

Chapter 5

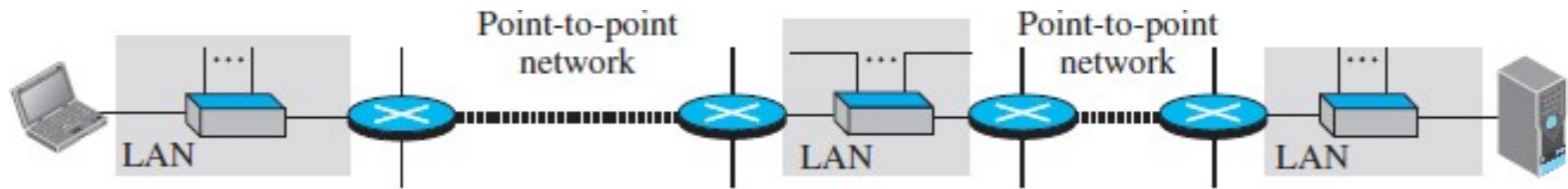
Data Link Layer

Data Link Layer

- Data Link Layer is present between Network layer and Physical layer
- Data Link Layer is also called as Link layer
- Data link layer is responsible for the following services:
 1. node-to-node / hop-to-hop communication
 2. Framing
 3. Error detection and correction
 4. Reliable Delivery
 5. Link Access

Data Link Layer Services

1. node-to-node / hop-to-hop communication



a. A small part of the Internet



- The source and destination system and the routers in between in 1st diagram is called as **nodes** and the networks in between is called as **links**
- Data link layer is responsible for **node to node delivery** because it is the responsibility of the data link layer to deliver the data to the next node in the network

Data Link Layer Services (contd..)

2. Framing

- ❑ Data Link layer encapsulate the packet received from network layer into frames
- ❑ Data in the Data Link Layer is usually called Frames

3. Error Detection and Correction

- ❑ Errors may occur during transmission of data through channel
- ❑ These errors should be detected and corrected at the receiver side

4. Reliable Delivery

- ❑ When a link-layer protocol provides reliable delivery service, it guarantees to move each network-layer datagram across the link without error

Data Link Layer Services (contd..)

5. Link Access

- When multiple nodes access a single broadcast link, data gets collided. This problem is called as multiple access problem
- In Data Link layer, MAC (Medium Access Control) protocol serves to coordinate the frame transmissions of the nodes
- A Medium Access Control (MAC) protocol specifies the rules by which a frame is transmitted onto the link.

Where Data Link layer is implemented?

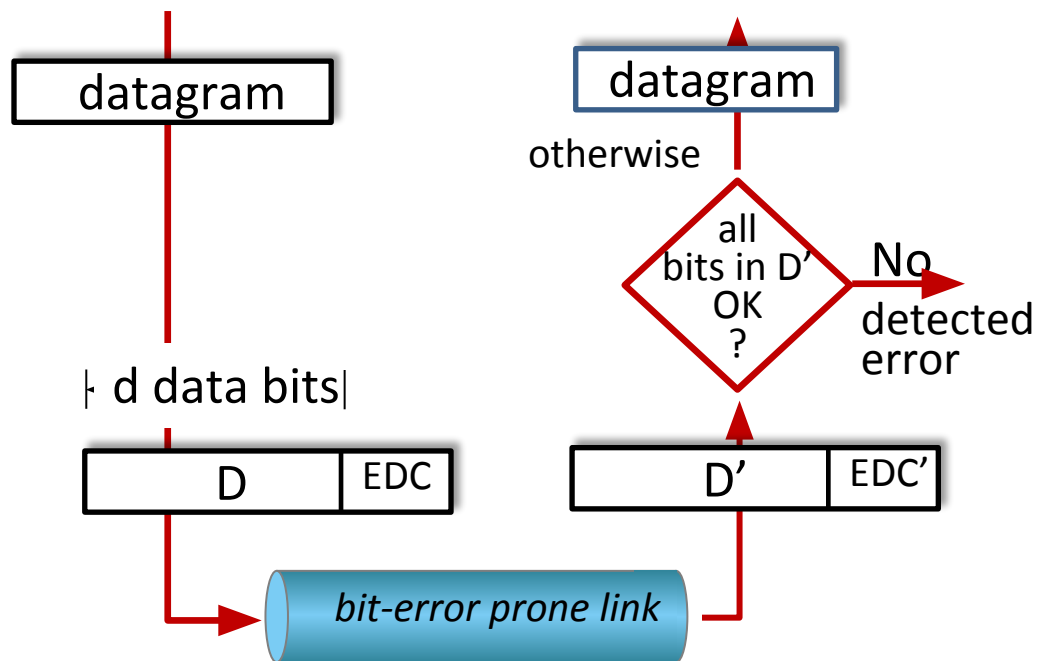
- The link layer is implemented on a chip called the **network adapter**, also sometimes known as a **network interface controller (NIC)**
- The network adapter implements many link layer services including framing, link access, error detection, and so on. Thus, much of a link-layer controller's functionality is implemented in hardware

Error Detection and Correction Techniques

- ❑ One of the main duty of Data link layer is to detect and correct the errors in the data that is been send by the sender
- ❑ Error detection and correction is been done at the receiver side. The receiver in order to do this error detection and correction, sender has to add the error detecting bits to the data
- ❑ This mechanism is shown in the diagram in next slide

Error Detection and Correction Techniques (contd..)

The error detection and correction techniques in link layer is going to add some extra bits to the data. These bits are called as Error Detection and Correction bits(EDC). This is done at the sender side



Receiver side is going to check error in the data with the help of these EDC bits

Error Detection and Correction Techniques (contd..)

- 3 types of Error detection and correction techniques are been used:
 1. Parity Check
 2. Cyclic Redundancy Check(CRC)
 3. Checksum

Error Detection and Correction Techniques (contd..)

1. Parity Check

(i) Single Bit Parity Check

- In single bit parity check only one bit is used as Parity bit
- Parity Check can be either **Even Parity** or **Odd Parity**
- Single bit Parity check detect only single bit error

Even Parity check

- In Even bit parity check sender counts the number of 1's in the data. If number of 1's is odd then parity bit is going to be 1
- If number of 1's is even means then parity bit is going to 0

Example:

- Consider the data = 1011. What is the parity bit at sender side and how it is verified at receiver side

Solution: Data = 1011, Number of 1's in the data is odd. So parity bit = 1

Data	Parity bit
1011	1

Error Detection and Correction Techniques (contd..)

- ❑ Sender after calculating the parity bit sends data + parity bit to the receiver
- ❑ Receiver checks whether the data contains even number of 1's.

If data contains even number of 1's: No error

If data contains odd number of 1's : Error

Odd Parity check

- ❑ In Odd bit parity check sender counts the number of 1's in the data. If number of 1's is odd then parity bit is going to be 0
- ❑ If number of 1's is even means then parity bit is going to 1

Example:

- ❑ Consider the data =1011. What is the parity bit at sender side

Solution:

Data = 1011, Number of 1's in the data is odd. So parity bit =0

Data	Parity bit
1011	0

Error Detection and Correction Techniques (contd..)

1. Parity Check

(ii) Two Dimensional Parity Check

- In two dimensional parity check, data is divided into rows and columns and the parity bits are calculated for each row and column. This method is used for both error detection and correction (specify which bit is corrupted)

Example: Consider the data unit to be transmitted is

10011001111000100010010010000100

Calculate the parity bits at the sender side if two-dimensional even parity check is used (use 8 bit words)

Solution: Divide data into 8 bits words and put each 8 bits in a row

								Parity Bit for Row
1	0	0	1	1	0	0	1	0
1	1	1	0	0	0	1	0	0
0	0	1	0	0	1	0	0	0
1	0	0	0	0	1	0	0	0
1	1	0	1	1	0	1	1	0

Parity Bit for column →

Error Detection and Correction Techniques (contd..)

2. Cyclic Redundancy Check(CRC)

In CRC error Detection method, CRC is calculated using following steps:

1. Initially data is augmented with (divisor-1) zero bits. After that
2. Perform XOR between data and divisor
3. Final remainder is going to be the **CRC bits**
4. Number of CRC bits is equal to (divisor-1) bits
5. Send data+CRC to receiver
6. At receiver side data+CRC is XOR'ed with divisor
7. If remainder ->zero means No Error
remainder->non-zero means Error

Error Detection and Correction Techniques (contd..)

2. Cyclic Redundancy Check(CRC)

Example 1:

Consider the Data = 1001 and divisor = 1011

CRC (Example)

Sender side

$$\begin{array}{r} 1011 \overline{) 10010000} \\ \underline{(XOR) 1011 \downarrow \downarrow} \\ 001000 \\ 1011 \downarrow \\ \hline 00110 \rightarrow \text{CRC} \end{array}$$

Data to Receiver: 1001110

Receiver side

$$\begin{array}{r} 1011 \overline{) 1001110} \\ \underline{1011 \downarrow \downarrow} \\ 001011 \\ 1011 \downarrow \\ \hline 00000 \rightarrow \text{Remainder} \\ \downarrow \\ 0 \\ \downarrow \\ \text{No error} \end{array}$$

$1011 \overline{) 10101110101}$
 $\underline{1011}$
 0001111
 $\underline{1011}$
 01000
 $\underline{1011}$
 001110
 $\underline{1011}$
 010101
 $\underline{1011}$
 0000
 \downarrow
 No Error

Error Detection and Correction Techniques (contd..)

3. Checksum

In Checksum error Detection method, checksum is calculated using following steps:

1. Data is divided into 16 bits words (by default data is divided into 16 bits words)
2. Binary addition is performed between each 16 words
3. Calculate the final sum for the given data
4. Take 1's complement for the final sum. This 1's complement result is going to be the **checksum**
5. Sender sends data + checksum to receiver
6. Receiver do the same steps as like that of sender
7. If final result is Zero -> No Error
Non zero -> Error

1's comp : 00 00 00 00 00 00 00 00
 ↳ No Error.

Error Detection and Correction Techniques (contd..)

3. Checksum

Example 2:

Consider the data unit to be transmitted is

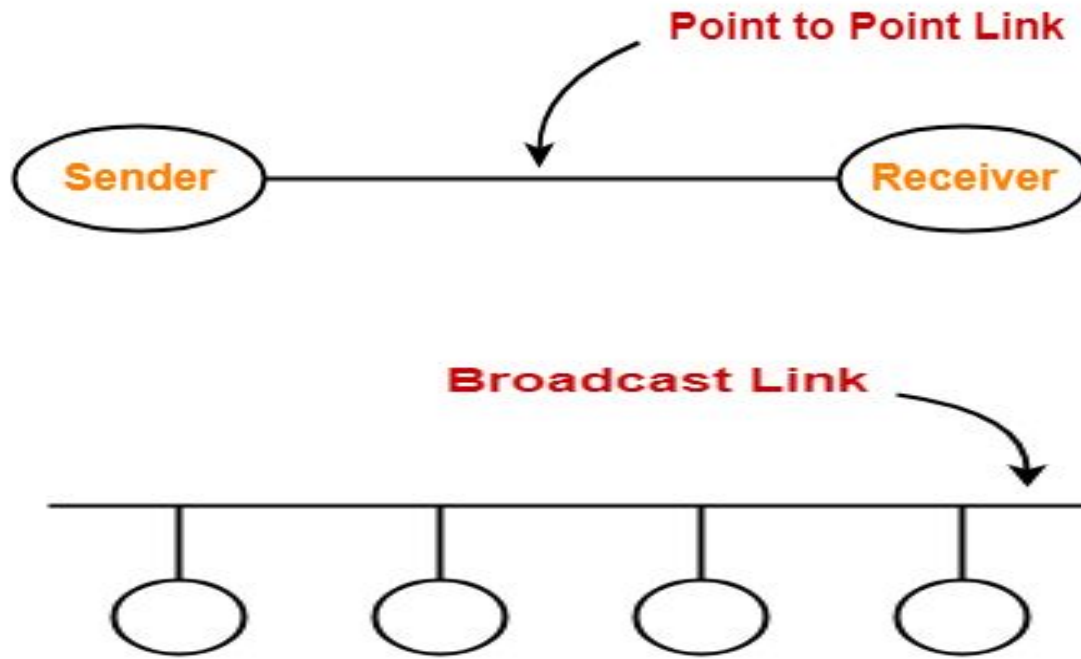
10011001111000100010010010000100

Calculate the checksum at sender side and how it is been verified at the receiver side
(Consider 8 bit checksum is used)

Multiple Access Protocols

2 types of Link,

1. Point-to-point link –dedicated link between 2 devices
2. Broadcast link – link shared between all devices



Multiple Access Protocols (contd..)

- When multiple stations are connected and use a common link(Broadcast or Multipoint link) data send by each system may get **collided**.
- To address this **collision problem, Multiple access protocols is been proposed**
- Multiple Access Protocols is responsible for coordinating the process of accessing the common link
- Multiple Access protocols is divided into 3 major categories
 1. Channel Partitioning Protocols
 - TDMA
 - FDMA
 - CDMA
 2. Random Access Protocols
 - ALOHA
 - CSMA
 - CSMA/CD
 - CSMA/CA
 3. Taking Turn Protocols
 - Polling Protocol
 - Token passing Protocol

Multiple Access Protocols (contd..)

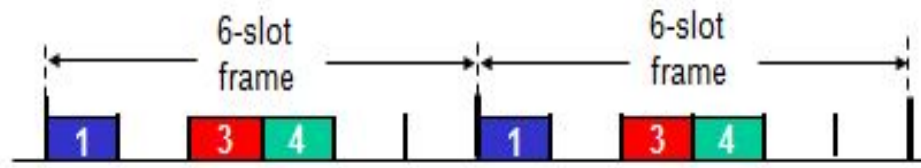
1. Channel Partitioning Protocols

(i) TDMA (Time Division Multiple Access)

- In TDMA time is divided into multiple slots based on number of systems and each station can transmit data only in its allocated time slot

Example:

6-station LAN, 1,3,4 have packets to send, slots 2,5,6 idle



Multiple Access Protocols (contd..)

1.Channel Partitioning Protocols

(ii) FDMA (Frequency Division Multiple Access)

- channel spectrum divided into frequency bands
- each station assigned fixed frequency band
- unused transmission time in frequency bands go idle

(iii) CDMA (Code Division Multiple Access)

- CDMA assigns a different code to each node.
- Each node then uses its unique code to encode the data bits it sends

Multiple Access Protocols (contd..)

2. Random Access Protocols

- ❑ In **random access** methods, no station is superior to another station and none is assigned the control over another. Transmission is random among the stations
- ❑ When multiple stations send data at the same time it may lead to **collision**. Some protocols have been designed in order to reduce this collision
- ❑ At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.

4 random access protocols:

1. ALOHA
2. CSMA
3. CSMA/CD
4. CSMA/CA

Multiple Access Protocols (contd..)

(i) ALOHA

- Protocol used for accessing the shared medium
- 2 versions under ALOHA protocol,
 - (i) Pure ALOHA
 - (ii) Slotted ALOHA

(i) Pure ALOHA:

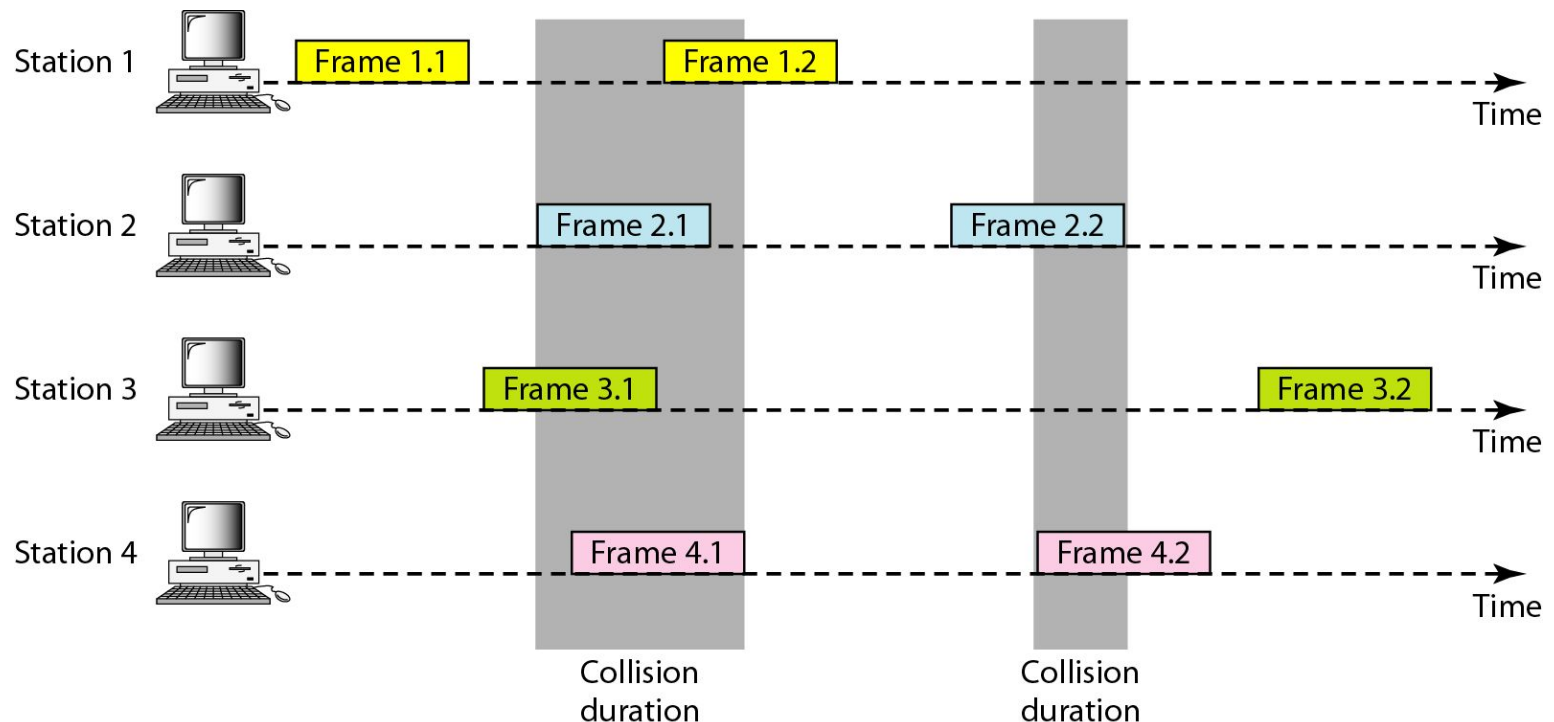
- The original ALOHA protocol is called Pure ALOHA
- Simplest protocol
- Whenever each station has a frame it sends through shared medium
- If multiple stations send data at the same time, there will be **collision**

Multiple Access Protocols (contd..)

(i) Pure ALOHA:

Frames in Pure ALOHA

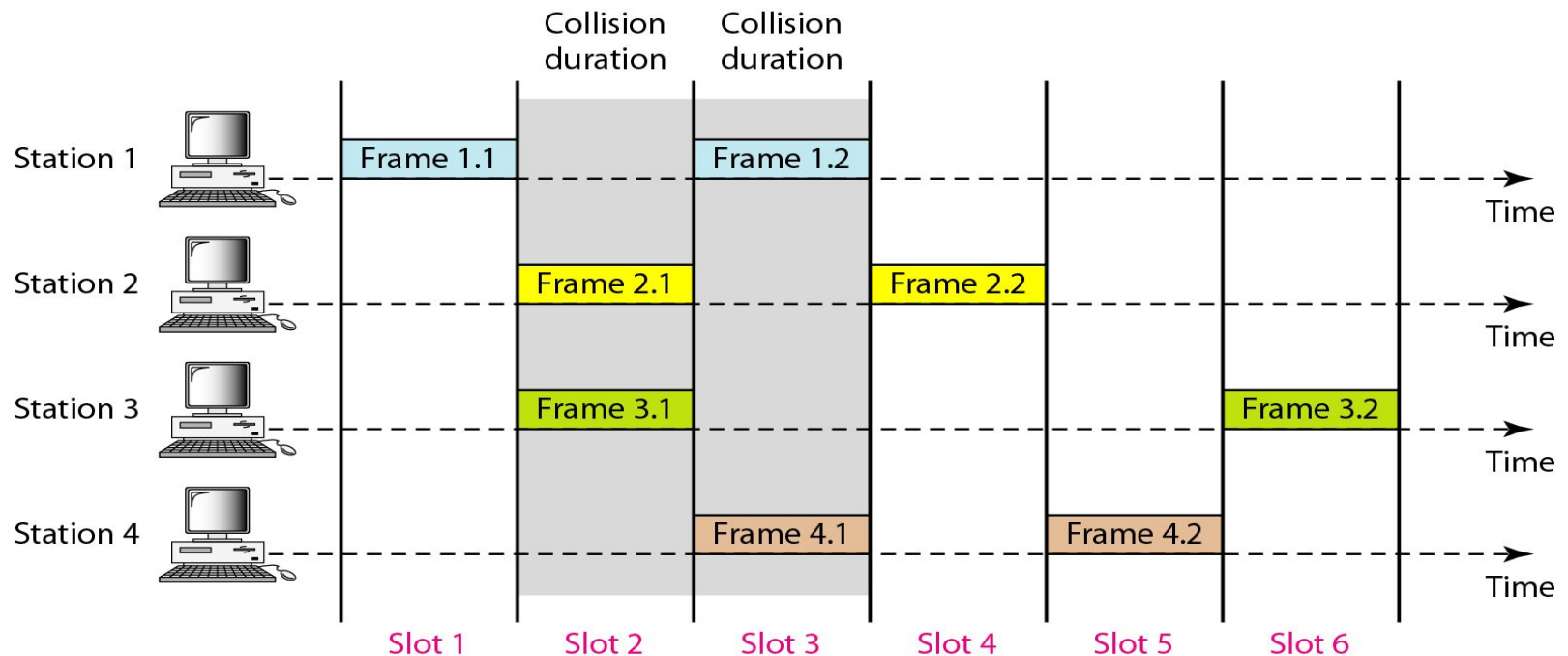
- ❑ In the following figure among 8 frames sent, only 2 frames survive(Frame 1.1, Frame 3.2) and remaining frames get collided
- ❑ After collision each station waits for some random time and then only retransmits the data
- ❑ Since random time vary from one station to another, collision during retransmission is somewhat reduced



Multiple Access Protocols (contd..)

(ii) Slotted ALOHA:

- ❑ Slotted ALOHA is used to improve the efficiency of pure ALOHA
- ❑ In slotted ALOHA, **time is divided into multiple slots and each station sends data only at the beginning of the time slot**. A station can't send frames during the middle of a time slot which reduces collision
- ❑ Since station sends data only at the beginning of the time slot, collision problem seen in pure ALOHA is reduced here but still collision problem exist when multiple stations send data at the beginning of a time slot



Multiple Access Protocols (contd..)

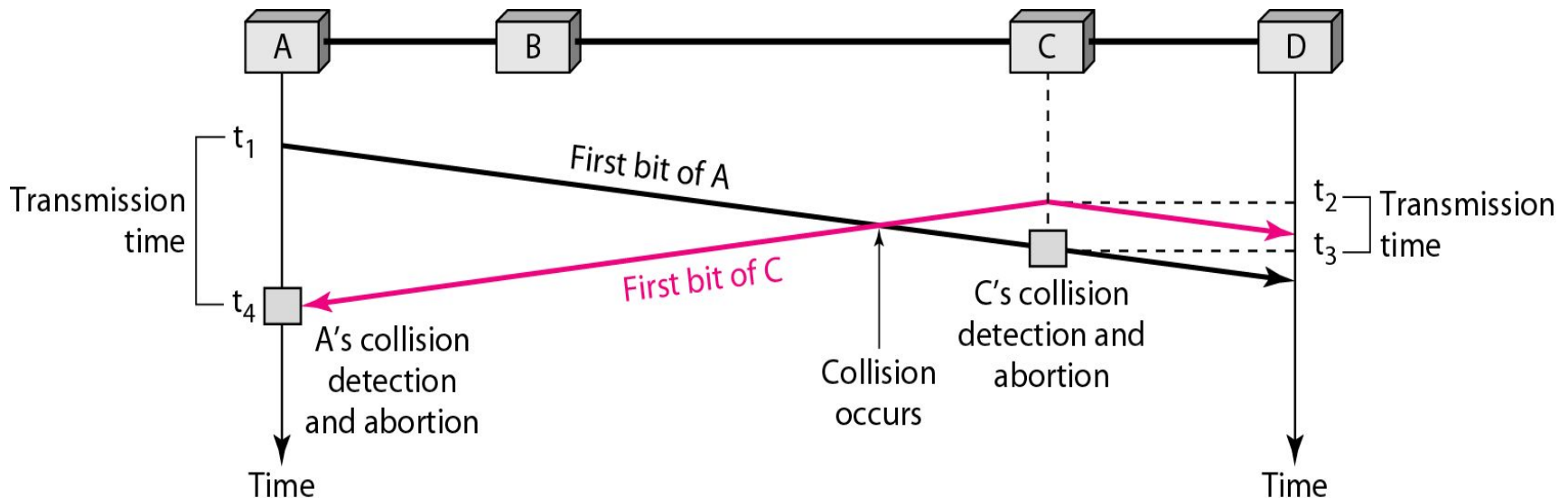
(ii) Carrier Sense Multiple Access (CSMA)

- ❑ “Carrier” means channel or medium. In this protocol channel is sensed before transmitting the data
- ❑ To minimize the chance of collision and to increase performance, CSMA method was developed
- ❑ Principle of CSMA: “sense before transmit” or “listen before talk”
- ❑ Carrier is busy means Transmission is currently taking place
- ❑ Carrier is idle means No transmission is currently taking place
- ❑ The channel is sensed and if it is idle means then station will send data. Otherwise station has to wait until channel becomes idle
- ❑ Possibility of collision still exists because when a station sends a frame, it takes time for the first bit of that frame to reach other stations. During that time some other stations may sense the channel and find it idle and send data

Multiple Access Protocols (contd..)

(iii) Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

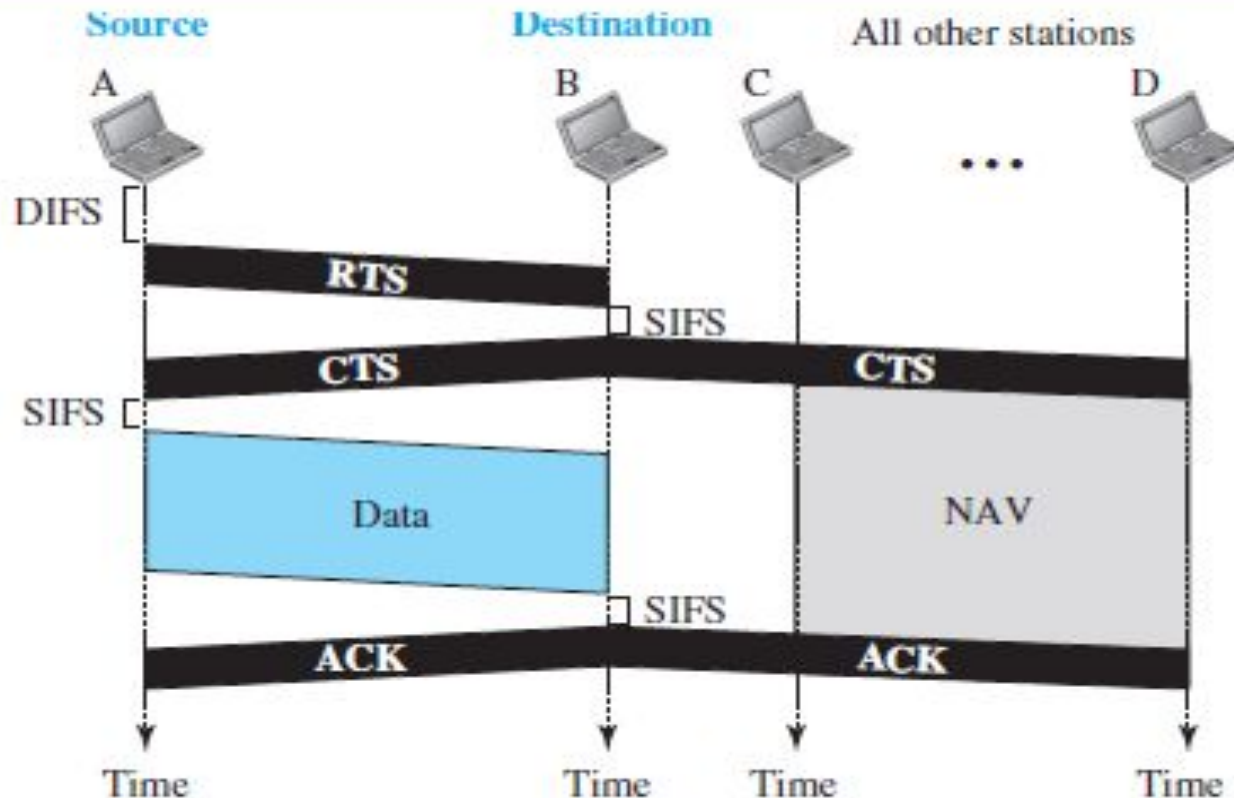
- CSMA/CD is the advancement of CSMA in which whenever collision occurs and station identifies that collision has occurred it is going to stop its transmission of data
- In below diagram, station A send data at time t_1 . Station C also wants data to send and senses channel at time t_2 . Since at time t_2 data sent by A has not reached C, C finds channel as idle and sends data. At time t_3 only C identifies collision had occurred and stop its further transmission. Similarly A also detects collision at time t_4 and stops transmission of data



Multiple Access Protocols (contd..)

(iv) Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

- In CSMA/CA, station that wants to send senses the channel. If channel is busy means then station will wait. If channel is idle means instead of sending data immediately station will wait for a period of time called **interframe space or IFS**.



Multiple Access Protocols (contd..)

(iv) Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

- ❑ In CSMA/CA station senses channel. If it is idle then station waits for a period of time called **DCF interframe space (DIFS)**. Then station sends a control frame called **Request To Send (RTS)**
- ❑ After receiving RTS and waiting a period of time called **short interframe space(SIFS)**, the destination station sends a frame called **clear to send (CTS)**. Clear to send indicates that the destination is ready to receive
- ❑ The source station sends data after waiting an amount of time equal to SIFS.
- ❑ The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received
- ❑ In CSMA/CA the collision avoidance is accomplished by a feature called **NAV(Network Allocation Vector)**.
- ❑ When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. Other stations create a timer called a network allocation vector (NAV) that shows how much time it should wait to check the channel idleness. Each time a station sends an RTS frame, other stations start their NAV. In other words, each station, before sensing the physical medium to see if it is idle, first checks its NAV to see if it has expired.

Multiple Access Protocols (contd..)

3. Taking Turn Protocols

- 2 types of taking turn protocols
 1. Polling Protocol
 2. Token Passing Protocol

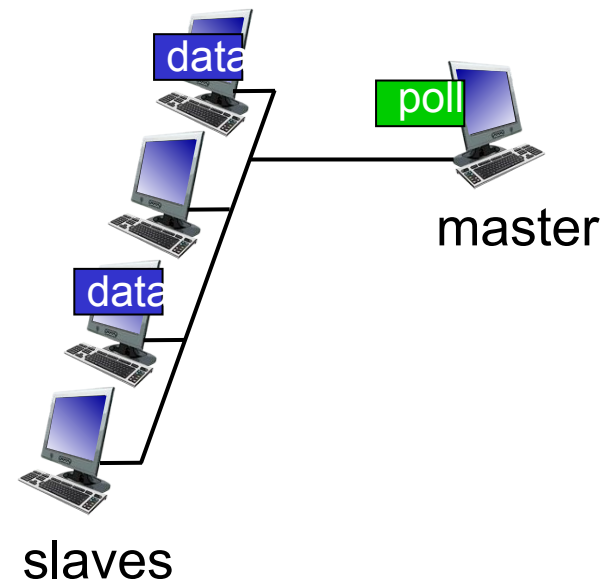
Multiple Access Protocols (contd..)

(i) Polling Protocol

- There should be a master node
- master node “invites” slaves nodes to transmit in turn (ie) master node “polls” the slave node. If it has data slave can transmit

Pros and Cons:

1. No collision
2. polling overhead
3. latency
4. single point of failure (master)



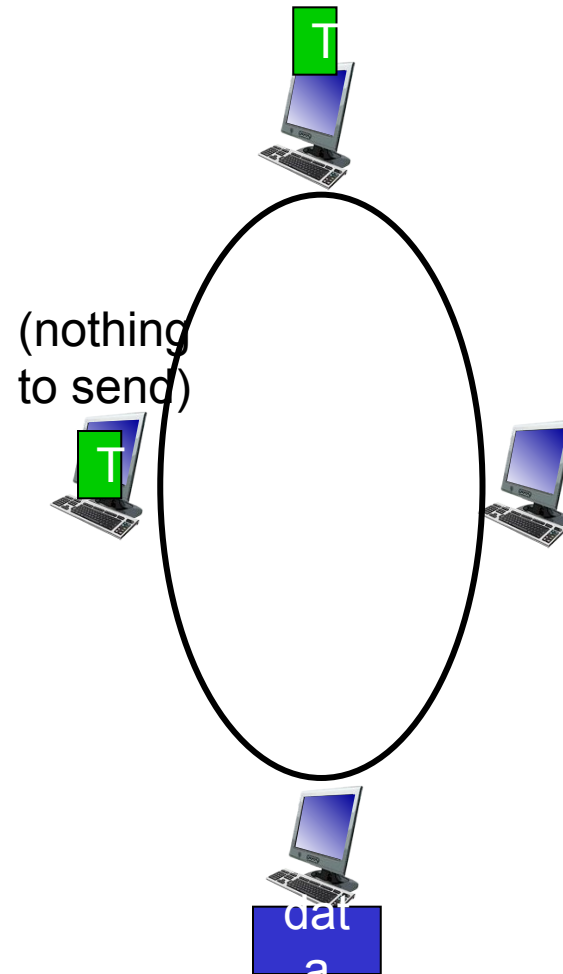
Multiple Access Protocols (contd..)

(ii) Token Passing Protocol

- ❑ No master-slave concept
- ❑ A concept called “Token” is used here
- ❑ If a node wants to send data first it has to hold the token and then only it can transmit the data
- ❑ After sending data, the node passes token to the next node

Pros and Cons:

1. No collision
2. token overhead
3. latency
4. single point of failure (token)



Link-Layer Addressing

MAC Address

- ❑ A Network Interface Card (NIC) is a hardware component without which a computer cannot be connected over a network.
- ❑ It is a circuit board installed in a computer that provides a dedicated network connection to the computer.
- ❑ It is also called network interface controller, network adapter or LAN adapter.
- ❑ Physical address is a globally unique address assigned to every Network Interface Card (NIC) in a system
- ❑ This address is used to uniquely identify a system in a network
- ❑ This address is provided by the manufacturer who manufactures the card and is embedded in the card itself
- ❑ This address is a **permanent address** . Even though we are moving a system from one network to another network this address remains same
- ❑ Physical address is mostly referred as called **Media Access Control (MAC) address**
- ❑ Also referred in other ways like **Link Layer address (or) LAN address**
- ❑ Useful for local communications

Physical Address/MAC Address (contd..)

Format of MAC address:

- ❑ Every MAC address is of 48 bits which is written in hexadecimal format as shown below
- ❑ Every byte is separated by colon

48-bit physical address

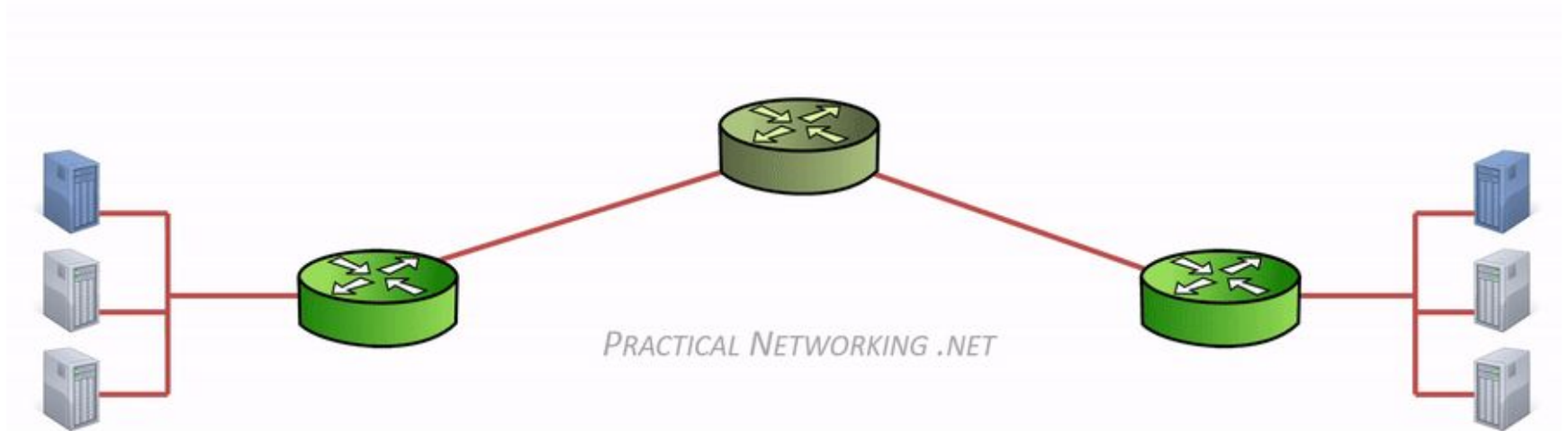
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
07:01:02:03:04:4B
└─┬─┬─┬─┬─
↑ ↑ ↑ ↑ ↑

Link-layer address

LAN address

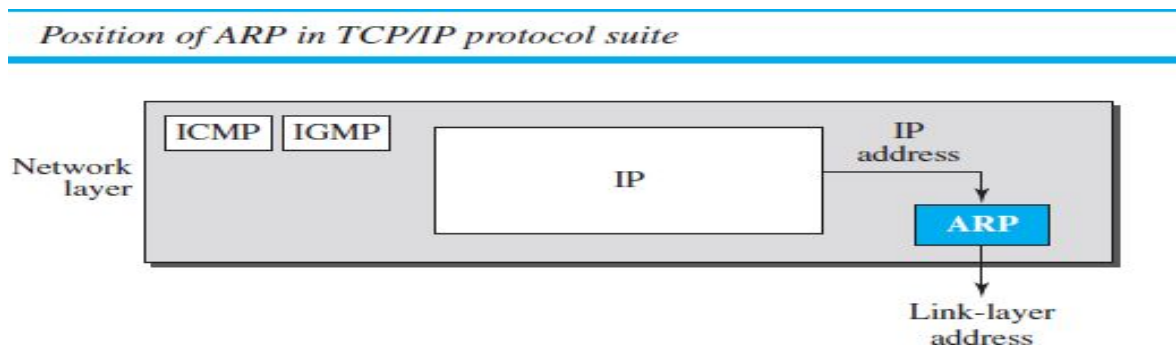
MAC address

Animation representing changing of MAC address at intermediate nodes (Put in slideshow and see)



Address Resolution Protocol (ARP)

- ARP accepts an IP address from the IP protocol, maps it to the corresponding link-layer address (MAC address) and passes it to the data-link layer.
- IP -> MAC address



Address Resolution Protocol (ARP) (contd..)

ARP packet format

0		8		16		31	
Hardware Type				Protocol Type			
Hardware length		Protocol length		Operation Request:1, Reply:2			
Source hardware address							
Source protocol address							
Destination hardware address (Empty in request)							
Destination protocol address							

Address Resolution Protocol (ARP) (contd..)

ARP packet format

- In the ARP packet format, Source Hardware address contains the MAC address of source, Source Protocol address contains the IP address of source
- Destination Hardware address is empty (ie) all bits is zero (In ARP Request message) and Destination Protocol address contains the IP address of Destination
- Using Destination IP address, the MAC address of Destination machine will be found

Address Resolution Protocol (ARP) (contd..)

ARP Operation

- There are two types of ARP messages,

1. ARP Request
2. ARP Reply

1. ARP Request message

- Since source does not know the MAC address of destination, ARP Request message will be sent as a Broadcast message.
- (ie) Destination MAC address in Ethernet Frame in Request message will be a Broadcast MAC address

2. ARP Reply message

- Since ARP request is sent as a broadcast message, all machines in the network will receive the ARP request.
- The machine which has the IP address present in the Destination IP address field of ARP request will give the ARP Reply.

Address Resolution Protocol (ARP) (contd..)

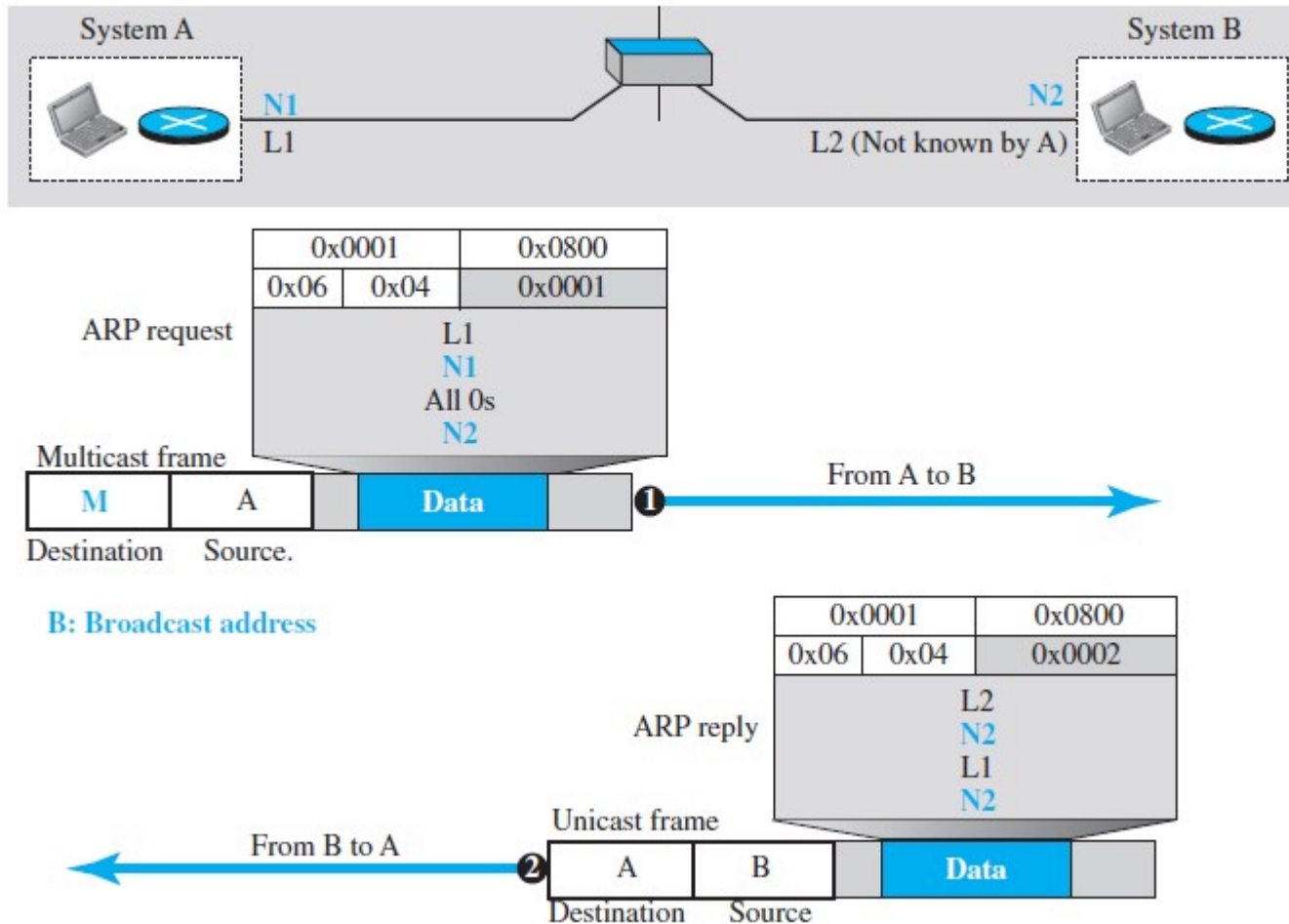
ARP Operation

2. ARP Reply message

- ARP Reply message is a unicast message. It will be sent only to the particular machine (the machine which has raised the ARP Request). Upon receiving the reply message, the sender machine gets the MAC address of destination present in the reply message
- Request and response message diagram shown in next slide

Address Resolution Protocol (ARP) (contd..)

ARP Operation



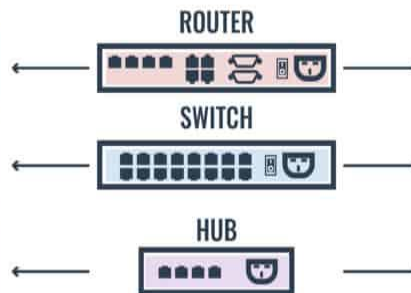
Connecting Devices

- 3 connecting devices,
 1. Hub (Physical layer device)
 2. Switch (Data link layer device)
 3. Router (Network layer device)

OSI REFERENCE MODEL



TCP/IP CONCEPTUAL LAYERS

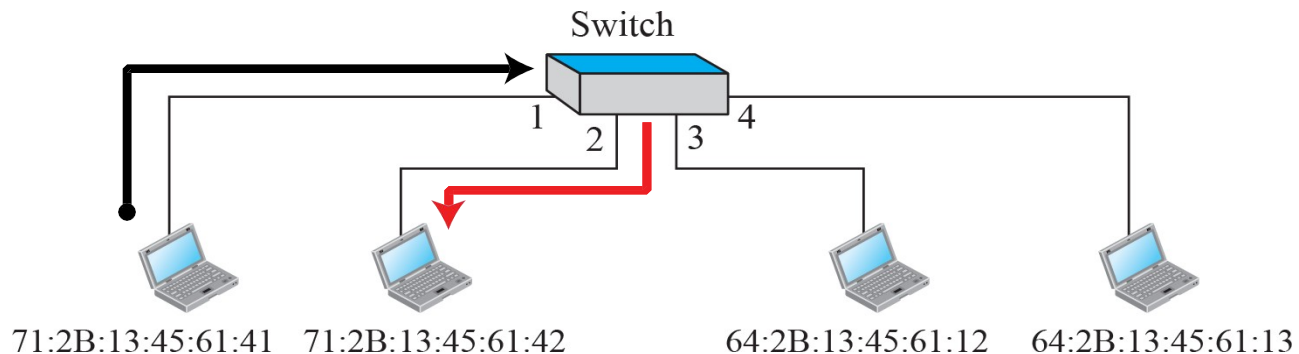


Switch

- ❑ Switch is a link layer device
- ❑ It operates in both physical layer and data link layer
- ❑ It checks the destination MAC address of incoming data and gives the data only to the appropriate destination
- ❑ Switch uses switching table for delivering data to the appropriate destination

Switching table

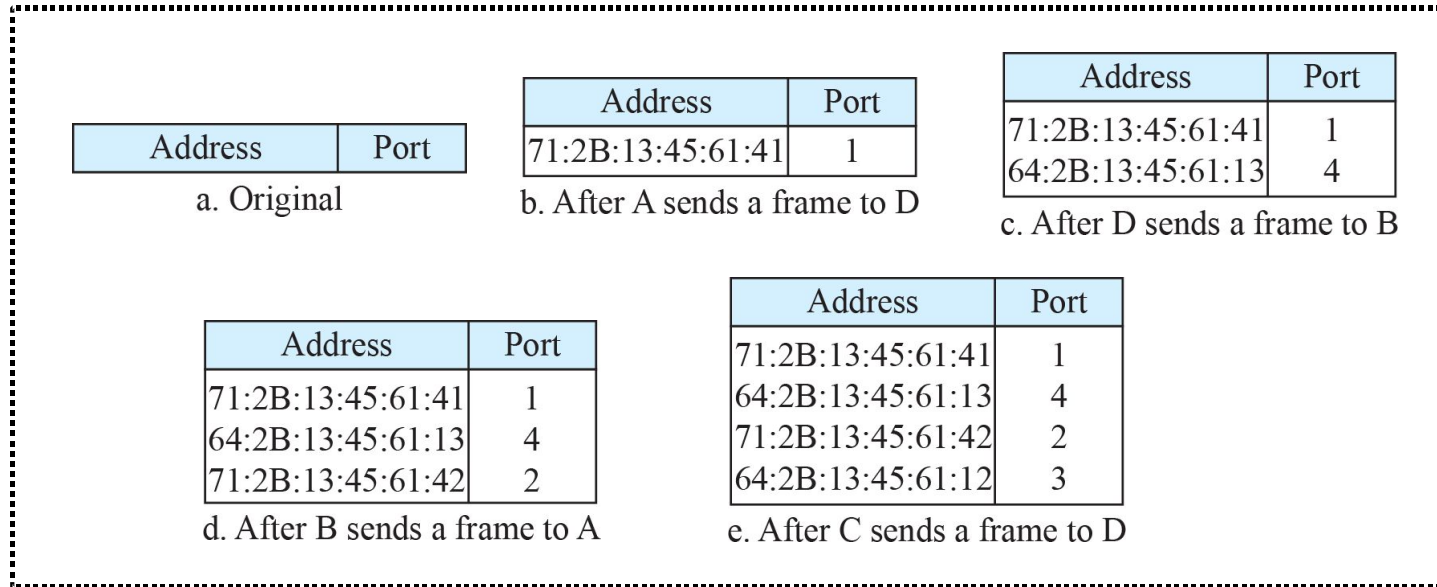
Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3
64:2B:13:45:61:13	4



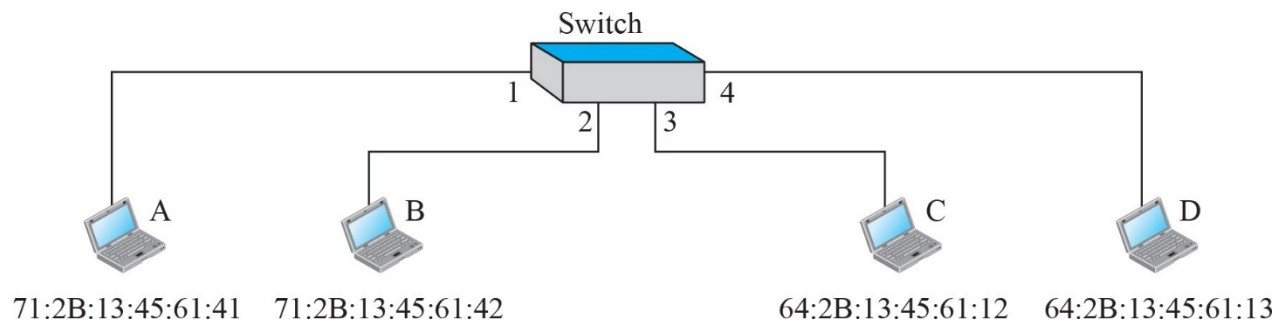
Switch (contd..)

- Each switch has a **switch table**,
- Each entry in the switch table has the following fields:
(MAC address of host, interface to reach host, time stamp)
- It looks like a routing table
- Switch **self learns** by itself to know which hosts can be reached through which interfaces
- when frame received, switch “learns” location of sender: incoming LAN segment and records sender/location pair in switch table
- Diagram shown in next slide

Switch (contd..)

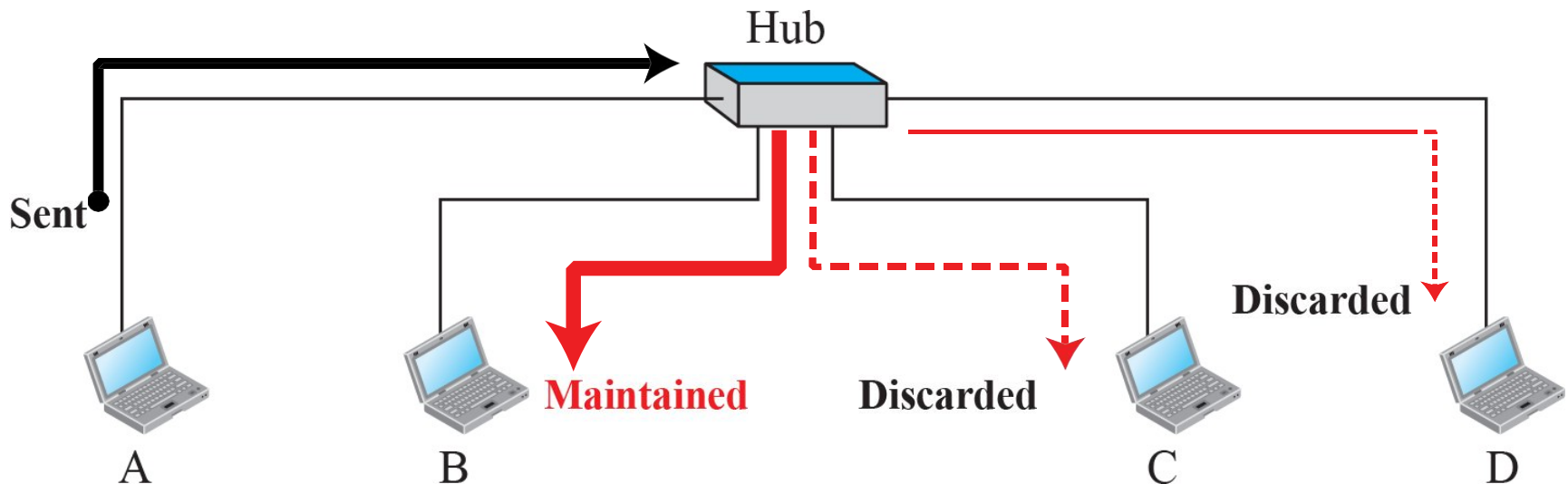


Gradual building of Table



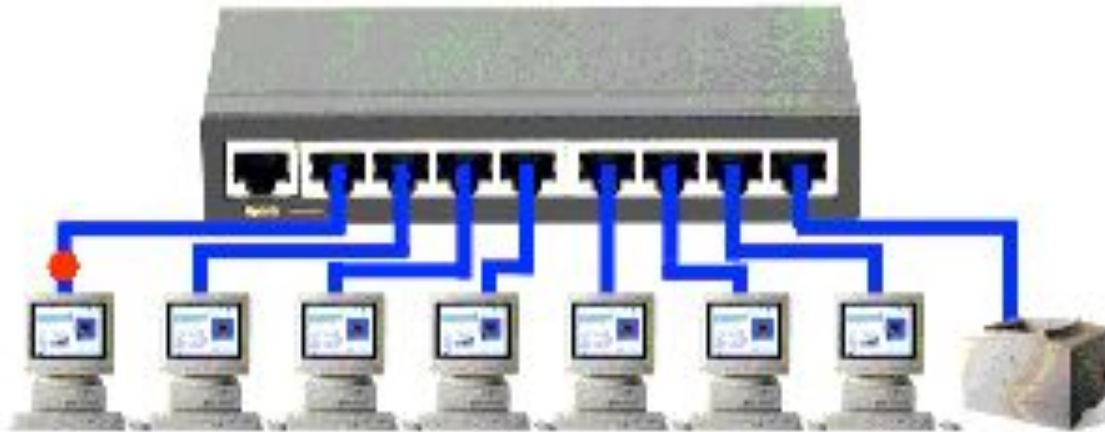
Hub

- ❑ Hub is a physical layer device
- ❑ Whenever data comes to a hub, it transmits it to all devices connected to it (ie) data is broadcasted.
- ❑ Hub is not an intelligent device. It does not have intelligence to find through which port the data should be sent out
- ❑ In below diagram when hub receives data from A it sends it to all devices connected to it. However B is the destination. So B keeps the data and remaining devices are going to discard it



Hub (contd...)




Hub



Comparison

	Hub	Switch	Router
Layer	Physical layer device	Link Layer Device	Network layer device
Connection of Devices	Connects two or more devices within a LAN	Connects two or more LAN devices	Can connect devices or a LAN and WAN
Device type	Non-intelligent, least expensive and least complex device	Intelligent device	Extremely smart and complex
Functionality	Cannot perform filtering	Filters packets before forwarding them	Highly configured to filter and forward packets
Used in	LAN	LAN	LAN, WAN, MAN
Transmission mode	Half-Duplex	Half-Duplex/ Full Duplex	Full Duplex

Comparison

	Hub	Switch	Router
Data Transmission form	Sends data in the form of electrical signal or bits	Sends data in the form of frames	Sends data in the form of Packet
Speed	10Mbps	10/100Mbps, 1Gbps	1-100Mbps(wireless); 100Mbps-1Gbps(wired)
Address	Does not store any IP or MAC address	Store MAC address	Store IP address
			

Ethernet

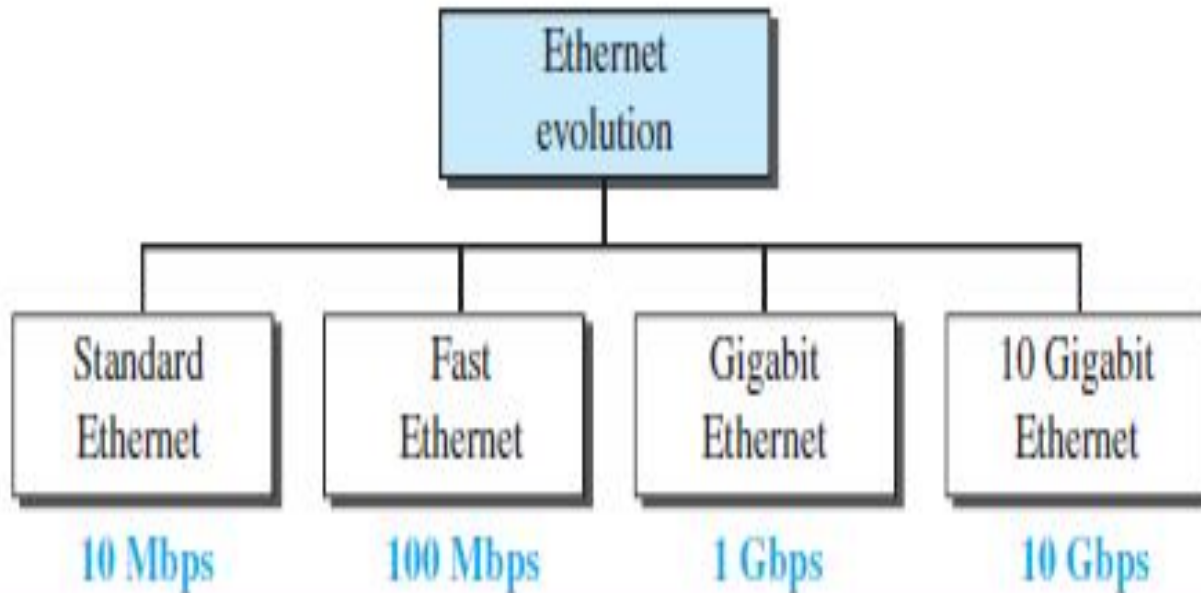
- ❑ Ethernet is a standard communication protocol used to connect computers within LAN and WAN
- ❑ Widely used wired LAN technology
- ❑ Ethernet was standardized into the standard **IEEE 802.3**

LAN vs Ethernet:

- ❑ LAN is a term used to describe a group of computers connected to each other within a small radius. Ethernet is a technology (based on IEEE 802.3) that describes how to connect the computers together

Ethernet Evolution

- 4 generations in Ethernet evolution,



Standard Ethernet

- Ethernet technology with **data rate of 10Mbps** is referred as Standard Ethernet

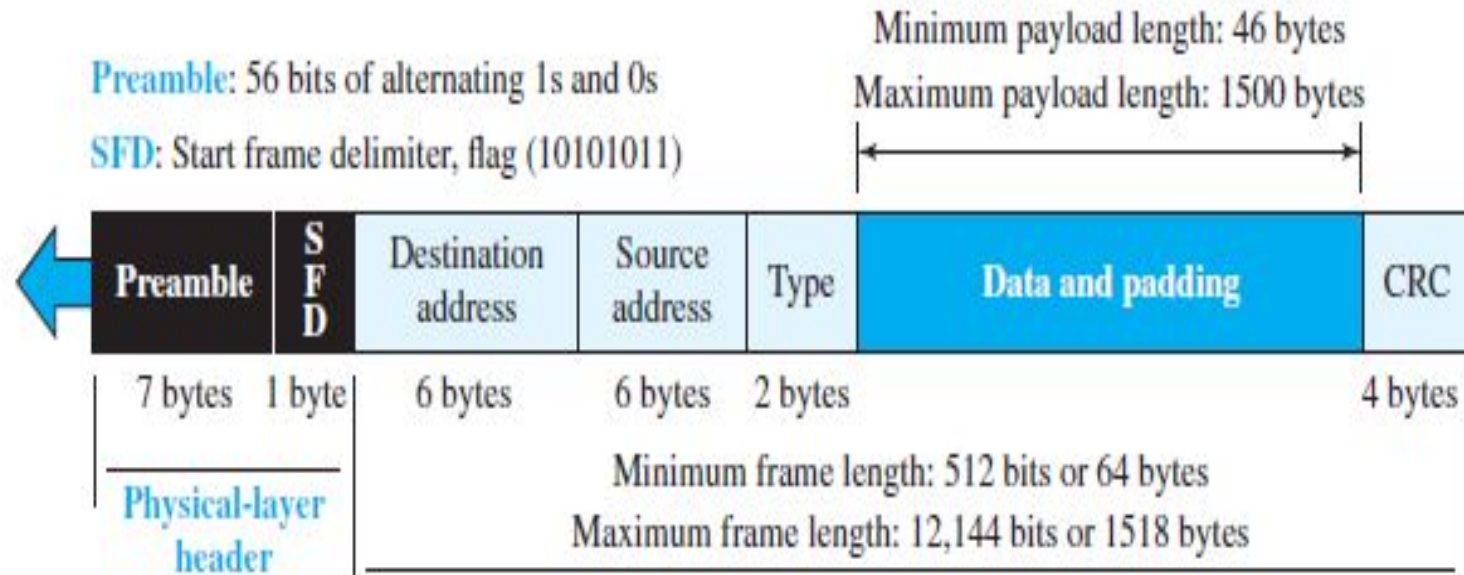
Characteristics:

Connectionless and unreliable Service:

- Each frame is independent of previous and next frame
- And also Ethernet is unreliable

Standard Ethernet (contd..)

Ethernet Frame Format:



Standard Ethernet (contd..)

Preamble:

- Contains 7 bytes (56 bits) of alternating 0's and 1's
- Alert the receiver about the incoming frame

Start Frame Delimiter (SFD):

- Start Frame Delimiter is a flag which indicates the beginning of a frame (Because Ethernet frames are of variable size flag is used)
- 1 byte field

Destination Address(DA):

- This field contains MAC address of destination system
- Length is 6 bytes(48-bits)

Source Address(SA):

- This field contains MAC address source system
- Length is 6 bytes(48-bits)

Type:

- Type field defines the upper layer protocol(like IP, ARP, OSPF)

Standard Ethernet (contd..)

Data and padding:

- This field represents the data from the upper layer
 - Minimum length of the data: 46 bytes
 - Maximum length of the data: 1500 bytes
- If data from upper layer is greater than 1500 bytes then data should be fragmented
- If data is less than 46 bytes then it should be added with extra 0s(padding)

CRC:

This field contains error detection information.

CRC is calculated over addresses, types and data field

Network Security

Network Security

- ▣ **Network Security** is the practice of protecting computer networks and their data from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure.

Properties of secure Communication

- **Confidentiality** - Only the sender and receiver should be able to understand the contents of the transmitted message
- **Message integrity** - ensure that the content of their communication is not altered
- **End-point authentication** - Both the sender and receiver should be able to confirm the identity of the other party involved in the communication
- **Operational security**

Principles of Cryptography

Following are the terms used in Network security,

Plaintext

- message in its original form. It is in a human-understandable form

Ciphertext

- Cipher text is the encrypted (coded) version of the plain text

Encryption

- The process of converting plain text (readable data) into cipher text (unreadable form).

Decryption

- The process of converting cipher text back into plain text (readable form).

Key

- A key is a secret value used by encryption algorithms to convert plaintext (readable data) into ciphertext (unreadable data) and back again. It ensures that only authorized users can access or modify information.

Symmetric Key Cryptography

- Symmetric key cryptography (also called secret key cryptography) is a method of encryption where the same key is used for both encryption and decryption.
- The sender and receiver share one secret key that must be kept private.

Symmetric Key Cryptography (contd..)

1. Caesar cipher

- The Caesar Cipher is one of the simplest encryption techniques.
- It works by shifting each letter of the plain text by a fixed number of positions (specified in Key) in the alphabet.

Example

Plain text= HELLO

Key, $k=3$

Shift each letter in plain text by 3 positions,

Cipher Text = **KHOOR**

Symmetric Key Cryptography (contd..)

2. Monoalphabetic cipher

- A Monoalphabetic Cipher is a substitution cipher in which each letter of the plaintext is replaced with another fixed letter of the alphabet.

Example

Each letter in the plaintext is replaced according to a substitution key

Let's take this substitution key:

Plaintext letter:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext letter:	m	n	b	v	c	x	z	a	s	d	f	g	h	j	k	l	p	o	i	u	y	t	r	e	w	q

- Plain text= hello
- Using above substitution key, Cipher Text =acggk

Symmetric Key Cryptography (contd..)

3. Polyalphabetic Encryption

- Polyalphabetic encryption is a type of substitution cipher in which multiple cipher alphabets are used to encrypt the message.
- This means the same letter in the plaintext can be encrypted to different letters in the ciphertext, depending on its position in the text.

Example

Plaintext letter:	a b c d e f g h i j k l m n o p q r s t u v w x y z
$C_1(k = 5)$:	f g h i j k l m n o p q r s t u v w x y z a b c d e
$C_2(k = 19)$:	t u v w x y z a b c d e f g h i j k l m n o p q r s

Figure 8.4 ♦ A polyalphabetic cipher using two Caesar ciphers

- We choose to use these two Caesar ciphers, C_1 and C_2 , in the repeating pattern C_1, C_2, C_2, C_1, C_2 . That is, the first letter of plaintext is to be encoded using C_1 , the second and third using C_2 , the fourth using C_1 , and the fifth using C_2 .

Symmetric Key Cryptography (contd..)

3. Polyalphabetic Encryption

Example

- plain text= hello
- Using two Caesar ciphers C1 and C2 and the pattern C1, C2, C2, C1, C2, the Cipher Text is = mxeqh

Symmetric Key Cryptography (contd..)

4. Block Ciphers

- In a block cipher, the message to be encrypted is processed in blocks of k bits (ie) Plaintext is divided into equal-sized blocks
- For example, if $k = 64$, then the message is broken into 64-bit blocks, and each block is encrypted independently.
- To encode a block, the cipher uses a one-to-one mapping to map the k -bit block of plaintext to a k -bit block of ciphertext.

Symmetric Key Cryptography (contd..)

Example

- Consider the case where the message is divided into blocks of 3-bits and converted to cipher text using the below table

input	output	input	output
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

Table 8.1 ♦ A specific 3-bit block cipher

- Thus the message 010110001111 gets encrypted into **101000111001** where the 1st 3-bits(010) is encrypted to 101 using above mapping. Similarly it is done for remaining bits.

Public Key Encryption

- Public Key Encryption (also called Asymmetric Encryption) is a method of encrypting data using two different keys:
 1. Public Key (used for encryption)
 2. Private Key (used for decryption)

1. Public Key

- A key that is shared openly with everyone to encrypt data or verify digital signatures.

2. Private Key

- A key that is kept secret by the owner and used to decrypt data or create digital signatures.

Public Key Encryption (contd..)

Key Generation:

- A pair of keys is created: one public and one private.
- The public key can be shared with anyone and the private key is kept secret by the owner.

Encryption:

- The sender uses the receiver's public key to encrypt the message.
- Once encrypted, only the receiver's private key can decrypt it.

Decryption:

- The receiver uses their **private key** to decrypt the message.
- Even if someone intercepts the ciphertext, they cannot decrypt it without the private key.

Public Key Encryption (contd..)

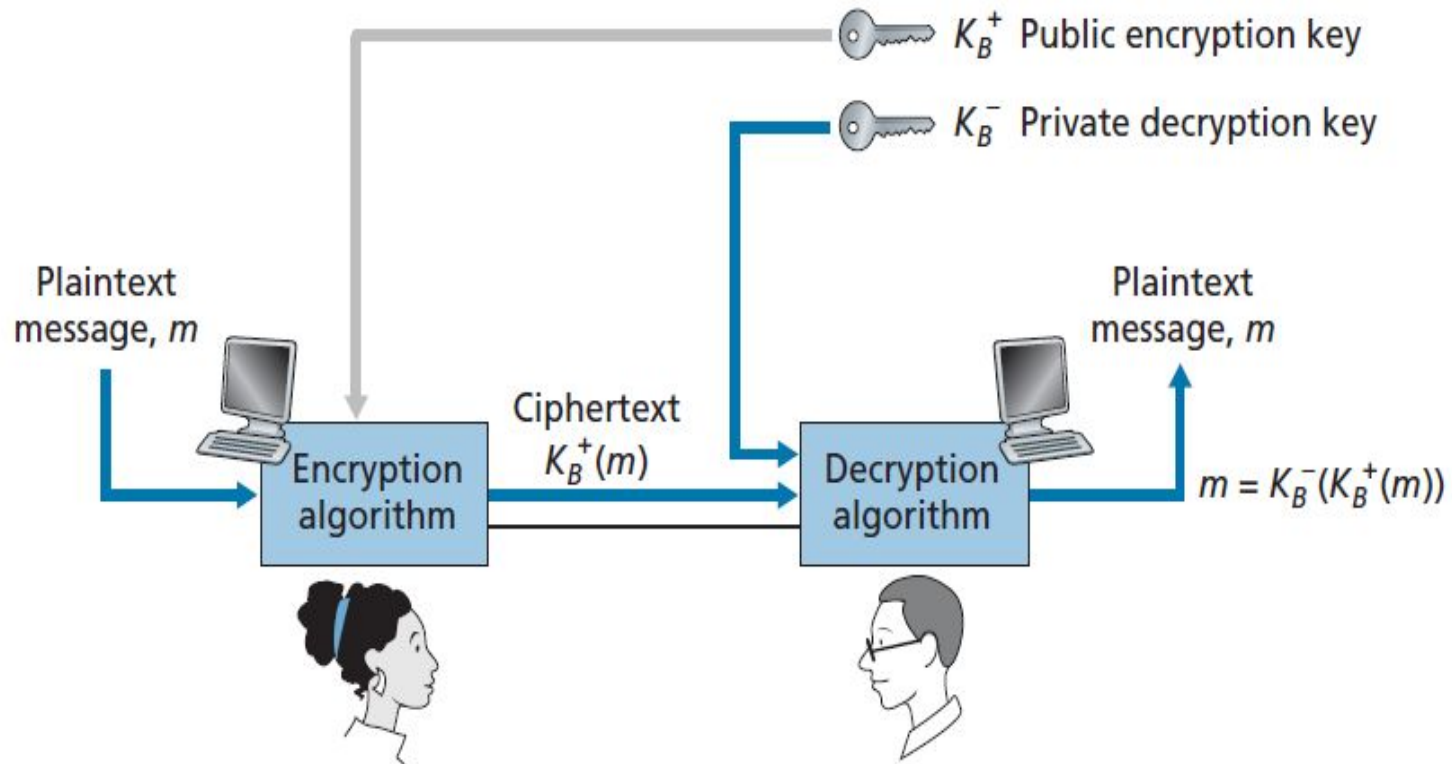


Figure 8.6 ♦ Public key cryptography

Public Key Encryption (contd..)

RSA Algorithm

- The RSA algorithm is the most widely used public key encryption algorithm
- RSA is used in digital signatures, secure data transmission, and SSL/TLS (https).