Unit -1

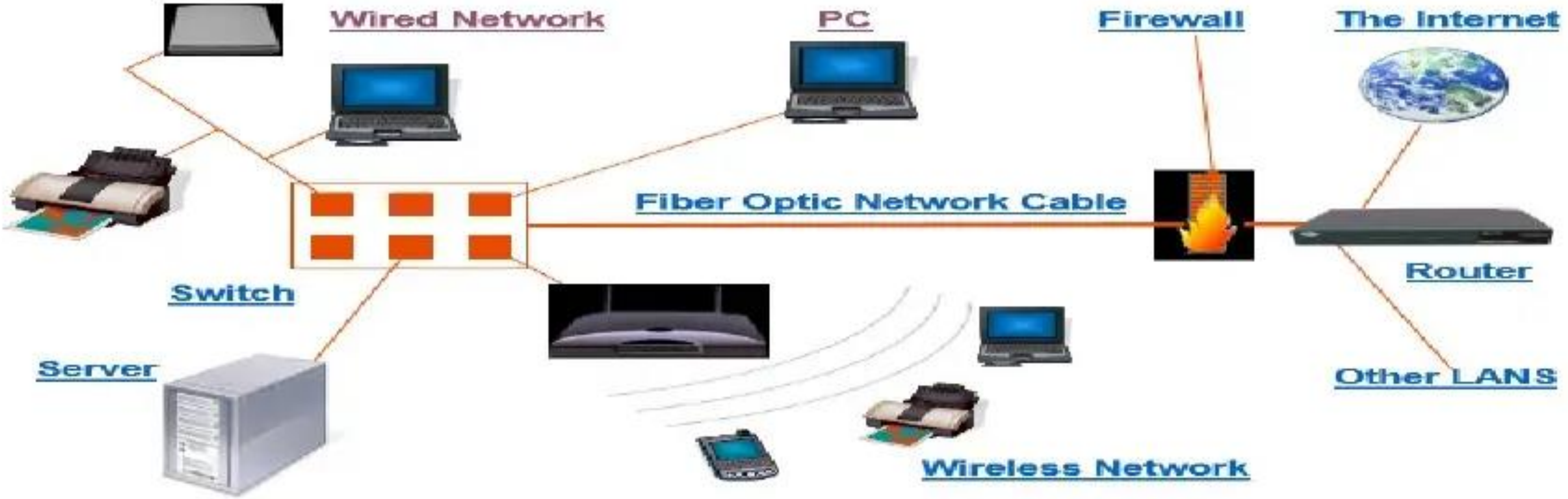
NETWORK BASICS

Concept of Network

A collection of computing devices that are connected in various ways in order to communicate and share resources.

Usually, the connections between computers in a network are made using physical wires or cables

However, some connections are wireless, using radio waves or infrared signals



The Network Diagram

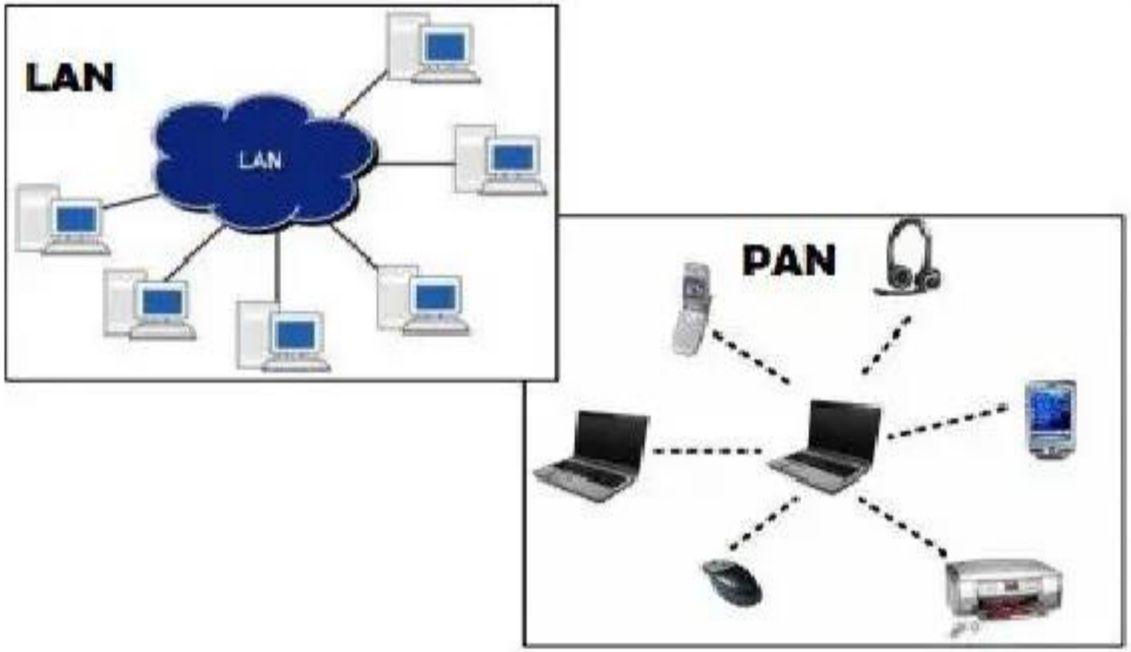
Types of Network

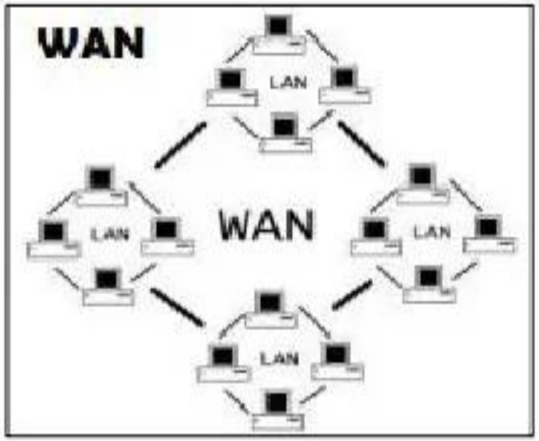
There are many types of computer networking which are used worldwide these days. There are some types of network that are using worldwide

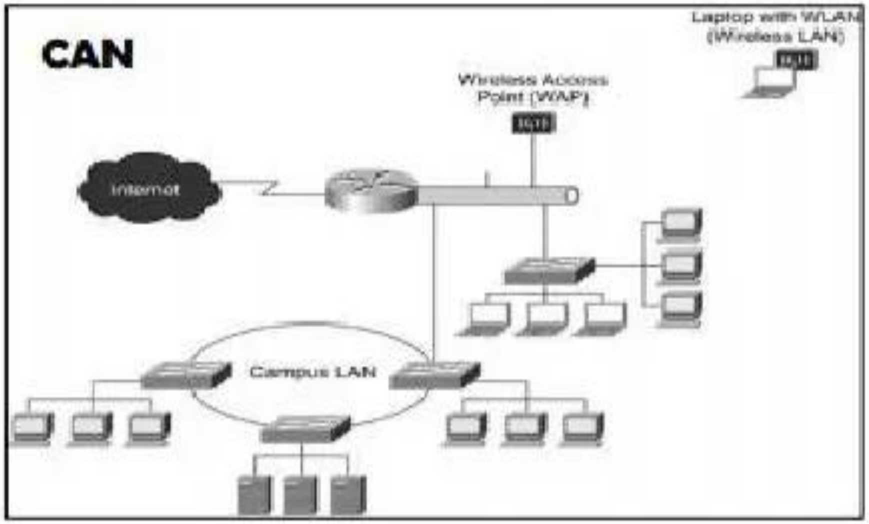
- **LAN -Local Area Network**

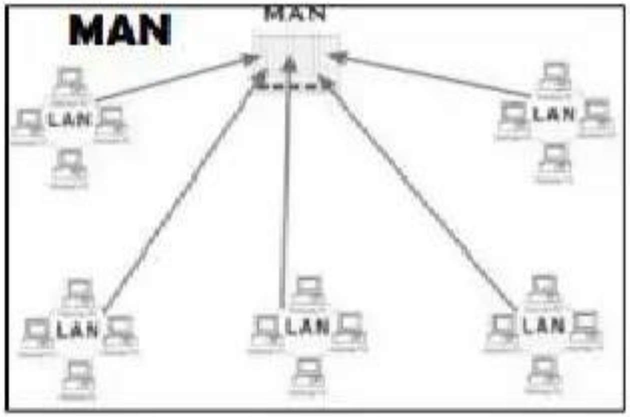
- **WAN -Wide Area Network**

- **MAN -Metropolitan Area Network**


LAN
LAN
PAN


WAN
LAN
LAN
WAN
LAN
LAN


CAN
Laptop with WLAN
(Wireless LAN)
Wireless Access
Point (WAP)
Internet
Campus LAN


MAN
MAN
LAN
LAN
LAN
LAN
LAN

Models of Network Computing

Three methods of organization, or *models*, are generally recognized. The three models for network computing are as follows:

❑Centralized computing

❑Distributed computing

❑Collaborative or cooperative computing

Centralized Computing

The centralized computing model involves the following:

- All processing takes place in the central, mainframe computer.
- Terminals are connected to the central computer and function only as input/output devices.
- Networks may be employed to interconnect two or more mainframe computers. Terminals connect only to the mainframe, never to each other.

This computing model worked well in large organizations

Distributed Computing

Distributed computing involves the following:

- Multiple computers are capable of operating independently.
- Tasks are completed locally on various computers.
- Networks enable the computers to exchange data and services but do not provide processing assistance.

It largely dealt with the sharing of data and printers

Collaborative Computing

Collaborative computing involves the following:

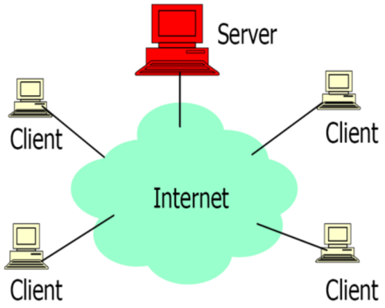
- Multiple computers cooperating to perform a task
- A network that enables the computers to exchange data and services
- Software designed to take advantage of the collaborative environment.

Obviously, collaborative computing cannot take place without a network to enable the various computers to communicate.

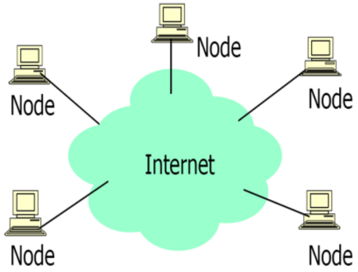
Networking Models

PC networks generally fall within one of these two network types:

- Server-based

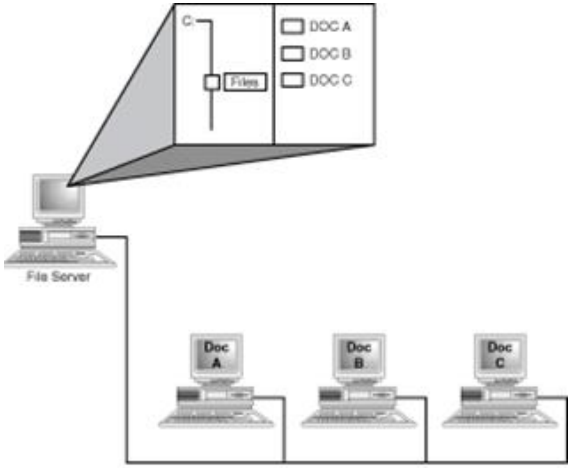


- Peer-to-peer



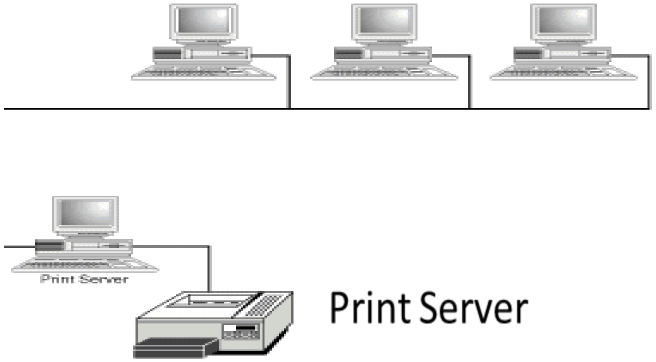
Server-Based Networking

- In a *server-based* network environment, resources are located on a central server or group of servers.
- A *server* is a computer that is specifically designated to provide services for the other computers on the network.
- A *network client* is a computer that accesses the resources available on the server.



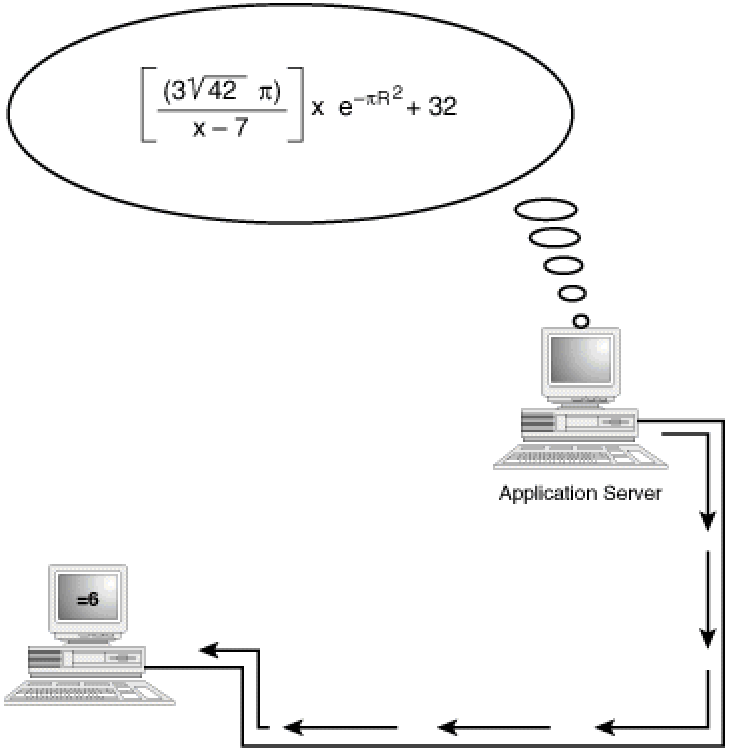
File Server

- A ***file server*** is a server that stores files on the network for users



Print Server

- A ***print server*** manages access to network printing resources, thus enabling several client machines to use the same printer


$\left[\frac{(3\sqrt{42}\ \pi)}{x-7}\right] x\ e^{-\pi R^2} + 32$
Application Server
=6

Application Server

An application server runs all or part of an application on behalf of the client and then transmits the result to the client for further processing.

The following network operating systems are designed to implement LANs based on server-based models:

- Novell NetWare
- Banyan VINES
- OpenVMS
- IBM OS/2 LAN Server
- Microsoft Windows NT Server

Peer-to-Peer Networking

- In the *peer-to-peer* network environment, resources are distributed throughout the network on computer systems that may act as both service requesters and service providers.

- In a peer-to-peer network, the user of each PC is responsible for the administration and sharing of resources for his PC, which is known as distributed or workgroup administration.
  A peer-to-peer network sometimes is called a *workgroup*.

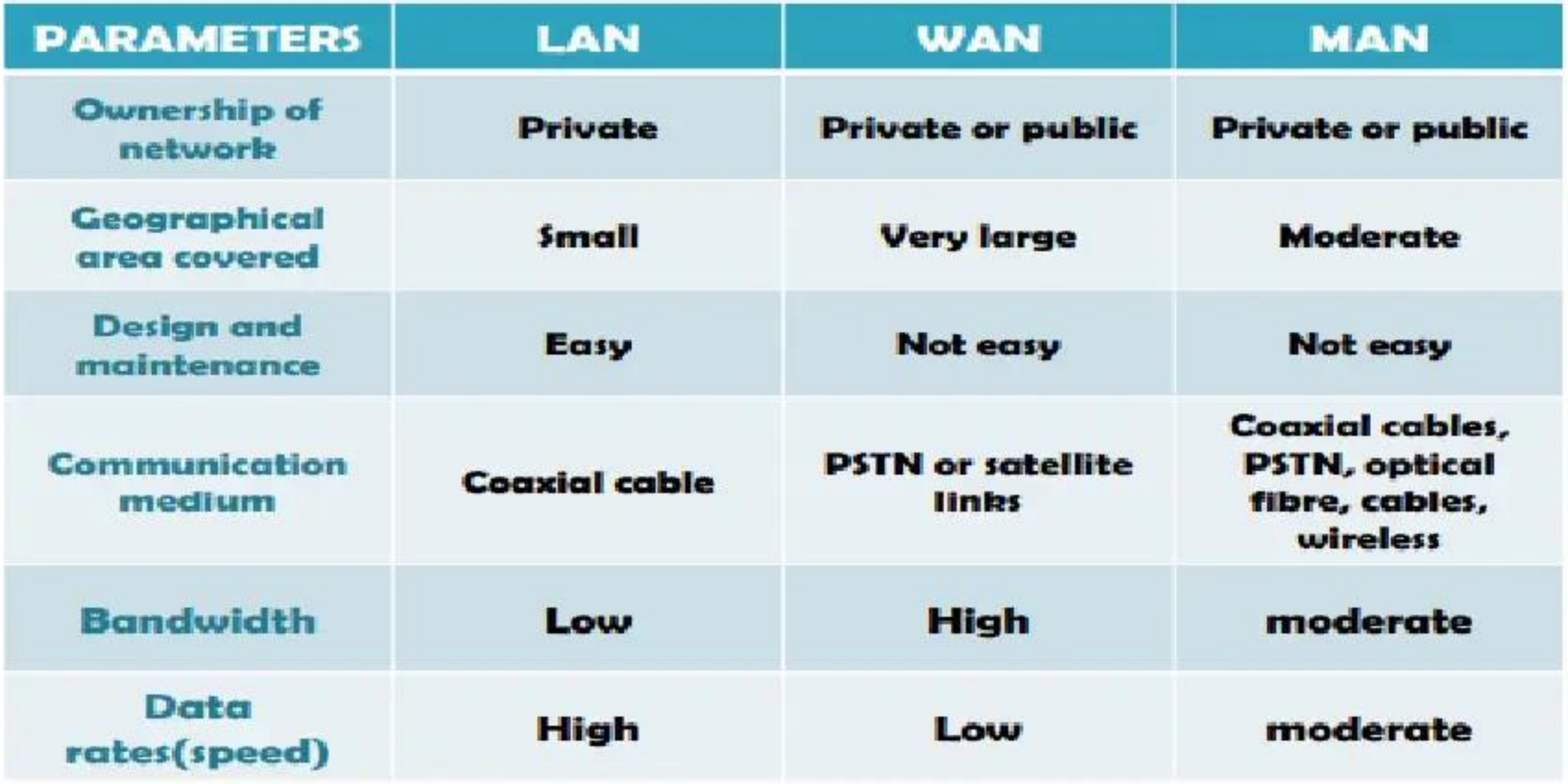
- Peer-to-peer networks are ideal for small organizations (fewer than ten users) where security is not of concern.

- Peer-to-peer networks also provide a decentralized alternative for situations in which server administration would be too large or complex a task.

The following, are designed to implement peer-to-peer networking models:

- Novell Personal NetWare
- AppleTalk (the networking system for Apple Macintosh computers)
- Artisoft LANtastic

LAN,MAN and WAN



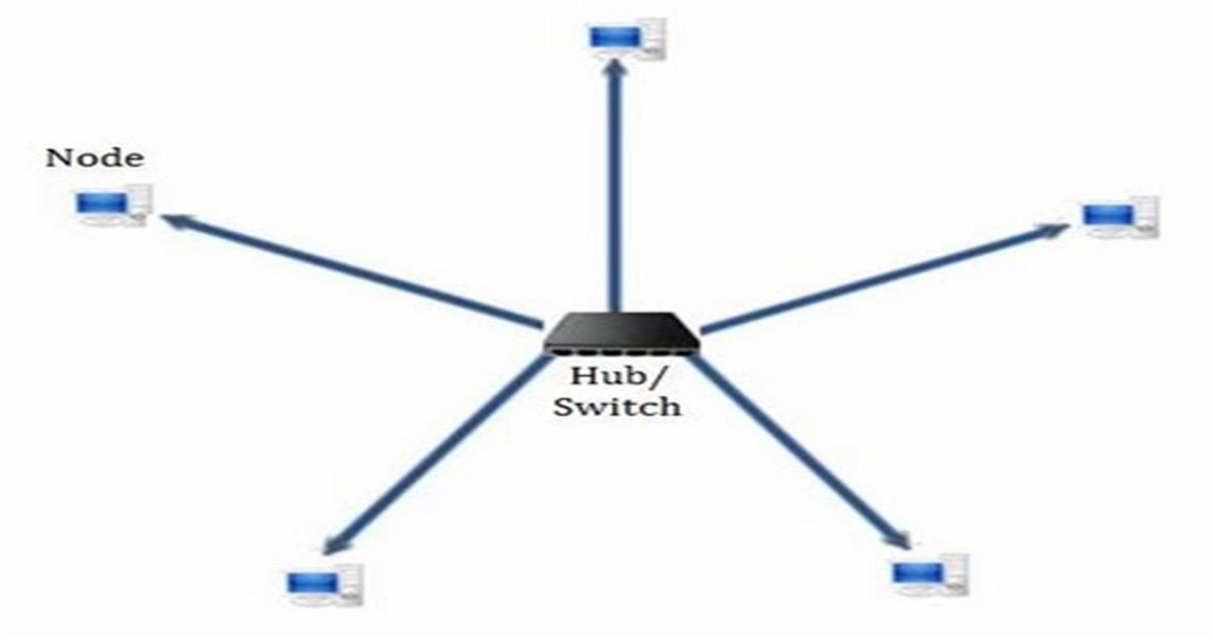
PARAMETERS	LAN	WAN	MAN
Ownership of network	Private	Private or public	Private or public
Geographical area covered	Small	Very large	Moderate
Design and maintenance	Easy	Not easy	Not easy
Communication medium	Coaxial cable	PSTN or satellite links	Coaxial cables, PSTN, optical fibre, cables, wireless
Bandwidth	Low	High	moderate
Data rates(speed)	High	Low	moderate

Topology

- The physical or logical way to connect computers is called topology.
  - **Ring topology**
  - **Star topology** **Bus topology** A bus technology called **Ethernet** has become the industry standard for local-area networks

Star topology

A configuration that centers around one node to which all others are connected and through which all messages are sent



Advantages of star topology

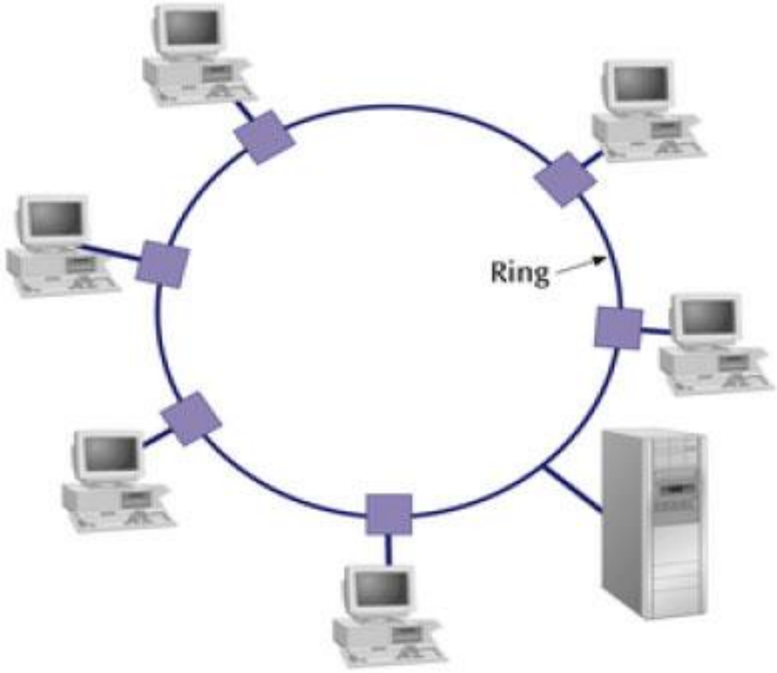
1) Compared to Bus topology it gives far much better performance
2) Easy to connect new nodes or devices
3) Centralized management. It helps in monitoring the network
4) Failure of one node or link doesn’t affect the rest of network

Disadvantages of star topology

1) If central device fails whole network goes down
2) The use of hub, a router or a switch as central device increases the overall cost of the network
3) Performance and as well number of nodes which can be added in such topology is depended on capacity of central device

Ring topology

A configuration that connects all nodes in a closed loop on which messages travel in one direction



Advantages of Ring topology

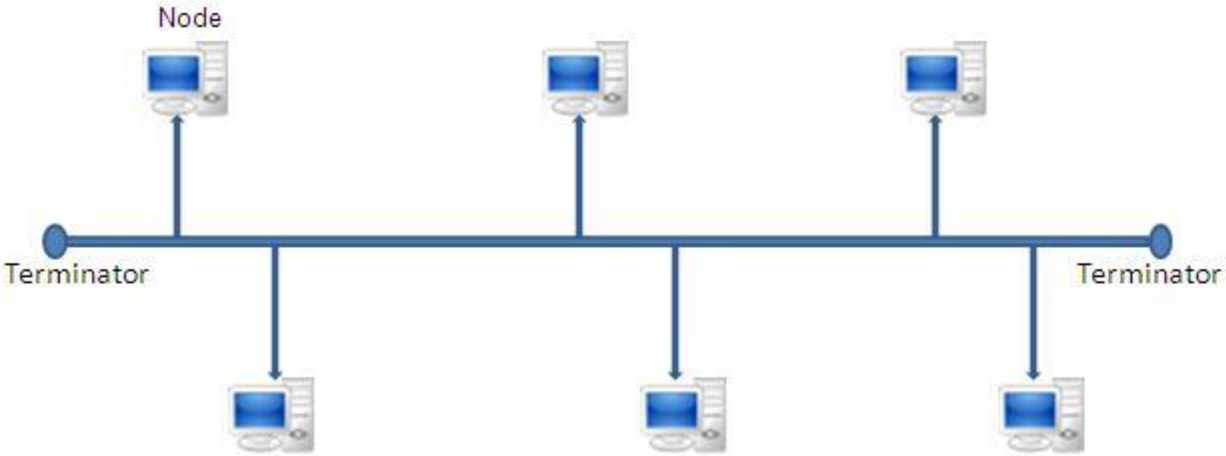
- This type of network topology is very organized
- Performance is better than that of Bus topology
- No need for network server to control the connectivity between workstations
- Additional components do not affect the performance of network
- Each computer has equal access to resources

Disadvantages of Ring topology

- Each packet of data must pass through all the computers between source and destination, slower than star topology
- If one workstation or port goes down, the entire network gets affected
- Network is highly dependent on the wire which connects different components

Bus topology

All nodes are connected to a single communication line that carries messages in both directions



Advantages of Bus topology

- Easy to implement and extend
- Well suited for temporary networks that must be set up in a hurry
- Typically the least cheapest topology to implement
- Failure of one station does not affect others

Disadvantages of Bus topology

- Difficult to administer/troubleshoot
- Limited cable length and number of stations
- A cable break can disable the entire network; no redundancy
- Maintenance costs may be higher in the long run
- Performance degrades as additional computers are added

Switching Techniques

In large networks there might be multiple paths linking sender and receiver. Information may be switched as it travels through various communication channels. There are three typical switching techniques available for digital traffic.

- Circuit Switching
- Message Switching
- Packet Switching

Circuit Switching

- **Circuit switching** is a technique that directly connects the sender and the receiver in an unbroken path.
- Telephone switching equipment, for example, establishes a path that connects the caller's telephone to the receiver's telephone by making a physical connection.
- In this type of switching technique, once a connection is established, a dedicated path exists between both ends until the connection is terminated.
- Routing decisions must be made when the circuit is first established, but decisions cannot be made after that time.

Circuit Switching

- **Circuit switching** networks operate almost the same way as the telephone system works.
- A complete end-to-end path must exist before communication can take place.
- The computer initiating the data transfer must ask for a connection to the destination.
- Before the establishment of the connection, the destination must send the acknowledge to the source node to indicate that it is ready and willing to send/receive data.

Circuit switching

Advantages:

- The communication channel (once established) is dedicated.

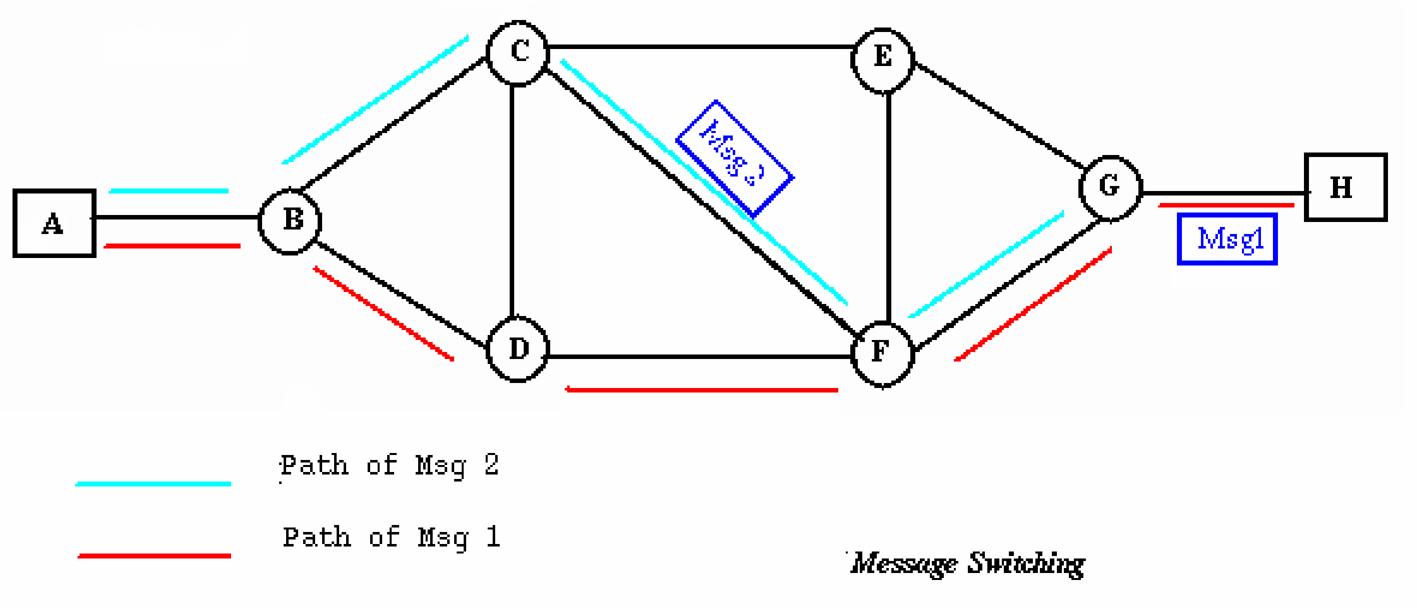
Disadvantages:

- Possible long wait to establish a connection, (10 seconds, more on long- distance or international calls.) during which no data can be transmitted.
- More expensive than any other switching techniques, because a dedicated path is required for each connection.
- Inefficient use of the communication channel, because the channel is not used when the connected systems are not using it.

Message Switching

- In message switching there is no need to establish a dedicated path between two stations.
- When a station sends a message, the destination address is appended to the message.
- The message is then transmitted through the network, in its entirety, from node to node.
- Each node receives the entire message, stores it in its entirety on disk, and then transmits the message to the next node.
- This type of network is called a store-and-forward network.

Message Switching



A message-switching node is typically a general-purpose computer. The device needs sufficient secondary-storage capacity to store the incoming messages, which could be long. A time delay is introduced using this type of scheme due to store- and-forward time, plus the time required to find the next node in the transmission path.

Message Switching

Advantages:

- Channel efficiency can be greater compared to circuit-switched systems, because more devices are sharing the channel.
- Traffic congestion can be reduced, because messages may be temporarily stored in route.
- Message priorities can be established due to store-and-forward technique.
- Message broadcasting can be achieved with the use of broadcast address appended in the message.

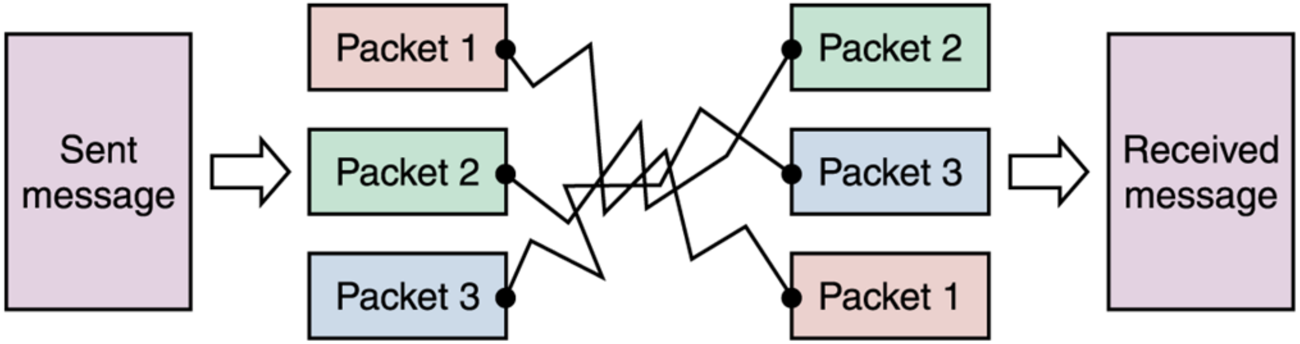
Message Switching

Disadvantages

- Message switching is not compatible with interactive applications.
- Store-and-forward devices are expensive, because they must have large disks to hold potentially long messages.

Packet Switching

- *Packet switching* can be seen as a solution that tries to combine the advantages of message and circuit switching and to minimize the disadvantages of both.
- There are two methods of packet switching: Datagram and virtual circuit.



Message is divided into packets

Packets are sent over the Internet by the most expedient route

Packets are reordered and then reassembled

Packet Switching

- In both packet switching methods, a message is broken into small parts, called packets.
- Each packet is tagged with appropriate source and destination addresses.
- Since packets have a strictly defined maximum length, they can be stored in main memory instead of disk, therefore access delay and cost are minimized.
- Also the transmission speeds, between nodes, are optimized.
- With current technology, packets are generally accepted onto the network on a first-come, first-served basis. If the network becomes overloaded, packets are delayed or discarded (“dropped'').

Advantages of packet switching

Advantages:

- Packet switching is cost effective, because switching devices do not need massive amount of secondary storage.
- Packet switching offers improved delay characteristics, because there are no long messages in the queue (maximum packet size is fixed).
- Packet can be rerouted if there is any problem, such as, busy or disabled links.
- The advantage of packet switching is that many network users can share the same channel at the same time. Packet switching can maximize link efficiency by making optimal use of link bandwidth.

Disadvantages of packet switching

Disadvantages:

- Protocols for packet switching are typically more complex.
- It can add some initial costs in implementation.
- If packet is lost, sender needs to retransmit the data.
- Another disadvantage is that packet-switched systems still can’t deliver the same quality as dedicated circuits in applications requiring very little delay - like voice conversations or moving images.

Network Services

Some basic services computer network can offer are:

- Directory Services
- File Services
- Communication Services
- Application Services

Directory Services

- These services are mapping between name and its value, which can be variable value or fixed. This software system helps to store the information, organize it, and provides various means of accessing it.

✓ Accounting

✓ Authentication and Authorization

✓ Domain Name Services

File Services

File services include sharing and transferring files over the network.

- File Sharing
- File Transfer

Communication Services

- Email
- Social Networking
- Internet Chat
- Discussion Boards
- Remote Access

Application Services

- Resource Sharing
- Databases
- Web Services

UNIT-2

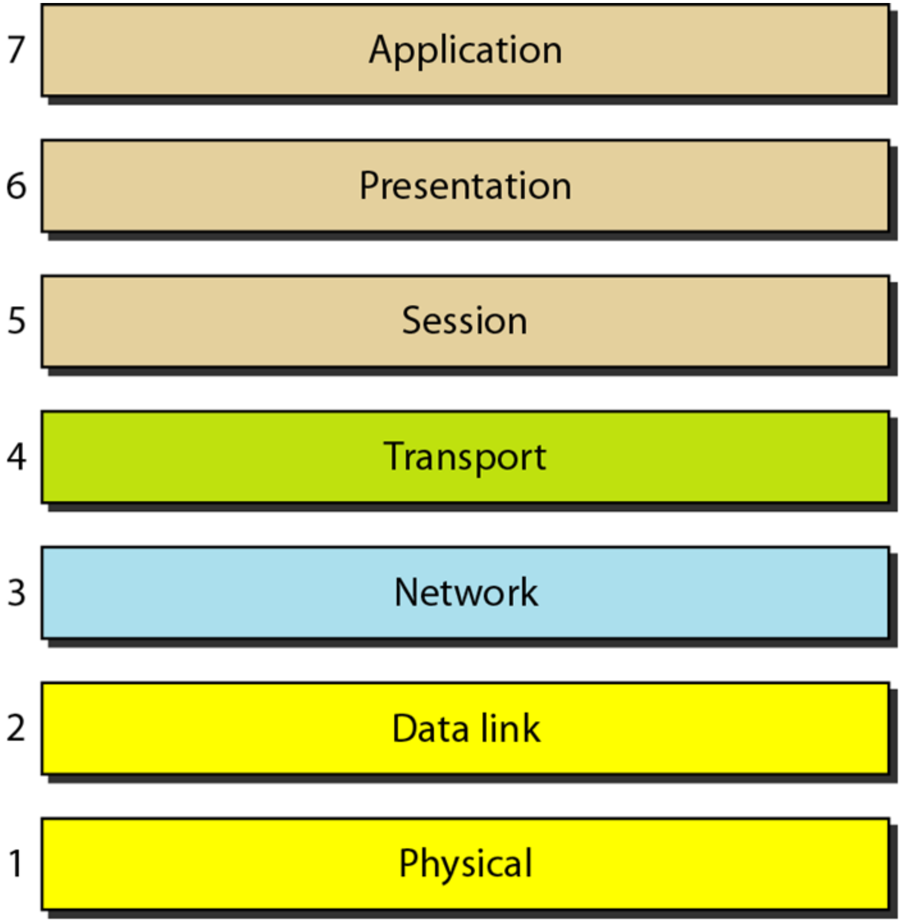
NETWORKING MODELS

OSI MODEL

- Definition : *Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.*

Layered Architecture

- *Seven layers of the OSI model*



7 Application

6 Presentation

5 Session

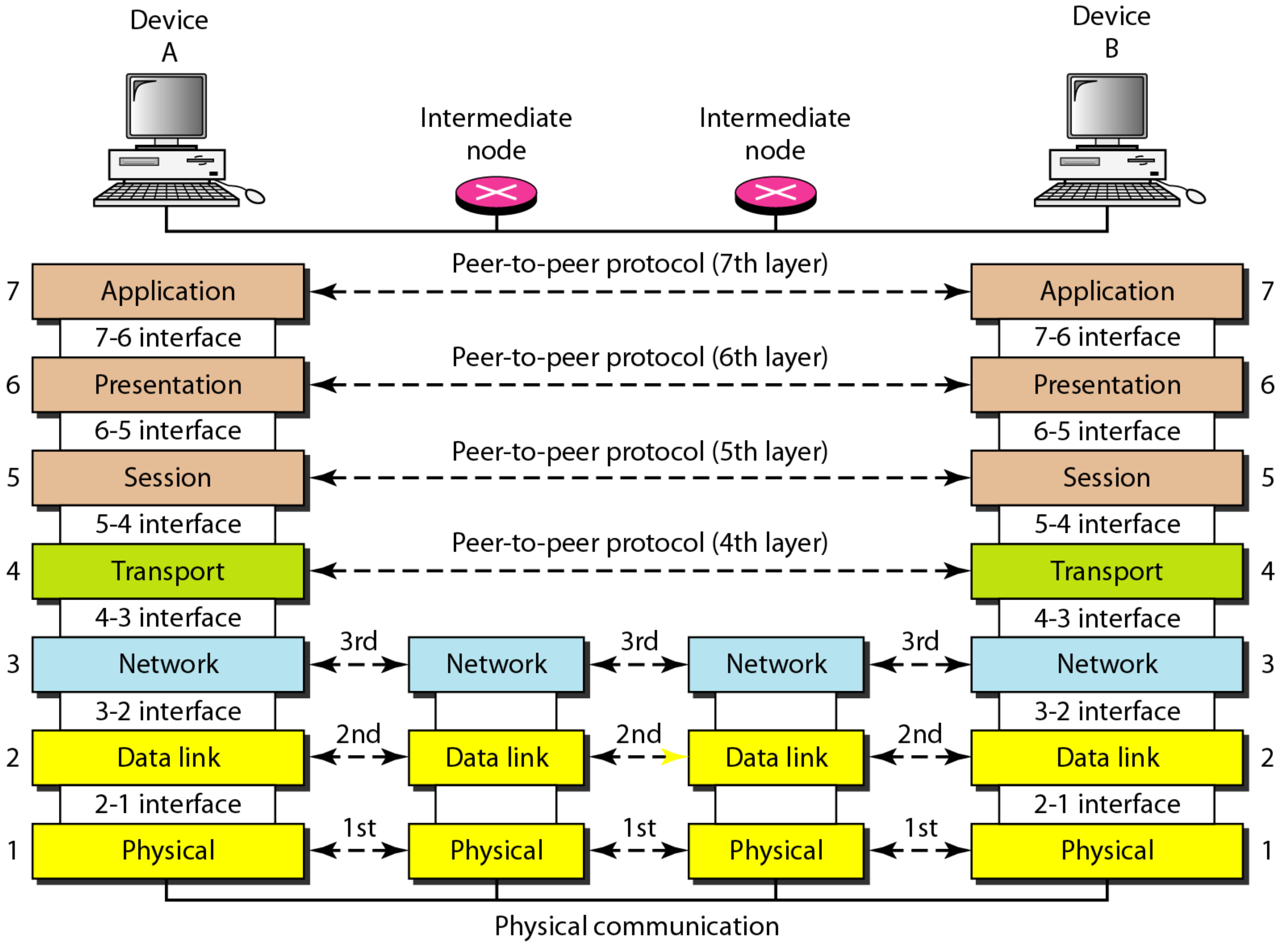
4 Transport

3 Network

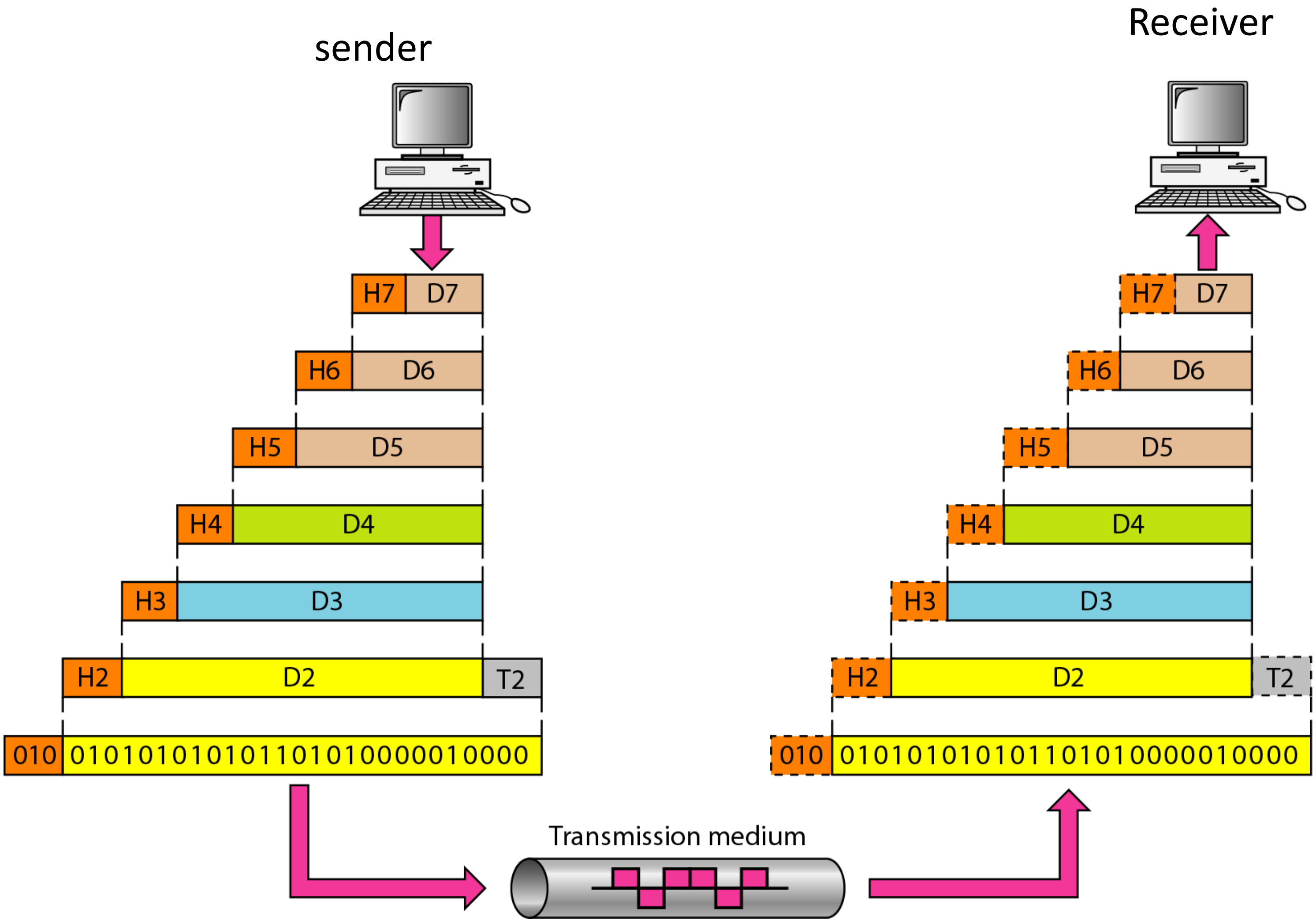
2 Data link

1 Physical

The interaction between layers in the OSI model



An exchange using the OSI model



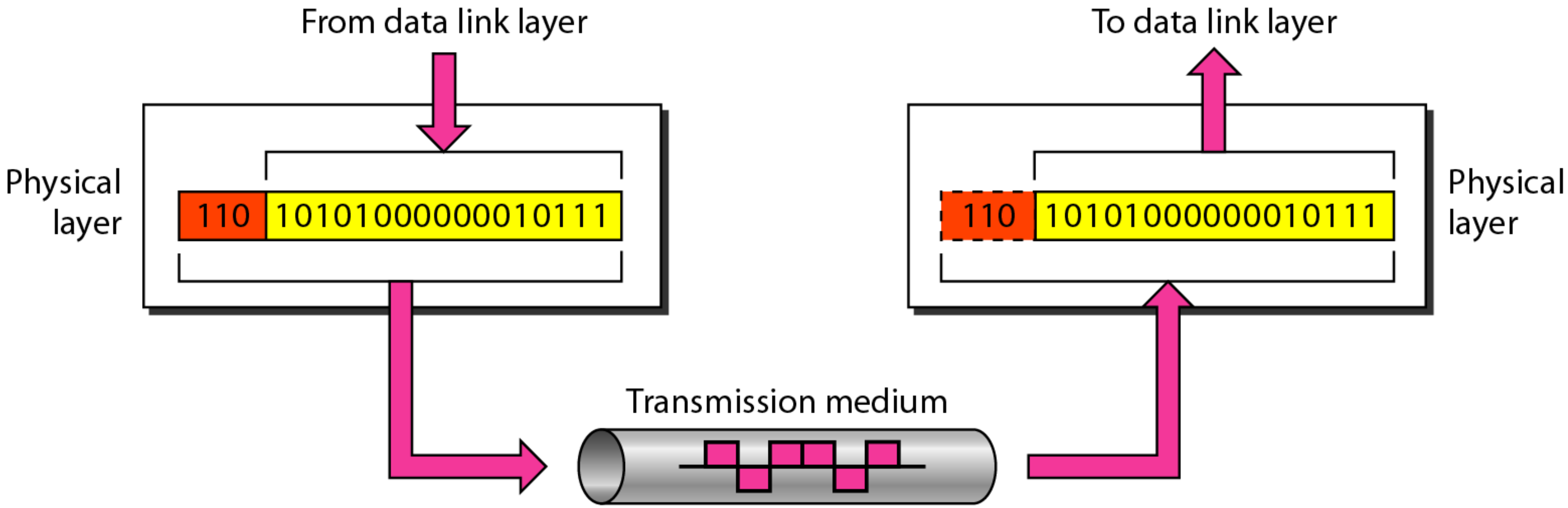
LAYERS IN THE OSI MODEL

- There are seven layers in OSI Model

- ➢ Physical Layer
- ➢ Data Link Layer
- ➢ Network Layer
- ➢ Transport Layer
- ➢ Session Layer
- ➢ Presentation Layer
- ➢ Application Layer

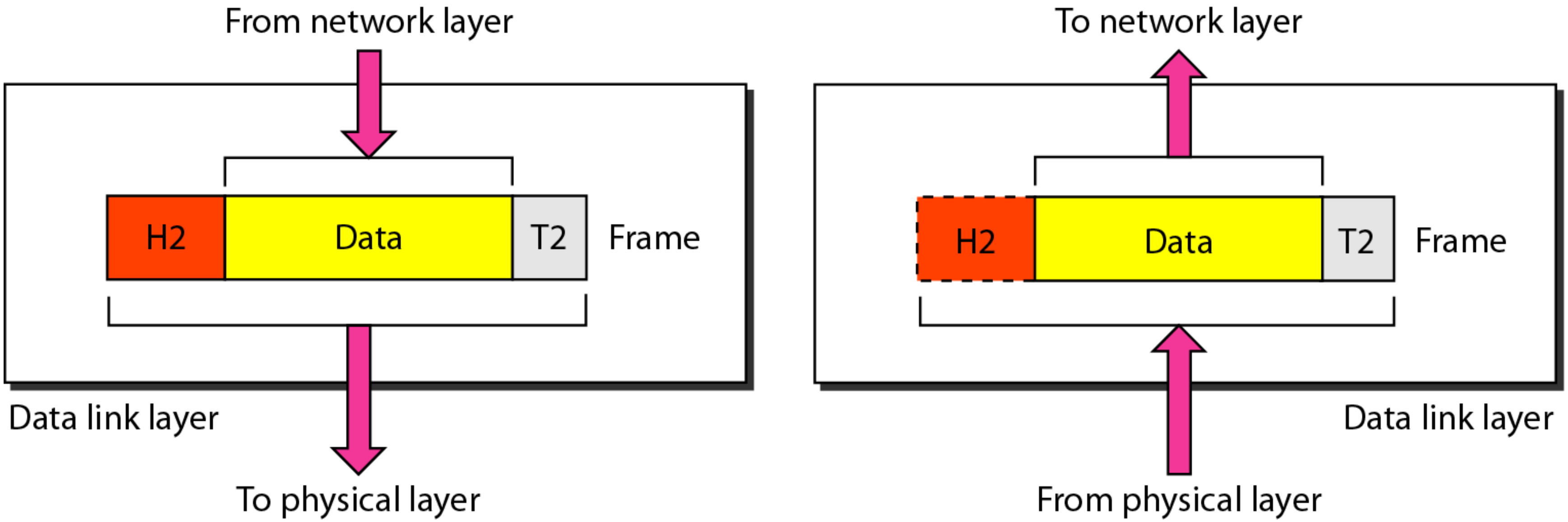
Physical Layer

The function of physical layer is to move individual bits from one hop (node) to the next.



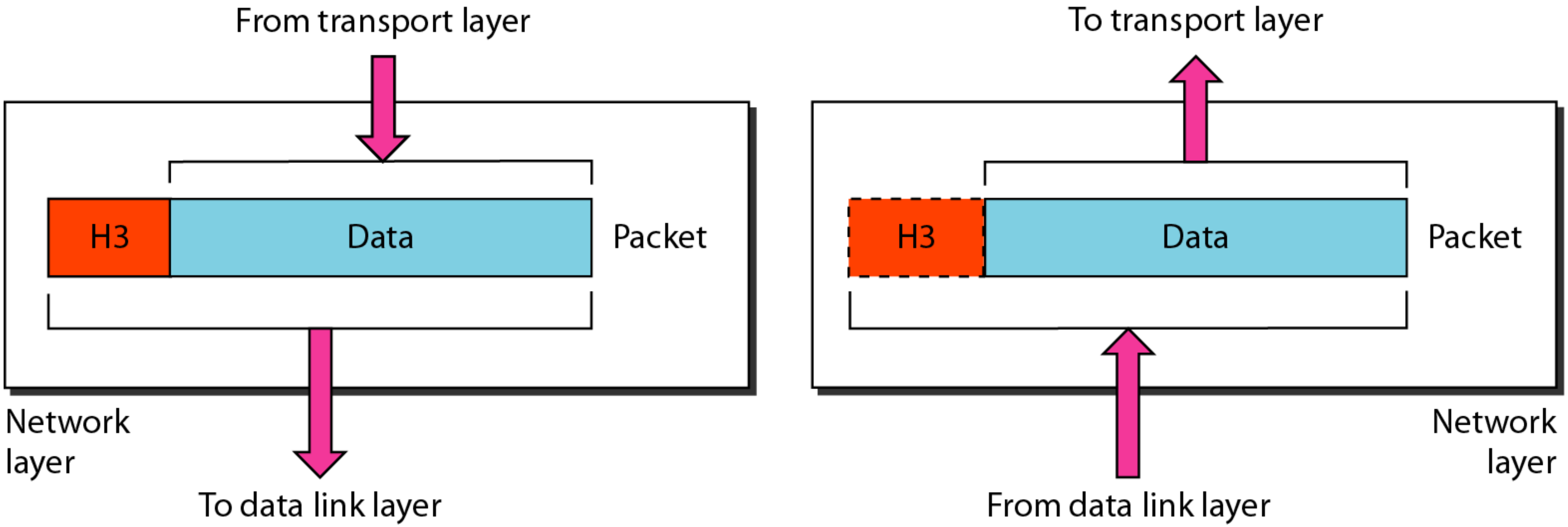
Data link layer

The data link layer is responsible for moving frames from one hop (node) to the next.



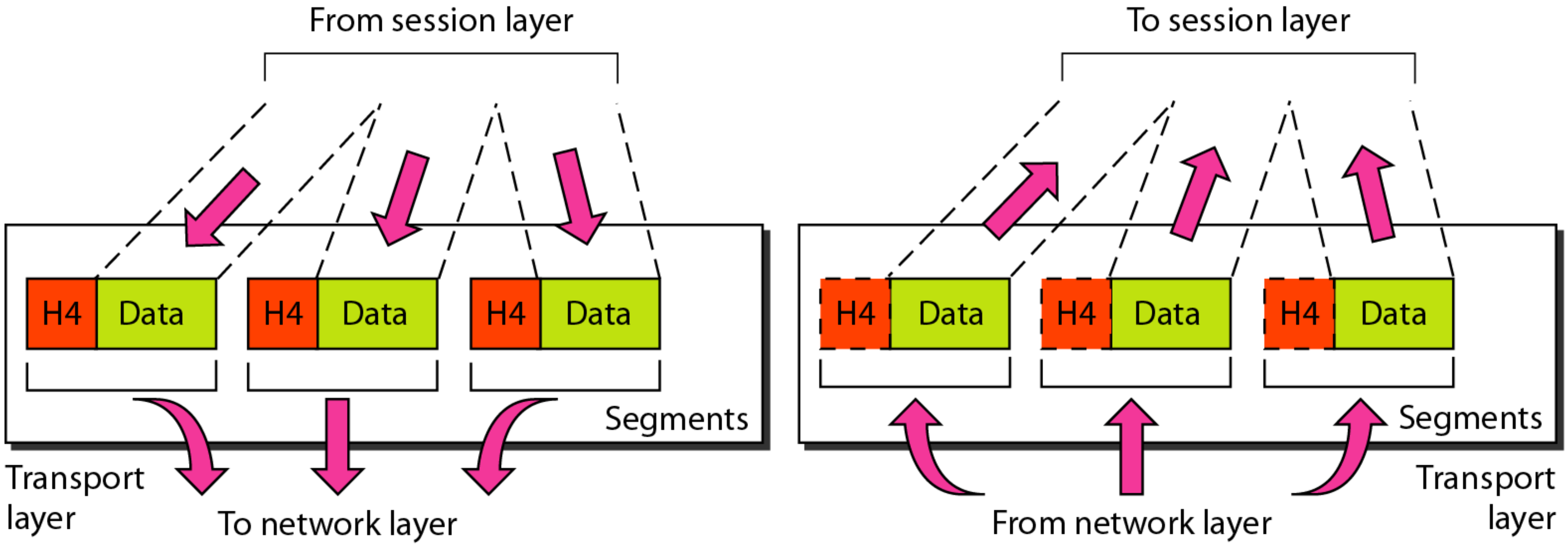
Network layer

The network layer is responsible for the delivery of individual packets from the source host to the destination host.



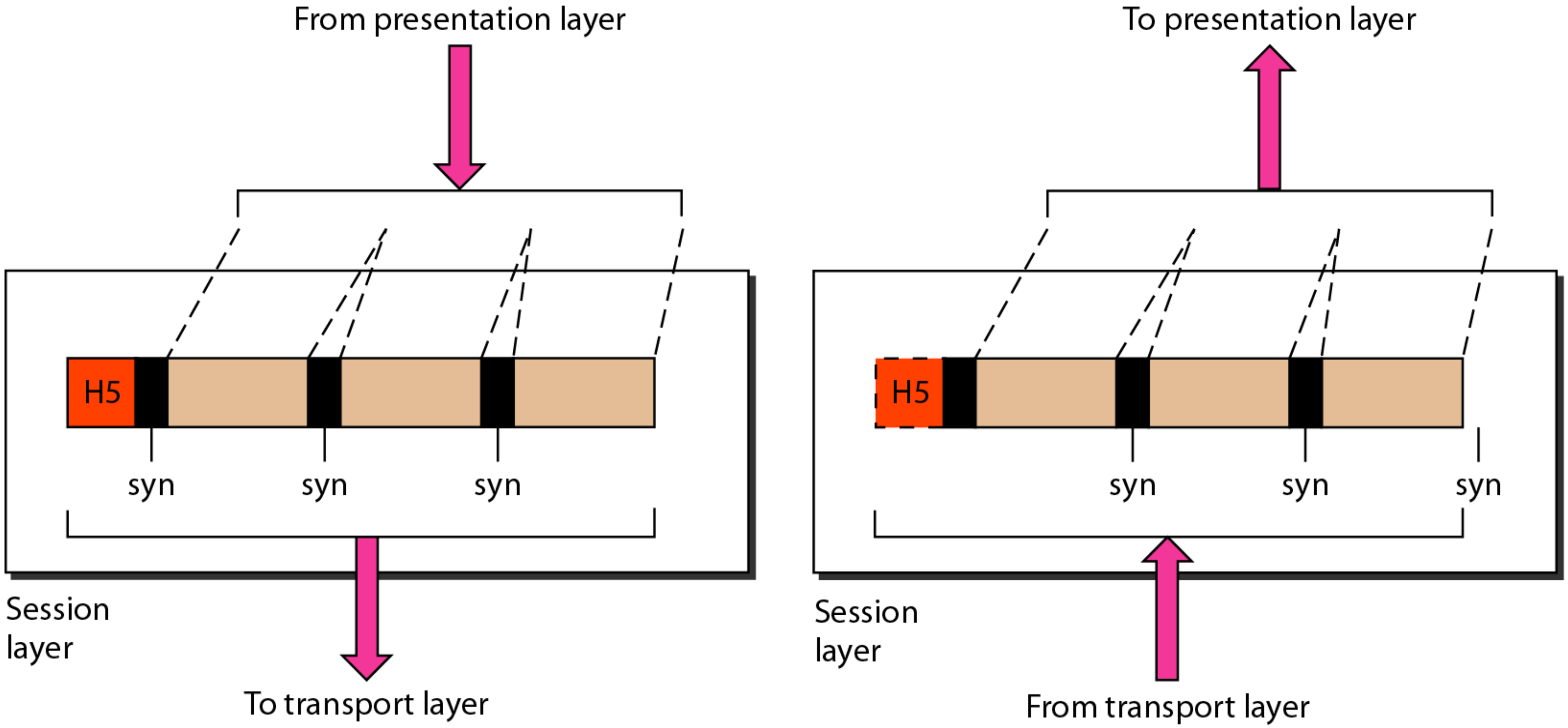
Transport layer

The transport layer is responsible for the delivery of a message from one process to another.



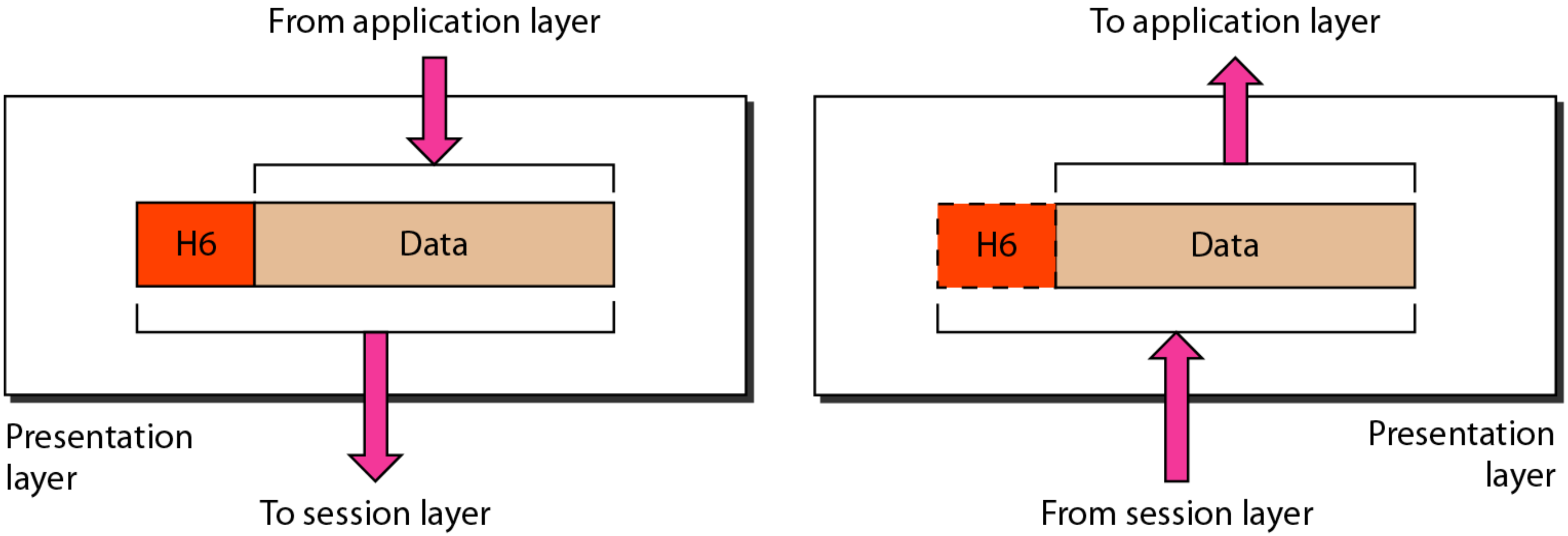
Session layer

The session layer is responsible for dialog control and synchronization.



Presentation layer

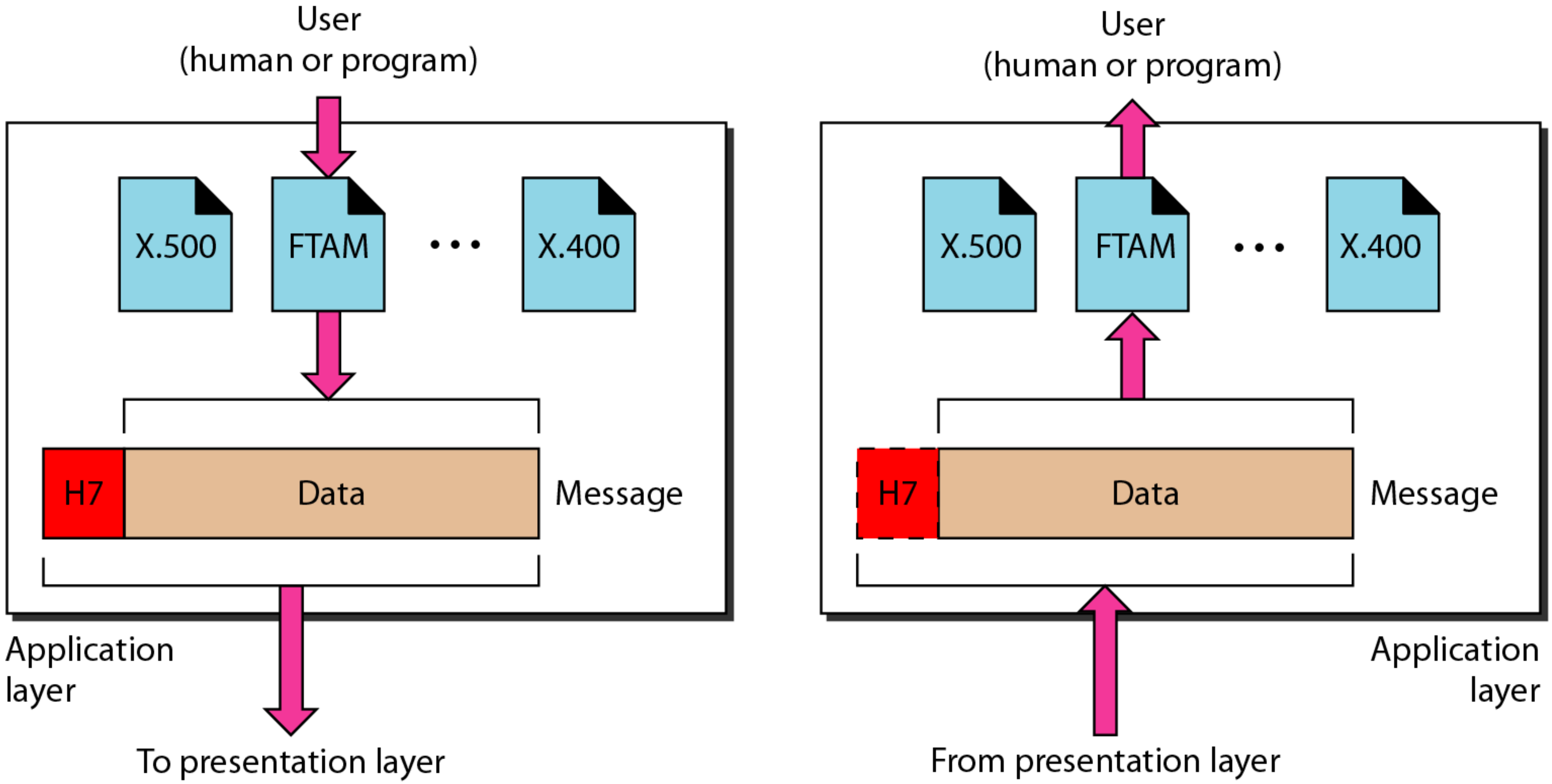
The presentation layer is responsible for translation, compression, and encryption.



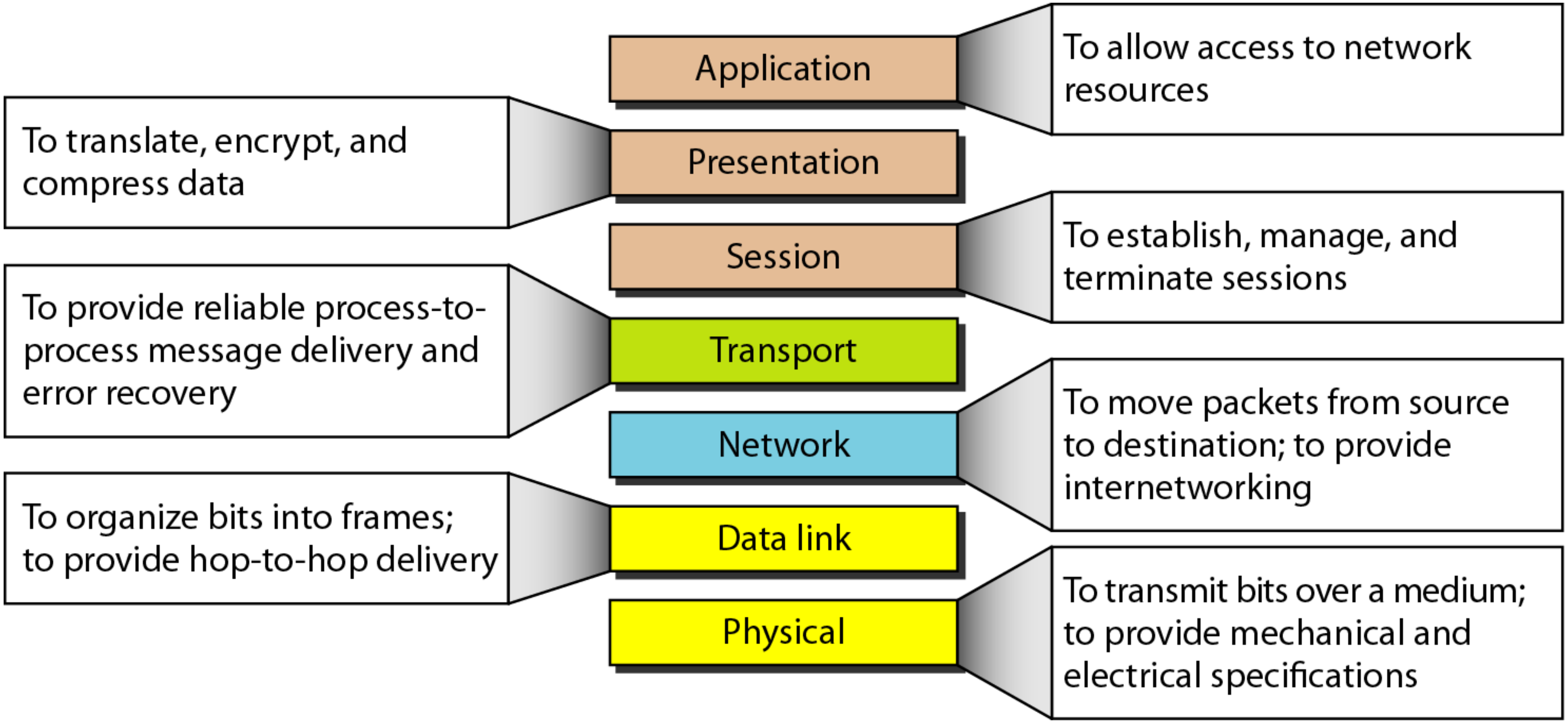
Application layer

The application layer is responsible for providing services to the user.

.



Summary

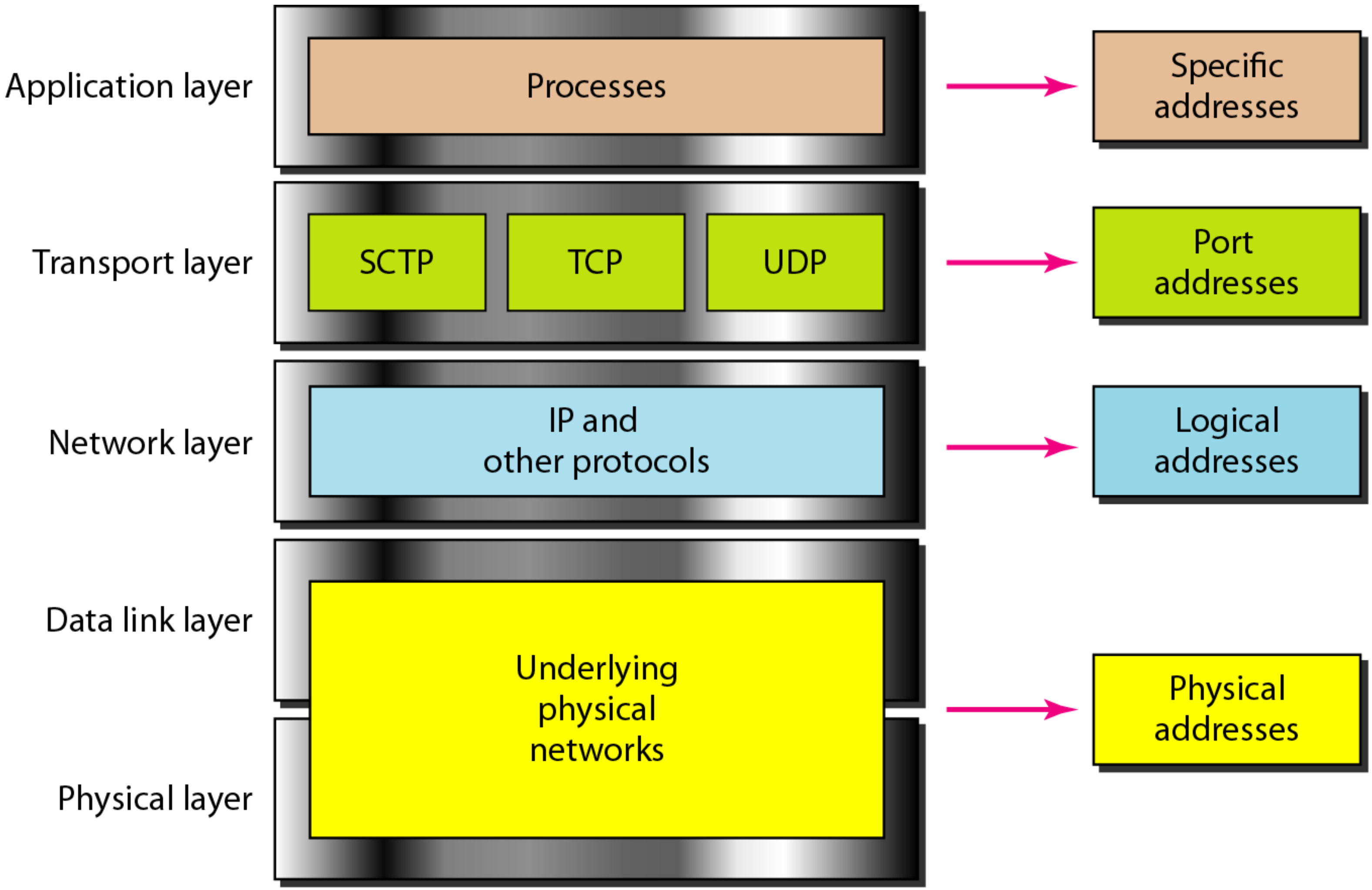

Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

TCP/IP Model

- *The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.*

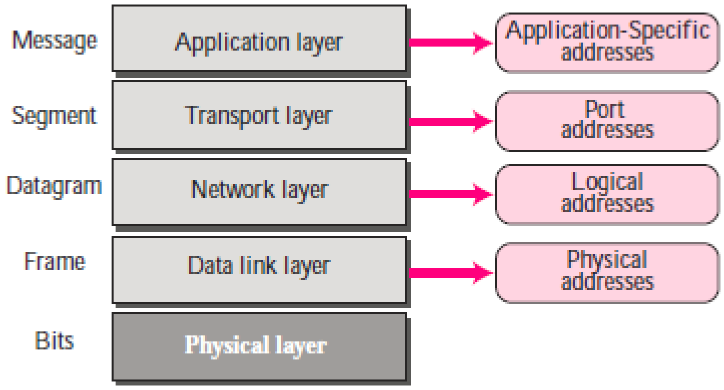
There are four layers in TCP/IP Model.

- Physical and Data Link Layers
- Network Layer
- Transport Layer
- Application Layer


Application layer
Processes
Specific addresses
Transport layer
SCTP
TCP
UDP
Port addresses
Network layer
IP and other protocols
Logical addresses
Data link layer
Underlying physical networks
Physical addresses
Physical layer

ADDRESSING

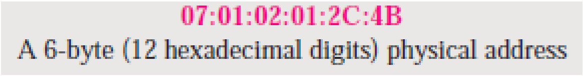
Four levels of addresses are used in an internet employing the TCP/IP protocols: physical address, logical address, port address, and application-specific address. Each address is related to a one layer in the TCP/IP architecture, as shown in the following Figure.



Physical Addresses

The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level address. The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC).

Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below.



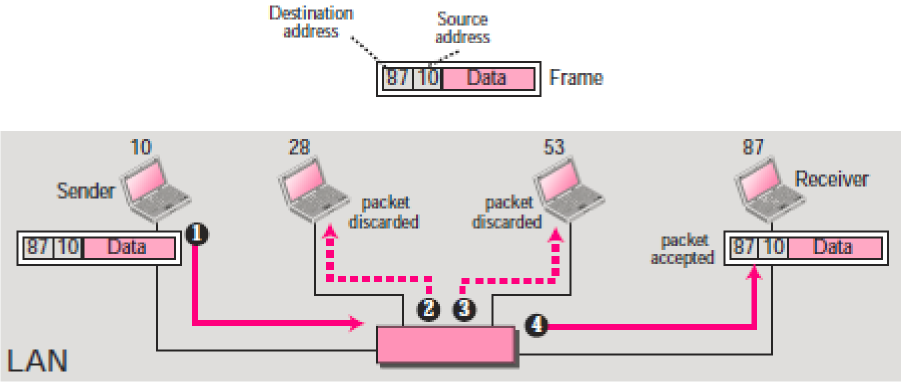
07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address

Example (1)

In Figure below a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (a LAN). At the data link layer, this frame contains physical (link) addresses in the header. These are the only addresses needed. The rest of the header contains other information needed at this level. The trailer usually contains extra bits needed for error detection. The data link layer at the sender receives data from an upper layer. It encapsulates the data in a frame, adding a header and a trailer. The header, among other pieces of information, carries the receiver and the sender physical (link) addresses.

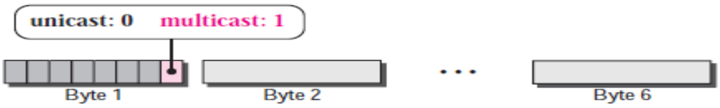
Note that in most data link protocols, the destination address 87 in this case, comes before the source address (10 in this case). The frame is propagated through the LAN. Each station with a physical address other than 87 drops the frame because the destination address in the frame does not match its own physical address. The intended destination computer, however, finds a match between the destination address in the frame and its own physical address. The frame is checked, the header and trailer are dropped, and the data part is decapsulated and delivered to the upper layer.



Unicast, Multicast, and Broadcast Physical Addresses

Physical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (to be received by all systems in the network). Some networks support all three addresses.

A source address is always a unicast address—the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast. The least significant bit of the first byte defines the type of address.



Q: Define the type of the following destination addresses:

1. 4A:30:10:21:10:1A
2. 47:20:1B:2E:08:EE
3. FF:FF:FF:FF:FF:FF

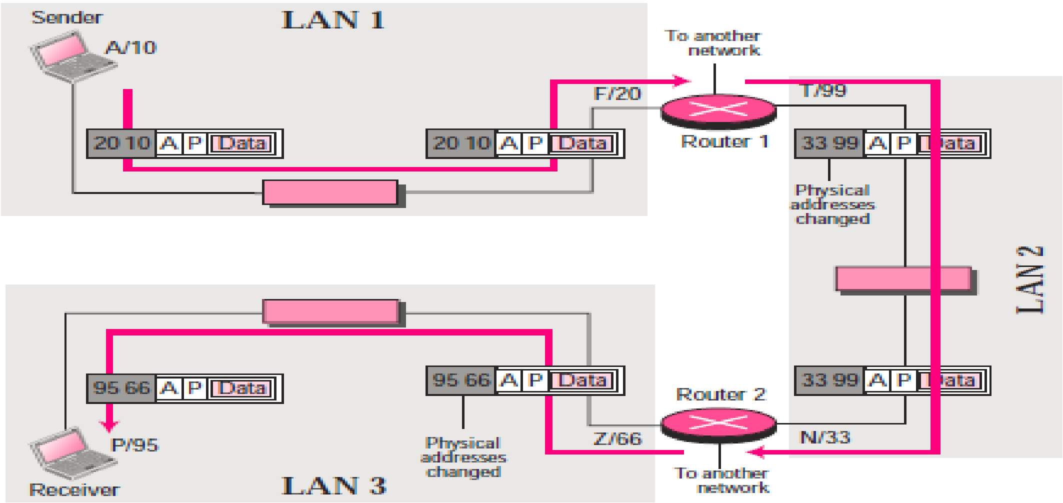
Logical Addresses

Logical addresses are necessary for universal communications that are independent of underlying physical networks. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address.

Example (2)

The Figure below shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection. Although it may be obvious that each router must have a separate physical address for each connection, it may. The computer with logical address

A and physical address **10** needs to send a packet to the computer with logical address **P** and physical address **95**. The sender encapsulates its data in a packet at the network layer and adds two logical addresses (A and P). Note that in most protocols, the logical source address comes before the logical destination address (contrary to the order of physical addresses). The network layer, however, needs to find the physical address of the next hop before the packet can be delivered. The network layer consults its routing table and finds the logical address of the next hop (router 1) to be F.



Another protocol, Address Resolution Protocol (ARP) finds the physical address of router 1 that corresponds to its logical address (20). Now the network layer passes this address to the data link layer, which in turn, encapsulates the packet with physical destination address 20 and physical source address 10. The router decapsulates the packet from the frame to read the logical destination address P. Since the logical destination address does not match the router's logical address, the router knows that the packet needs to be forwarded. The router consults its routing table and ARP to find the physical destination address of the next hop (router 2), creates a new frame, encapsulates the packet, and sends it to router 2.

Note the physical addresses in the frame. The source physical address changes from 10 to 99. The destination physical address changes from 20 (router 1 physical address) to 33 (router 2 physical address). The logical source and destination addresses must remain the same; otherwise the packet will be lost. At router 2 we have a similar scenario. The physical addresses are changed, and a new frame is sent to the destination computer. When the frame reaches the destination, the packet is decapsulated. The destination logical address P matches the logical address of the computer. The data are decapsulated from the packet and delivered to the upper layer. Note that although physical addresses will change from hop to hop, logical addresses remain the same from the source to destination.

**The physical addresses will change from hop to hop,
but the logical addresses remain the same.**

Unicast, Multicast, and Broadcast Addresses

The logical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (all systems in the network).

Port Addresses

The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet. Computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process. For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes.

In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a port address. A port address in TCP/IP is 16 bits in length.

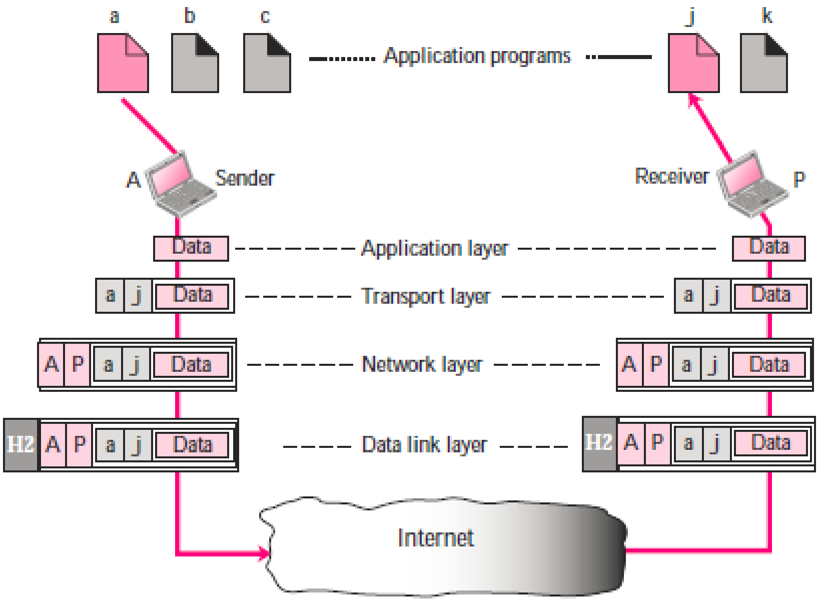
A port address is a 16-bit address represented by one decimal number as shown.

753

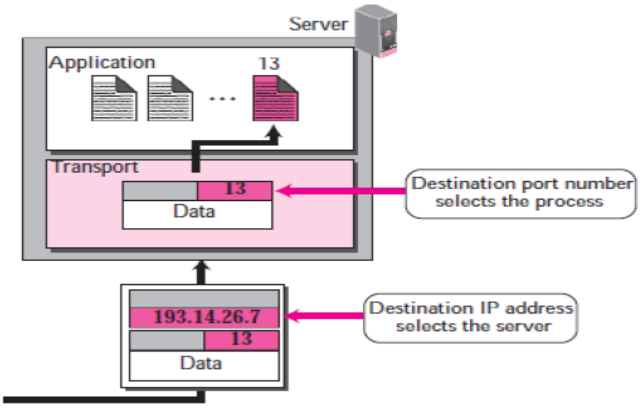
A 16-bit port address represented as one single number

Example (3)

The following Figure shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses **a**, **b**, and **c**. The receiving computer is running two processes at this time with port addresses **j** and **k**. Process **a** in the sending computer needs to communicate with process **j** in the receiving computer. Note that although both computers are using the same application, FTP, for example, the port addresses are different because one is a client program and the other is a server program.



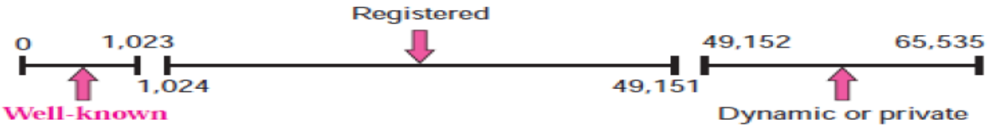
To show that data from process **a** need to be delivered to process **j**, and not **k**, the transport layer encapsulates data from the application layer in a packet and adds two port addresses (**a** and **j**), source and destination. The packet from the transport layer is then encapsulated in another packet at the network layer with logical source and destination addresses (**A** and **P**). Finally, this packet is encapsulated in a frame with the physical source and destination addresses of the next hop. We have not shown the physical addresses because they change from hop to hop inside the cloud designated as the Internet. Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.


Server
Application
13
Transport
13
Data
Destination port number selects the process
193.14.26.7
13
Data
Destination IP address selects the server

- In the TCP/IP protocol suite, the port numbers are integers between 0 and 65,535.
- The client program defines itself with a port number, called the **ephemeral port number** (chosen randomly). The word ephemeral means *short lived*.
- The server process must also define itself with a port number (called well-known port numbers). This port number, however, cannot be chosen randomly.

ICANN Ranges (Internet Corporation for Assigned Names and Numbers)

ICANN has divided the port numbers into three ranges: well-known, registered, and dynamic (or private)



- **Well-known ports:** The ports ranging from 0 to 1,023 are assigned and controlled by ICANN..
- **Registered ports:** The ports ranging from 1,024 to 49,151 are not assigned or controlled by ICANN. They can only be registered with ICANN to prevent duplication.
- **Dynamic ports:** The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used as temporary or private port numbers. The original recommendation was that the ephemeral port numbers for clients be chosen from this range. However, most systems do not follow this recommendation.

Application-Specific Addresses

Some applications have user-friendly addresses that are designed for that specific application. Examples include the e-mail address (for example, co_sci@yahoo.com) and the Universal Resource Locator (URL) (for example, www.mhhe.com). The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web. These addresses, however, get changed to the corresponding port and logical addresses by the sending computer.

Network Layer (3): Subnetting

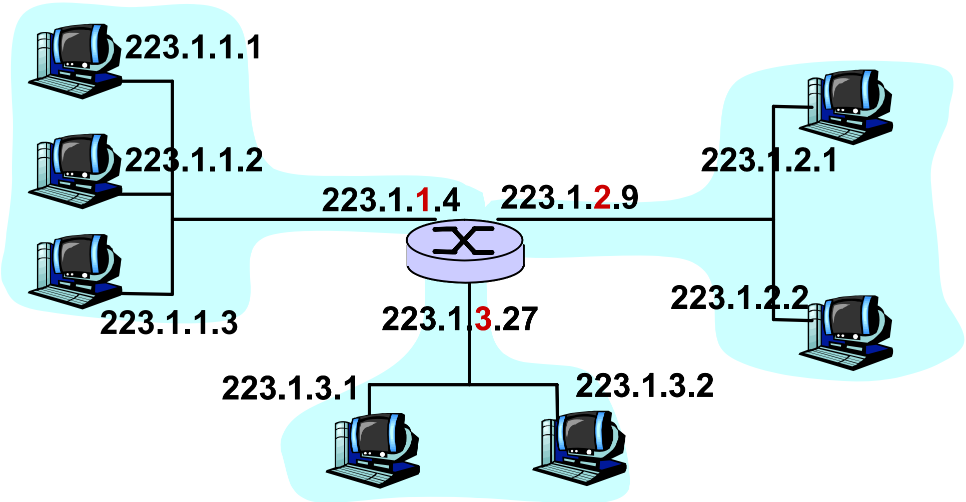
Required reading:
Kurose 4.4.2

CSE 4213, Fall 2006
Instructor: N. Vlajic

IP Addressing

Internetwork Address – uniquely and universally identifies each device connected to the (inter)network

- **IP Address**: 32-bit (4-byte) binary address that identifies a host / router interface to the Internet
- two devices on the Internet can never have the same address at the same time;
  but, a single device can have two IP addresses if it is connected to the Internet via two networks
- routers typically have multiple interfaces, i.e. IP multiple IP addresses



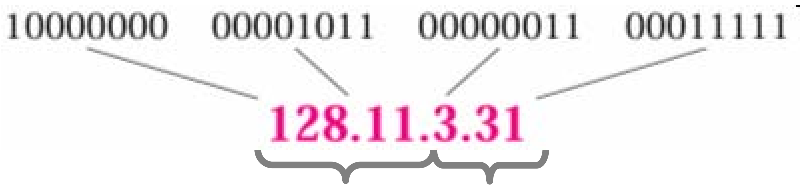
IP Addressing (cont.)

IP Address: Binary Notation – **32-bit / 4-byte representation with a space inserted between each octet (byte)**

IP Address: Decimal Notation – **4-number decimal representation with a decimal dot separating the numbers**

- **each decimal number corresponds to a byte**

  ⇒ **each decimal number $\in$ [0, 255]**



How many bits go to network and how many to host part!?

IP address = network part + host part

assigned by global authority (ICANN) to organization

assigned by local authority to particular machine

Example [IP Address Conversion]

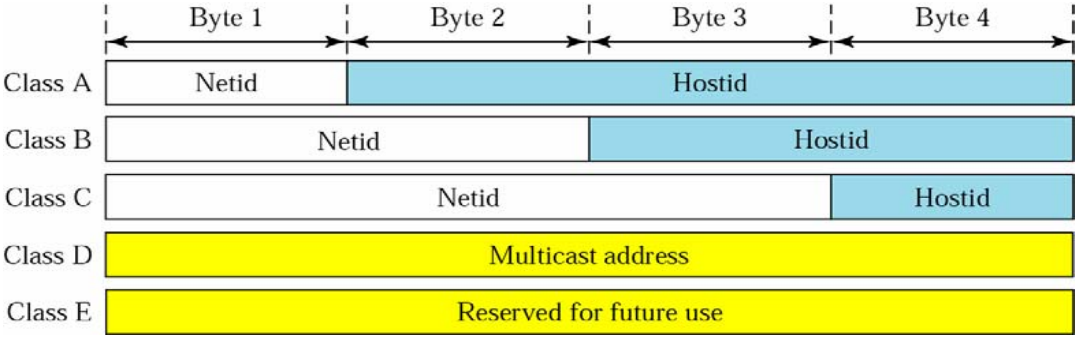
Change the following IP addresses from binary to dotted decimal notation.

(a) 10000001 00001011 00001011 11101111 ⇒ 129.11.11.239
(b) 11111001 10011011 11111011 00001111 ⇒ 249.155.251.15

Classful IP Addressing

Classful IP Addressing – supports addressing of different size networks by dividing address space into 5 classes: A, B, C, D, E (older concept of addressing, still in use)

- an IP address in classes A, B, and C is divided into **Netid** and **Hostid**
- class A addresses (1-byte Netid): get assigned to organizations with a large number of hosts or routers – there are only 126 class A networks with up to 16 million hosts in each
- class B addresses (2-byte Netid): allow around 16,000 networks and around 64,000 hosts per each network
- class C addresses (3-byte Netid): allow around 2 million networks and around 254 hosts per each network



While many class A and B addresses are wasted, the number of addresses in class C is smaller than the needs of most organizations.

How do we know if an IP address is a class-A / B or C!?

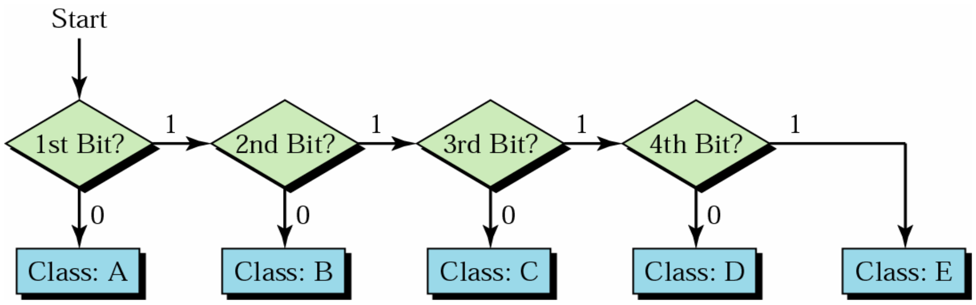
Classful IP Addressing (cont.)

Recognizing Classes

(1) Binary Notation – first few bits of an IP address in binary notation immediately identify the class of the given address

(2) Decimal Notation – each class has a specific range of numbers in decimal notation ⇒ it is enough to look at the first number to determine the class

	First byte	Second byte	Third byte	Fourth byte	
Class A	0	🟨	🟦	🟩	⇒ first byte: 0 - 127
Class B	10	🟨	🟦	🟩	⇒ first byte: 128 - 191
Class C	110	🟨	🟦	🟩	⇒ first byte: 192 - 223
Class D	1110	🟨	🟦	🟩	⇒ first byte: 224 - 239
Class E	1111	🟨	🟦	🟩	⇒ first byte: 240 - 255



Classful IP Addressing (cont.)

Example **[classes of IP Address – binary notation]**

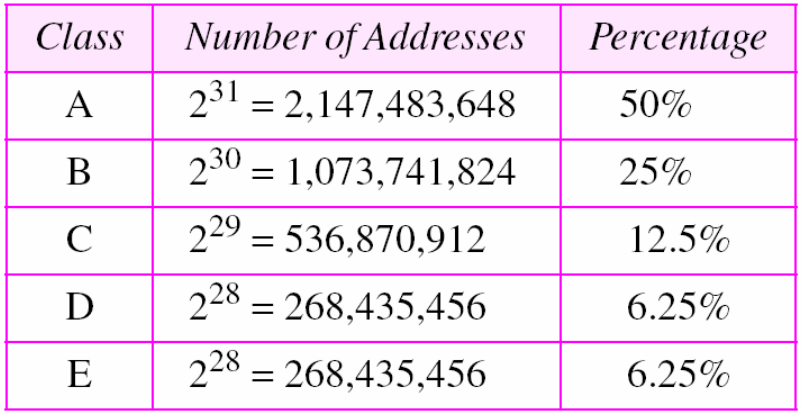
Find the class of each address:

(a) 00000001 00001011 00001011 11101111
(b) 11110011 10011011 11111011 00001111

<u>Solution</u>:

(a) The first bit is 0 ⇒ this is a class A address.
(b) The first 4 bits are 1 ⇒ this is a class E address.

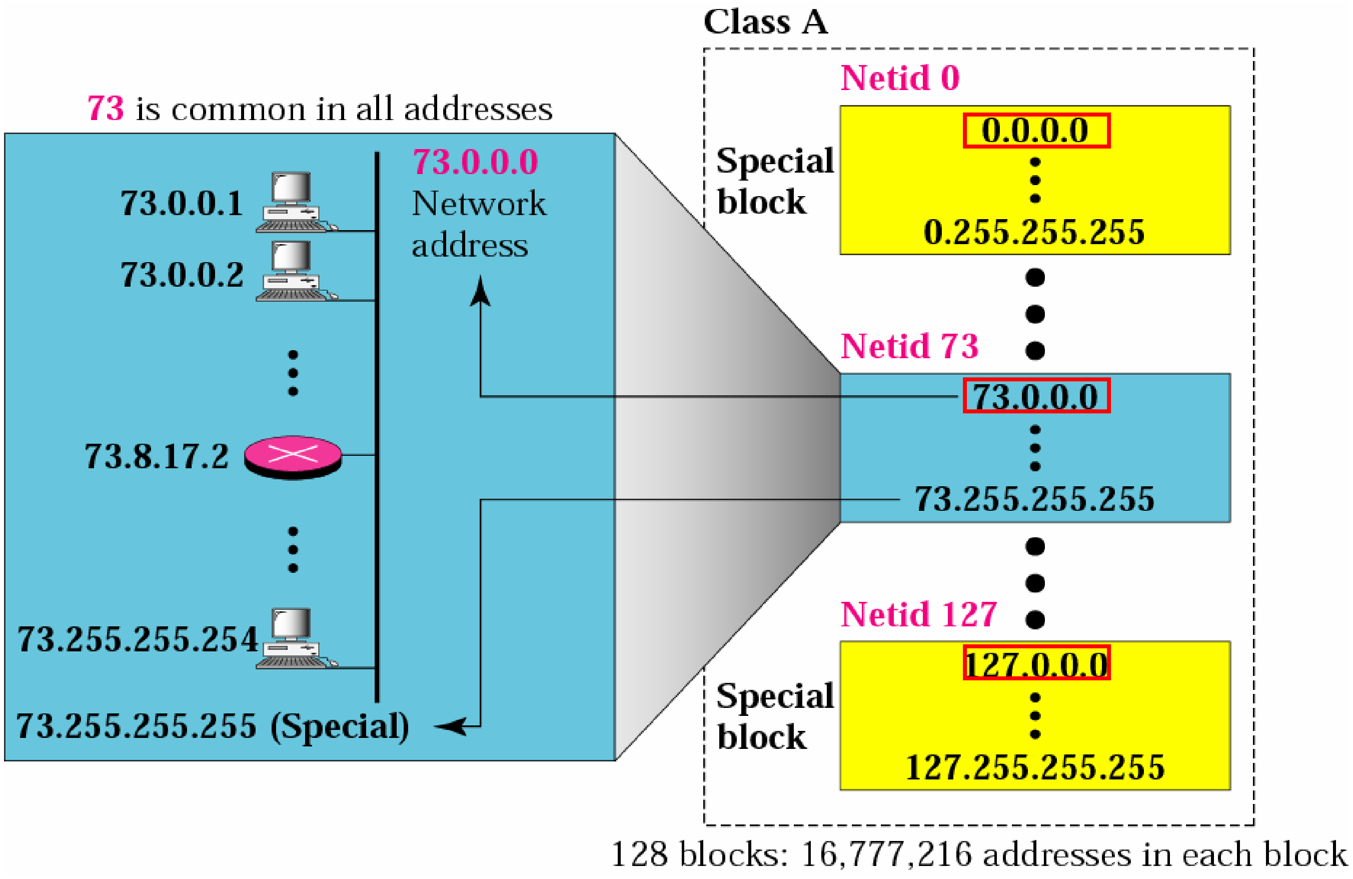
Example **[classes of IP Address – number of addresses per class]**



Class	*Number of Addresses*	*Percentage*
A	$2^{31} = 2{,}147{,}483{,}648$	50%
B	$2^{30} = 1{,}073{,}741{,}824$	25%
C	$2^{29} = 536{,}870{,}912$	12.5%
D	$2^{28} = 268{,}435{,}456$	6.25%
E	$2^{28} = 268{,}435{,}456$	6.25%

Classful IP Addressing (cont.)

Example [blocks in class A]



128 blocks: 16,777,216 addresses in each block

Classful IP Addressing (cont.)

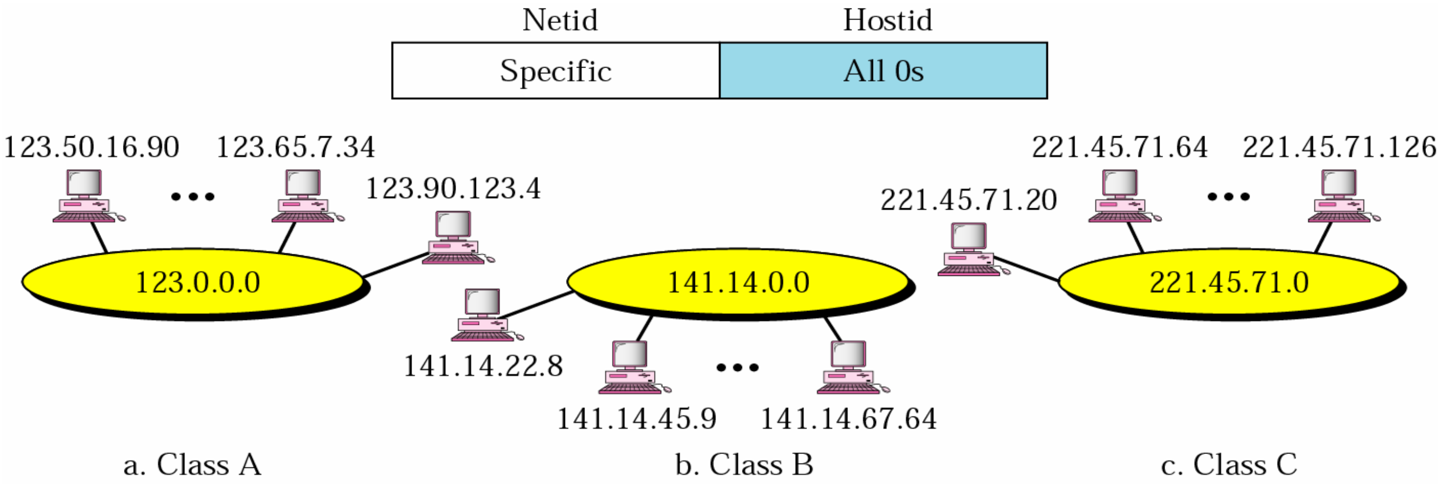
Special Addressing – some parts of address space are used for special purposes – cannot be assigned to a host

Special Address	*Netid*	*Hostid*	*Source or Destination*
Network Address	Specific	All 0-s	None
Direct Broadcast Address	Specific	All 1-s	Destination
Limited Broadcast Address	All 1-s	All 1-s	Destination
This host on this network (used at bootstrap time)	All 0-s	All 0-s	Source
Specific host on this network (used to confine packet to LAN)	All 0-s	Specific	Destination
Loopback Address	127	Any	Destination

Classful IP Addressing (cont.)

Network Address – defines the network to the rest of the Internet – cannot be assigned to a host

- network address ≠ Netid – network address has both Netid and Hostid, with 0s for the Hostid
- Netid alone is also known as network prefix
- routers route packets based on their respective network address
- reduces the number of available addresses in classes A, B and C by 1



In a class-B network of network address 141.14.0.0
all hosts have IP addresses of the form 141.14.xxx.xxx.

Classful IP Addressing (cont.)

Example [network address]

Given the (classful) address 23.56.7.91, find the network address.

Solution:

The class is A ⇒ only the first byte defines the Netid. We can find the network address by replacing the Hostid bytes with 0s. Therefore, the network address is 23.0.0.0

Example [network address]

Given the (classful) address 132.6.17.85, find the network address.

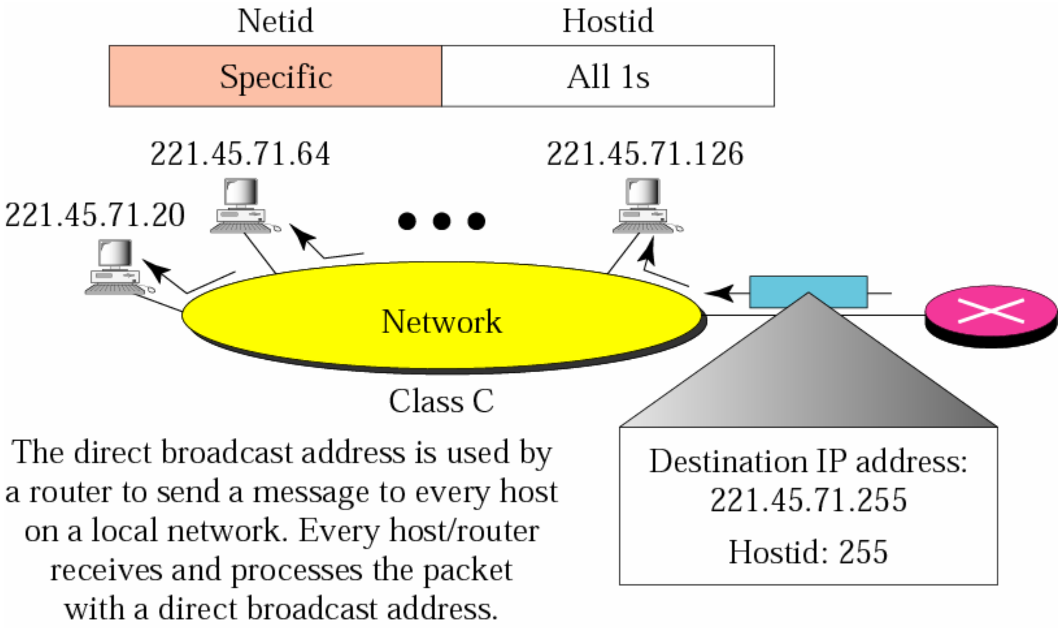
Solution:

The class is B ⇒ the first two byte define the Netid. We can find the network address by replacing the hostid bytes with 0s. Therefore, the network address is 132.6.0.0.

Classful IP Addressing (cont.)

Direct Broadcast Address – **hostid = all 1s** – **used by a router to send packets to all hosts in a specific network**

- **can be only used as a destination address in an IP packet**
- **further reduces the number of available addresses by 1**



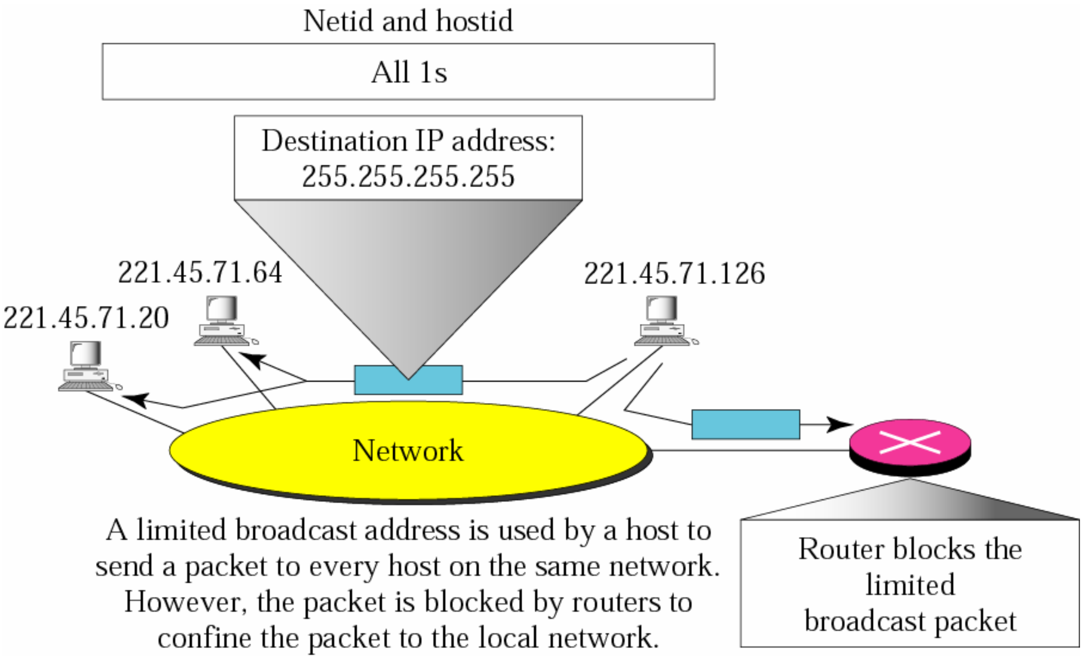
The direct broadcast address is used by a router to send a message to every host on a local network. Every host/router receives and processes the packet with a direct broadcast address.

Allows a remote system to send a single packet that will be broadcast on the specified LAN. To avoid potential problems, many sites configure routers to reject all direct broad. packets.

Classful IP Addressing (cont.)

Limited Broadcast Address – all 1-s ⇒ class E address – used by host to send packets to every other host in its current LAN

- limited broadcast packet is NOT forwarded by routers ⇒ packet is confined within its LAN
- can be only used as a IP destination address

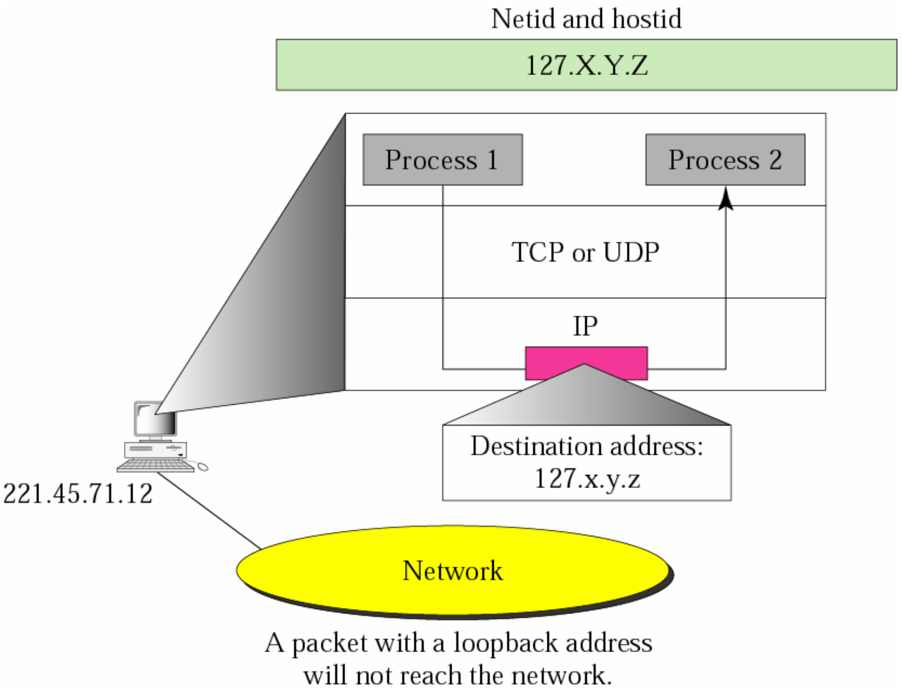


A limited broadcast address is used by a host to send a packet to every host on the same network. However, the packet is blocked by routers to confine the packet to the local network.

Classful IP Addressing (cont.)

Loopback Address – **first byte = 127** – **used to test software on a machine**

- **packet with loopback address as destination address never leaves machine**
- **e.g. to test if IP software works – execute "ping 127.x.y.z"**
- **e.g. can be used by a client process to send a message to a server process on the same machine**
- **can be only used as a destination address**



A packet with a loopback address will not reach the network.

Classful IP Addressing (cont.)

Disadvantages of Classful Network Addressing

- **lack of a class to support medium-sized organizations**
  - **class C which supports 254 hosts - too small**
  - **class B which supports 65534 hosts - too large**
- **a premature depletion of class B addresses has already occurred**
  - **in the early days of the Internet, addresses were freely assigned to those who asked for them, without concerns about the eventual depletion of the IP address space**
- **three existing mechanisms for overcoming the limitations of classful addressing:**

  (1) **subnetting** – if an organization gets assigned a "big" block of IP addresses how to distribute these internally, among multiple LAN

  (2) **supernetting** – how an organization can combine several class C blocks to create a larger range of addresses

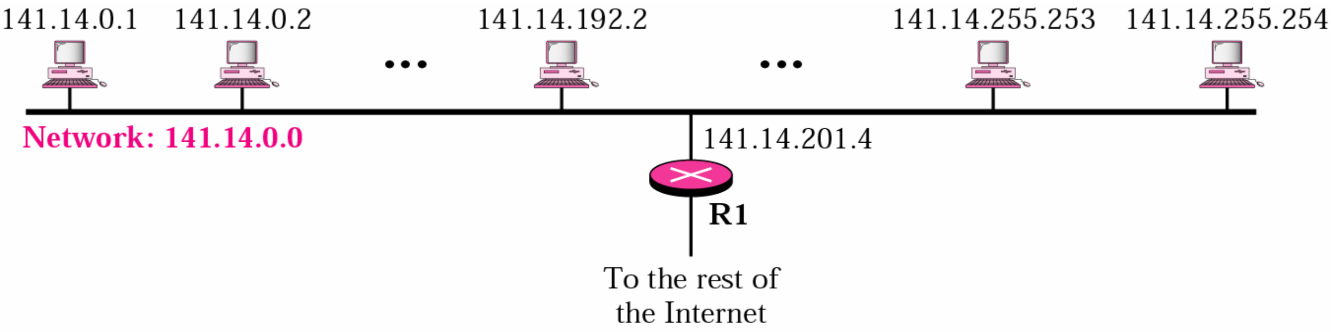
  (3) **classless addressing** – if an organization gets assigned several small size blocks of IP addresses how to do efficient routing

Subnetting

Hierarchical Nature of IP Addressing and IP Routing

(1) the 1st part of an IP address (*Netid*) is used by outside routers to reach the network

(2) the 2nd part of an IP address (*Hostid*) is used by local routers to reach the host



Network with 2 Levels of Hierarchy

Problems with 2 Level Classful Addressing

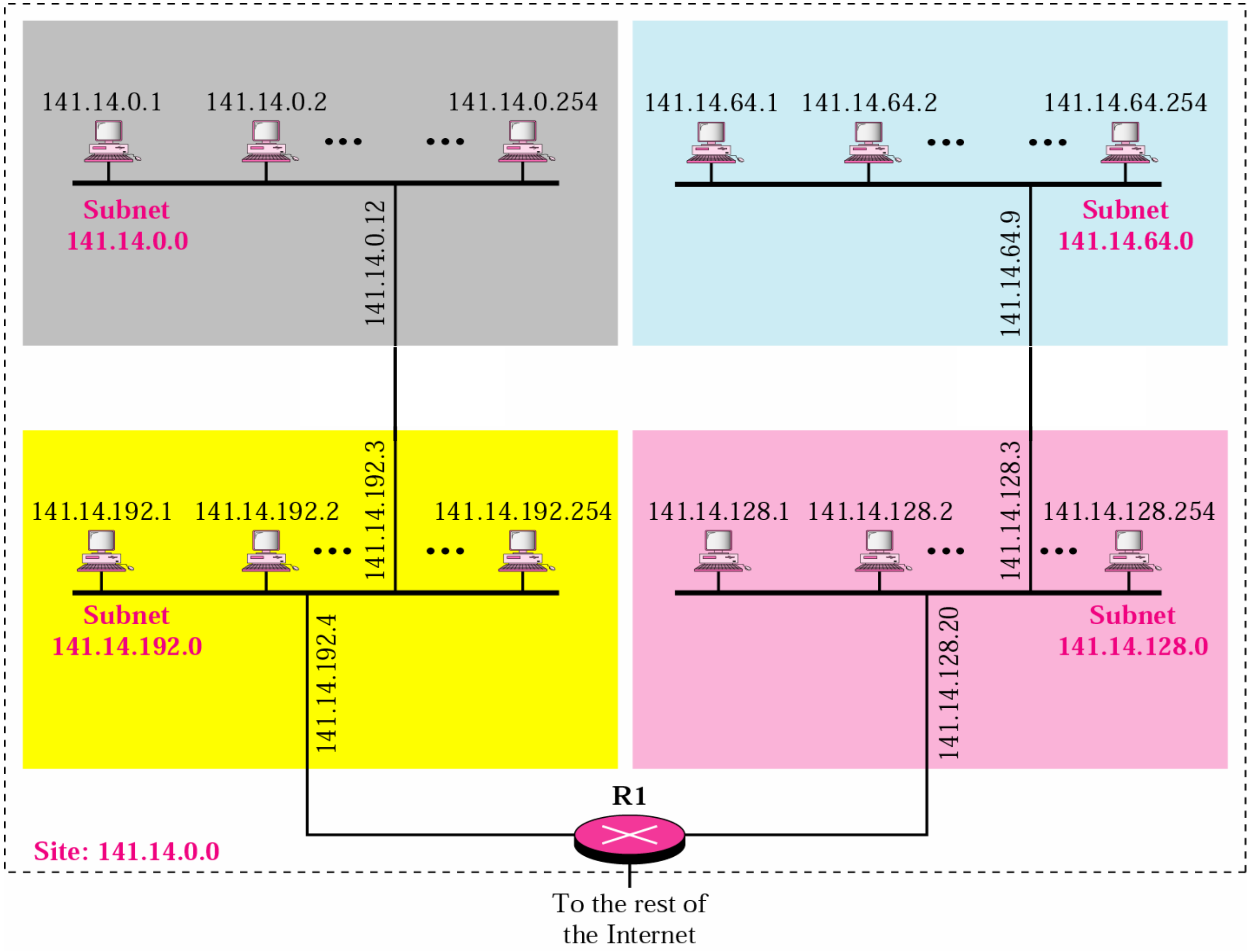
(1) local administrators have to request another network number to install a new subnetwork

(2) with every new (sub)network, the size of global Internet routing tables grow

Subnetting (cont.)

Example [subnetting a big LAN]

What would be the advantages of ‘breaking’ a big LAN into a few smaller subnets?



Subnetting (cont.)

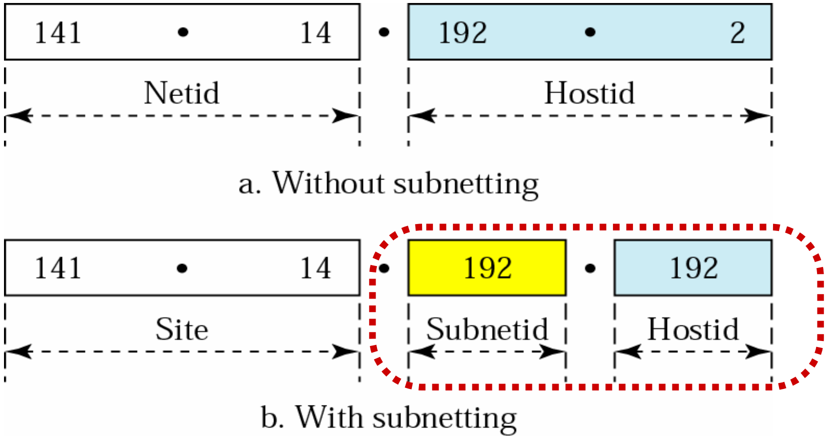
Subnetted Network – network divided into several smaller subnetworks each having its own subnetwork address

- internally, each subnetwork is recognized by its subnetwork address; to the rest of the Internet all subnetworks still appear as a single network

Routing in Subnetted Networks

(1) deliver to the network
(2) deliver to the subnetwork
(3) deliver to the host

3 levels of hierarchy



a. Without subnetting

b. With subnetting

hostid is divided into 2 parts:
1) subnet number
2) host number on that subnet

How can a router find the network / subnetwork / host address to route the packet ?!

Subnetting (cont.)

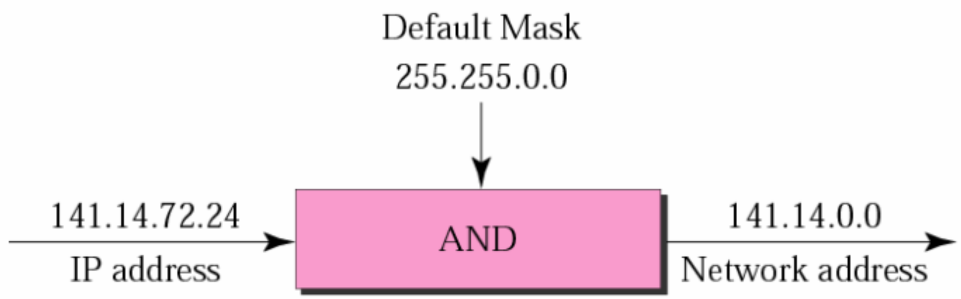
Default Mask – **32-bit binary number, used by outside routers, that helps extracting the network address when AND-ed with an IP address in the block**

- **if the bit in the mask is 1 ⇒ retain the bit in the address**
- **if the bit in the mask is 0 ⇒ put 0 bit in the address**

Class	*In Binary*	*In Dotted-Decimal*	*Using Slash*
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 111111111 11111111 00000000	255.255.255.0	/24

# of 1s in mask

Default Masks in Binary / Dotted-Decimal / Slash Notation



Subnetting (cont.)

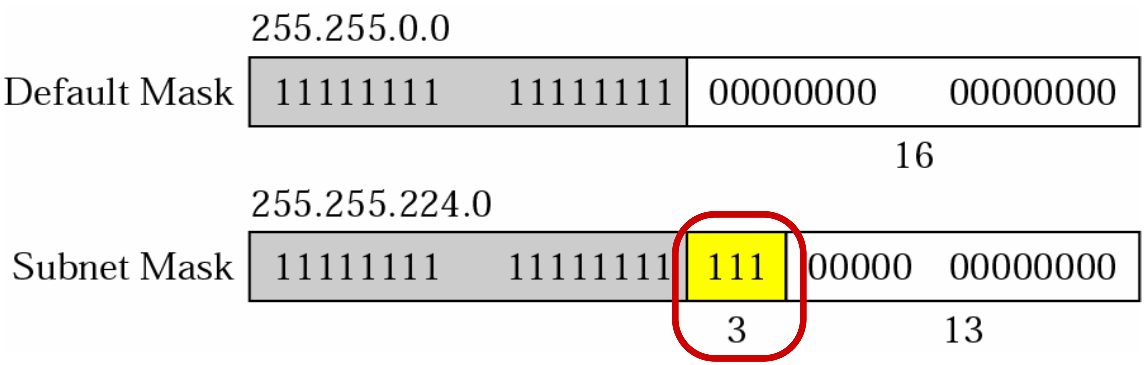
Subnet Mask – **32-bit binary number, used by inside routers in a subnetted network, that helps extracting the subnet address when AND-ed with an IP address from the block**

- **# of 1-s in subnet mask > # of 1-s in default mask**
- **# of subnets is determined by # of extra 1-s in subnet mask**

  if # of extra 1-s = n ⇒ # of subnets is 2^n

- **# of addresses per subnet is determined by # of 0 in subnet mask**

  if # of 0-s = m ⇒ # of addresses per subnets is 2^m



255.255.0.0

Default Mask 11111111 11111111 00000000 00000000

16

255.255.224.0

Subnet Mask 11111111 11111111 111 00000 00000000

3 13

# of extra 1-s = 3 ⇒ 2^3=8 subnets

# of 0-s = 13 ⇒ 2^{13} addresses per subnet

Subnetting (cont.)

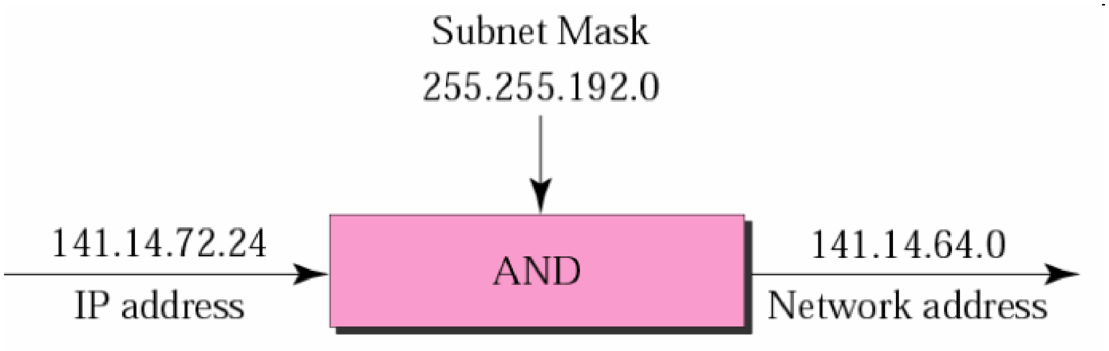
Example **[subnet mask]**

What is the subnetwork address if the destination address is 141.14.72.24 and the subnet mask is 255.255.192.0

Solution:

Address 1	**10001101**	**00001110**	**01001000**	**00011000**
Subnet Mask	**11111111**	**11111111**	**11000000**	**00000000**
Subnet Address	**10001101**	**00001110**	**01000000**	**00000000**

The subnetwork address is 141.14.64.0.



Subnetting (cont.)

Example [subnet mask]

For the given IP address and Subnet mask determine Network class, Network ID, Sub-network ID, and Host ID.

(a) IP Address: 187.199.127.5
Sub-net mask: 255.255.255.0

Solution:

Network Class: B
Default Mask: 255.255.0.0
Network ID: 187.199
Result of logical AND: 187.199.127
Sub-network ID: 127
Host ID: 5

(b) IP Address: 187.199.127.5
Sub-net mask: 255.255.128.0

Solution:

Network Class: B
Default Mask: 255.255.0.0
Network ID: 187.199
Result of logical AND: 187.199.0.0
Sub-network ID: 0
Host ID: 127.5

Subnetting (cont.)

Subnet Design Considerations

- How many subnets does the organization need today and how many it will need in the future? ($<2^n$)
- How many hosts are there on the organization's largest subnet today; and how many there will be in the future? ($<2^m$)

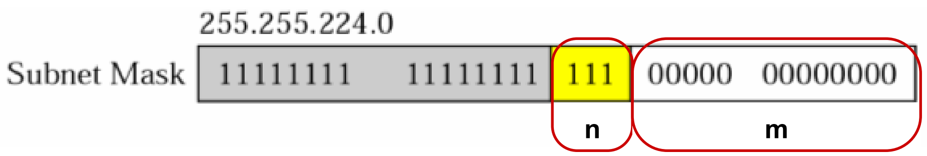
Subnet Design Procedure

(1) take the maximum number of subnets required and round up to the nearest higher power of two

- for example, if a organization needs 9 subnets, the network administrator will have to round up to 2^4=16
- if 9 subnets are required today, but 8 more will have to be added in two years, it might be wise to allow for more growth and select 2^5 (32) as the max number of subnets

(2) make sure that there are enough host addresses for the organization's largest subnet

- if the largest subnet needs to support 50 host addresses today, 2^5 (32) will not provide enough host address space so the network administrator will have to round up to 2^6 (64)



Subnetting (cont.)

Example [subnetting]

A customer has been given the site IP address 128.100.0.0 (a Class B address) for his company. He requires 3 separate networks with the maximum possible number of host connections on each network. How should he subnet his network?

Solution:

The first two octets 128.100 are fixed since the given address is a Class B address. Therefore we have the last two octets to play with.

Possibility 1

Let us just use the first 2 bits for a subnet IDs:

Octet 1	Octet 2	Octet 3	Octet 4
10000000	01100100	00000000	00000000
128.	100.	0.	0

The possible combinations for these two bits are:

00 = 0	->	128.100.0.0
01 = 64	->	128.100.64.0
10 = 128	->	128.100.128.0
11 = 192	->	128.100.192.0

Subnetting (cont.)

However all 1’s and all 0’s cannot be used as subnet IDs! (RFC 950 rules out '11' and '00' as useable subnet IDs, since these combined with all 1-s and all 0-s hostid are special addresses.)
Hence, we would be left with only two subnets instead of the 3 we required.

Possibility 2

Let us use an extra bit in octet 3 for subnet IDs.

Octet 1	Octet 2	Octet 3	Octet 4
10000000	01100100	00000000	00000000
128.	100.	0.	0

The possible combinations for these three bits are:

000 = 0	-> 128.100.0.0
001 = 32	-> 128.100.32.0
010 = 64	-> 128.100.64.0
011 = 96	-> 128.100.96.0
100 = 128	-> 128.100.128.0
101 = 160	-> 128.100.160.0
110 = 192	-> 128.100.192.0
111 = 224	-> 128.100.224.0

Subnetting (cont.)

As before all 1's and all 0's are not permitted for subnets, therefore we are left with 6 possible subnets (2^3 - 2):

001 = 32	-> 128.100.32.0
010 = 64	-> 128.100.64.0
011 = 96	-> 128.100.96.0
100 = 128	-> 128.100.128.0
101 = 160	-> 128.100.160.0
110 = 192	-> 128.100.192.0

This leaves the rest of the bits (from power 16 downwards) in octet 3 and all the bits in octet 4 to construct the individual host addresses.

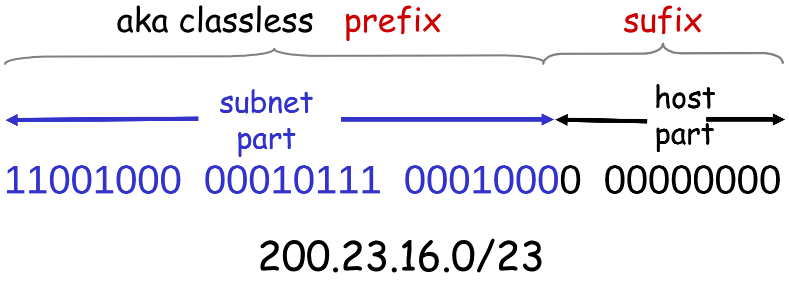
An example of a host address in subnet 128.100.192.0 would be: 128.100.194.23 . On first inspection it would appear that address 128.100.194.23 has nothing to do with the subnet 128.100.192.0. However, by looking a little more closely at the final two octets of the host address, we can see that this host is indeed a part of the given subnet.

Octet 1	Octet 2	Octet 3	Octet 4	
10000000	01100100	11100000	00000000	**Subnet 6**
128.	100.	192.	0	
10000000	01100100	11100010	00010111	
128.	100.	194.	23	**Host on Subnet 6**

Classless Addressing

Classless Addressing – **known as CIDR "Classless InterDomain Routing" addressing – allows the division between netid and hostid to occur on arbitrary bit boundaries**

- **CIDR address format: a.b.c.d/x, where x is # of bits in network portion of address and/or # of 1's in the network mask** (aka prefix length)



aka classless prefix

sufix

subnet part

host part

11001000 00010111 00010000 00000000

200.23.16.0/23

CIDR Routing – **packets are routed according to the prefix of the destination IP address without distinguishing different address classes**

- **CIDR enables reduction in sizes of routing tables – a single routing entry covers a block of classfull addresses**
- **e.g. instead of having 4 entries for a contiguous set of Class C addresses (205.100.0.0, 205.100.1.0, 205.100.2.0, 205.100.3.0), a single substitute routing entry can be used: 205.100.0.0/22**

Classless Addressing (cont.)

Example [network Address in Classless Addressing]

What is the network address if one of its addresses is: 167.199.170.82/27.

Solution:

The prefix length is 27 ⇒ keep the first 27 bits as is and change the remaining 5 bits to 0s.

The last 5 bits affect only the last byte. The last byte is 01010010. By changing the last 5 bits to 0s, we get 01000000 = 64.

So, network address = 167.199.170.64/27.

Example [network Address in Classless Addressing]

What is the network address if one of its addresses is: 202.78.5.34/22.

Solution:

The prefix length is 22 ⇒ keep the first 22 bits as is and change the remaining 10 bits to 0s.

The last 10 bits affect the last two bytes. The last two bytes are 00000101 00100000. By changing the last 10 bits to 0s, we get 00000100 00000000 = 4.0

So, network address = 202.78.4.0/22 .

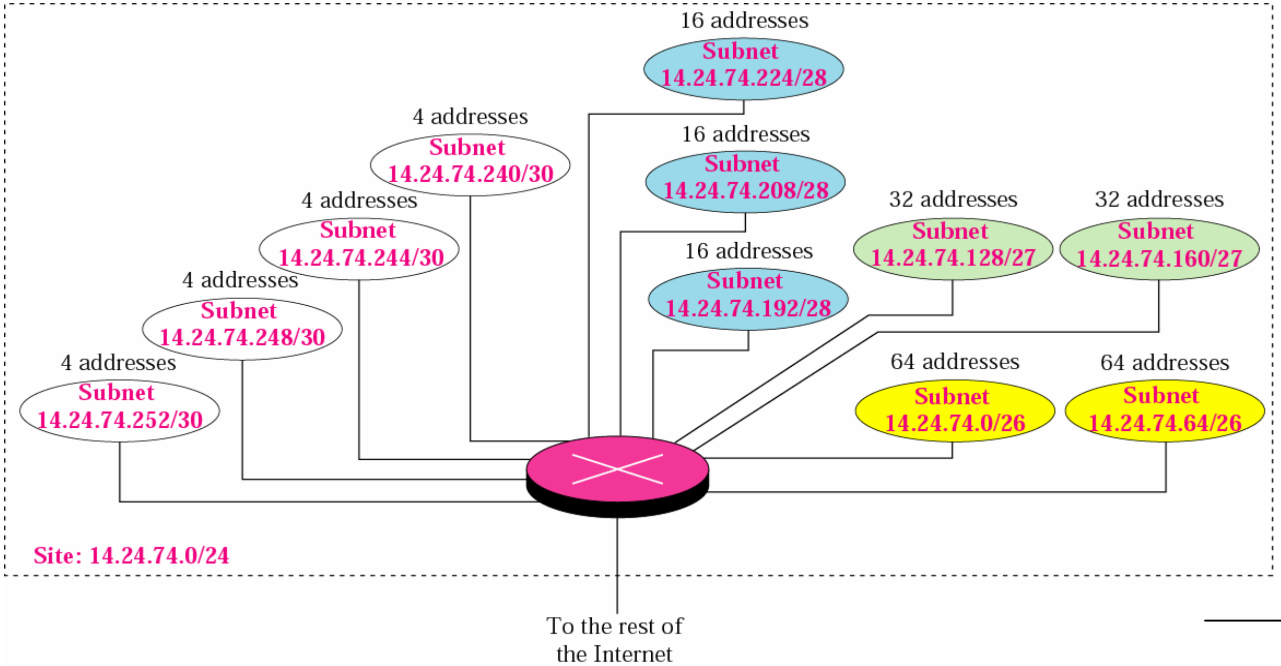
Classless Addressing (cont.)

Example [variable-length subnets]

An organization is granted a block of addresses with the beginning address: 14.24.74.0/24. There are 2^{32-24}=256 addresses in this block. The organization needs to have 11 subnets as shown below:

- 2 subnets, each with 64 addresses – need 6-bit long hostIDs!
- 2 subnets, each with 32 addresses – need 5-bit long hostIDs!
- 3 subnets, each with 16 addresses – need 4-bit long hostIDs!
- 4 subnets, each with 4 addresses – need 2-bit long hostIDs!

Design the subnets. (To simplify your work, assume all 0-s and all 1-s subnet ID are allowed.)



Classless Addressing (cont.)

14.24.74.00/24 = $\underbrace{00001110\ \ 00011000\ \ 01001010}_{/24\ \text{bits}}$ / $\underbrace{00000000}_{\text{remaining 8 bits}}$

1) With first 2 out of 8 available bits, we can create 4 networks (i.e. 4 blocks of addresses) each with 64 host. We use the first of the two blocks for the first two subnets.

6 bits for host IDs

Subnet 1:	14.24.74.00/26 =	00001110	00011000	01001010	00000000
Subnet 2:	14.24.74.64/26 =	00001110	00011000	01001010	01000000
unused 1:	14.24.74.128/26 =	00001110	00011000	01001010	10000000
unused 2:	14.24.74.192/26 =	00001110	00011000	01001010	11000000

2) We use the third block of 64 addresses (unused 1) for the next two subnets, each with 32 hosts.

5 bits for host IDs

Subnet 3:	14.24.74.128/27 =	00001110	00011000	01001010	10000000
Subnet 4:	14.24.74.160/27 =	00001110	00011000	01001010	10100000

3) We split the fourth block of 64 addresses (unused 2) into 4 sub-blocks, each with 16 hosts.

4 bits for host IDs

Subnet 5:	14.24.74.192/28 =	00001110	00011000	01001010	11000000
Subnet 6:	14.24.74.208/28 =	00001110	00011000	01001010	11010000
Subnet 7:	14.24.74.224/28 =	00001110	00011000	01001010	11100000
unused 3:	14.24.74.224/28 =	00001110	00011000	01001010	11110000

Classless Addressing (cont.)

4) **We use the last available sub-block for the last four subnets, each with 4 addresses.**

2 bits for host IDs

Subnet 8:	**14.24.74.240/30 =**	**00001110**	**00011000**	**01001010**	**11110000**
Subnet 9:	**14.24.74.244/30 =**	**00001110**	**00011000**	**01001010**	**11110100**
Subnet 10:	**14.24.74.248/30 =**	**00001110**	**00011000**	**01001010**	**11111000**
Subnet 11:	**14.24.74.252/30 =**	**00001110**	**00011000**	**01001010**	**11111100**

Note: The advantages of classless addressing come at certain price!

From: http://www.ietf.org/internet-drafts/draft-ietf-grow-rfc1519bis-02.txt

*"With the change from classful network numbers to classless prefixes, it is not possible to infer the network **mask** from the initial bit pattern of an **IPv4** address. This has implications for how routing information is stored and propagated. Network masks or prefix lengths must be explicitly carried in routing protocols …*

*Similarly, routing and forwarding tables in layer-3 network equipment must be organized to store both prefix and prefix length or **mask**. Equipment which organizes its routing/forwarding information according to legacy class A/B/C network/subnet conventions cannot be expected to work correctly … "*

Obtaining IP Address and Masks

Which IP address info should be known to host?

– each computer attached to the Internet must have the following information

- its own IP address [host IP address]
- its subnet mask
- the IP address of a router
- the IP address of a DNS server

How does host get its IP address?

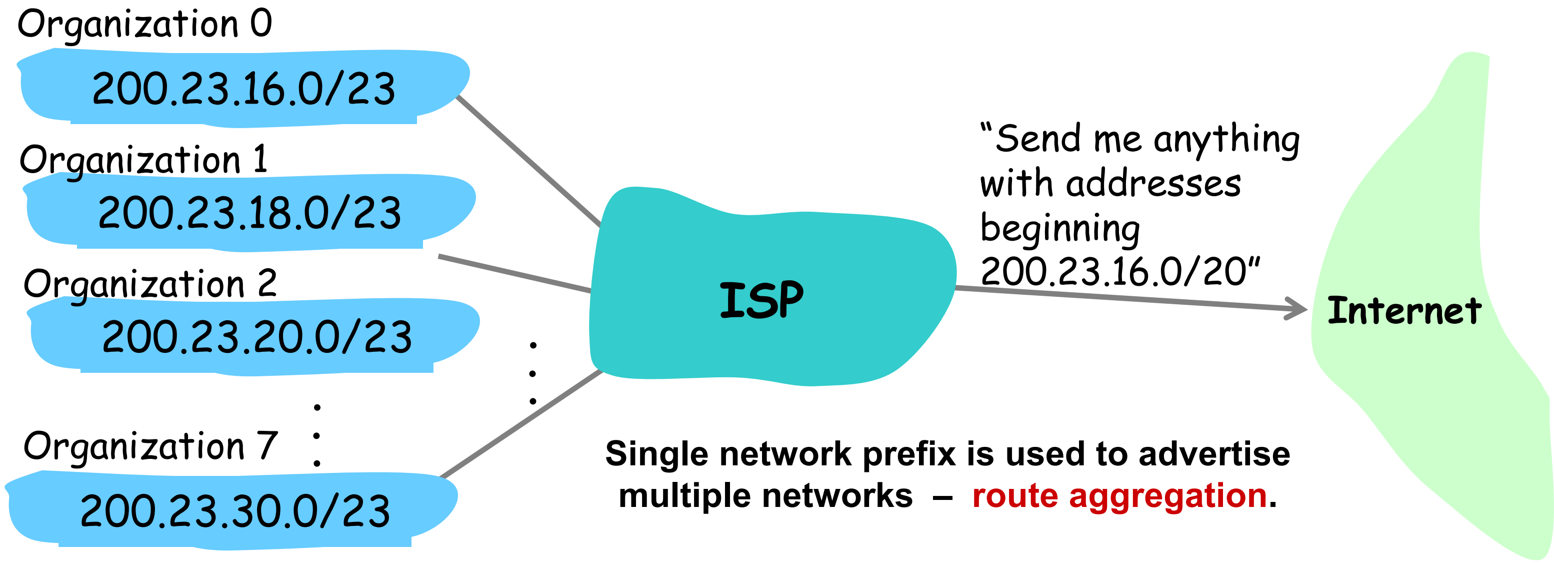
(1) manual configuration: a system administrator manually configures the IP address into the host (typically in a file)

- Wintel: *control-panel->network->configuration->tcp/ip->properties*, or simply type *ipconfig*
- UNIX: */etc/rc.config*

(2) Dynamic Host Configuration Protocol (DHCP): host obtains an IP address automatically, as well as additional information such as the address of its first-hop router and the address of its DNS server

Obtaining IP Address (cont.)

How does network get its IP address? – **to obtain a block of IP addresses network administrator must first contact its ISP**



Single network prefix is used to advertise multiple networks – route aggregation.

How does ISP get a block of IP addresses? – **apply to Internet Corporation for Assigned Names and Numbers (ICANN) – international authority for managing the IP address space**

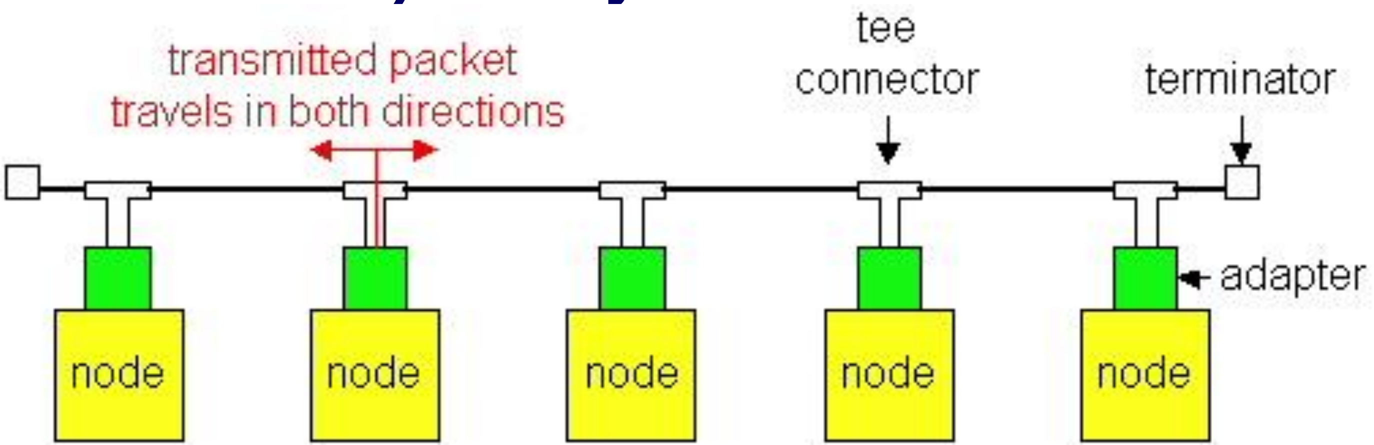
(see: http://www.icann.org/general/)

Network Architecture

- Ethernet (Traditional Ethernet)
- Fast Ethernet
- Gigabit Ethernet

Media Access

- **Ethernet and Wi-Fi are both "multi-access" technologies**
  - Broadcast medium, shared by many hosts
  - Simultaneous transmissions will result in collisions
- **Media Access Control (MAC) protocol required**
  - Rules on how to share medium
- **The Data Link Layer is divided into two Part MAC Media Access Control) Sublayer and LLC (Logic Link Control) Sublayer**



802.3 Ethernet

- **Carrier-sense multiple access with collision detection (CSMA/CD).**
  - CS = carrier sense
  - MA = multiple access
  - CD = collision detection
- **Base Ethernet standard is 10 Mbps.**
  - 100Mbps, 1Gbps, 10Gbps standards came later

Ethernet CSMA/CD

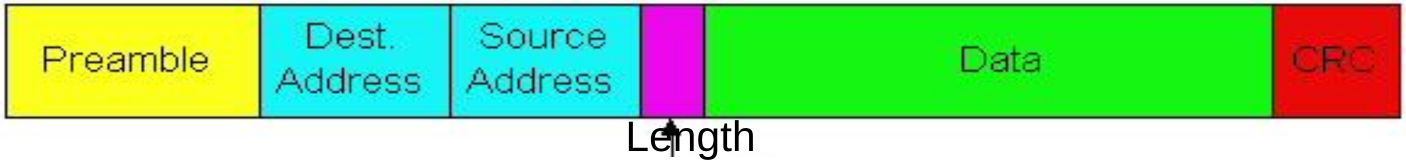
- **CSMA/CD (carrier sense multiple access with collision detection) media access protocol is used.**
    - Data is transmitted in the form of packets.
    - Sense channel prior to actual packet transmission.
    - Transmit packet only if channel is sensed idle; else, defer the transmission until channel becomes idle.
    - After packet transmission is started, the node monitors its own transmission to see if the packet has experienced a collision.
    - If the packet is observed to be undergoing a collision, the transmission is aborted and the packet is retransmitted after a random interval of time using Binary Exponential Backoff algorithm.

Ethernet Address

- End nodes are identified by their Ethernet Addresses (MAC Address or Hardware Address) which is a unique 6 Byte address.
- MAC Address is represented in Hexa Decimal format e.g 00:05:5D:FE:10:0A
- The first 3 bytes identify a vendor (also called prefix) and the last 3 bytes are unique for every host or device

Ethernet Frame Structure

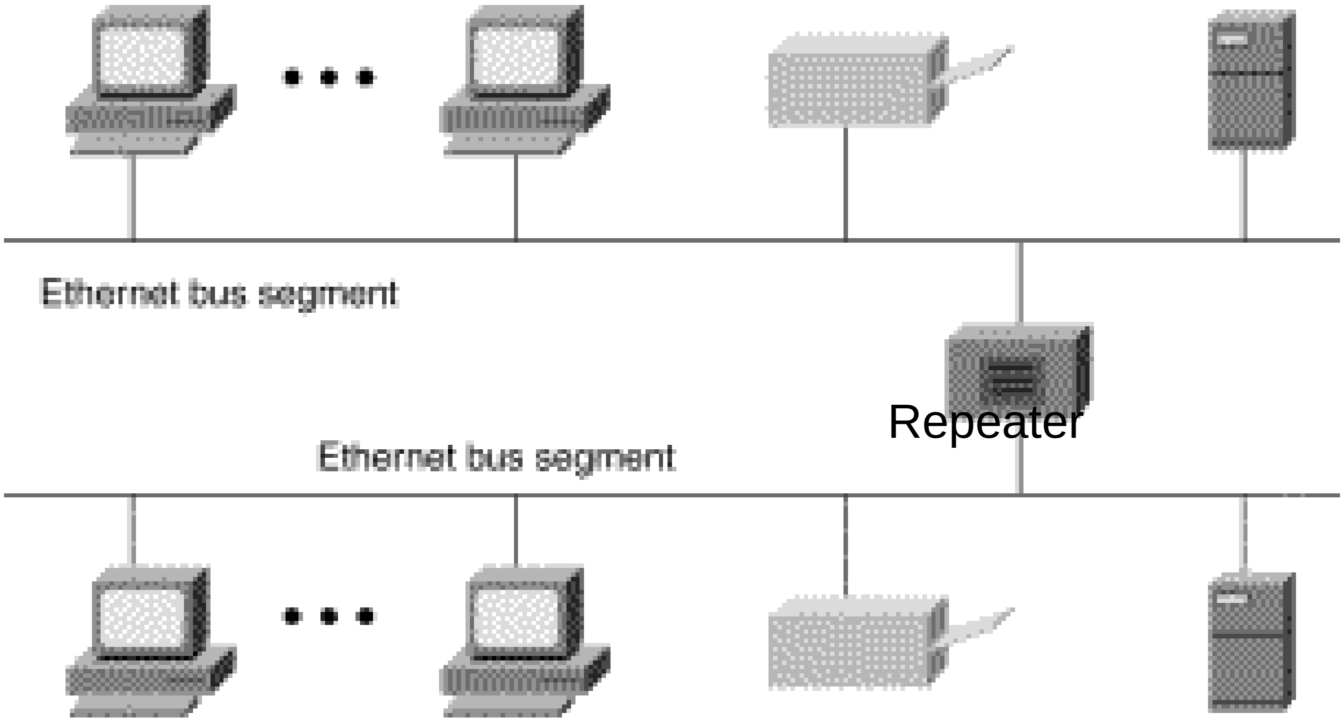
- **Preamble:**
  - 7 bytes with pattern 10101010 followed by one byte with pattern 10101011
  - Used to synchronize receiver, sender clock rates
- **Addresses:** 6 bytes, frame is received by all adapters on a LAN and dropped if address does not match
- **Length:** 2 bytes, length of Data field
- **CRC:** 4 bytes generated using CR-32, checked at receiver, if error is detected, the frame is simply dropped
- **Data Payload:** Maximum 1500 bytes, minimum 46 bytes
  - If data is less than 46 bytes, pad with zeros to 46 bytes



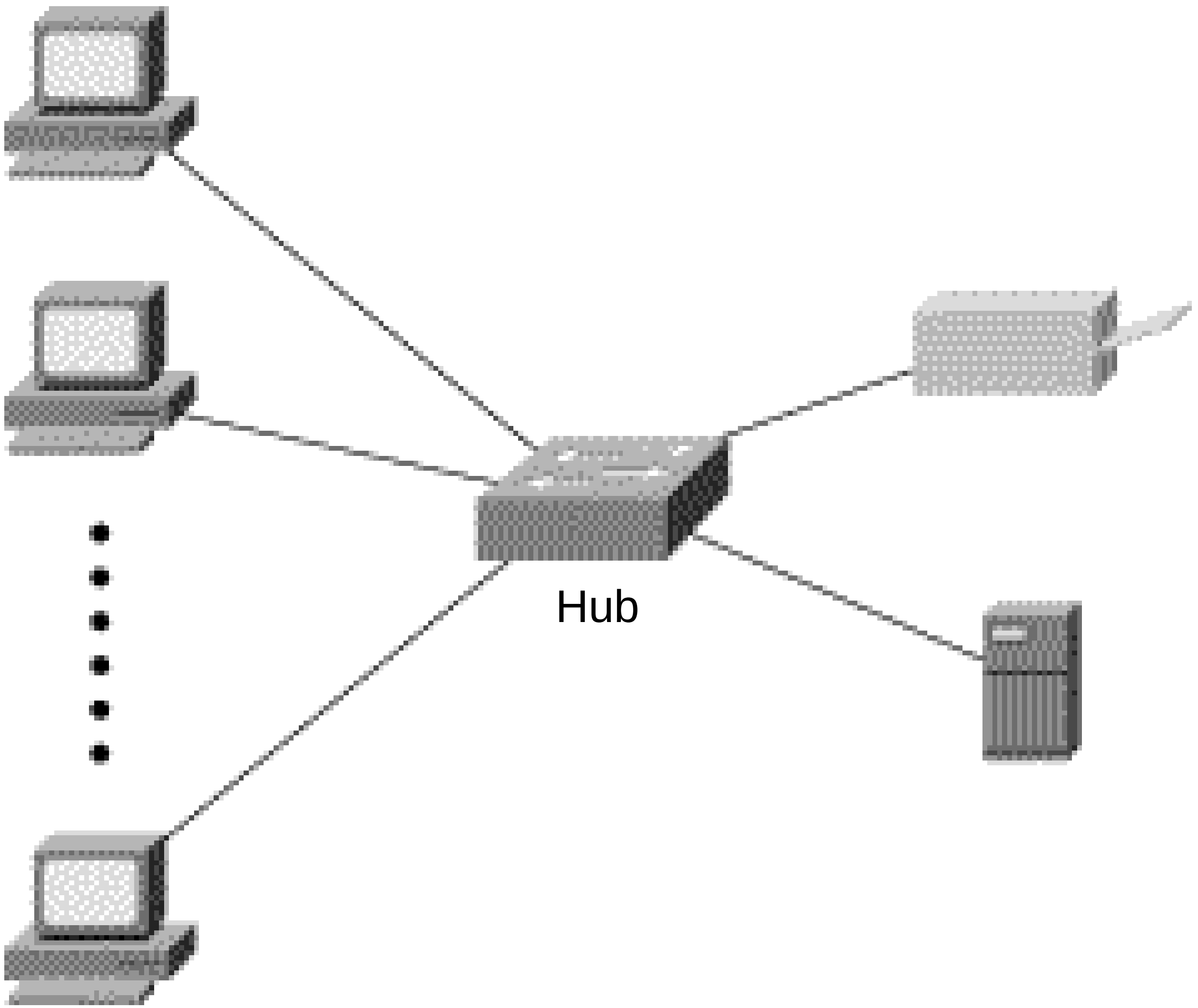
Ethernet

- 10 Base 5 (Thicknet) (Bus Topology)
- 10 Base 2 (Thinnet) (Bus Topology)
- 10 Base T (UTP) (Star/Tree Topology)
- 10 Base FL (Fiber) (Star/Tree Topology)

Ethernet BUS Topology



Ethernet STAR Topology



Ethernet

- **Physical Media :-**
  - 10 Base5 - Thick Co-axial Cable with Bus Topology
  - 10 Base2 - Thin Co-axial Cable with Bus Topology
  - 10 BaseT - UTP Cat 3/5 with Tree Topology
  - 10 BaseFL - Multimode/Singlemode Fiber with Tree
  - Topology
- **Maximum Segment Length**
  - 10 Base5 - 500 m with at most 4 repeaters (Use Bridge to extend
    the network)
  - 10 Base2 - 185 m with at most 4 repeaters (Use Bridge to extend
    the network)
  - 10 BaseT - 100 m with at most 4 hubs (Use Switch to extend the network)

Fast Ethernet

- **100 Mbps bandwidth**
- **Uses same CSMA/CD media access protocol and packet format as in Ethernet.**
- **100BaseTX (UTP) and 100BaseFX (Fiber) standards**
- **Physical media :-**
  - 100 BaseTX - UTP Cat 5e
  - 100 BaseFX - Multimode / Single mode Fiber
- **Full Duplex/Half Duplex operations.**

Fast Ethernet

- Provision for Auto-Negotiation of media speed: 10 Mbps or 100Mbps (popularly available for copper media only).

- Maximum Segment Length
  - 100 Base TX - 100 m
  - 100 Base FX - 2 Km (Multimode Fiber)
  - 100 Base FX - 20 km (Singlemode Fiber)

Gigabit Ethernet

- **1 Gbps bandwidth.**
- **Uses same CSMA/CD media access protocol as in Ethernet and is backward compatible (10/100/100 modules are available).**
- **1000BaseT (UTP), 1000BaseSX (Multimode Fiber) and 1000BaseLX (Multimode/Singlemode Fiber) standards.**
- **Maximum Segment Length**
  - 1000 Base T - 100m (Cat 5e/6)
  - 1000 Base SX - 275 m (Multimode Fiber)
  - 1000 Base LX - 512 m (Multimode Fiber)
  - 1000 Base LX - 20 Km (Singlemode Fiber)
  - 1000 Base LH - 80 Km (Singlemode Fiber)