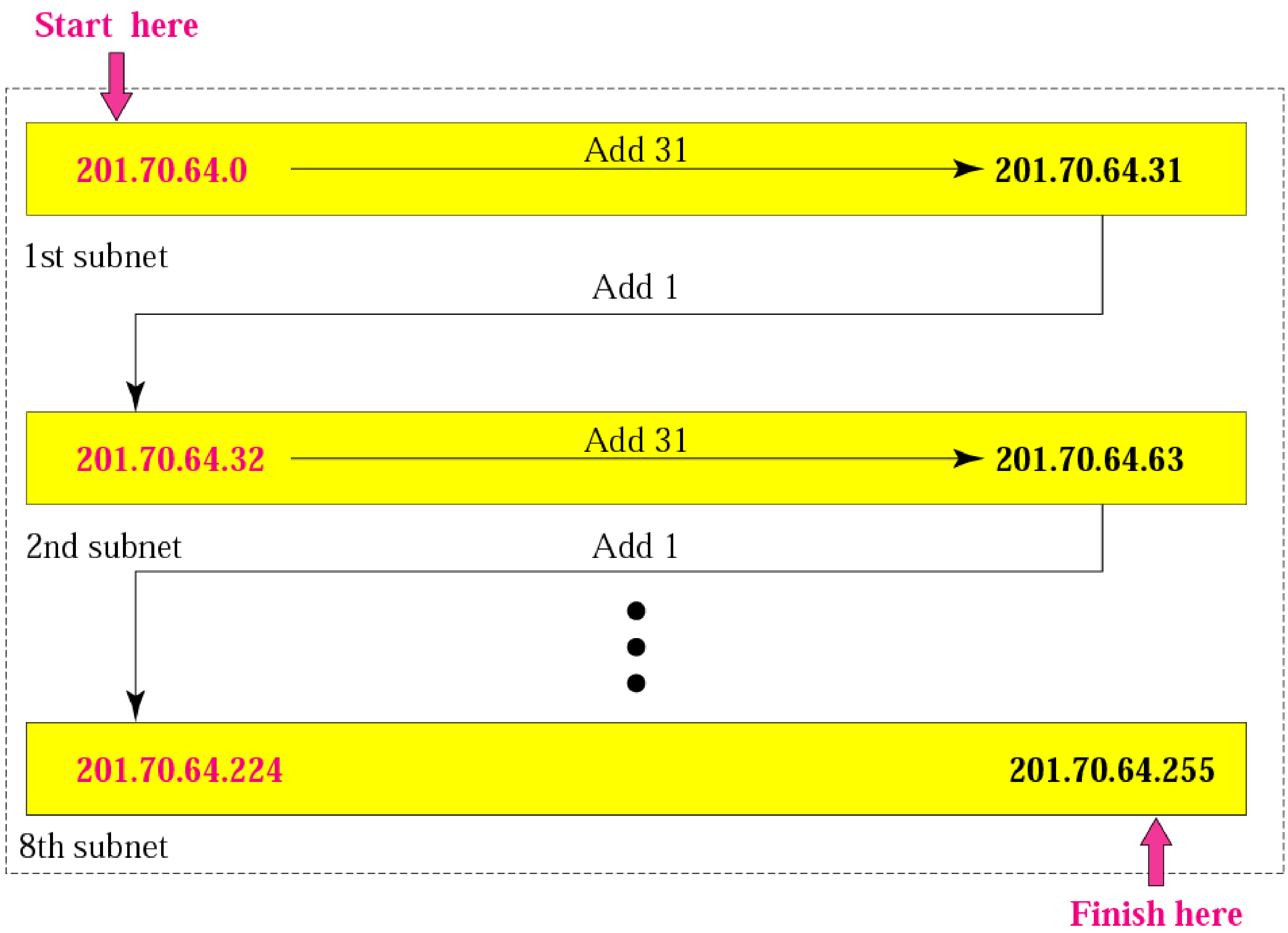
The number of subnets is 8.

The number of addresses in each subnet is 2^5 (5 is the number of 0s) or 32.

See Figure 5.8

Figure 5-8

Example 3



Example 4

A company is granted the site address 181.56.0.0 (class B). The company needs 1000 subnets. Design the subnets.

Solution

The number of 1s in the default mask is 16 (class B).

Solution (Continued)

The company needs 1000 subnets. This number is not a power of 2. The next number that is a power of 2 is 1024 (2^{10}). We need 10 more 1s in the subnet mask.

The total number of 1s in the subnet mask is 26 (16 + 10).

The total number of 0s is 6 (32 – 26).

Solution (Continued)

The mask is

11111111 11111111 11111111 11000000

or

255.255.255.192.

The number of subnets is 1024.

The number of addresses in each subnet is 2^6 (6 is the number of 0s) or 64.

See Figure 5.9

Figure 5-9

Example 4

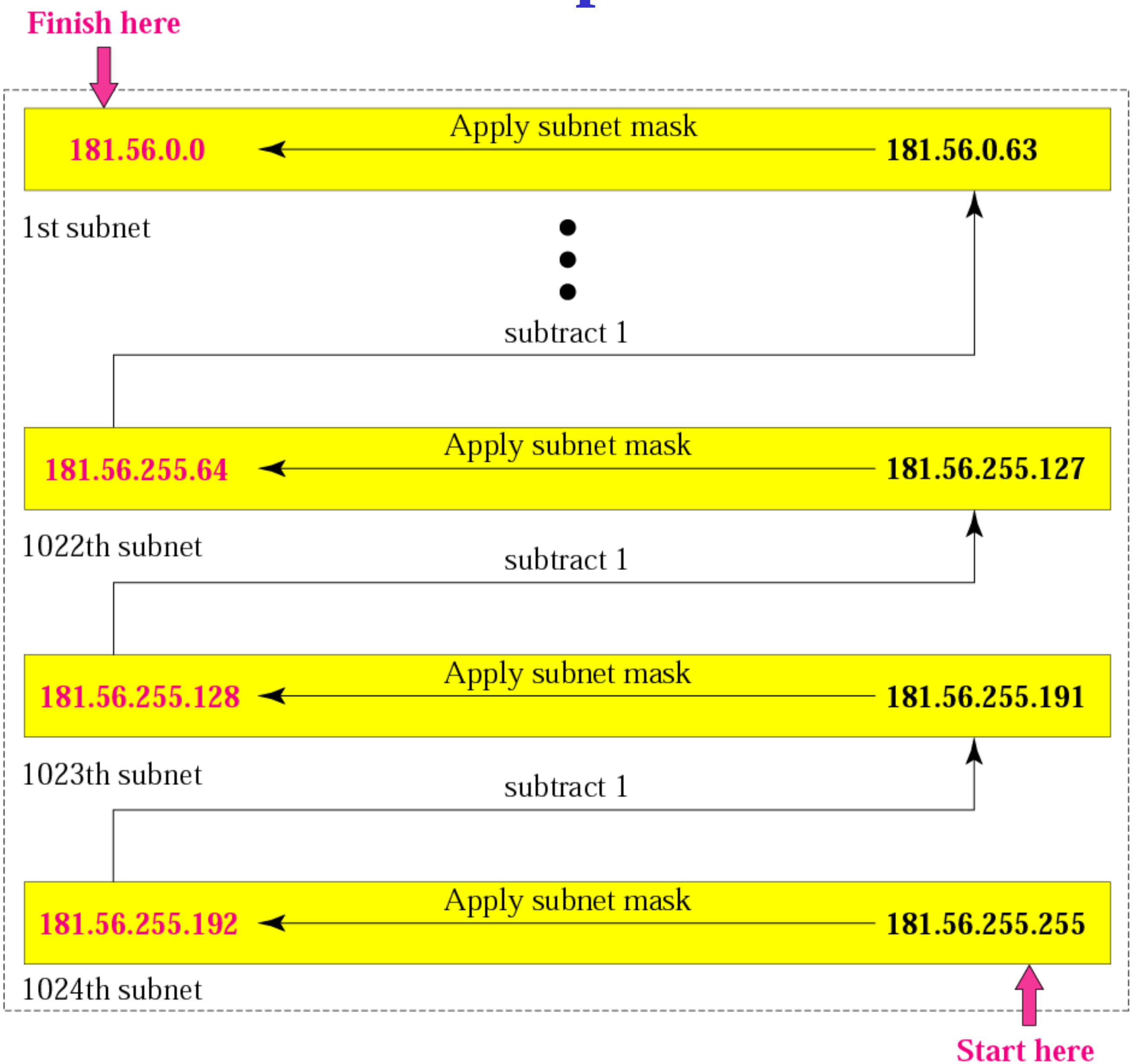
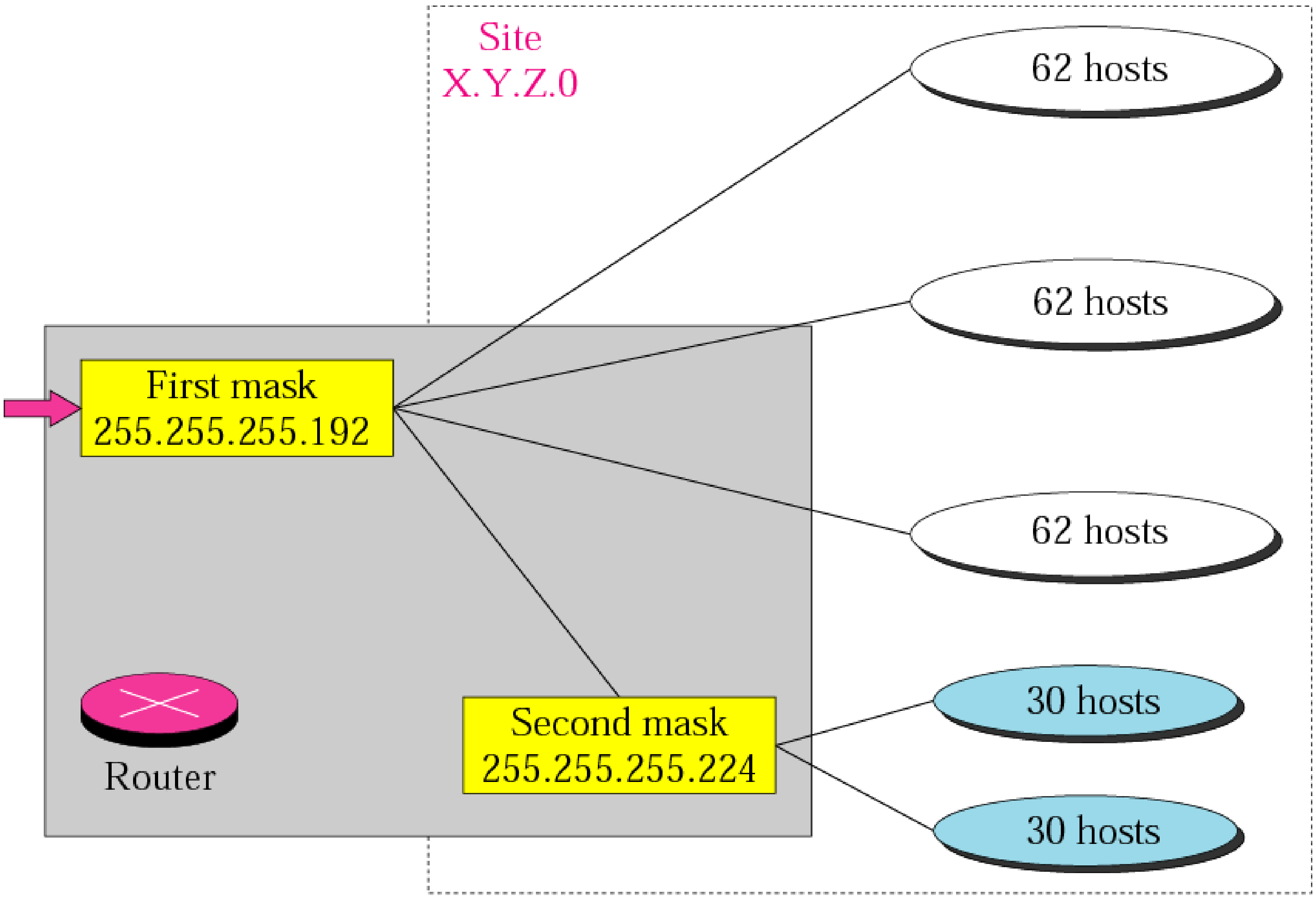


Figure 5-10

Variable-length subnetting

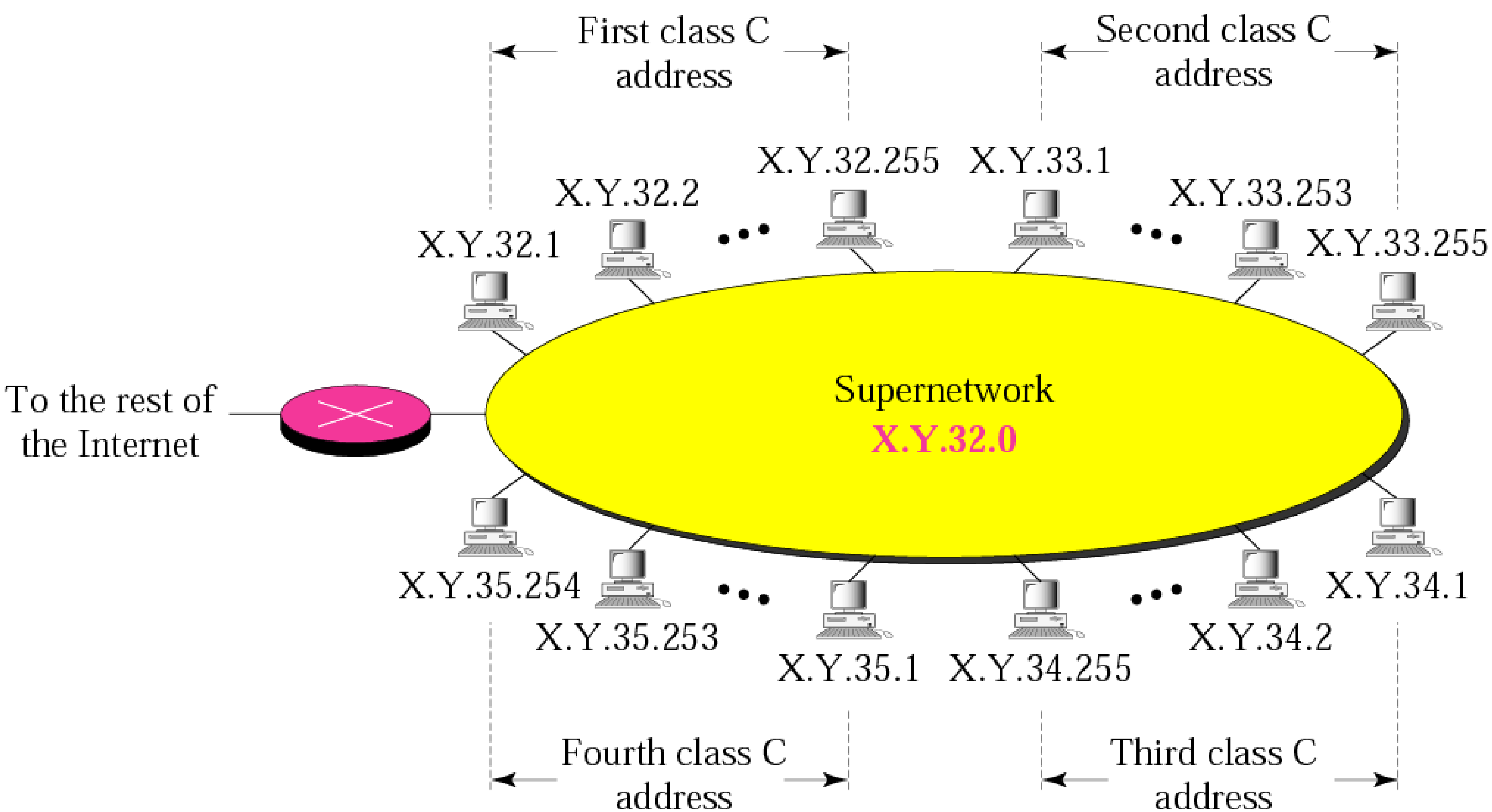


5.2

SUPERNETTING

Figure 5-11

A supernetwork



Rules:

** The number of blocks must be a power of 2 (1, 2, 4, 8, 16, . . .).

** The blocks must be contiguous in the address space (no gaps between the blocks).

** The third byte of the first address in the superblock must be evenly divisible by the number of blocks. In other words, if the number of blocks is N, the third byte must be divisible by N.

Example 5

A company needs 600 addresses. Which of the following set of class C blocks can be used to form a supernet for this company?

198.47.32.0 198.47.33.0 198.47.34.0

198.47.32.0 198.47.42.0 198.47.52.0 198.47.62.0

198.47.31.0 198.47.32.0 198.47.33.0 198.47.52.0

198.47.32.0 198.47.33.0 198.47.34.0 198.47.35.0

Solution

1: No, there are only three blocks.

2: No, the blocks are not contiguous.

3: No, 31 in the first block is not divisible by 4.

4: Yes, all three requirements are fulfilled.

Note

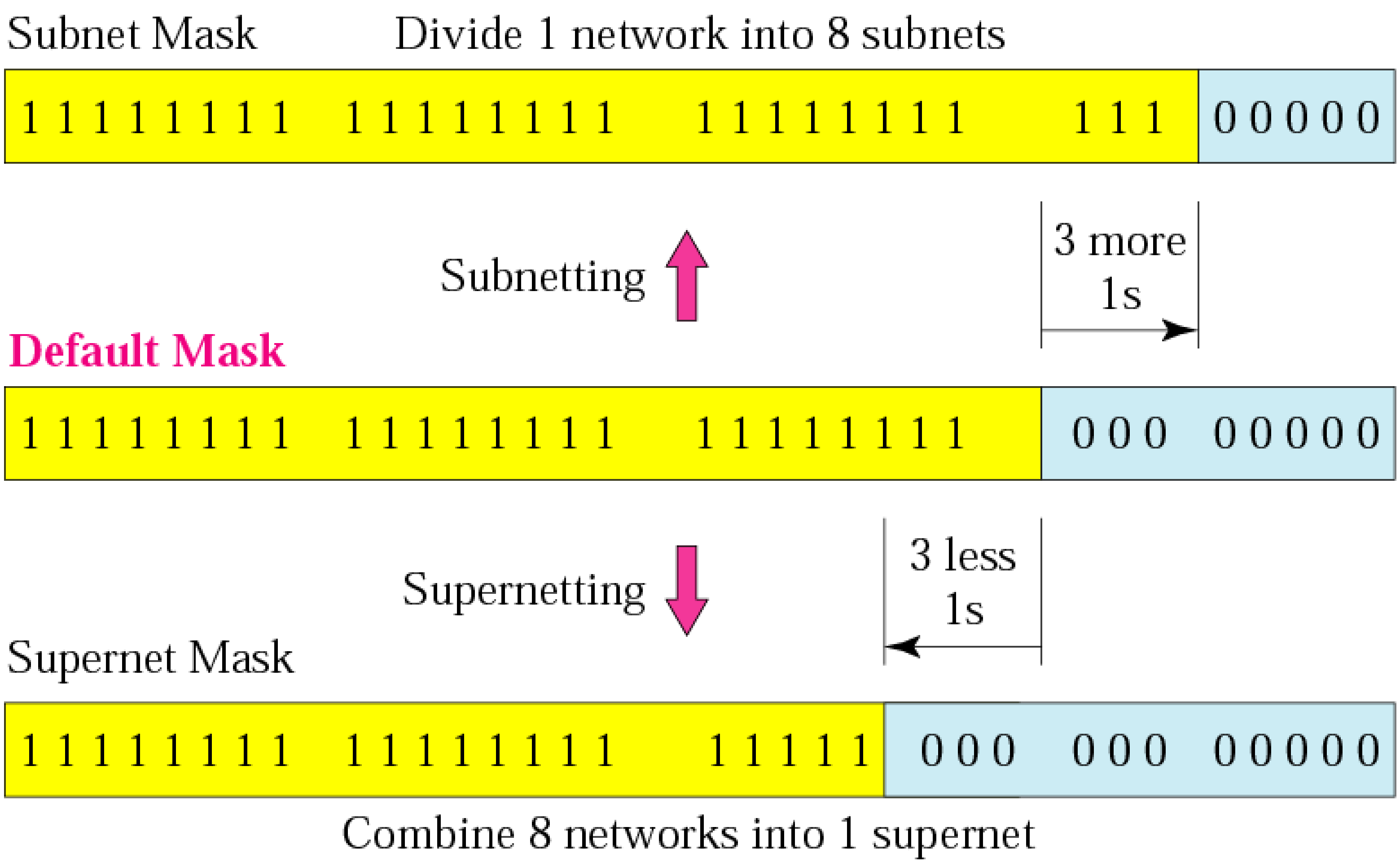
***In subnetting,
we need the first address of the subnet and the subnet mask to define the range of addresses.***

Note

**In supernetting,
we need the first address of
the supernet
and the supernet mask to
define the range of addresses.**

Figure 5-12

Comparison of subnet, default, and supernet masks



Example 6

We need to make a supernetwork out of 16 class C blocks. What is the supernet mask?

Solution

We need 16 blocks. For 16 blocks we need to change four 1s to 0s in the default mask. So the mask is

11111111 11111111 1111**0000** 00000000

or

255.255.240.0

Example 7

A supernet has a first address of 205.16.32.0 and a supernet mask of 255.255.248.0. A router receives three packets with the following destination addresses:

205.16.37.44

205.16.42.56

205.17.33.76

Which packet belongs to the supernet?

Solution

We apply the supernet mask to see if we can find the beginning address.

205.16.37.44 AND 255.255.248.0 → 205.16.32.0

205.16.42.56 AND 255.255.248.0 → 205.16.40.0

205.17.33.76 AND 255.255.248.0 → 205.17.32.0

Only the first address belongs to this supernet.

Example 8

A supernet has a first address of 205.16.32.0 and a supernet mask of 255.255.248.0. How many blocks are in this supernet and what is the range of addresses?

Solution

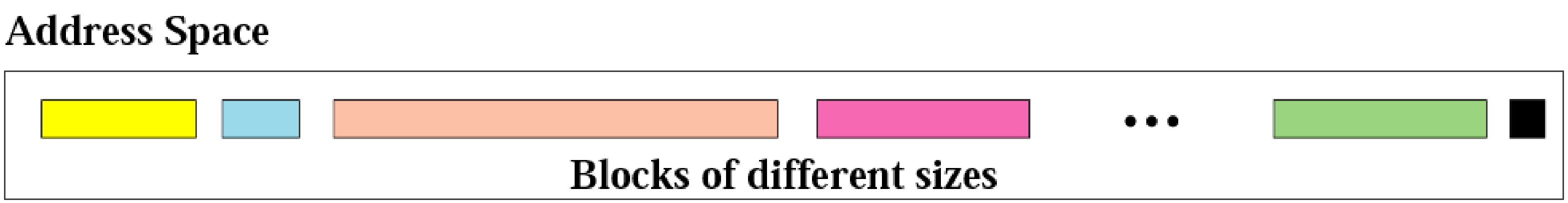
The supernet has 21 1s. The default mask has 24 1s. Since the difference is 3, there are 2^3 or 8 blocks in this supernet. The blocks are 205.16.32.0 to 205.16.39.0. The first address is 205.16.32.0. The last address is 205.16.39.255.

5.3

CLASSLESS ADDRESSING

Figure 5-13

Variable-length blocks



Number of Addresses in a Block

There is only one condition on the number of addresses in a block; it must be a power of 2 (2, 4, 8, . . .). A household may be given a block of 2 addresses. A small business may be given 16 addresses. A large organization may be given 1024 addresses.

Beginning Address

The beginning address must be evenly divisible by the number of addresses. For example, if a block contains 4 addresses, the beginning address must be divisible by 4. If the block has less than 256 addresses, we need to check only the rightmost byte. If it has less than 65,536 addresses, we need to check only the two rightmost bytes, and so on.

Example 9

Which of the following can be the beginning address of a block that contains 16 addresses?

205.16.37.32
190.16.42.44
17.17.33.80
123.45.24.52

Solution

The address 205.16.37.32 is eligible because 32 is divisible by 16. The address 17.17.33.80 is eligible because 80 is divisible by 16.

Example 10

Which of the following can be the beginning address of a block that contains 1024 addresses?

205.16.37.32
190.16.42.0
17.17.32.0
123.45.24.52

Solution

To be divisible by 1024, the rightmost byte of an address should be 0 and the second rightmost byte must be divisible by 4. Only the address 17.17.32.0 meets this condition.

Slash notation

A.B.C.D/*n*

Note

Slash notation is also called CIDR notation.

Example 11

A small organization is given a block with the beginning address and the prefix length **205.16.37.24/29** (in slash notation). What is the range of the block?

Solution

The beginning address is 205.16.37.24. To find the last address we keep the first 29 bits and change the last 3 bits to 1s.

Beginning:**<u>11001111 00010000 00100101 00011</u>**000
Ending : **<u>11001111 00010000 00100101 00011</u>**111

There are only 8 addresses in this block.

Example 12

We can find the range of addresses in Example 11 by another method. We can argue that the length of the suffix is 32 – 29 or 3. So there are $2^3 = 8$ addresses in this block. If the first address is 205.16.37.24, the last address is 205.16.37.31 (24 + 7 = 31).

Note

A block in classes A, B, and C can easily be represented in slash notation as

A.B.C.D/ *n*

where *n* is either 8 (class A), 16 (class B), or 24 (class C).

Example 13

What is the network address if one of the addresses is 167.199.170.82/27?

Solution

The prefix length is 27, which means that we must keep the first 27 bits as is and change the remaining bits (5) to 0s. The 5 bits affect only the last byte. The last byte is 01010010. Changing the last 5 bits to 0s, we get 01000000 or 64. The network address is 167.199.170.64/27.

Example 14

An organization is granted the block 130.34.12.64/26. The organization needs to have four subnets. What are the subnet addresses and the range of addresses for each subnet?

Solution

The suffix length is 6. This means the total number of addresses in the block is 64 (2^6). If we create four subnets, each subnet will have 16 addresses.

Solution (Continued)

Let us first find the subnet prefix (subnet mask). We need four subnets, which means we need to add two more 1s to the site prefix. The subnet prefix is then /28.

Subnet 1: 130.34.12.64/28 to 130.34.12.79/28.

Subnet 2 : 130.34.12.80/28 to 130.34.12.95/28.

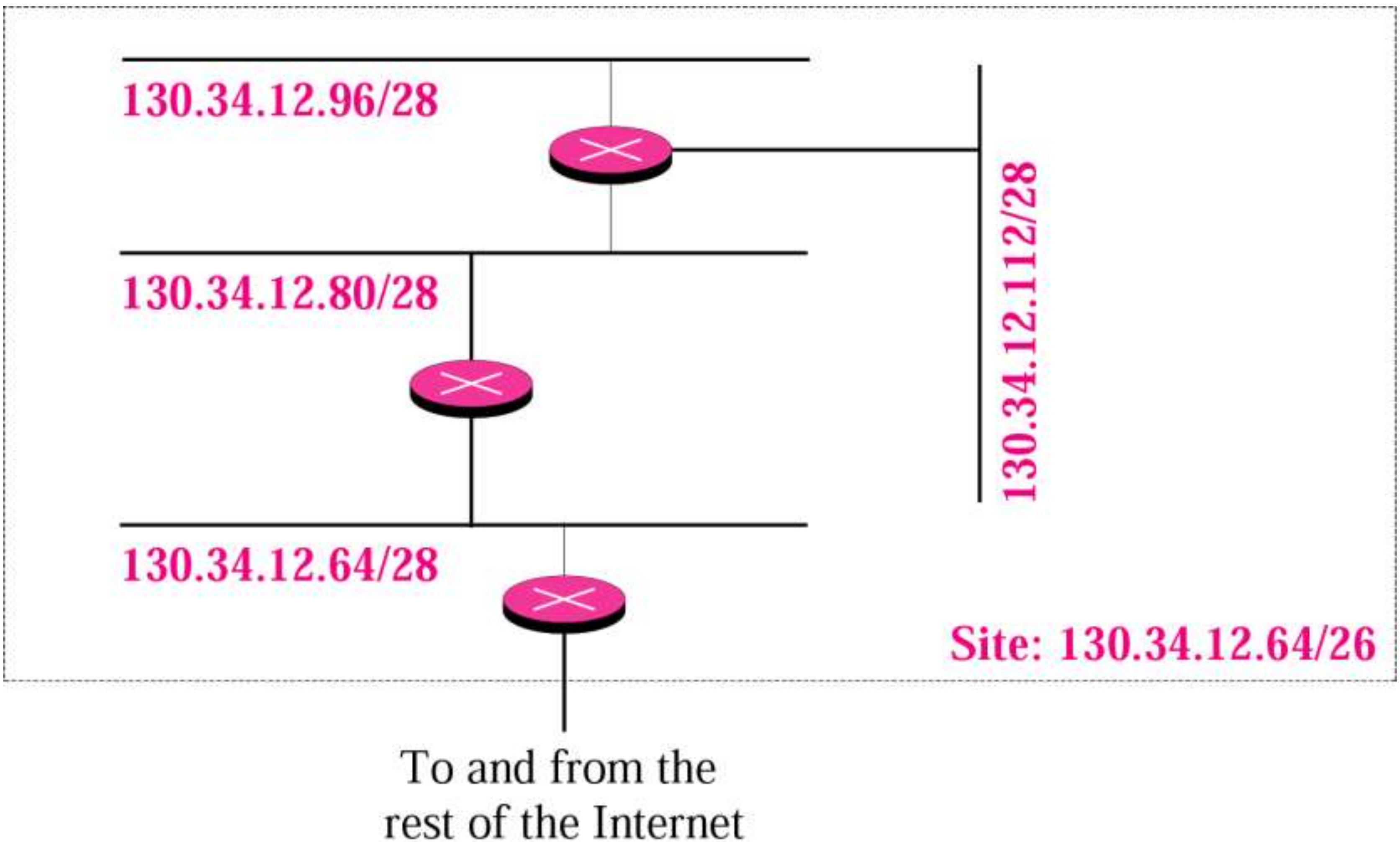
Subnet 3: 130.34.12.96/28 to 130.34.12.111/28.

Subnet 4: 130.34.12.112/28 to 130.34.12.127/28.

See Figure 5.15

Figure 5-15

Example 14



Example 15

An ISP is granted a block of addresses starting with 190.100.0.0/16. The ISP needs to distribute these addresses to three groups of customers as follows:

1. The first group has 64 customers; each needs 256 addresses.
2. The second group has 128 customers; each needs 128 addresses.
3. The third group has 128 customers; each needs 64 addresses.

Design the subblocks and give the slash notation for each subblock. Find out how many addresses are still available after these allocations.

Solution

Group 1

For this group, each customer needs 256 addresses. This means the suffix length is 8 ($2^8 = 256$). The prefix length is then $32 - 8 = 24$.

01: 190.100.0.0/24 → 190.100.0.255/24

02: 190.100.1.0/24 → 190.100.1.255/24

…………………………………..

64: 190.100.63.0/24 → 190.100.63.255/24

Total = $64 \times 256 = 16{,}384$

Solution (Continued)

Group 2

For this group, each customer needs 128 addresses. This means the suffix length is 7 ($2^7 = 128$). The prefix length is then 32 − 7 = 25. The addresses are:

001: 190.100.64.0/25 → 190.100.64.127/25

002: 190.100.64.128/25 → 190.100.64.255/25

003: 190.100.127.128/25 → 190.100.127.255/25

Total = 128 × 128 = 16,384

Solution (Continued)

Group 3

For this group, each customer needs 64 addresses. This means the suffix length is 6 ($2^6 = 64$). The prefix length is then $32 - 6 = 26$.

001:190.100.128.0/26 → 190.100.128.63/26

002:190.100.128.64/26 → 190.100.128.127/26

…………………………

128:190.100.159.192/26 → 190.100.159.255/26

Total = 128 × 64 = 8,192

Solution (Continued)

Number of granted addresses: 65,536

Number of allocated addresses: 40,960

Number of available addresses: 24,576

Chapter 6

Delivery and Routing of IP Packets

CONTENTS

- CONNECTION
- DELIVERY
- ROUTING METHODS
- STATIC AND DYNAMIC ROUTING
- ROUTING TABLE AND MODULE
- CLASSLESS ADDRESSING

6.1

CONNECTION-ORIENTED VERSUS CONNECTIONLESS SERVICES

In a connection-oriented situation,
the network layer protocol
first makes a connection.

In a connectionless situation,
the network layer protocol treats each
packet independently,
with each packet having
no relationship to any other packet.

6.2

DIRECT VERSUS INDIRECT DELIVERY

Figure 6-1

Direct delivery

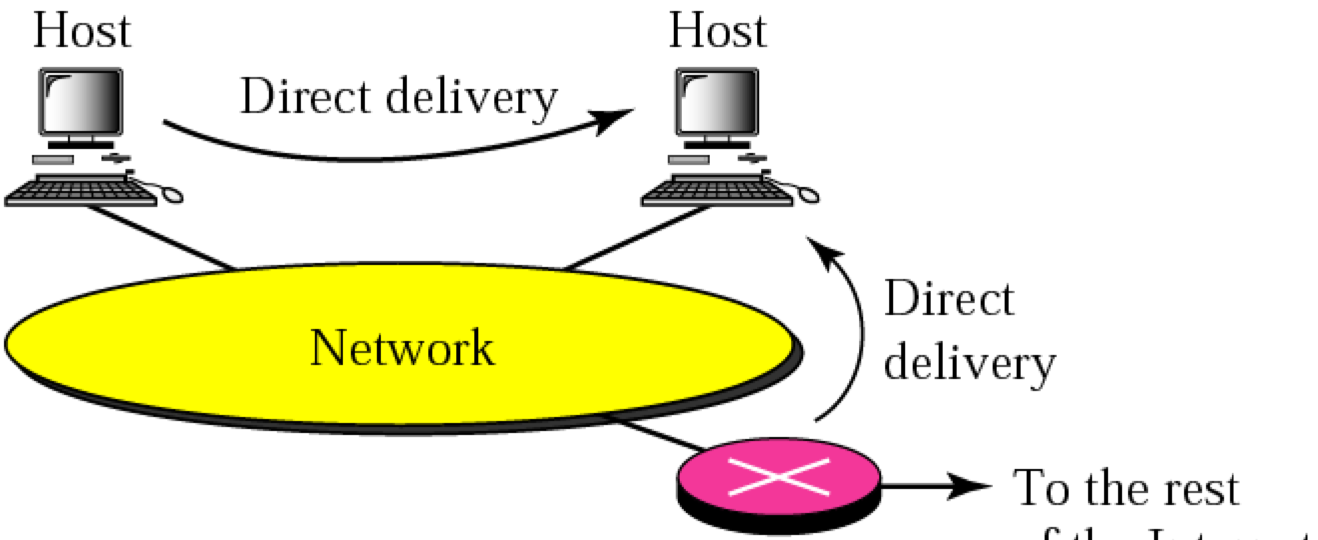
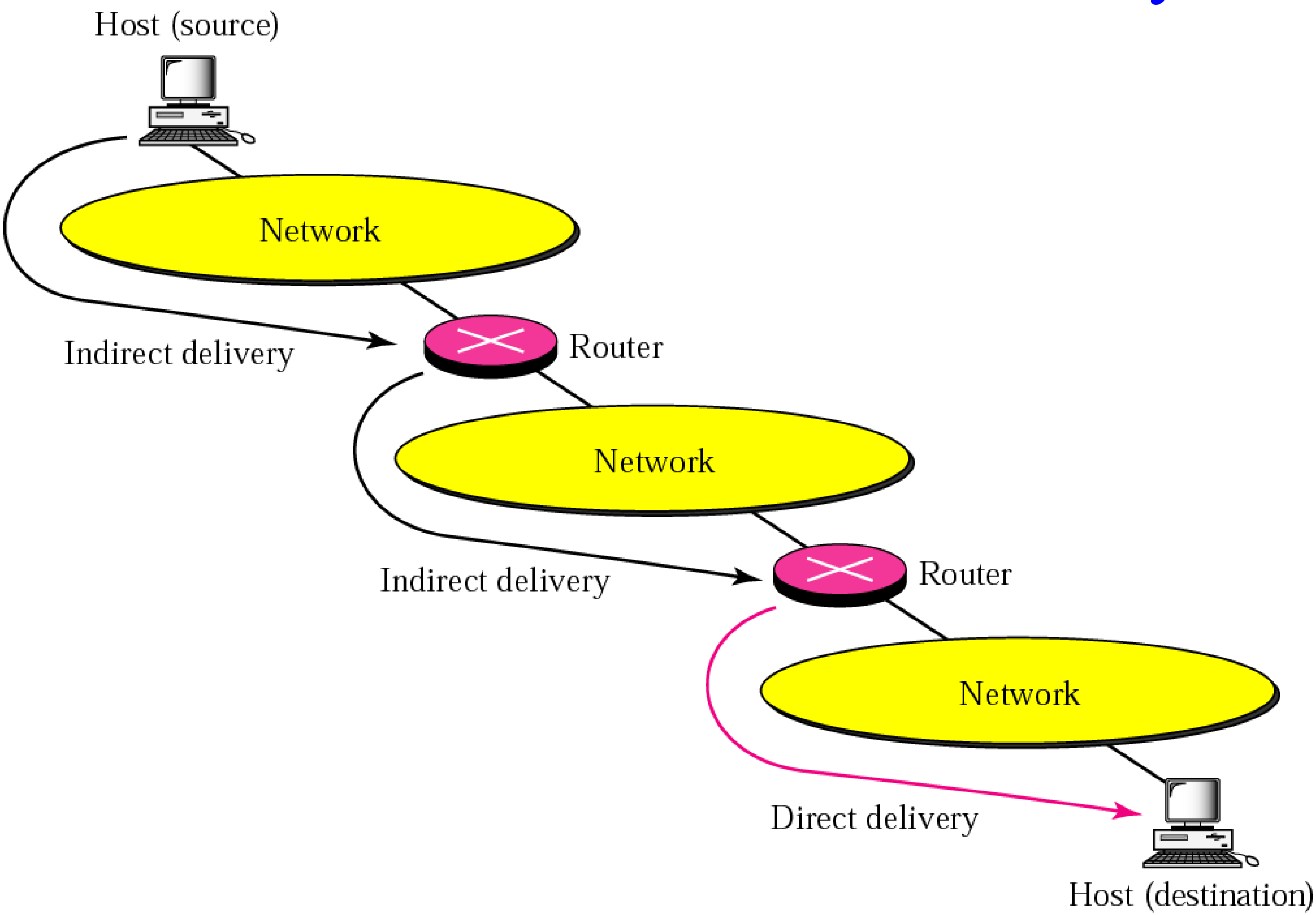


Figure 6-2

Indirect delivery



6.3

ROUTING METHODS

Next-hop routing

Routing table for host A

Destination	Route
Host B	R1, R2, Host B

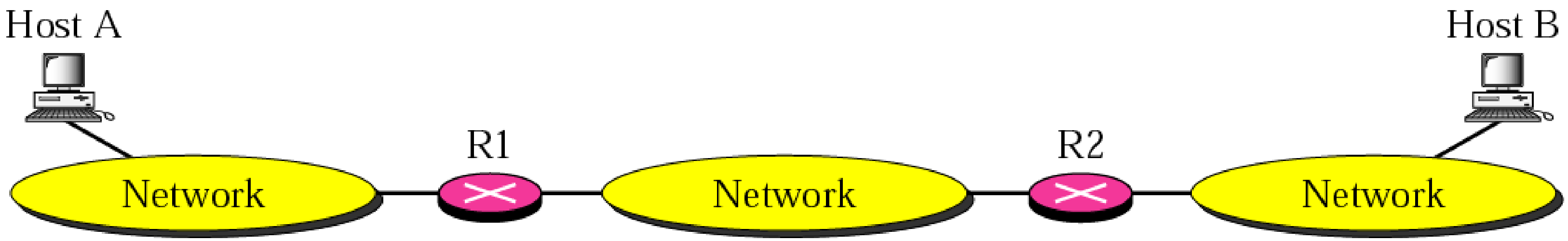
Routing table for R1

Destination	Route
Host B	R2, Host B

Routing table for R2

Destination	Route
Host B	Host B

a. Routing tables based on route



Routing table for host A

Destination	Next Hop
Host B	R1

Routing table for R1

Destination	Next Hop
Host B	R2

Routing table for R2

Destination	Next Hop
Host B	—

b. Routing tables based on next hop

Figure 6-4

Network-specific routing

Routing table for host S based on host-specific routing

Destination	Next Hop
A	R1
B	R1
C	R1
D	R1

Routing table for host S based on network-specific routing

Destination	Next Hop
N2	R1

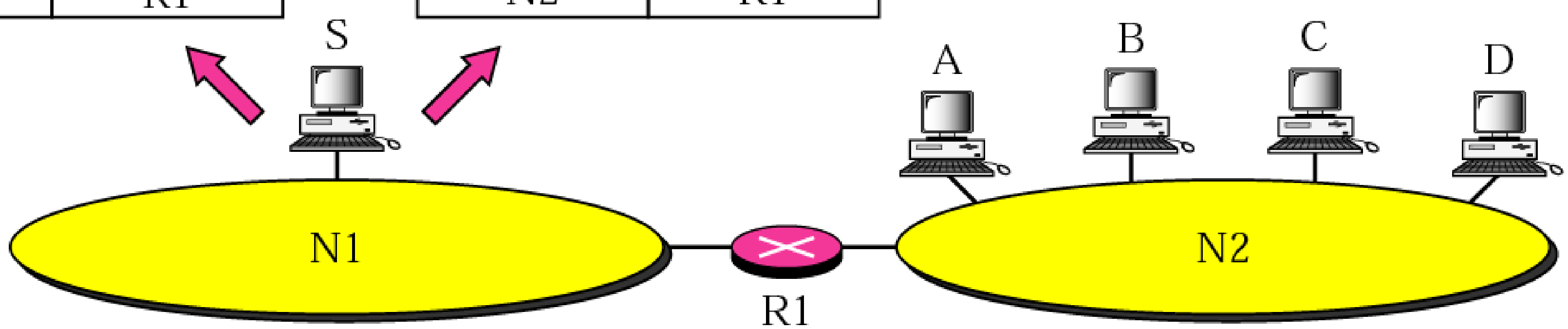


Figure 6-5

Host-specific routing

Routing table for host A

Destination	Next Hop
Host B	R3
N2	R1
N3	R3
......	......

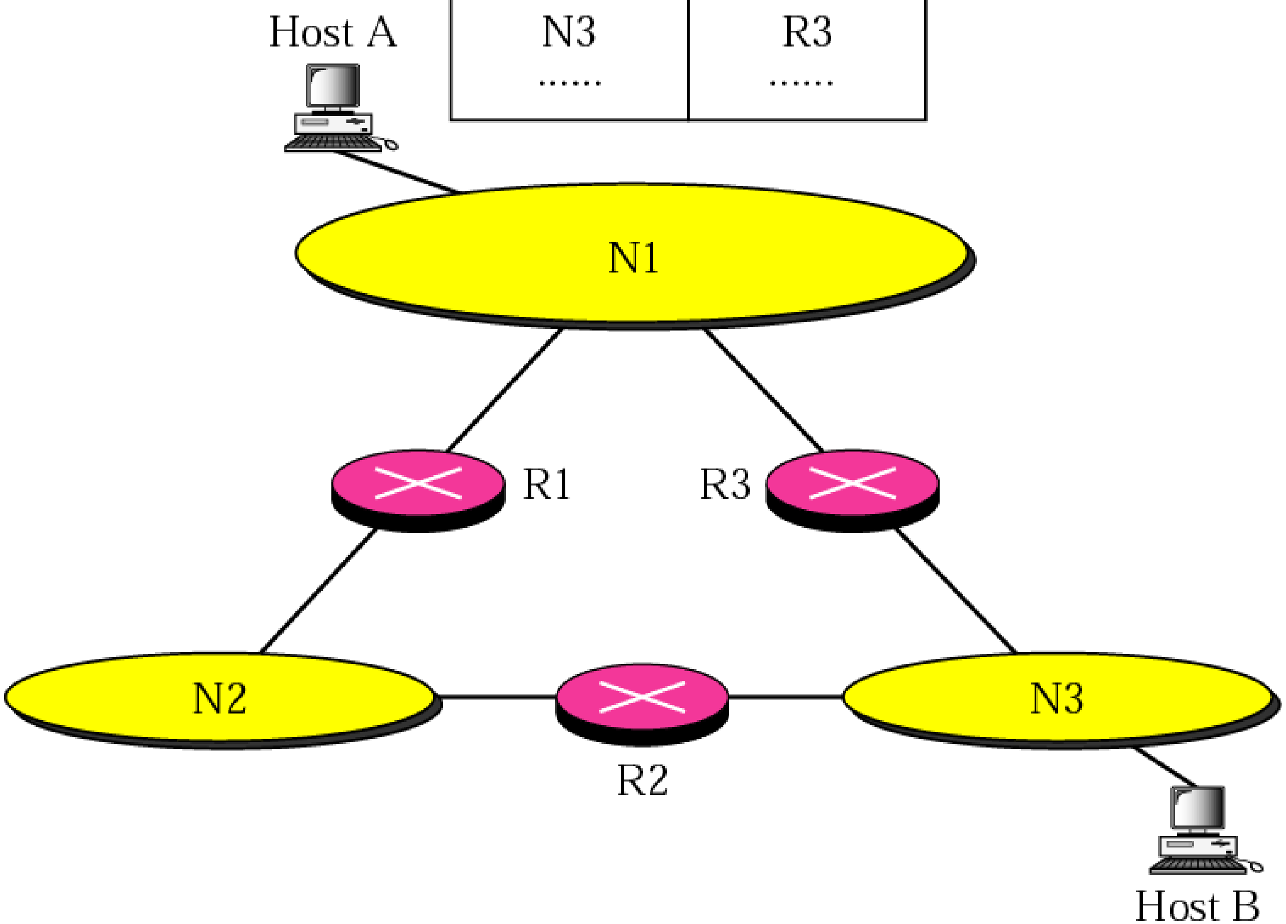
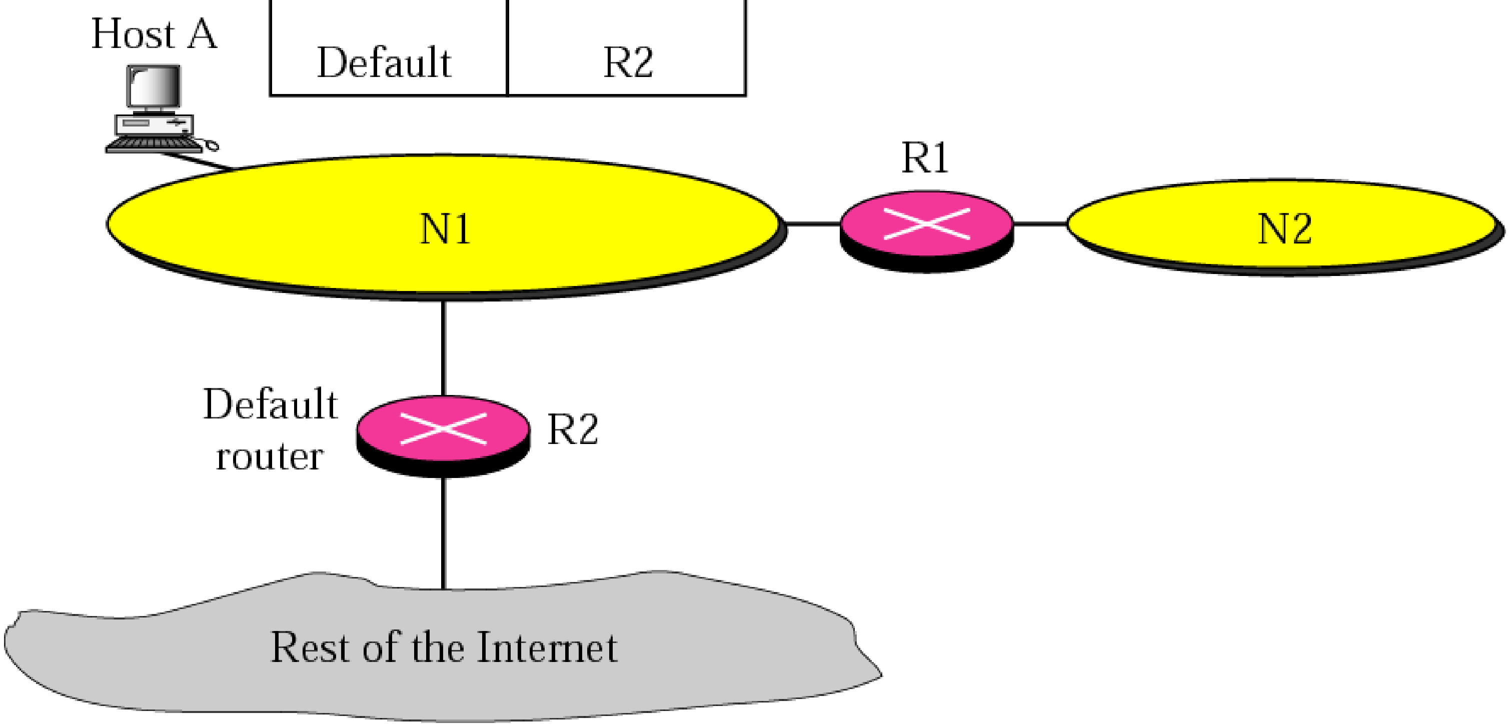


Figure 6-6

Default routing

Routing table for host A

Destination	Next Hop
N2	R1
......	......
Default	R2



6.4

STATIC VERSUS DYNAMIC ROUTING

A **static routing table** contains information entered manually.

A **dynamic routing table** is updated periodically using one of the dynamic routing protocols such as RIP, OSPF, or BGP.

6.5

ROUTING TABLE AND ROUTING MODULE

Routing module and routing table

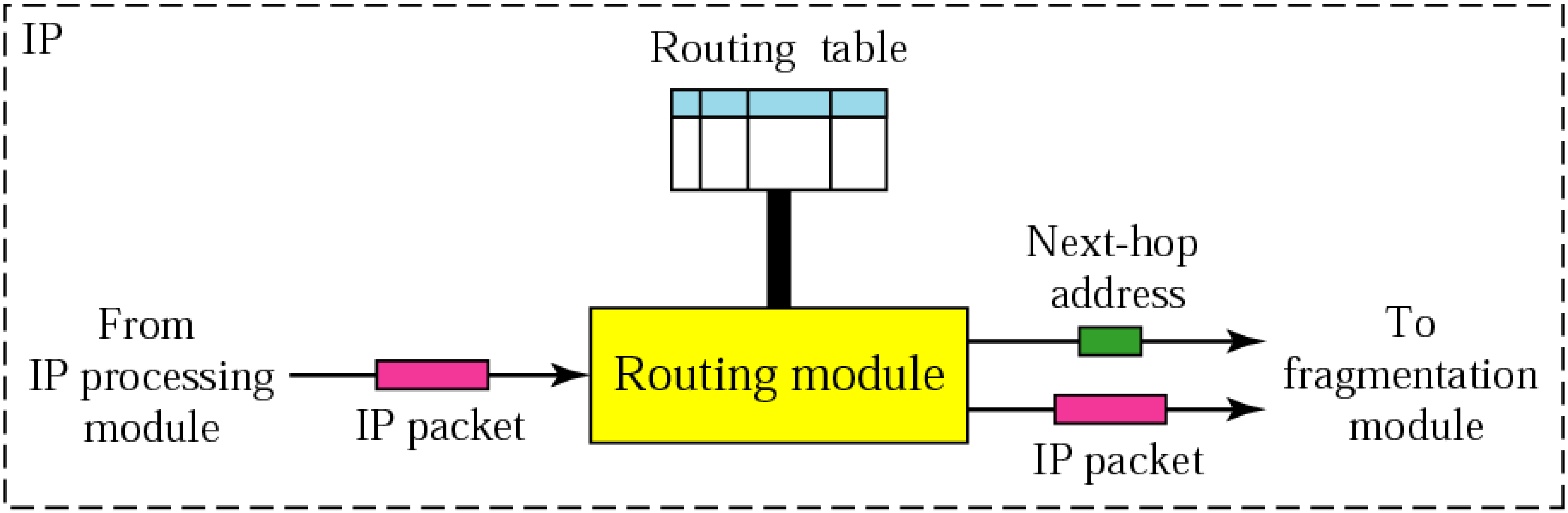


Figure 6-8

Routing Table

Mask	Destination address	Next-hop address	Flags	Reference count	Use	Interface
255.0.0.0	124.0.0.0	145.6.7.23	UG	4	20	m2
....	....		....	....	....	....
....	....	....	....	....	....	....

Flags

U The router is up and running.

G The destination is in another network.

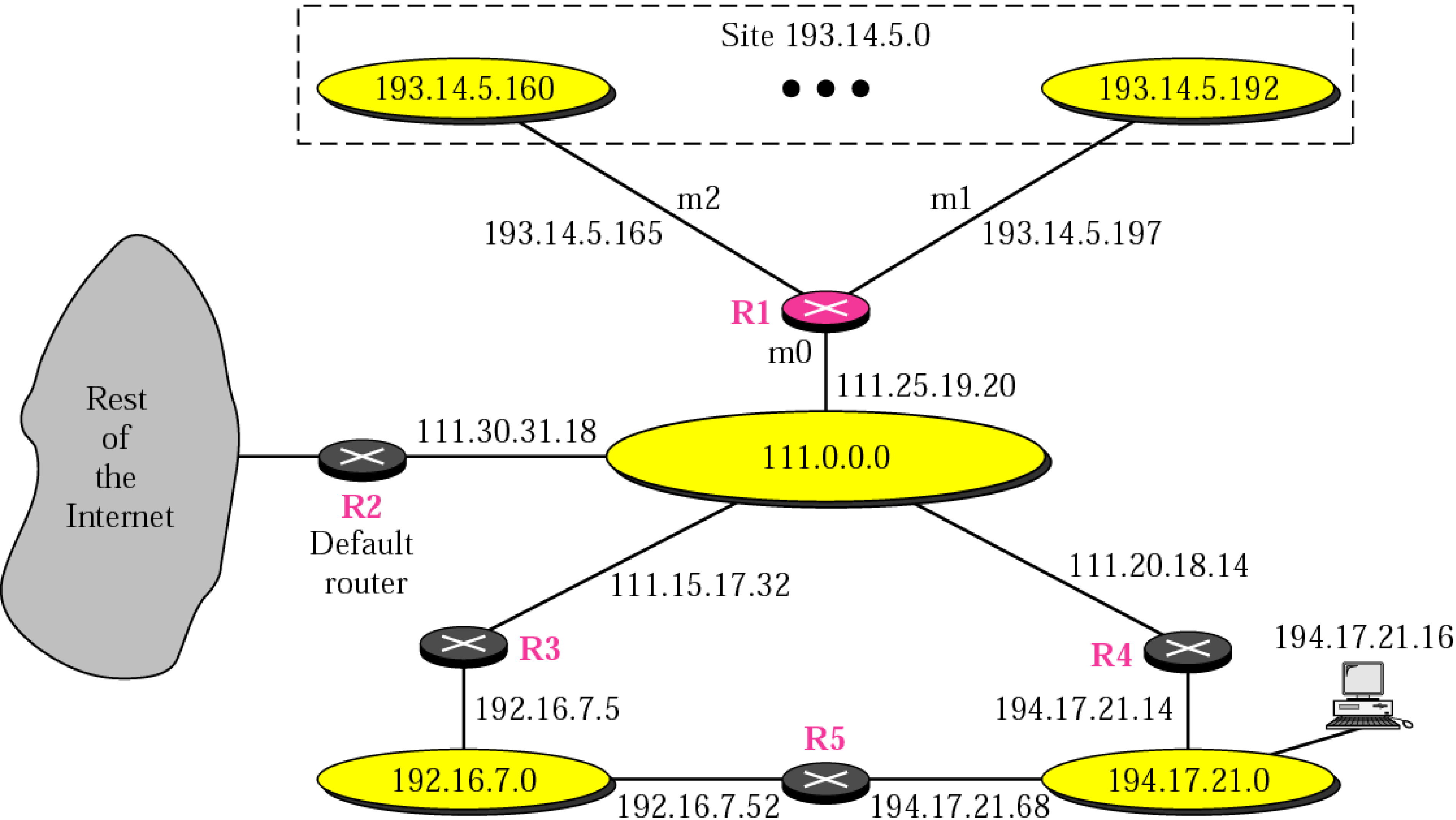
H Host-specific address.

D Added by redirection.

M Modified by redirection.

Figure 6-9

Configuration for routing example



Mask	**Dest.**	**Next Hop**	**I.**
255.0.0.0	111.0.0.0	--	m0
255.255.255.224	193.14.5.160	-	m2
255.255.255.224	193.14.5.192	-	m1
255.255.255.255	194.17.21.16	111.20.18.14	m0
255.255.255.0	192.16.7.0	111.15.17.32	m0
255.255.255.0	194.17.21.0	111.20.18.14	m0
0.0.0.0	0.0.0.0	111.30.31.18	m0

Example 1

Router R1 receives 500 packets for destination 192.16.7.14; the algorithm applies the masks row by row to the destination address until a match (with the value in the second column) is found:

Solution

Direct delivery

192.16.7.14 & 255.0.0.0 → 192.0.0.0 no match

192.16.7.14 & 255.255.255.224 → 192.16.7.0 no match

192.16.7.14 & 255.255.255.224 → 192.16.7. no match

Host-specific

192.16.7.14 & 255.255.255.255 →192.16.7.14 no match

Network-specific

192.16.7.14 & 255.255.255.0 →192.16.7.0 **match**

Example 2

Router R1 receives 100 packets for destination 193.14.5.176; the algorithm applies the masks row by row to the destination address until a match is found:

Solution

Direct delivery

193.14.5.176 & 255.0.0.0 → 193.0.0.0 no match

193.14.5.176 & 255.255.255.224 → 193.14.5.160 **match**

Example 3

Router R1 receives 20 packets for destination 200.34.12.34; the algorithm applies the masks row by row to the destination address until a match is found:

Solution

Direct delivery

200.34.12.34	&	255.0.0.0	→ 200.0.0.0	no match
200.34.12.34	&	255.255.255.224	→ 200.34.12.32	no match
200.34.12.34	&	255.255.255.224	→ 200.34.12.32	no match

Host-specific

200.34.12.34	&	255.255.255.255	→ 200.34.12.34	no match

Solution

Network-specific

200.34.12.34 & 255.255.255.0 → 200.34.12.0 no match

200.34.12.34 & 255.255.255.0 → 200.34.12.0 no match

Default

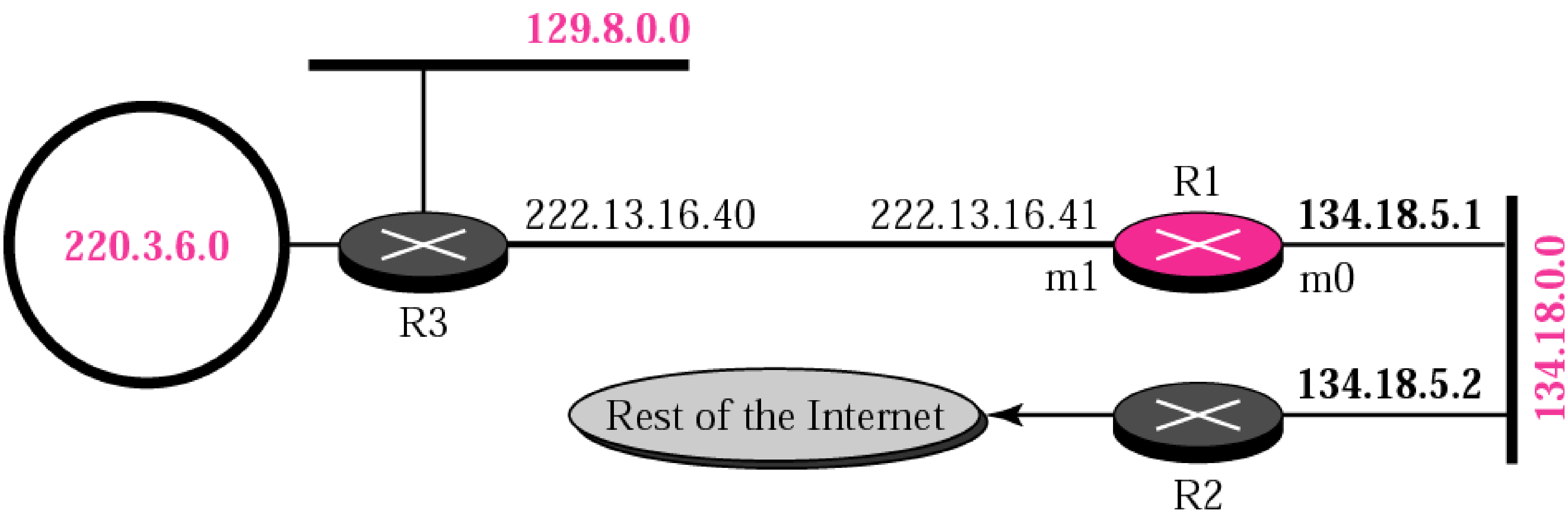
200.34.12.34 & 0.0.0.0 → 0.0.0.0. **match**

Example 4

Make the routing table for router R1 in Figure 6.10

Figure 6-10

Example 4



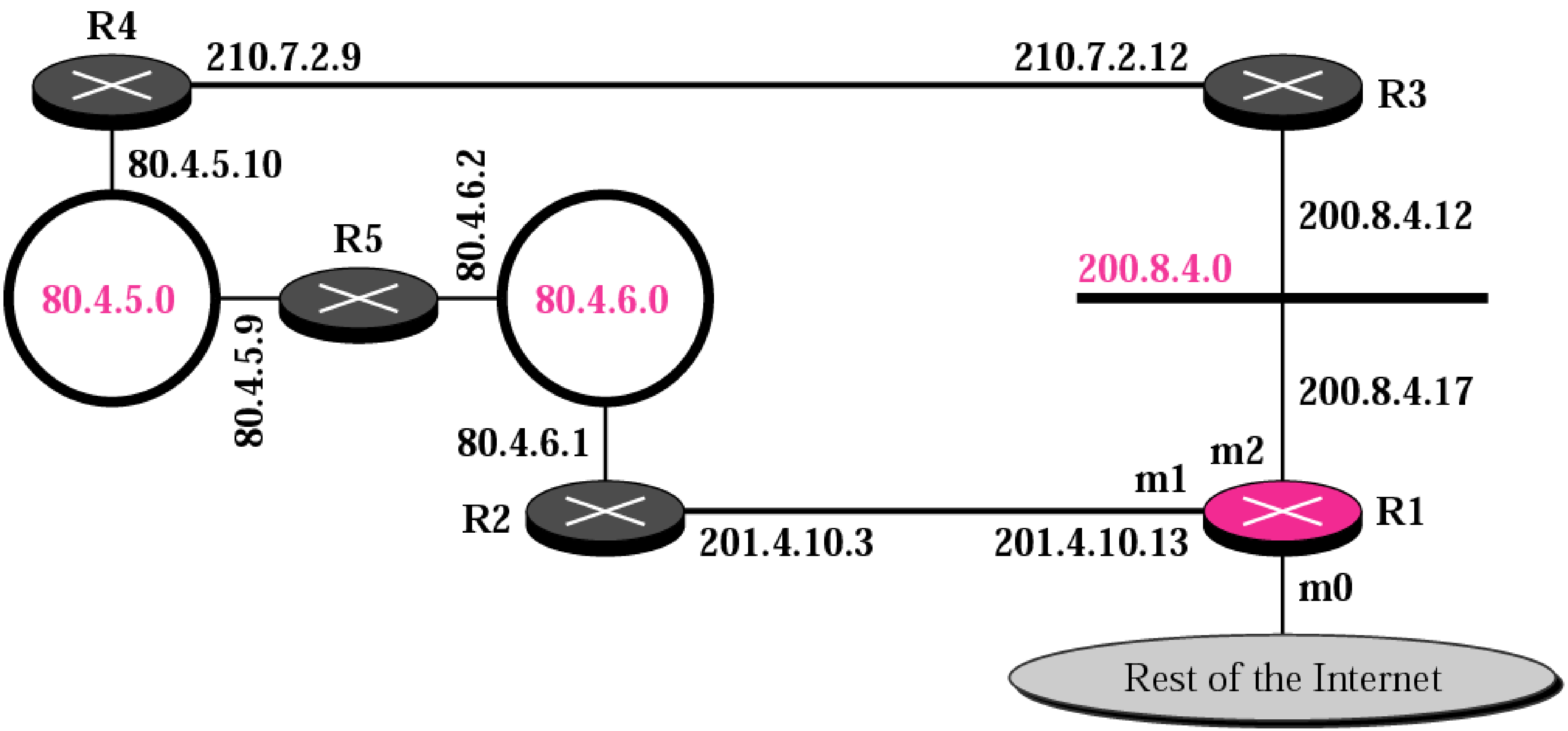
Solution

Mask	Destination	Next Hop	I.
255.255.0.0	134.18.0.0	--	m0
255.255.0.0	129.8.0.0	222.13.16.40	m1
255.255.255.0	220.3.6.0	222.13.16.40	m1
0.0.0.0	0.0.0.0	134.18.5.2	m0

Example 5

Make the routing table for router R1 in Figure 6.11

Example 5


R4
210.7.2.9
210.7.2.12
R3
80.4.5.10
80.4.6.2
R5
80.4.5.0
80.4.6.0
200.8.4.12
200.8.4.0
80.4.5.9
200.8.4.17
80.4.6.1
m2
m1
R2
R1
201.4.10.3
201.4.10.13
m0
Rest of the Internet

Solution

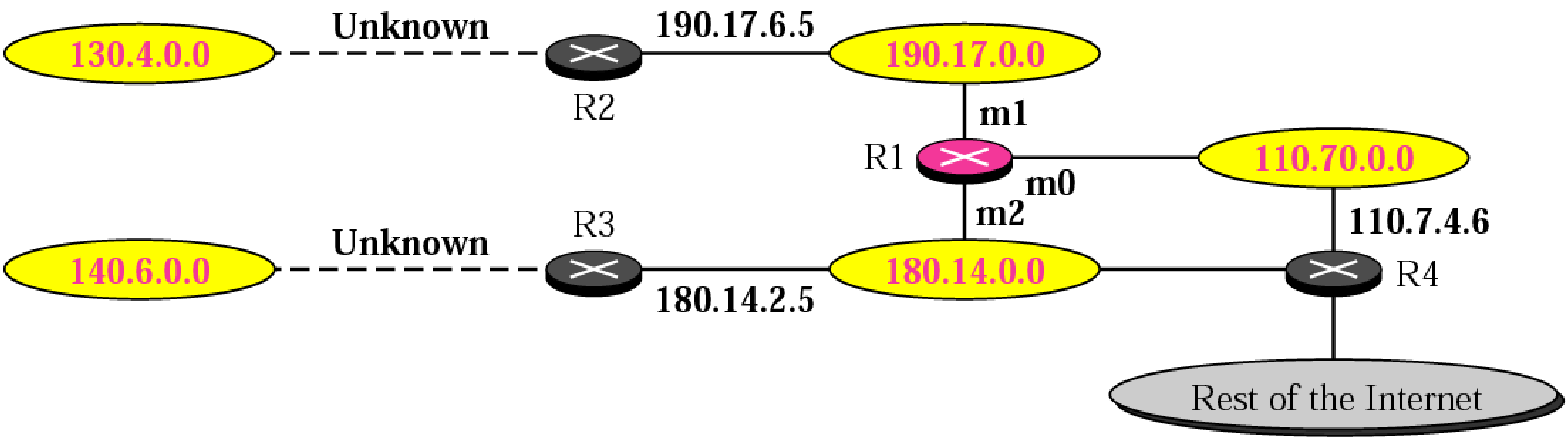
Mask	Destination	Next Hop	I.
255.255.255.0	200.8.4.0	----	m2
255.255.255.0	80.4.5.0	201.4.10.3 or 200.8.4.12	m1 or m2
255.255.255.0	80.4.6.0	201.4.10.3 or 200.4.8.12	m1 or m2
0.0.0.0	0.0.0.0	????????????	m0

Example 6

The routing table for router R1 is given below. Draw its topology

Mask	Destination	Next Hop	I.
255.255.0.0	110.70.0.0	-	m0
255.255.0.0	180.14.0.0	-	m2
255.255.0.0	190.17.0.0	-	m1
255.255.0.0	130.4.0.0	190.17.6.5	m1
255.255.0.0	140.6.0.0	180.14.2.5	m2
0.0.0.0	0.0.0.0	110.70.4.6	m0

Example 6
(Solution)



6.6

CLASSLESS ADDRESSING: CIDR

ISSUES

Routing Table Size

Hierarchical Routing

Geographical Routing

Routing Table Search Algorithms

Note

In classful addressing, each address has self-contained information that facilitates routing table searching.

Note

In classless addressing, there is no self-contained information in the destination address to facilitate routing table searching.

Chapter 7

ARP and RARP

CONTENTS

- **ARP**
- **ARP PACKAGE**
- **RARP**

Figure 7-1

ARP and RARP

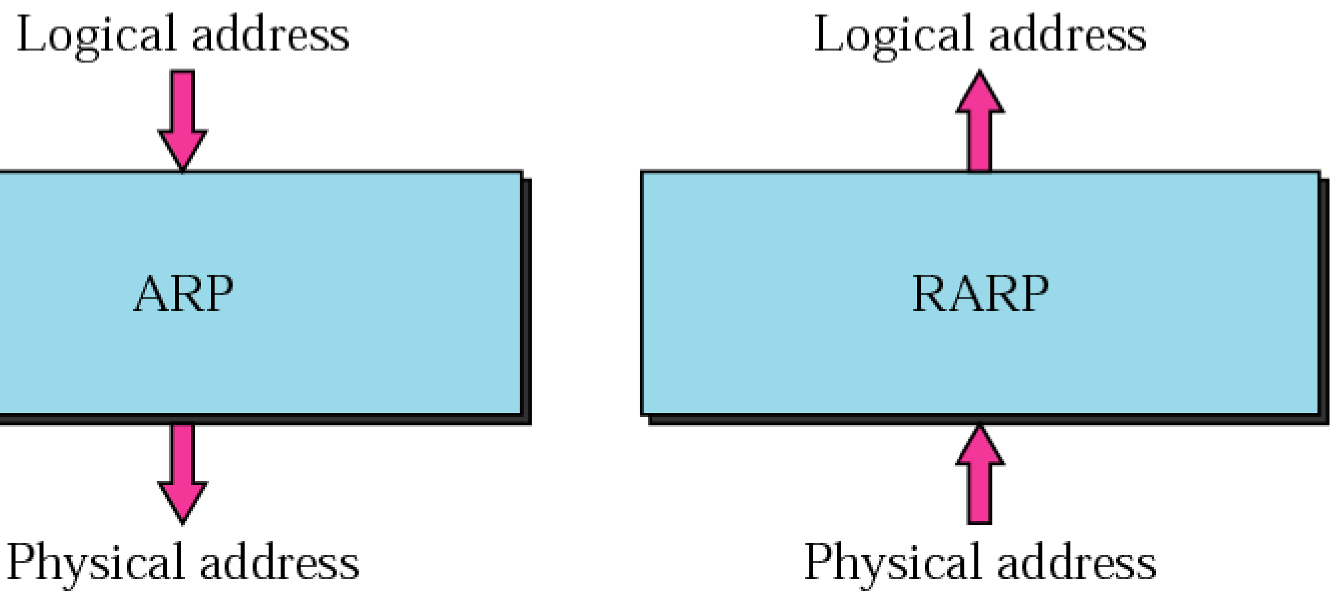
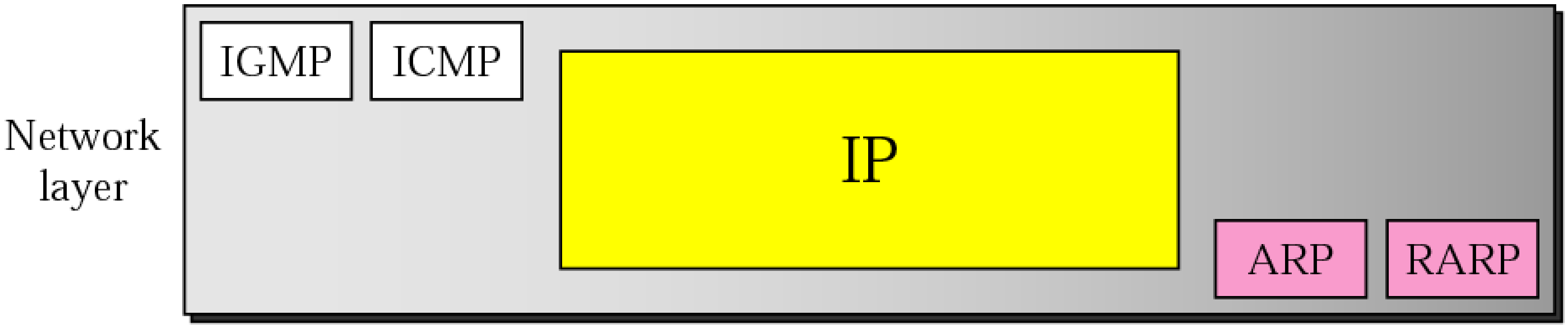


Figure 7-2

Position of ARP and RARP in TCP/IP protocol suite



7.1

ARP

ARP operation

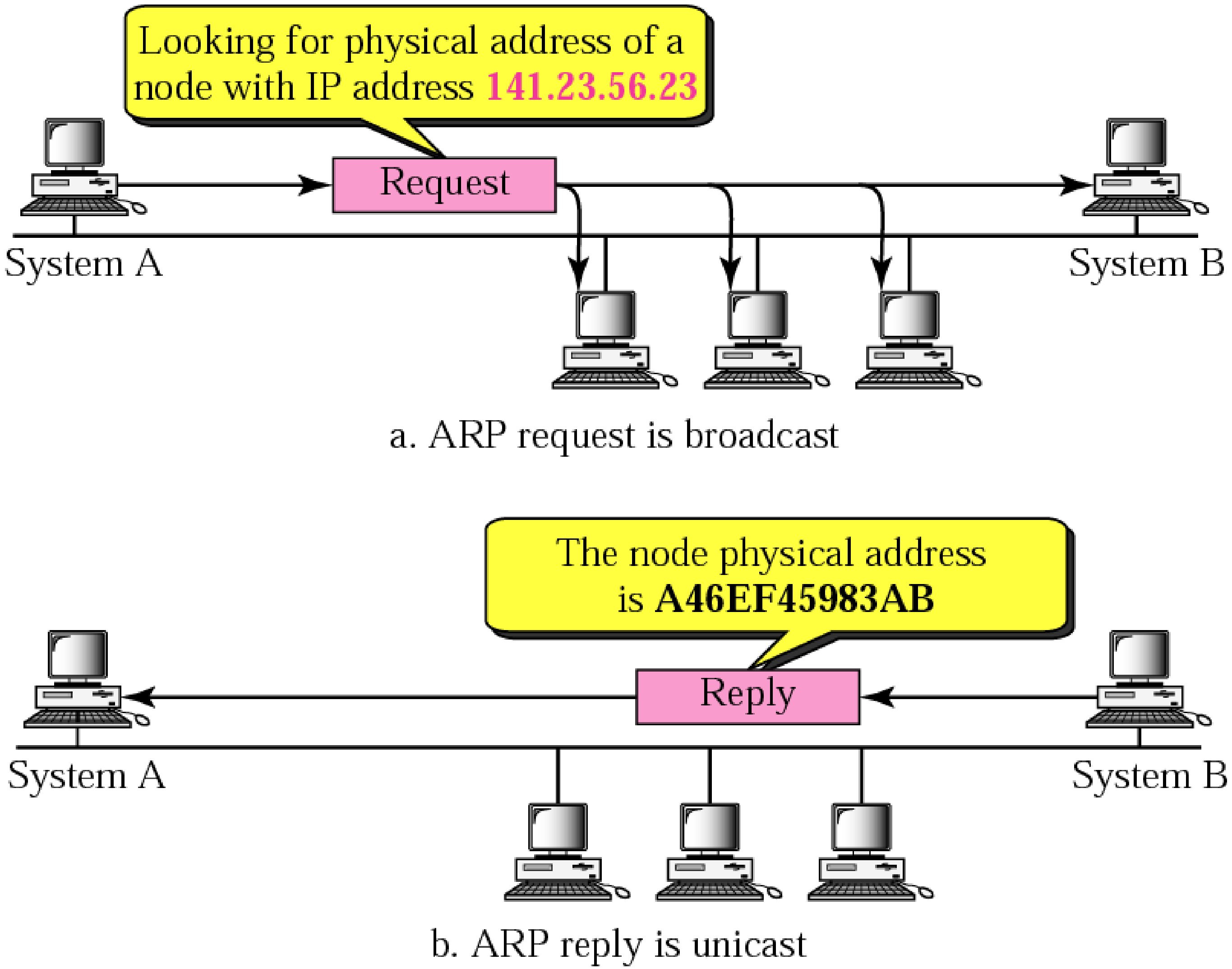


Figure 7-4

ARP packet

<table>
<tr><td colspan="2">Hardware Type</td><td>Protocol Type</td></tr>
<tr><td>Hardware length</td><td>Protocol length</td><td>Operation
Request 1, Reply 2</td></tr>
<tr><td colspan="3">Sender hardware address
(For example, 6 bytes for Ethernet)</td></tr>
<tr><td colspan="3">Sender protocol address
(For example, 4 bytes for IP)</td></tr>
<tr><td colspan="3">Target hardware address
(For example, 6 bytes for Ethernet)
(It is not filled in a request)</td></tr>
<tr><td colspan="3">Target protocol address
(For example, 4 bytes for IP)</td></tr>
</table>

Encapsulation of ARP packet

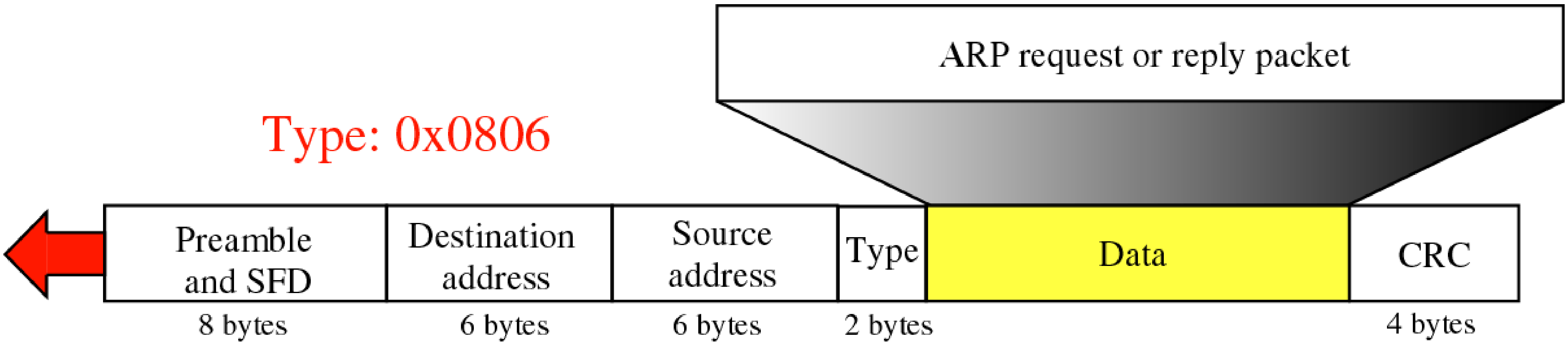
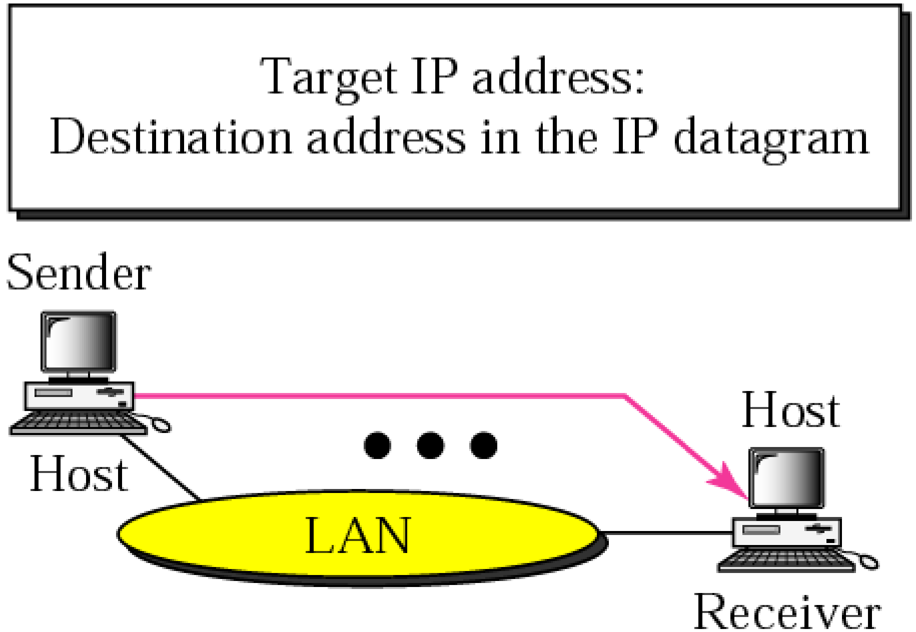


Figure 7-6:a

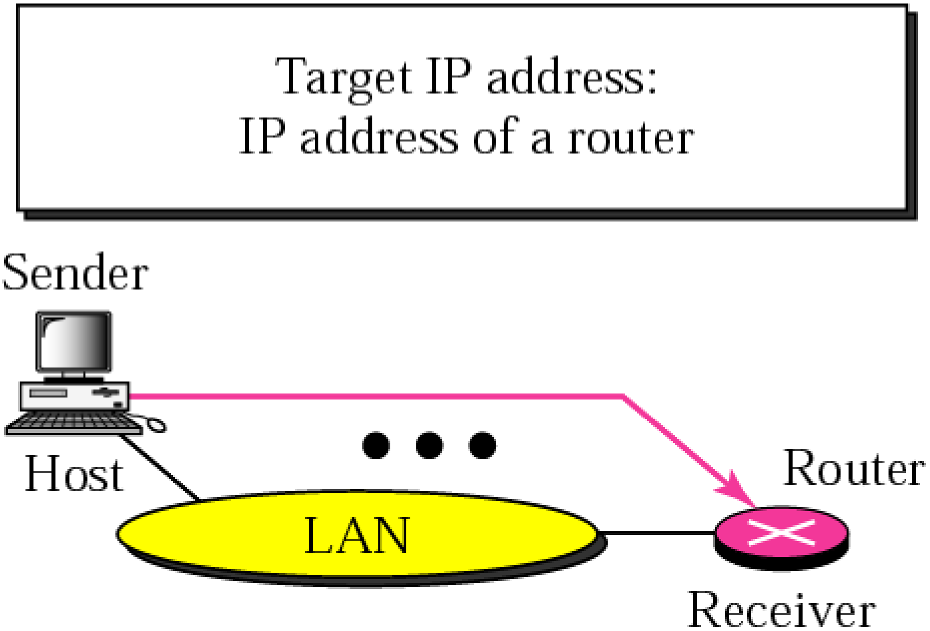
Four cases using ARP



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

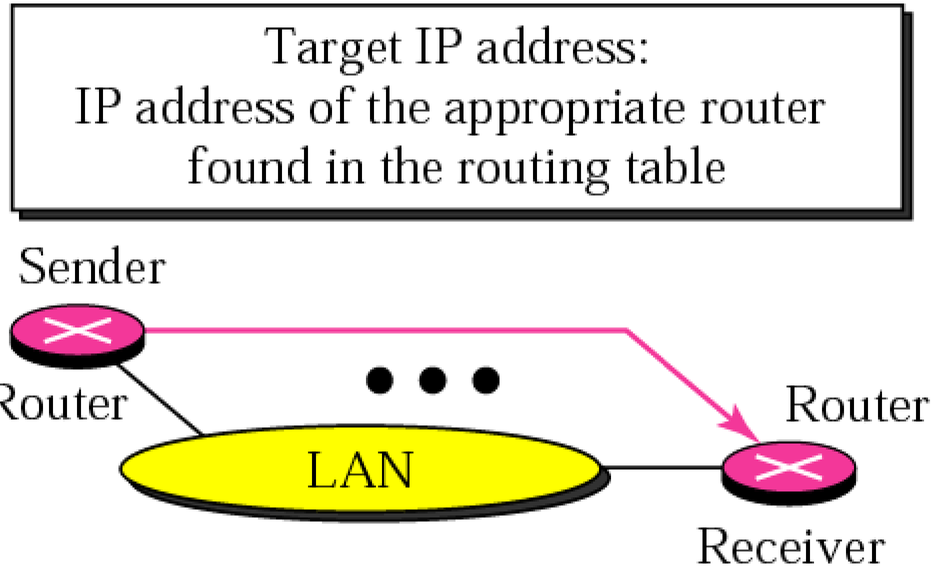
Figure 7-6:b

Four cases using ARP



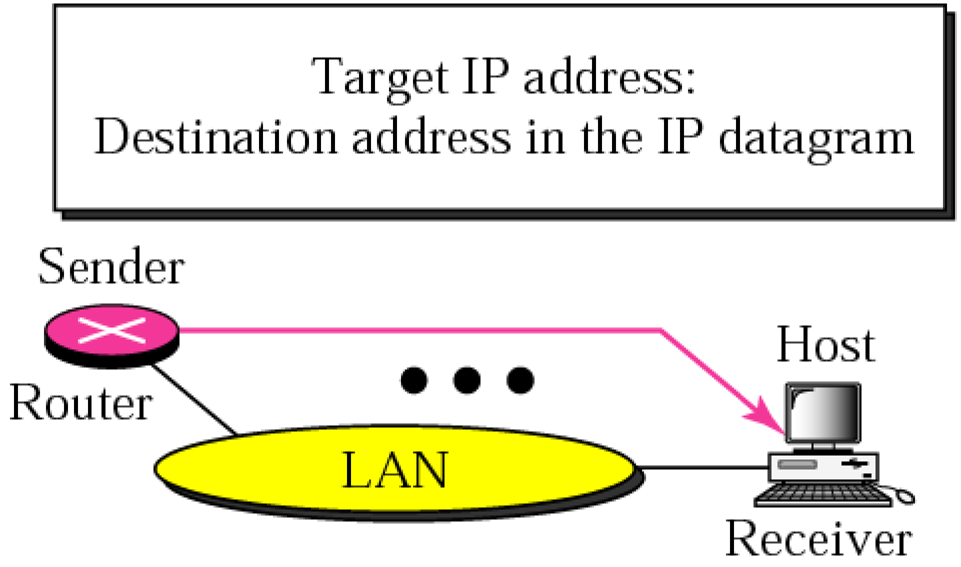
Case 2. A host wants to send a packet to another host on another network.
It must first be delivered to a router.

Four cases using ARP



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.

Four cases using ARP



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.

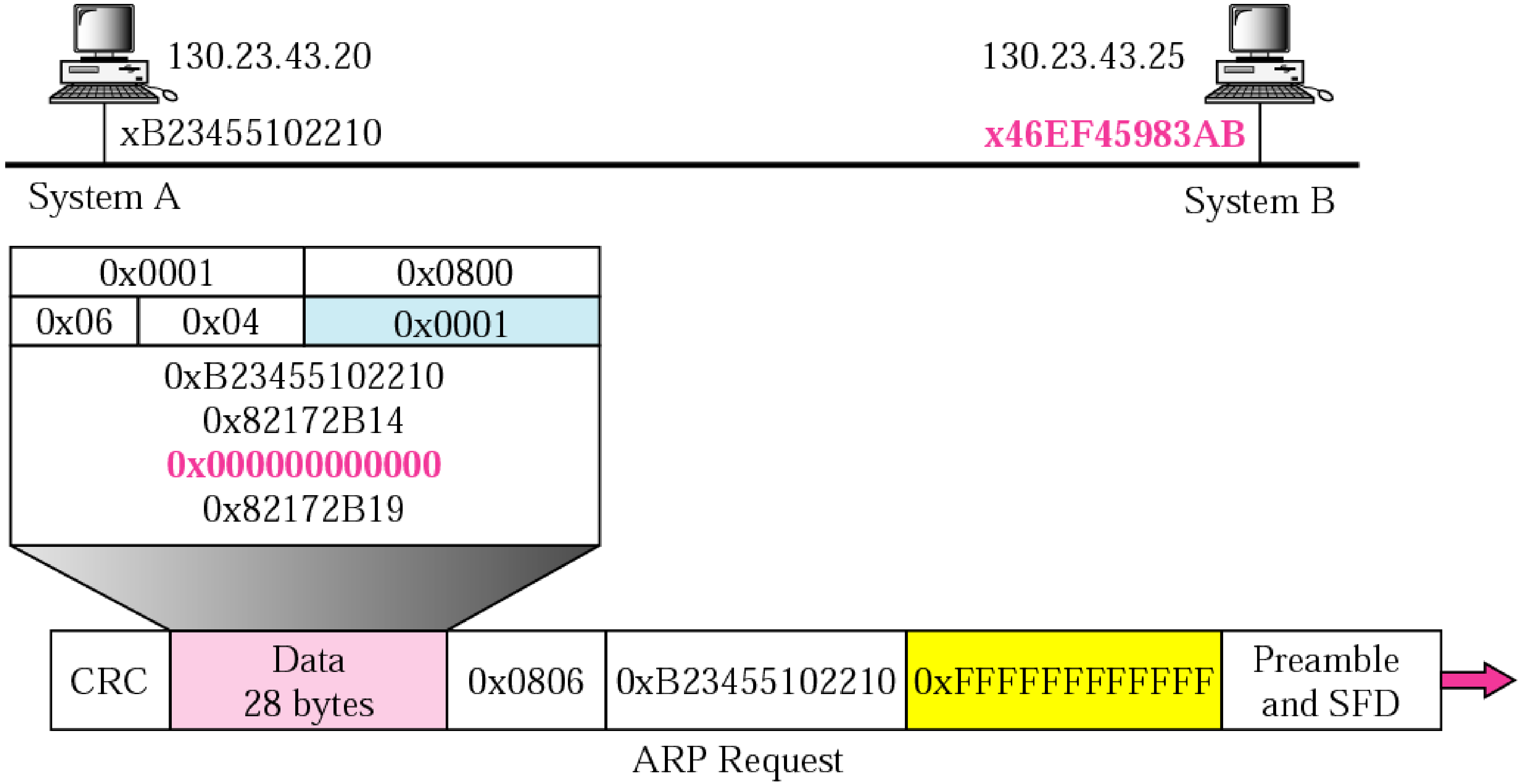
Example 1

A host with IP address 130.23.43.20 and physical address 0xB23455102210 has a packet to send to another host with IP address 130.23.43.25 and physical address 0xA46EF45983AB. The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.

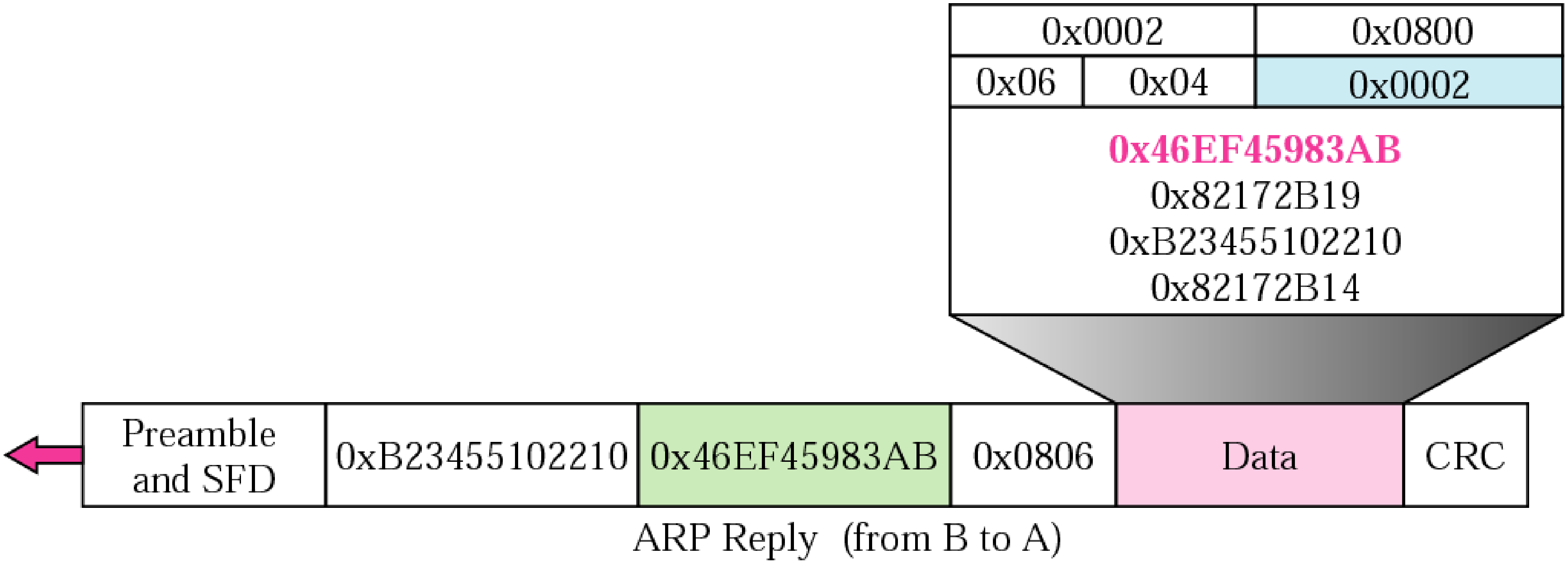
Solution

Figure 7.7 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.

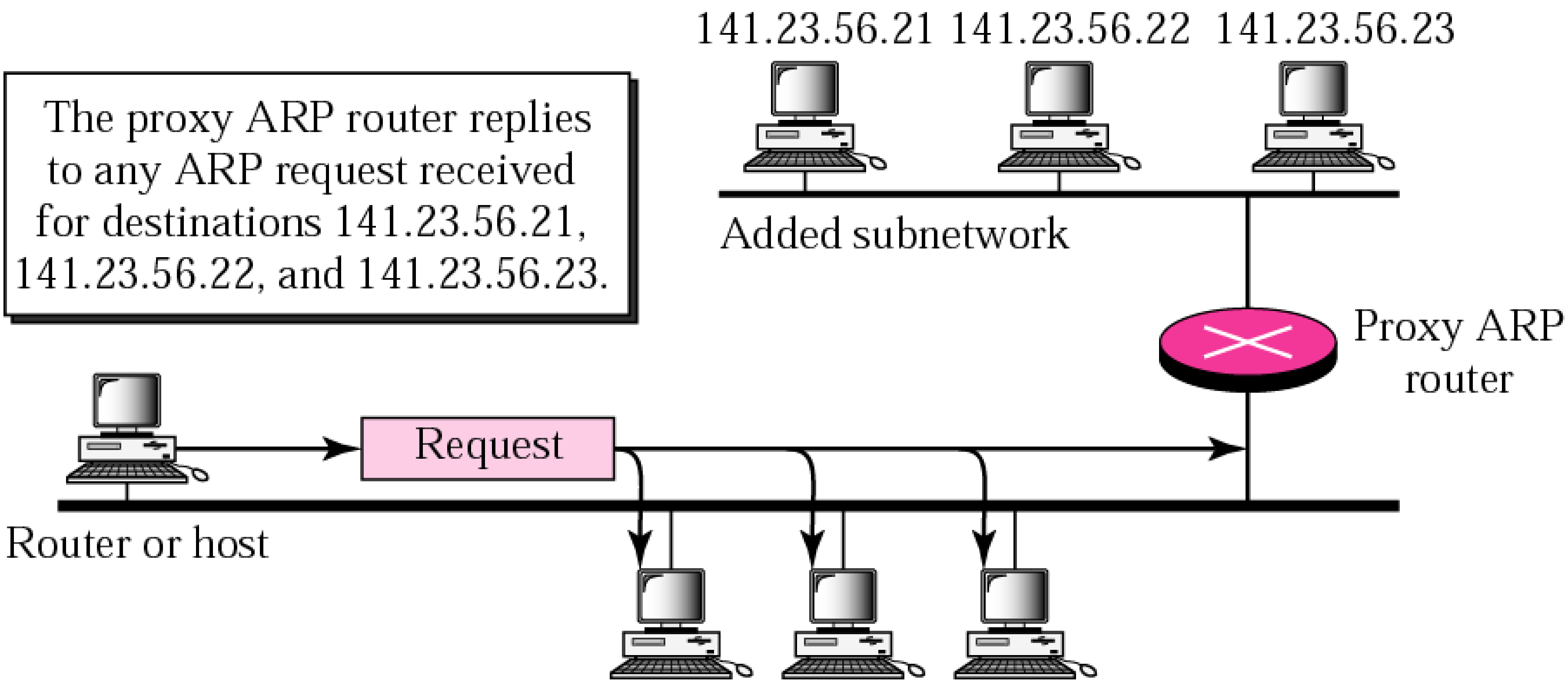
Example 1


130.23.43.20
xB23455102210
System A
130.23.43.25
x46EF45983AB
System B
0x0001
0x0800
0x06
0x04
0x0001
0xB23455102210
0x82172B14
0x000000000000
0x82172B19
CRC
Data
28 bytes
0x0806
0xB23455102210
0xFFFFFFFFFFFF
Preamble
and SFD
ARP Request

Example 1 (Continued)



Proxy ARP

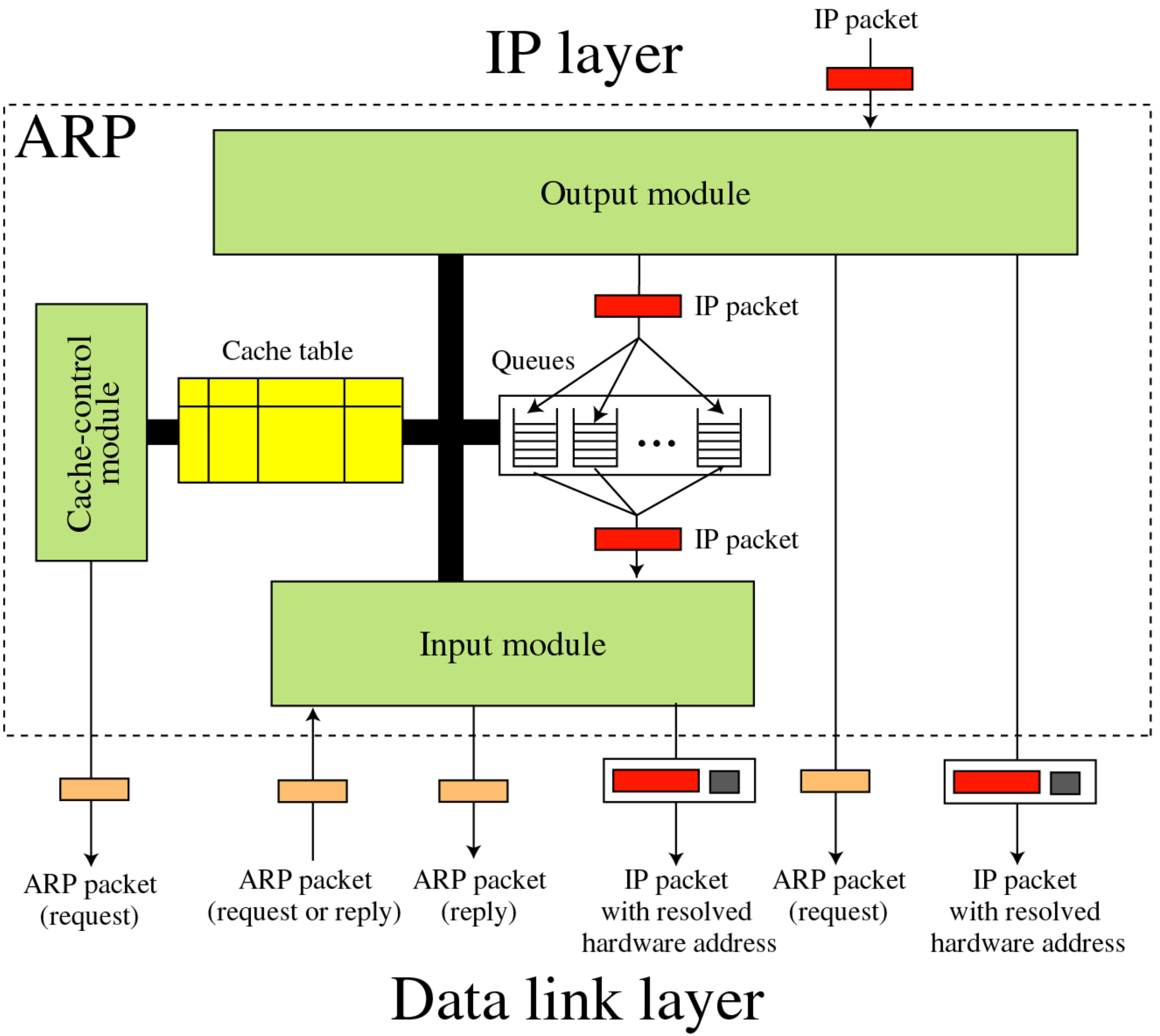

The proxy ARP router replies to any ARP request received for destinations 141.23.56.21, 141.23.56.22, and 141.23.56.23.
141.23.56.21
141.23.56.22
141.23.56.23
Added subnetwork
Proxy ARP router
Request
Router or host

7.2

ARP PACKAGE

Figure 7-9

ARP components



Original cache table

State	Queue	Attempt	Time-out	Protocol Addr.	Hardware Addr.
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
F					
R	9		60	19.1.7.82	4573E3242ACA
P	18	3		188.11.8.71	

Example 2

The ARP output module receives an IP datagram (from the IP layer) with the destination address 114.5.7.89. It checks the cache table and finds that an entry exists for this destination with the RESOLVED state (R in the table). It extracts the hardware address, which is 457342ACAE32, and sends the packet and the address to the data link layer for transmission. The cache table remains the same.

Example 3

Twenty seconds later, the ARP output module receives an IP datagram (from the IP layer) with the destination address 116.1.7.22. It checks the cache table and does not find this destination in the table. The module adds an entry to the table with the state PENDING and the Attempt value 1. It creates a new queue for this destination and enqueues the packet. It then sends an ARP request to the data link layer for this destination.

Cache table for Example 3

State	*Queue*	*Attempt*	*Time-out*	*Protocol Addr.*	*Hardware Addr.*
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
P	**23**	**1**		**116.1.7.22**	
R	9		60	19.1.7.82	4573E3242ACA
P	18	3		188.11.8.71	

Example 4

Fifteen seconds later, the ARP input module receives an ARP packet with target protocol (IP) address 188.11.8.71. The module checks the table and finds this address. It changes the state of the entry to RESOLVED and sets the time-out value to 900. The module then adds the target hardware address (E34573242ACA) to the entry. Now it accesses queue 18 and sends all the packets in this queue, one by one, to the data link layer.

Cache table for Example 4

State	Queue	Attempt	Time-out	Protocol Addr.	Hardware Addr.
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
P	**23**	**1**		**116.1.7.22**	
R	9		60	19.1.7.82	4573E3242ACA
R	18		900	188.11.8.71	E34573242ACA

Example 5

Twenty-five seconds later, the cache-control module updates every entry. The time-out values for the first three resolved entries are decremented by 60. The time-out value for the last resolved entry is decremented by 25. The state of the next-to-the last entry is changed to FREE because the time-out is zero. For each of the three entries, the value of the attempts field is incremented by one. After incrementing, the attempts value for one entry (the one with IP protocol address 201.11.56.7) is more than the maximum; the state is changed to FREE, the queue is deleted.

Cache table for Example 5

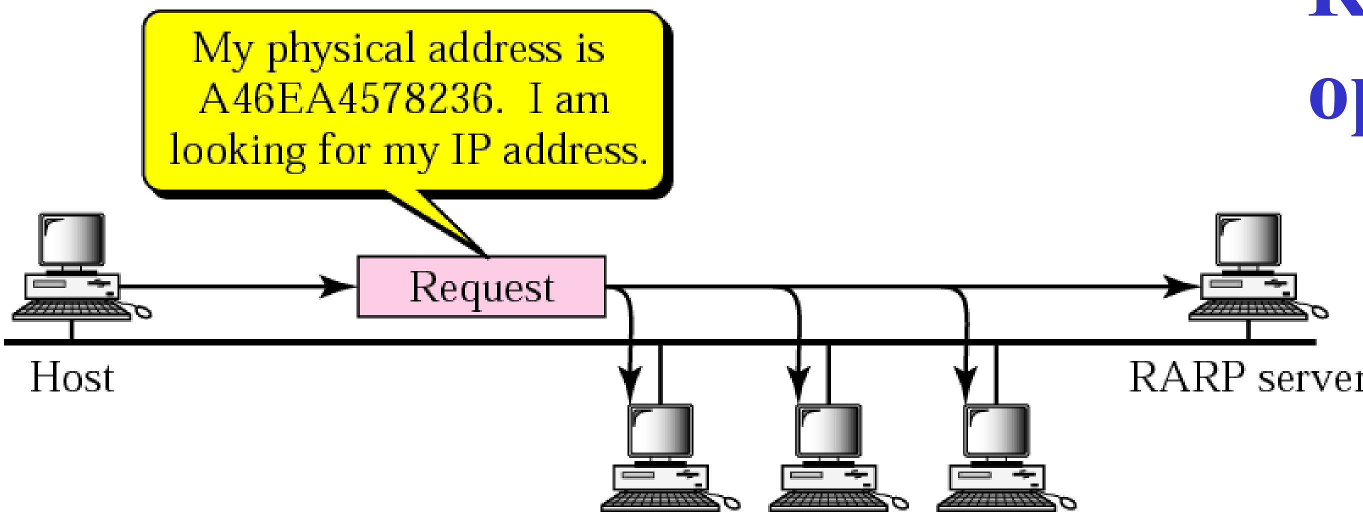
State	*Queue*	*Attempt*	*Time-out*	*Protocol Addr.*	*Hardware Addr.*
R	5		840	180.3.6.1	ACAE32457342
P	2	3		129.34.4.8	
F					
R	8		390	114.5.7.89	457342ACAE32
P	12	2		220.55.5.7	
P	**23**	**2**		**116.1.7.22**	
F					
R	18		875	188.11.8.71	E34573242ACA

7.3

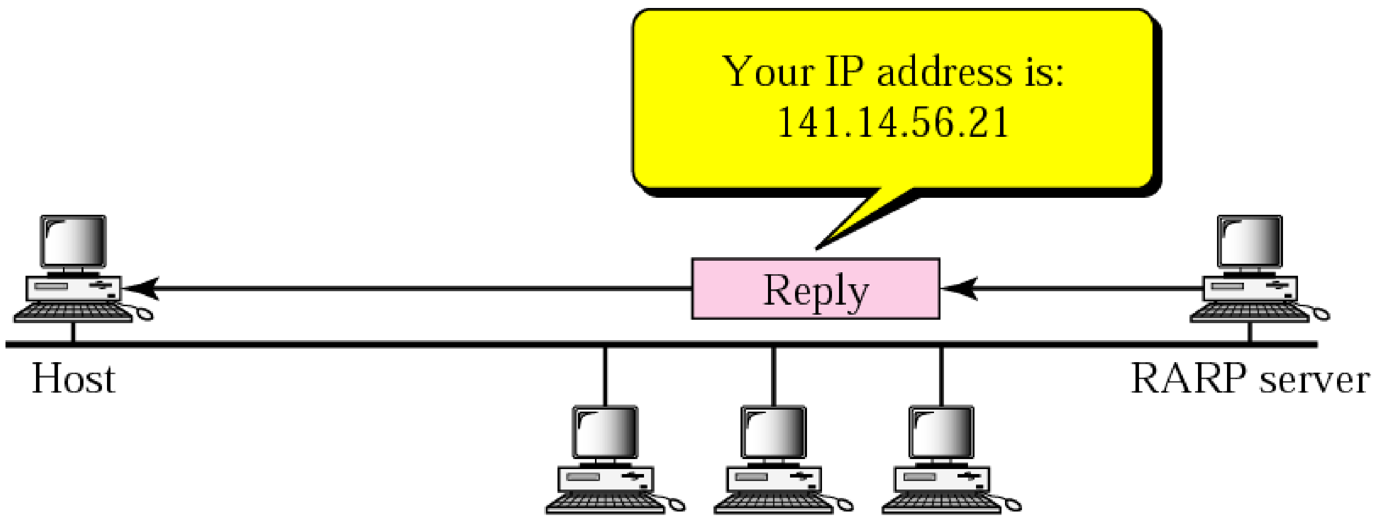
RARP

Figure 7-10

RARP operation



a. RARP request is broadcast



b. RARP reply is unicast

Note

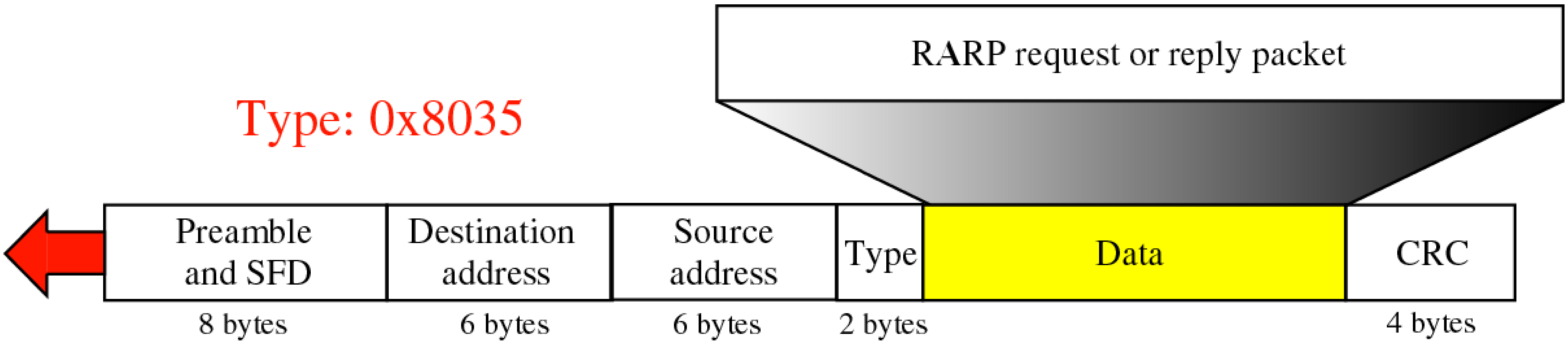
The RARP request packets are broadcast; the RARP reply packets are unicast.

Figure 7-11

RARP packet

<table>
<tr><td colspan="2">Hardware type</td><td>Protocol type</td></tr>
<tr><td>Hardware length</td><td>Protocol length</td><td>Operation
Request 3, Reply 4</td></tr>
<tr><td colspan="3">Sender hardware address
(For example, 6 bytes for Ethernet)</td></tr>
<tr><td colspan="3">Sender protocol address
(For example, 4 bytes for IP)
(It is not filled for request)</td></tr>
<tr><td colspan="3">Target hardware address
(For example, 6 bytes for Ethernet)
(It is not filled for request)</td></tr>
<tr><td colspan="3">Target protocol address
(For example, 4 bytes for IP)
(It is not filled for request)</td></tr>
</table>

Encapsulation of RARP packet



Alternative Solutions to RARP

When a diskless computer is booted, it needs more information in addition to its IP address. It needs to know its subnet mask, the IP address of a router, and the IP address of a name server. RARP cannot provide this extra information. New protocols have been developed to provide this information. In Chapter 17 we discuss two protocols, BOOTP and DHCP, that can be used instead of RARP.