DATCOMM
Local Area Network Technologies

Engr. Melvin K. Cabatuan, MsE

De La Salle University

February 2013

Objectives

- To briefly discuss the technology of dominant wired LANs- Ethernet, and other LAN media.

Objectives

- To briefly discuss the technology of dominant wired LANs- Ethernet, and other LAN media.
- Describe Media Access Control (MAC) and Carrier Sense Multiple Access/Collision Detection (CSMA/CD)

Objectives

- To briefly discuss the technology of dominant wired LANs- Ethernet, and other LAN media.
- Describe Media Access Control (MAC) and Carrier Sense Multiple Access/Collision Detection (CSMA/CD)
- Explain Address Resolution Protocol (ARP) and Bridges.

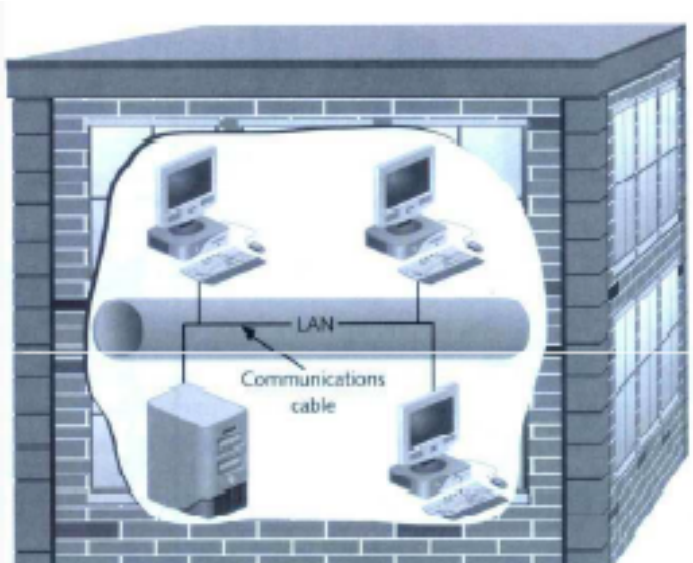
Objectives

- To briefly discuss the technology of dominant wired LANs- Ethernet, and other LAN media.
- Describe Media Access Control (MAC) and Carrier Sense Multiple Access/Collision Detection (CSMA/CD)
- Explain Address Resolution Protocol (ARP) and Bridges.
- Discuss Switched Ethernet and Virtual LAN (VLAN).

Local Area Network

LAN

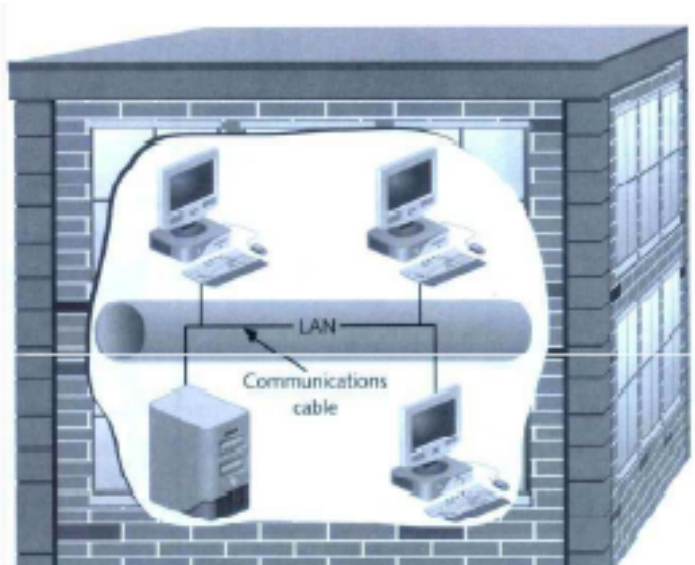
- A computer network that is designed for a limited geographic area such as a building or a campus.



Local Area Network

LAN

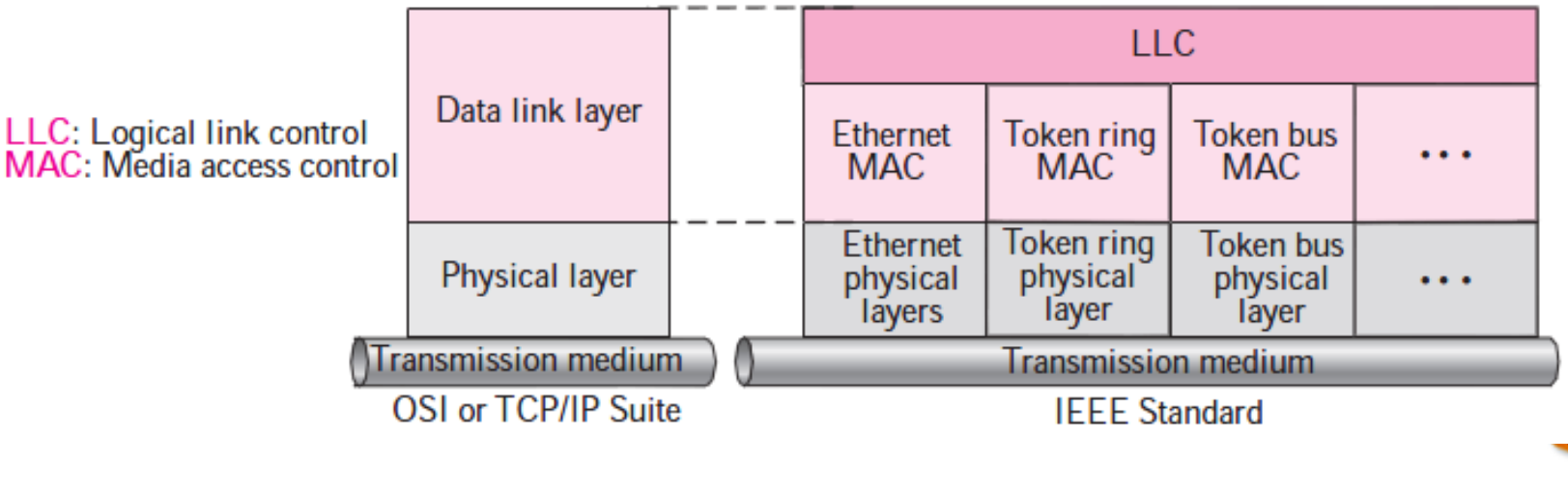
- A computer network that is designed for a limited geographic area such as a building or a campus.
- LAN technologies: Ethernet, token ring, token bus, FDDI, and ATM LAN.



IEEE Project 802

IEEE standard for LANs

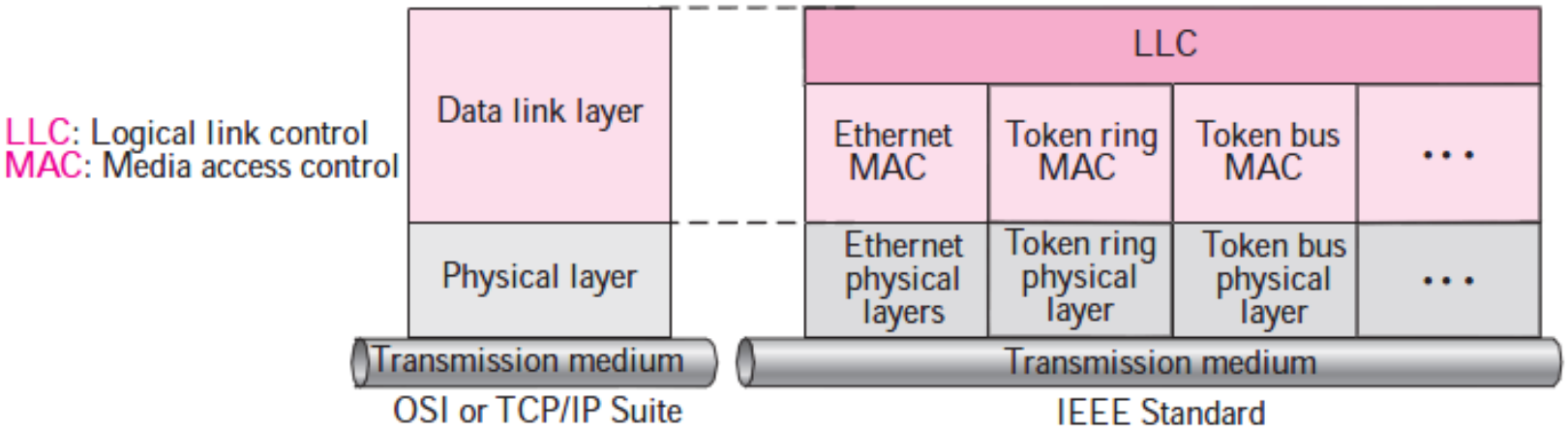
- specify functions of the physical and data link layer of major LAN protocols.



IEEE Project 802

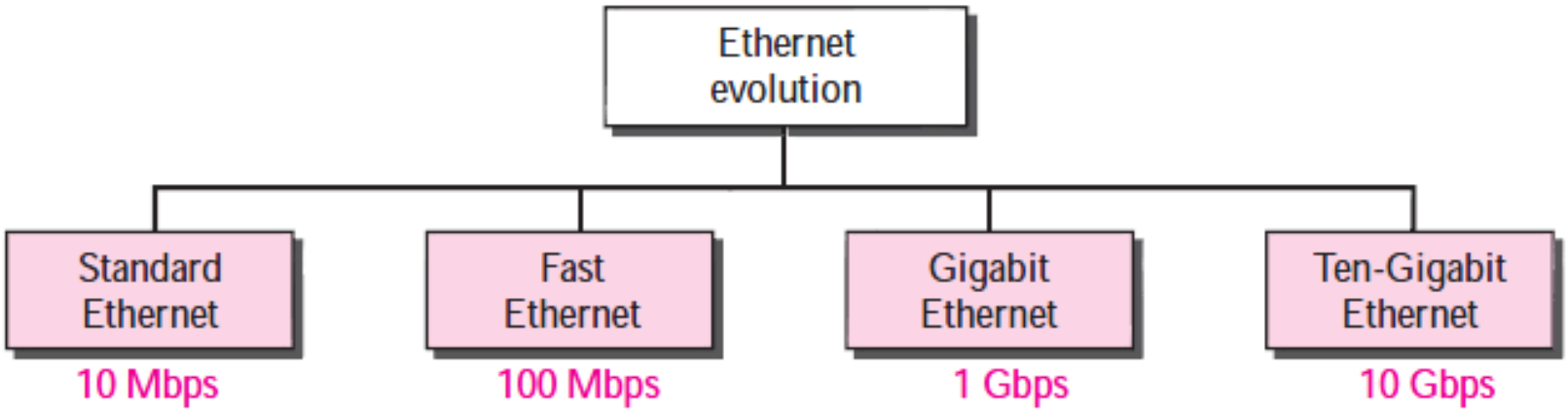
IEEE standard for LANs

- specify functions of the physical and data link layer of major LAN protocols.
- subdivided the data link layer into two sublayers: logical link control (LLC) and media access control (MAC).



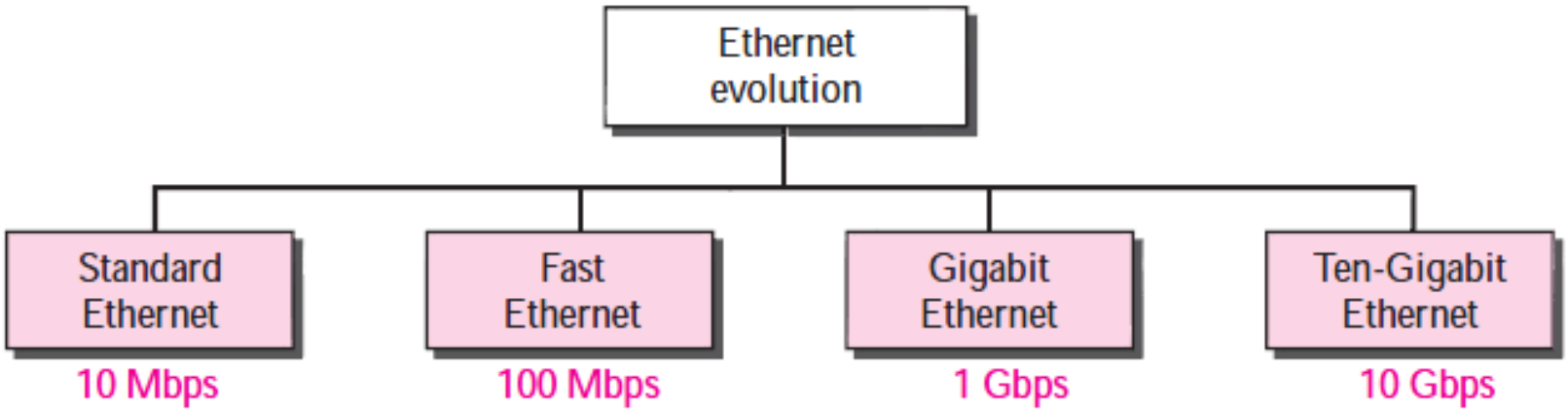
Ethernet

- was created in 1976 at Xerox's Palo Alto Research Center (PARC).



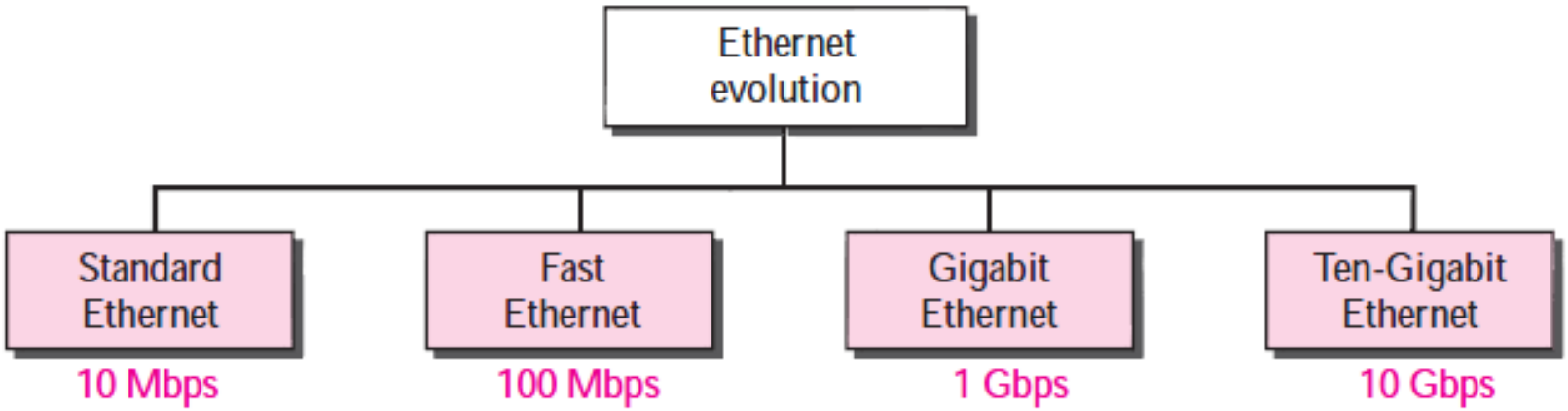
Ethernet

- was created in 1976 at Xerox's Palo Alto Research Center (PARC).
- de facto standard technology that is used for connecting LANs.



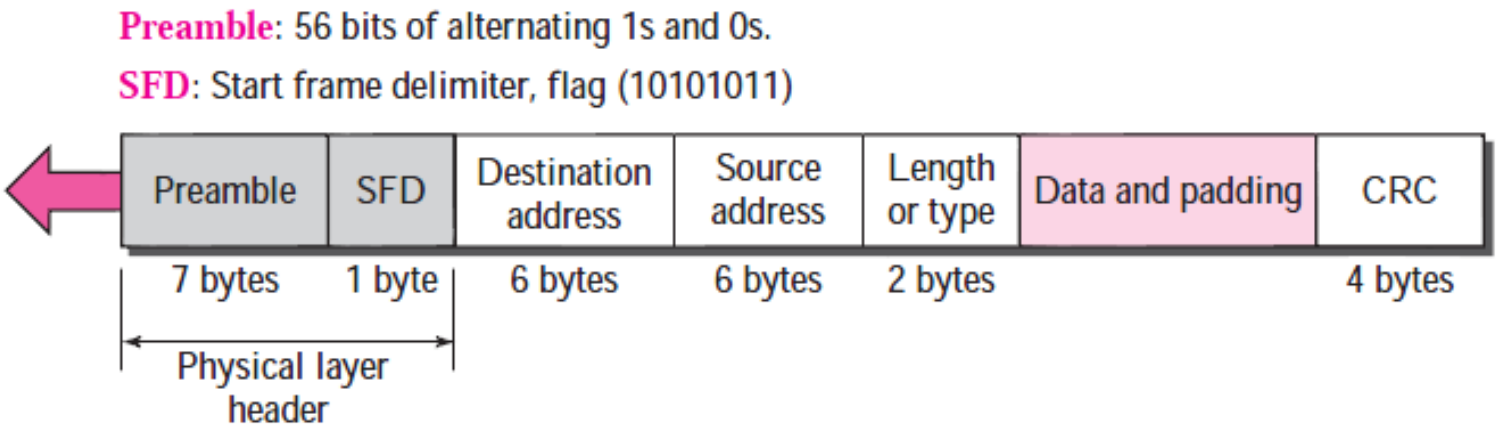
Ethernet

- was created in 1976 at Xerox's Palo Alto Research Center (PARC).
- de facto standard technology that is used for connecting LANs.
- first implemented by a group called DIX (Digital, Intel, and Xerox).



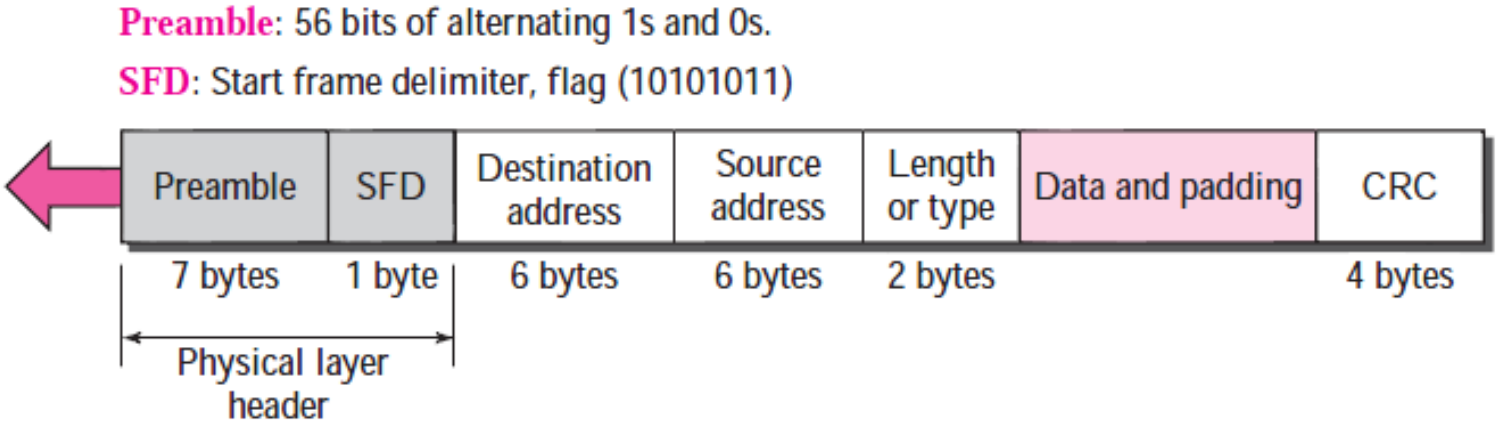
Ethernet (802.3) Frame

- Preamble
  contains 7 bytes (56 bits) of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing.



Ethernet (802.3) Frame

- Start frame delimiter (SFD)
  (1 byte: 10101011) signals the beginning of the frame; the last 2 bits are 11 and alert the receiver that the next field is the destination address.

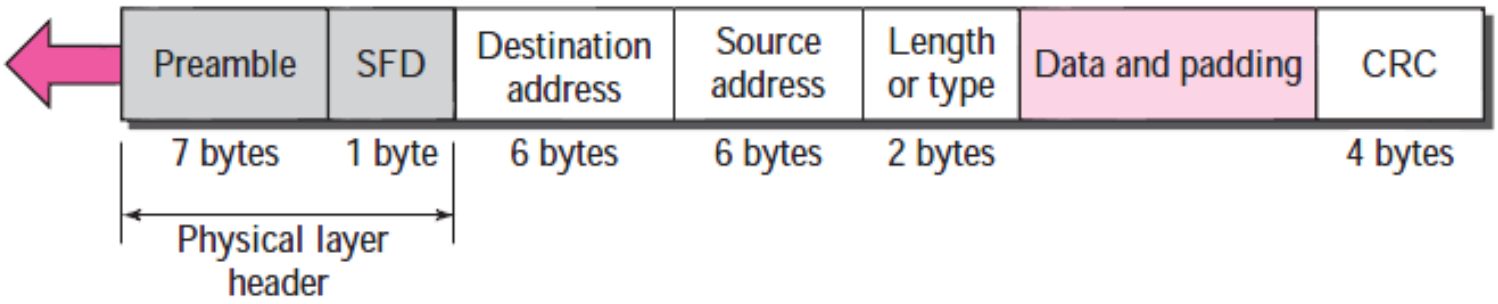


Ethernet (802.3) Frame

- Destination address (DA)
  is 6 bytes and contains the physical address of the destination station/s to receive the packet.

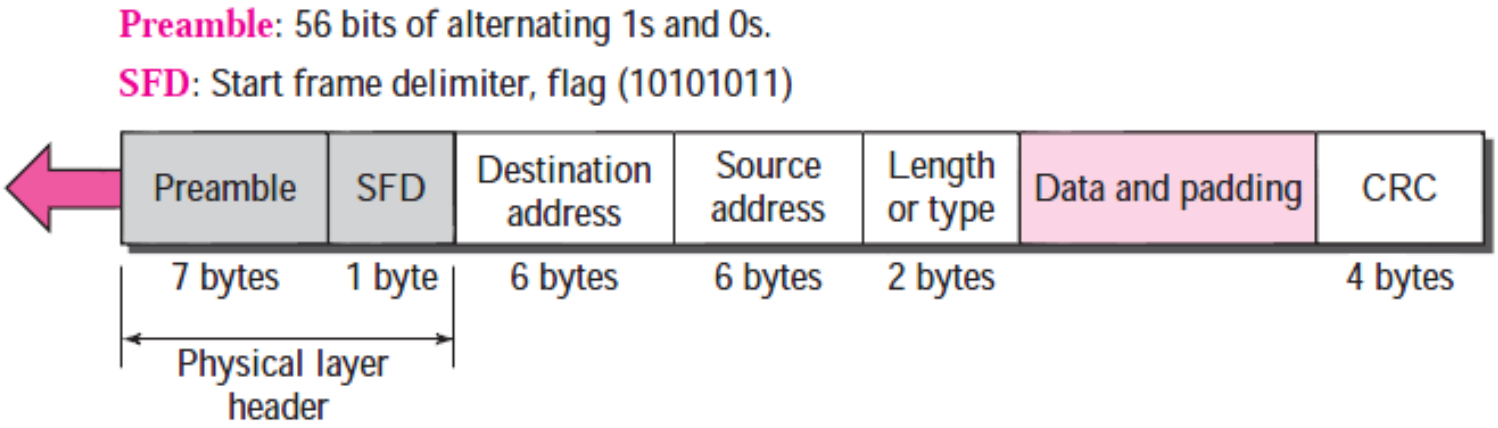
Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)



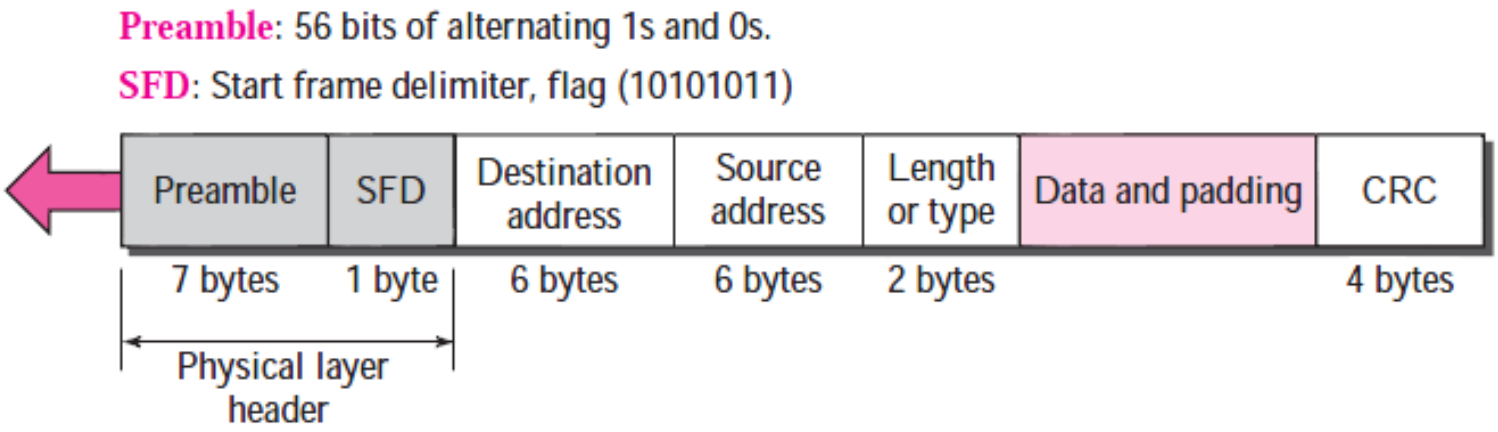
Ethernet (802.3) Frame

- Destination address (DA)
  is 6 bytes and contains the physical address of the destination station/s to receive the packet.
- Source address (SA)
  is 6 bytes and contains the physical address of the sender of the packet.



Ethernet (802.3) Frame

- Length or Type
  - 802.3: length field to define the number of bytes in the data field or
  - Ethernet: type field to define the upper-layer protocol using the MAC frame.

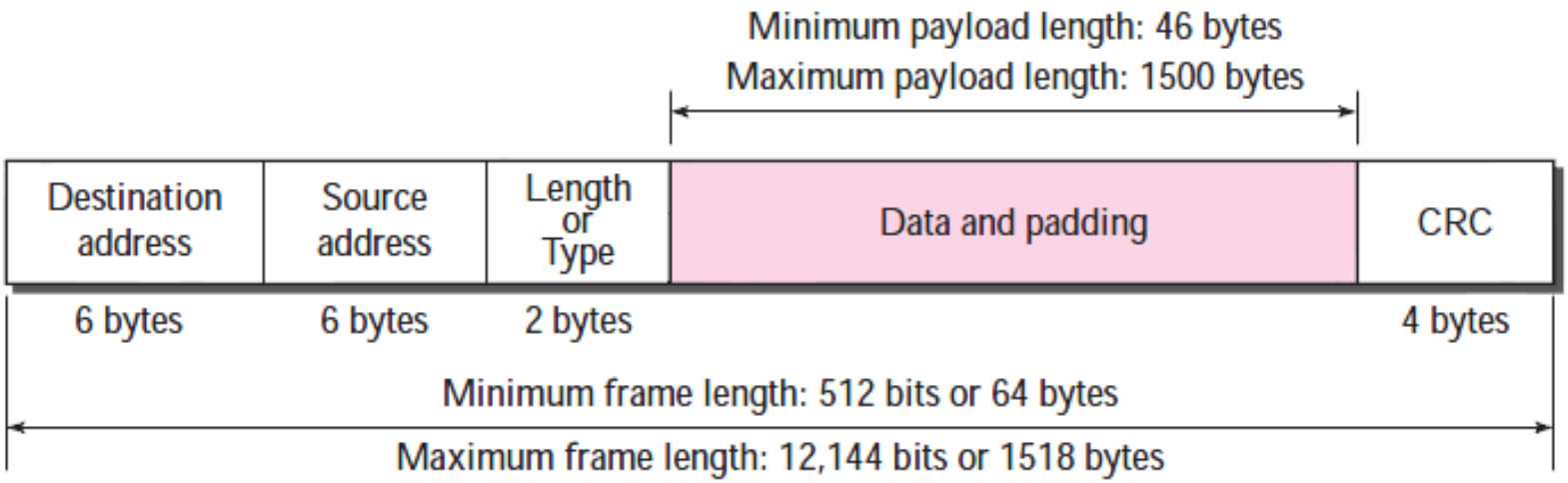


Ethernet (802.3) Frame

- Data
  - carries data encapsulated from the upper-layer protocols;
  - a minimum of 46 and a maximum of 1500 bytes.

Ethernet (802.3) Frame

- Data
  - carries data encapsulated from the upper-layer protocols;
  - a minimum of 46 and a maximum of 1500 bytes.



☞ Understand

What if the upper-layer packet is less than the minimum 46 bytes?

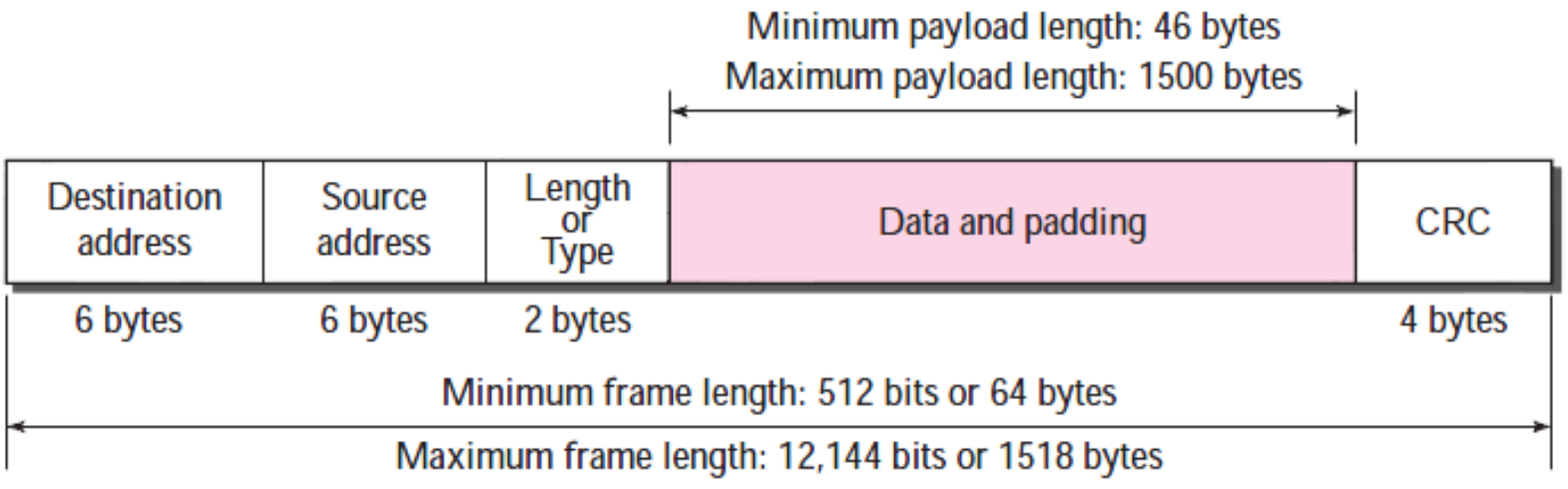
☞ Understand

What if the upper-layer packet is less than the minimum 46 bytes?

- Padding is added to make up the difference.

Ethernet (802.3) Frame

- Cyclic Redundancy Check (CRC) verifies that the data that left the source computer did not change at all during the transmission.



☞ Understand

The 802.3 standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. Give the historical reasons for this restriction.

☞ Understand

The 802.3 standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. Give the historical reasons for this restriction.

- Memory was very expensive when Ethernet was designed: a maximum length restriction helped to reduce the size of the buffer.

☞ Understand

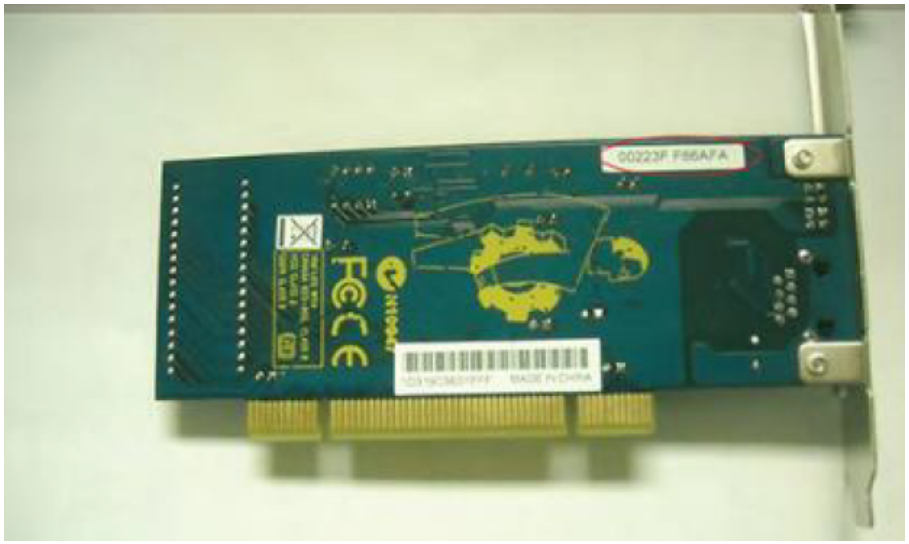
The 802.3 standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. Give the historical reasons for this restriction.

- Memory was very expensive when Ethernet was designed: a maximum length restriction helped to reduce the size of the buffer.
- It prevents one station from monopolizing the shared medium, blocking other stations that have
data to send.

MAC Address

also referred to as the data link address or physical address

- a 6 bytes (48 bits) physical address applied to the network interface card (NIC) by the manufacturer during production.



MAC Address

- normally written in hexadecimal notation, with a colon between the bytes.

d: Hexadecimal digit

$$d_1d_2 : d_3d_4 : d_5d_6 : d_7d_8 : d_9d_{10} : d_{11}d_{12}$$

6 bytes = 12 hexadecimal digits = 48 bits

MAC Address

- normally written in hexadecimal notation, with a colon between the bytes.

d: Hexadecimal digit

$$d_1d_2 : d_3d_4 : d_5d_6 : d_7d_8 : d_9d_{10} : d_{11}d_{12}$$

6 bytes = 12 hexadecimal digits = 48 bits

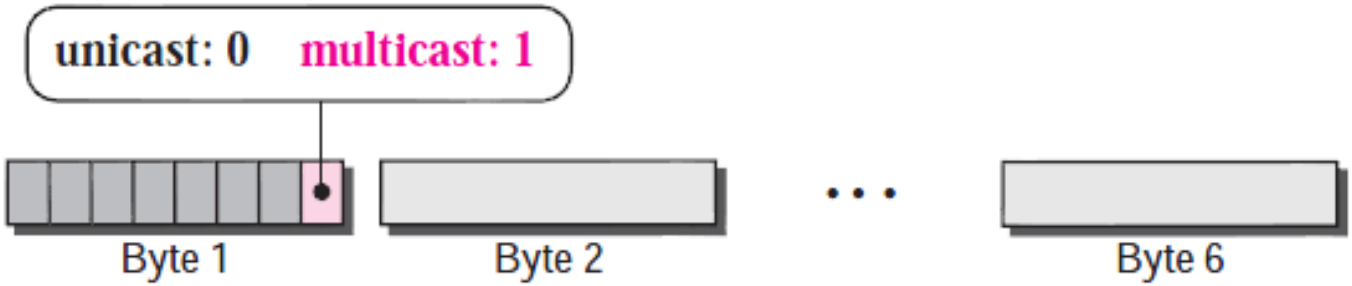
- Ex. Ethernet MAC address

  4A: 30 : 10 : 21 : 10 : 1A

```
Physical Address. . . . . . . . . : EC-A8-6B-D3-D2-63
```

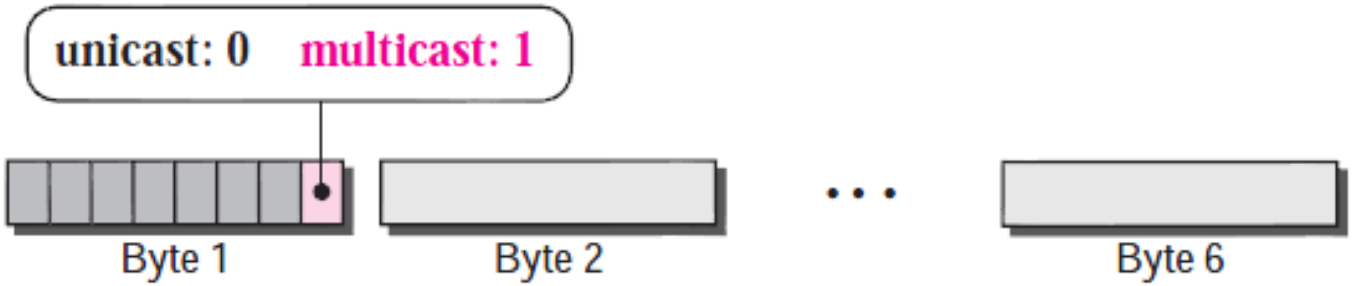
Source and Destination Addressing Modes

- Source address is always a unicast address - the frame comes from only one station.



Source and Destination Addressing Modes

- Source address is always a unicast address - the frame comes from only one station.
- Destination address can be unicast, multicast, or broadcast.



Exercise

Define the type of the following destination addresses:

☞ Exercise

Define the type of the following destination addresses:

- $4A:30:10:21:10:1A$

☞ Exercise

Define the type of the following destination addresses:

- $4A:30:10:21:10:1A$
- $47:20:1B:2E:08:EE$

☞ Exercise

Define the type of the following destination addresses:

- $4A:30:10:21:10:1A$
- $47:20:1B:2E:08:EE$
- $FF:FF:FF:FF:FF:FF$

☞ Exercise

Define the type of the following destination addresses:

- $4A:30:10:21:10:1A$
- $47:20:1B:2E:08:EE$
- $FF:FF:FF:FF:FF:FF$

Solution: Refer to the second hexadecimal digit from the left:

even ==> unicast;

odd ==> multicast;
all F's ==> Broadcast

Transmission of Addresses

- transmission is left-to-right, byte by byte; however, for each byte, the least significant bit is sent first and the most significant bit is sent last.

Transmission of Addresses

- transmission is left-to-right, byte by byte; however, for each byte, the least significant bit is sent first and the most significant bit is sent last.
- Ex. Show how the address $47:20:1B:2E:08:EE$ is sent out on line.

Transmission of Addresses

- transmission is left-to-right, byte by byte; however, for each byte, the least significant bit is sent first and the most significant bit is sent last.
- Ex. Show how the address $47:20:1B:2E:08:EE$ is sent out on line.

$\leftarrow$ 11100010 00000100 11011000 01110100 00010000 01110111

CSMA/CD

Carrier Sense Multiple Access with Collision Detection

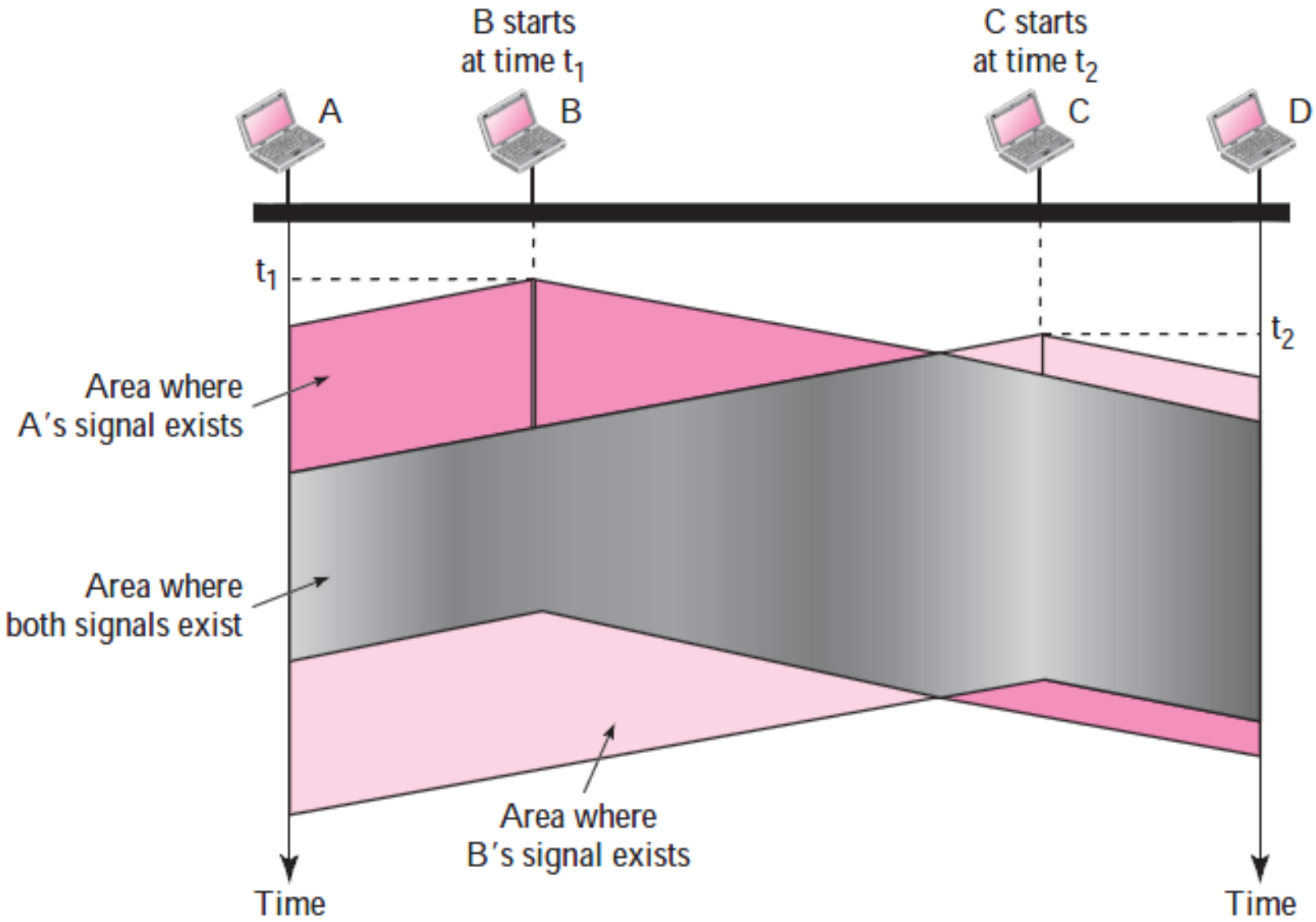
- access method for traditional Ethernet (10-Mbps) that senses the medium before trying to use it.

CSMA/CD

Carrier Sense Multiple Access with Collision Detection

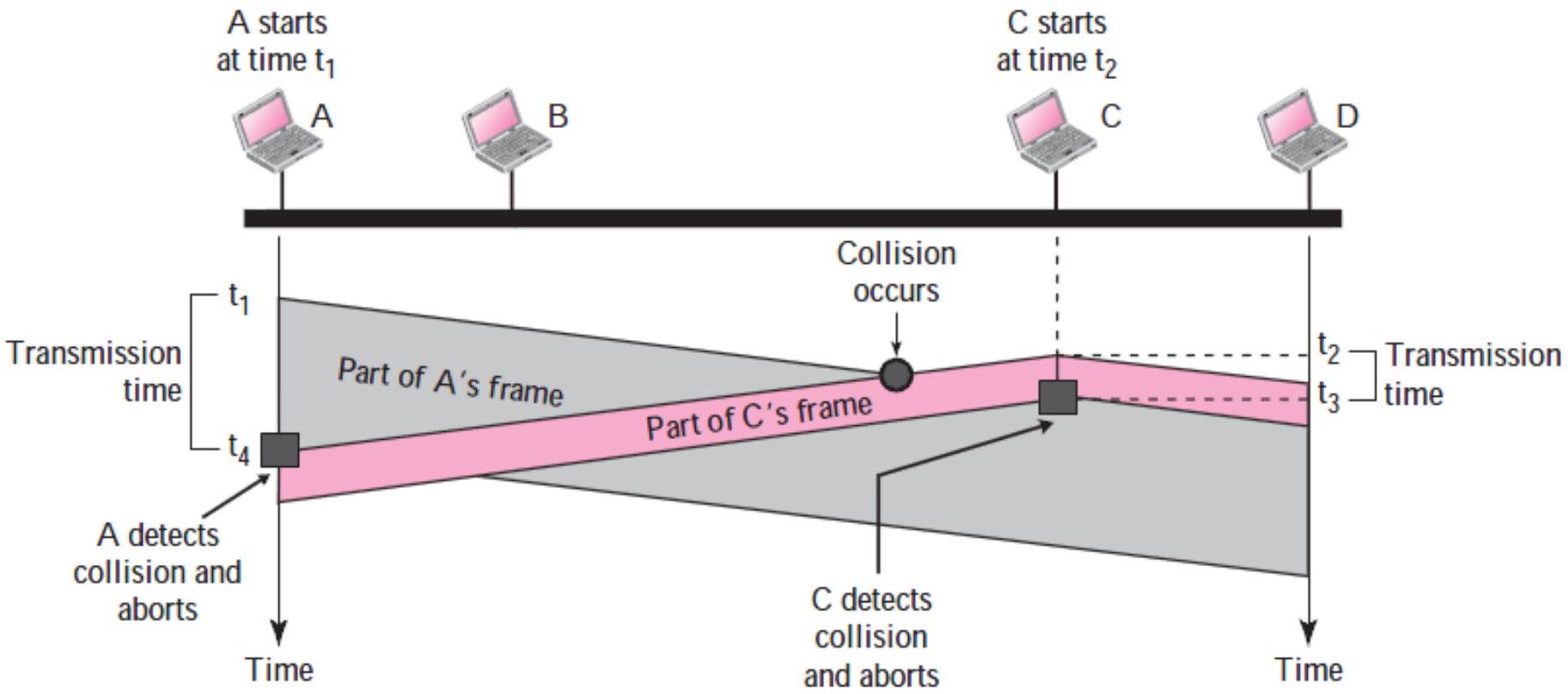
- access method for traditional Ethernet (10-Mbps) that senses the medium before trying to use it.
- Ethernet stations can be connected together using a physical bus or star topology but its logical topology is always a bus.

CSMA Collision



CSMA/CD

Carrier Sense Multiple Access with Collision Detection Algorithm



CSMA/CD

Minimum Frame Size

- a restriction on the frame size is required.

CSMA/CD

Minimum Frame Size

- a restriction on the frame size is required.
- before sending the last bit of the frame, the sending station must detect a collision and abort.

CSMA/CD

Minimum Frame Size

- a restriction on the frame size is required.
- before sending the last bit of the frame, the sending station must detect a collision and abort.
- thus, transmission time T_{fr} must be at least two times the maximum propagation time T_p.

☞ Exercise

In the standard Ethernet, if the maximum propagation time is $25.6\mu s$, what is the minimum size of the frame?

☞ Exercise

In the standard Ethernet, if the maximum propagation time is $25.6\mu s$, what is the minimum size of the frame?

$$T_{fr} = 2 \times T_p = 51.2\mu s$$

☞ Exercise

In the standard Ethernet, if the maximum propagation time is $25.6\mu s$, what is the minimum size of the frame?

$$T_{fr} = 2 \times T_p = 51.2\mu s$$

$$10 \text{ Mbps} \times 51.2\mu s = 512 \text{ bits or } 64 \text{ bytes}$$

☞ Exercise

In the standard Ethernet, if the maximum propagation time is $25.6\mu s$, what is the minimum size of the frame?

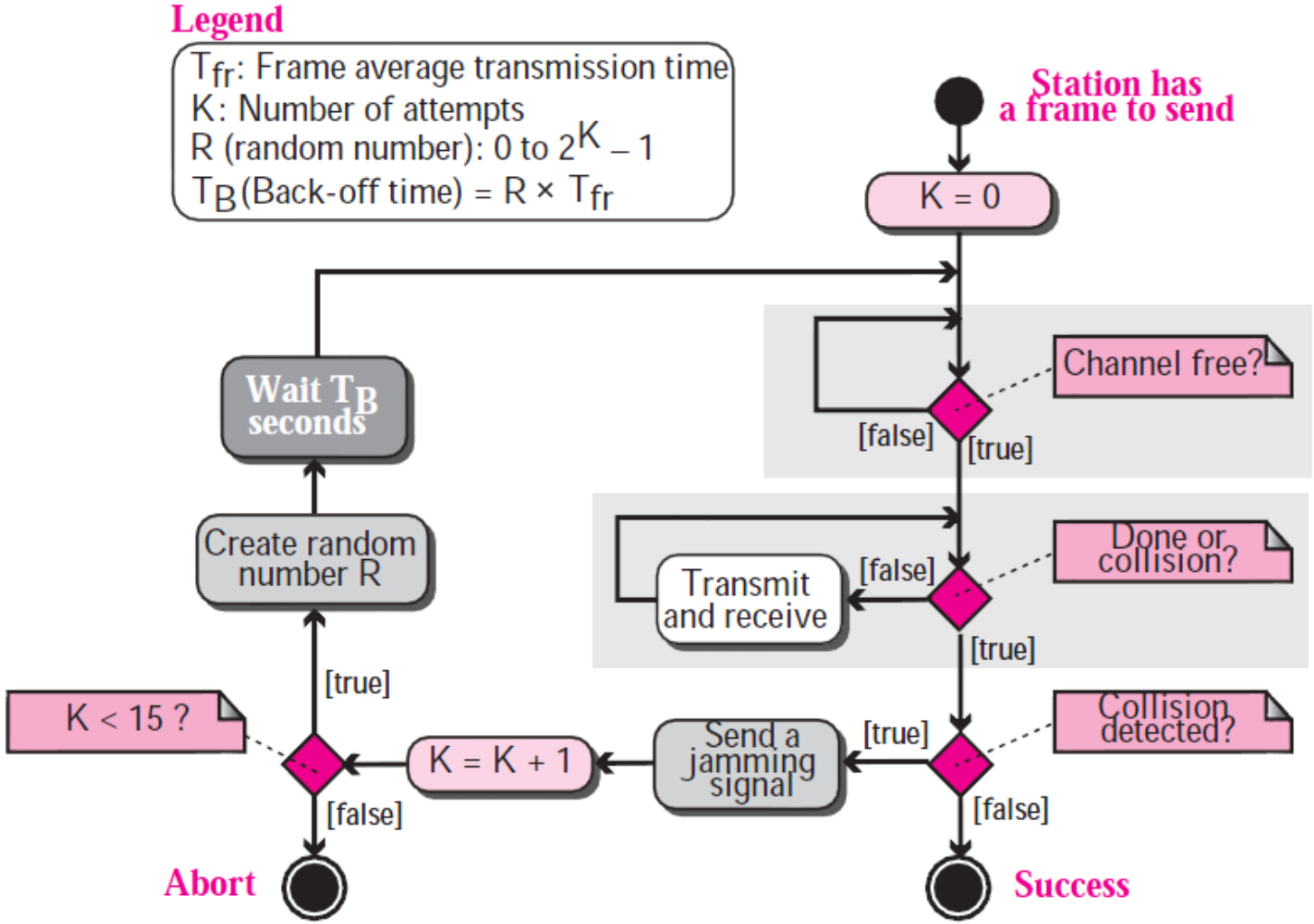
$$T_{fr} = 2 \times T_p = 51.2\mu s$$

10 Mbps $\times 51.2\mu s = 512$ bits or 64 bytes

- This is the minimum size of the frame for Standard Ethernet.

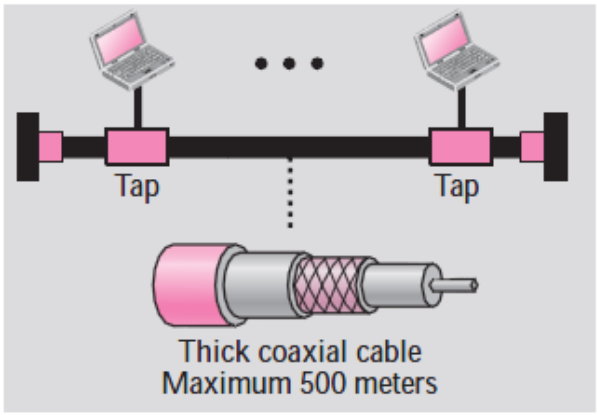
CSMA/CD

Flow Diagram

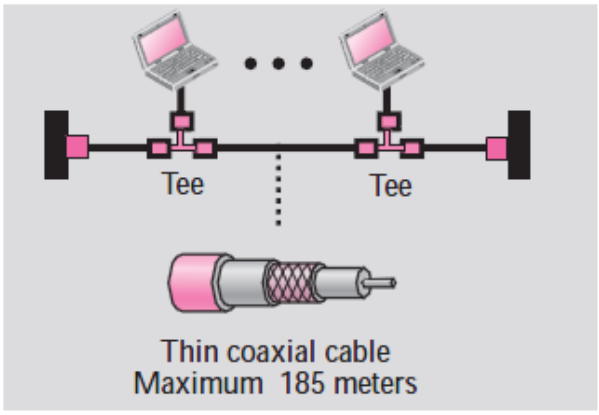


Standard Ethernet

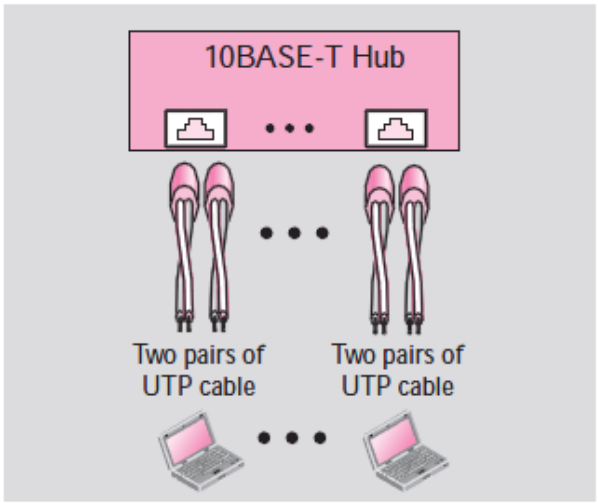
Implementation



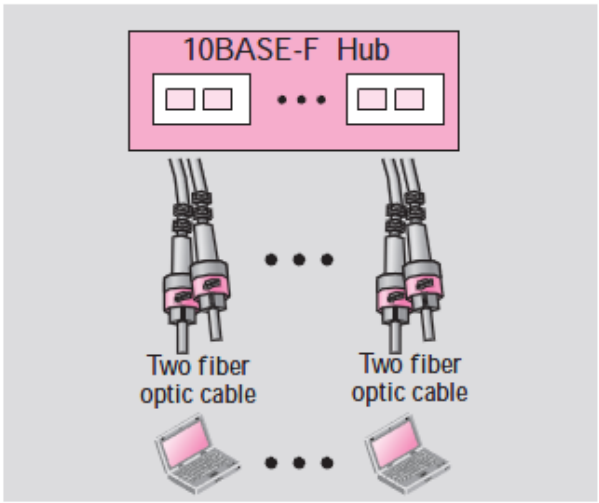
a. 10BASE5



b. 10BASE2



c. 10BASE-T

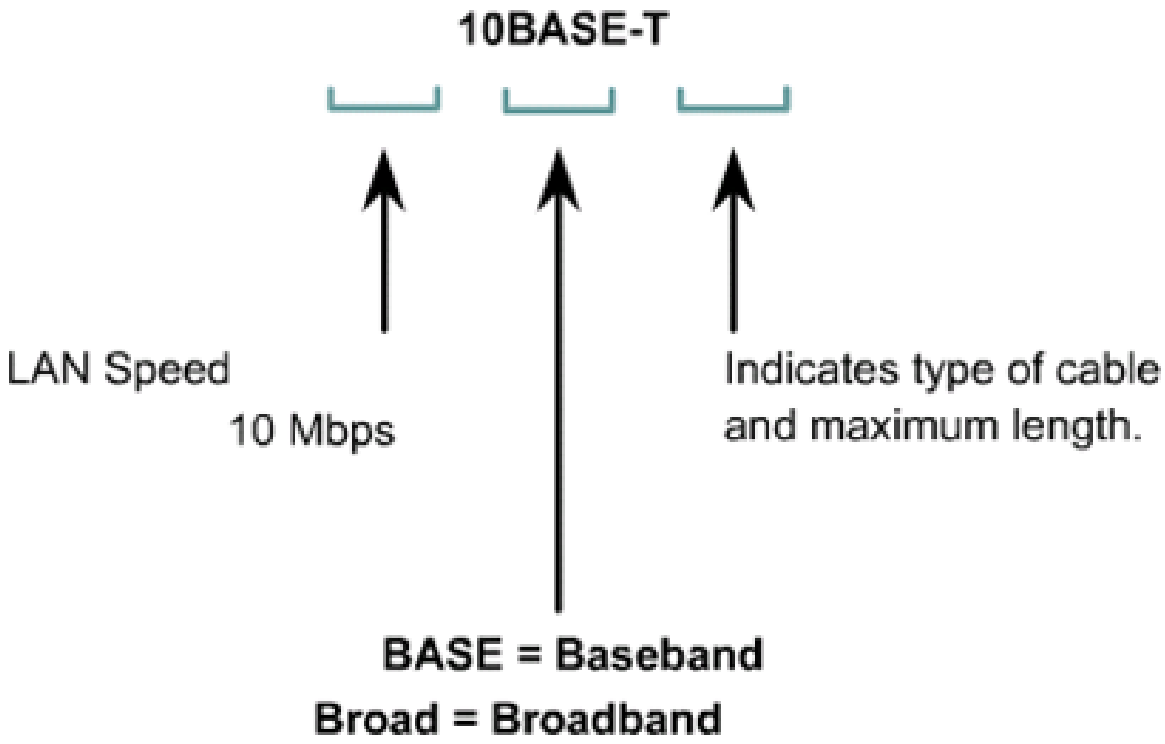


d. 10BASE-F

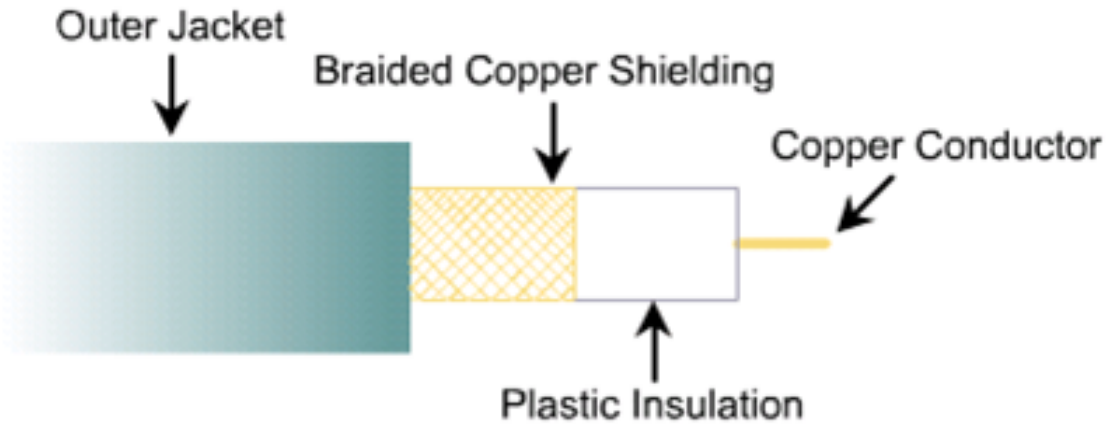
Reading Assignment

- Report about the IEEE 802.3 Standard, in your own words.
- Submit through www.turnitin.com.

Cable Specifications

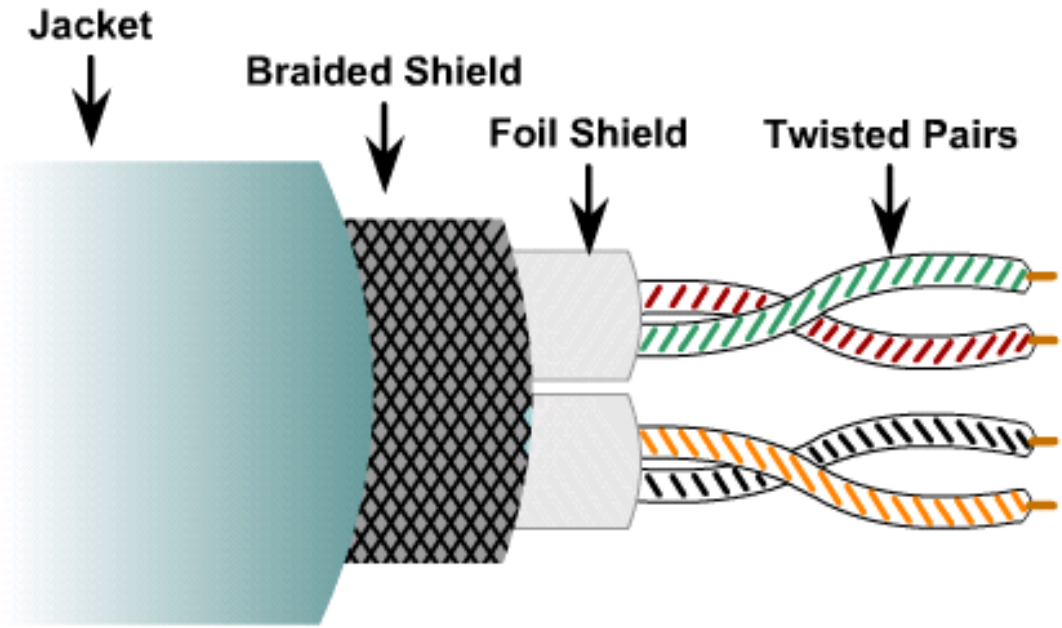


Coaxial Cable



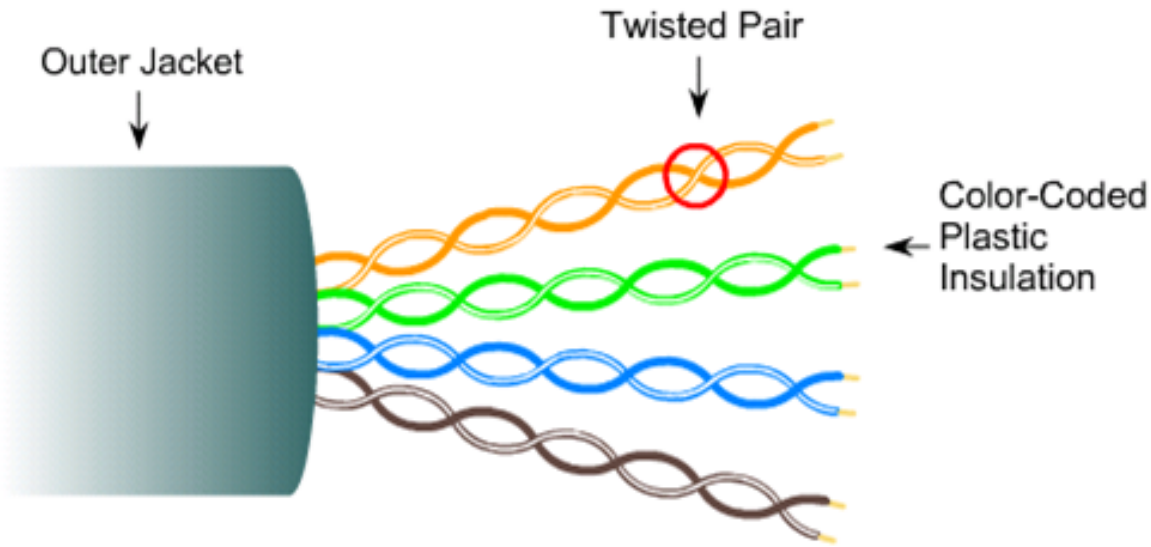
- Speed and throughput: 10 - 100 Mbps
- Cost: Inexpensive
- Media and connector size: Medium
- Maximum cable length: 500m

Shielded Twisted Pair (STP)



- Speed and throughput: 0 - 100 Mbps
- Cost: Moderate
- Media and connector size: Medium to Large
- Maximum cable length: 100m

Unshielded Twisted Pair (UTP)



Speed and throughput: 10 - 100 - 1000 Mbps (depending on the quality/category of cable)
Cost: Least Expensive
Media and connector size: Small
Maximum cable length: 100m

☞ Readings

It is the standards body that creates the Physical layer specifications for Ethernet.

☞ Readings

It is the standards body that creates the Physical layer specifications for Ethernet.

- EIA/TIA (Electronic Industries Association and the newer Telecommunications Industry Association)

☞ Readings

It is the standards body that creates the Physical layer specifications for Ethernet.

- EIA/TIA (Electronic Industries Association and the newer Telecommunications Industry Association)
- EIA/TIA specifies that Ethernet use a registered jack (RJ) connector with a 4 5 wiring sequence on unshielded twisted-pair (UTP) cabling (RJ-45).

UTP Connections (RJ-45)

- RJ-45 connector is clear so you can see the eight colored wires that connect to the connector's pins. These wires are twisted into four pairs.

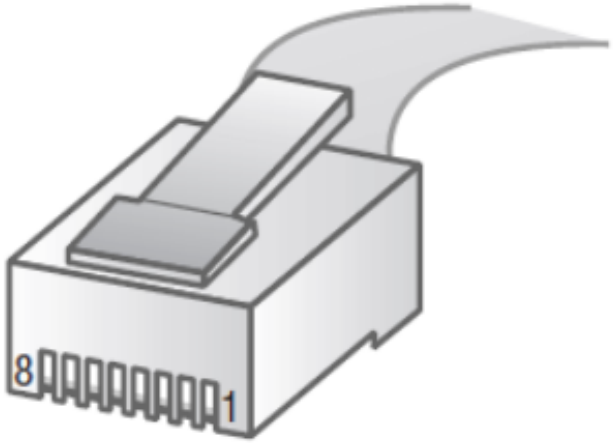
UTP Connections (RJ-45)

- RJ-45 connector is clear so you can see the eight colored wires that connect to the connector's pins. These wires are twisted into four pairs.
- Four wires (two pairs) carry the voltage and are considered tip. The other four wires are grounded and are called ring.

UTP Connections (RJ-45)

8-pin modular connector

Pin	Wire Pair (T Is Tip; R Is Ring)
1	Pair 2 T2
2	Pair 2 R2
3	Pair 3 T3
4	Pair 1 R1
5	Pair 1 T1
6	Pair 3 R3
7	Pair 4 T4
8	Pair 4 R4

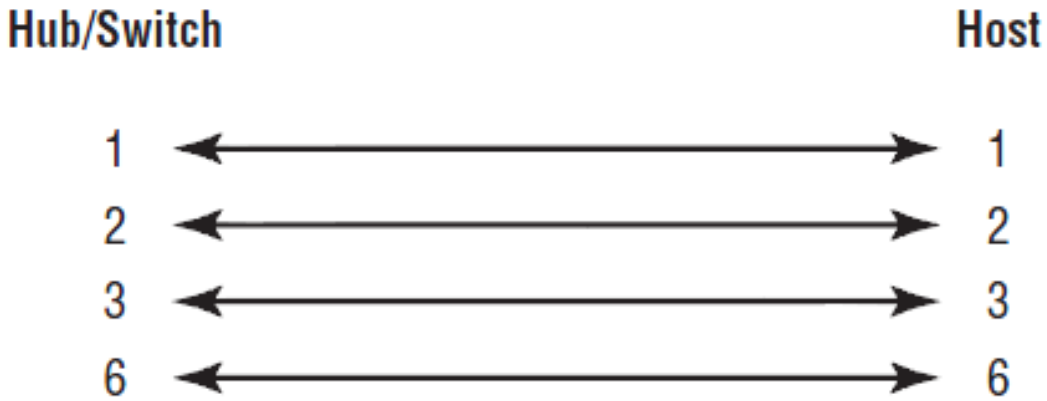


RJ-45 connector

Ethernet Cabling

Straight-through cable: used to connect

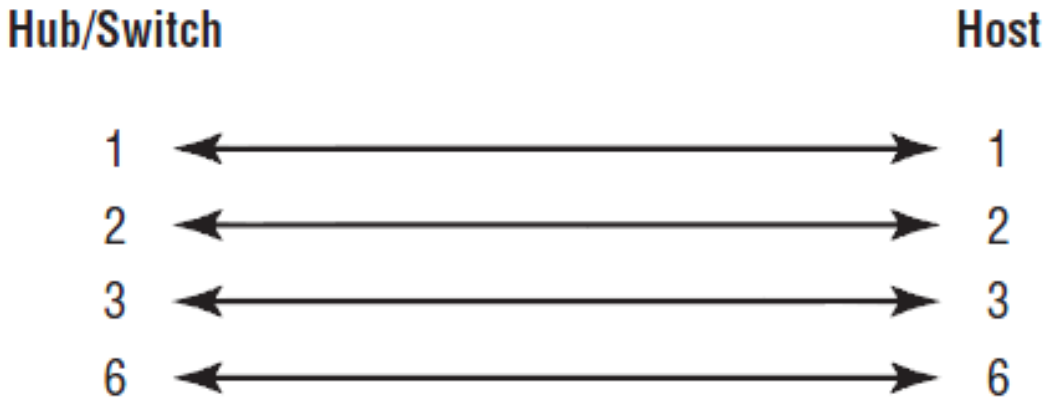
- Host to switch or hub.



Ethernet Cabling

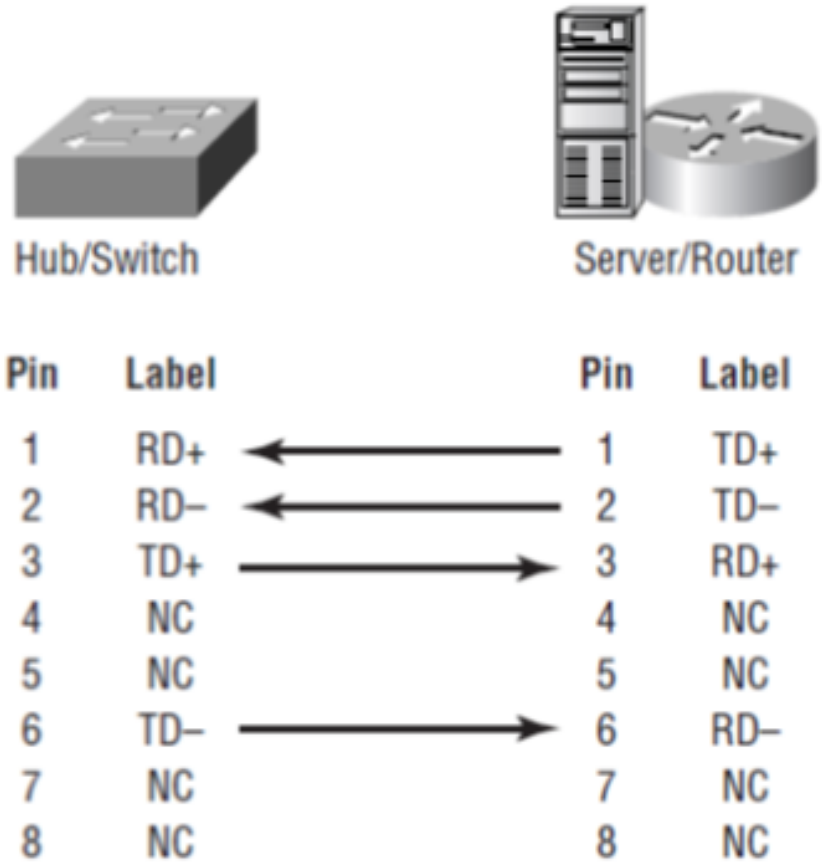
Straight-through cable: used to connect

- Host to switch or hub.
- Router to switch or hub



Ethernet Cabling

Straight-through cable: wires on both cable ends are in the same order.



Ethernet Cabling

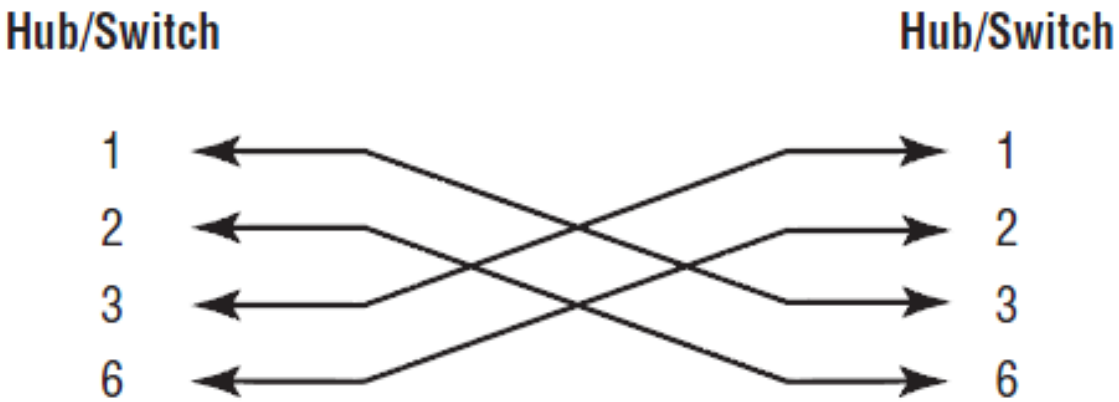
Crossover Cable: used to connect

- Switch to switch

Ethernet Cabling

Crossover Cable: used to connect

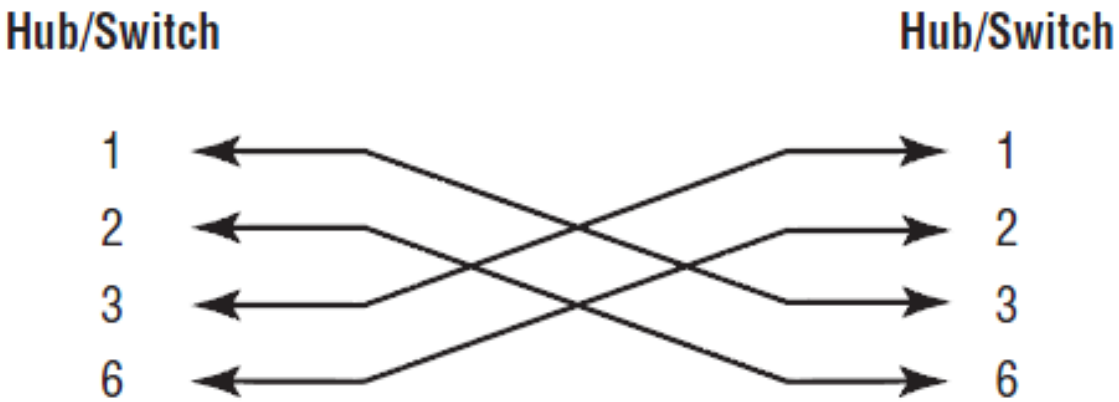
- Switch to switch
- Hub to hub



Ethernet Cabling

Crossover Cable: used to connect

- Switch to switch
- Hub to hub
- Host to host



Ethernet Cabling

Crossover Cable: used to connect

- Switch to switch
- Hub to hub
- Host to host
- Hub to switch

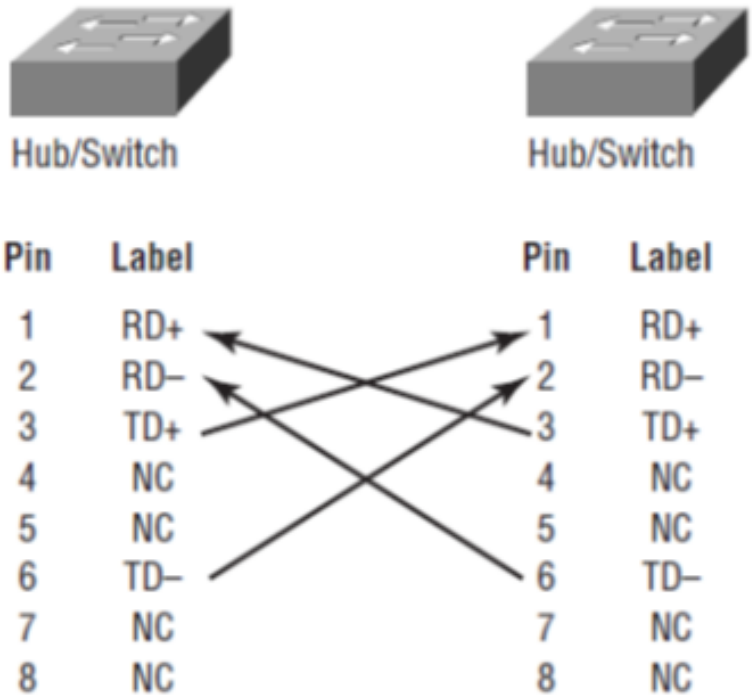
Ethernet Cabling

Crossover Cable: used to connect

- Switch to switch
- Hub to hub
- Host to host
- Hub to switch
- Router direct to host

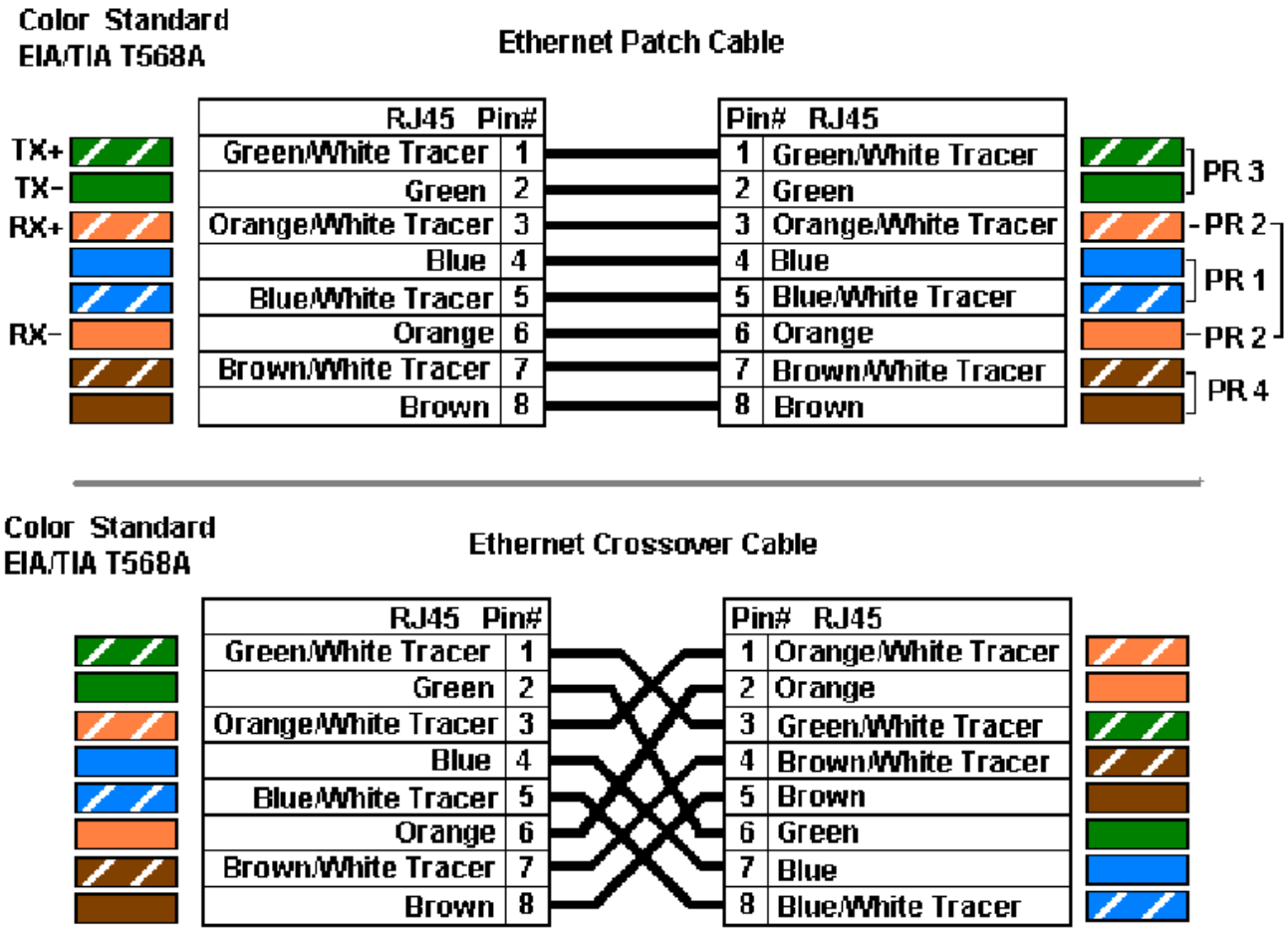
Ethernet Cabling

Crossover Cable: wires on each end of the cable are crossed - Transmit to Receive and Receive to Transmit on each side, for both tip and ring.



Ethernet Cabling

Summary



Fast Ethernet (802.3u)

- designed to compete with LAN protocols such as FDDI or Fiber Channel.

Fast Ethernet (802.3u)

- designed to compete with LAN protocols such as FDDI or Fiber Channel.
- upgrade the data rate to 100 Mbps.

Fast Ethernet (802.3u)

- designed to compete with LAN protocols such as FDDI or Fiber Channel.
- upgrade the data rate to 100 Mbps.
- backward-compatible with Standard Ethernet.

Fast Ethernet (802.3u)

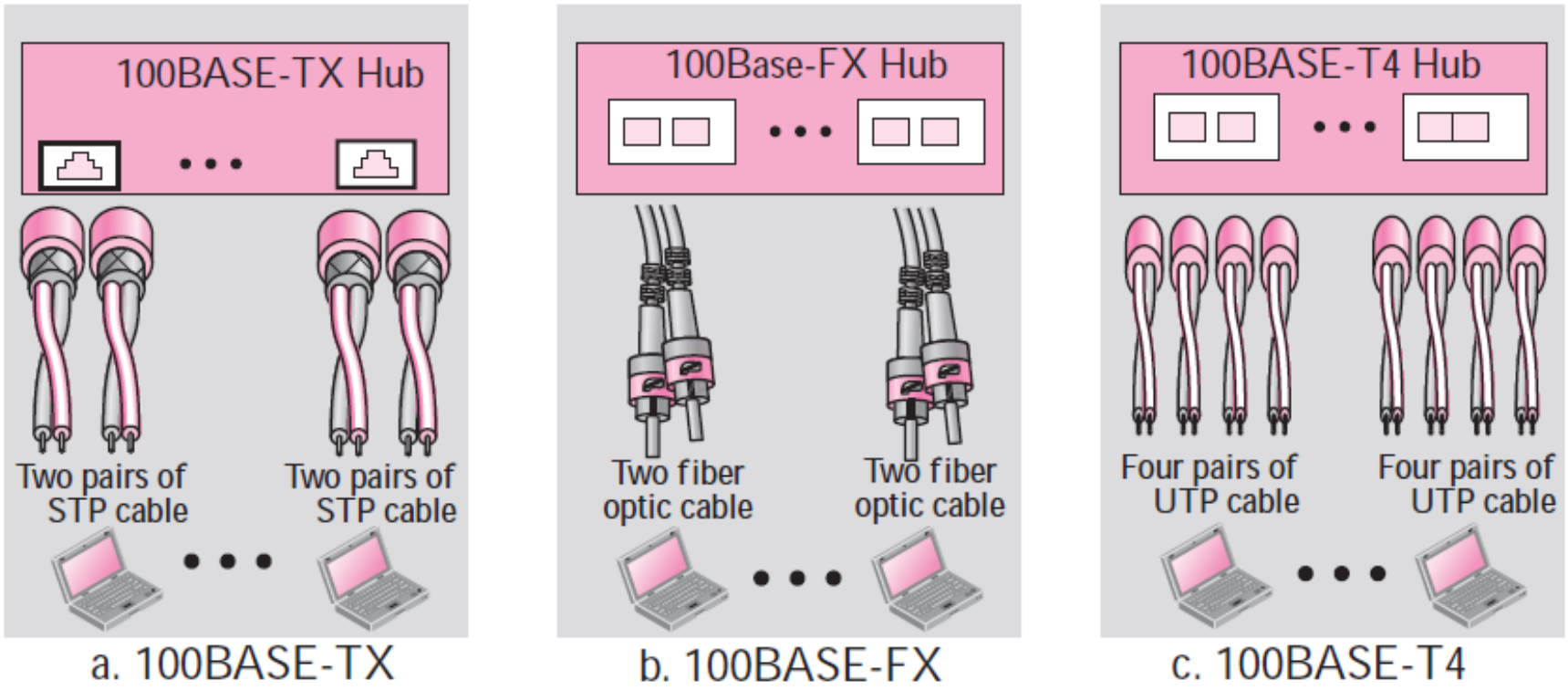
- designed to compete with LAN protocols such as FDDI or Fiber Channel.
- upgrade the data rate to 100 Mbps.
- backward-compatible with Standard Ethernet.
- same frame format and 48-bit address.

Fast Ethernet (802.3u)

- designed to compete with LAN protocols such as FDDI or Fiber Channel.
- upgrade the data rate to 100 Mbps.
- backward-compatible with Standard Ethernet.
- same frame format and 48-bit address.
- same minimum and maximum frame lengths.

Fast Ethernet (802.3u)

Implementation



a. 100BASE-TX b. 100BASE-FX c. 100BASE-T4

Fast Ethernet (802.3u)

- MAC sublayer was kept untouched

Fast Ethernet (802.3u)

- MAC sublayer was kept untouched
- star topology: half duplex and full duplex

Fast Ethernet (802.3u)

- MAC sublayer was kept untouched
- star topology: half duplex and full duplex
- access method is the same (CSMA/CD) for the half-duplex

Fast Ethernet (802.3u)

- MAC sublayer was kept untouched
- star topology: half duplex and full duplex
- access method is the same (CSMA/CD) for the half-duplex
- autonegotiation allows two devices to negotiate the mode or data rate of operation.

Address Resolution Protocol (ARP)

- accepts a logical address from the IP protocol, then, identify and place the source and destination MAC address in the frame

Address Resolution Protocol (ARP)

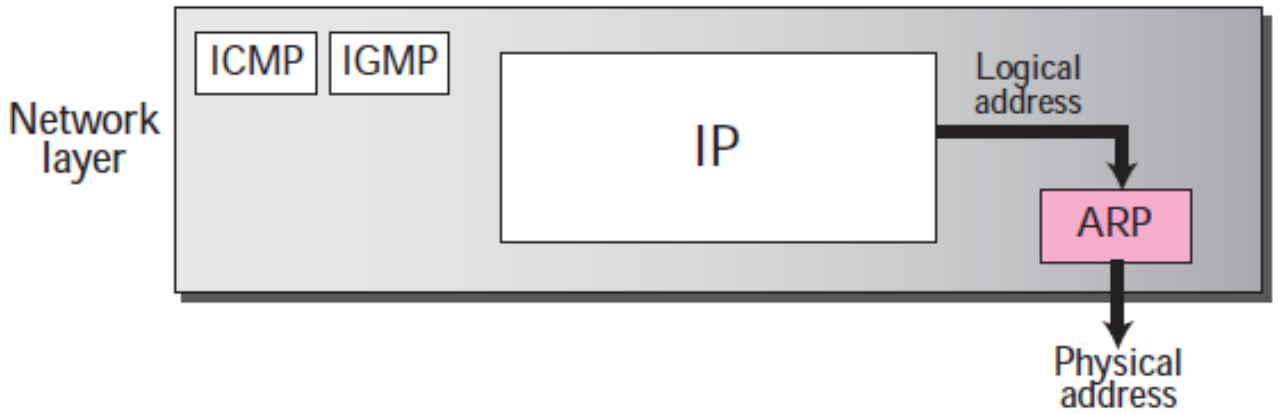
- accepts a logical address from the IP protocol, then, identify and place the source and destination MAC address in the frame
- operates at the Internet layer, but the the MAC address is attached at the Network Access layer.

Address Resolution Protocol (ARP)

- accepts a logical address from the IP protocol, then, identify and place the source and destination MAC address in the frame
- operates at the Internet layer, but the the MAC address is attached at the Network Access layer.
- maps a logical address to its corresponding physical address

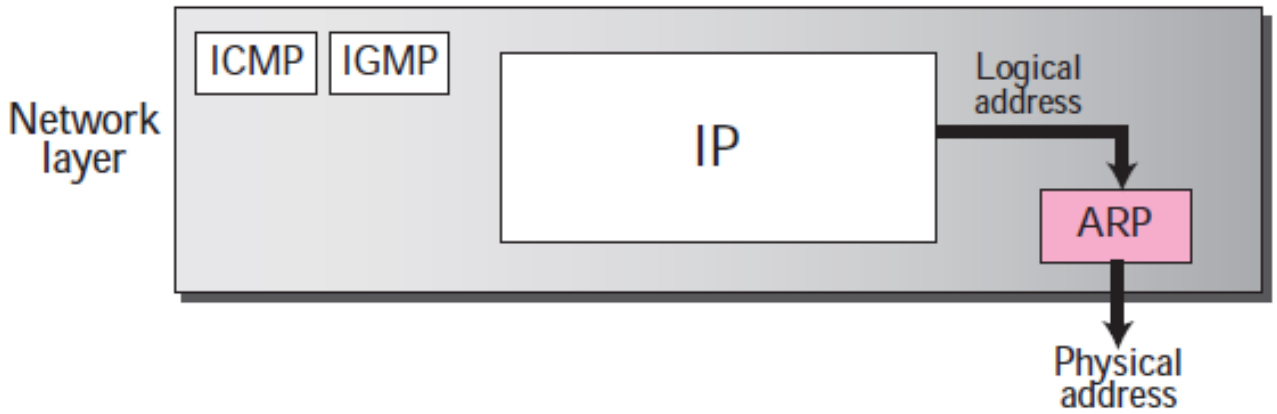
Address Resolution Protocol (ARP)

Position of ARP in TCP/IP protocol suite



Address Resolution Protocol (ARP)

Position of ARP in TCP/IP protocol suite

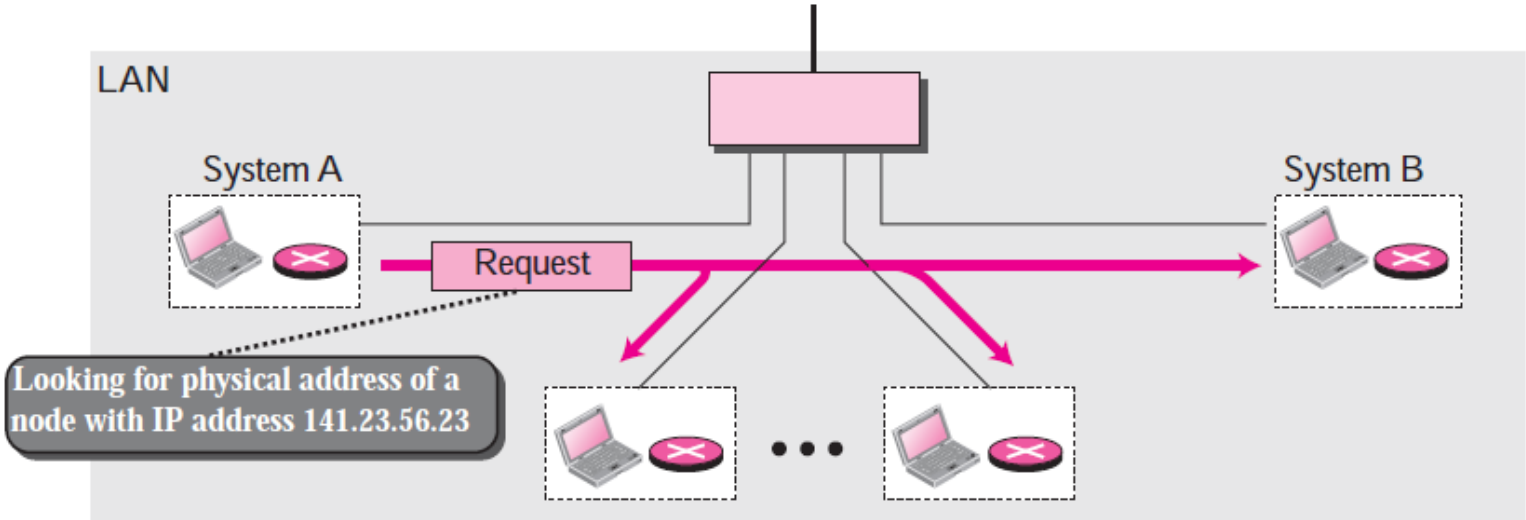


- Why do we need ARP?

ARP Operation

ARP request is broadcast

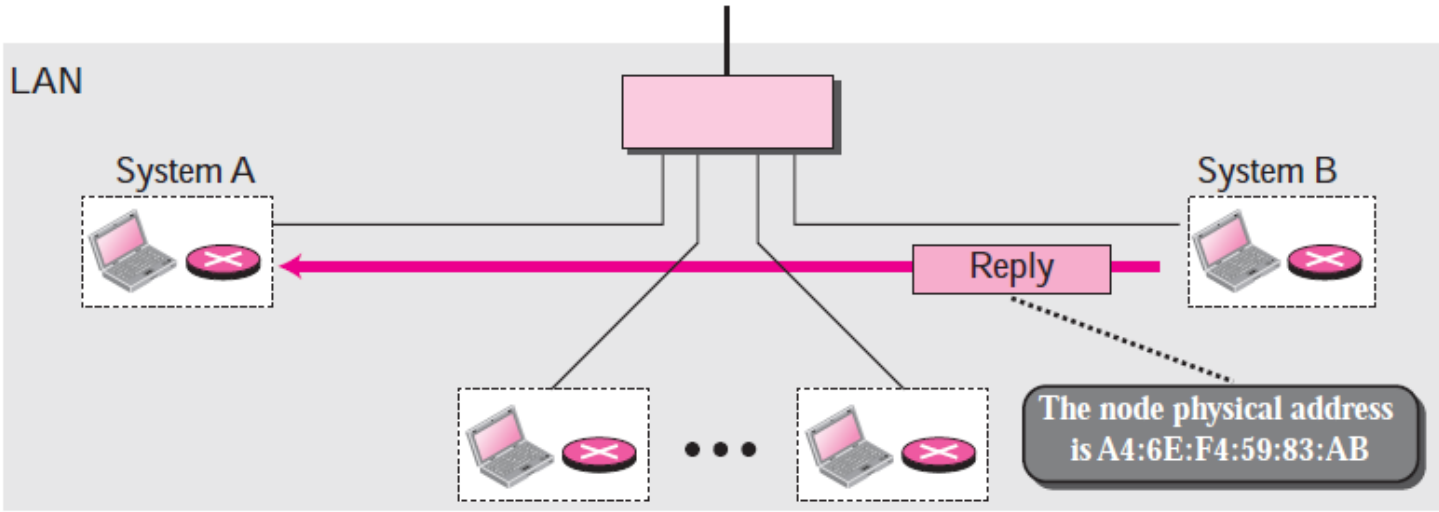
❝ If this is your IP address, send me your MAC address. ❞



ARP Operation

ARP reply is unicast

❝ This is my MAC address. ❞



ARP Packet Format

Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)		
Target protocol address (For example, 4 bytes for IP)		

ARP Packet Format

- Hardware type
  16-bit field defining the type of the network on which ARP is running. Each LAN has been assigned.
    Ex. Ethernet: type 1

ARP Packet Format

- Hardware type
  16-bit field defining the type of the network on which ARP is running. Each LAN has been assigned.
    Ex. Ethernet: type 1
- Protocol type
  16-bit field defining the protocol.
    Ex. IPv4 protocol: 0800_{16}

ARP Packet Format

- Hardware type
  16-bit field defining the type of the network on which ARP is running. Each LAN has been assigned.
    Ex. Ethernet: type 1
- Protocol type
  16-bit field defining the protocol.
    Ex. IPv4 protocol: 0800_{16}
- Hardware length
  8-bit field defining the length of the physical address in bytes.
    Ex. Ethernet: 6 bytes

ARP Packet Format

- Protocol Length
  8-bit field defining the length of the logical address in bytes.
    Ex. IPv4 protocol: 4

ARP Packet Format

- Protocol Length
  8-bit field defining the length of the logical address in bytes.
    Ex. IPv4 protocol: 4
- Operation
  16-bit field defining the type of packet
    Ex. ARP request (1), ARP reply (2).

ARP Packet Format

- Protocol Length
  8-bit field defining the length of the logical address in bytes.
  Ex. IPv4 protocol: 4
- Operation
  16-bit field defining the type of packet
  Ex. ARP request (1), ARP reply (2).
- Sender hardware address
  variable-length field defining the physical address of the sender.
  Ex. Ethernet: 6 bytes

ARP Packet Format

- Sender protocol address
  variable-length field defining the logical address of the sender.
    Ex. IPv4 protocol: 4 bytes

ARP Packet Format

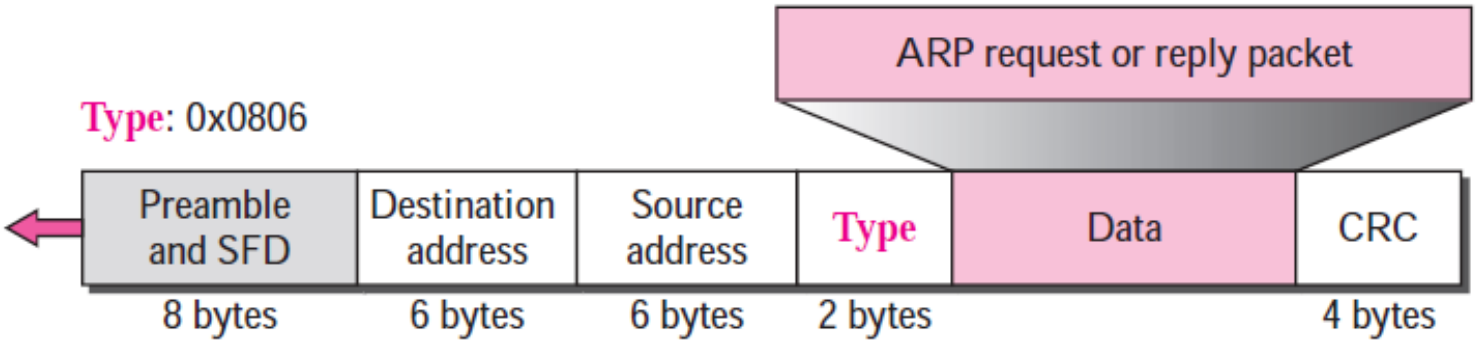
- Sender protocol address
  variable-length field defining the logical address of the sender.
  Ex. IPv4 protocol: 4 bytes
- Target hardware address
  variable-length field defining the physical address of the target.
  Ex. Ethernet: 6 bytes

ARP Packet Format

- Sender protocol address
  variable-length field defining the logical address of the sender.
  Ex. IPv4 protocol: 4 bytes
- Target hardware address
  variable-length field defining the physical address of the target.
  Ex. Ethernet: 6 bytes
- Target protocol address
  variable-length field defining the logical address of the target.
  Ex. IPv4 protocol: 4*bytes*

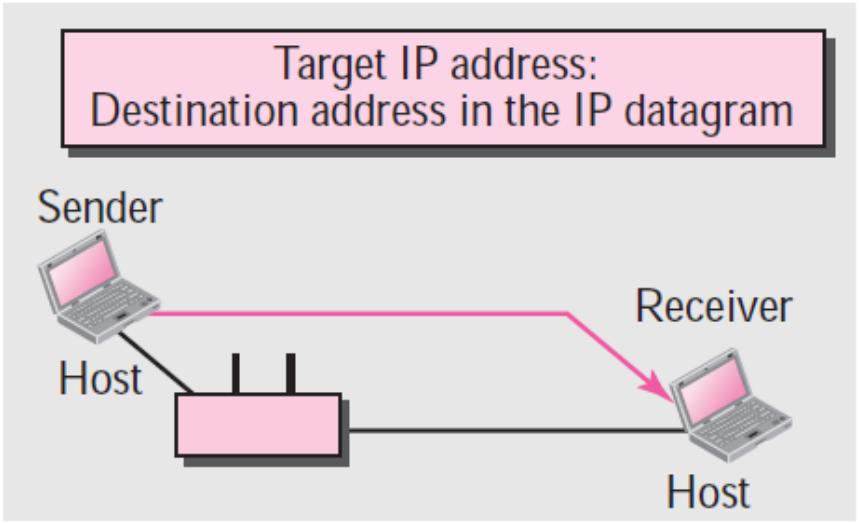
Encapsulation of ARP packet

An ARP packet is encapsulated directly into a data link frame.

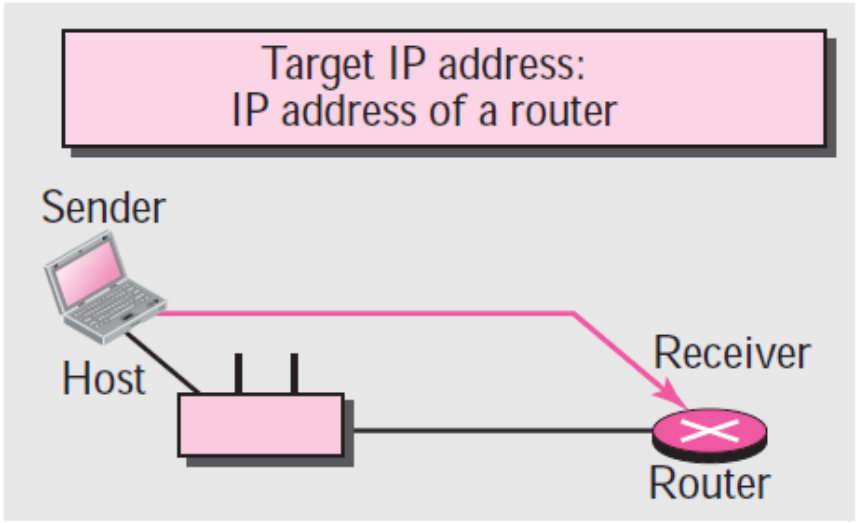


ARP Usage Scenarios

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

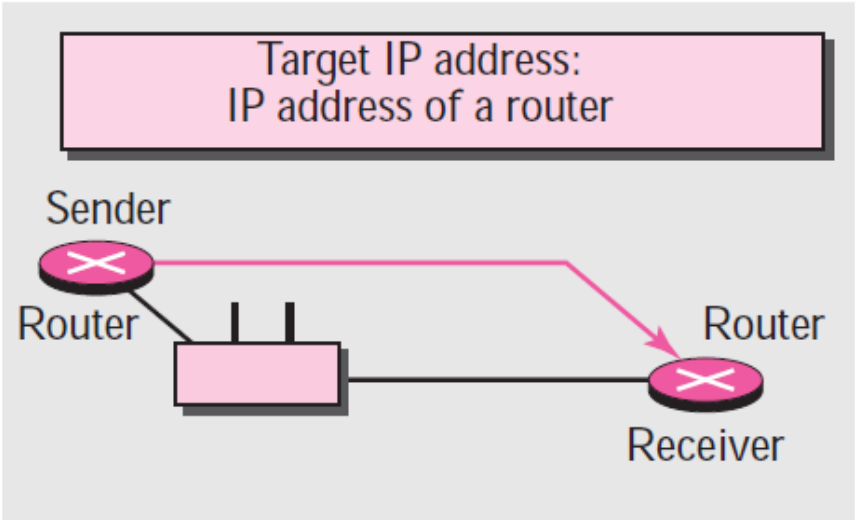


Case 2: A host has a packet to send to a host on another network.

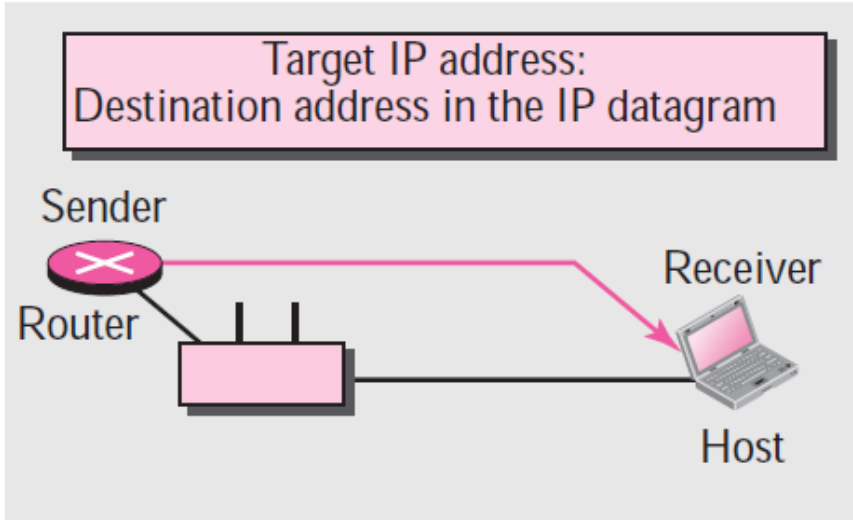


ARP Usage Scenarios

Case 3: A router has a packet to send to a host on another network.



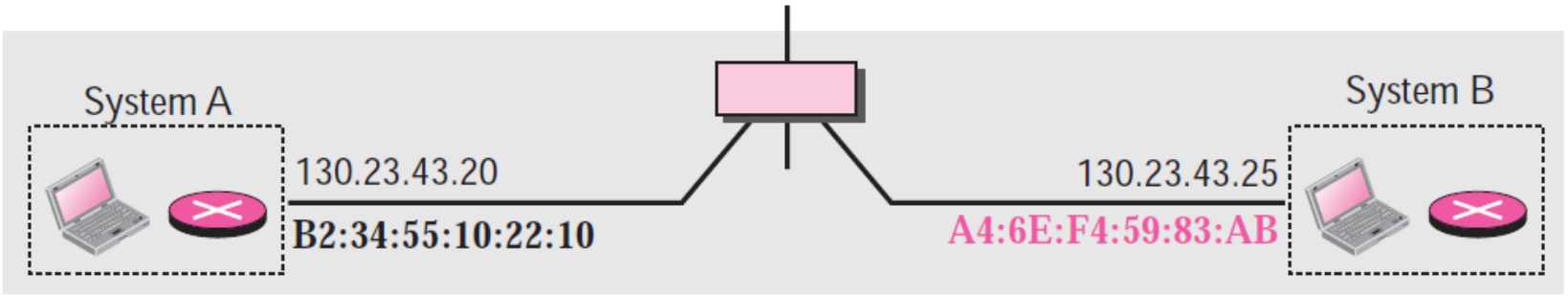
Case 4: A router has a packet to send to a host on the same network.

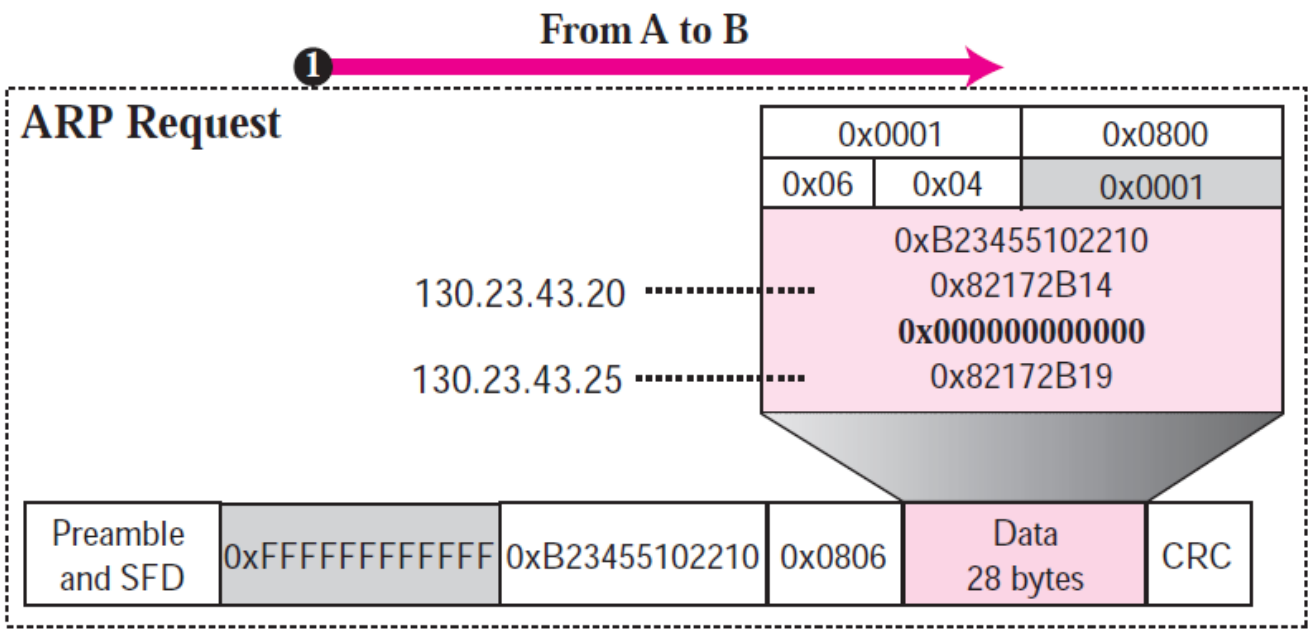


☞ Exercise

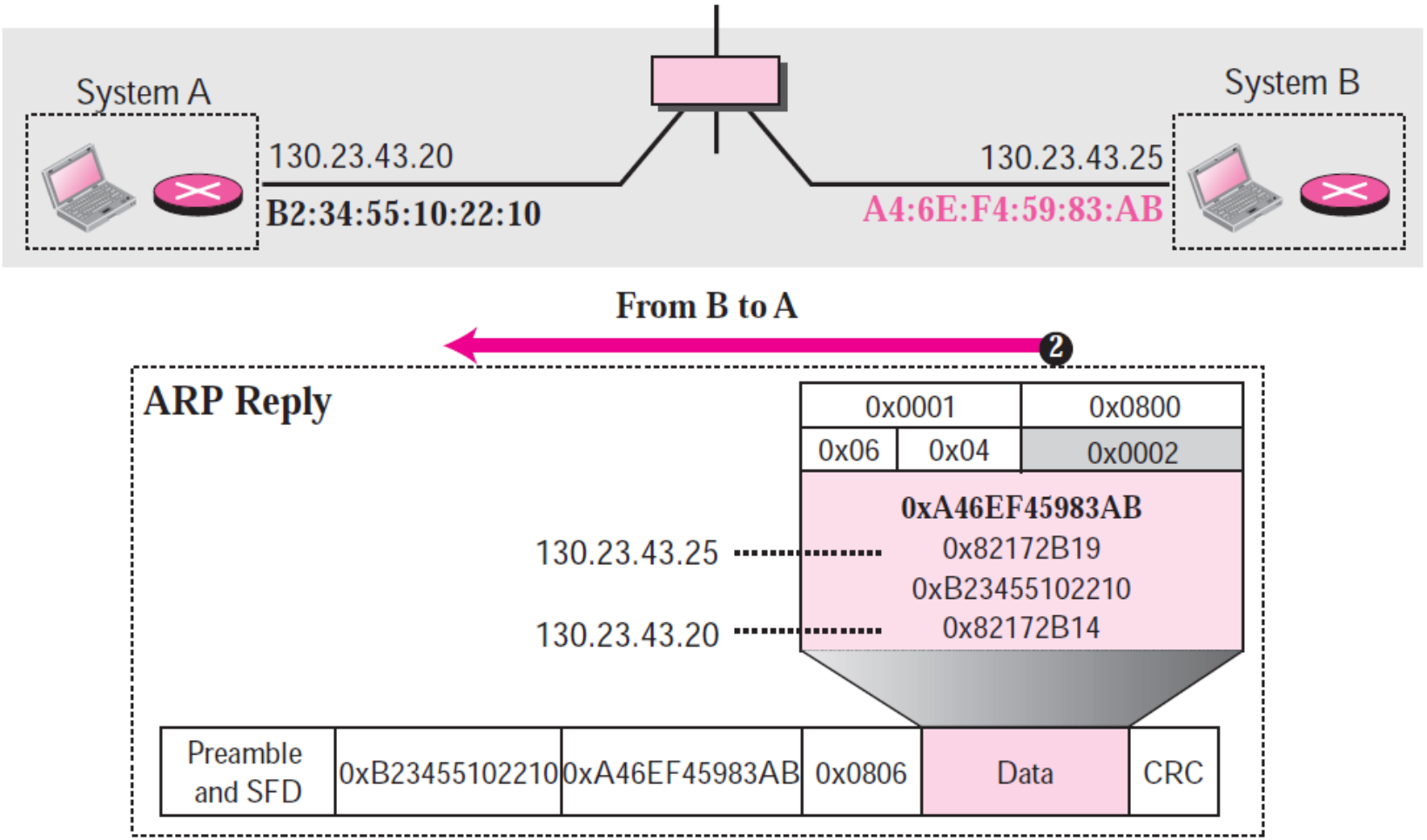
A host with IP address 130.23.43.20 and physical address $B2:34:55:10:22:10$ has a packet to send to another host with IP address 130.23.43.25 and physical address $A4:6E:F4:59:83:AB$ (which is unknown to the first host). The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.

ARP Exercise Request





ARP Exercise Reply



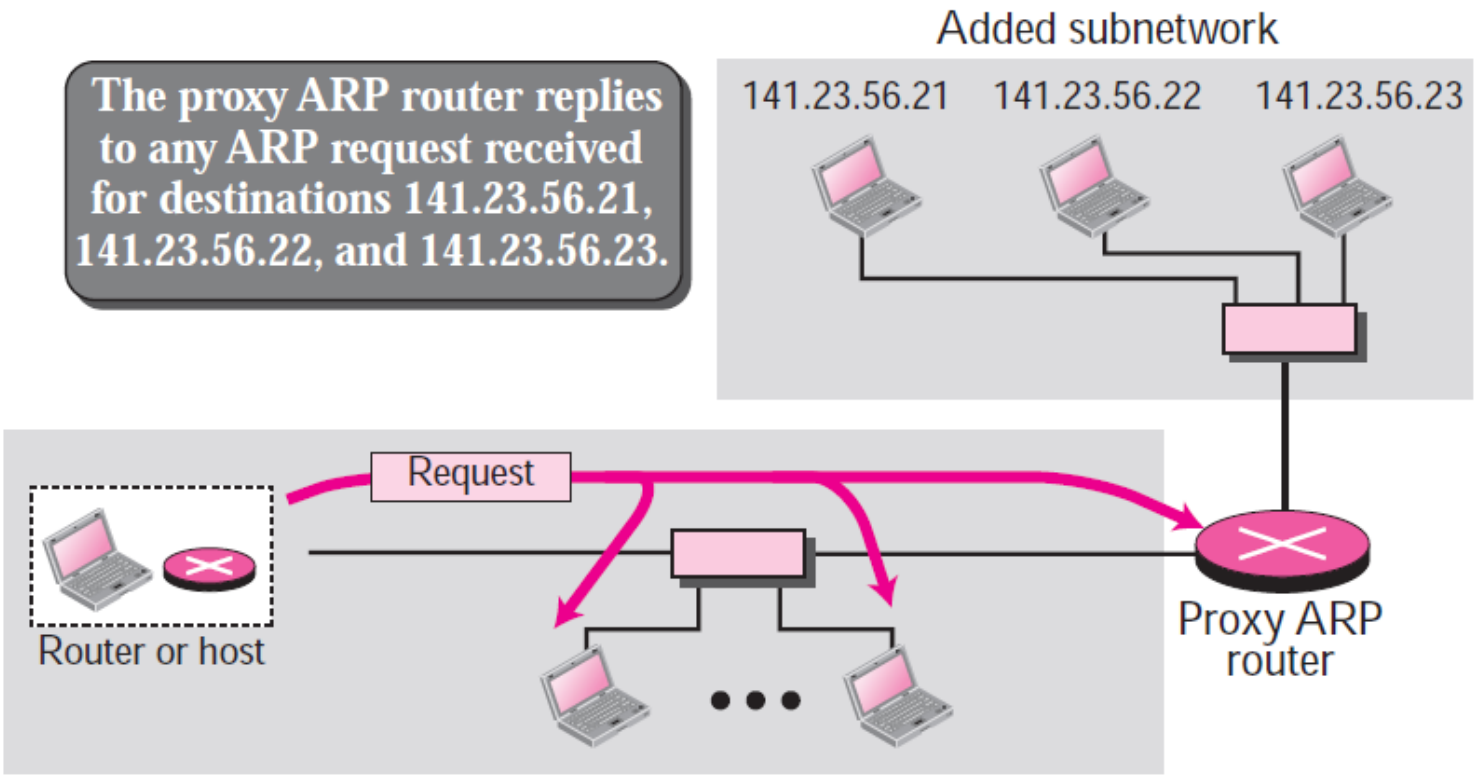
Proxy ARP Router

- acts on behalf of a set of hosts.

Proxy ARP Router

- acts on behalf of a set of hosts.
- whenever a router running a proxy ARP receives an ARP request looking for the IP address of one of its hosts, the router sends an ARP reply announcing its own hardware (physical) address.

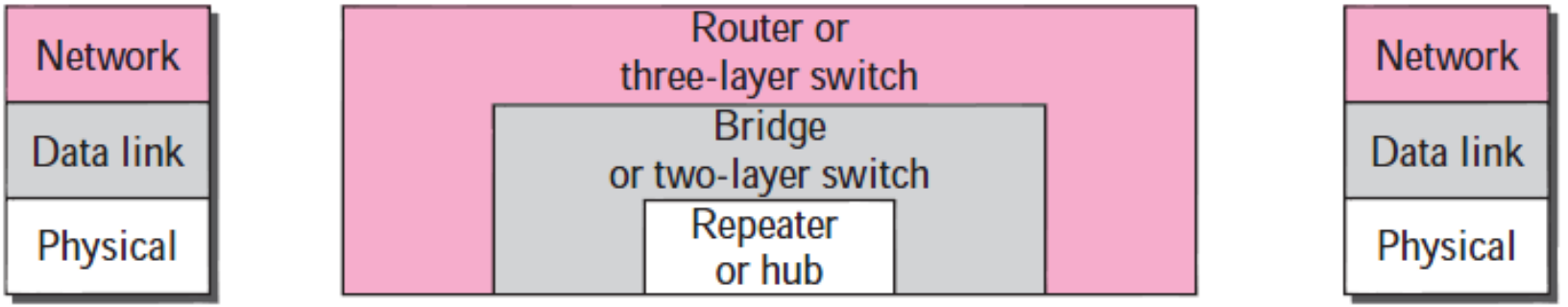
Proxy ARP Router



After the router receives the actual IP packet, it sends the packet to the appropriate host or router.

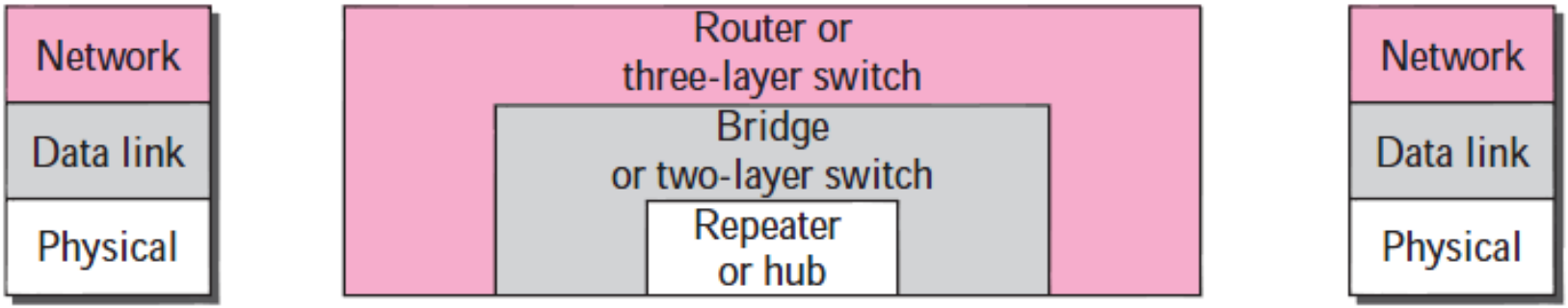
Connecting Devices

- To connect LANs and WANs together we use connecting devices.

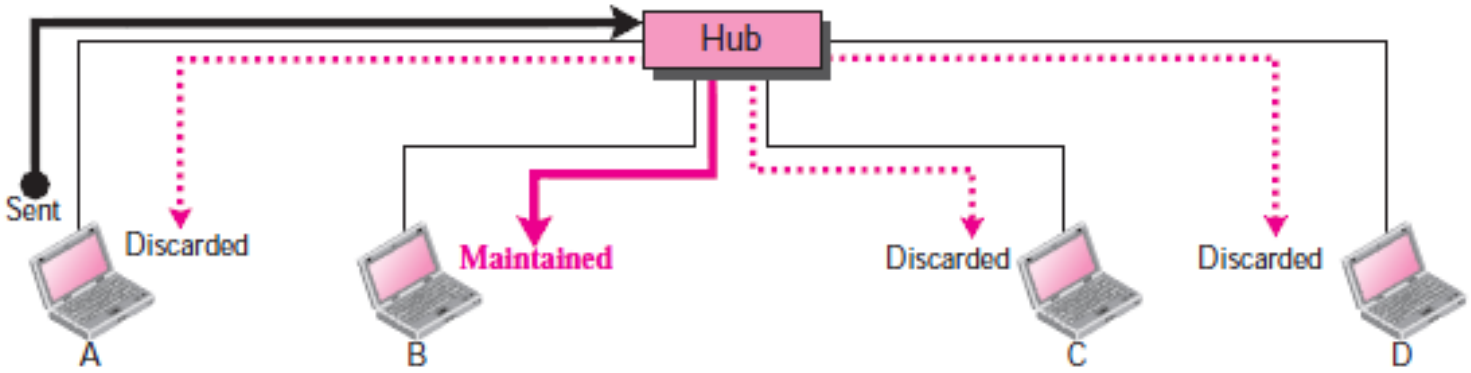


Connecting Devices

- To connect LANs and WANs together we use connecting devices.
- Ex. Repeaters (or hubs), Bridges (or two-layer switches), and Routers (or three-layer switches).



Repeater



A repeater forwards every bit; it has no filtering capability.

Bridge

Two-layer switch

- operates in both the physical and the data link layers.

Bridge

Two-layer switch

- operates in both the physical and the data link layers.
- PHY: regenerates the signal it receives.

Bridge

Two-layer switch

- operates in both the physical and the data link layers.
- PHY: regenerates the signal it receives.
- DLL: check the MAC addresses (source and destination) contained in the frame.

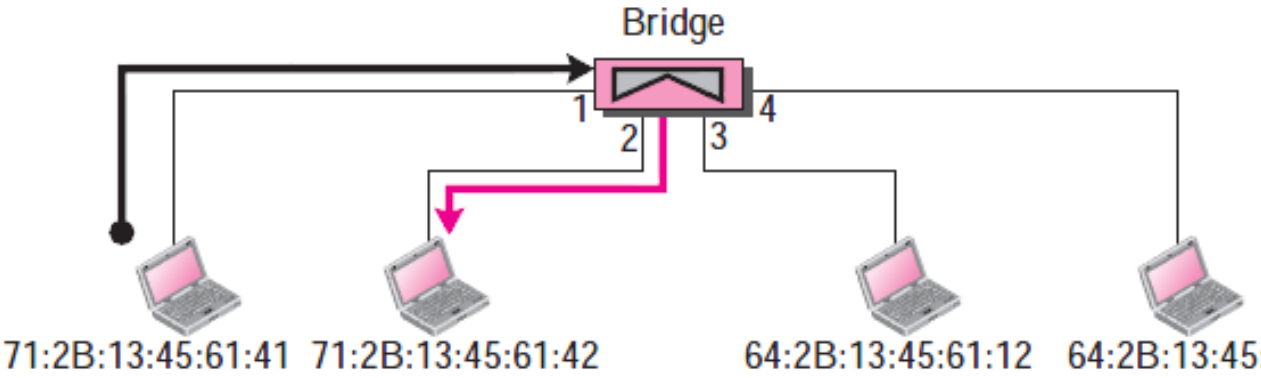
Bridge

Two-layer switch

- operates in both the physical and the data link layers.
- PHY: regenerates the signal it receives.
- DLL: check the MAC addresses (source and destination) contained in the frame.
- has a table used in filtering decisions.

Bridge
Example

The bridge consults its table to find the departing port.



Bridge 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

Transparent Bridge

- a bridge in which the stations are completely unaware of the bridge's existence.

Transparent Bridge

- a bridge in which the stations are completely unaware of the bridge's existence.
- reconfiguration of the stations is unnecessary when added or deleted.

Transparent Bridge

- a bridge in which the stations are completely unaware of the bridge's existence.
- reconfiguration of the stations is unnecessary when added or deleted.
- forwarding function with dynamic forwarding table

Bridge Learning

Gradual building of Table

Address	Port

a. Original

Address	Port
71:2B:13:45:61:41	1

b. After A sends a frame to D

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

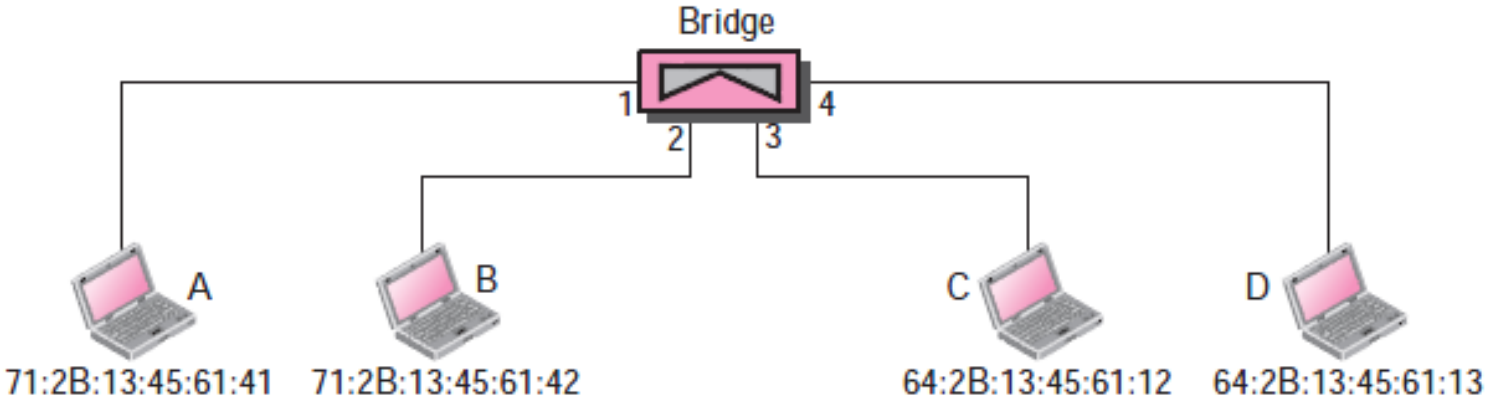
c. After D sends a frame to B

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

d. After B sends a frame to A

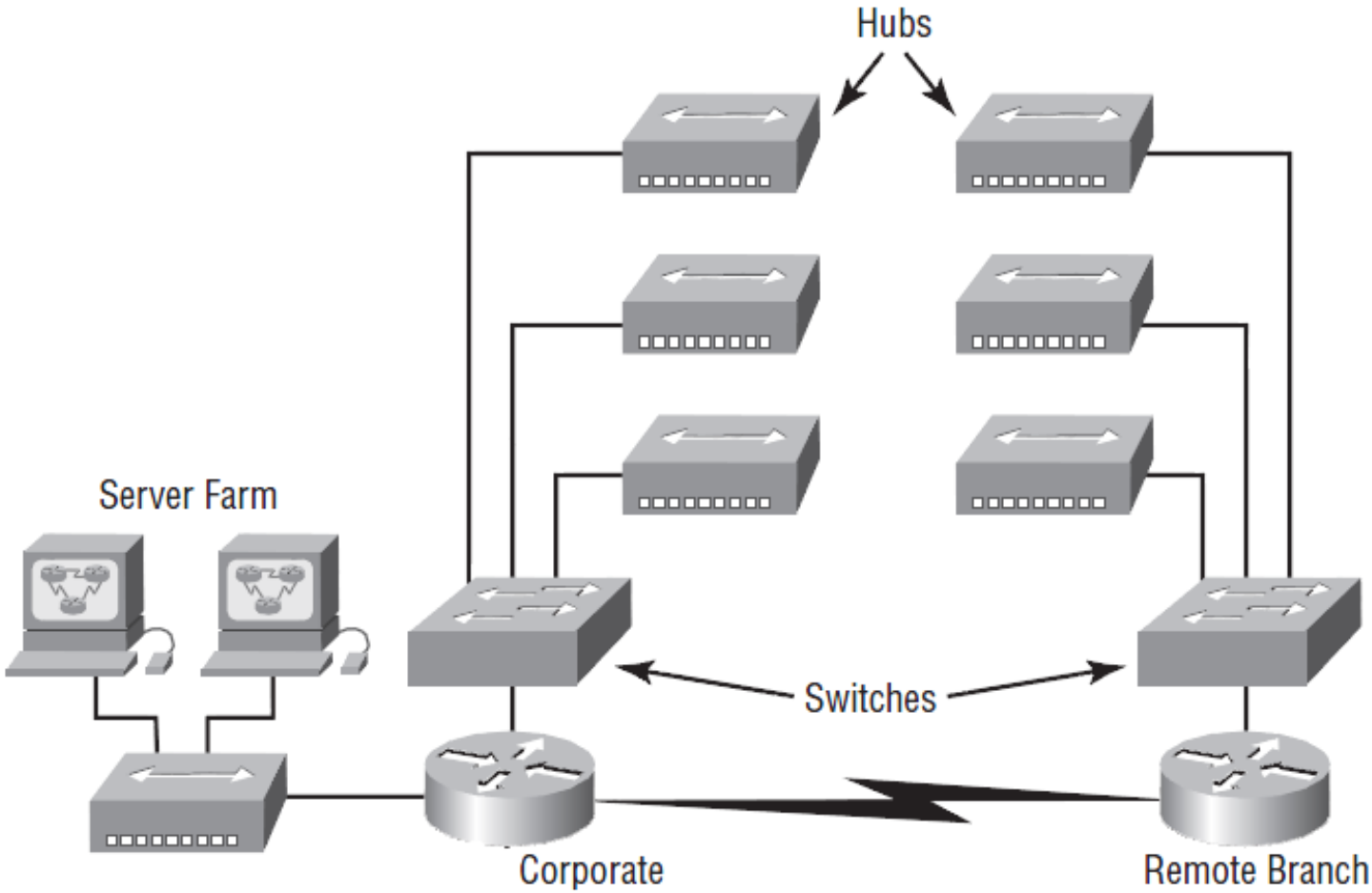
Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3

e. After C sends a frame to D



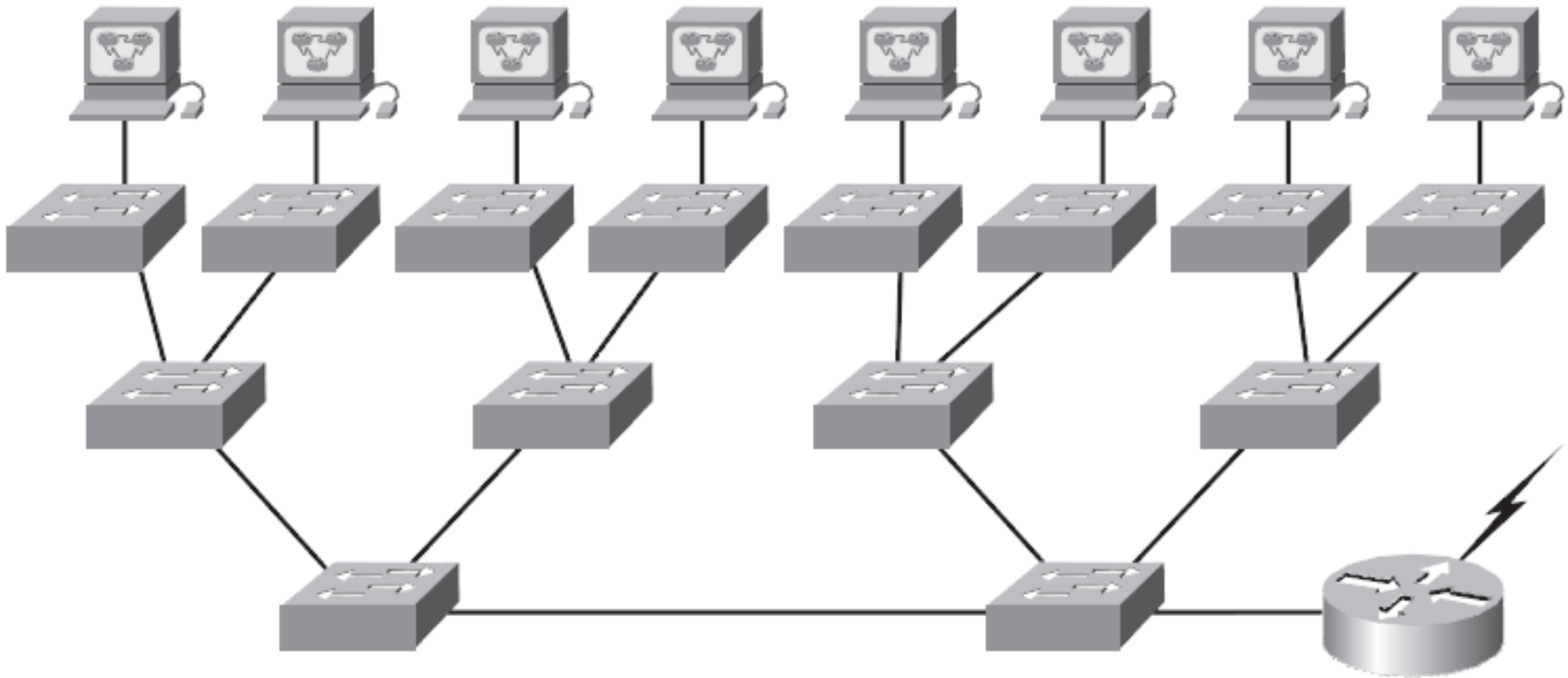
Switched LAN

Traditional



Switched LAN

Contemporary



Bridging vs. LAN Switching

- Bridges are software based, while switches are hardware based (ASIC for filtering)

Bridging vs. LAN Switching

- Bridges are software based, while switches are hardware based (ASIC for filtering)
- A switch can be viewed as a multiport bridge.

Bridging vs. LAN Switching

- Bridges are software based, while switches are hardware based (ASIC for filtering)
- A switch can be viewed as a multiport bridge.
- Switches have a higher number of ports than most bridges.

Bridging vs. LAN Switching

- Bridges are software based, while switches are hardware based (ASIC for filtering)
- A switch can be viewed as a multiport bridge.
- Switches have a higher number of ports than most bridges.
- Both bridges and switches forward layer 2 broadcasts.

Layer 2 Switch Functions

- Address learning
  remember the source hardware address of each frame received, and save in forward/filter table.

Layer 2 Switch Functions

- Address learning
  remember the source hardware address of each frame received, and save in forward/filter table.
- Forward/filter decisions
  When a frame is received, the switch looks at the destination hardware address and finds the exit interface.

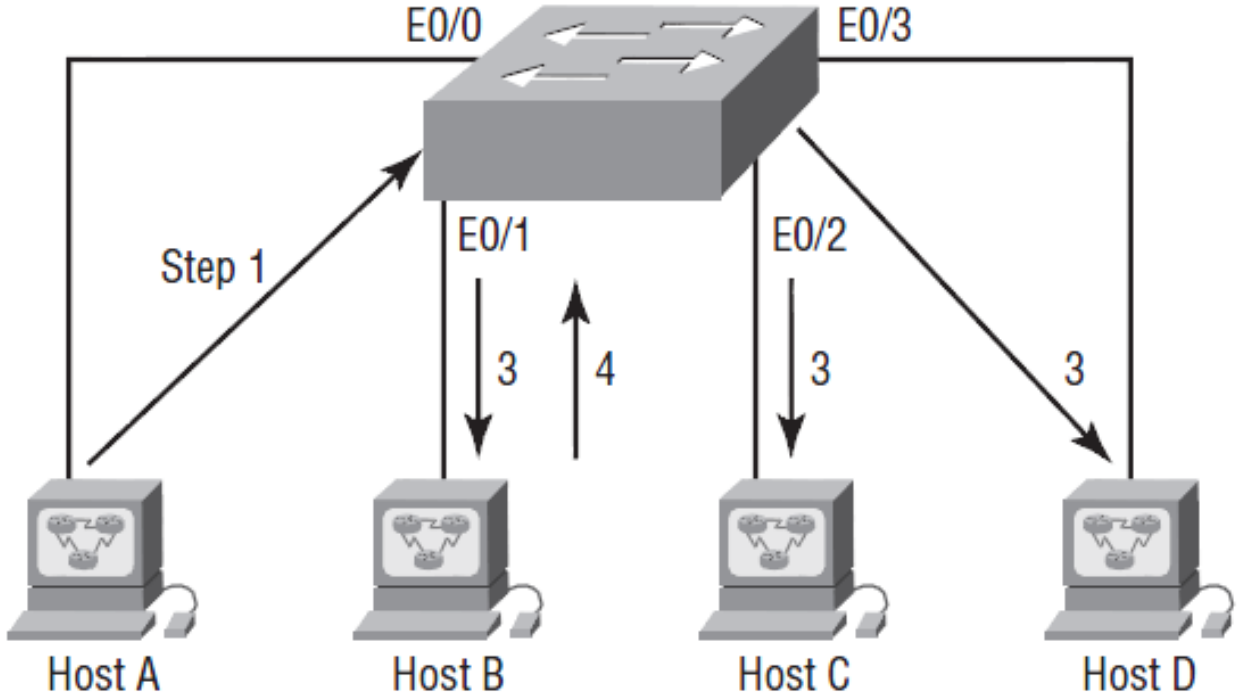
Layer 2 Switch Functions

- Address learning
  remember the source hardware address of each frame received, and save in forward/filter table.
- Forward/filter decisions
  When a frame is received, the switch looks at the destination hardware address and finds the exit interface.
- Loop avoidance
  stop network loops while still permitting redundancy.

Address Learning

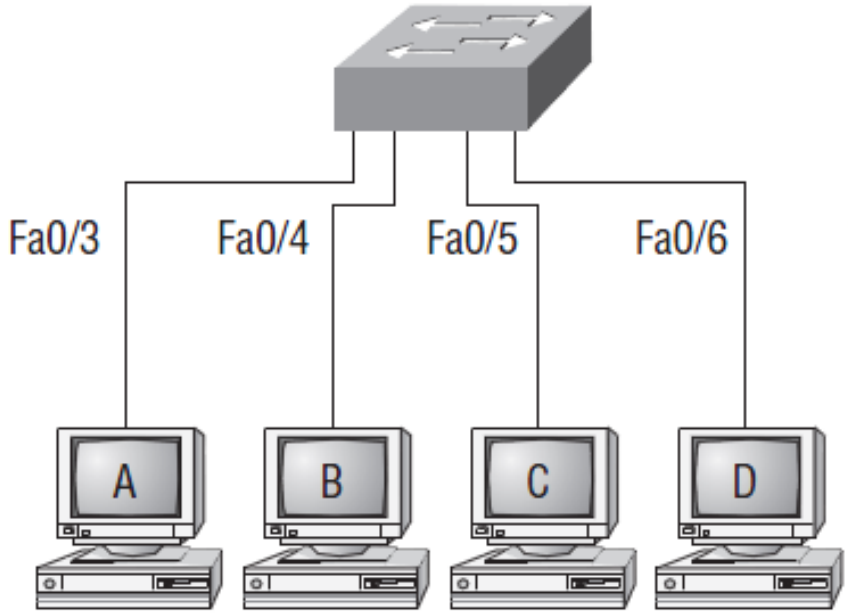
MAC Forward/Filter Table

E0/0: 0000.8c01.000A step 2
E0/1: 0000.8c01.000B step 4
E0/2:
E0/3:



Forward/Filter Decisions

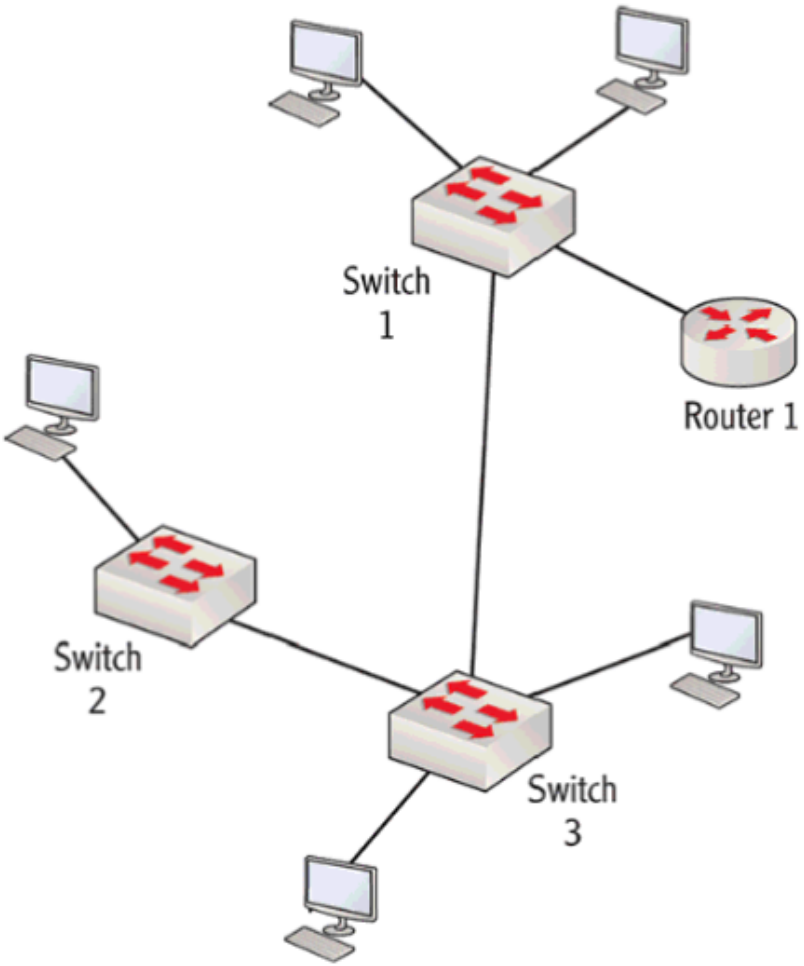
Host A sends a data frame to Host D. What will the switch do when it receives the frame from Host A?

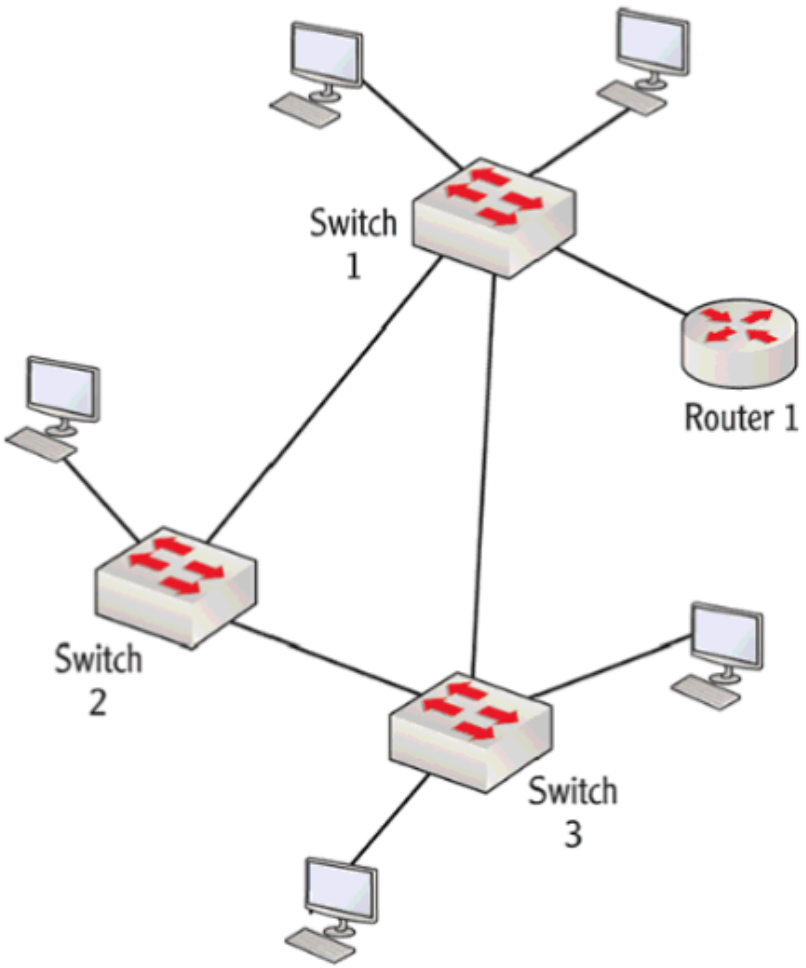



```
Switch#sh mac address-table
Vlan    Mac Address       Ports
----    -----------       -----
   1    0005.dccb.d74b    Fa0/4
   1    000a.f467.9e80    Fa0/5
   1    000a.f467.9e8b    Fa0/6
```

Network Redundancy

Importance and Problem

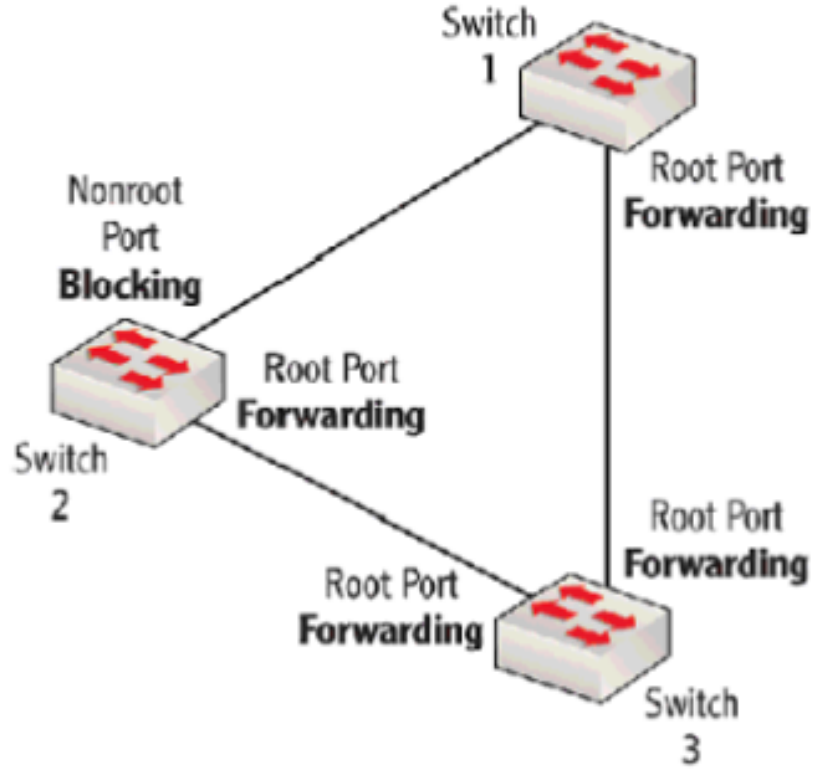




Loop Avoidance

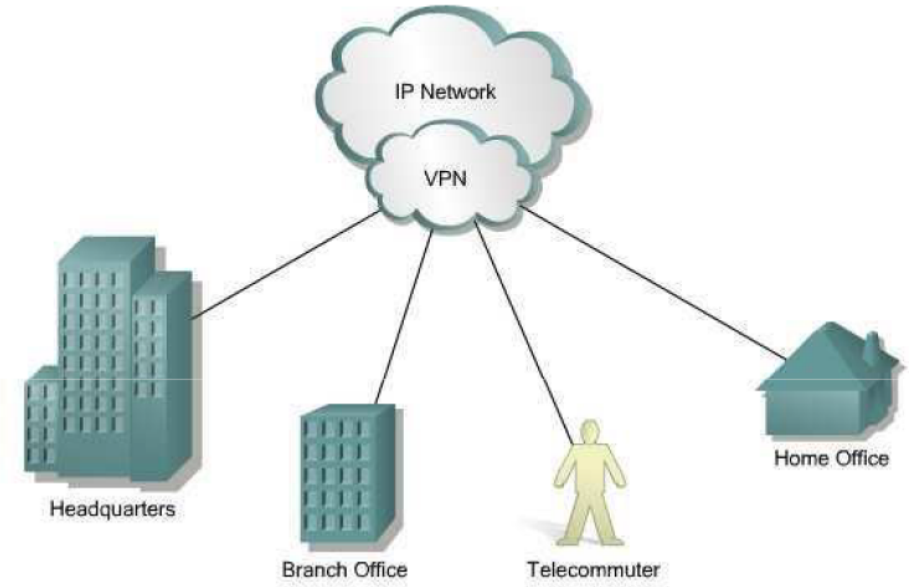
Spanning Tree Protocol (STP)

" All root ports forward,
All nonroot ports block ".



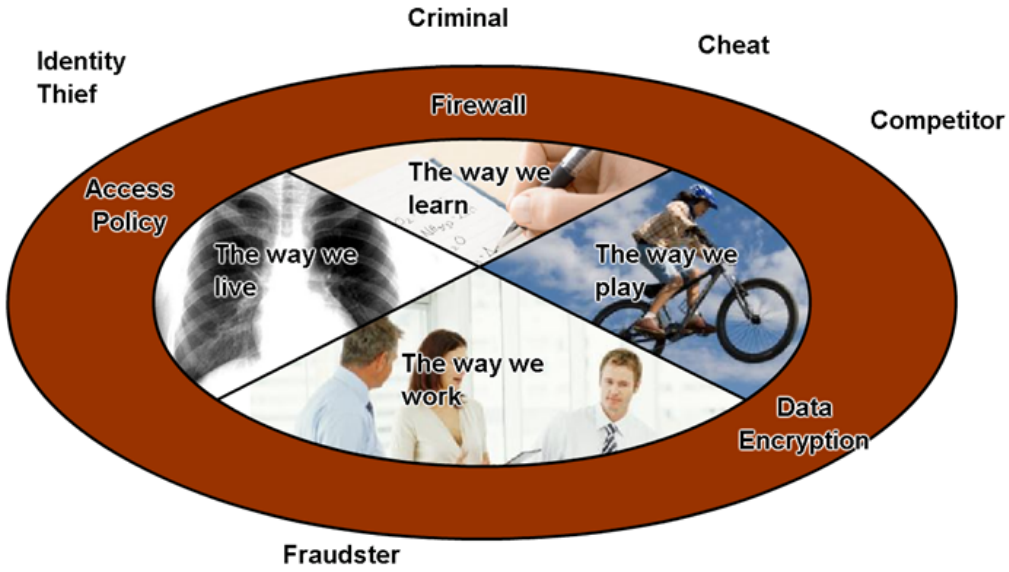
Virtual Private Network
VPN

- It enables a host computer to send and receive data across shared or public networks as if it were a private network with all the functionality



Network Security Issue

- Ensure confidentiality through use of
  - User authentication
  - Data encryption



Virtual Private Networks

- network connection that uses the Internet to give users or branch offices secure access to a company's network resources.

Virtual Private Networks

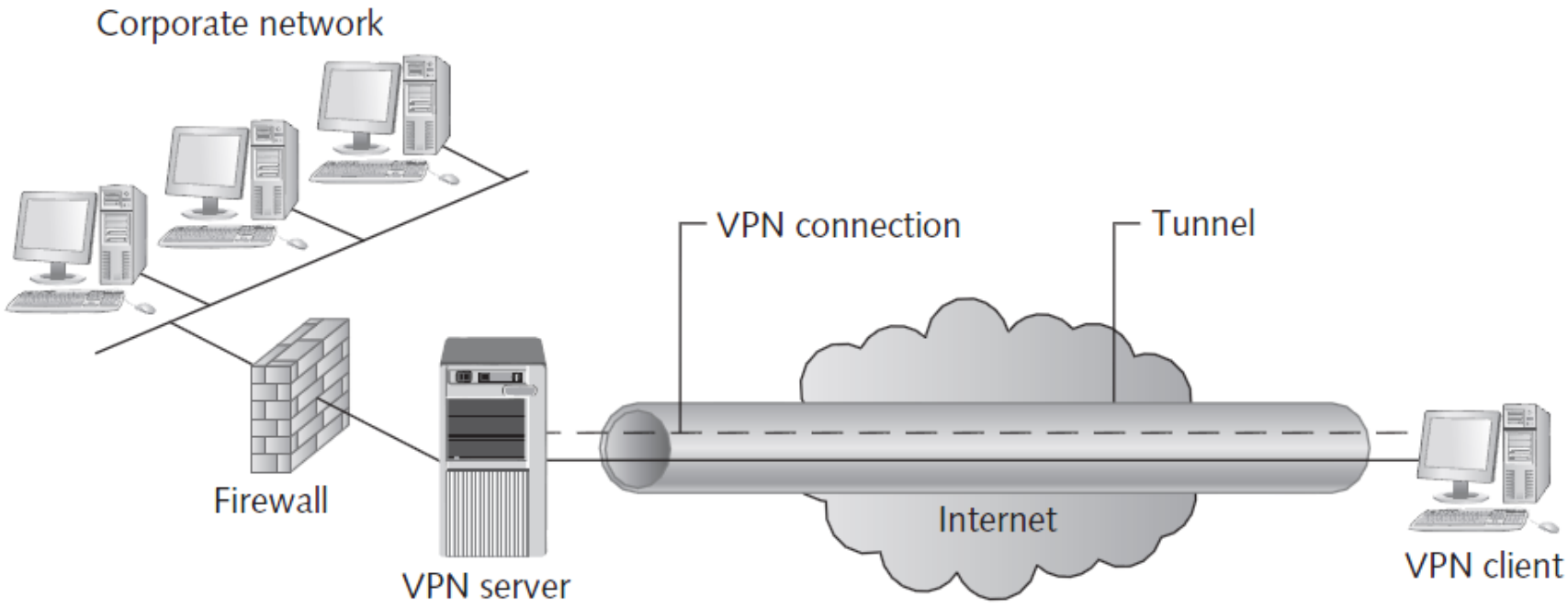
- network connection that uses the Internet to give users or branch offices secure access to a company's network resources.
- use encryption technology to ensure that communication is private and secure

Virtual Private Networks

- network connection that uses the Internet to give users or branch offices secure access to a company's network resources.
- use encryption technology to ensure that communication is private and secure
- Privacy is achieved by creating a "tunnel" between the VPN client and VPN server.

Virtual Private Network

A tunnel is created by encapsulation, in which the inner packet containing the data is encrypted and the outer headers contain the unencapsulated addresses.



VPN Types/ Benefits

- Remote access VPNs
  Enable mobile users to connect with corporate networks securely wherever an Internet connection is available.

VPN Types/ Benefits

- Remote access VPNs
  Enable mobile users to connect with corporate networks securely wherever an Internet connection is available.
- Site-to-site VPNs or intranet
  Allow multiple sites to maintain permanent secure connections via the Internet instead of using expensive WAN links.

VPN Types/ Benefits

- Reduce costs by using the ISP's support services instead of paying for more expensive WAN support.

VPN Types/ Benefits

- Reduce costs by using the ISP's support services instead of paying for more expensive WAN support.
- Eliminate the need to support dial-up remote access, which is a higher-cost solution requiring more personnel.

IP Security

IPSec

- a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level..

IP Security

IPSec

- a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level..
- helps create authenticated and confidential packets for the IP layer.

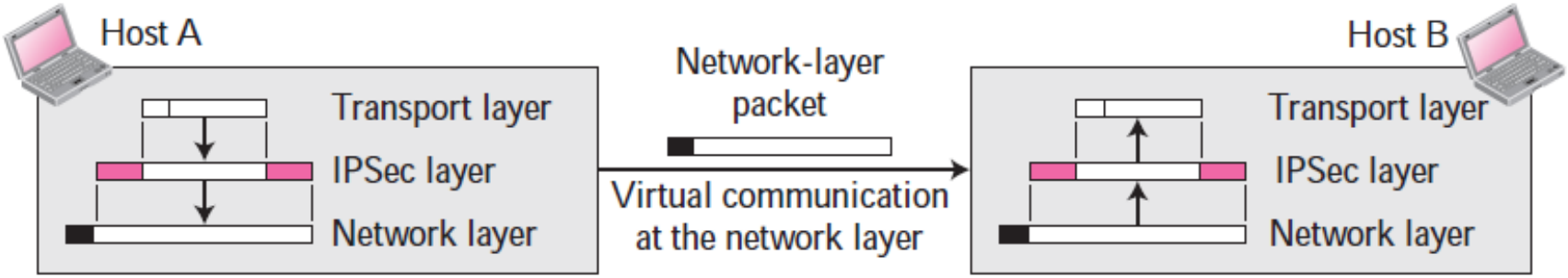
IP Security

IPSec

- a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level..
- helps create authenticated and confidential packets for the IP layer.
- operates in one of two different modes: transport or tunnel mode.

IPSec Transport Mode

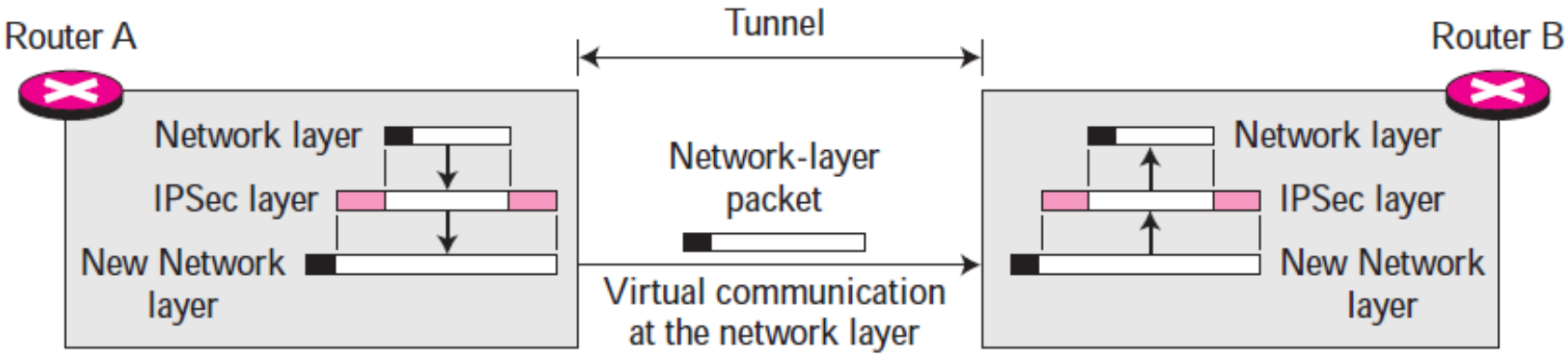
IPSec in transport mode does not protect the IP header;
it only protects the information coming from the transport layer.



It is used when we need host-to-host (end-to-end) protection of data.

IPSec Tunnel Mode

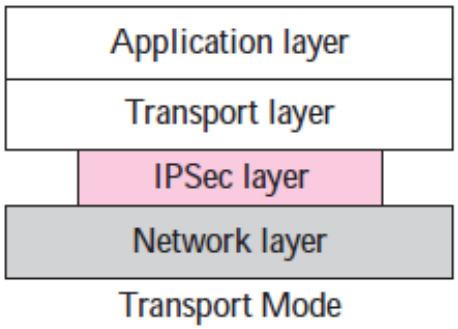
IPSec in tunnel mode protects the original IP header.



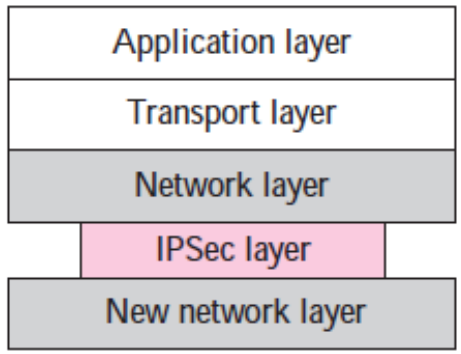
It is used between two routers, between a host and a router, or between a router and a host.

Tunnel vs. Transport Mode

- In transport mode, the IPSec layer comes between the transport layer and the network layer.
- In tunnel mode, the flow is from the network layer to the IPSec layer and then back to the network layer again.



Transport Mode



Tunnel Mode

Other Terms

- 1000BASE-CX, 1000BASE-LX, 1000BASE-SX, 1000BASE-T
  The IEEE 802.3 standards for Ethernet implementation with 1-Gbps data rate.
- 100BASE-FX, 100BASE-T4, 100BASE-TX, 100BASE-X
  The IEEE 802.3 standards for Fast Ethernet implementation with 100-Mbps data rate.
- 10BASE2, 10BASE5, 10BASE-F, 10BASE-E, 10BASE-L
  The IEEE 802.3 standard for Thin Ethernet with 10-Mbps data rate.

Other Terms

- Address Resolution Protocol (ARP)
  In TCP/IP, a protocol for obtaining the physical address of a node when the Internet address is known.
- Address space
  The total number of addresses used by a protocol.
- Bandwidth
  The difference between the highest and lowest frequencies available for network signals. The term is also used to describe the rated throughput capacity of a given network medium or protocol.

Other Terms

- Bridge
  A network device operating at the first two layers of the OSI model with filtering and forwarding capabilities.
- Broadcast address
  An address that allows transmission of a message to all nodes of a network.
- Congestion
  Excessive network or internetwork traffic causing a general degradation of service. This can be seen in slower response times, longer file transfers and network users becoming less productive due to network delays.

Other Terms

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  An access method in wireless LANs that avoids collision by forcing the stations to send reservation messages when they find the channel is idle.
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
  An access method in which stations transmit whenever the transmission medium is available and retransmit when collision occurs.
- Collision
  The event that occurs when two transmitters send at the same time on a channel designed for only one transmission at a time; data will be destroyed.

Other Terms

- Consultative Committee for International Telegraphy and Telephony (CCITT)
  An international standards group now known as the ITU-T.
- Defense Advanced Research Projects Agency (DARPA)
  A government organization, which, under the name of ARPA, funded ARPANET and the Internet.
- Ethernet
  A local area network using the CSMA/CD access method.

Other Terms

- Extranet
  A private network that uses the TCP/IP protocol suite that allows authorized access from outside users.
- Flooding
  Saturation of a network with a message. intranet A private network that uses the TCP/IP protocol suite.
- Intranet
  A private network that uses the TCP/IP protocol suite.

Other Terms

- Institute of Electrical and Electronics Engineers (IEEE)
  A group consisting of professional engineers that has specialized societies whose committees prepare standards in members' areas of specialty.
- Logical tunnel
  The encapsulation of a multicast packet inside a unicast packet to enable multicast routing by non-multicast routers.
- Physical address
  The address of a device used at the data link layer (MAC address).

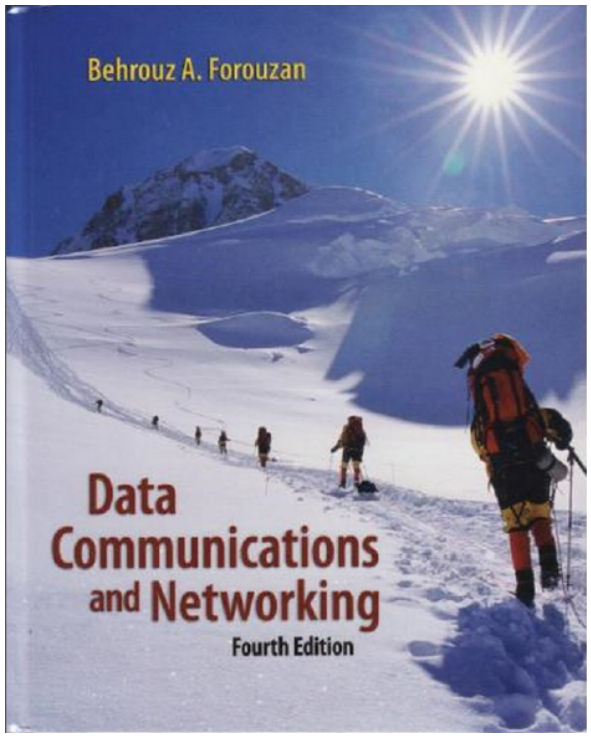
Other Terms

- Request for Comment (RFC)
  A formal Internet document concerning an Internet issue.
- Reverse Address Resolution Protocol (RARP)
  A TCP/IP protocol that allows a host to find its Internet address, given its physical address.
- Switch
  A device connecting multiple communication lines together.
- Switched Ethernet
  An Ethernet in which a switch, replacing the hub, can direct a transmission to its destination.

References

TEXTBOOK:

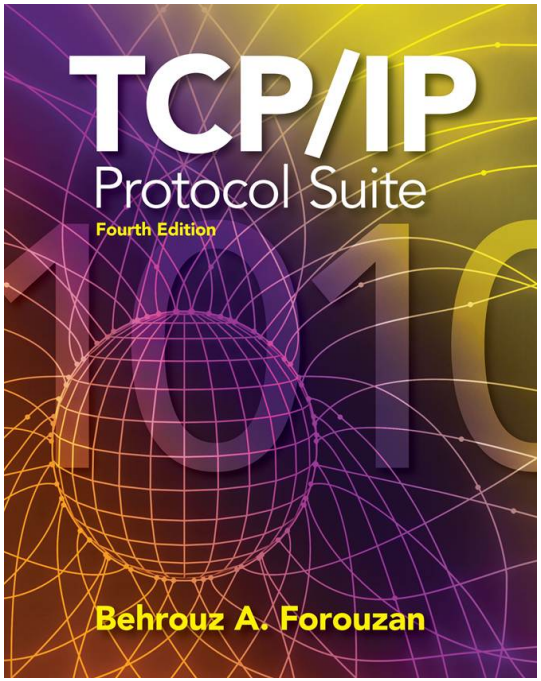
- Data Communications and Networking, Behrouz Forouzan, 4th Edition, McGraw-Hill, 2007



References

SECONDARY SOURCE:

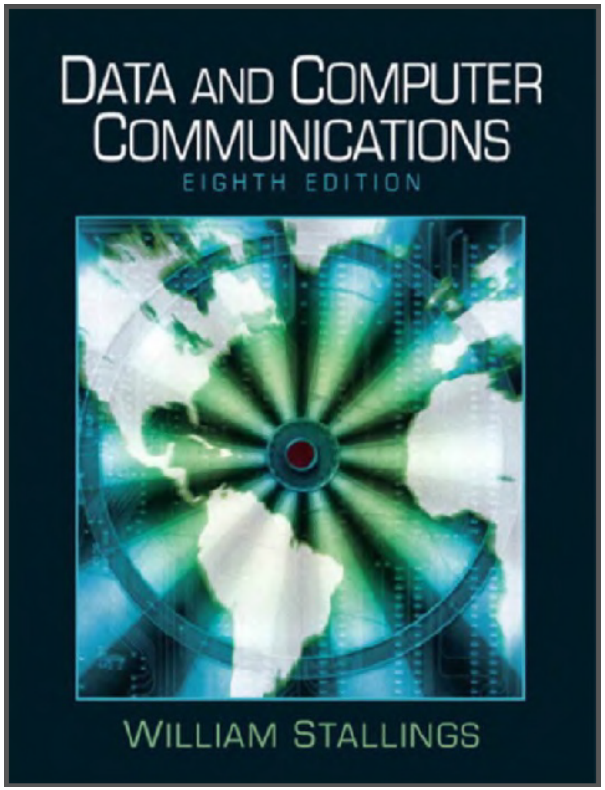
- TCP/IP Protocol Suite, Behrouz Forouzan, 4th edition, 2010



References

SECONDARY SOURCE:

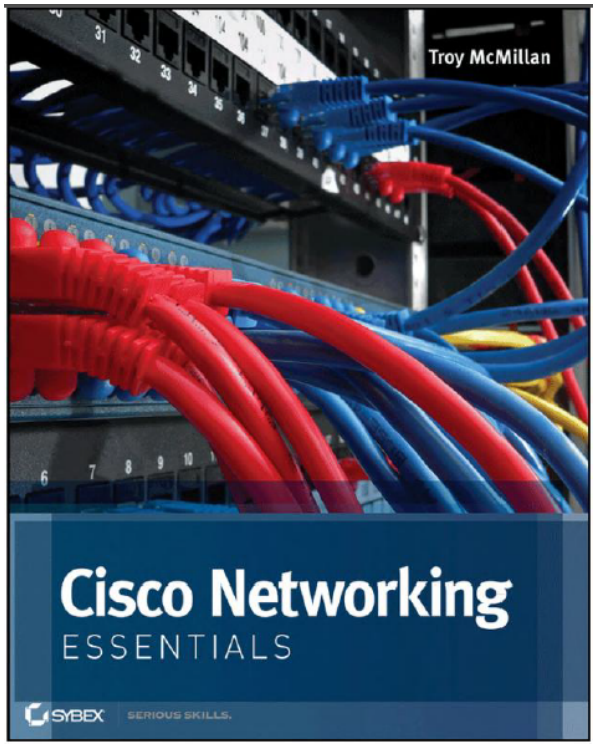
- Data and Computer Communications, William Stallings, 2007



References

SECONDARY SOURCE:

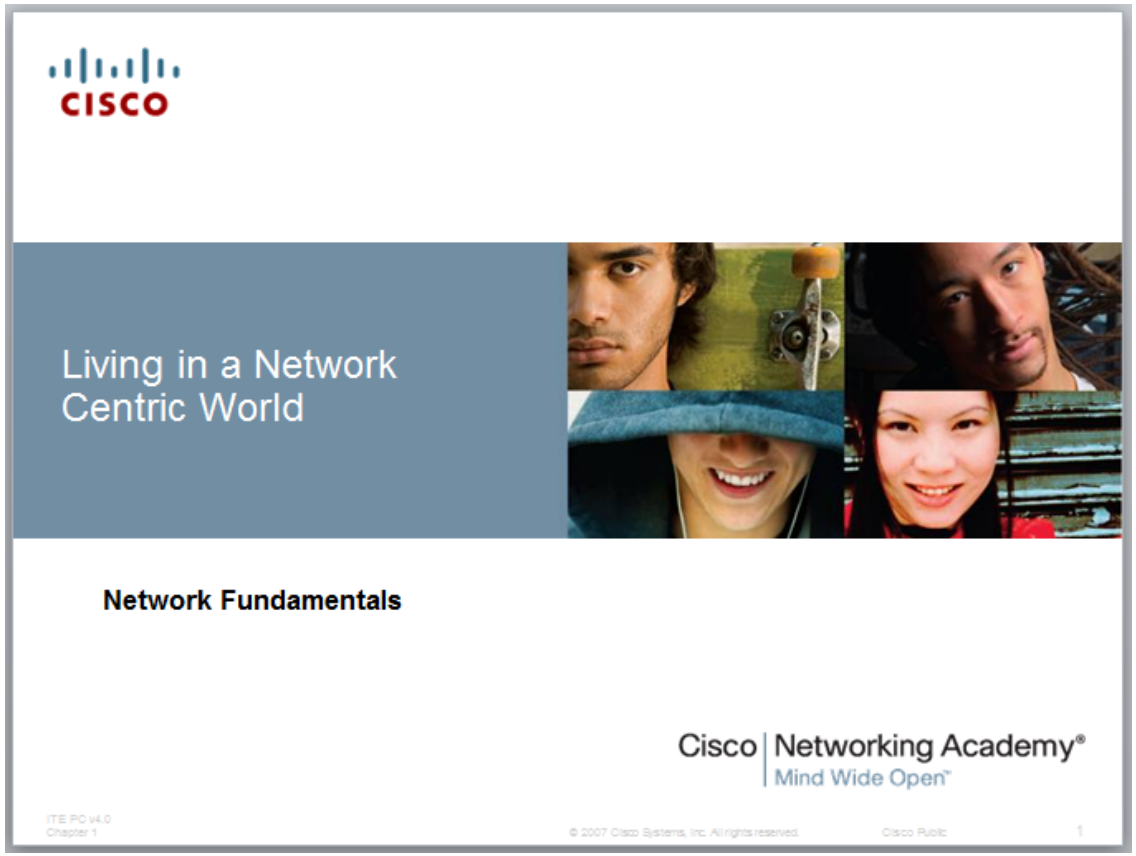
- CISCO Networking Essentials, Troy McMillan, 2012



References

SECONDARY SOURCE:

- Network Fundamentals, Cisco Networking Academy, 2007



Thank you for your attention!