

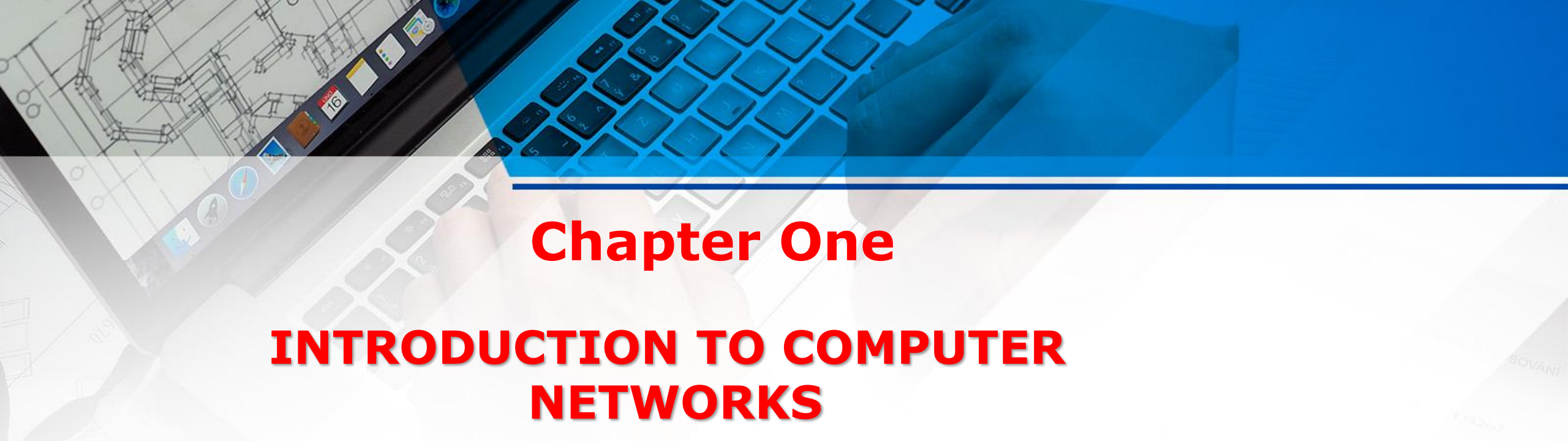


**JAMHURIYA UNIVERSITY
OF SCIENCE AND TECHNOLOGY (JUST)**

Networking Essentials

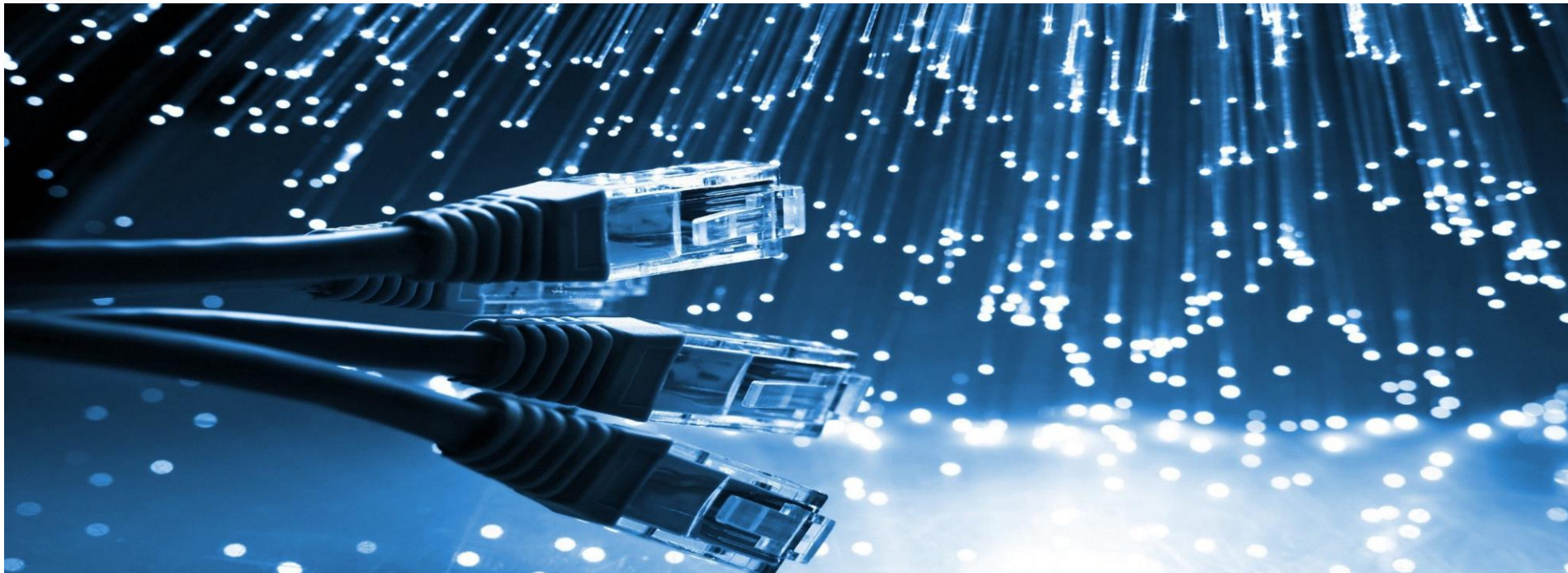
Semester III

Lecturer: Abdullahi Ahmed Aden



Chapter One

INTRODUCTION TO COMPUTER NETWORKS





Chapter Outlines

- ☒ Introduction
- ☐ Networking Topologies
- ☐ The OSI Model
- ☐ The Ethernet LAN
- ☐ Addresses
- ☐ Home Networking
- ☐ Assembling an Office LAN



INTRODUCTION TO NETWORKING

Network Definition

- Networking, or computer networking, **is the process of connecting two or more computing devices, such as desktop computers, mobile devices, routers or applications**, to enable the transmission and exchange of information and resources.
- Computer networking refers to interconnected computing devices that can exchange data and share resources with each other. These networked devices use a system of rules, called communications protocols, to transmit information over physical or wireless technologies.
- The first working network, called **ARPANET**, was created in the late **1960s** and was funded by **the U.S. Department of Defense**. Government researchers used to share information at a time when computers were large and difficult to move.
- We have come a long way today from that basic kind of network. Today's world revolves around the internet, which is a network of networks that connects billions of devices across the world. Organizations of all sizes use networks to connect their employees' devices and shared resources such as printers.



Continue

Every day, people use computer networks for a wide range of activities: **browsing the Internet, sending and receiving email, scheduling meetings, sharing files, exchanging images, and accessing online applications.** Networks connect computers and devices together with the goal of enabling resource sharing. When local networks around the world are interconnected, they form the Internet

Purpose Of The Network

- Sharing Information and Sharing Resource
- Internet
- Sending and Receiving Emails
- Online meetings and Video Conference
- And itc.

Network Examples



Figure 1:
Basic and start network - just two PCs
connecting together using UTP Crossover Cable.



Figure 2:
Five computers connecting
together using a HUB to
share information



Figure 3:
An UTP Cable Ends

Network Example

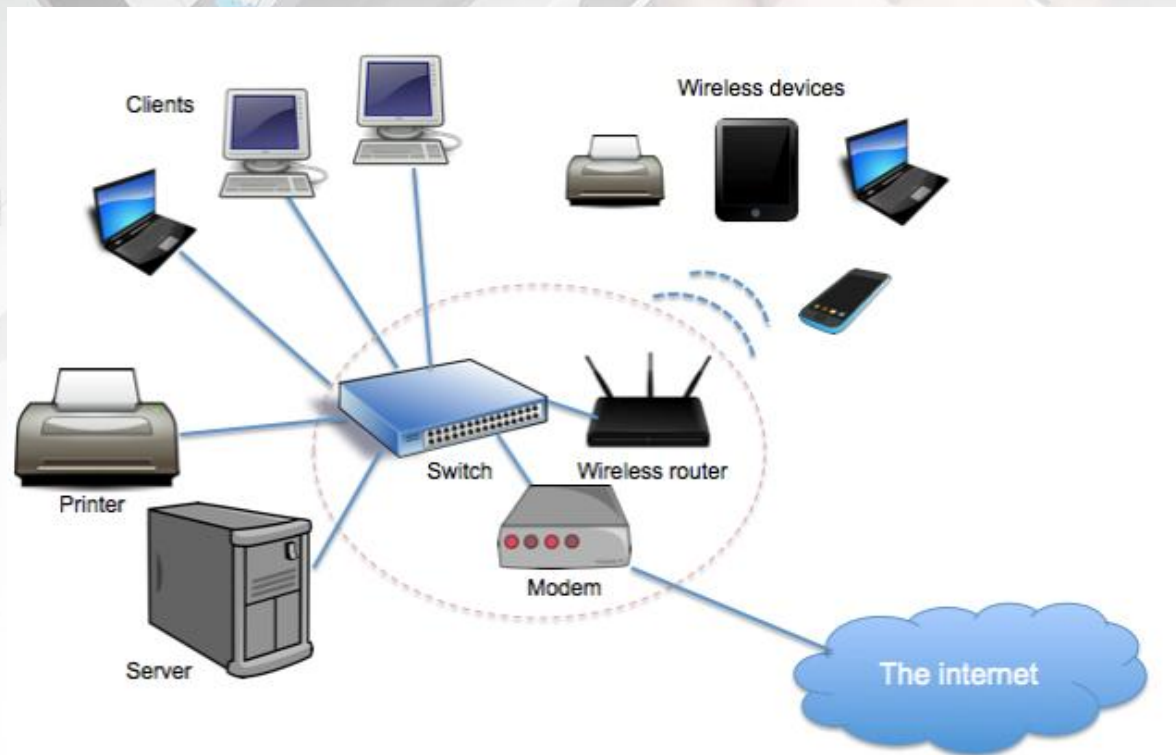


Figure 4:
A basic office network with an Internet Connection

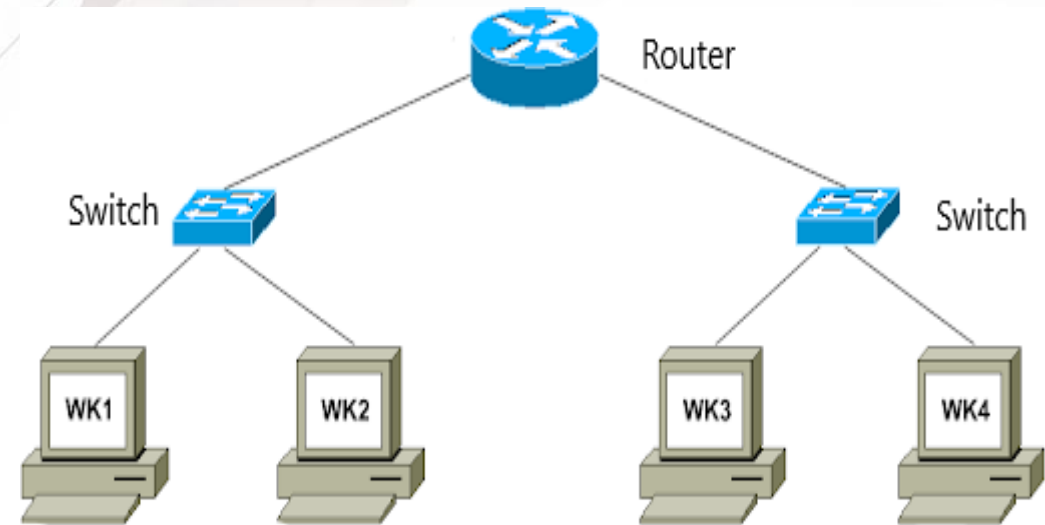


Figure 5:
Two switched networks connected together with a Router to share Data



Basic Requirements to build a network

Minimum Requirement for Creating a Network

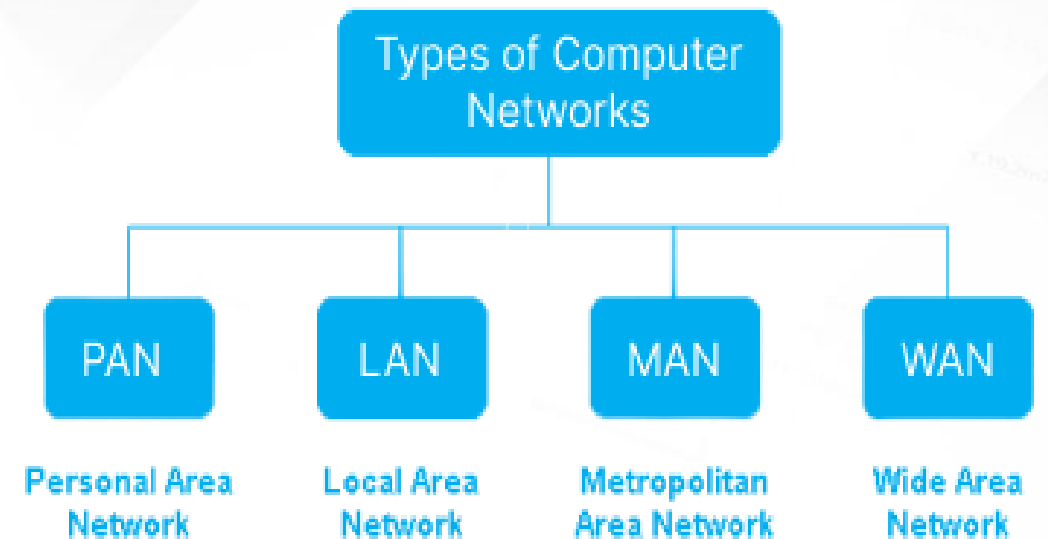
- More than one Computer/device (Desktop, Laptop, Server etc.)
- An Operating System (OS)
- Network Interface Card (NIC)
- Protocol (TCP/IP)
- Transmission Media(guided and unguided)
- Hub, Switch, Router....



Types of Network

Types of Networks

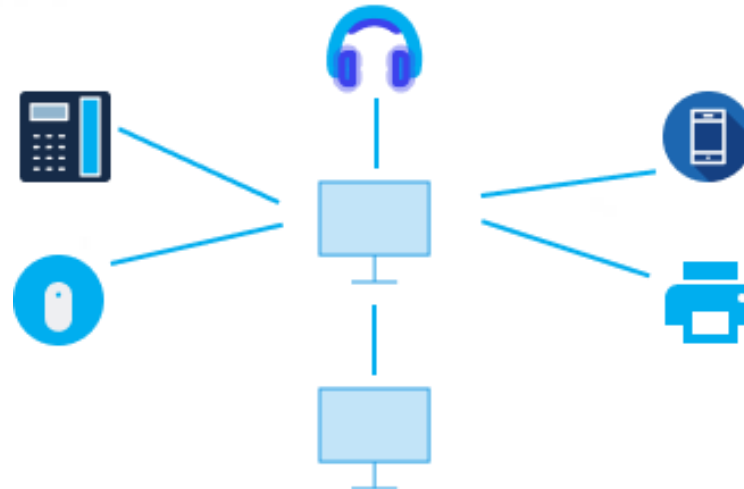
- According to the communication requirements, multiple types of network connections are available. The networks in use today can be generally categorized based on their geographic span.



Personal Area Network (PAN)

Personal area network (PAN): A PAN is the smallest type of network and has a limited span, interconnecting personal devices such as **Bluetooth** or **Wi-Fi**. They are commonly used for **sharing files, printing documents, and streaming media among devices**.

Personal Area Network (PAN)



Advantage:

- Convenient communication among personal devices.
- Flexible, wireless connection.
- Cost-effective using low-cost technologies.
- More secure communication channels over short distances.

Advantage:

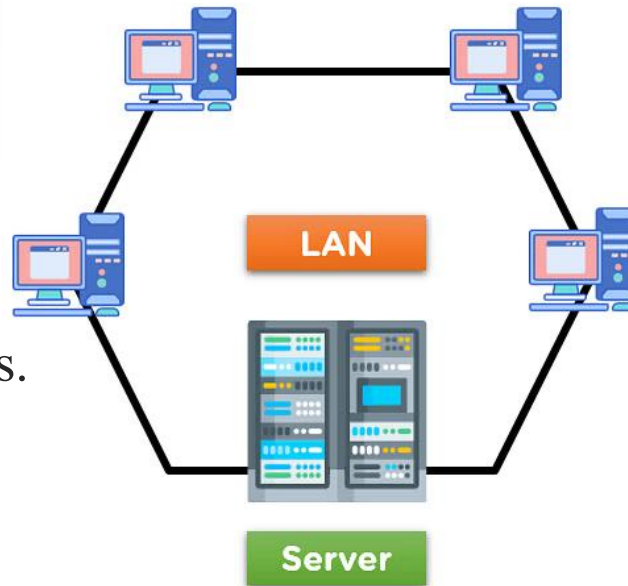
- Limited range of communication.
- Only a particular amount of devices can be linked.
- Susceptible to interference from other wireless devices.
- Slower data transfer speeds compared to wired connections.

Local Area Network (LAN)

Local area network (LAN): A LAN is a network commonly used to interconnect and share computer resources inside a building or multiple buildings in a limited area, such as a **home**, **office**, or **school**. LANs typically use **wired** or **wireless technologies** to connect devices to a local network.

Advantage:

- Fast and reliable communication among devices.
- A cost-effective way to share resources such as printers and files.
- Secure communication within a closed network.
- Easy to set up and manage.



Disdvantage:

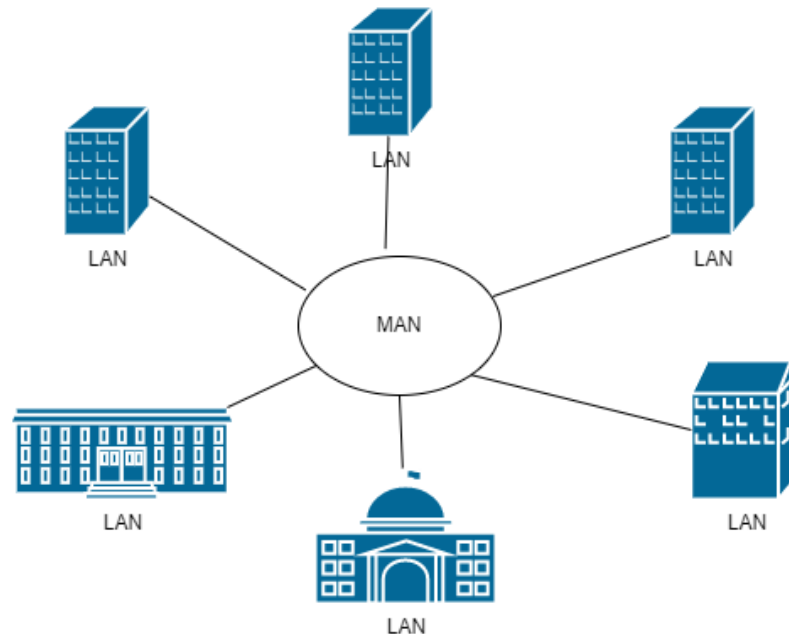
- Limited geographical coverage.
- High setup cost for wired LANs.
- Limited mobility for wired devices.
- Helpless to security breaches if not properly configured.

Metropolitan Area Network (MAN)

Metropolitan area network (MAN): A MAN spans multiple buildings in a city area. It is larger in scale than a Local Area Network (LAN) but smaller than a Wide Area Network (WAN).

Advantage:

- Provides Full-Duplex data transmission in the network channel for devices.
- The network connection area covers an entire city or some parts using the optic cables.

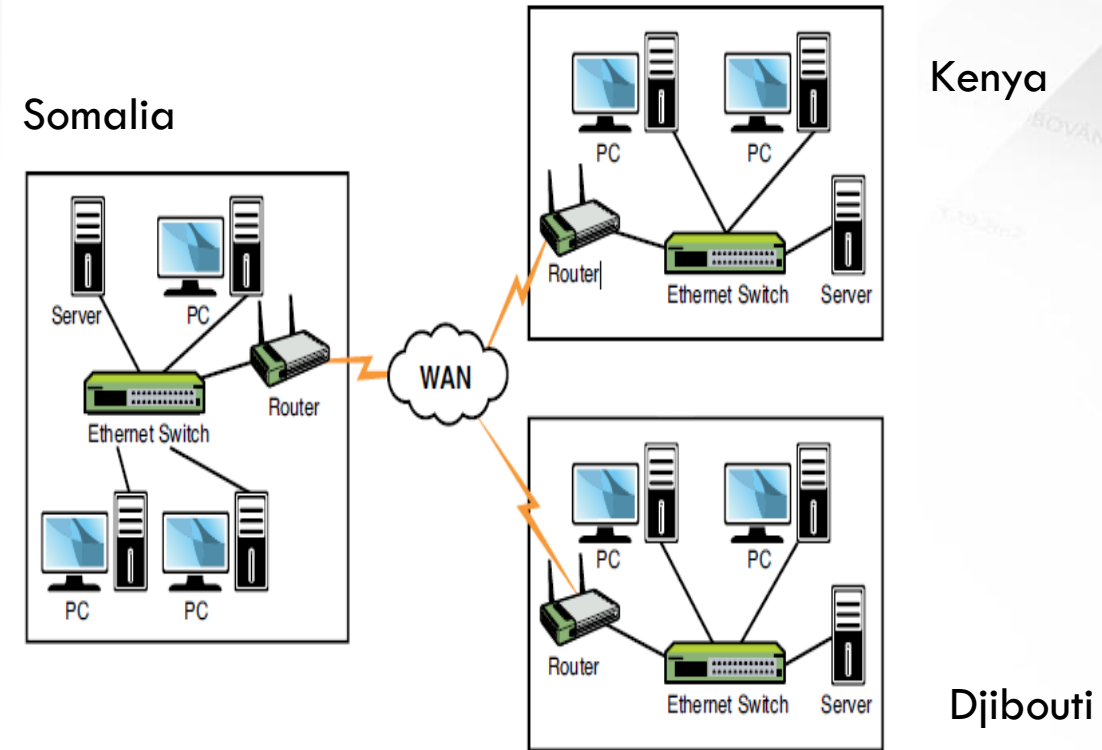


Disadvantage:

- High probability of attack from hackers and cybercriminals due to large networks.
- The need for good quality hardware and the installation cost is very high.

A Wide Area Network (WAN)

- **A Wide Area Network (WAN)** is a type of network that covers a large geographical area. It connects different smaller networks, such as Local Area Networks (LANs) and Metropolitan Area Networks (MANs), allowing computers and users in one location to communicate with computers and users in other locations.
- **Wide Area Network (WAN):** A WAN is much larger than the other network types and can span many areas, such as cities, states, or countries





Network Topology



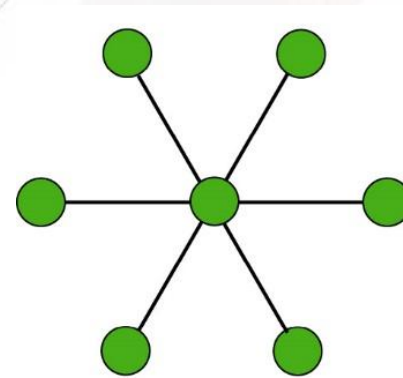
Network Topologies

- Local area networks are defined in terms of the **protocol** and the **topology** used for accessing the network.
- The networking **protocol** is the set of rules established for users to exchange information.
- The **topology** is the network architecture used to interconnect the networking equipment.

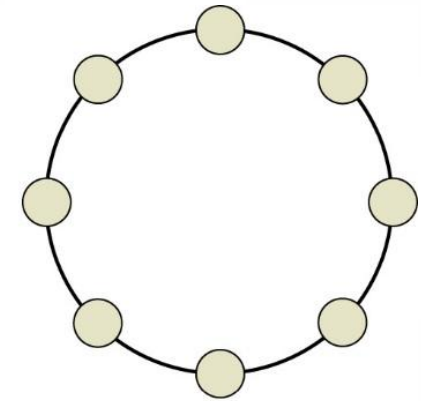
Network Topology

Topology

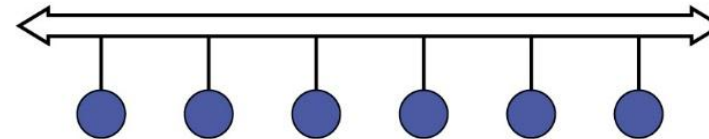
The most common architectures for LANs are the point-to-point, ring, bus, and star/hub-and-spoke architectures, as illustrated in Figure 1-1



(a) Star network



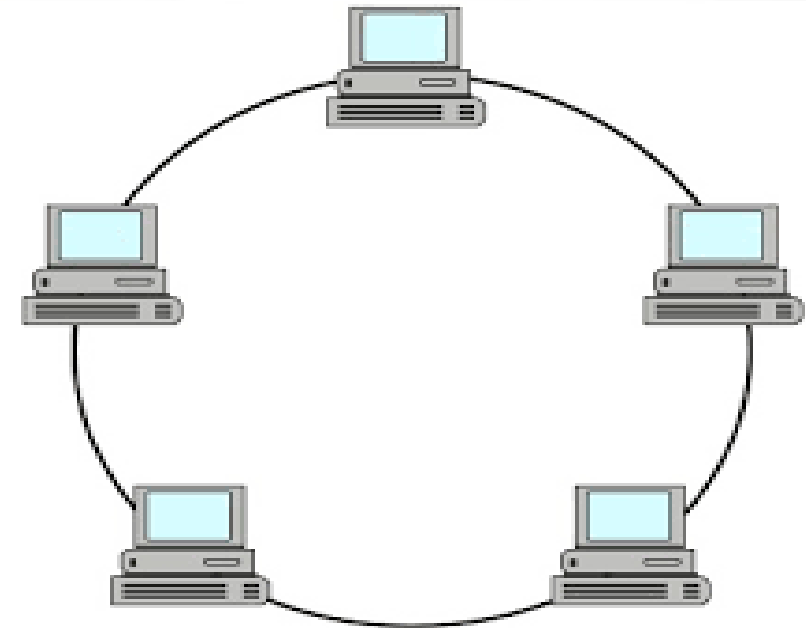
(b) Ring network



(c) Bus network

Ring Topology

- **A ring topology** is a specific type of Local Area Network (**LAN**) topology that connects each device to exactly two of its neighboring devices for communication purposes. In a ring topology, messages are transmitted through the network in the same direction.
- However, if any cable or device in the network fails, it will break the loop and cause the entire segment to go down.



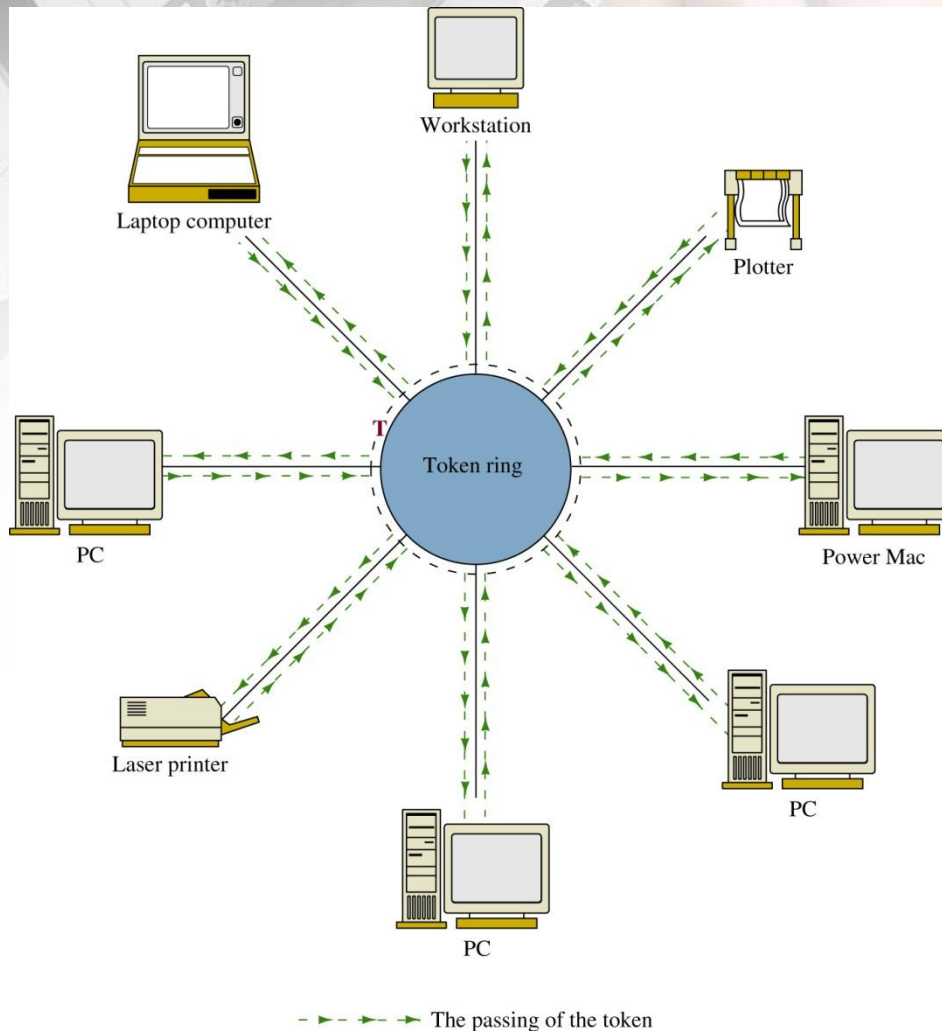
Token-Ring (IEEE 802.3)

Features:

Token Passing: A technique in which an electrical token circulates around a network, and control of the token enables the user to gain access to the network

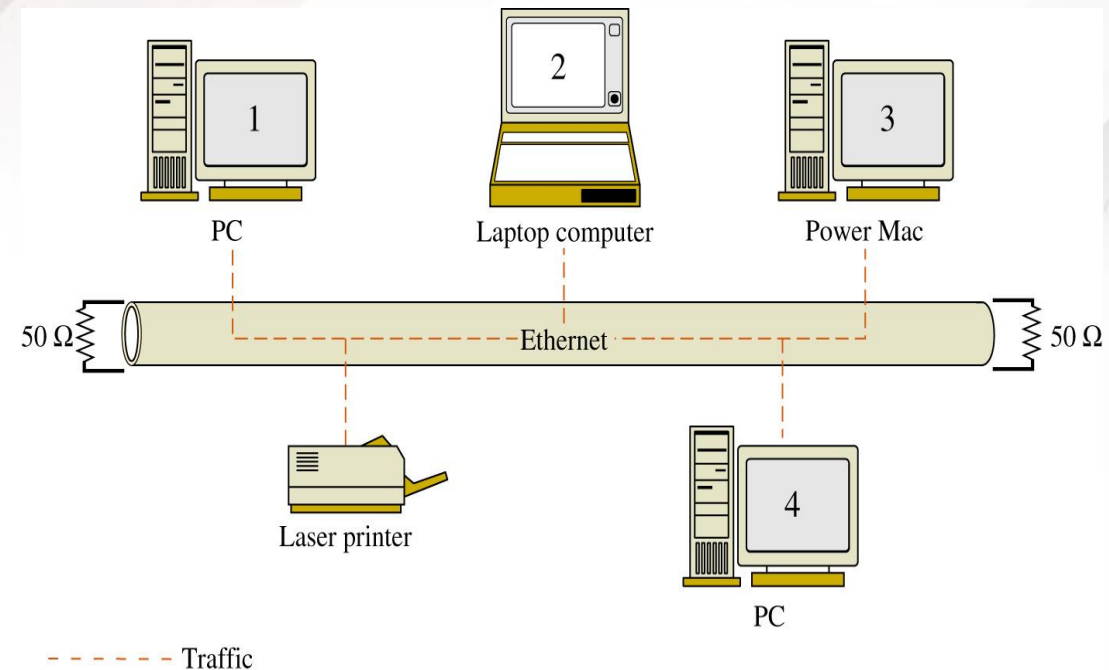
Advantage:

Deterministic – meaning that the networking devices gain control of the network at fixed time intervals.



Bus Topology

- **A bus topology** is a type of Local Area Network (LAN) topology where all the nodes are connected to a single cable referred to as a "**backbone**". If the backbone is compromised, the entire segment fails.
- in which the computers share the media (coaxial cable) for data transmission. In this topology, a coaxial cable (called **ThinNet**) is looped through each networking device to facilitate data transfer.

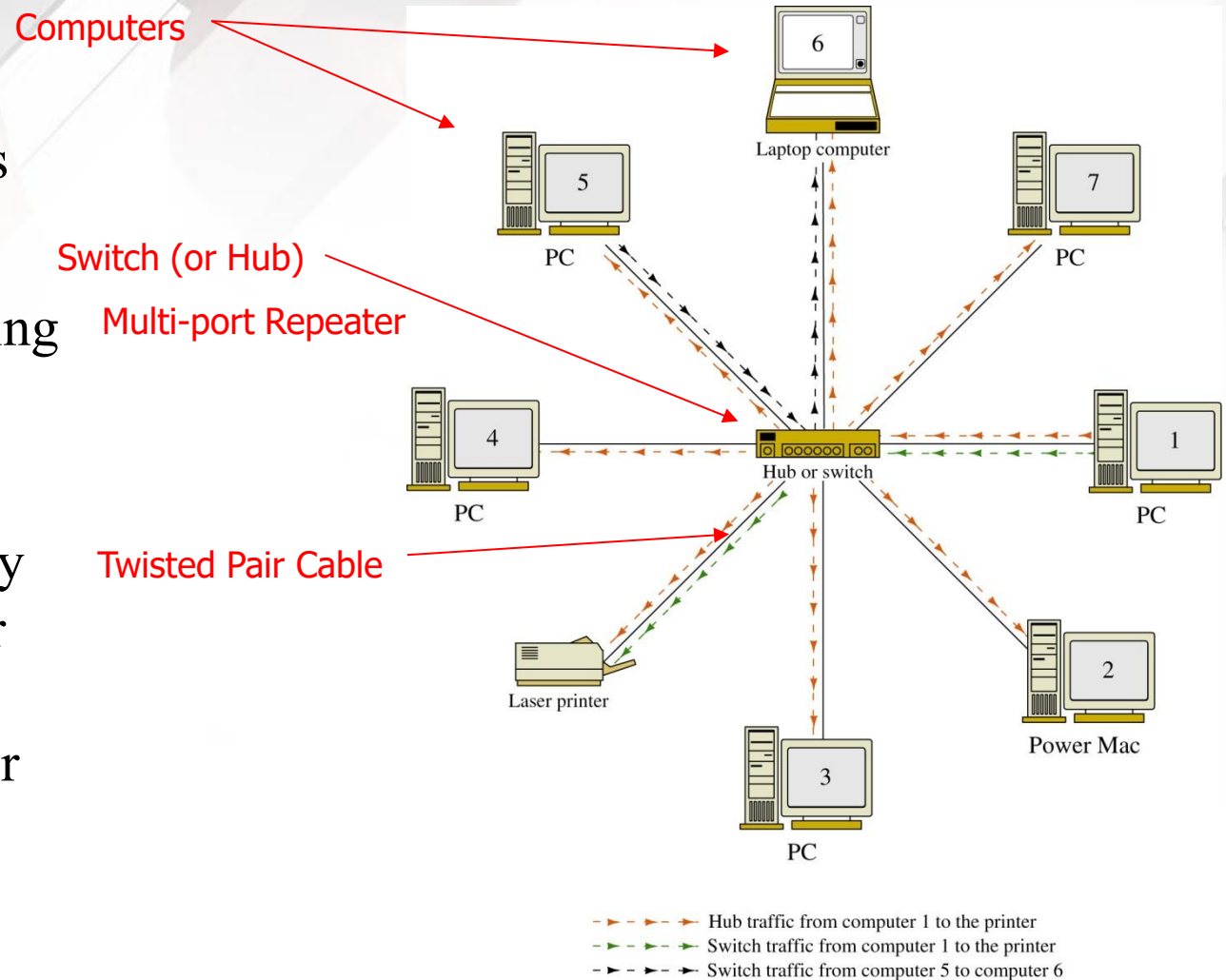


Features - network data traffic is carried over a common data link

Star Topology

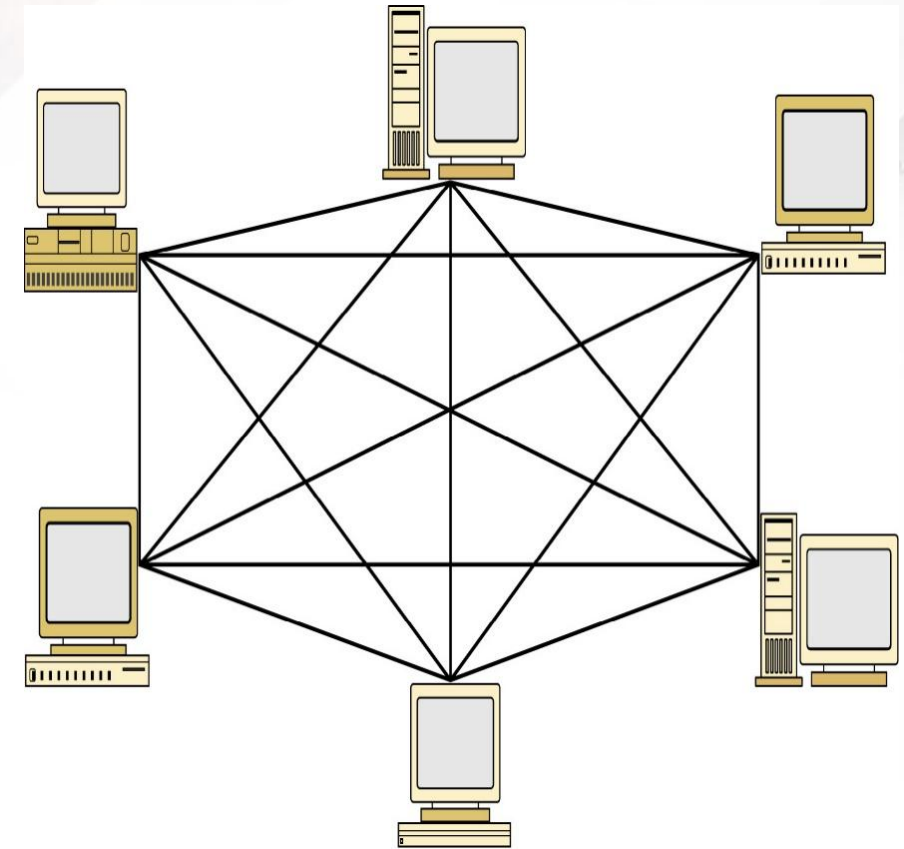
1. A **star topology** is a LAN where all devices connect to a central hub or switch.
2. The networking devices share data connections to/from the central hub or switch
3. A hub broadcasts all data traffic to all networking devices connected to its data ports.

The **star topology** (also called hub-and-spoke topology) is the most common networking topology in today's LANs. Twisted-pair cables with modular plugs are used to connect the computers and other networking devices (see Chapter 2, "Physical Layer Cabling: Twisted-Pair")



Mesh Topology

- In a **mesh topology**, all devices are directly connected, ensuring full redundancy in data paths. If one path fails, alternate paths can still transmit data. However, this redundancy increases costs due to the need for extra cabling, networking hardware, and multiple network ports for each device. The design also adds complexity, making network management more difficult. Mesh topology is ideal for high-reliability applications but may be too costly for general networking need.





The OSI Model

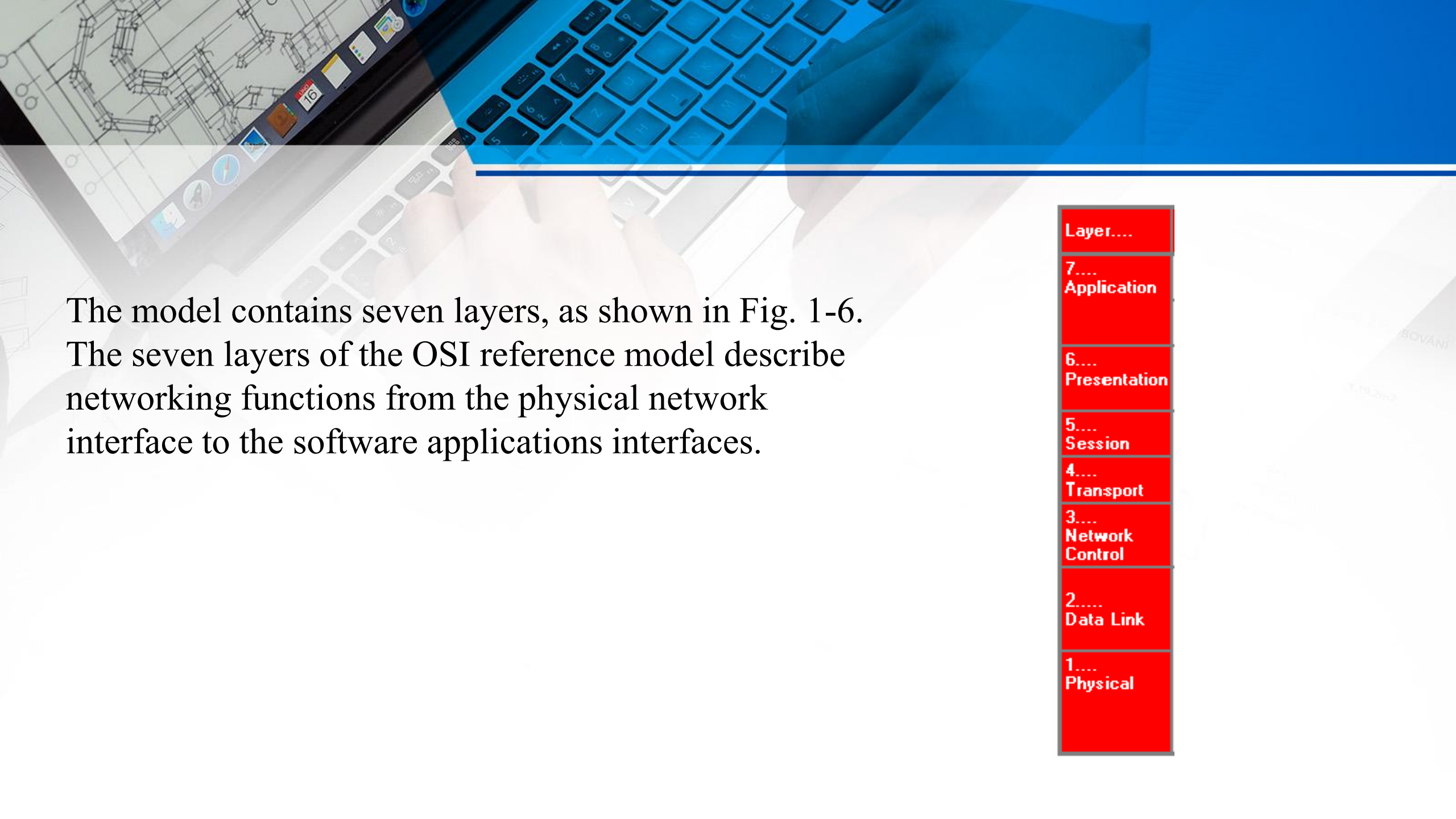
Why a Layered Network Model?

The OSI Model

An open systems interconnection (**OSI**) reference model was developed by the International Organization for Standardization in 1984 to enable different types of networks to be linked together.

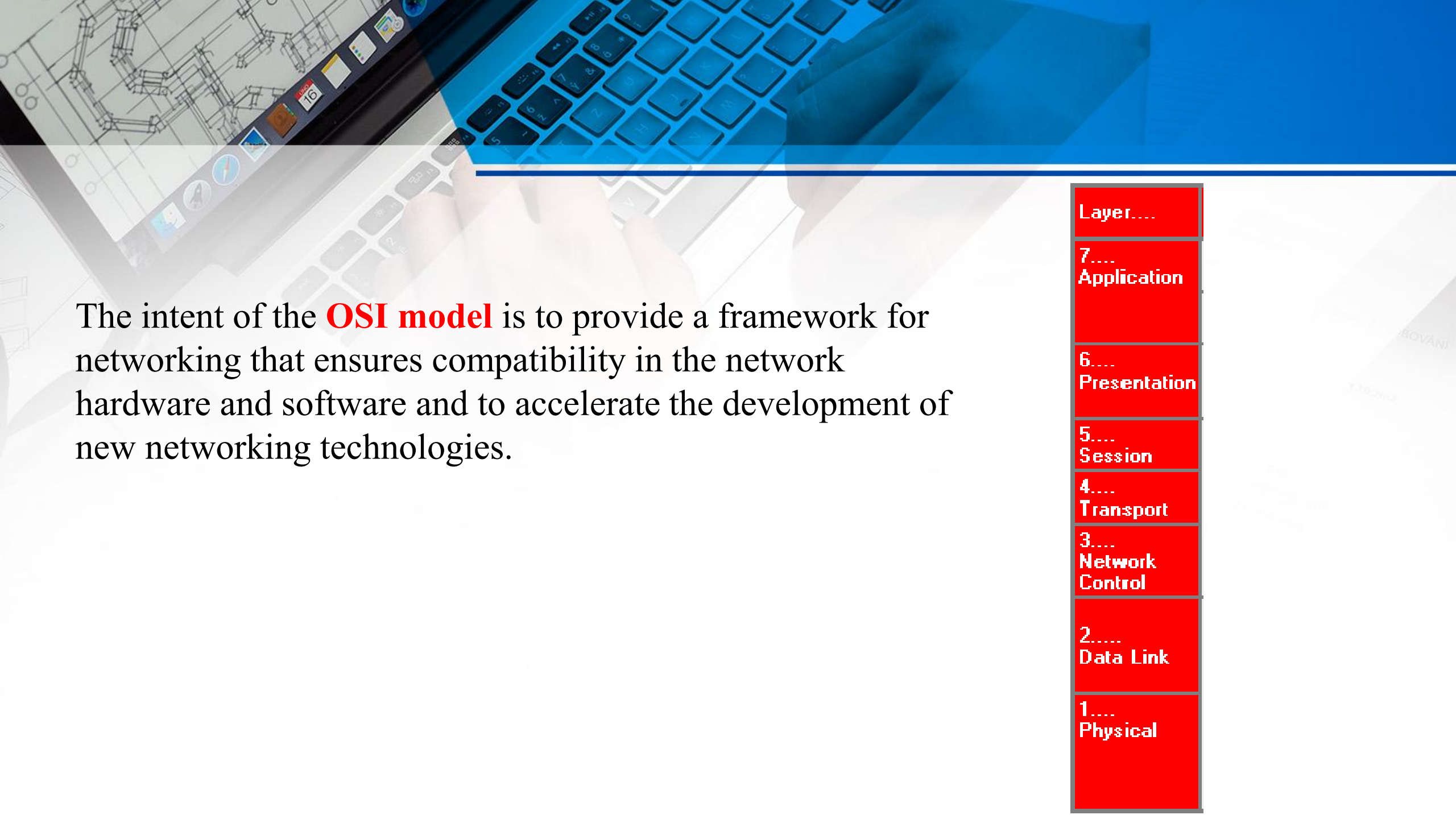


The OSI Model



The model contains seven layers, as shown in Fig. 1-6. The seven layers of the OSI reference model describe networking functions from the physical network interface to the software applications interfaces.





The intent of the **OSI model** is to provide a framework for networking that ensures compatibility in the network hardware and software and to accelerate the development of new networking technologies.

Layer....

7....
Application

6....
Presentation

5....
Session

4....
Transport

3....
Network
Control

2....
Data Link

1....
Physical




Table 1-1 A summary of the OSI layers

Layer	Function	Examples
7. Application	support for applications	HTTP, FTP, SMTP (email)
6. Presentation	protocol conversion, data translation	ASCII, JPEG
5. Session	establishes, manages, and terminates sessions	
4. Transport	ensures error free packets	TCP, UDP
3. Network	provides routing decisions	IP, IPX
2. Data link	provides for the flow of data	MAC addresses
1. Physical	signals and media	NICs, twisted pair cable, fiber

**Table 1-1 A summary of the
OSI Layers**




Table 1-1 A summary of the OSI layers

Layer	Function	Examples
7. Application	support for applications	HTTP, FTP, SMTP (email)
6. Presentation	protocol conversion, data translation	ASCII, JPEG
5. Session	establishes, manages, and terminates sessions	
4. Transport	ensures error free packets	TCP, UDP
3. Network	provides routing decisions	IP, IPX
2. Data link	provides for the flow of data	MAC addresses
1. Physical	signals and media	NICs, twisted pair cable, fiber

Physical layer - provides the electrical and mechanical connection to the network. Examples of technologies working in this layer are EIA/TIA related technologies, UTP, fiber, and NICs

Table 1-1 A summary of the OSI layers

Layer	Function	Examples
7. Application	support for applications	HTTP, FTP, SMTP (email)
6. Presentation	protocol conversion, data translation	ASCII, JPEG
5. Session	establishes, manages, and terminates sessions	
4. Transport	ensures error free packets	TCP, UDP
3. Network	provides routing decisions	IP, IPX
2. Data link	provides for the flow of data	MAC addresses
1. Physical	signals and media	NICs, twisted pair cable, fiber

Data Link layer - handles error recovery, flow control (synchronization), and sequencing (which terminals are sending and which are receiving). It is considered the "media access control layer" and is where the MAC addressing is defined. The Ethernet 802.3 standard is defined in this area, which is why the MAC address is sometimes called the Ethernet address.




Table 1-1 A summary of the OSI layers

Layer	Function	Examples
7. Application	support for applications	HTTP, FTP, SMTP (email)
6. Presentation	protocol conversion, data translation	ASCII, JPEG
5. Session	establishes, manages, and terminates sessions	
4. Transport	ensures error free packets	TCP, UDP
3. Network	provides routing decisions	IP, IPX
2. Data link	provides for the flow of data	MAC addresses
1. Physical	signals and media	NICs, twisted pair cable, fiber

Network layer - accepts outgoing messages and combines messages or segments into packets, adding a header that includes routing information. It acts as the network controller. Examples are IP and IPX

Table 1-1 A summary of the OSI layers

Layer	Function	Examples
7. Application	support for applications	HTTP, FTP, SMTP (email)
6. Presentation	protocol conversion, data translation	ASCII, JPEG
5. Session	establishes, manages, and terminates sessions	
4. Transport	ensures error free packets	TCP, UDP
3. Network	provides routing decisions	IP, IPX
2. Data link	provides for the flow of data	MAC addresses
1. Physical	signals and media	NICs, twisted pair cable, fiber

Transport layer - is concerned with message integrity between the source and destination. It also segments/reassembles (the packets) and handles flow control. Examples are TCP and UDP.

Table 1-1 A summary of the OSI layers

Layer	Function	Examples
7. Application	support for applications	HTTP, FTP, SMTP (email)
6. Presentation	protocol conversion, data translation	ASCII, JPEG
5. Session	establishes, manages, and terminates sessions	
4. Transport	ensures error free packets	TCP, UDP
3. Network	provides routing decisions	IP, IPX
2. Data link	provides for the flow of data	MAC addresses
1. Physical	signals and media	NICs, twisted pair cable, fiber

Session layer - provides the control functions necessary to establish, manage, and terminate the connections as required to satisfy the user request.

Table 1-1 A summary of the OSI layers

Layer	Function	Examples
7. Application	support for applications	HTTP, FTP, SMTP (email)
6. Presentation	protocol conversion, data translation	ASCII, JPEG
5. Session	establishes, manages, and terminates sessions	
4. Transport	ensures error free packets	TCP, UDP
3. Network	provides routing decisions	IP, IPX
2. Data link	provides for the flow of data	MAC addresses
1. Physical	signals and media	NICs, twisted pair cable, fiber

Presentation layer - accepts and structures the messages for the application. It translates the message from one code to another if necessary. This layer is responsible for data compression and encryption.

Table 1-1 A summary of the OSI layers

Layer	Function	Examples
7. Application	support for applications	HTTP, FTP, SMTP (email)
6. Presentation	protocol conversion, data translation	ASCII, JPEG
5. Session	establishes, manages, and terminates sessions	
4. Transport	ensures error free packets	TCP, UDP
3. Network	provides routing decisions	IP, IPX
2. Data link	provides for the flow of data	MAC addresses
1. Physical	signals and media	NICs, twisted pair cable, fiber

Application layer - application programs such as word processing, spreadsheets, and email log the message in, interpret the request, and determine what information is needed to support the request.

The OSI Model

Each layer defines a set of functions in data communications-useful for network troubleshooting

Application Layer (7)

Presentation Layer (6)

Session Layer (5)

Transportation Layer (4)

Network Layer (3)

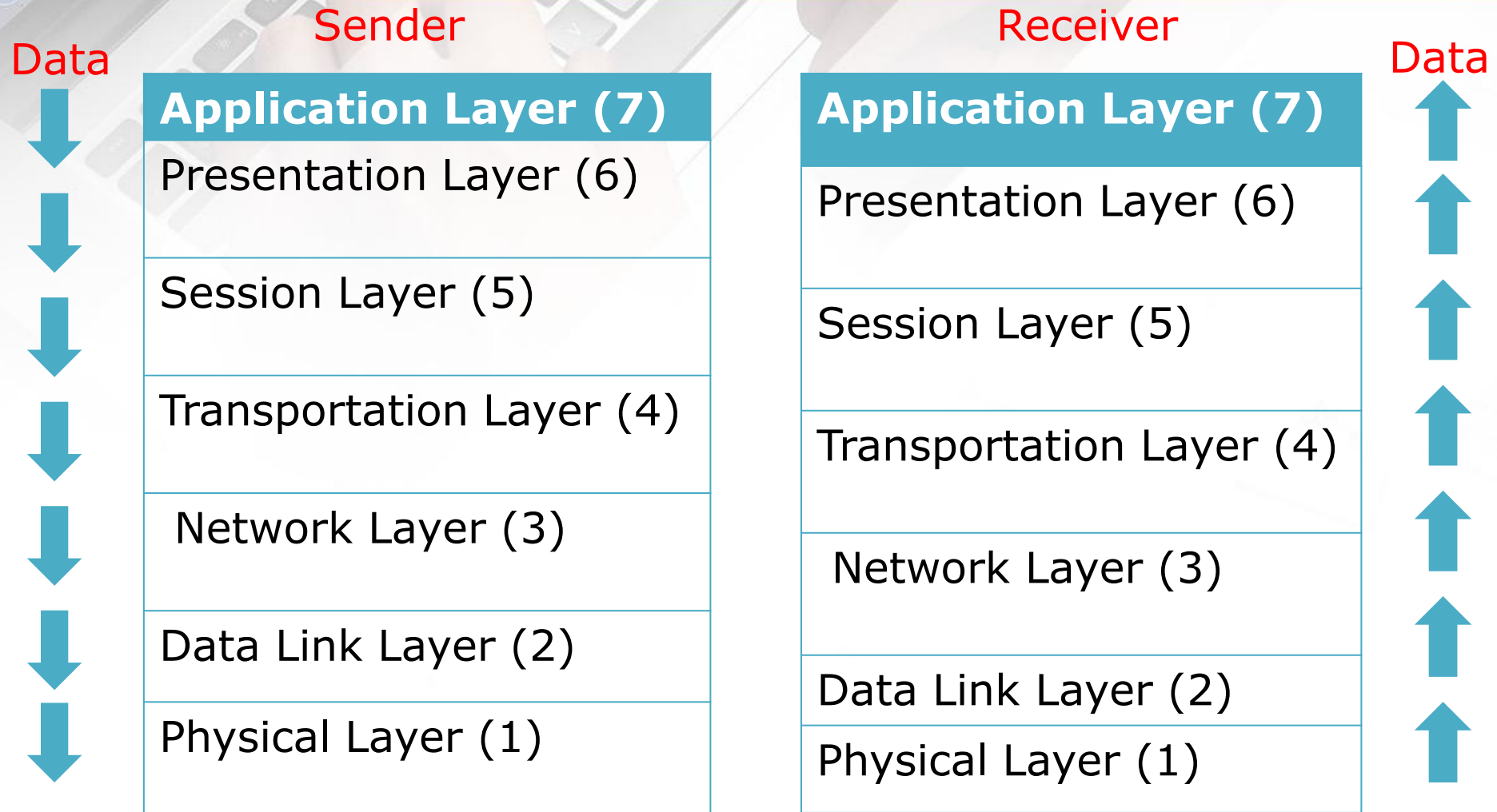
Data Link Layer (2)

Physical Layer (1)

Upper Layers

Lower Layers

The OSI Model





The Network Administrator and the OSI Model

The network administrator uses the OSI model for troubleshooting network problems by verifying functionality of each layer. In many cases, troubleshooting the network problem requires that the network administrator isolate what layer the network problem occurs.



The Network Administrator and the OSI Model

- Assume that a network is having problems accessing an email server (a layer 7 application).
- The first troubleshooting step for the network administrator is to ping the IP address of the email server (layer 3 test). A “ping” to an IP address can be used to quickly check that there is a network connection. A “**reply from**” response for the ping indicates the connection to the server is up. A “**request timed out**” response indicates there the network connection is down.
- This could be due to a cabling problem (layer 1) or a problem with a switch (layer 2), or a router (layer 3), or the server could be completely down (layer 7).

The Network Administrator and the OSI Model

- In the case of “**request timed out**” the network administrator will have to go directly to telecommunications closet or the machine to troubleshoot the problem.
- In this case, the network administrator should first check for layer 1 (**the physical layer**) problems. Many times, this just requires that the network administrator verify that a network cable is connected.
- Remember the concept of checking for a “**link light**?” Cables do get knocked loose or break.



The Network Administrator and the OSI Model - summary

- The networking administrator needs to have a good understanding of the all seven layers of the OSI model. Knowledge of the layers can help to isolate the network problem. There are three basic steps in the process of isolating the network problem:
- Is the connection to the machine down? (**layer 1**)
- Is the network down? (**layer 3**)
- Is a service on a specific machine down? (**layer 7**)



The Ethernet LAN

- The networking protocol used in most modern computer networks is **Ethernet**.
- Ethernet is a **CSMA/CD** LAN protocol.
 - CS** – Carrier Sense
 - MA** – Multiple Access
 - CD** – Collision Detection

The Ethernet Packet

Preamble	Start frame delimiter	Destination MAC address	Source MAC address	Length type	Data	Pad	Frame check sequence
----------	-----------------------------	-------------------------------	--------------------------	----------------	------	-----	----------------------------

Preamble – an alternating pattern of 1's and 0's used for synchronization

The Ethernet Packet

Preamble	Start frame delimiter	Destination MAC address	Source MAC address	Length type	Data	Pad	Frame check sequence
----------	-----------------------	-------------------------	--------------------	-------------	------	-----	----------------------

Start Frame Delimiter – a binary 8-bit sequence of 1 0 1 0 1 0 1 1 that indicates the start of the frame

The Ethernet Packet

Preamble	Start frame delimiter	Destination MAC address	Source MAC address	Length type	Data	Pad	Frame check sequence
----------	-----------------------	-------------------------	--------------------	-------------	------	-----	----------------------

Destination MAC Address and Source MAC Address –
Each computer has an Ethernet network interface card (NIC) or network adapter that has a unique media access control (MAC) address associated with it.

The MAC address is 6 bytes (12 hex characters) in length.

The Ethernet Packet

Preamble	Start frame delimiter	Destination MAC address	Source MAC address	Length type	Data	Pad	Frame check sequence
----------	-----------------------	-------------------------	--------------------	-------------	------	-----	----------------------

Length / Type - an indication of the number of bytes in the data field if this value is less than 1500.

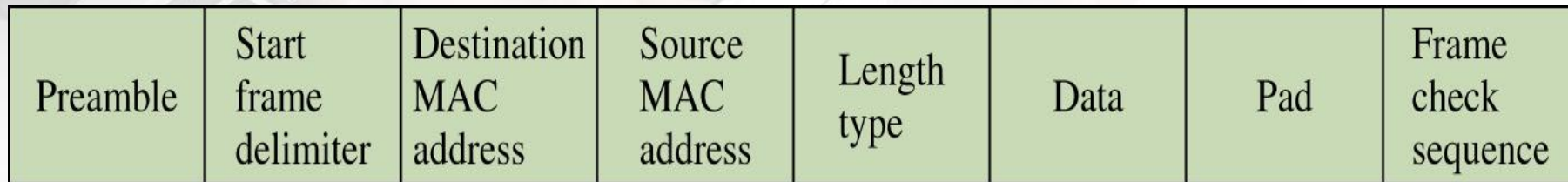
If this number is greater than 1500, it indicates the type of data format, for example IP or IPX.

The Ethernet Packet

Preamble	Start frame delimiter	Destination MAC address	Source MAC address	Length type	Data	Pad	Frame check sequence
----------	-----------------------	-------------------------	--------------------	-------------	------	-----	----------------------

This is the data being transferred from the source to the destination and destination to the source.

The Ethernet Packet



This is the data being transferred from the source to the destination and destination to the source.

The Ethernet Packet

Preamble	Start frame delimiter	Destination MAC address	Source MAC address	Length type	Data	Pad	Frame check sequence
----------	-----------------------	-------------------------	--------------------	-------------	------	-----	----------------------



This is the data being transferred from the source to the destination and destination to the source.

The Ethernet Packet

Preamble	Start frame delimiter	Destination MAC address	Source MAC address	Length type	Data	Pad	Frame check sequence
----------	-----------------------------	-------------------------------	--------------------------	----------------	------	-----	----------------------------

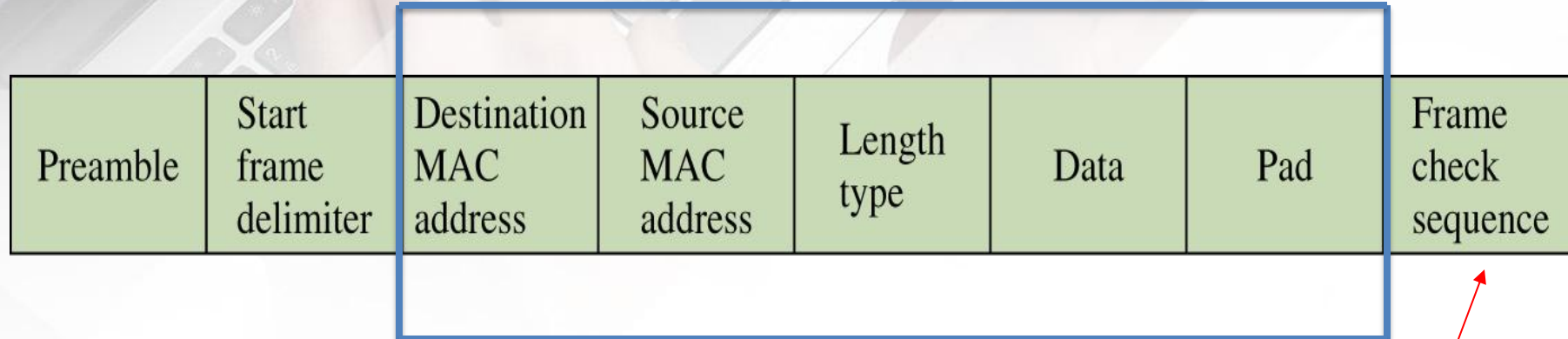
A field used to bring the total number of bytes up to the minimum of 46 if the data field is less than 46 bytes.

The Ethernet Packet

Preamble	Start frame delimiter	Destination MAC address	Source MAC address	Length type	Data	Pad	Frame check sequence
----------	-----------------------	-------------------------	--------------------	-------------	------	-----	----------------------

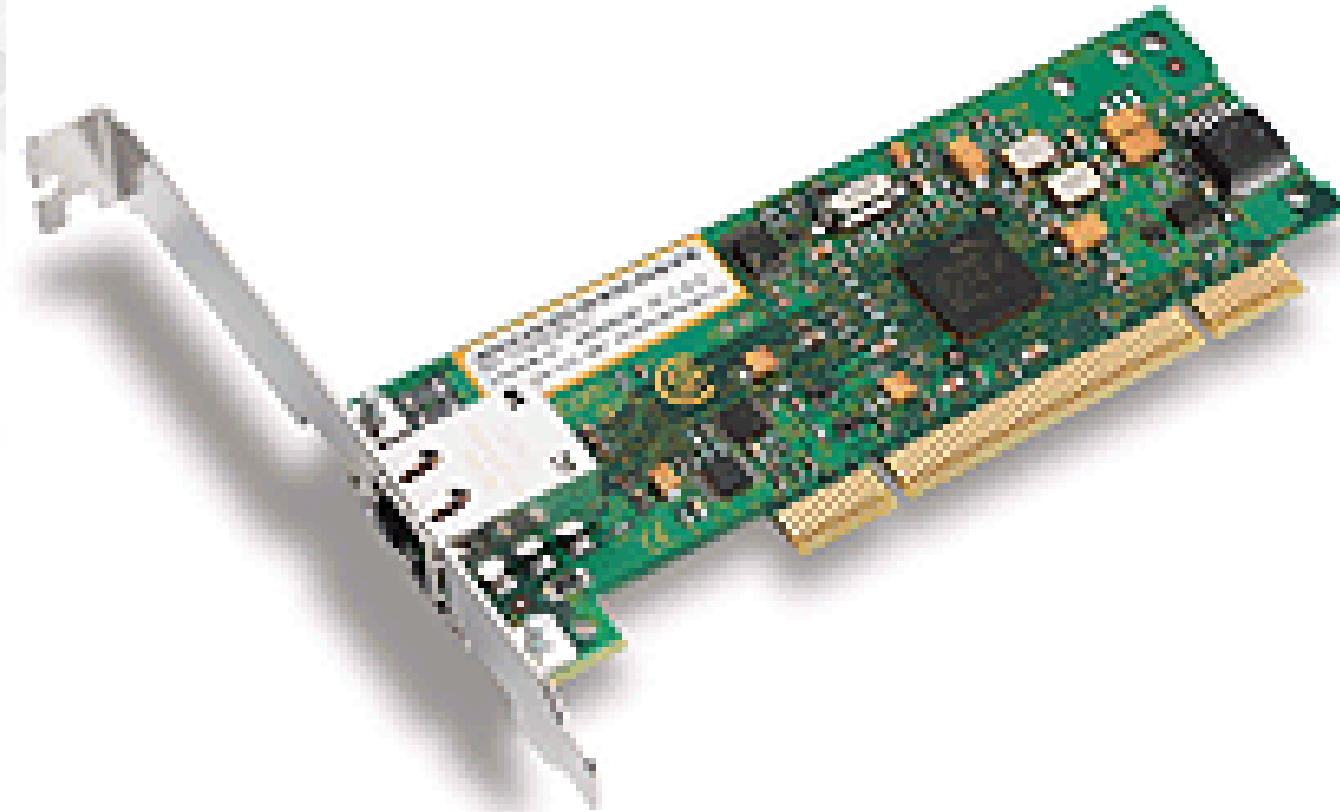
A 4-byte CRC (cyclic redundancy check) value used for error detection. The CRC is performed on the characters from the destination MAC address through the Pad fields. If an error is detected, the system retransmits the data.

The Ethernet Packet



A 4-byte CRC (cyclic redundancy check) value used for error detection. The CRC is performed on the characters from the destination MAC address through the Pad fields. If an error is detected, the system retransmits the data.

A Network Interface Card

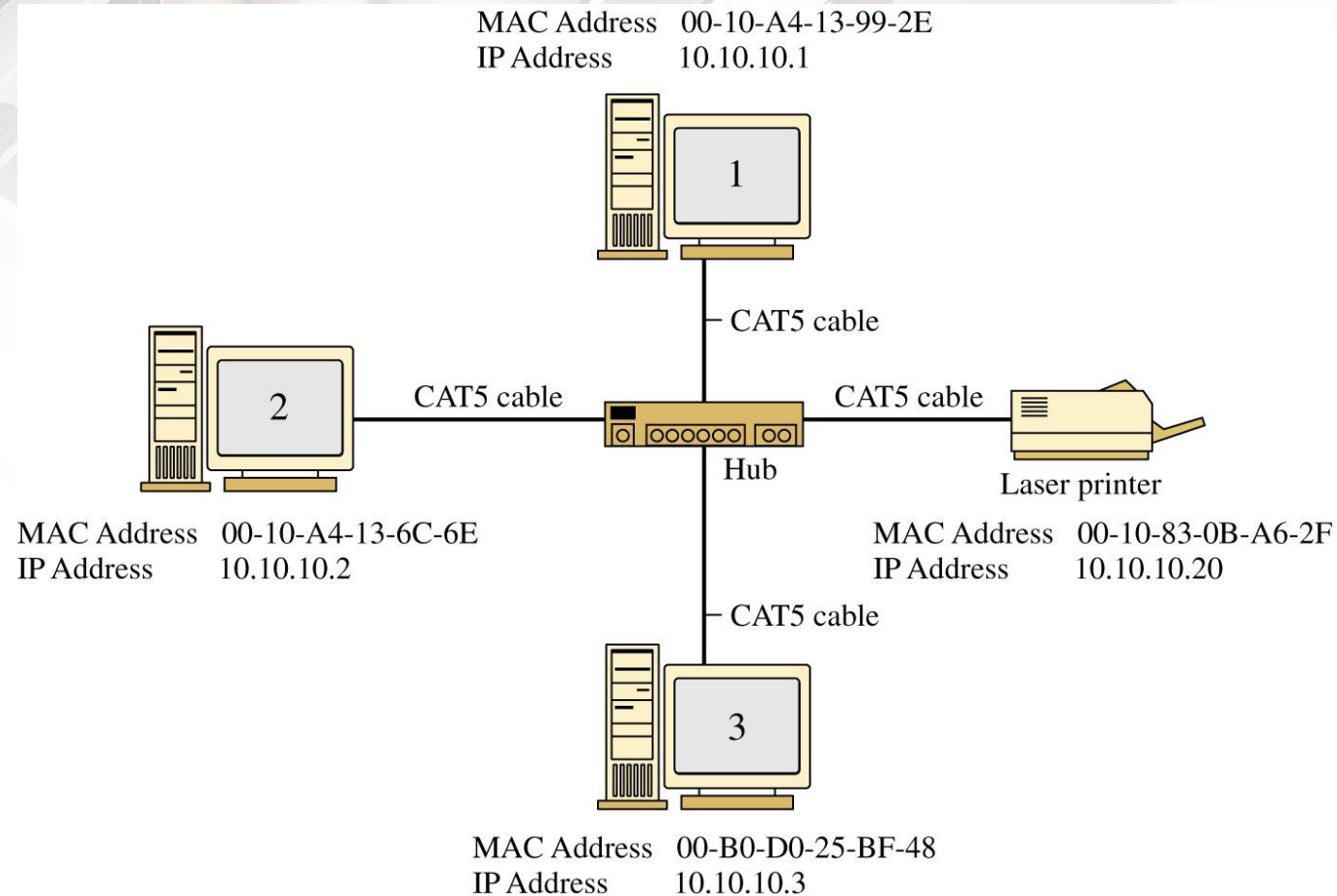




The MAC address

- **How is the destination and source addresses for the data determined within a LAN?**
- Networked devices, such as computers and network printers each have an electronic hardware interface to the LAN called a **Network Interface Card (NIC)** or integrated network port. The NIC contains a unique network address called the **MAC address**.

FIGURE 1-26 An example of a small office LAN star topology.





The MAC address

- The MAC address is **6** bytes (**48 bits**) in length.
- The address is displayed in **12** hexadecimal codes.
The first **6** hexadecimal codes are used to indicate the vendor of the network interface, also called the **Organizationally Unique Identifier (OUI)**
- the last **6** hexadecimal values are unique numbers assigned by the vendor.
- **IEEE is the worldwide source of registered OUIs.**

The MAC address

Table 1-4 A Sample of MAC Addresses

**Company ID / Vendor
Serial #**

Manufacturer

00-AA-00-B6-7A-57

Intel Corporation (00-AA-00)

00-50-73-6C-32-11

Cisco Systems, Inc. (00-50-73)

**00-0A-27-B7-3E-F8
(00-0A-27)**

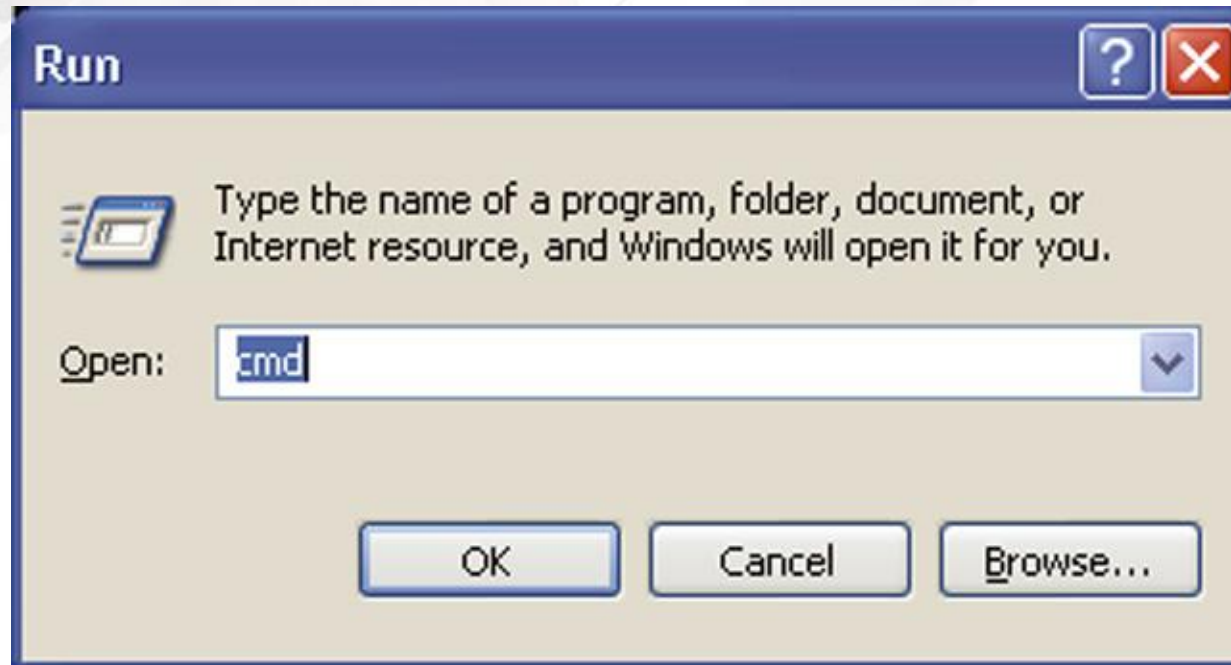
Apple Computer Inc.




The MAC address

- The MAC address, also called the **Ethernet, physical, hardware or adapter address**
- The MAC address can be obtained from computers operating under Microsoft Windows by typing the **ipconfig /all** command while in the command mode.

FIGURE 1-9 The Run window used to enter the command prompt in Windows 7.





```
C:\WINDOWS\System32\cmd.exe

C:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : COMPUTER-1
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Broadcast
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Description . . . . . : Intel(R) PRO/100+ MiniPCI
    Physical Address. . . . . : 00-10-A4-13-99-2E

C:\>_
```

The MAC address is listed under the **Ethernet adapter Local Area Connection:** heading. The **Media State - Media disconnected** text indicates that there is not an active Ethernet device connected to the computer. The **Description** lists the manufacturer and model of the network interface and the **Physical Address** of **00-10-A4-13-99-2E** is the actual MAC address for the computer.

ipconfig /all demonstration

- Click on **Start – Run** and enter the command ***cmd***
- Enter ***ipconfig /all*** to display the MAC address

IPv4 Addressing

- The **IP address** is a unique 32-bit address that identifies on which network the computer is located. The address is divided into four 8-bit parts. The format for the IP address is

A . B . C . D.

- where the A.B.C.D. values are written as the decimal equivalent of the 8-bit binary value. The range for each of the decimal values is 0 to 255.

IPv4 Addresses

- IP addresses are issued based upon the class of the network. Examples of the classes of IP networks are provided in Table 1-4 of the text.

TABLE 1-6 The Classes of IPv4 Networks

Class	Description	Examples of IP Address Numbers	Maximum Number of Hosts
Class A	Governments, very large networks	44.x.x.x	$2^{24}=16,777,214$
Class B	Midsize companies, universities, and so on	128.123.x.x	$2^{16}=65,534$
Class C	Small networks	192.168.1.x	$2^8=254$
Class D	Reserved for multicast groups	224.x.x.x	Not applicable
Class E	Reserved for future use and experimentation	240.x.x.x	Not applicable

IPv4 Addressing

Table 1-6 The Address Range for each Class of Network

Class A	0.0.0.0 to 126.255.255.255
Class B	128.0.0.0 to 191.255.255.255
Class C	192.0.0.0 to 223.255.255.255

IPv4 Addressing

- **network number** is the portion of the IP address that defines which network the IP packet is originating from or being delivered to.
- The * entries for each class represent the **host number**. The host number is the portion of the IP address that defines the address of the networking device connected to the network. The host number is also called the **host address**.

10.10.20.200

172.16.25.191

192.168.12.5



IPv4 Addressing

- The network number provides sufficient information for routing the data to the appropriate destination network.
- The destination network then uses the remaining information (the * portion) to direct the packet to the destination computer or host.
- The * portion of the address is typically assigned by the local network system administrator or is dynamically assigned when users need access outside their local networks.

10.10.20.200

172.16.25.191

192.168.12.5

IPv4 Addressing - ISP

- your **Internet Service Provider (ISP)** dynamically assigns an IP address to your computer when you log on to the Internet.
- Remember, you can check the IP address assigned to your computer by your ISP using the ***ipconfig*** command in the command prompt.

10.10.20.200

172.16.25.191

192.168.12.5

IPv4 Private Addresses

Private IP Addresses

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255



Private IP Addresses

- Private addresses are IP addresses set aside for use in private **intranets**.
- An intranet is an internal network that provides file and resource sharing.
- Private addresses are not valid addresses for Internet use because they have been reserved but can be used within a private LAN to create an **IP network**.