Network Layer

Objectives:

- To introduce packet switching as the mechanism of data delivery in the network layer.
- To discuss two distinct types of services a packet-switch network can provide: connectionless and connection-oriented services.
- To introduce the concept of an address space in general and the address space of IPv4 in particular.
- To discuss the idea of hierarchical addressing and how it has been implemented in classful addressing.
- To discuss some special blocks and some special addresses in each block.

Introduction

- The network layer was designed to solve the problem of delivering packet through several links.
- The network layer is responsible for host-to-host delivery and for routing the packets through the routers.

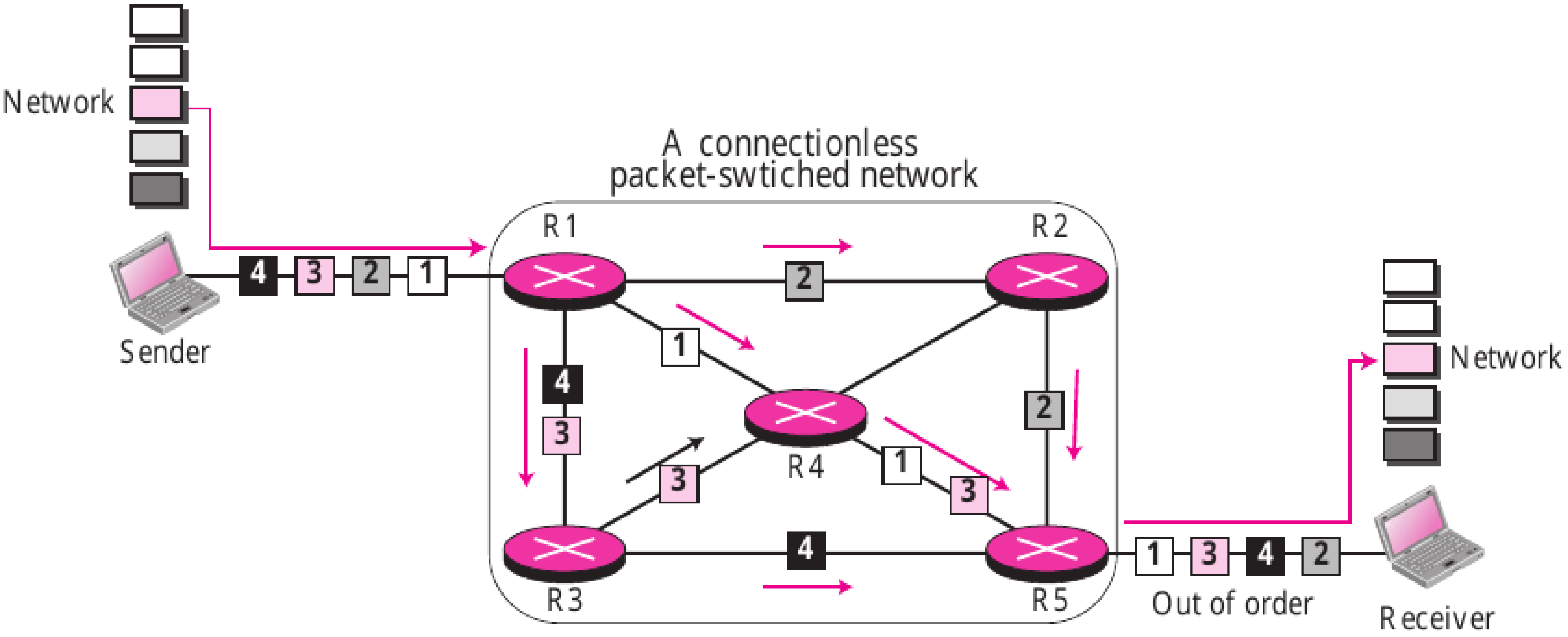
Packet Switching

- A message from the upper layer is divided into manageable packets and each packet is sent through the network

Connectionless Service

- Network layer was designed to provide a connectionless service.
- Network layer protocol treats each packet independently with each packet having no relationship to any other packet.
- When the Internet started, it was decided to make the network layer a connectionless service to make it simple.
- Each packet is routed based on the information contained in its header: source and destination address.

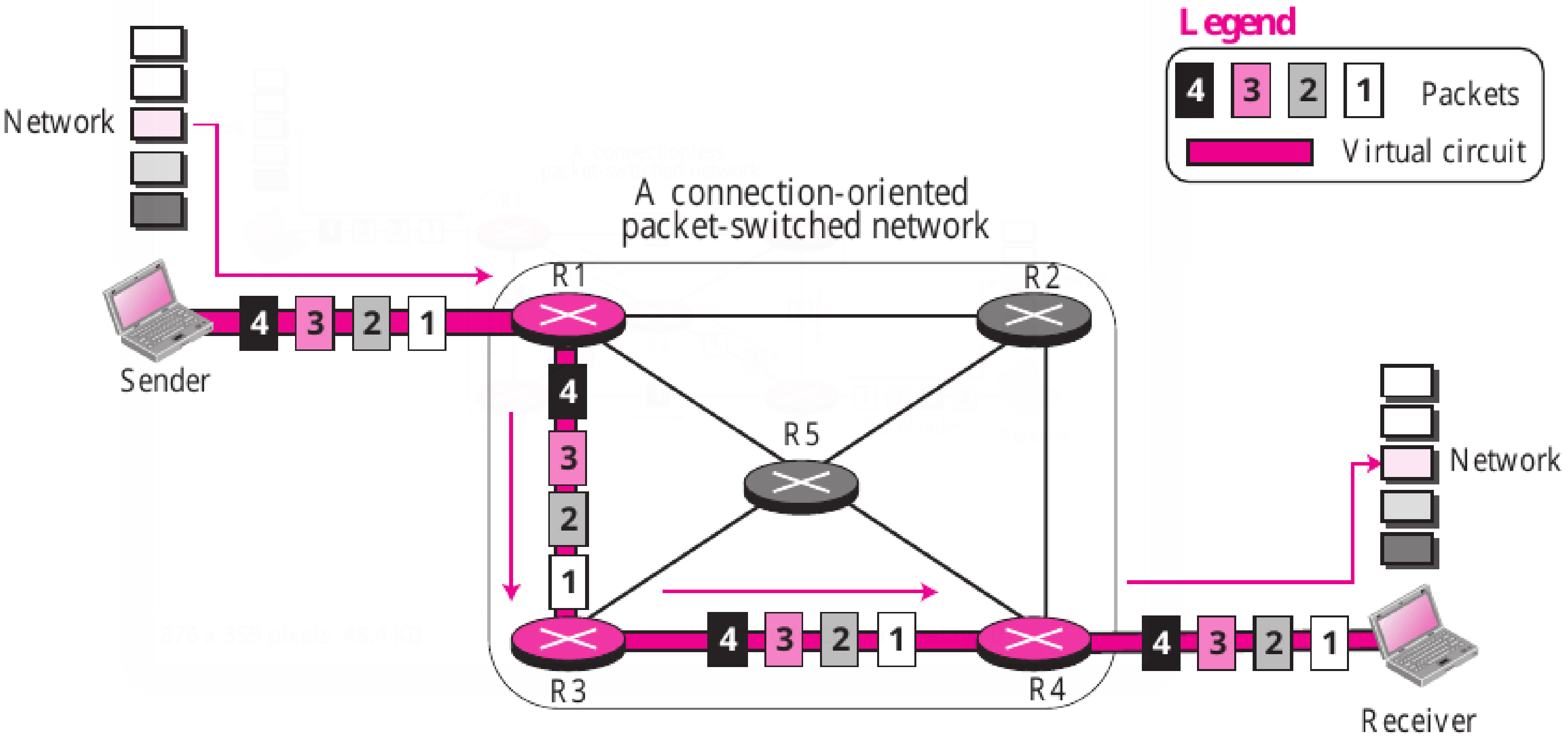
Illustration: Connectionless Service



Connection-Oriented Service

- In connection-oriented service, there is a relation between all packets belonging to a message.
- Before all datagrams in a message can be sent, a virtual connection should be setup to define the path for the datagrams.
- After connection setup, the datagrams can follow the same path.

Illustration: Connection-Oriented



IPv4 Address

Introduction

- Internet protocol (IP) is used to identify each device connected to the Internet.
- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.

Notation

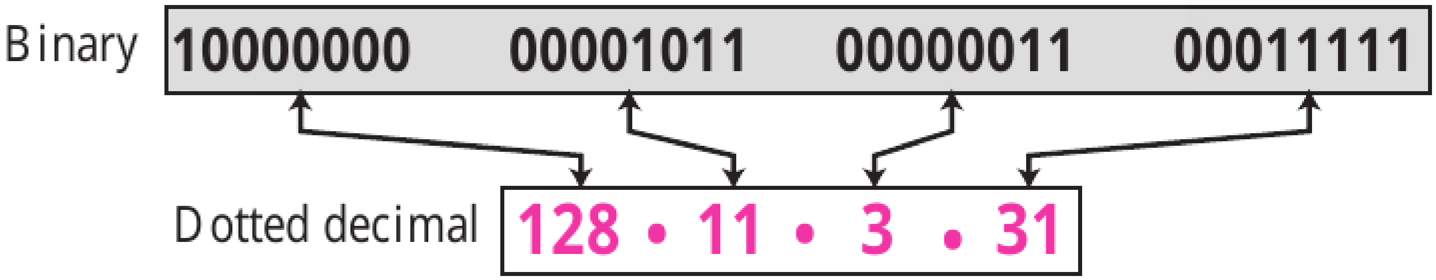
- There are two common notations to show an IPv4 address:
  - Binary notation (base 2)
  - Dotted-decimal notation (base 256)

Binary Notation (Base 2)

- In binary notation, an IPv4 address is displayed as 32 bits.
- To make the address more readable, one or more spaces is usually inserted between each octet (8 bits)
- Each octet is often referred to as a byte.
  - Example: **01110101 10010101 00011101 11101010**

Dotted-Decimal Notation: Base 256

- An IPv4 address is usually written in decimal form with a decimal point (dot) separating the bytes.
- Each number in the dotted-decimal notation is between 0 and 255.

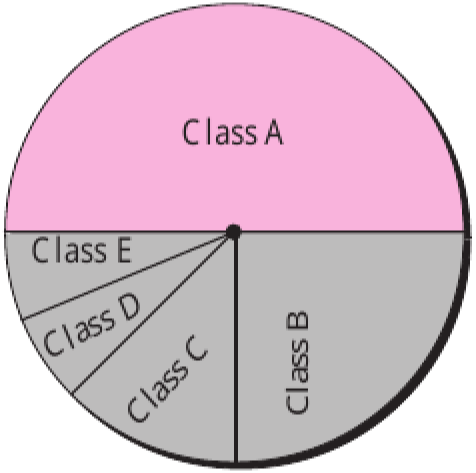


Example Binary to Dotted-Decimal

- Change the following IPv4 addresses from binary notation to dotted-decimal notation.
    1. 10000001 00001011 00001011 11101111
    2. 11000001 10000011 00011011 11111111
    3. 11100111 11011011 10001011 01101111
    4. 11111001 10011011 11111011 00001111

Classful Addressing

- IP address space is divided into five classes: A, B, C, D, and E.



Class A: 2^{31} = 2,147,483,648 addresses, 50%

Class B: 2^{30} = 1,073,741,824 addresses, 25%

Class C: 2^{29} = 536,870,912 addresses, 12.5%

Class D: 2^{28} = 268,435,456 addresses, 6.25%

Class E: 2^{28} = 268,435,456 addresses, 6.25%

Recognizing Classes

	Octet 1	Octet 2	Octet 3	Octet 4
Class A	0........			
Class B	10......			
Class C	110.....			
Class D	1110....			
Class E	1111....			

Binary notation

	Byte 1	Byte 2	Byte 3	Byte 4
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–299			
Class E	240–255			

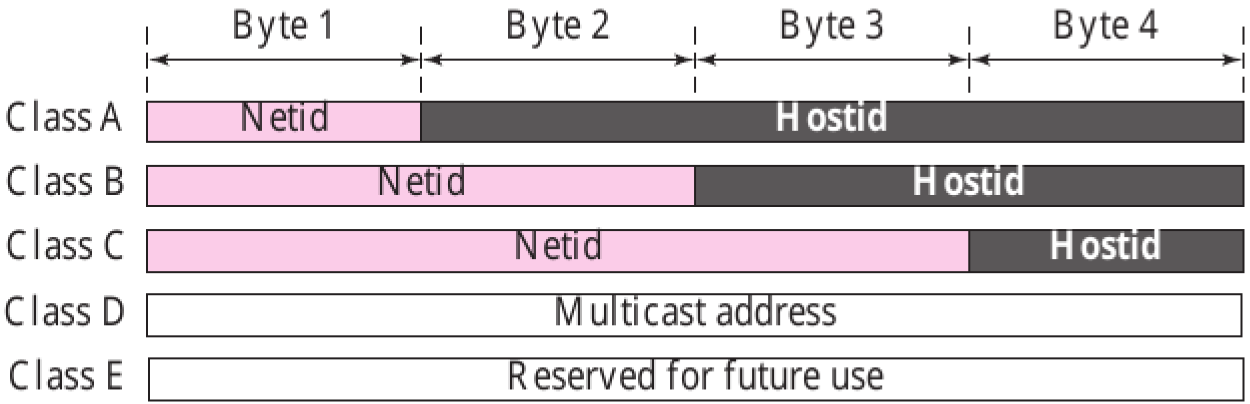
Dotted-decimal notation

Example

- Find the class of each address:
    1. 00000001 00001011 00001011 11101111
    2. 11000001 10000011 00011011 11111111
    3. 10100111 11011011 10001011 01101111
    4. 11110011 10011011 11111011 00001111
    5. 227.12.14.87
    6. 193.14.56.22
    7. 14.23.120.8
    8. 252.5.15.111

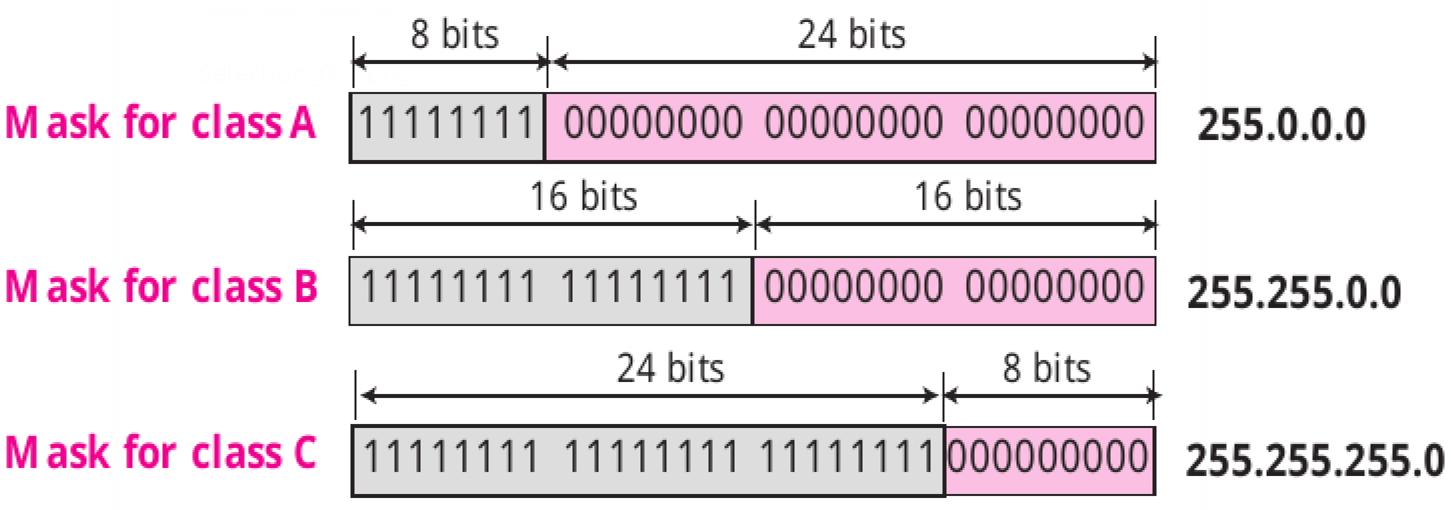
Netid and Hostid

- In classful addressing, an IP address in classes A, B, and C is divided into netid and hostid.



Network Address and Network Mask

- The network address is the identifier of a network.



Special Addresses

- All-Zeros Address
  - The block 0.0.0.0/32 is reserved for communication when a host needs to send an IPv4 packet but it does not know its own address.
- All-Ones Address
  - 255.255.255.255/32 which contains one single address, is reserved for limited broadcast address in the current network.
- Loopback Addresses
  - The block 127.0.0.0/8 is used to test the software on a machine.

Private Addresses

- A number of blocks are assigned for private use. They are not recognized globally.

Block	Number of addresses	Block	Number of addresses
10.0.0.0/8	16,777,216	192.168.0.0/16	65,536
172.16.0.0/12	1,047,584	169.254.0.0/16	65,536

Address Resolution Protocol (ARP)

- To delivery a packet to a host or a router requires two levels of addressing:
  - Logical address
  - Physical address
- ARP maps a logical address to its corresponding physical address and vice versa.
- These can be done using either static or dynamic mapping

Static Mapping

- Static mapping means creating a table that associates logical address with a physical address.
- Each machine that knows, the IP address of another machine but not its physical address can look it up in the table.
- This has some limitations:
  - A machine could change its NIC.
  - In some LANs, such as LocalTalk, the physical address changes every time the computer is turned on.

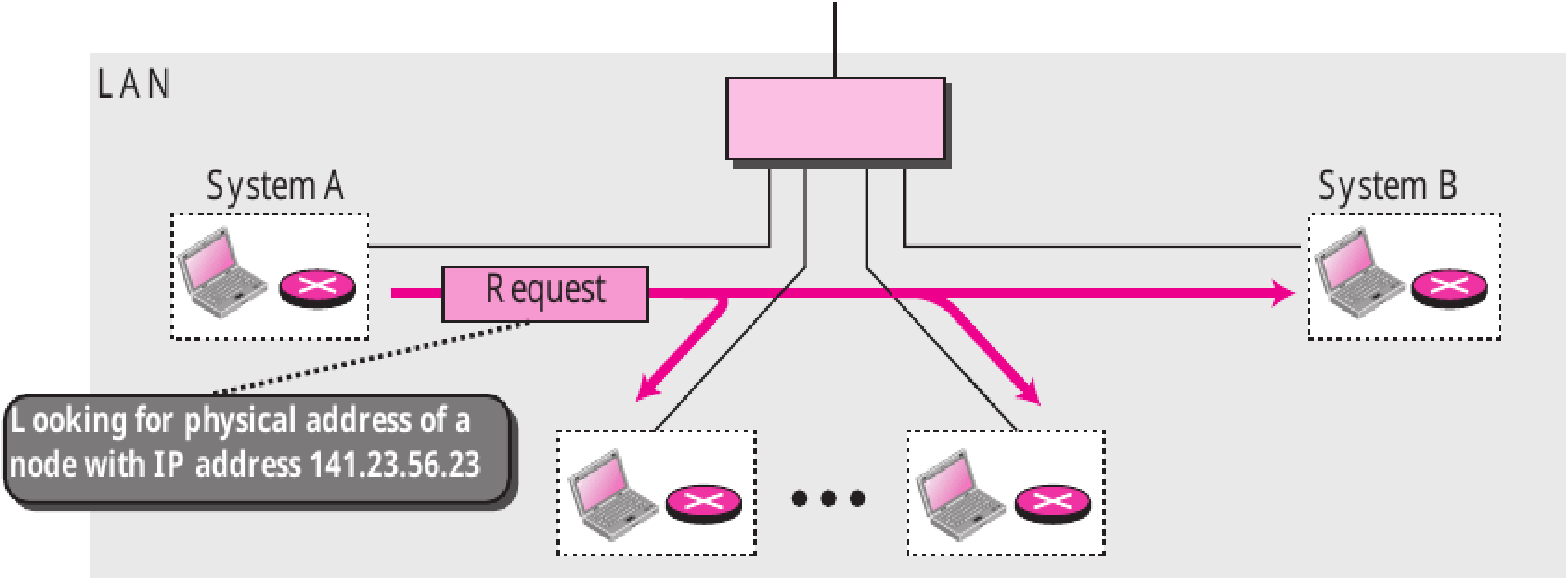
Dynamic Mapping

- In dynamic mapping each time a machine knows the logical address of another machine it can use a protocol to find the physical address.
- Two protocols have been designed to perform dynamic mapping: Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP)
- ARP maps logical address to physical address
- RARP maps physical address to logical address

The ARP Protocol

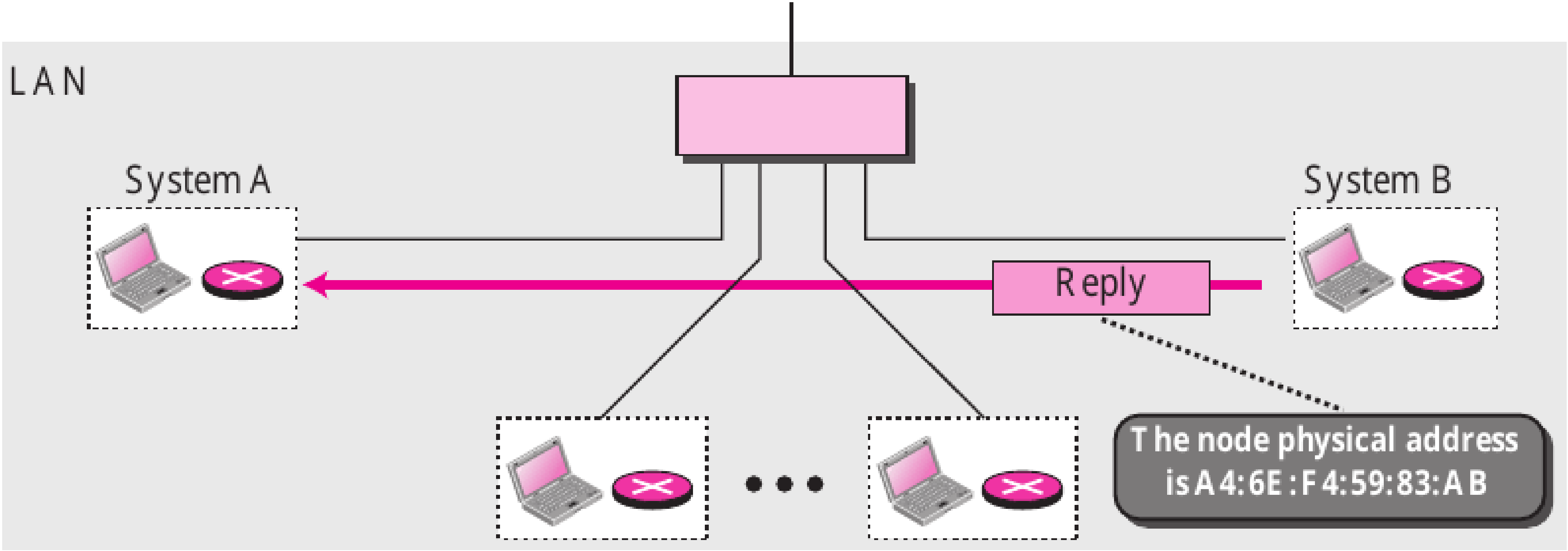
- ARP sends query packets, the packet includes the physical and IP address of the sender and the IP address of the receiver.
- Because the sender does not know the physical address of the receiver, the query is broadcast over the network.
- Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP and sends back an ARP response packet.

Illustration: ARP Query



a. ARP request is multicast

Illustration: ARP Reply



b. ARP reply is unicast

Internet Control Message Protocol (ICMP)

- ICMP was designed to provide error-reporting or error-correcting mechanisms.
- ICMP messages are divided into two broad categories: error-reporting messages and query messages.
- Error-reporting messages reports problems that a router or a host may encounter when it process 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.

ICMP Messages

Category	Type	Message
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

Debugging Tools

- There are several tools that can be used in the Internet for debugging.
  - Ping: can be used to find if a host is alive and responding.
  - The source host send ICMP echo request messages, if the destination is alive responds with echo reply message.
  - Traceroute: can be used to trace the route of the packet from the source to the destination.

End of Chapter 4
:)