
## Lecture 1

# INTRODUCTION TO COMPUTER NETWORKS

Dr.Lway Faisal Abdulrazak

# Pedagogy

Lecture

Problem Solving

Simulation using Cisco packet tracer

# What is a Network?

*A network is a set of devices (nodes) connected by communication links. A node can be a computer, printer, CCTV cameras or any other device capable of sending and/or receiving data generated by other nodes on the network. A link can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.*

## Why we need Networking?

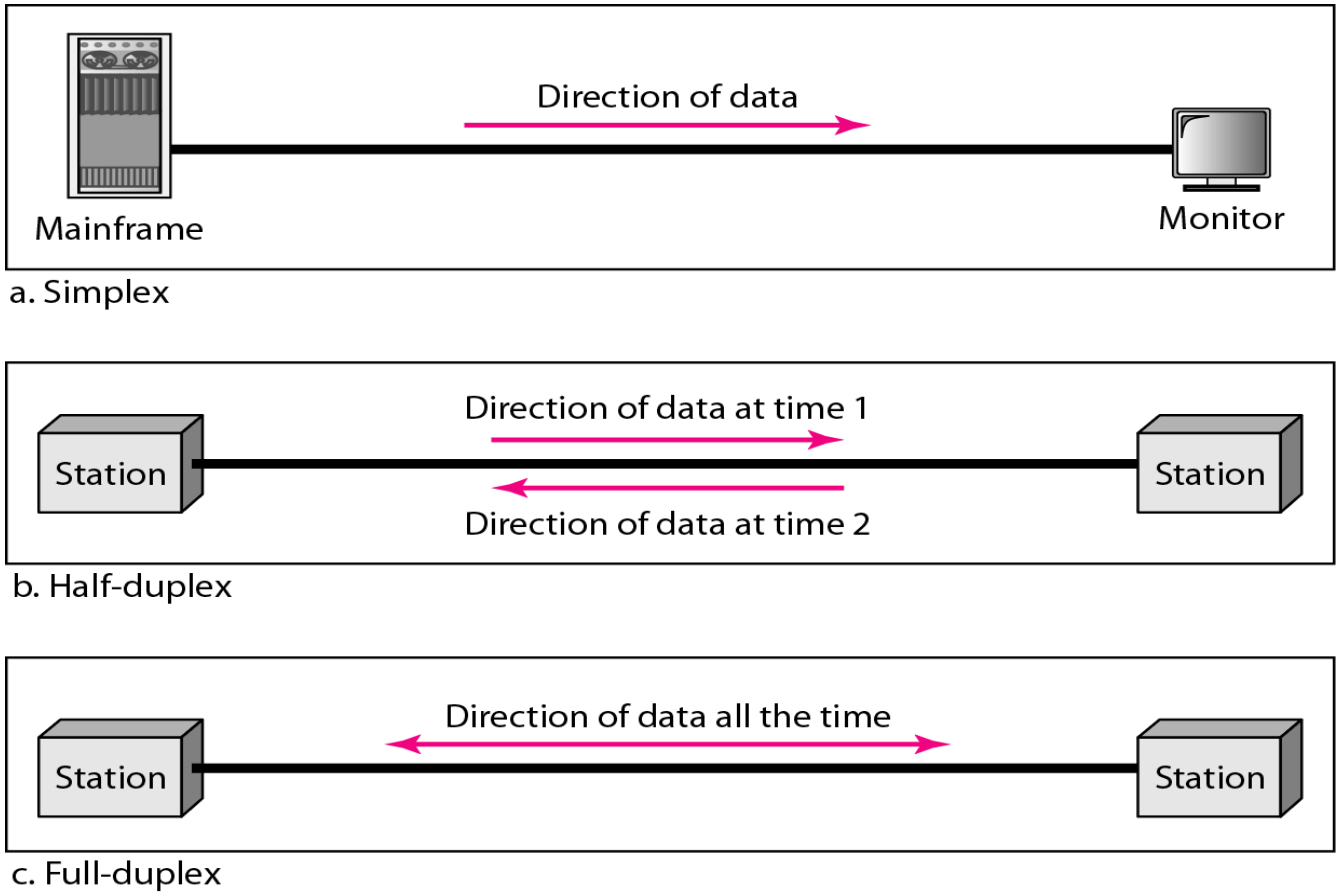
- **Sharing information**
- **Sharing hardware or software.**
- **Centralize administration and support.**

| Example for nodes: | Computer |
| --- | --- |
| | Server |
| | Printer |
| | Security Camera |

# Basic characteristics of computer network

- ★ Fault Tolerance
- ★ Scalability
- ★ Quality of Service (QoS)
- ★ Security

# *Data flow (simplex, half-duplex, and full-duplex)*




Simplex : one way like radio broadcast, Paging system satellite broadcasting.
Half-duplex: two-way of communication Like: walky-talky,
Full: like cellular system, Telephone.

# Protocols

Protocol = Rule.

It is a set of rules that govern data communication.

Protocol determines:

- ❑ What is communicated?
- ❑ How it is communicated?
- ❑ When it is communicated?

# Protocols – Network Communication

Protocols used in network communications also define:

- ★ Message encoding
- ★ Message formatting and encapsulation
- ★ Message timing
- ★ Message size
- ★ Message delivery options

# Elements of a Protocol

1. Message encoding
2. Message formatting and encapsulation
3. Message timing
4. Message size
5. Message delivery options

# 1. Message Encoding


# 2. Message Formatting and Encapsulation

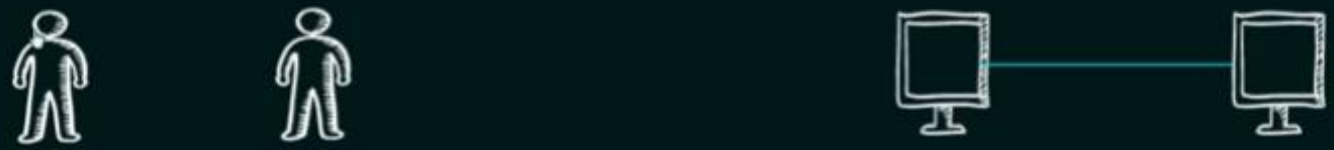
Agreed format.

Encapsulate the information to identify the sender and the receiver rightly.

# 3. Message Size

Humans break long messages into smaller parts or sentences.

Long messages must also be broken into smaller pieces to travel across a network.



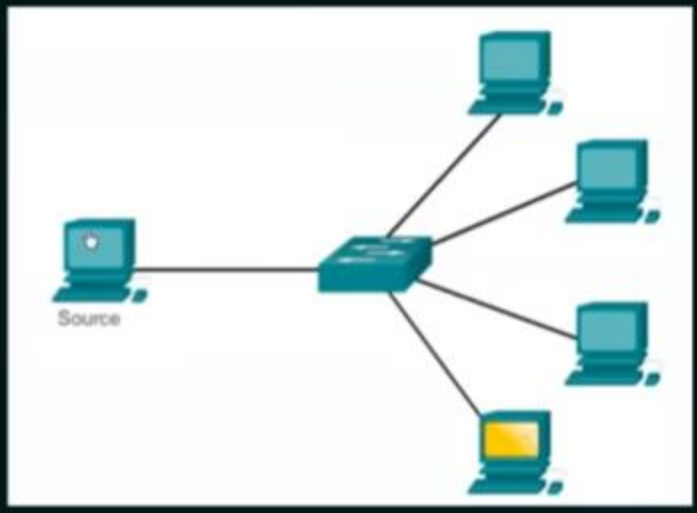
# 4. Message Timing

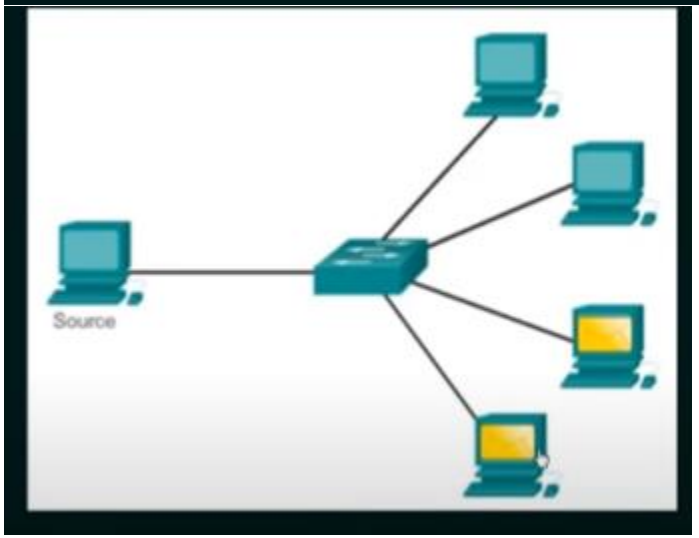
Flow Control.

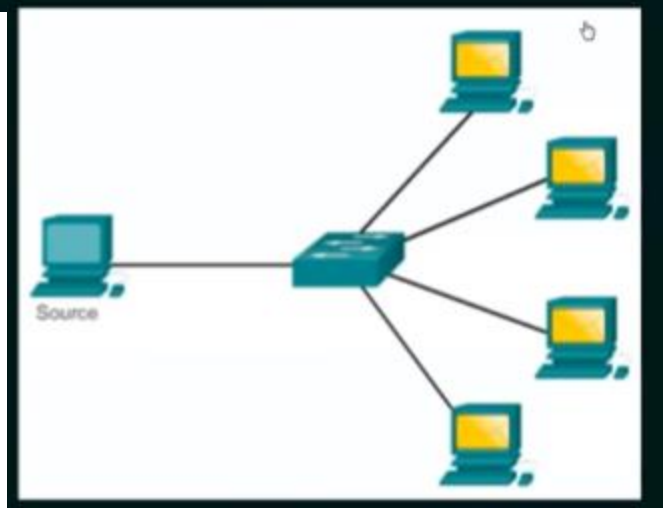
Response Timeout.

# 5. Message Delivery Options

- ★ Unicast
- ★ Multicast
- ★ Broadcast

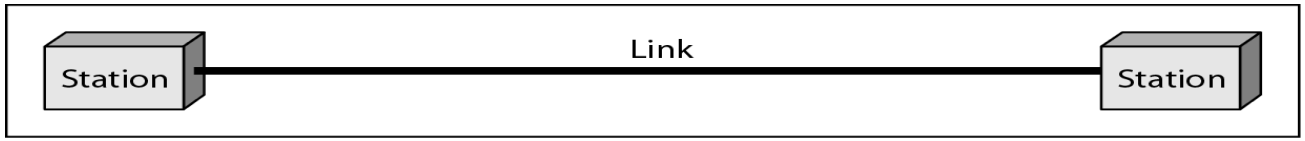


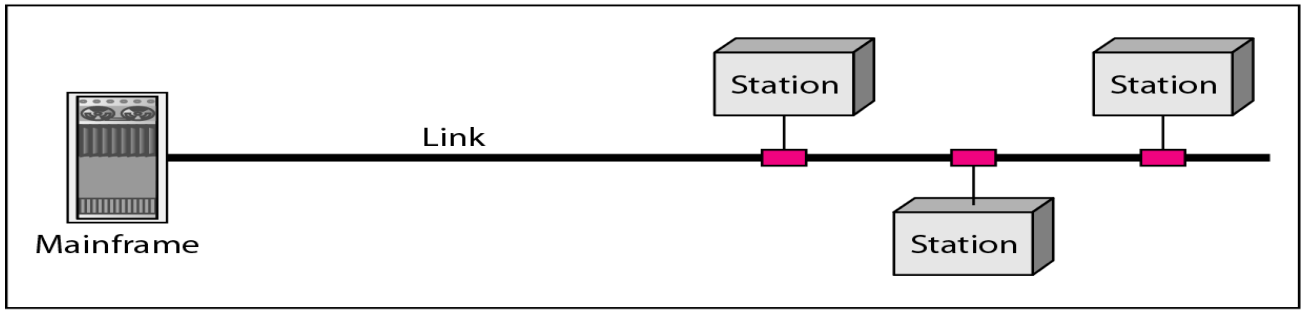



# Physical Structures

- **Type of Connection**
  - **Point to Point - single transmitter and receiver**
  - **Multipoint - multiple recipients of single transmission**




a. Point-to-point



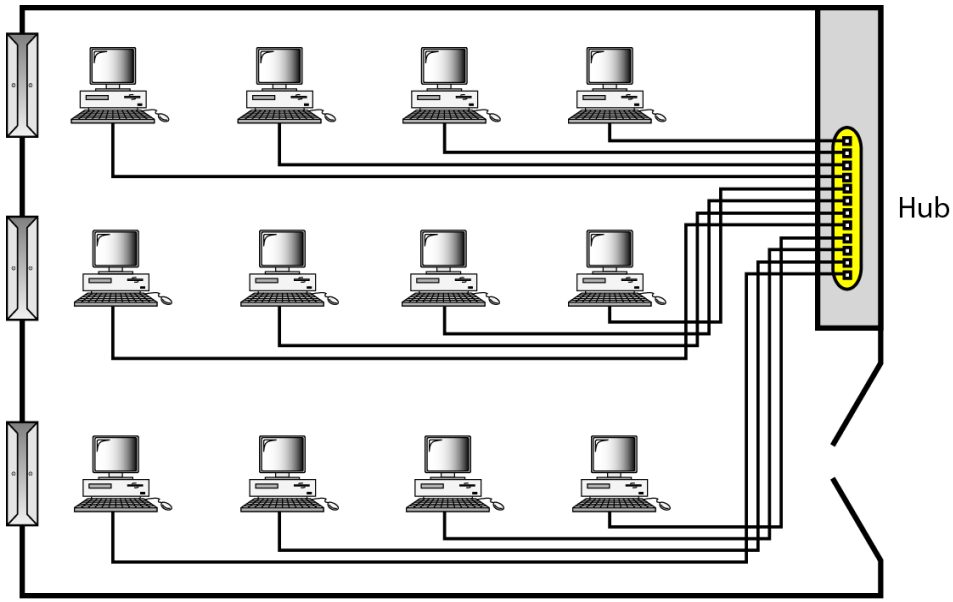

b. Multipoint

# How many kinds of Networks?

- **we can classify networks in different ways:**
- **Based on network size: LAN and WAN (and MAN)**
- **Based on management method: Peer-to-peer and Client/Server**
- **Based on topology (connectivity): Bus, Star, Ring ..**
- **Based on transmission media: Wired (UTP, coaxial cables, fiber-optic cables) and Wireless**

# Network Size

- **Local Area Network (LAN)**
  - **Small network, short distance suitable for a room, a floor, and building. It is limited by number of computers and distance covered or serve a department within an organization**
  - **Examples: Network inside your home**



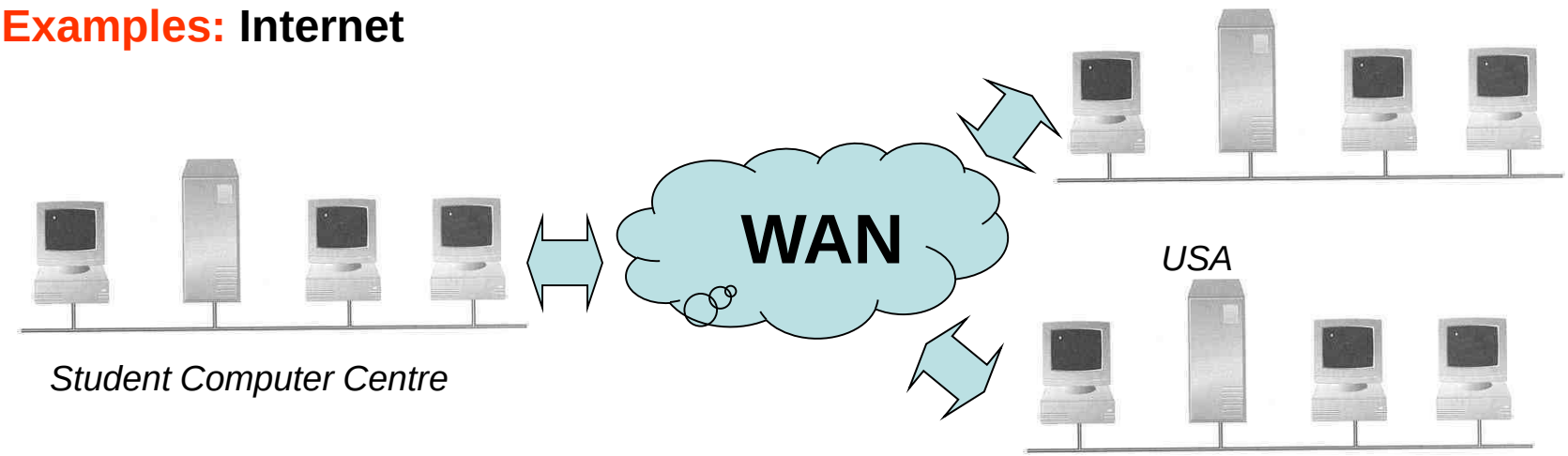

*An isolated LAN connecting 12 computers to a hub*

# Network Size

**A metropolitan area network (MAN)** is a network that interconnects users with computer resources in a geographic area or region larger than that covered by LAN but smaller than the WAN. The term is applied to the interconnection of networks in a city into a single larger network. It is also used to mean the interconnection of several local area networks by bridging them with backbone lines.

**Wide Area Network (WAN)**

- **A network that uses long-range telecommunication links to connect 2 or more LANs/computers housed in different places far apart.**
  - **Towns, states, countries**
- **Examples: Internet**



# Network Size

- **Example WAN technologies:**
  - **ISDN – Integrated Service Digital Network**
    - **Basic rate: 192 Kbps  Primary rate: 1.544Mbps**
  - **T-Carriers — basically digital phone lines**
    - **T1: 1.544Mbps  T3: 28×T1**
  - **Frame relay**
    - **Each link offers 1.544Mbps or even higher**
  - **ATM – Asynchronous Transfer Mode**
    - **Support : 155Mbps or 622Mbps or higher**
  - **SONET – Synchronous Optical Network**
    - **Basic rate OC1: 51.84Mbps**
    - **Support OC12 and up to OC192 (9953.28Mbps) or even higher in the future**

# Peer-to-Peer Networks

- **No hierarchy among computers ⇒ all are equal.**
- **No administrator responsible for the network.**


- **Where peer-to-peer network is appropriate:**
  - **10 or less users**
  - **Security is not an issue**
  - **Only limited growth in the future**

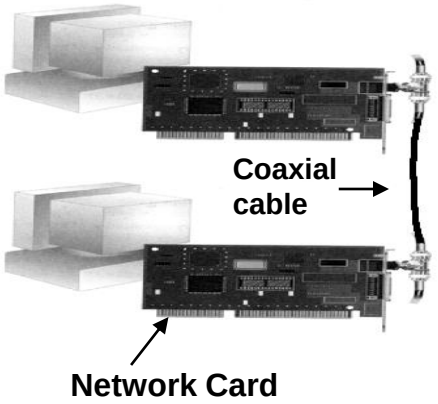
# Clients and Servers

- Network Clients (Workstation)
  - Computers that request network resources or services
- Network Servers
  - Computers that manage and provide network resources and services to clients.
    - Usually have more processing power, memory and hard disk space than clients.
    - Run Network Operating System that can manage not only data, but also users, groups, security, and applications on the network.

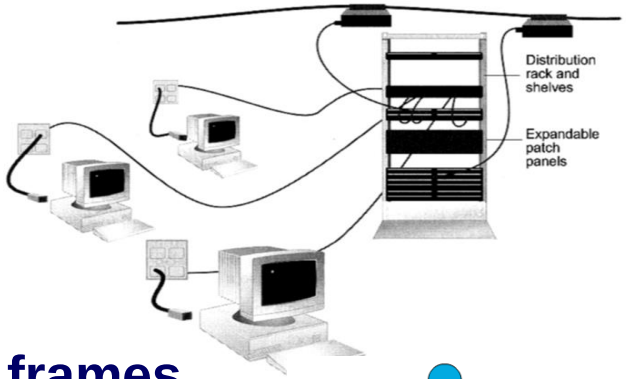
- Advantages of client/server networks
  - Enhance security – only administrator can have access to Server.
  - Support more users – difficult to achieve with peer-to-peer networks

# Network Topology

- **Bus Topology**
  - Simple and low-cost
  - A single cable called a trunk (backbone, segment)
  - Only one computer can send messages at a time

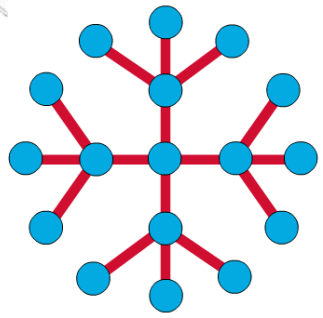



- **Star Topology**
  - Each computer has a cable connected to a single point
  - All signals transmission through the hub; if down, entire network down.



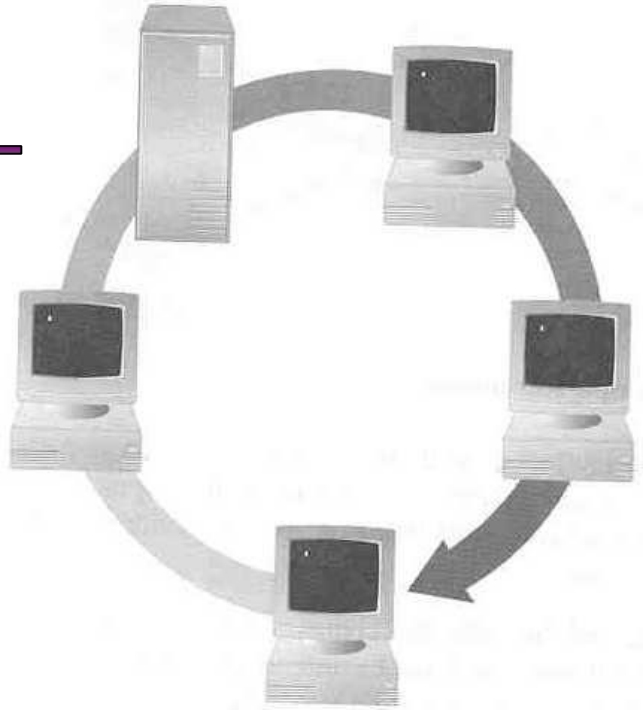

## Extended Star or Tree Topology

- When used with network devices that filter frames or packets, like bridges, switches, and routers, this topology significantly reduces the traffic on the wires by sending packets only to the wires of the destination host.



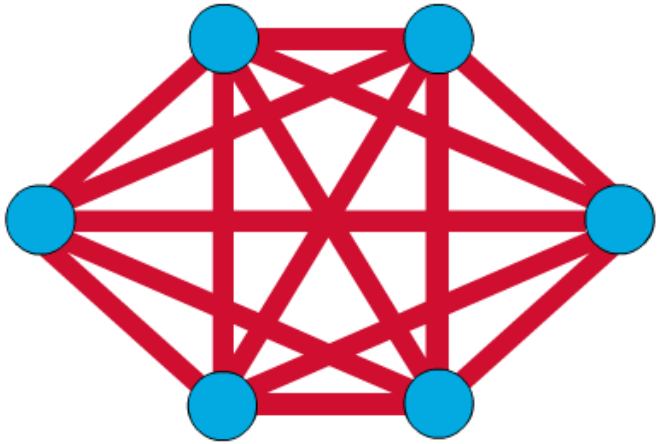
# Ring Topology

- Every computer serves as a repeater to boost signals
- Typical way to send data:
  - Difficult to add computers
  - If one computer fails, whole network fails



# Mesh Topology

- The mesh topology connects all devices (nodes) to each other for redundancy and fault tolerance.
- Implementing the mesh topology is expensive and difficult.

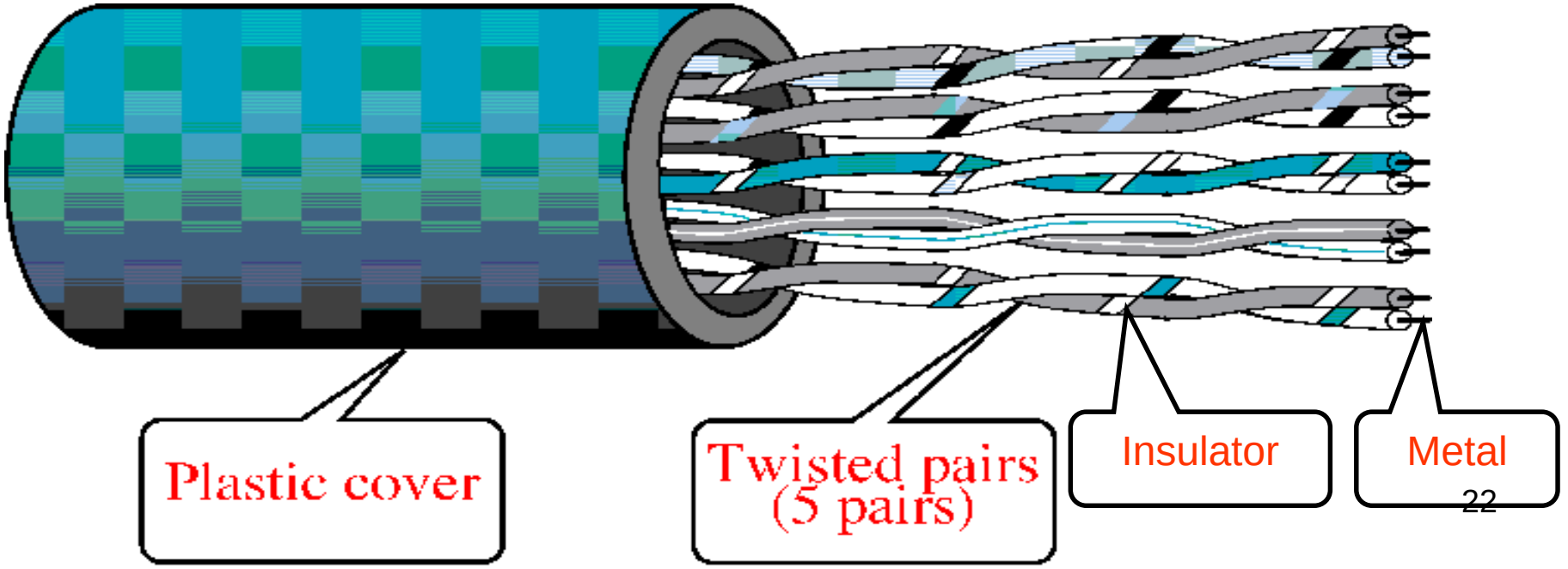


# Transmission Media

- **Two main categories:**
  - **Guided — wires, cables**
  - **Unguided — wireless transmission, e.g. radio, microwave, infrared, sound, sonar**
- **We will concentrate on guided media here:**
  - **Twisted-Pair cables:**
    - **Unshielded Twisted-Pair (UTP) cables**
    - **Shielded Twisted-Pair (STP) cables**
  - **Coaxial cables**
  - **Fiber-optic cables**

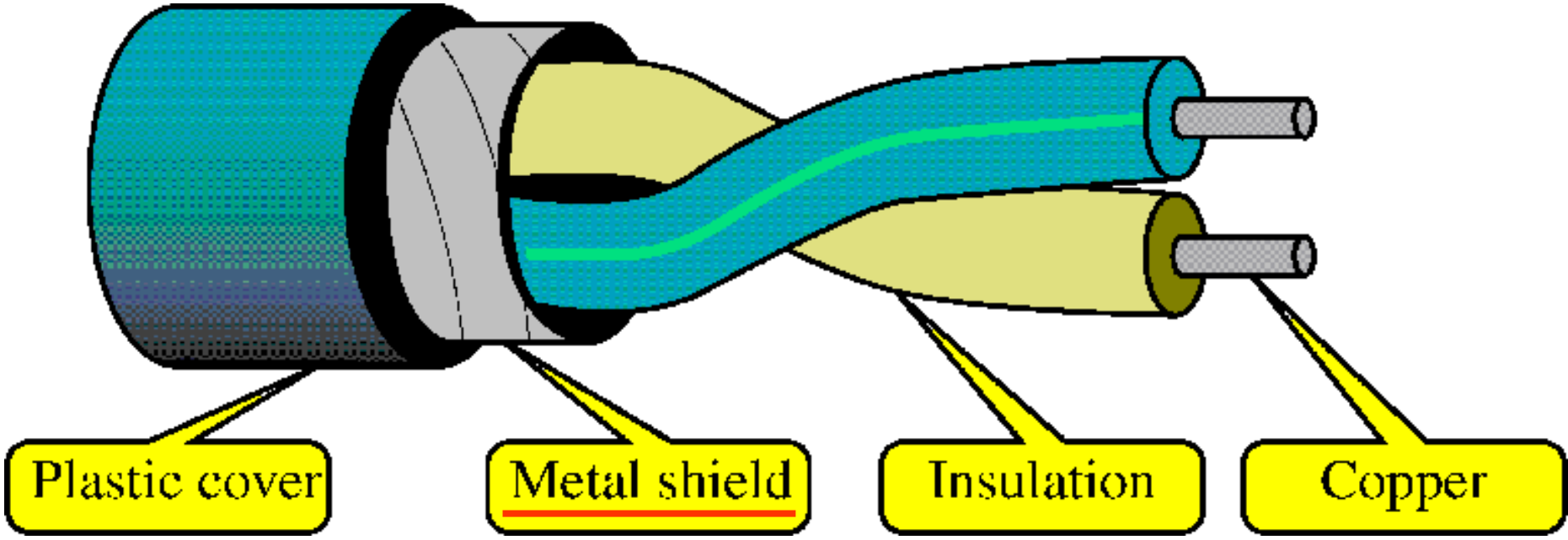
# Unshielded Twisted-Pair (UTP)

- **Typically wrapped inside a plastic cover (for mechanical protection)**
- **A sample UTP cable with 5 unshielded twisted pairs of wires**



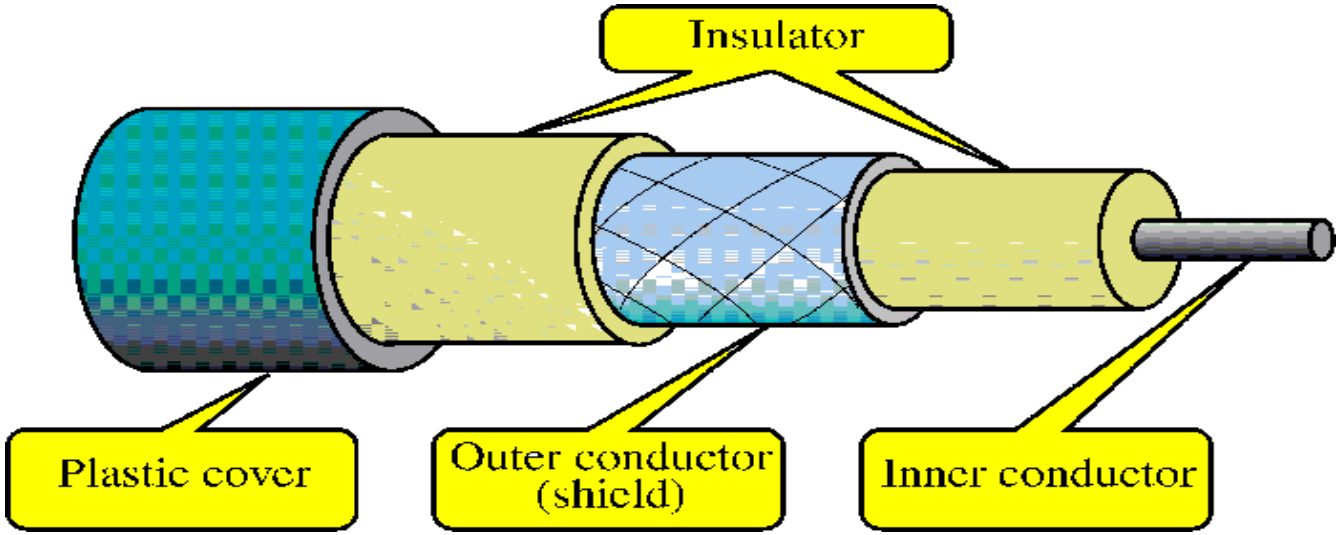
# Shielded Twisted-Pair (STP)

- **STP cables are similar to UTP cables, except there is a metal foil or braided-metal-mesh cover that encases each pair of insulated wires**



# Coaxial Cables

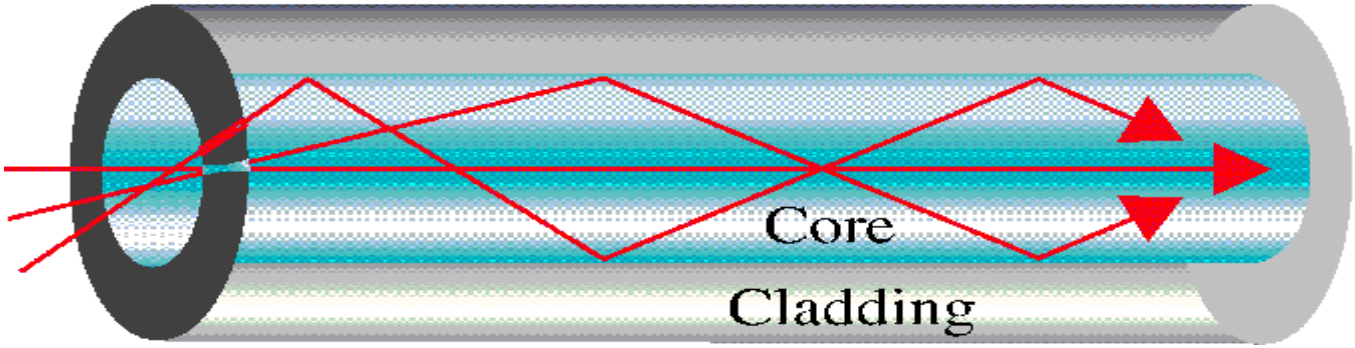
- In general, coaxial cables, or coax, carry signals of 100KHz–500MHz, and speed of up to 10Mbps.
- Outer metallic wrapping serves as a shield against noise.
- Advantage: It is very resistant to Electromagnetic Interference, easy to cut it and adjust the size.
- Disadvantage: not supported by fast Internet standard, more expensive.



# Fiber-Optic Cables

- **Light travels at $3\times10^{8}\ ms^{-1}$ in free space and is the fastest possible speed in the Universe**
- **Light slows down in denser media, e.g. glass**
- **Refraction occurs at interface, with light bending away from the normal when it enters a less dense medium.**
- **We have also Diffraction and Reflection.**

- **An optical fiber consists of a core (denser material) and a cladding (less dense material).**
- **Simplest one is Single mode (with single path 10 Microns).**
- **Multimode 50-100 Microns = multiple paths, whereas step-index = refractive index follows a step-function profile (i.e. an abrupt change of refractive index between the core and the cladding).**
- **Light bounces back and forth along the core.**
- **Common light sources: LEDs and lasers**



# Advantages and Disadvantages

- ☺ Noise resistance — external light is blocked by outer jacket
- ☺ Less signal attenuation — a signal can run for miles without regeneration (currently, the lowest measured loss is about ~4% or 0.16dB per km)
- ☺ Higher bandwidth — currently, limits on data rates come from the signal generation/reception technology, not the fiber itself
- ☹ Cost — Optical fibers are expensive
- ☹ Installation/maintenance — any crack in the core will degrade the signal, and all connections must be perfectly aligned

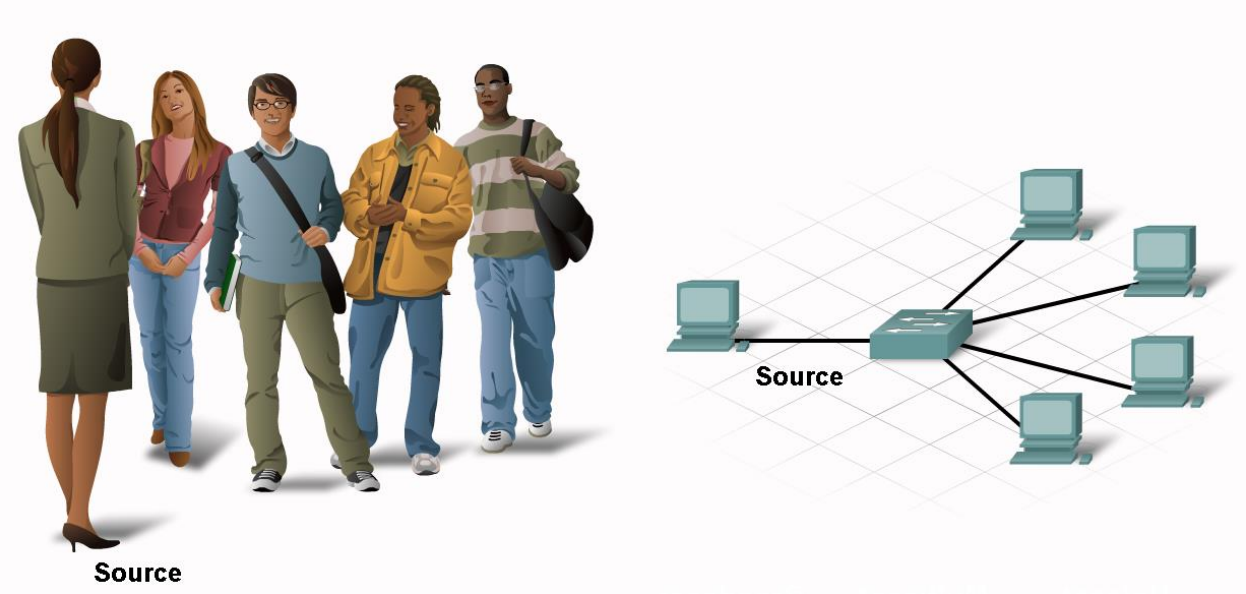
# Communication Protocols

Message Patterns

**Unicast** – single destination

**Multicast** – same message to a group

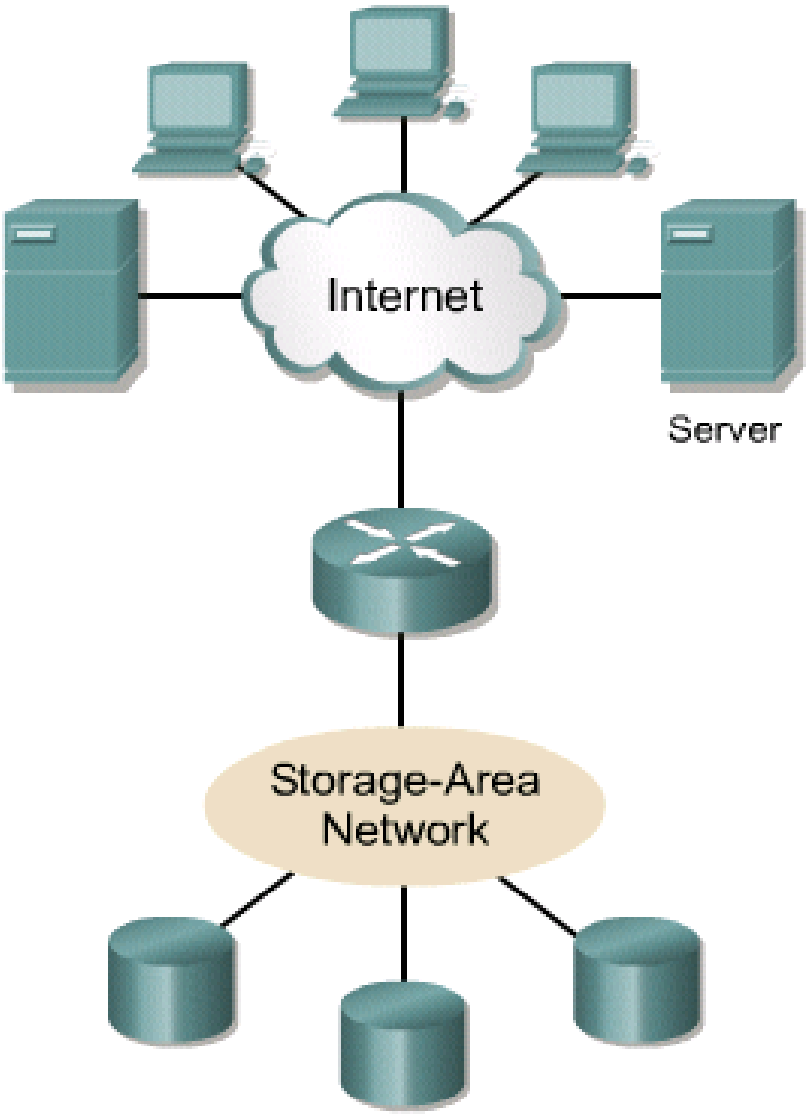
**Broadcast** – all hosts need to receive the message



# Storage-Area Networks (SANs)

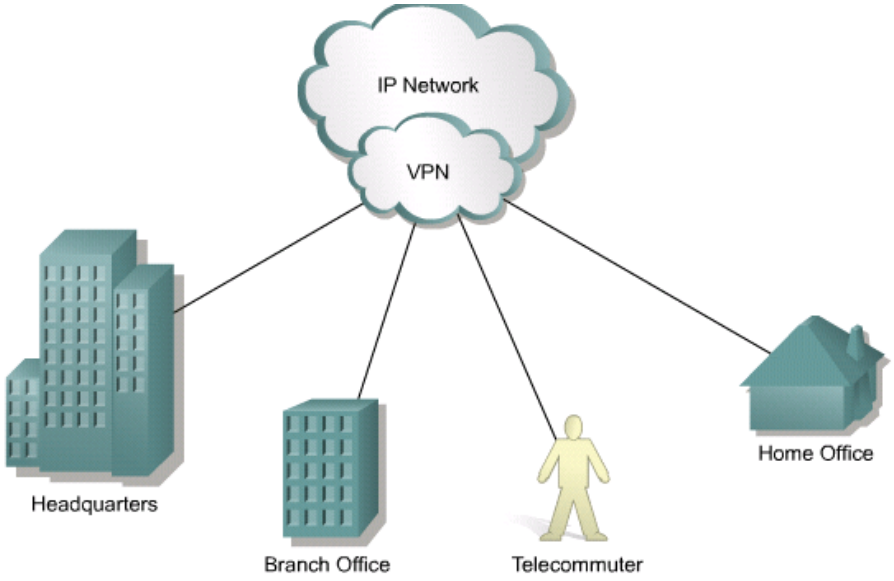
- A SAN is a dedicated, high-performance network used to move data between servers and storage resources.
- Separate, dedicated network, that avoids any traffic conflict between clients and servers
- SANs offer the following features:
  - **Performance** – allows concurrent access of disk or tape arrays by two or more servers at high speeds
  - **Availability** – have disaster tolerance built in, because data can be mirrored using a SAN up to 10km or 6.2 miles away.
  - **Scalability** – Like a LAN/WAN, it can use a variety of technologies. This allows easy relocation of backup data, operations, file migration, and data replication between systems.

# SAN



# Virtual private network (VPN)

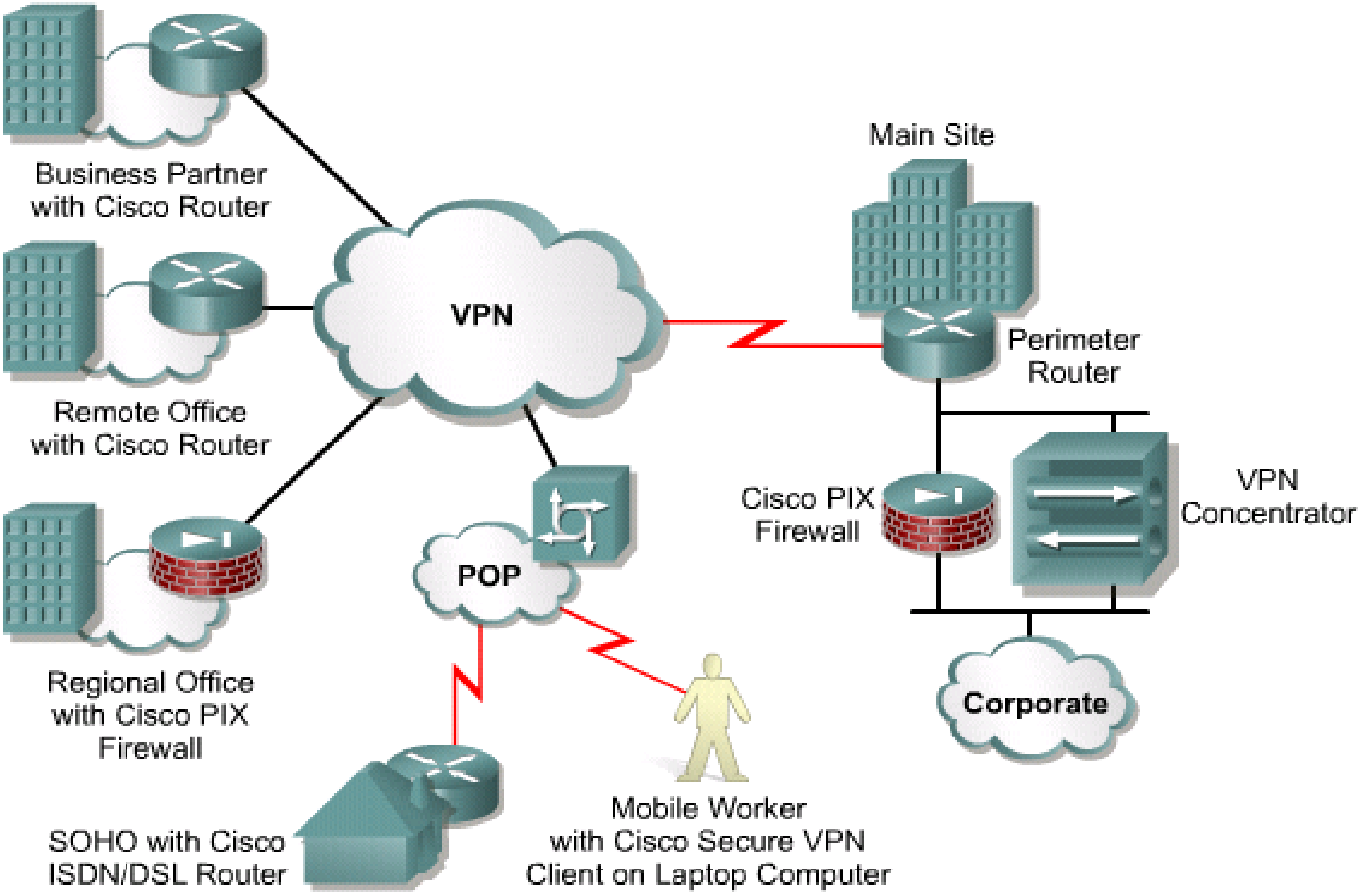
- A VPN is a private network that is constructed within a public network such as the Internet.
- It offers secure, reliable connectivity over a shared public network infrastructure such as the Internet.
- A telecommuter can access the network of the company through the Internet by building a secure tunnel between the telecommuter's PC and a VPN router in the company



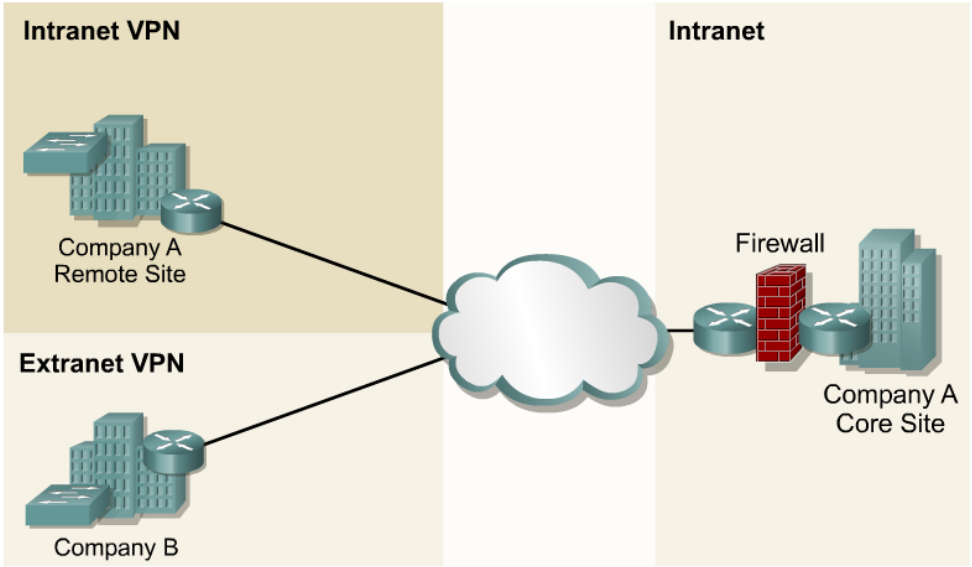
# Benefits of VPNs

- Three main types of VPNs:
  - **Access VPNs** – provide remote access to a mobile worker and a SOHO to the hq of the Intranet or Extranet over a shared infrastructure.
  - **Intranet VPNs** – link regional and remote offices to the hq of the internal network over a shared infrastructure using *dedicated connections*. They allow access only to the employees of the enterprise.
  - **Extranet VPNs** – link business partners to the hq of the network over a shared infrastructure using *dedicated connections*. They allow access to users outside the enterprise

# VPNs

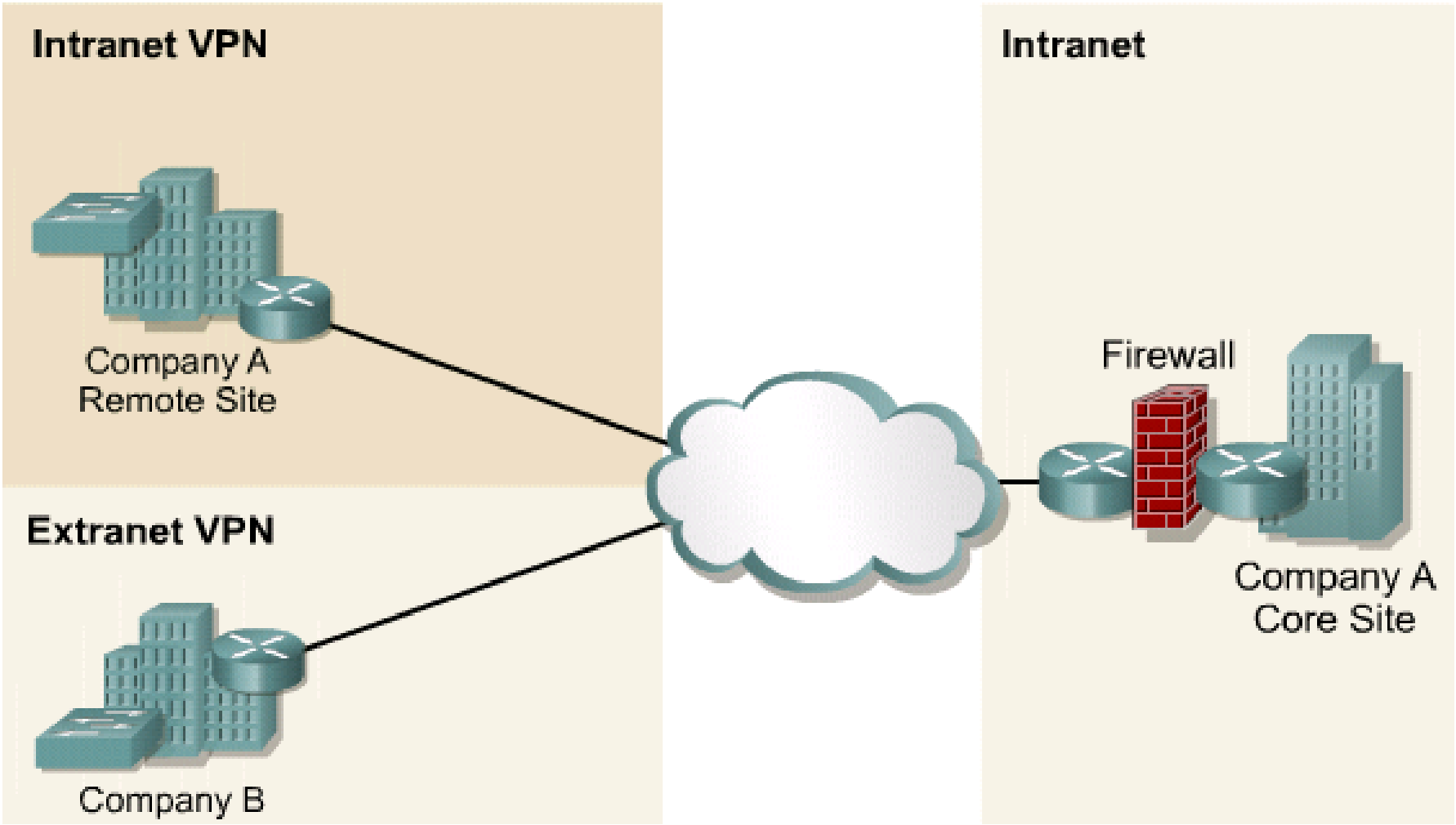

Business Partner
with Cisco Router
Remote Office
with Cisco Router
Regional Office
with Cisco PIX
Firewall
SOHO with Cisco
ISDN/DSL Router
VPN
POP
Mobile Worker
with Cisco Secure VPN
Client on Laptop Computer
Main Site
Perimeter
Router
Cisco PIX
Firewall
VPN
Concentrator
Corporate

# Intranets and extranets




- **Intranets** are designed to permit access by users who have access privileges to the internal LAN of the organization.
- Within an Intranet, Web servers are installed in the network.
- Browser technology is used as the common front end to access information such as financial data or graphical, text-based data stored on those servers.
- **Extranets** refer to applications and services that are Intranet based, and use extended, secure access to external users or enterprises.
- This access is usually accomplished through passwords, user IDs, and other application-level security.

# Intranets and extranets



# Importance of bandwidth

- Bandwidth is the amount of information that can flow through a network connection in a given period of time.
- **Bandwidth is finite**
  - the bandwidth of a modem is limited to about 56 kbps by both the physical properties of twisted-pair phone wires and by modem technology
- **Bandwidth is not free**
  - For WAN connections bandwidth is purchased from a service provider
- A key factor in analyzing network performance and designing new networks
- The demand for bandwidth is ever increasing

# Measurement

- In digital systems, the basic unit of bandwidth is bits per second (bps)
- The actual bandwidth of a network is determined by a combination of the physical media and the technologies chosen for signaling and detecting network signals

| Typical Media | Maximum Theoretical Bandwidth | Maximum Theoretical Distance |
|---|---|---|
| 50-Ohm Coaxial Cable (10BASE2 Ethernet; Thinnet) | 10 Mbps | 185 m |
| 50-Ohm Coaxial Cable (10BASE5 Ethernet; Thicknet) | 10 Mbps | 500 m |
| Category 5 Unshielded Twisted Pair (UTP) (10BASE-T Ethernet) | 10 Mbps | 100 m |
| Category 5 Unshielded Twisted Pair (UTP) (100BASE-TX Ethernet) | 100 Mbps | 100 m |
| Category 5 Unshielded Twisted Pair (UTP) (1000BASE-TX Ethernet) | 1000 Mbps | 100 m |
| Multimode Optical Fiber (62.5/125mm) (100BASE-FX Ethernet) | 100 Mbps | 2000 m |
| Multimode Optical Fiber (62.5/125mm) (1000BASE-SX Ethernet) | 1000 Mbps | 220 m |
| Multimode Optical Fiber (50/125mm) (1000BASE-SX Ethernet) | 1000 Mbps | 550 m |

# Limitations

- Bandwidth is limited by a number of factors
  - Media
  - Network devices
  - Physics
- Each have their own limiting factors
- Actual bandwidth of a network is determined by a combination of the physical media and the technologies chosen for signaling and detecting network signals

# Throughput

- Throughput is the actual, measured, bandwidth, at a specific time of day, using specific internet routes, while downloading a specific file.  The throughput is often far less than the maximum bandwidth
- Factors that determine throughput:
  - Internetworking devices
  - Type of data being transferred
  - Network topology
  - Number of users on the network
  - User computer
  - Server computer

# Data transfer calculation

**Best Download**

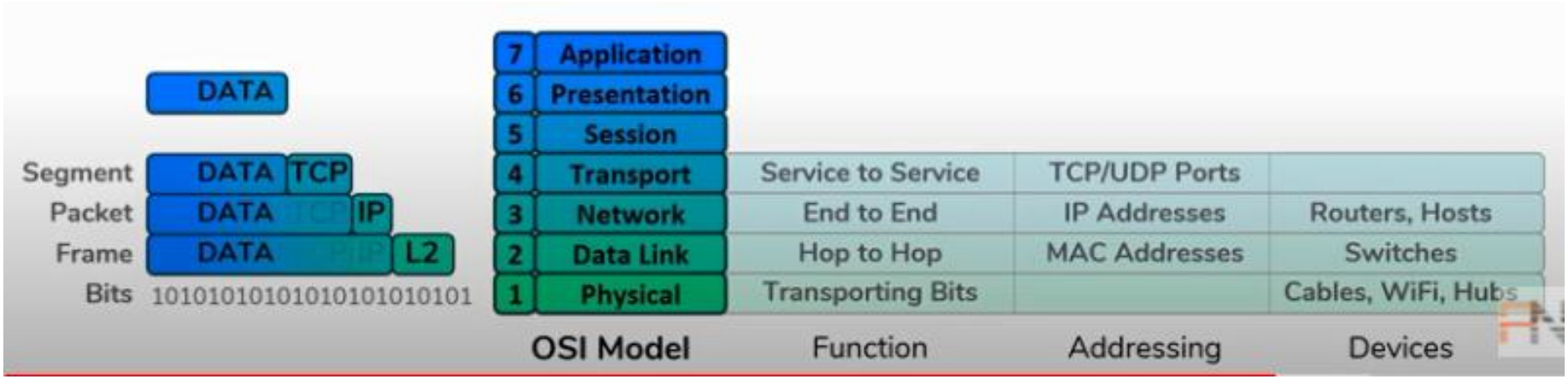
$$T = \frac{S}{BW}$$

**Typical Download**

$$T = \frac{S}{P}$$

| | |
|---|---|
| BW | Maximum theoretical bandwidth of the "slowest link" between the source host and the destination host (measured in bits per second) |
| P | Actual throughput at the moment of transfer (measured in bits per second) |
| T | Time for file transfer to occur (measured in seconds) |
| S | File size in bits |

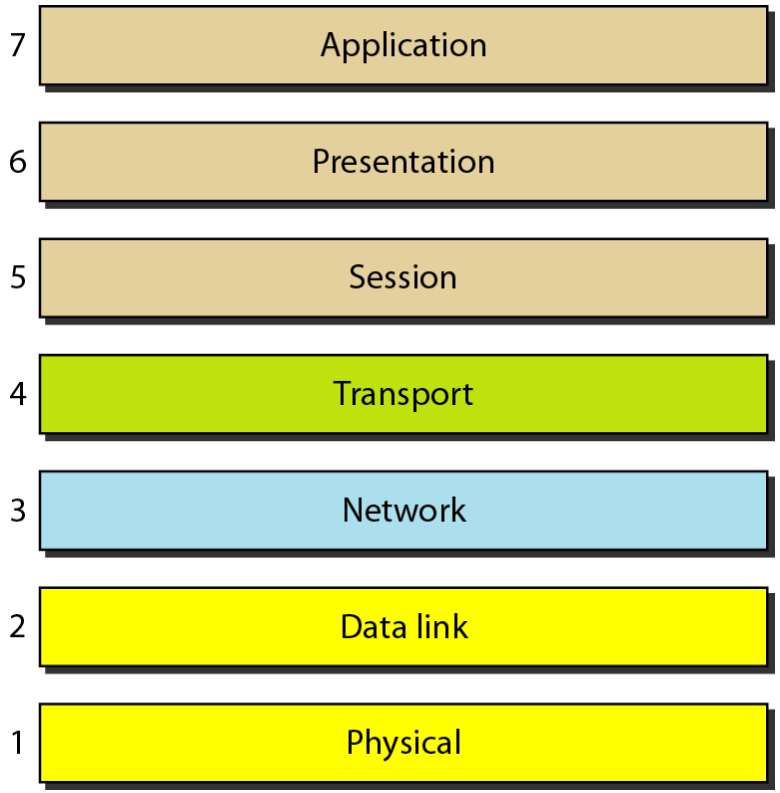
# Network Models



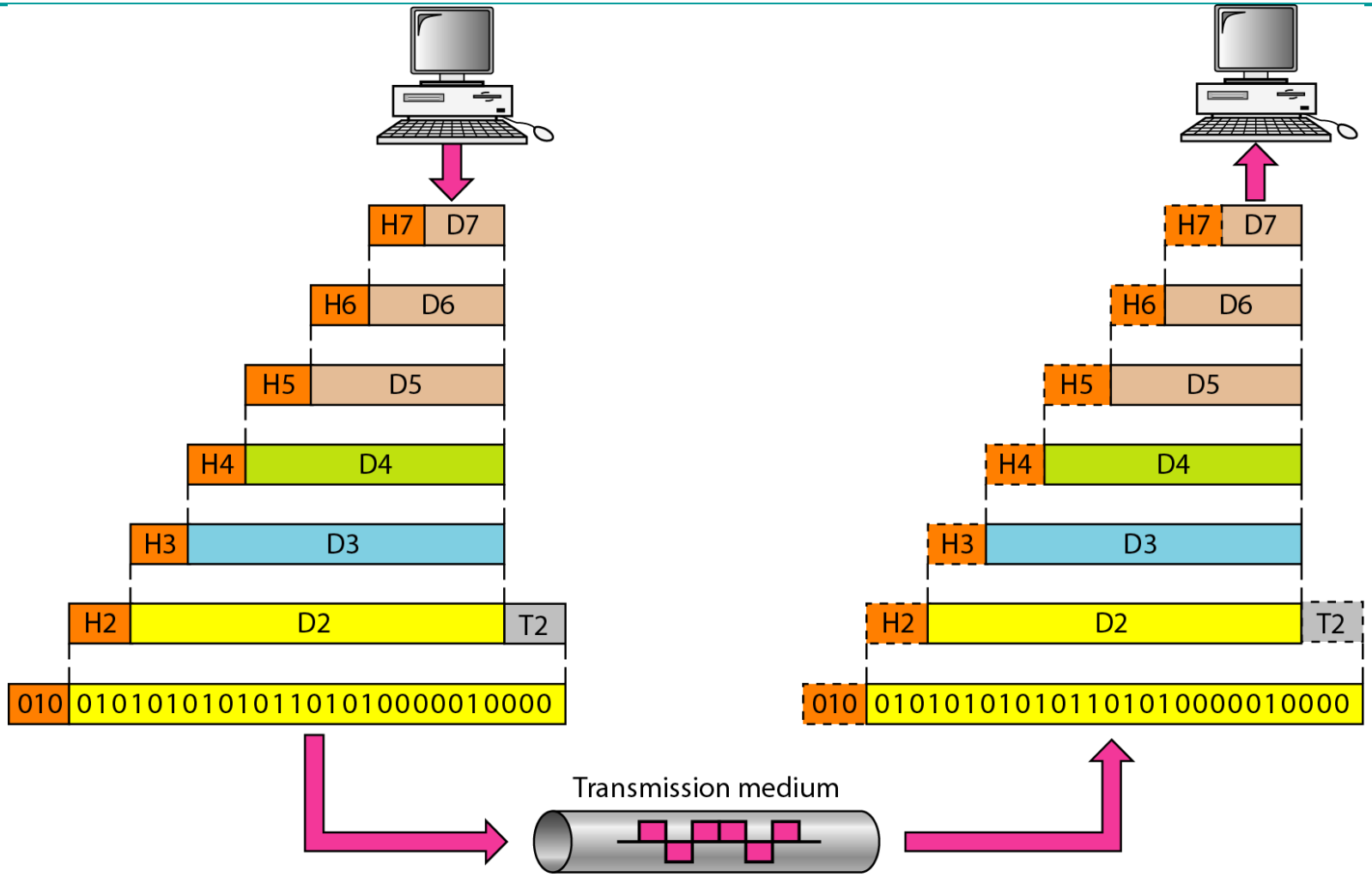
# THE OSI MODEL

*Established in 1947, the International Standards Organization (ISO). 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.*

*Seven layers of the OSI model*



# *An exchange using the OSI model*

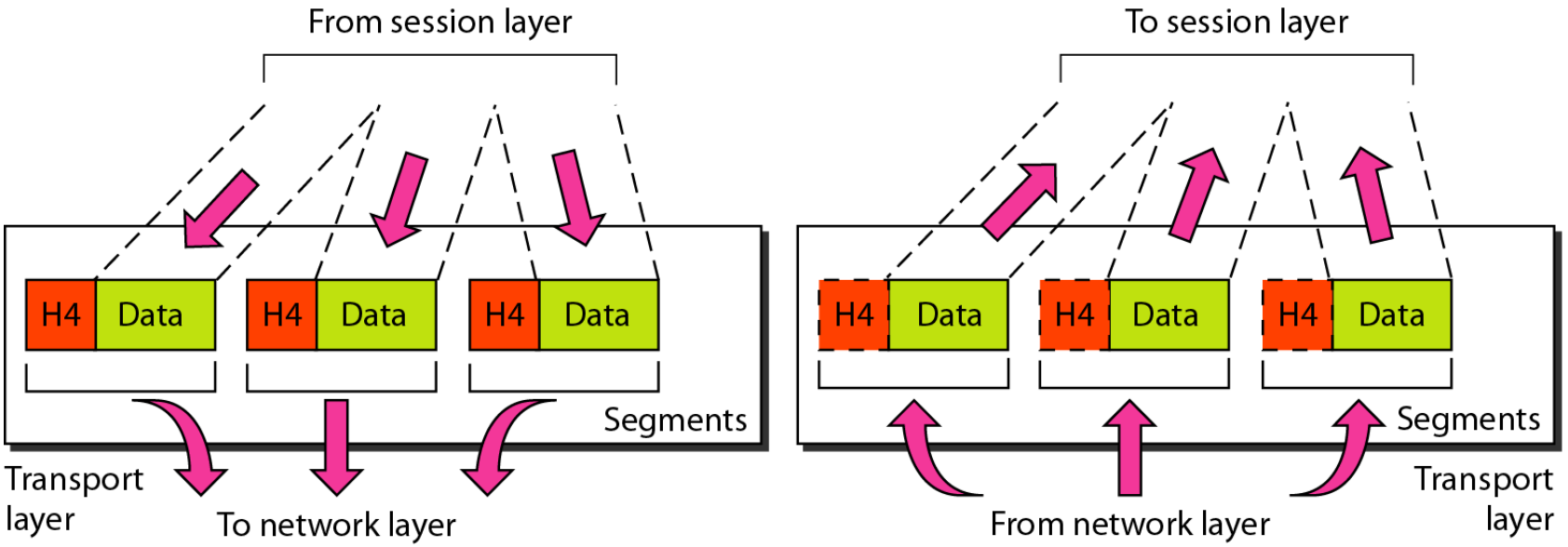



The data link layer is responsible for moving frames from one hop (node) to the next.

*Network layer:*

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

*Transport layer:*

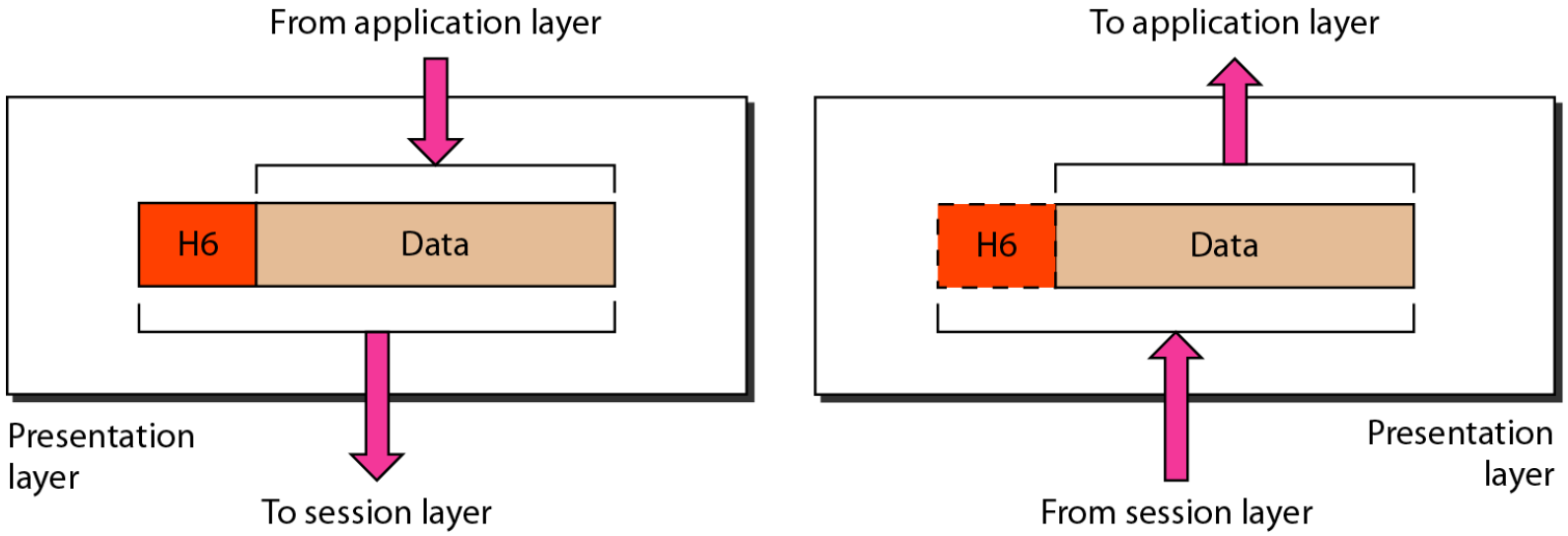



The transport layer is responsible for the delivery of a message from one process to another.

*Session layer:*

The session layer is responsible for dialog control and synchronization.

*Presentation layer:*

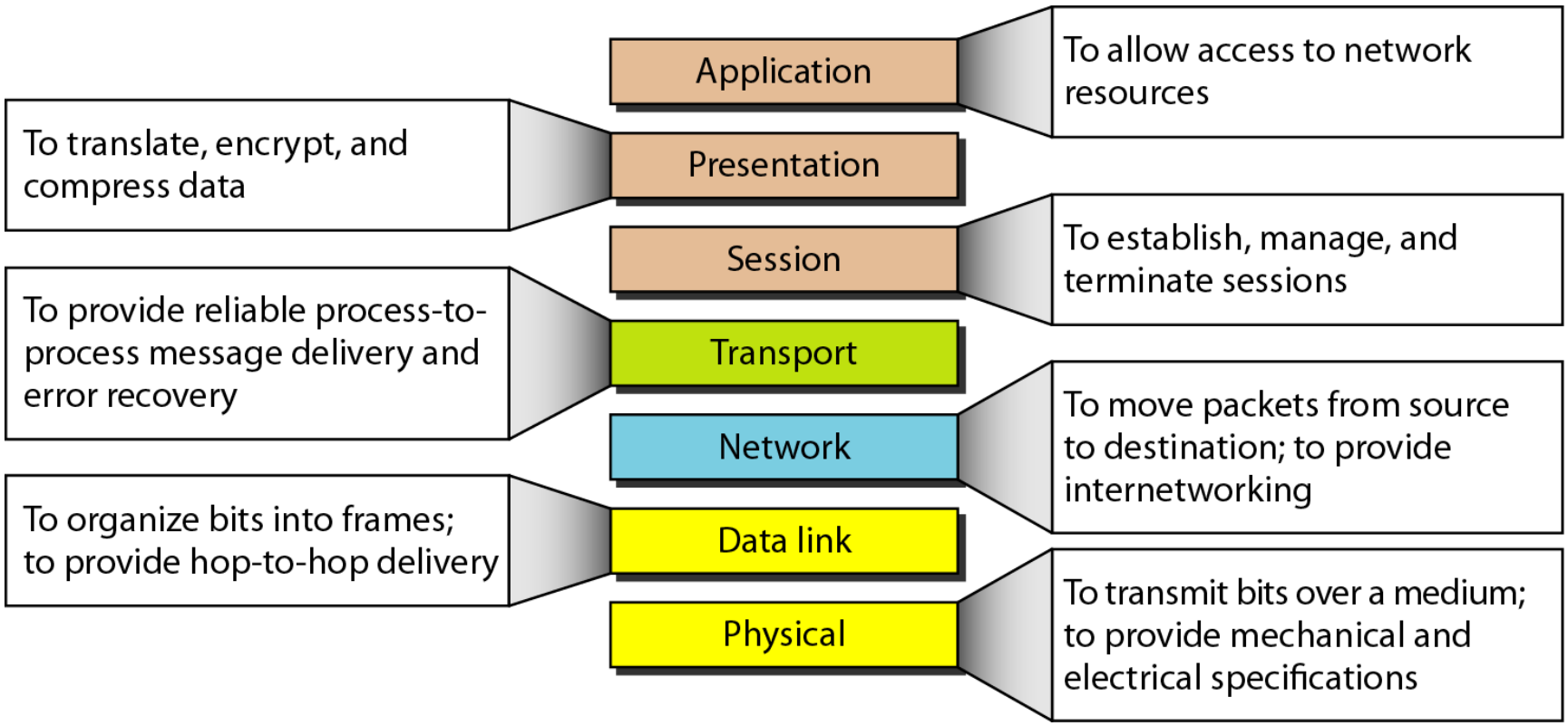


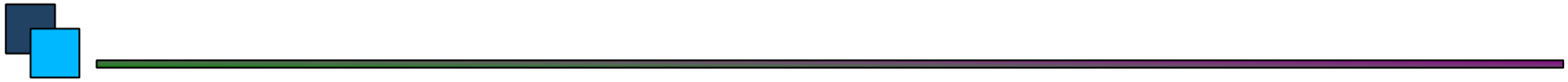

The presentation layer is responsible for translation, compression, and encryption.

*Application layer:*

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

# *Summary of layers*





# TCP/IP

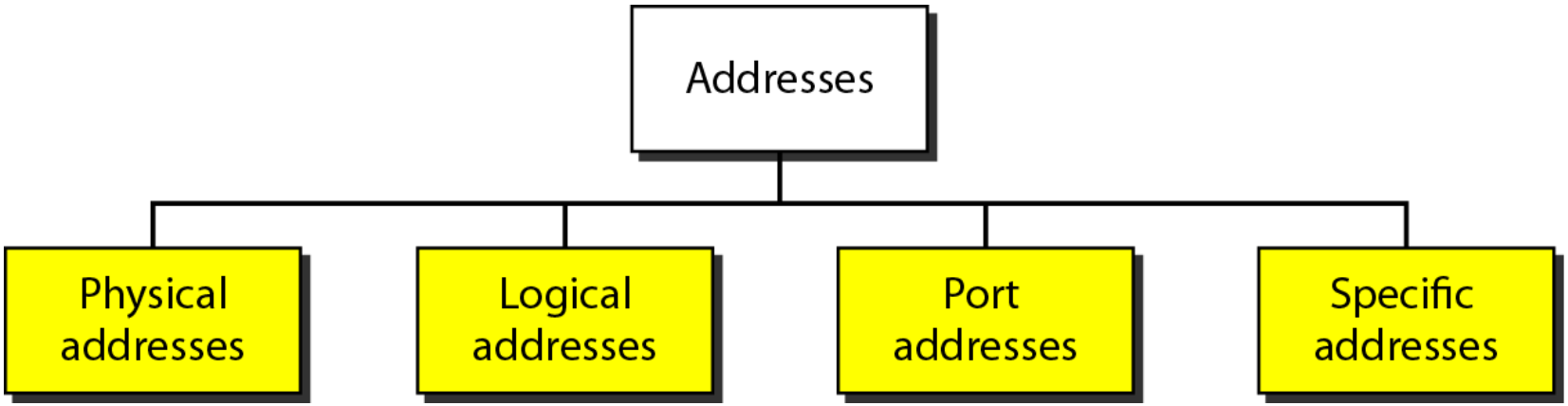
Dr. Lway Faisal

# TCP/IP PROTOCOL SUITE

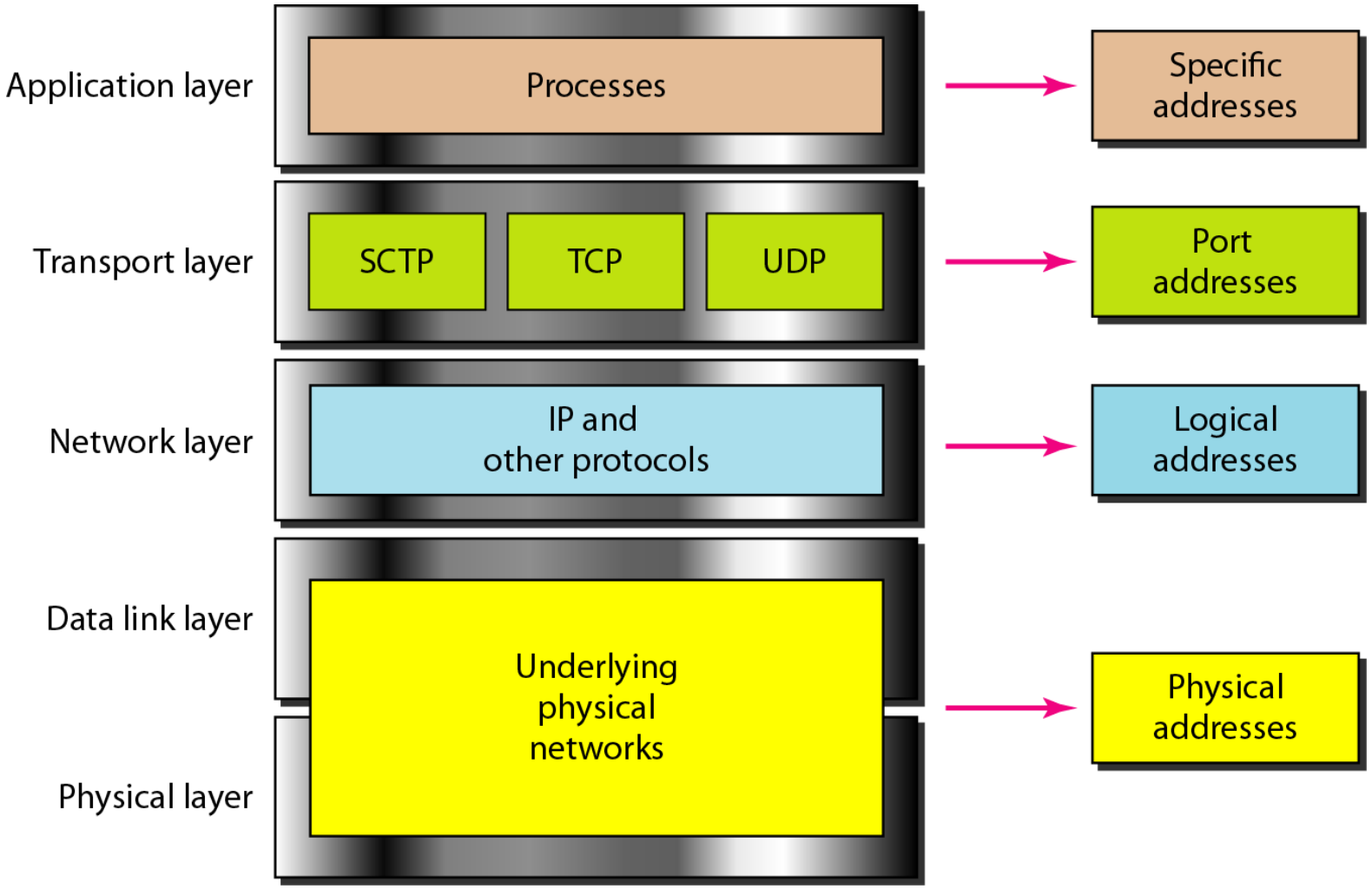
*When TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.*

# ADDRESSING

*Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.*



## *Relationship of layers and addresses in TCP/IP*

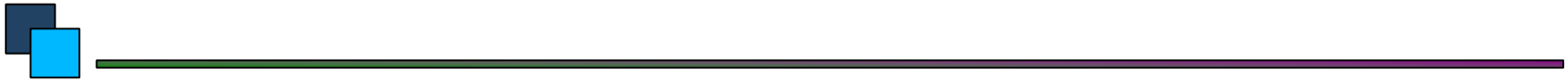


# *Physical Address*

- *Physical address or (hardware Address), or MAC address.*
- *Each node has a unique MAC Address: Globally identifier that burned into your RAM of your network interface card.*
- *MAC Address assigned by manufacturer , each factory has a block of address assigned by IEEE.*
- *No two networks in the world have the same Address.*
- *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.



# Network Layer:
# Logical Addressing

Dr. Lway Faisal

An IP address (Internet Protocol Address) or (logical Address) is a unique address that devices use it in order to communicate with each other.

IP addresses are managed and created by the Internet Assigned Numbers Authority (**IANA**).

IP have two versions:

1. IPv4 is 32bits
2. IPv6 is 128bits

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

# IPv4 ADDRESSES

**An IPv4 address is 32 bits long, are unique and universal.**

A protocol IPv4 has an address space. An **address space** is the total number of addresses used by the protocol. If a protocol uses *N* bits to define an address, the address space is $2^N$.

IPv4 uses 32-bit addresses, which means that the address space is $2^{32}$ or 4,294,967,296 (more than 4 billion). This means that, theoretically, if there were no restrictions, *more than 4 billion devices could be connected to the Internet.*

## Notations

There are two prevalent notations to show an IPv4 address: binary notation and dotted-decimal notation.

### *Binary Notation*

In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address. Example:

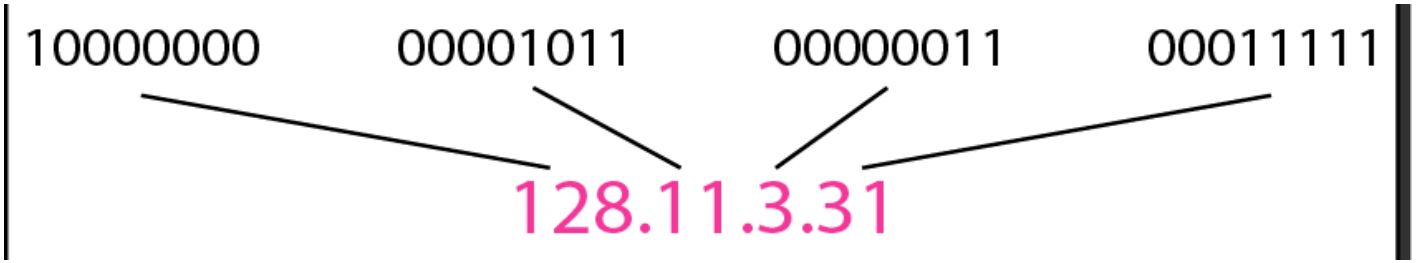
01110101 10010101 00011101 00000010

00000000.00000000.00000000.00000000

11111111.11111111.11111111.11111111

## *Dotted-Decimal Notation*

To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. Example:




Note that because each byte (octet) is 8 bits, each number in dotted-decimal notation is a value ranging from 0 to 255.

# Example 2.1

***Change the following IPv4 addresses from binary notation to dotted-decimal notati***

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

***Solution***

***We replace each group of 8 bits with its equivalent decimal number and add dots for separation.***

a. 129.11.11.239

b. 193.131.27.255

# Example 2.2

***Change the following IPv4 addresses from dotted-decimal notation to binary no***

a. 111.56.45.78

b. 221.34.7.82

***Solution***

***We replace each decimal number with its binary equivalent (see Appendix B).***

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

## Example 2.3

***Find the error, if any, in the following IPv4 addresses.***

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

***Solution***

***a. There must be no leading zero (045).***

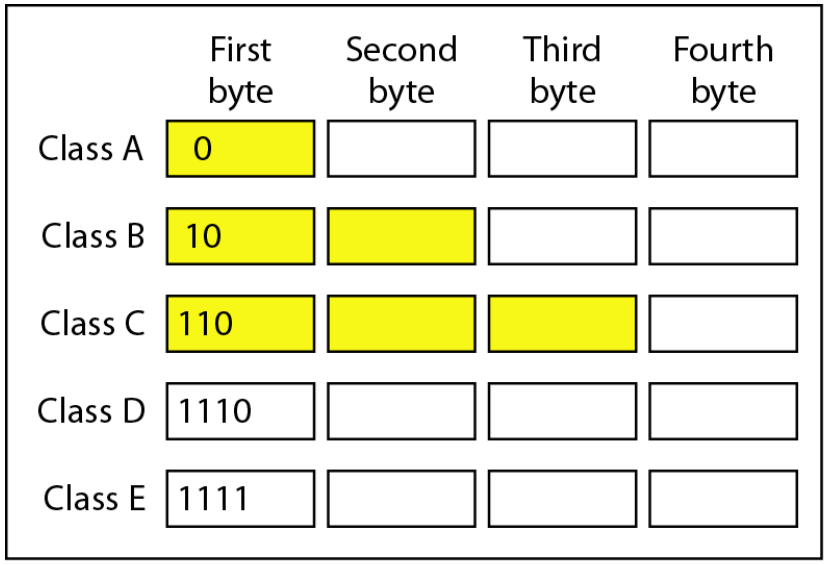
***b. There can be no more than four numbers.***

***c. Each number needs to be less than or equal to 255.***

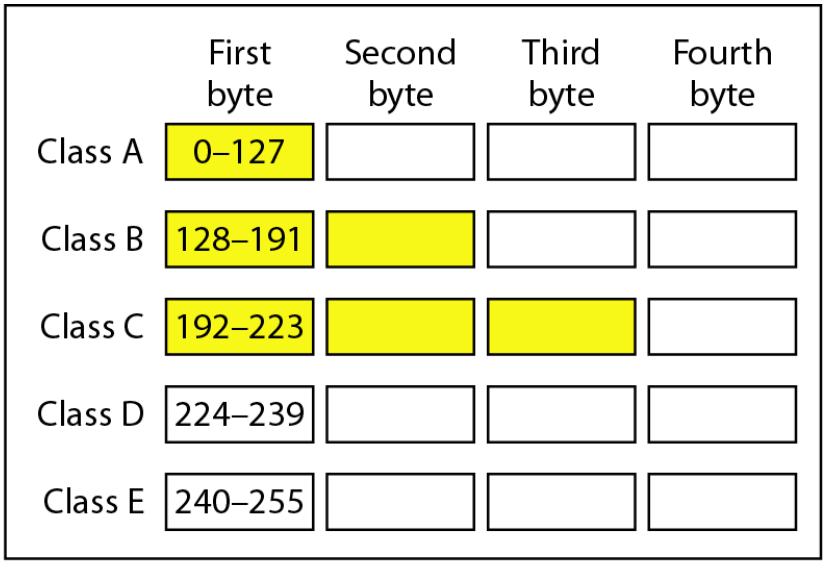
***d. A mixture of binary notation and dotted-decimal notation is not allowed.***

# Classful Addressing

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




a. Binary notation




b. Dotted-decimal notation

***Finding the classes in binary and dotted-decimal notation***

# *Example 2.4*

***Find the class of each address?***

***a.*** **0**0000001 00001011 00001011 11101111

***b.*** **110**00001 10000011 00011011 11111111

***c.*** **14**.23.120.8

***d.*** **252**.5.15.111

***Solution***

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

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

***c. The first byte is 14; the class is A.***

***d. The first byte is 252; the class is E.***