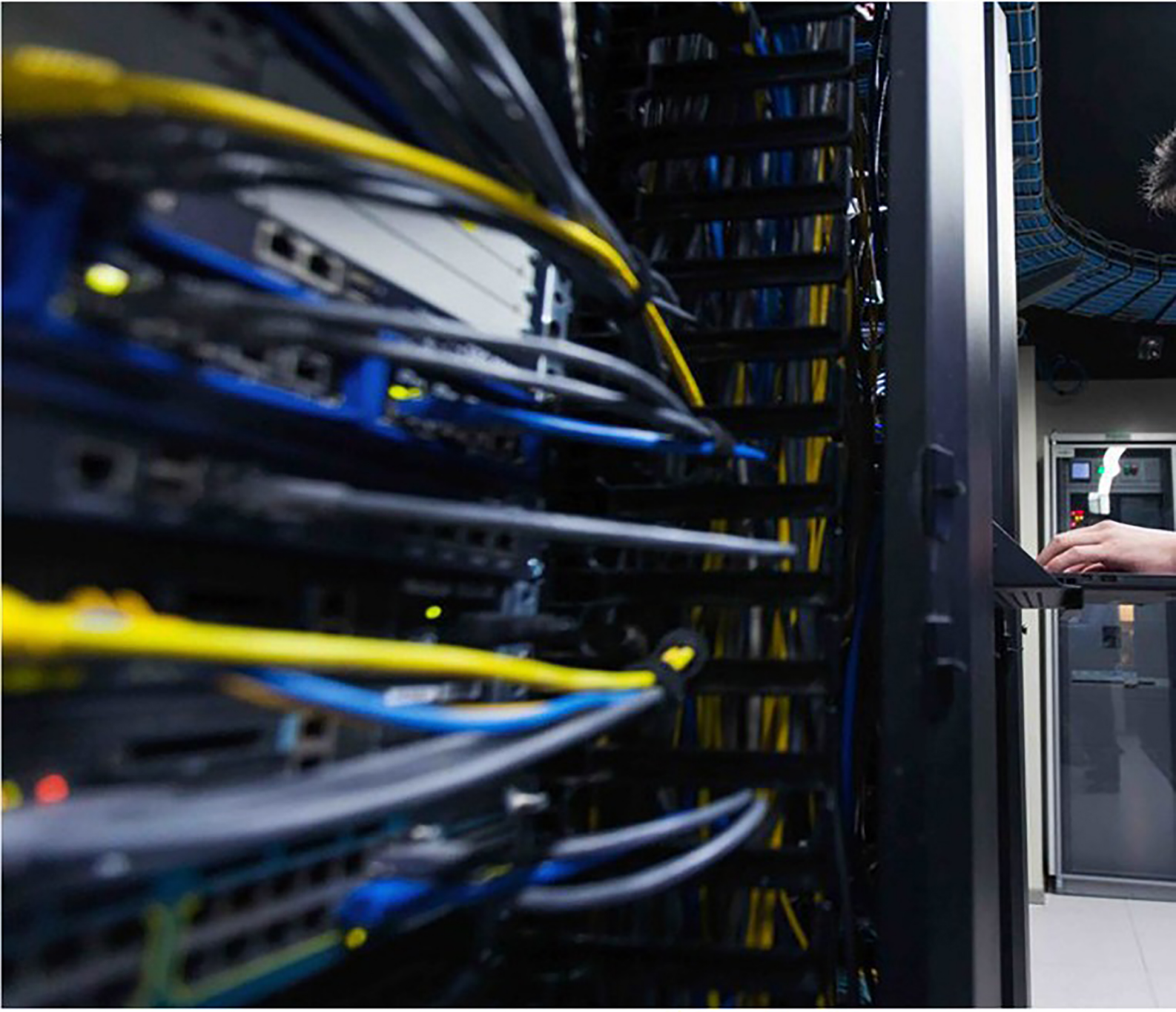


# الشامل لأساسيات شبكات الحاسوب Network Fundamental



إعداد أ. عبدالسلام صالح الراشدي  
2021

 [abdelsalam.elrashdi@gmail.com](mailto:abdelsalam.elrashdi@gmail.com)

 [facebook.com/abdelsalam.elrashdi](https://facebook.com/abdelsalam.elrashdi)

# الشامل لأساسيات شبكات الحاسوب

## Networking fundamentals



بسم الله والصلاة والسلام على أفضل خلق الله سيدنا محمد وعلى آله وصحبه اجمعين. نقدم لكم هذا الكتاب الذي هو بعنوان الشامل لأساسيات شبكات الحاسوب، حيث يحتوي هذا الكتاب على أهم الجوانب العملية والنظرية الخاصة بأساسيات شبكات الحاسوب. حيث يعتبر هذا الكتاب البداية الصحيحة والسليمة لمن يريد البدا في عالم الشبكات بطريقة تمكنه من الفهم الجيد والعميق لعملية انتقال البيانات داخل الشبكات المختلفة. تم التركيز في كتابة وأعداد هذا الكتاب باللغة الإنجليزية نظراً لأهمية هذه اللغة في مجال تقنية المعلومات وأن أغلب الكتب و الأبحاث والمقالات العلمية المؤثرة وذات الأهمية البالغة مكتوبة باللغة الانجليزية .

كم أود ان اشكر زميلي وصديقي المهندس احمد جعفر على تصميم الغلاف الخارجي للكتاب، وكذلك المهندس إسراء أحمد عوفى على التنسيق الرائع .

وفي الختام نسأل الله أن يجعل هذا العمل خالصاً لوجهه الكريم وأن يجعل ما درسناه نافعاً لنا في الدنيا والآخرة .




# Contents

page number	Topic	Topic number
<b>Chapter 1</b> ✍		
9	Defining a computer Network	1.1
10	The Purpose of Networks	1.2
11-13	Network Components	1.3
14-17	Types of computer network	1.4
<b>Chapter 2</b> ✍		
20-29	Types of computer network	2.1
30	types of network architectures	2.2
30-32	Peer to peer (Workgroups )	2.3
33-39	Client and server architecture	2.4
<b>Chapter 3</b> ✍		
57	Network media	3.1
58-59	Coaxial cable	3.2
60	Types of coaxial cables	3.3

60	Common connectors used on coaxial cables	3.4
60	Twisted-Pair Cable	3.5
61-67	Unshielded Twisted-Pair	3.6
68	Industry-standard	3.7
69	Shielded Twisted-Pair	3.8
70	Comparison Between UTP and STP	3.9
70	Common connectors used on twisted-pair cables	3.10
71	Fiber-Optic Cable	3.11
72	Single-Mode Fiber	3.12
73-76	Multimode Fiber	3.13
77-79	Pros and cons Fiber Optic•	3.14
80	Console (Rollover) cable	3.15
<b>Chapter 4 ✍</b>		
84	Introduction to IPv4 address	4.1
84	Purpose of IPv4	4.2
85	IP Address Classes	4.3
85	Examples of IP Addressing	4.4
86	Default Subnet Masks	4.5

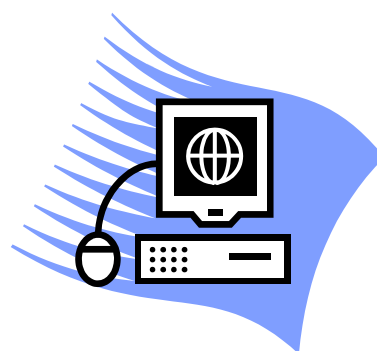


87	Reserved Ip V4 Address	4.6
87	Public IP address	4.7
89-89	Private IP address	4.8
89	Private V public IP address	4.9
90	Network address translation (NAT)	4.10
91	The subnetting	4.11
91	Classless Inter-Domain Routing (CIDR)	4.12
<b>Chapter 5 </b>		
102	Open System Interconnection Model (OSI)	5.1
103	OSI 7 layer	5.2
104	The Purpose of Reference Models	5.3
105	Protocol Suites and Industry Standards	5.4
106	Standards Organizations Other Standards Organization	5.5
106-107	The Application Layer(Layer 7)	5.6
107-108	Presentation layer(Layer6)	5.7
109-110	The Session Layer(layer 5)	5.8
110-113	The Transport Layer	5.9
113-117	The Network Layer (Layer 3)	5.10

117-121	The Data Link Layer (Layer 2)	5.11
121-126	The Physical Layer (Layer)	5.12
126-127	Speed and bandwidth	5.13
128	Protocol Data Units (PDUs)	5.14
129-130	Encapsulating data	5.15
<b>Chapter 6 ✍</b>		
133	The Transmission Control Protocol/Internet	6.1
133-134	History of TCP/IP	6.2
136	OSI Model vs TCP/IP Model	6.3
137	Similarities between TCP/IP model and OSI	6.4
137	Differences between OSI model and TCP/IP	6.5
139	Application Layer	6.6
139	The Application-layer includes some protocols like	6.7
141	DHCP server	6.8
143	File Transfer Protocol (FTP) And TFTP	6.9
144	Domain name system (DNS) server	6.10
145	Hypertext Transfer Protocol (HTTP) And HTTPS	6.11

145	Web server	6.12
146	Telnet and SSH	6.13
147	E-mail server	6.14
148	Transport layer or host to host Layer	6.15
148-149	TCP And UDP	6.16
151	TCP Header	6.17
152-153	Port Numbers	6.18
154-155	Three way handshake	6.19
155-156	Four way handshake	6.20
158	Address Resolution Protocol (ARP)	6.21
158	Reverse Address Resolution Protocol (RARP)	6.22
158	Internet Control Message Protocol (ICMP)	6.23
164	Broadcast Domain	6.24
16-165	Collision	6.25
165-167	Question	6.26
<b>Chapter 7 ✍</b>		
170-171	IP address version 6	7.1
172	Address Types : ipv6	7.2
172	UniCast addresses	7.3

172-173	Subnetting	7.4
174	EUI-64	7.5
174	Assignment	7.6
175	stateless autoconfiguration	7.7
176	IPv6 Routing	7.8
177-178	Migration to IPv6	7.9
<b>Lab part</b>		
181-189	Make LAN Network	1
190-199	Connect a wireless network	2
	Wireless security	3
203-205	Make password on switch	4
206-209	Connect two difference networks by router	5
209-211	Cerate VIANS	6
211-212	Make Port Security on Switch	7



## Chapter 1 ☺✍

### Outlines



1. Define a computer networks
2. The purpose of computer networks
3. How networks impact daily life
4. Network components
5. Networks defined by geography

---

### Objectives

*By end of this lecture the student will be able :*

- Define a computer networks.
- Explain the basic operation of network fundamentals .
- Explain the purposes of computer networks.
- Describe network components (switch, hub, router, repeater ETC) .
- Describe basic operation of network components .
- Describe types of computer networks.
- Describe and list the different types of network components
- List the different types of Networks as defined by Geography.



## *Defining a computer Network*

- ✓ A **computer network** is a set of computers connected together for the purpose of sharing resources. The most common resource shared today is connection to the Internet. Other shared resources can include a printer or a file server.
- The Internet itself can be considered a computer network.
  - computer network or data network is a telecommunications network that allows computers to exchange data.
  - In computer networks, networked computing devices pass data to each other along data connections.
  - The connections (network links) between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

---

## Defining a computer Network (cont)



# The Purpose of Networks

• **At its essence**, a network's purpose focus on four major Items cost, speed, performance and effort ) is to make connections. These connections might be between a PC and a printer or between a laptop and the Internet, as just a couple **of examples :-**

1. Easy access and sharing of information
2. Sharing of files and network resources (printers , scanners, fax,)
3. Networks (e-commerce, IP telephony, Video on Demand, Video conferencing ...etc)
4. Electronic mail
5. An automated teller machine (ATM)
6. Ability to use network software

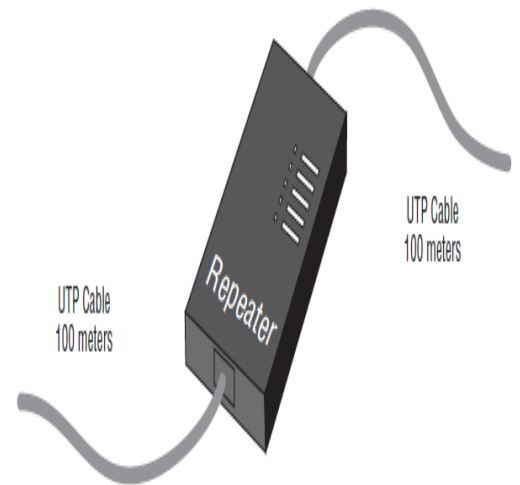
## How Networks Impact Daily Life



# Network Components

## 1. Repeater :-

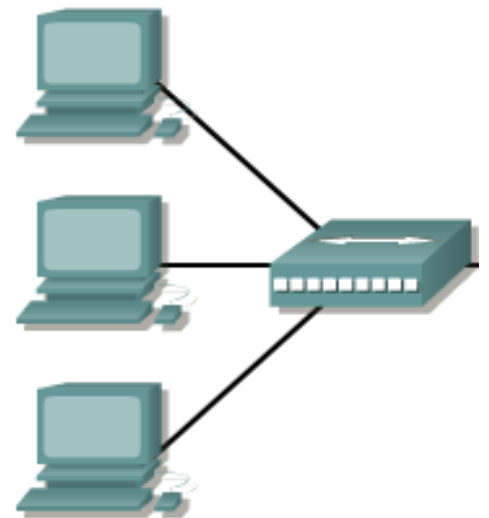
- Repeater receives a signal and preamplifies or regenerates that signal and then forwards the digital signal out all active ports without looking at any data
- Most of the time, repeaters were used in the old Thinnet networks of yesteryear. Today, they're just employed as the multi-port repeaters that we call hubs.



---

## 2. Hub

a hub is the device that connects all the devices of the network together in a star topology. Every device in the network connects directly to the hub through a single cable. An transmission received on one port will be sent out all the other ports in the hub, including the receiving pair for the transmitting device, so that

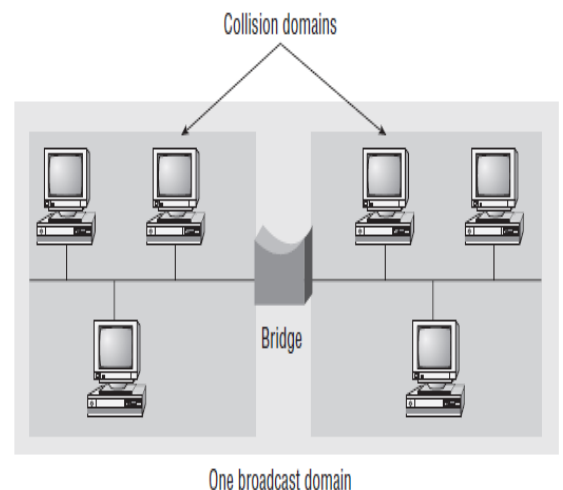


Carrier Sense Multiple Access with Collision Detection (CSMA/CD) on the transmitter can monitor for collisions.

---

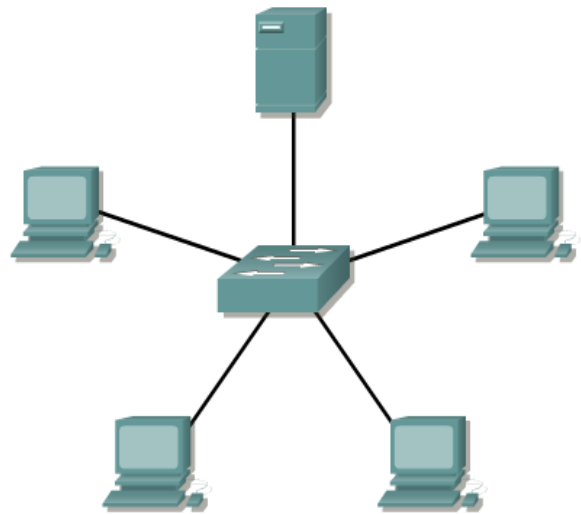
## 3. Bridge

A bridge —specifically, a transparent bridge—is a network device that connects two similar network segments together. Its primary function is to keep traffic separated on either side of the bridge



## 4. Switch

Switches connect multiple devices of a network together much like hubs do, but with three significant differences—a switch recognizes frames and pays attention to the source and destination MAC address of the incoming frame as well as the port on which it was received. Hubs don't do those things.

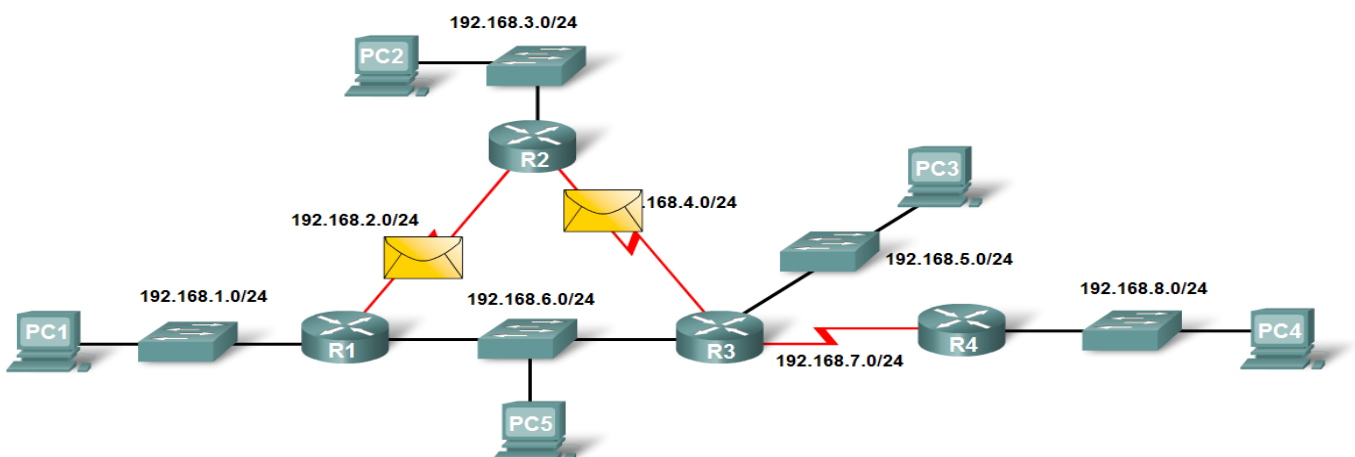


The switch will only forward the frame out from the specific port on which its destination is located

---

## 5. Router

- A router is a network device used to connect two or more network together. A well-configured router can make intelligent decisions about the best way to get network data to its destination. It gathers the information it needs to make these decisions based on a network's particular performance data.
- Routers are used to connect networks together
- Route packets of data from one network to another.
- Router chooses best path to final destination



- Cisco became the standard of routers because of their high-quality router products
- 

## 6. *Wireless Access Point (AP)*

- A wireless access point (AP) allows mobile users to connect to a network wirelessly via radio frequency technologies. Using wireless technologies, APs also allow wired networks to connect to wireless network.
- 

## 7. *Network Interface Card*

A network interface card (NIC) is a printed circuit board that provides network communication capabilities to and from a personal computer. Also called a LAN adapter.

---



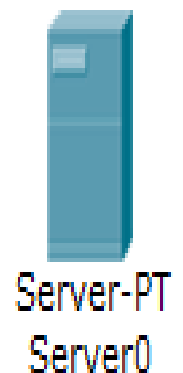
## 8. *Firewall*

A firewall protects your LAN resources from invaders that prowl the Internet for unprotected networks, while simultaneously preventing all or some of your LAN's computers from accessing certain services on the Internet. You can employ them to filter packets based on rules that you or the network administrator create and configure to strictly delimit the type of information allowed to flow in and out of the network's Internet connection.

---

## 9. *Servers*

Servers are also powerful computers, They get their name because they truly are “at the service” of the network and run specialized software for the network's maintenance and control known as the network operating system.





# *Types of computer network*

- ✓ **Networks Defined by Geography** we can classify networks is how geographically dispersed the networks components are. For example, a network might interconnect devices within an office, or a network might interconnect a database at a corporate headquarters location with a remote sales office located on the opposite side of the globe.

Based on the geographic dispersion of network components, networks can be classified into various categories, including the following:

- Personal-area network (PAN)
- Campus-area network (CAN)
- Local-area network (LAN)
- Metropolitan-area network (MAN)
- Wide-area network (WAN)

---

## *Personal-area network (PAN)*

- A PAN is a network whose scale is even smaller than a LAN. For example, a connection between a PC and a digital camera via a universal serial bus (USB) cable could be considered a PAN. Another example is a PC connected to an external hard drive via a FireWire connection.

- A PAN, however, is not necessarily a wired connection.

- A Bluetooth connection between your cell phone and your car's audio system is considered a wireless PAN (WPAN). The main distinction of a PAN, however, is that its range is typically limited to just a few meters.

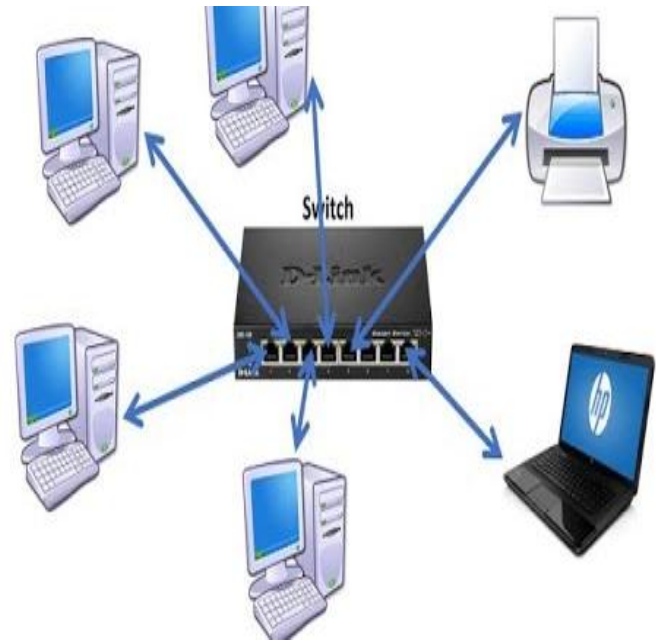
### PERSONAL AREA NETWORK(PAN)



## *Local Area Network (LAN)*

- A LAN interconnects network components within a local area (for example, within a building). Examples of common LAN technologies you are likely to encounter include Ethernet (that is, IEEE 802.3) and wireless networks (that is, IEEE 802.11).

- It connect many devices in small area to share the data and resources like a home ,office , building , school , or airport • It is a group of network components that work within small area .



- It characterized by high data speeds (up to 40Gbps cat8) using:

- 10m bps (Ethernet), 100 mbps (Fast Ethernet), 1000mbPs (GigaEthernet),10Gigabit Ethernet , fiber optical and ATM.

---

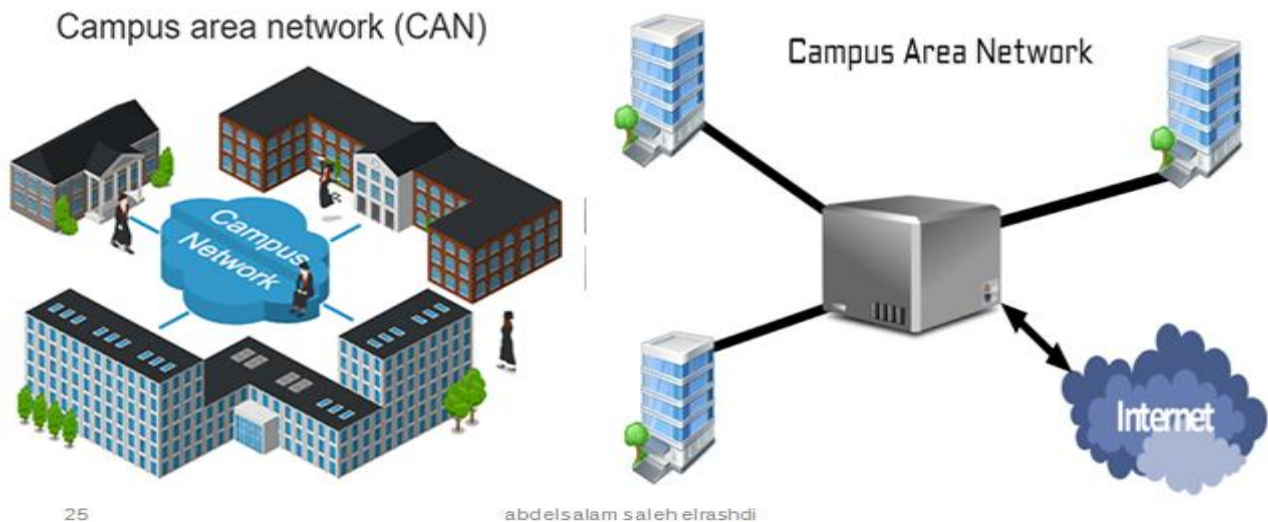
## *Campus-area network (CAN)*

- A campus area network is larger than a local area network LAN since it may span multiple buildings within a specific area. Most CANs are comprised of several LANs connected via switches and routers that combine to create a single network. They operate similar to LANs, in that users with access to the network (wired or wireless) can communicate directly with other systems within the network.

- A campus area network (CAN) is a network of multiple interconnected local area networks (LAN) in a limited geographical area. A CAN is smaller than a wide area network (WAN) or metropolitan area network (MAN).

- 10mbps(Ethernet),100mbps(FastEthernet),1000mbPs (GigaEthernet),10Gigabit Ethernet , fiber optical and ATM.

## CAN cont

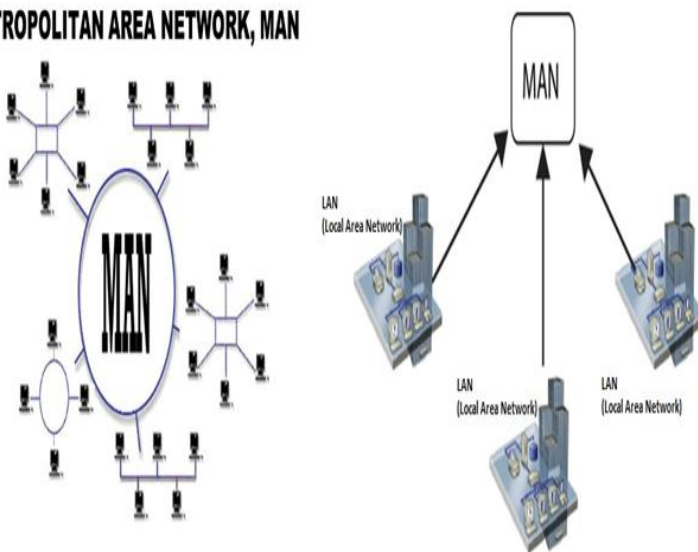


## MAN (Metropolitan Area Network):

- A metropolitan area network (MAN) is a network with a size greater than LAN but smaller than a WAN. It normally comprises networked interconnections within a city that also offers a connection to the Internet.

### Metropolitan-area network (MAN)

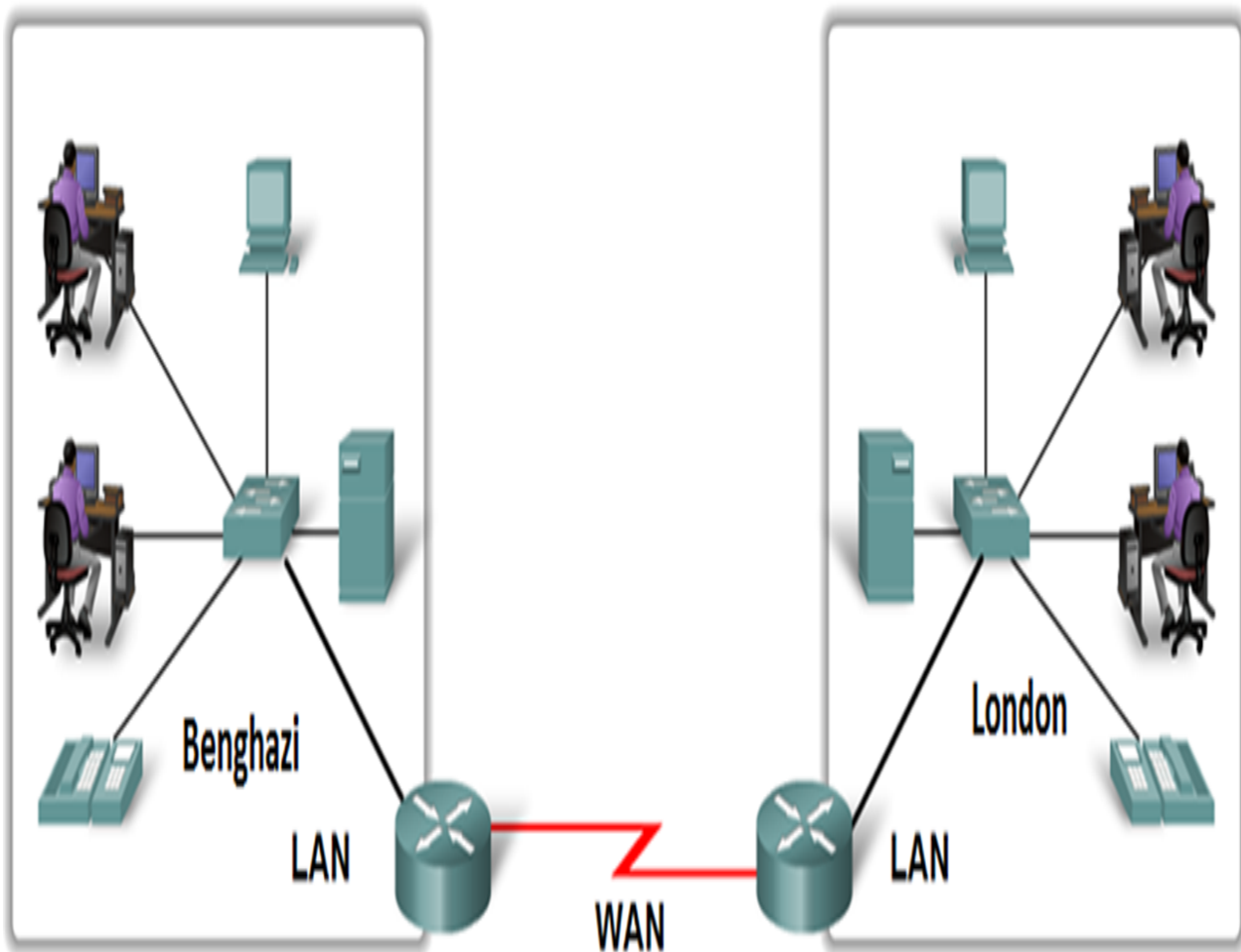
#### METROPOLITAN AREA NETWORK, MAN



- It is a group of LANs that are interconnected within small area.
- Some references point that Man distance about 10 to 100KM
- It characterized by very high data speeds (up to 10Gbps) using: Metro Ethernet, ATM over SONET, fiber optical and SDH.

## Wide-area network (WAN)

- A wide area network (WAN) is a network that exists over a large-scale geographical area. A WAN connects different smaller networks, including local area networks (LANs) and metro area networks (MANs). This ensures that computers and users in one location can communicate with computers and users in other locations. WAN implementation can be done either with the help of the public transmission system or a private network.
  - It is a group of MAN that are interconnected within large area
  - It characterized by slow data speeds .
  - using: analog dial-up, digital dial-up (ISDN), leased lines, X.25, DSL, Frame-Relay, ATM.PPP,VPN and fiber optical .
- 





## Chapter 2 ☺ ✍

---

### *Networks Defined by Topology*

ABDELSALAM SALEH ELRASHDI

Networking fundamentals





## Chapter 2 ☺✍

### Outlines

- Define a computer networks
- The purpose of computer networks
- How networks impact daily life
- Network components
- Networks defined by geography
- Network topologies
- Architecture of a computer network Objectives.



-----

*By end of this lecture the student will be able :*

- ✓ Define a computer networks.
- ✓ Explain the basic operation of network fundamentals .
- ✓ Explain the purposes of computer networks.
- ✓ Describe network components (switch, hub, router, repeater ETC) .
- ✓ Describe basic operation of network components .
- ✓ Describe types of computer networks.
- ✓ Describe and list the different types of network components
- ✓ List the different types of Networks as defined by Geography.
- ✓ Describe network topology.
- ✓ Explain architecture of computer network.

# *Types of computer network*

- Networks Defined by Topology Before we starting in this type You need to be able to distinguish between a physical topology and a logical topology.
- Physical Versus Logical Topology
- A physical network topology diagram shows the structure of how devices are connected physically inside a network.
- A logical network topology diagram shows the logical method of communication used by the devices inside the network for network communication.
- Physical topology specifies the layout how devices are physically connected in the network. Instead,
- logical topology specifies the manner in which data travels between devices in the network.

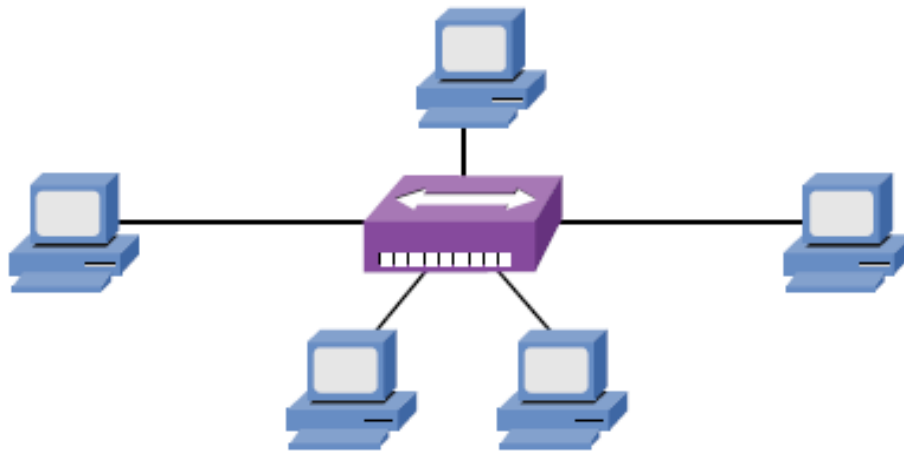
Physical topology shows how a network looks physically, but logical topology shows the fashion in which data is circulated inside the network.

---

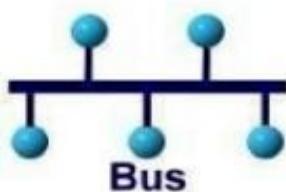
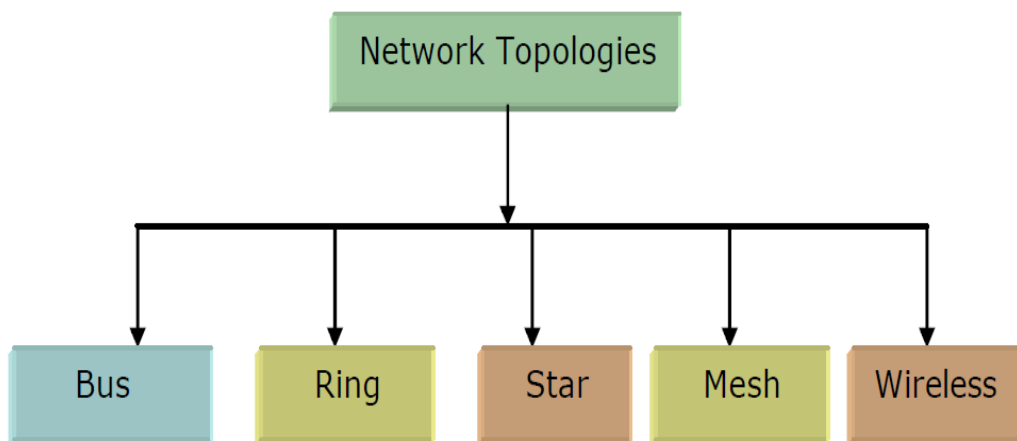
## *Physical Versus Logical Topology*

<b>BASIS FOR COMPARISON</b>	<b>PHYSICAL TOPOLOGY</b>	<b>LOGICAL TOPOLOGY</b>
Basic	Refer to how a network look and functions.	Fashion in which data travels logistically.
Types	Bus, star, ring and mesh topologies.	Logical bus and the logical ring.
Founded on	Physical connections of cables and devices.	Path traveled by data in a network.
Can affect	Cost, scalability, flexibility, bandwidth capacity, etcetera.	Data delivery causing lost packets or congestion.

## Physical Versus Logical Topology (cont)



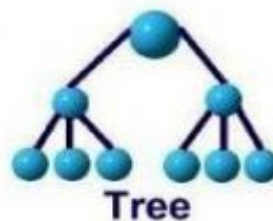
## Network topologies



Bus



Star



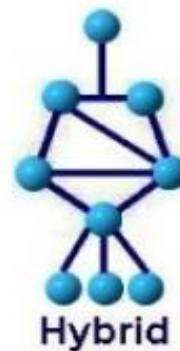
Tree



Ring



Mesh



Hybrid

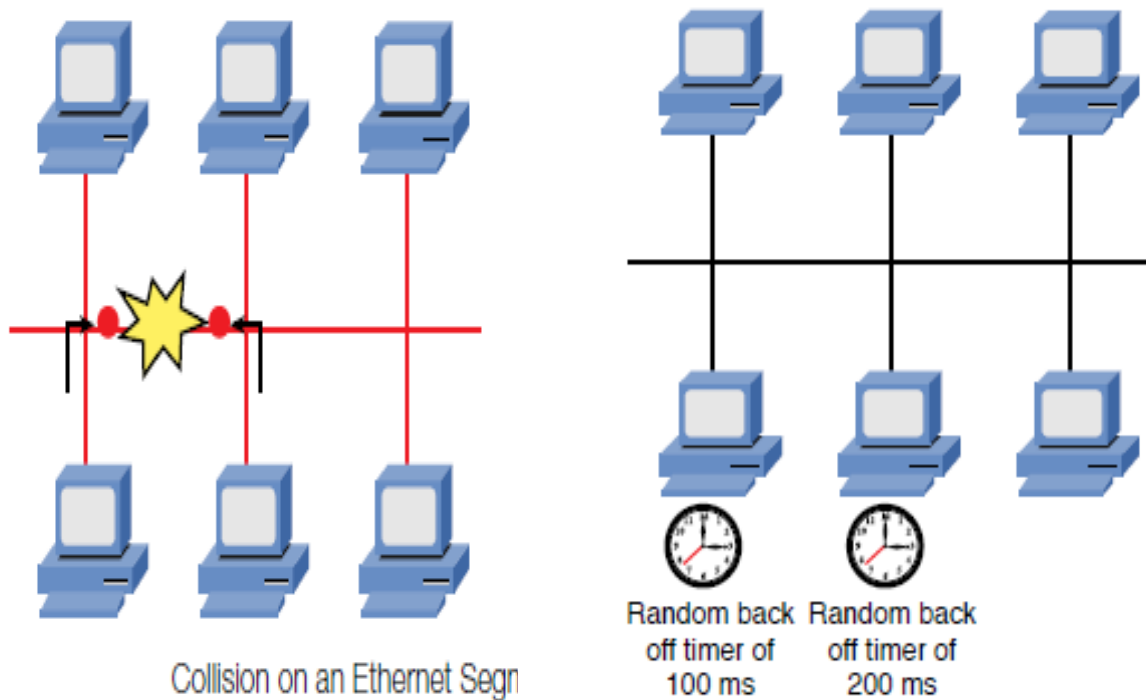
## *Bus Topology*

- A bus topology uses a single backbone cable that is terminated at both ends.
- All the hosts connect directly to a backbone.
- If one host send data, the data will move through the bus and reaches all the other hosts .

A bus and all devices connected to that bus make up a network segment . A single network segment is a single collision domain, which means that all devices connected to the bus might try to gain access to the bus at the sametime, resulting in an error condition known as a collision .

CSMA / CD = Carrier Sense Multiple Access /Collision Detection

Ex.: Ethernet (10 Base 5, 10 Base 2, & 10 Base T)

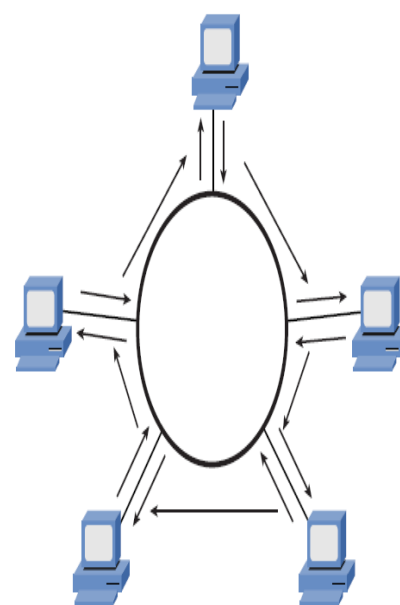


## Characteristics, Benefits, and Drawbacks of a Bus Topology

Characteristics	Benefits	Drawbacks
One cable is used per network segment.	Less cable is required to install a bus topology, as compared with other topologies.	Because a single cable is used per network segment, the cable becomes a potential single point of failure.
To maintain appropriate electrical characteristics of the cable, the cable requires a terminator (of a specific resistance) at each end of the cable.	Depending on the media used by the bus, a bus topology can be less expensive.	Troubleshooting a bus topology can be difficult because problem isolation might necessitate an inspection of multiple network taps to make sure they either have a device connected or they are properly terminated.
Bus topologies were popular in early Ethernet networks.	Installation of a network based on a bus topology is easier than some other topologies, which might require extra wiring to be installed.	Adding devices to a bus might cause an outage for other users on the bus.
Network components tap directly into the cable via a connector such as a T connector or a vampire tap.		An error condition existing on one device on the bus can impact performance of other devices on the bus.

## *Ring Topology*

- ring topology, where traffic flows in a circular fashion around a closed network loop (that is, a ring). Typically, a ring topology sends data, in a single direction, to each connected device in turn, until the intended destination receives the data. Token Ring networks typically relied on a ring topology, • although the ring might have been the logical topology, whereas physically, the topology was a star topology.



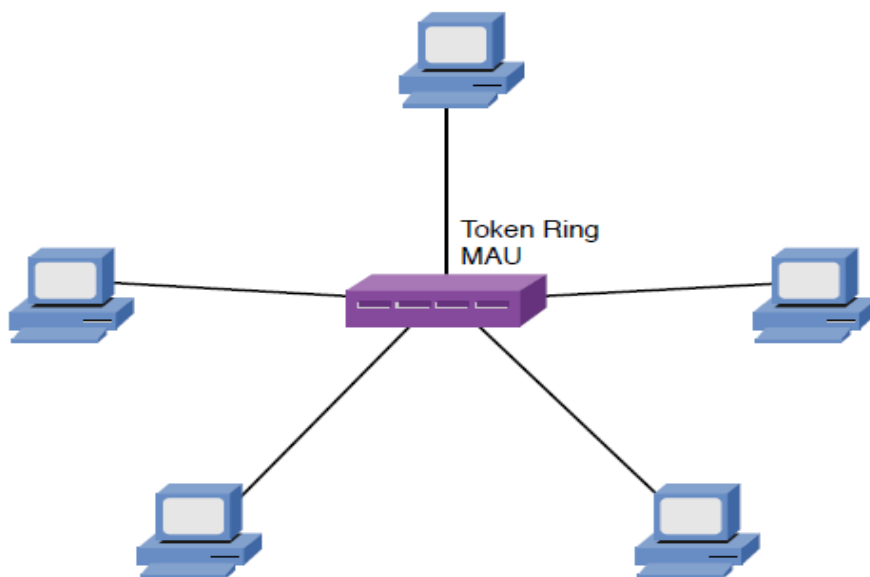


- A ring topology connects one host to the next and the last host to the first.
- If the first host needs to send data to the last host, the data must path through all the hosts before reaching the end host.
- ***Difficult to solve the problem.***
  - If one host is down all connection is down .
  - Ex.: Token Ring, & FDDI.

### ▶ ***Ring Topology (cont)***

- Because a ring topology allows devices on the ring to take turns transmitting on the ring, contention for media access was not a problem, as it was for a bus topology. If • a network had a single ring, however, the ring became a single point of failure. If the ring were broken at any point, data would stop flowing.
- Characteristics, Benefits, and Drawbacks of a ring Topology

#### *Media Access Unit*

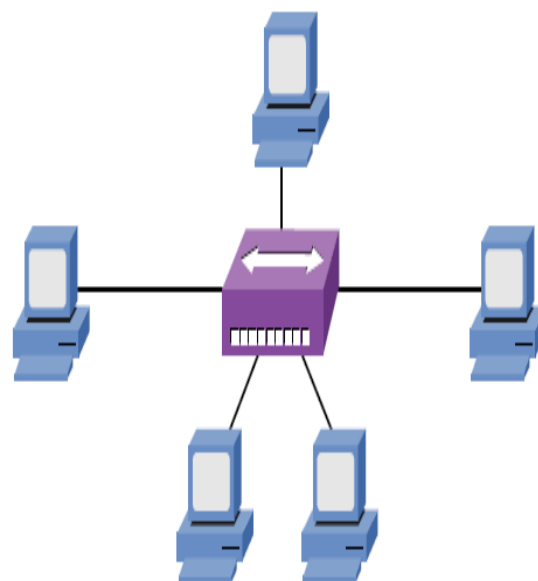


### ***Characteristics, Benefits, and Drawbacks of a ring Topology :-***

Characteristics	Benefits	Drawbacks
Devices are interconnected by connecting to a single ring or, in some cases (for example, FDDI), a dual ring.	A dual ring topology adds a layer of fault tolerance. Therefore, if a cable break occurred, connectivity to all devices could be restored.	A break in a ring when a single ring topology is used results in a network outage for all devices connected to the ring.
Each device on a ring includes both a receiver (for the incoming cable) and a transmitter (for the outgoing cable).	Troubleshooting is simplified in the event of a cable break, because each device on a ring contains a repeater. When the repeater on the far side of a cable break does not receive any data within a certain amount of time, it reports an error condition (typically in the form of an indicator light on a network interface card [NIC]).	Rings have scalability limitations. Specifically, a ring has a maximum length and a maximum number of attached stations. Once either of these limits is exceeded, a single ring might need to be divided into two interconnected rings. A network maintenance window might need to be scheduled to perform this ring division.
Each device on the ring repeats the signal it receives.		Because a ring must be a complete loop, the amount of cable required for a ring is usually higher than the amount of cable required for a bus topology serving the same number of devices.

## Star Topology

- A star topology connects all cables to a central point of concentration. All devices is connected to each other through the central device (switch,Hub).
- If one device want send data to another device first sent to central device then to destination device not directly.
- The star topology is the most popular physical LAN topology in use today, with an Ethernet switch at the center of the star and unshielded twisted-pair cable (UTP) used to connect from the switch ports to clients.
- If one device down not all the network will be down .



- Low cost.
- Easy to find the problem in network .
- Easy to solve the problem.
- If the central device down all network is down.
- Use Ethernet (10 Base T, 100 Base TX, 1000 Base T).

Characteristics	Benefits	Drawbacks
Devices have independent connections back to a central device (for example, a hub or a switch).	A cable break only impacts the device connected via the broken cable, and not the entire topology.	More cable is required for a star topology, as opposed to bus or ring topologies because each device requires its own cable to connect back to the central device.
Star topologies are commonly used with Ethernet technologies	Troubleshooting is relatively simple because a central device in the star topology acts as the aggregation point of all the connected devices.	Installation can take longer for a star topology, as opposed to a bus or ring topology, because more cable runs that must be installed.

## *Full mesh Topology*

- Because each site connects directly to every other site, an optimal path can be selected, as opposed to relaying traffic via another site. Also, a full-mesh topology is highly fault tolerant. you can see that multiple links in the topology could be lost, and every site might still be able to connect to every other site.
- A mesh topology is implemented to provide as much protection as possible from interruption of service.
- Each host has its own connections to all other hosts.
- Although the Internet has multiple paths to any one location.
- High cost.

- High security .
- Many cables and NIC.
- Easy to found the problem in network .
- Easy to solve the problem.
- If one device down not all the network will be down .

---

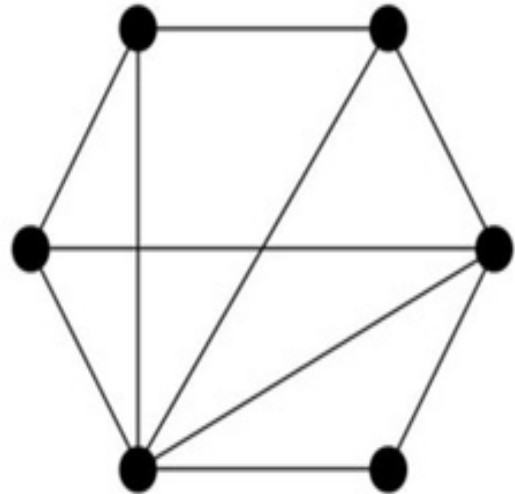
### *Characteristics, Benefits, and Drawbacks of a ring Topology Full mesh Topology :-*

Characteristics	Benefits	Drawbacks
Every site has a direct WAN connection to every other site.	An optimal route exists between any two sites.	A full-mesh network can be difficult and expensive to scale, because the addition of one new site requires a new WAN link between the new site and every other existing site.
The number of required WAN connections can be calculated with the formula $w = n * (n - 1) / 2$ , where $w$ = the number of WAN links and $n$ = the number of sites. For example, a network with 10 sites would require 45 WAN connections to form a fully meshed network: $45 = 10 * (10 - 1) / 2$ .	A full-mesh network is fault tolerant because one or more links can be lost and reachability between all sites might still be maintained.	
	Troubleshooting a full-mesh network is relatively easy because each link is independent of the other links.	

### *Partial-Mesh Topology*

- Topology means the study of mapping things one among others. Partial mesh topology is a way to map multiple routers in such a way that they are tightly coupled among themselves but not fully inter-connected.

• A partial-mesh WAN topology, as depicted in Figure 1-12, is a hybrid of the previously described hub-and-spoke topology and full-mesh topology. Specifically, a partial-mesh topology can be designed to provide an optimal route between selected sites, while avoiding the expense of interconnecting every site to every other site.

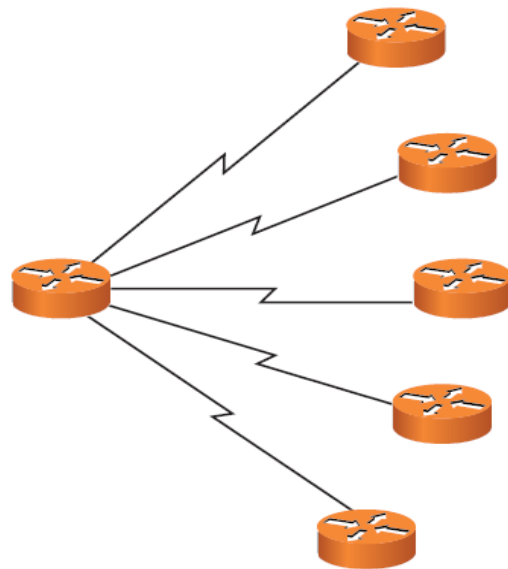


*Characteristics, Benefits, and Drawbacks of a ring Topology Partial-Mesh Topology :-*

Characteristics	Benefits	Drawbacks
Selected sites (that is, sites with frequent intersite communication) are interconnected via direct links, whereas sites that have less-frequent communication can communicate via another site.	A partial-mesh topology provides optimal routes between selected sites with higher intersite traffic volumes, while avoiding the expense of interconnecting every site to every other site.	A partial-mesh topology is less fault tolerance than a full-mesh topology.
A partial-mesh topology uses fewer links than a full-mesh topology and more links than a hub-and-spoke topology for interconnecting the same number of sites.	A partial-mesh topology is more redundant than a hub-and-spoke topology.	A partial-mesh topology is more expensive than a hub-and-spoke topology.

## Hub-and-Spoke Topology

- ✓ When interconnecting multiple sites (for example, multiple corporate locations) via WAN links, a hub-and-spoke topology has a WAN link from each remote site (that is, a spoke site ) to the main site (that is, the hub site ). This approach, an example of which is shown in Figure 1-10 , is similar to the star topology used in LANs.
- ✓ With WAN links, a service provider is paid a recurring fee for each link. Therefore, a hub-and-spoke topology helps minimize WAN expenses by not directly connecting any two spoke locations. If two spoke locations need to communicate between themselves, their communication is sent via the hub location. contrasts the benefits and drawbacks of a hub-and-spoke WAN topology



---

## Wireless topology

- A wireless access point (AP) allows mobile users to connect to a wired network wirelessly via radio frequency technologies. Using wireless technologies, APs also allow wired networks to connect to each other and are basically the wireless equivalent of hubs or switches because they can connect multiple wireless (and often wired) devices together to form a network.
- The main difference between LAN and WLAN is WLANs use radiated energy waves, generally called radio waves, to transmit data, whereas LAN uses electrical signals flowing over a cable .



abdelsamir@alsharif.com

23



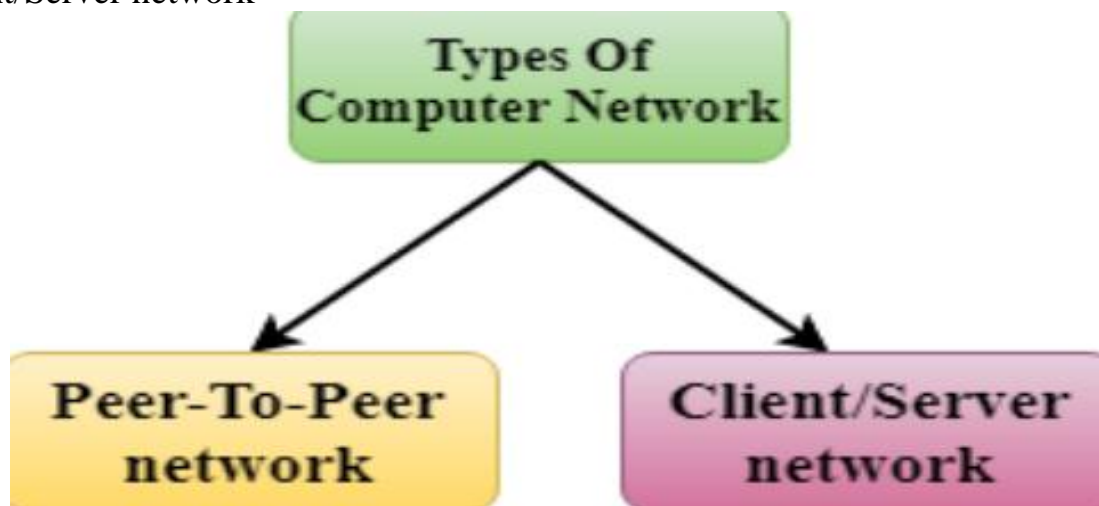
Networks Defined by Resource Location or computer network architecture

Network architecture refers to how computers are organized in a system and how tasks are allocated between these computers.

Two of the most widely used types of network architecture are peer-to-peer and client/server. Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

○ *The two types of network architectures are used:*

- ✓ Peer-To-Peer network
- ✓ Client/Server network



### *Peer to peer (Workgroups )*

• **Peer-to-peer networks** allow interconnected devices (for example, PCs) to share their resources with one another. Those resources could be, for example, files or printers and so on. • Each PC that's a member of the group can access the resources being shared by other PCs and in turn can share its own if configured to do so. Windows workgroups can be found in homes, schools and small businesses.

• **Joining a workgroup** requires setting up the PC with a workgroup name matching that of other PCs in the group. All Windows PCs are automatically assigned to a default group named "WORKGROUP" (in Windows XP,



"MSHOME"). Users with administrative privileges can change this name from the Windows Control Panel (the "Change settings" link under System). Note that workgroup names are managed separately from computer names.

- **In computer networking**, a workgroup is a collection of computers on a local area network (LAN) that share common resources and responsibilities. The term is most commonly associated with Microsoft Windows workgroups but also applies in other environments

---

### *Peer to peer (Workgroups ) (cont.)*

- In workgroup all computers have equal rights.
- Workgroup has a limit of twenty computers.
- In workgroup all computers must be on same local network.
- Workgroup works on all windows version.
- Workgroup works on both IP versions: IPv4 and IPv6.
- In workgroup every computer requires same workgroup name.
- Workgroup needs technical knowledge to setup.
- Workgroup requires security and sharing permissions to be set.
- To use a workgroup computer you need to have a user account on that computer.
- Passwords can become out of synchronize, if changed on one computer and not others

---

### *Characteristics, Benefits, and Drawbacks of a Peerto-Peer Network :-*

Characteristics	Benefits	Drawbacks
Client devices (for example, PCs) share their resources (for example, file and printer resources) with other client devices.	Peer-to-peer networks can be installed easily because resource sharing is made possible by the clients' operating systems, and knowledge of advanced NOSs is not required.	Scalability is limited because of the increased administration burden of managing multiple clients.
Resource sharing is made available through the clients' operating systems.	Peer-to-peer networks usually cost less than client/server networks because there is no requirement for dedicated server resources or advanced NOS software.	Performance might be less than that seen in a client/server network because the devices providing network resources might be performing other tasks not related to resource sharing (for example, word processing).

### *What is a homegroup?*

- A homegroup makes it easier to share files and printers on a home network. You can share pictures, music, videos, documents, and printers with other people in your homegroup. Other people can't change the files that you share, unless you give them permission to do so.
- When you set up a computer with this version of Windows, a homegroup is created automatically if one doesn't already exist on your home network. If a homegroup already exists, you can join it. After you create or join a homegroup, you can select the libraries that you want to share. You can prevent specific files or folders from being shared, and you can share additional libraries later. You can help protect your homegroup with a password, which you can change at any time.
- A homegroup is protected with a password, but you only need to type the password once

---

### *Homegroup :-*

- Homegroup does not have a limit of computers.
- You can join as much computers as you want.
- Homegroup can be password protected.
- Homegroup is easy to setup. All sharing options are enabled automatically.
- Homegroup can be span over the subnet.
- Homegroup requires window7 or higher version.
- If your network has all computers lower than windows 7 then you should use workgroup. But if you have windows 7 or higher version then you should always use homegroup to take the advantage of new features.

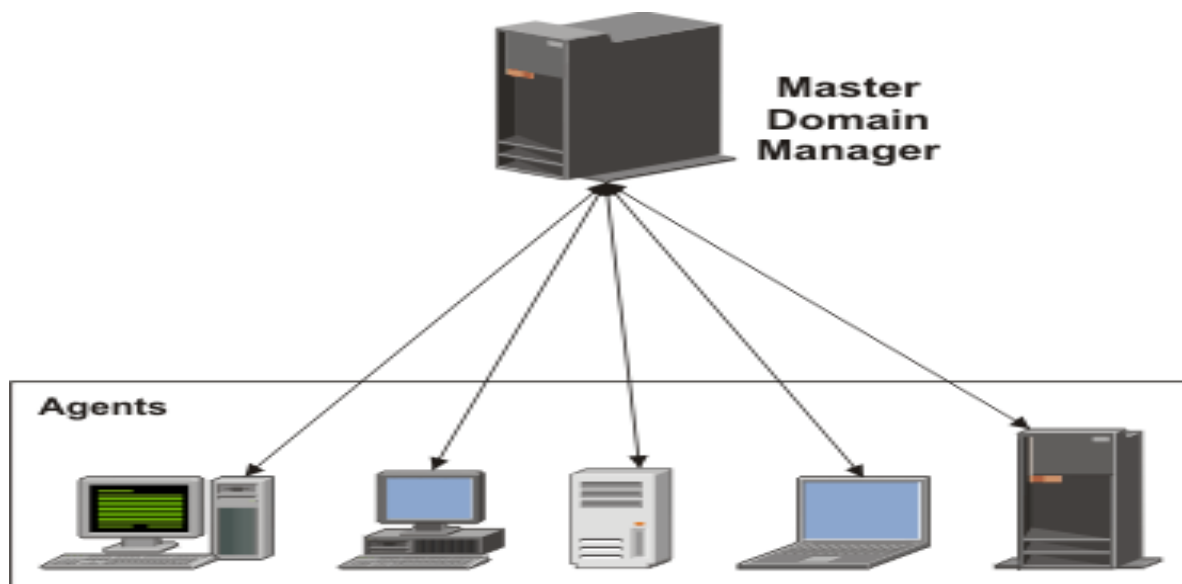
---

## *Client and server architecture :-*

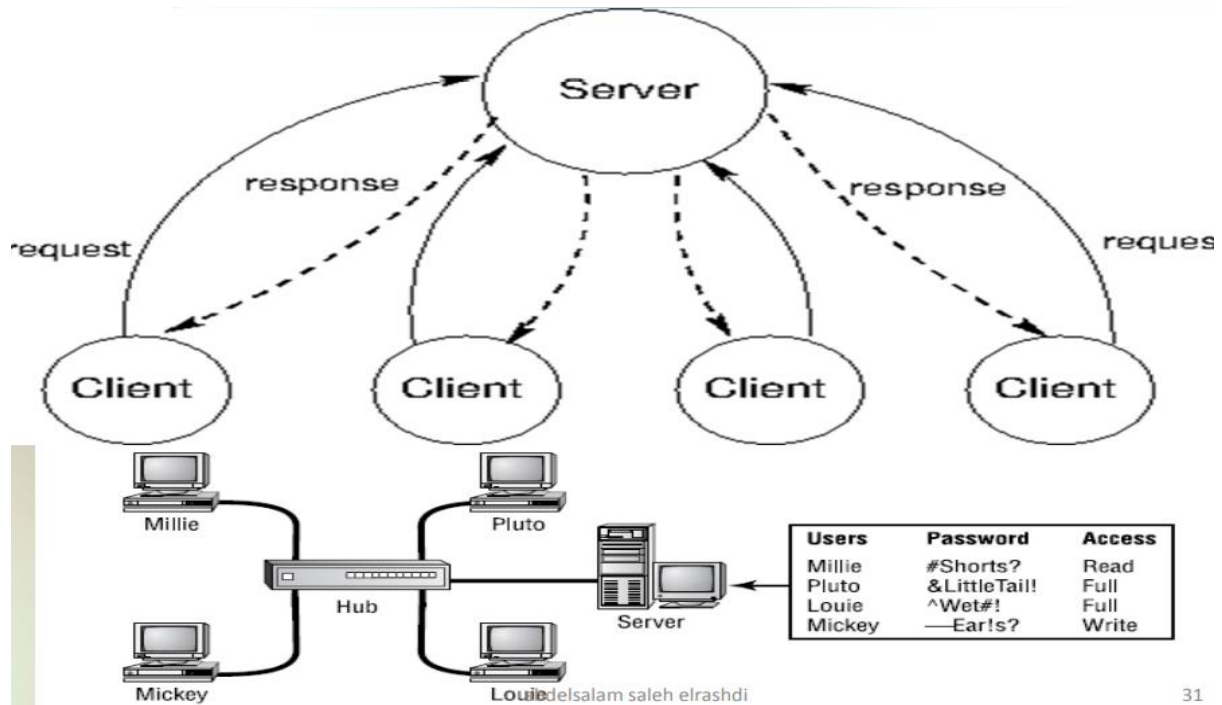
- Client-server architecture is an architecture of a computer network in which many clients (remote processors) request and receive service from a centralized server (host computer). Client computers provide an interface to allow a computer user to request services of the server and to display the results the server returns.

Servers wait for requests to arrive from clients and then respond to them. Ideally, a server provides a standardized transparent

interface to clients so that clients need not be aware of the specifics of the system (i.e., the hardware and software) that is providing the service. Clients are often situated at workstations or on personal computers, while servers are located elsewhere on the network, usually on more powerful machines.



## Client/Server Networks



31

## Client/Server Networks

- Client/server networks are pretty much the polar opposite of peer-to-peer networks because in them, a single server is specified that uses a network operating system for managing the whole network.
- Any a client machine's request for a resource goes to the main server, which responds by handling security and directing the client to the resource it wants .
- it's a whole lot easier to find the files you need because everything is stored in one spot on that special server.
- Your security also gets a lot tighter because all usernames and passwords are on that server.
- It uses for big network with huge number of users on the network.
- It doesn't require a lot of security.
- Need to operating system special with network like Windows

---

## *Characteristics, Benefits, and Drawbacks of a Client/Server Network*

<b>Characteristics</b>	<b>Benefits</b>	<b>Drawbacks</b>
Client devices (for example, PCs) share a common set of resources (for example, file or print resources) located on one or more dedicated servers.	Client/server networks can easily scale, which might require the purchase of additional client licenses.	Because multiple clients might rely on a single server for their resources, the single server can become a single point of failure in the network.
Resource sharing is made possible via dedicated server hardware and network operating systems.	Administration is simplified, because parameters, such as file sharing permissions and other security settings, can be administered on a server as opposed to multiple clients.	Client/server networks can cost more than peer-to-peer networks. For example, client/server networks might require the purchase of dedicated server hardware and a network OS with an appropriate number of licenses.

### *servers :-*

- File server Stores ,dispenses and shared files.
- E`Mail server The network`'s post office, which handles email functions.
- Print server Manages all printers on the network.
- Web server Manages web-based activities by running

Hypertext Transfer Protocol (HTTP) for storing web content and accessing web pages.

- Application server Manages network applications.
- Telephony server Handles the call center and call routing and can be thought of as a sophisticated network answering machine.

- Remote-access server Provides remote users with access to the network through modems, an IP connection, or wirelessly.

### *Client and server network (domain)*

- In a domain One or more computers are servers.
- Network administrators use servers to control the security and permissions for all computers on the domain ,This makes it easy to make changes because the changes are automatically made to all computers.
- If you have a user account on the domain, you can log on to any computer on the domain without needing an account on that computer.
- You probably can make only limited changes to a computer's settings because network administrators often want to ensure consistency among computers.
- There can be thousands of computers in a domain.
- The computers can be on different local networks.
- Need to operating system special with network like Windows server 2003,2008,2012,2016,2019

---

### *Characteristics, Benefits, and Drawbacks of a Client/Server Network :-*

Characteristics	Benefits	Drawbacks
Client devices (for example, PCs) share a common set of resources (for example, file or print resources) located on one or more dedicated servers.	Client/server networks can easily scale, which might require the purchase of additional client licenses.	Because multiple clients might rely on a single server for their resources, the single server can become a single point of failure in the network.
Resource sharing is made possible via dedicated server hardware and network operating systems.	Administration is simplified, because parameters, such as file sharing permissions and other security settings, can be administered on a server as opposed to multiple clients.	Client/server networks can cost more than peer-to-peer networks. For example, client/server networks might require the purchase of dedicated server hardware and a network OS with an appropriate number of licenses.

### *Application server :-*

Hosts web apps (computer programs that run inside a web browser) allowing users in the network to run and use them, without having to install a copy on their own computers. Unlike what the name might imply, these servers need not be part of the world wide web; any local network would do Database server Maintains and shares any form of database (organized collections of data with predefined properties that may be displayed in a table) over a network.

A database server is a computer system that provides other computers with services related to accessing and retrieving data from a database. Access to the database server may occur via a "front end" running locally a user's machine , or "back end" running on the database server itself, accessed by remote shell.

### *File server :-*

a file server (or fileserver) is a computer attached to a network that provides a location for shared disk access, shared storage of computer files (such as documents, sound files, photographs, movies, images, databases, etc.) that can be accessed by the workstations that are able to reach the computer that shares the access through a computer network. The term server highlights the role of



the machine in the client–server scheme, where the clients are the workstations using the storage. It is common that a file server does not perform computational tasks, and does not run programs on behalf of its clients. It is designed primarily to enable the storage and retrieval of data while the computation is carried out by the workstations.

---

### *Print server :-*

- A print server, or printer server, is a device that connects printers to client computers over a network. It accepts print jobs from the computers and sends the jobs to the appropriate printers, queuing the jobs locally to accommodate the fact that work may arrive more quickly than the printer can actually handle. Ancillary functions include the ability to inspect the queue of jobs to be processed, the ability to reorder or delete waiting print jobs, or the ability to do various kinds of accounting (such as counting pages, which may involve reading data generated by the printer(s)).

### *A Game server*

- (also sometimes referred to as a host) is a server which is the authoritative source of events in a multiplayer video game. The server transmits enough data about its internal state to allow its connected clients to maintain their own accurate version of the game world for display to players. They also receive and process each player's input.

---

### *A web server*

- A web server is a computer system that processes requests via HTTP, the basic network protocol used to distribute information on the World Wide Web. The term can refer to the entire system, or specifically to the software that accepts and supervises the HTTP requests • The primary function of a web server is to store, process and deliver web pages to clients. The communication between client and server takes place using the Hypertext Transfer Protocol (HTTP).

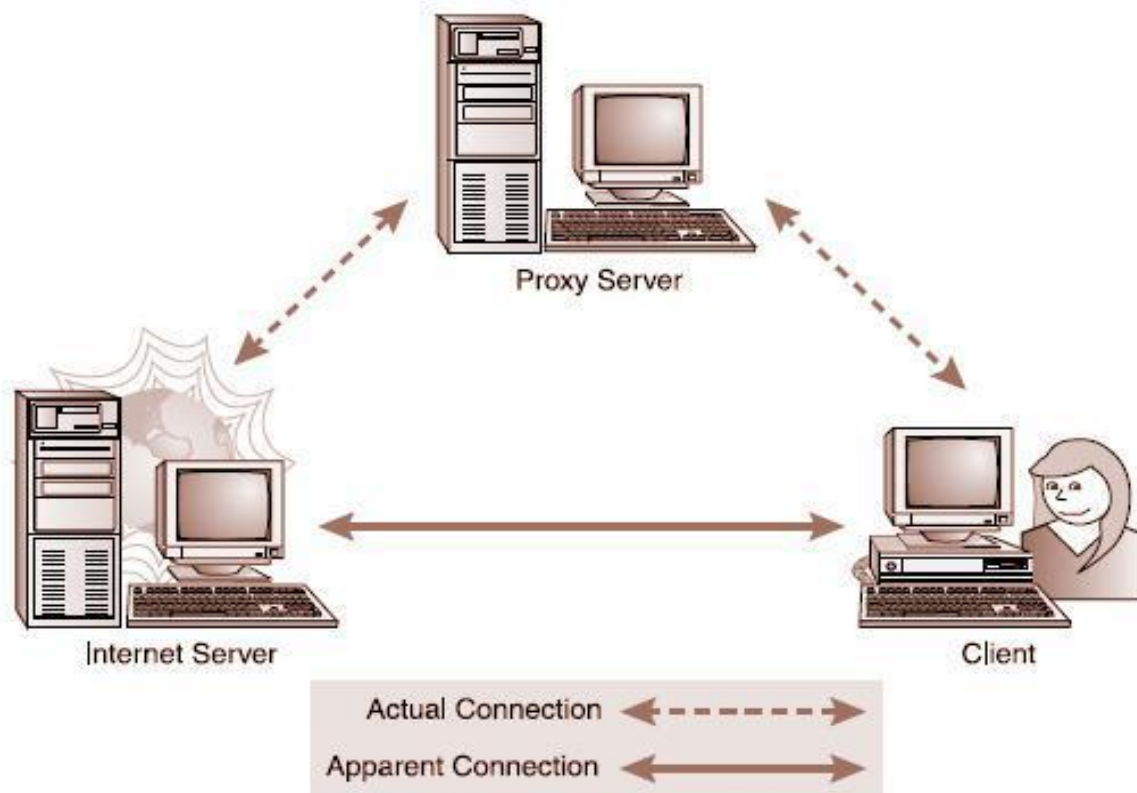
---

### *Proxy server*

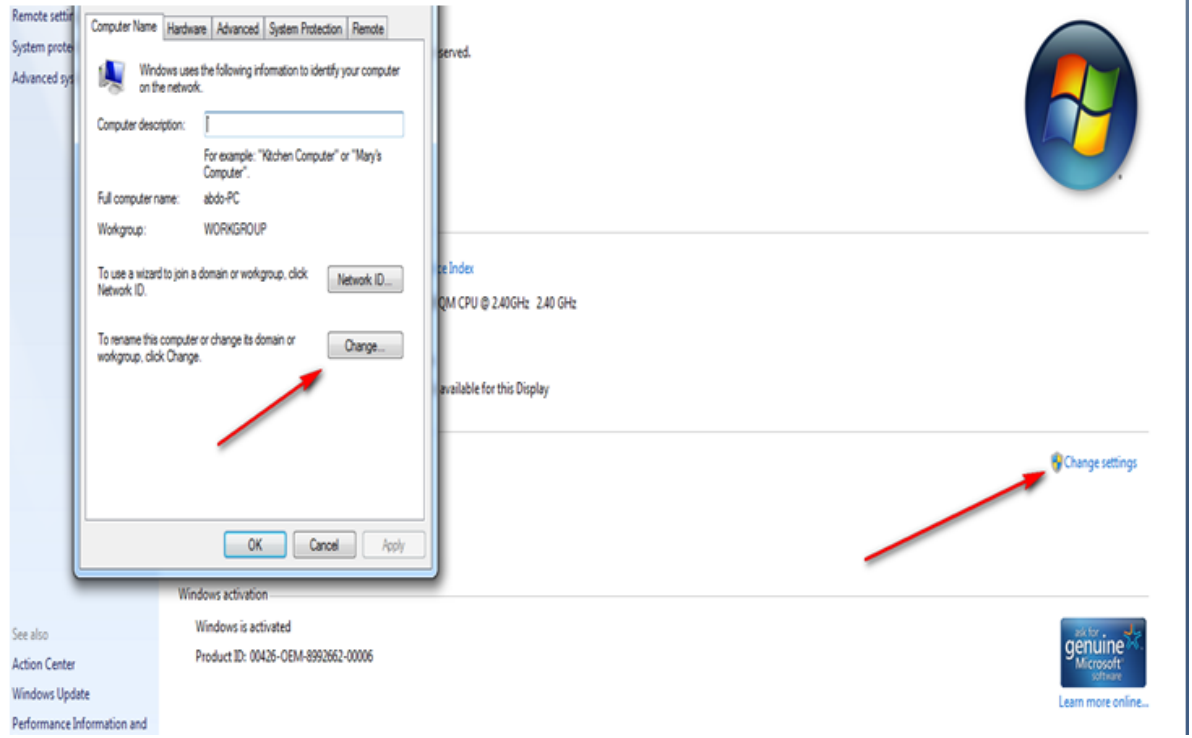
- In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking

resources from other servers. • A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity

- Today, most proxies are web proxies, facilitating access to content on the World Wide Web, providing anonymity and may be used to bypass IP address blocking.

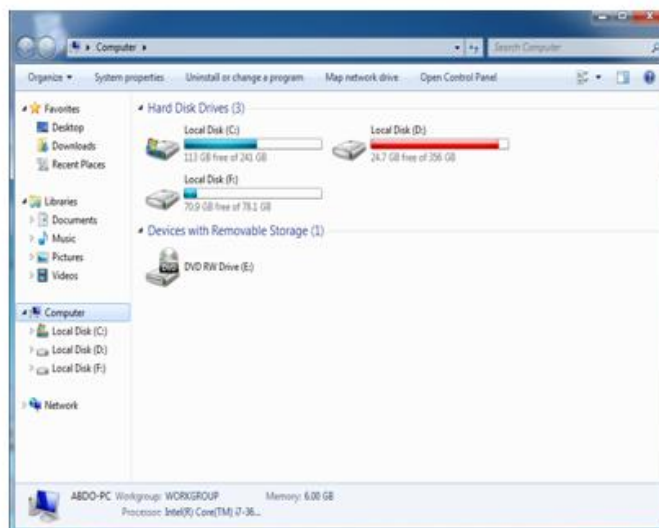


# Install workgroup network



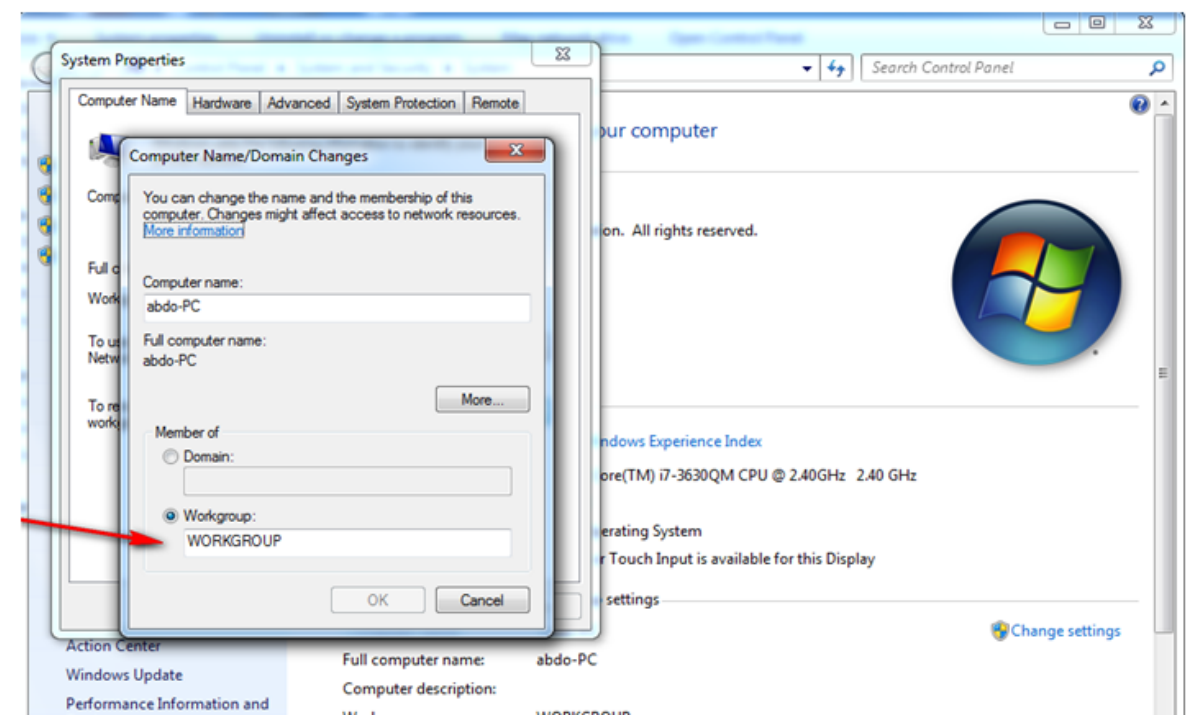
## Configure peer to peer network

Make sure from workgroup name must be same (computer + properties)



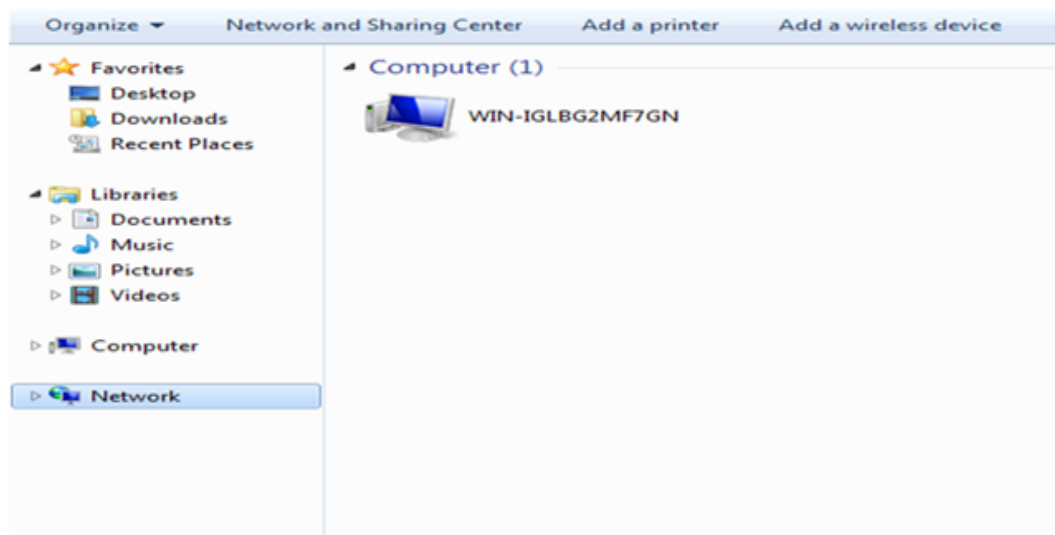
23

## Install workgroup network(cont)

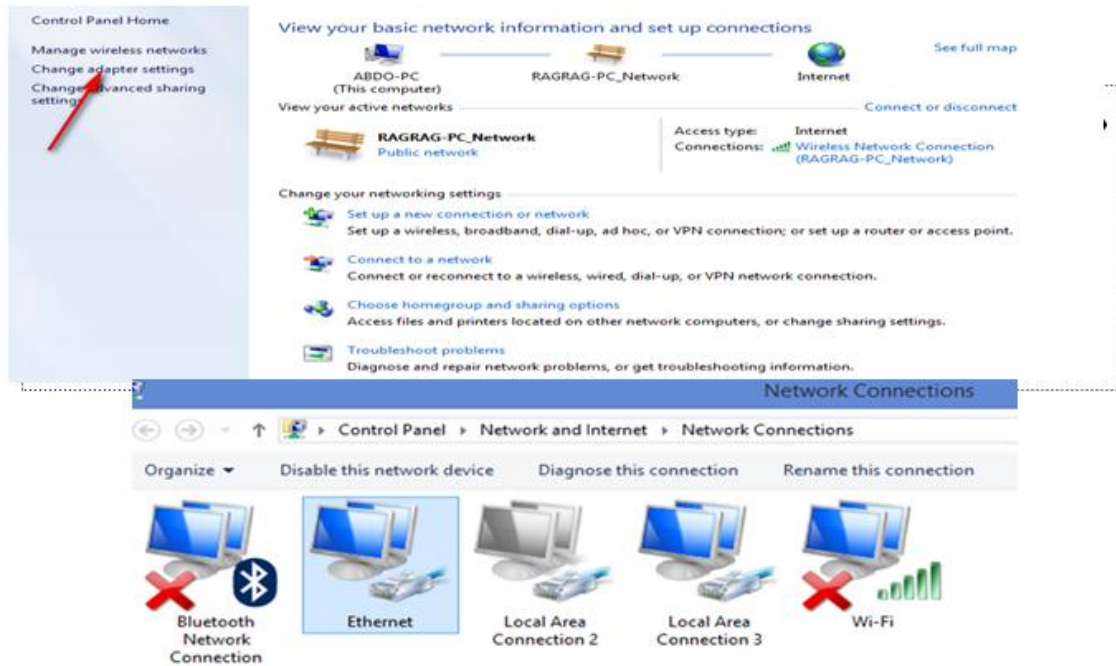


## Install workgroup network

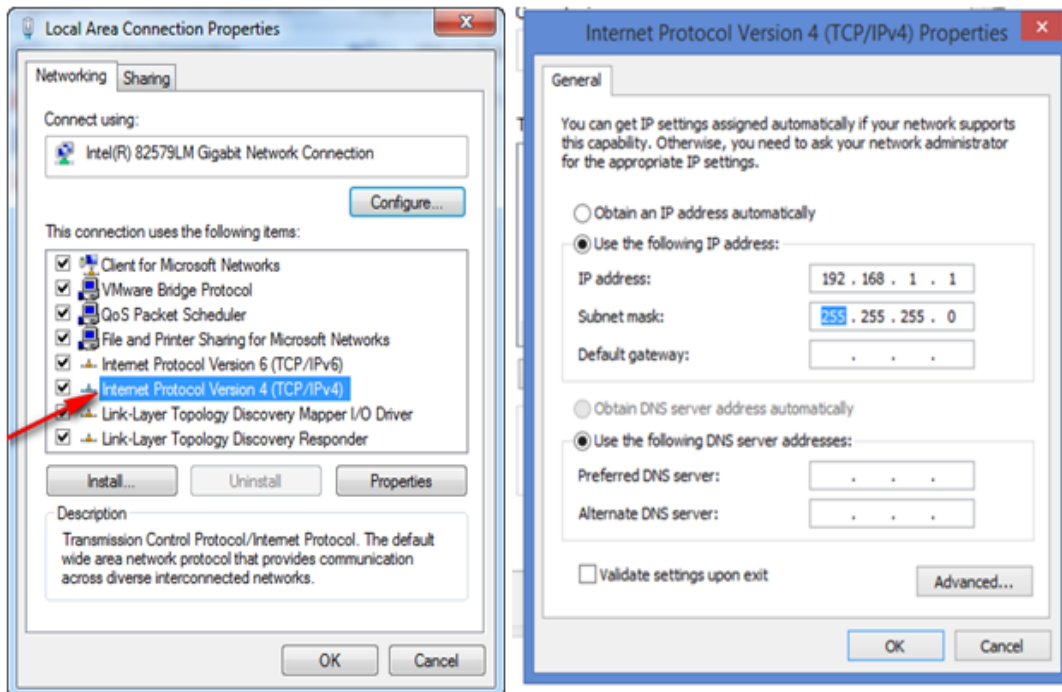
Configure IP address IPV4



# Configure IP address IPV4

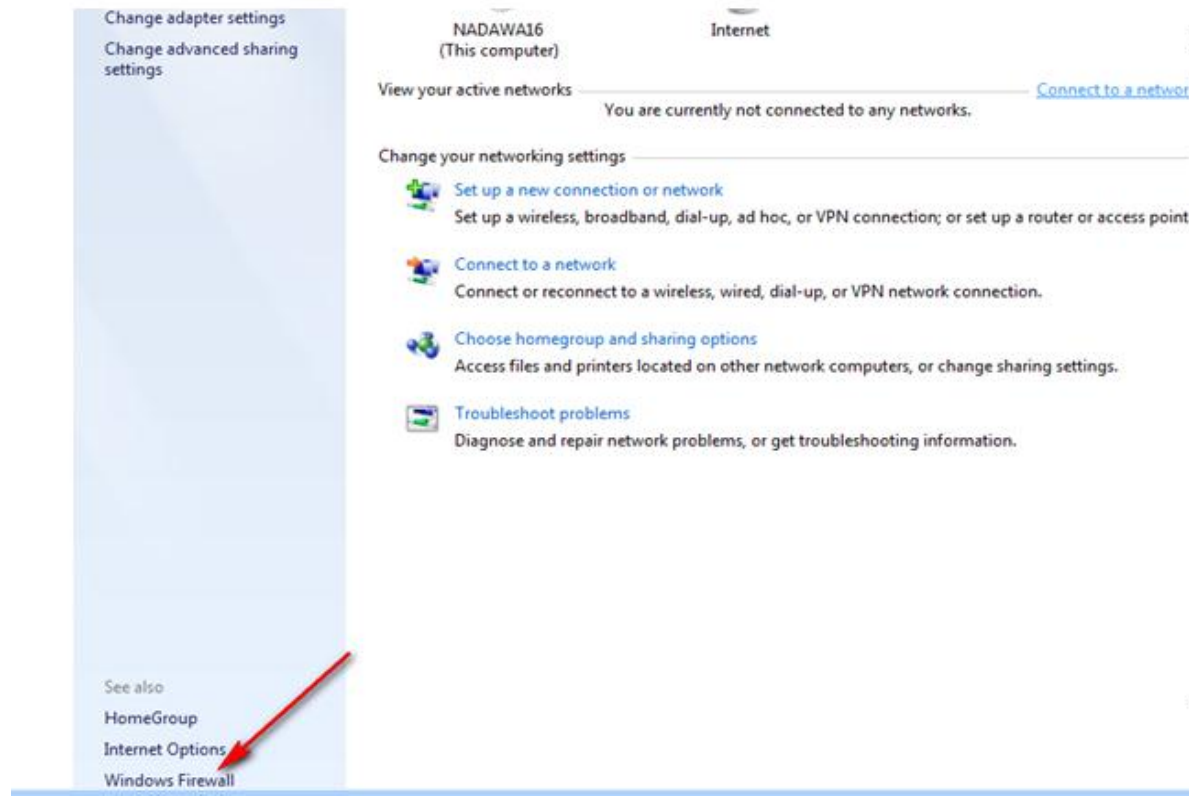


# Configure IP address

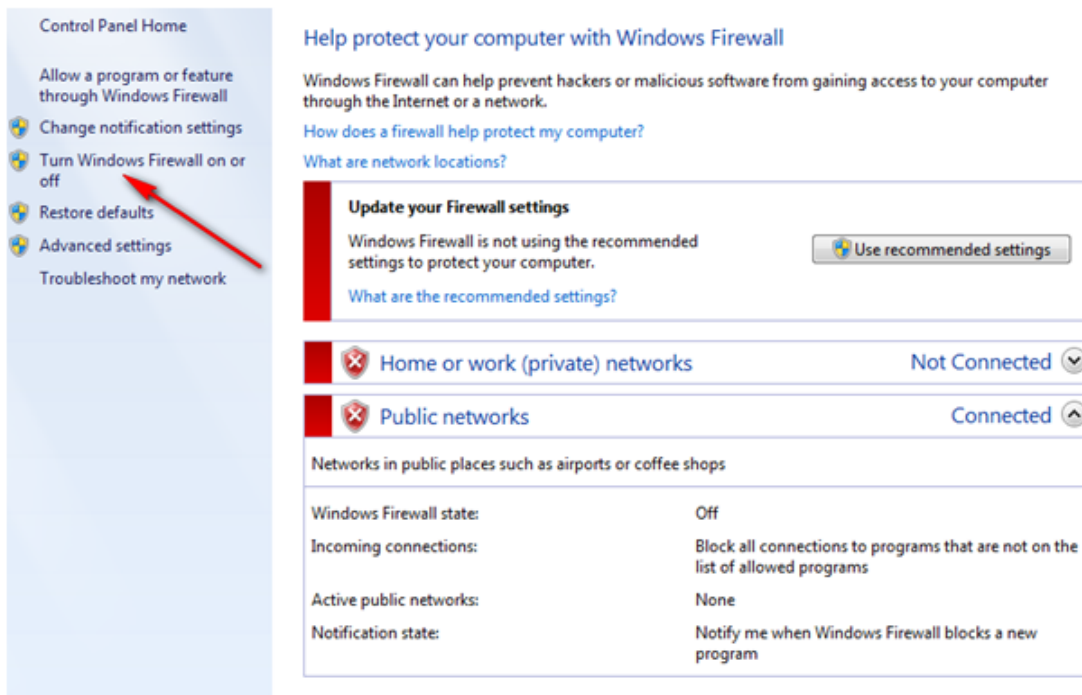


Same in all hosts in network with same network address

# Turn of firewall



## Turn of firewall (cont)





# Turn of firewall (cont)

## Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

### Home or work (private) network location settings



Turn on Windows Firewall

Block all incoming connections, including those in the list of allowed programs

Notify me when Windows Firewall blocks a new program



Turn off Windows Firewall (not recommended)

### Public network location settings



Turn on Windows Firewall

Block all incoming connections, including those in the list of allowed programs

Notify me when Windows Firewall blocks a new program



Turn off Windows Firewall (not recommended)

# Turn of firewall (cont)

Control Panel Home

- Allow a program or feature through Windows Firewall
- Change notification settings
- Turn Windows Firewall on or off
- Restore defaults
- Advanced settings
- Troubleshoot my network

## Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

### Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

Use recommended settings

What are the recommended settings?



Home or work (private) networks

Not Connected



Public networks

Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	Off
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active public networks:	None
Notification state:	Notify me when Windows Firewall blocks a new program



## Turn of firewall (cont)

Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

- Turn on Windows Firewall
- Block all incoming connections, including those in the list of allowed programs
- Notify me when Windows Firewall blocks a new program

Turn off Windows Firewall (not recommended)

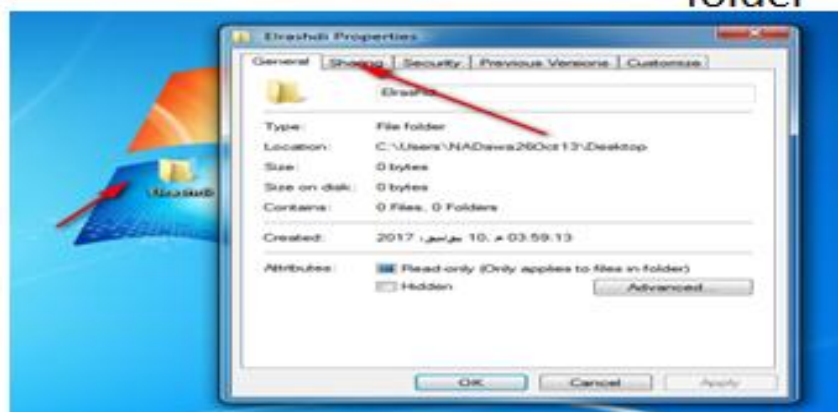
Public network location settings

- Turn on Windows Firewall
- Block all incoming connections, including those in the list of allowed programs
- Notify me when Windows Firewall blocks a new program

Turn off Windows Firewall (not recommended)

## Sharing folders

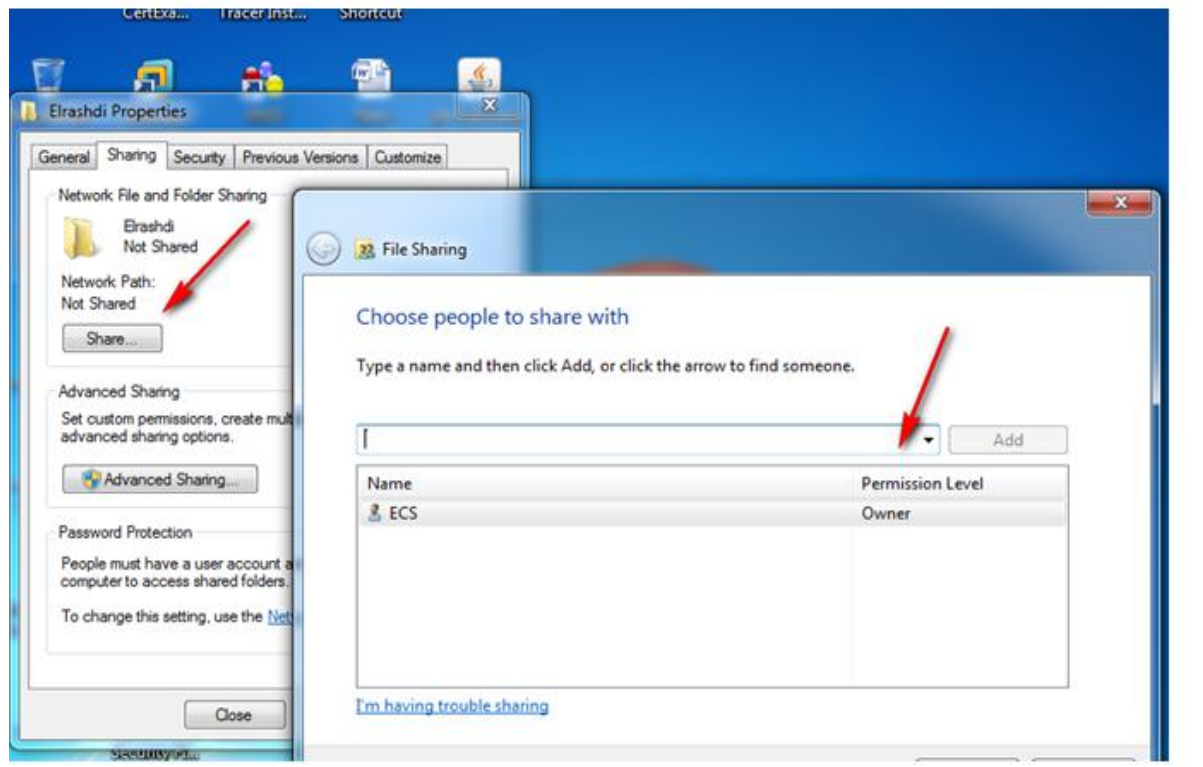
- Right click on folder then properties ,sharing
- then choice the people that can access to folder



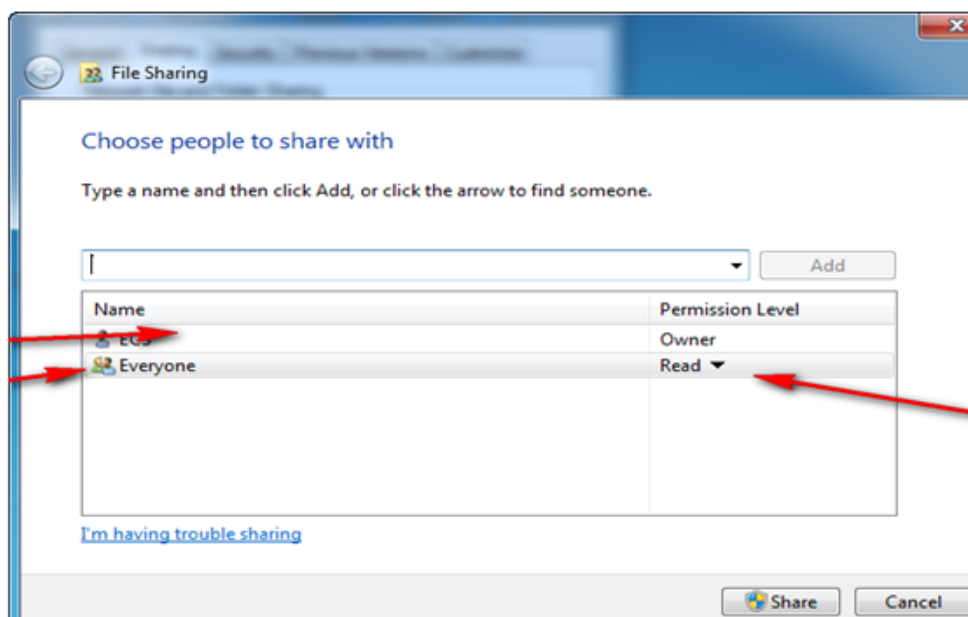
32

eng abdel salam saleh elnashdi

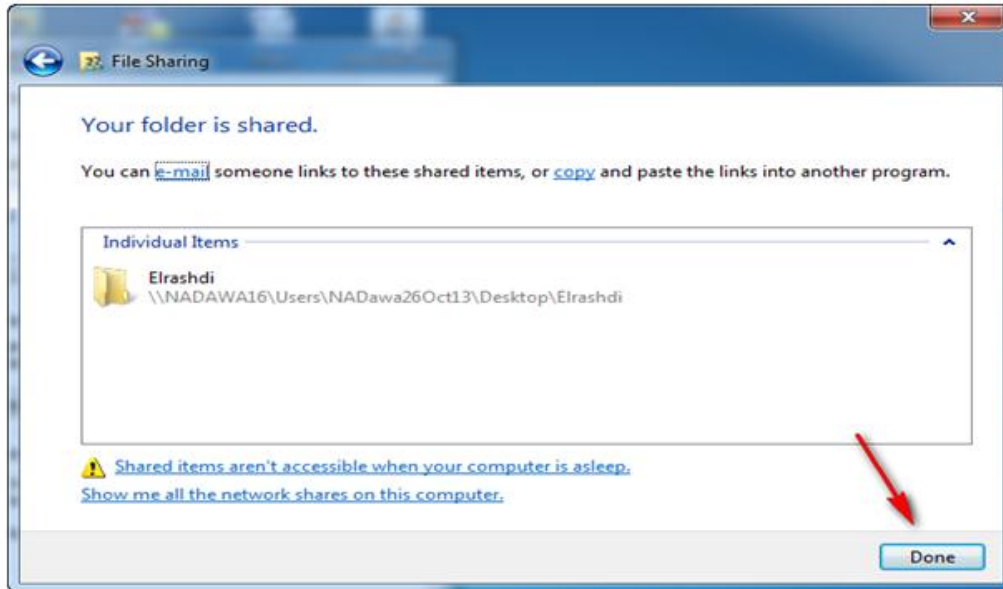
## sharing folders (cont)



## sharing folders (cont)

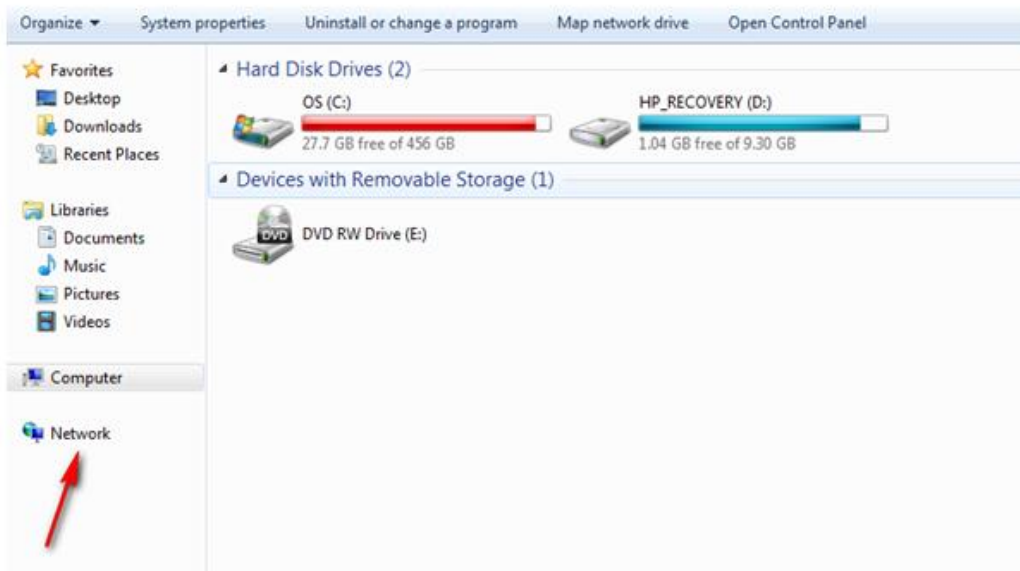


# sharing folders

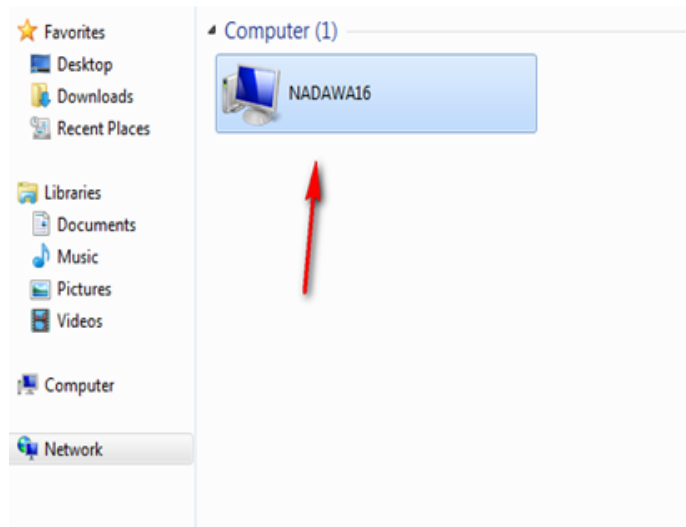


# Access to sharing folders

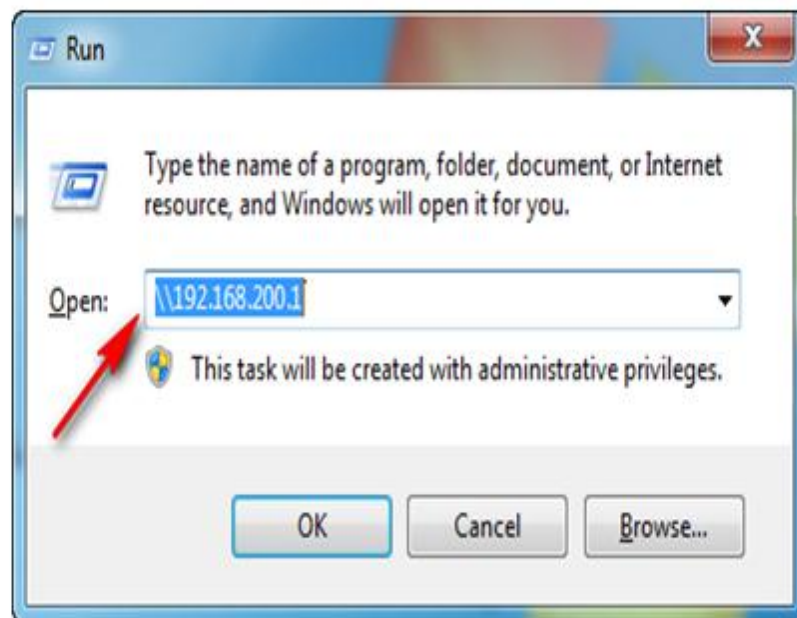
My computer ,network



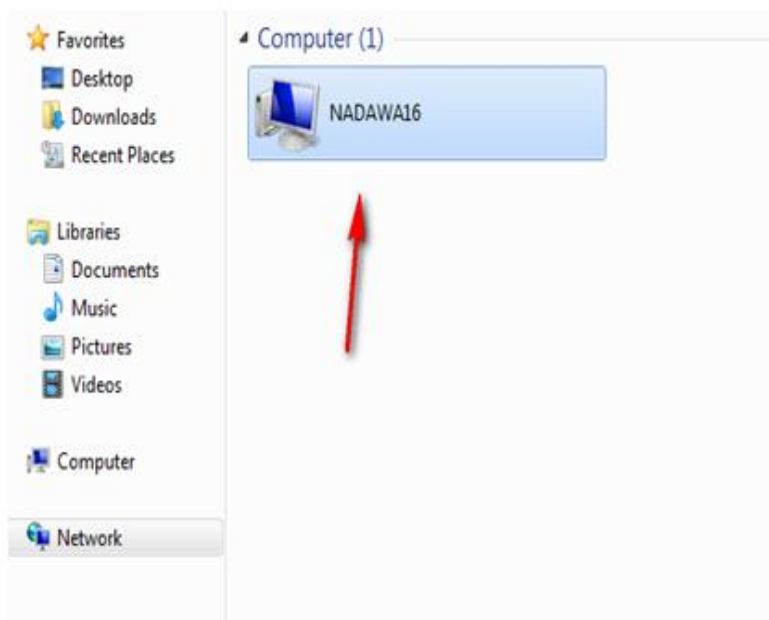
## Access to sharing folders(cont)



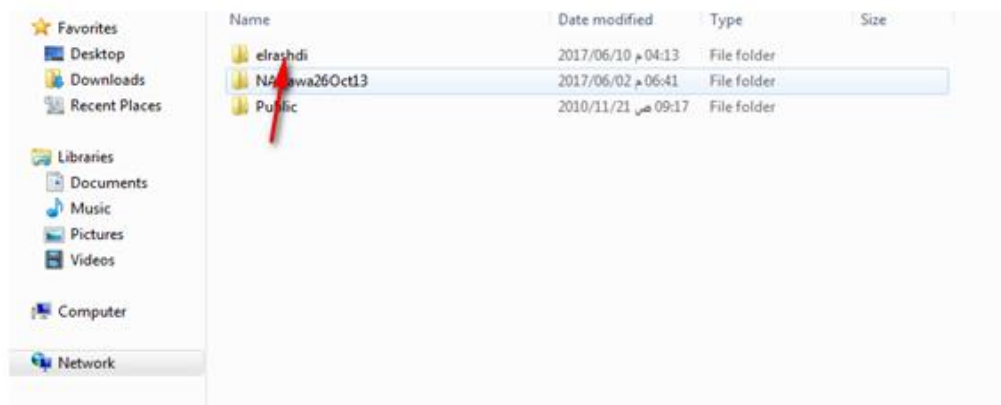
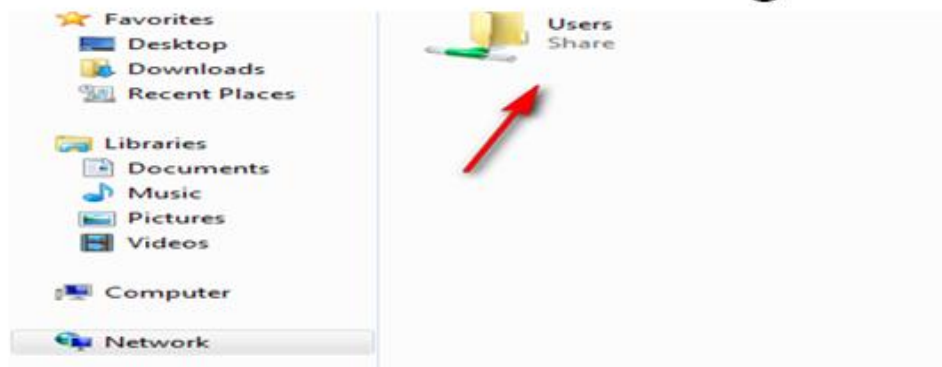
Another way to access to sharing folders



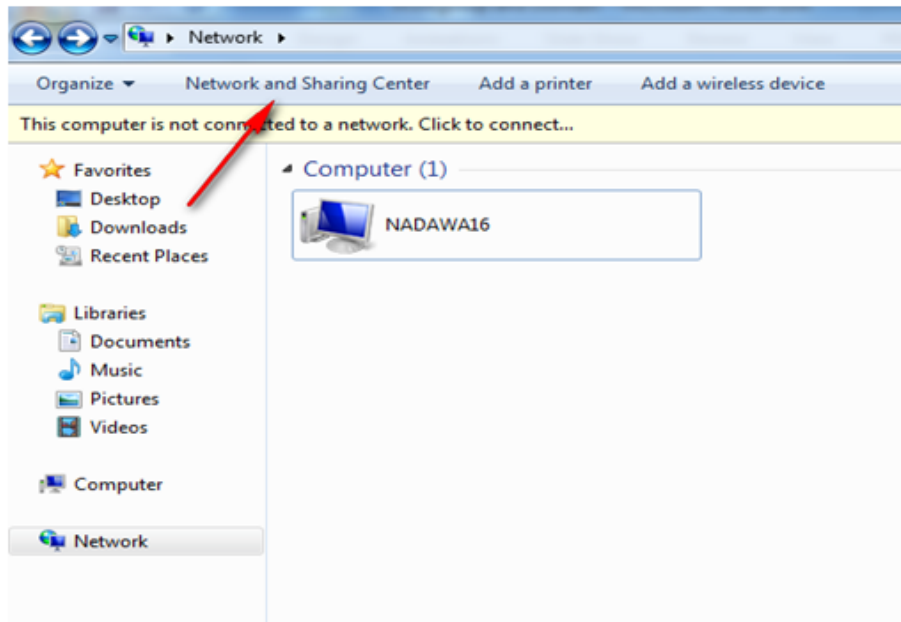
# Access to sharing folders



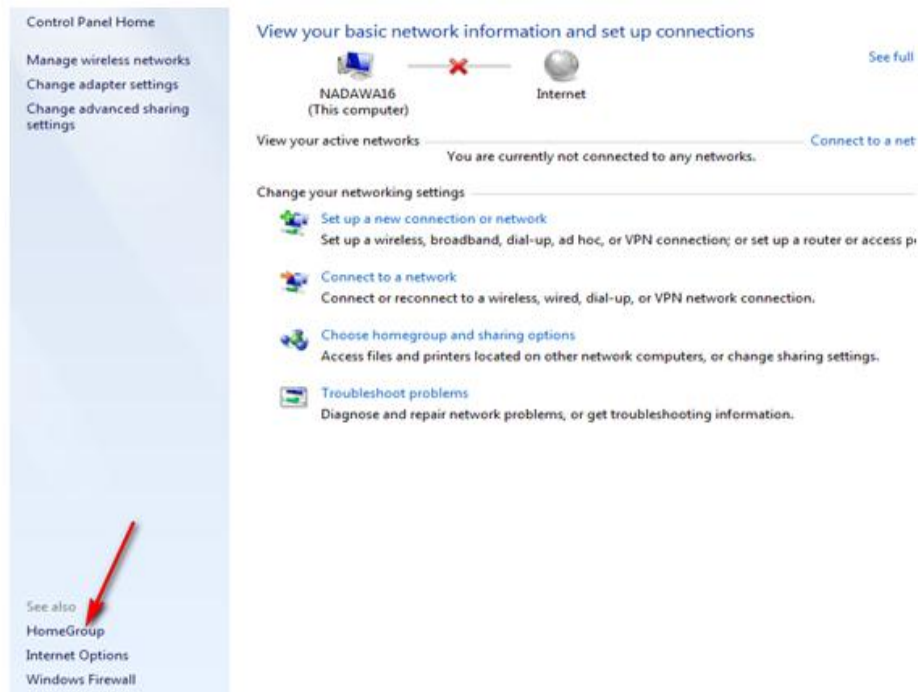
# Access to sharing folders



# Configure home group network

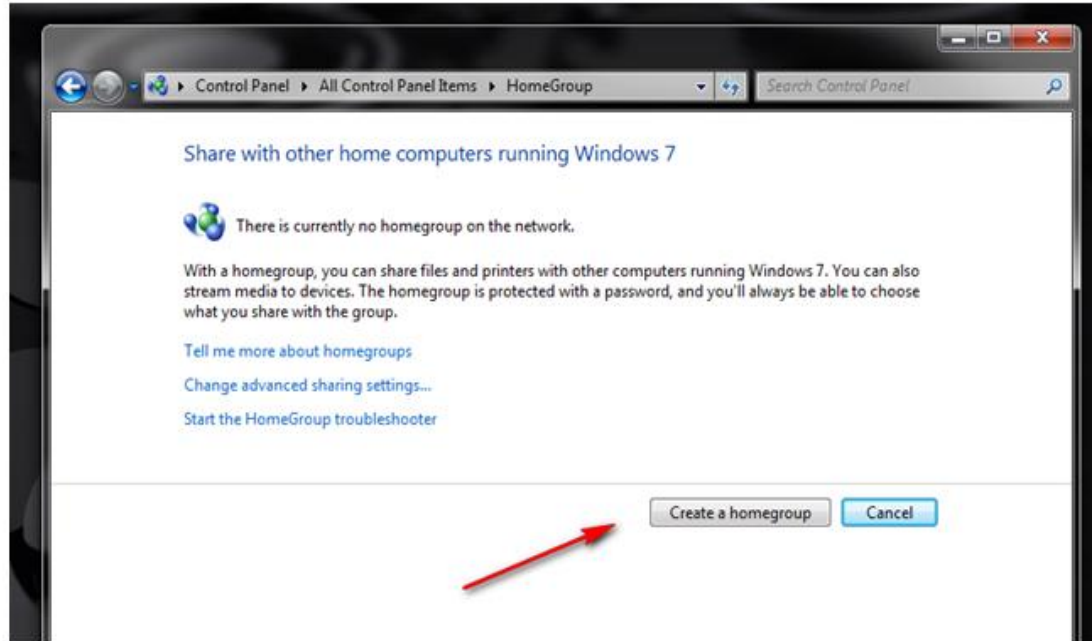


## Configure home group network (cont)





## Configure home group network (cont)

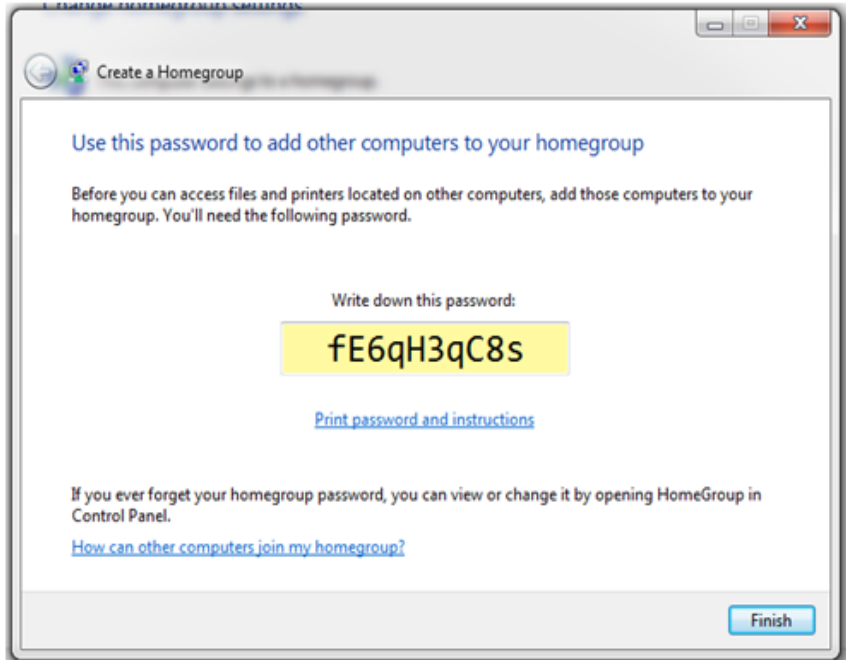


## Configure home group network(cont)



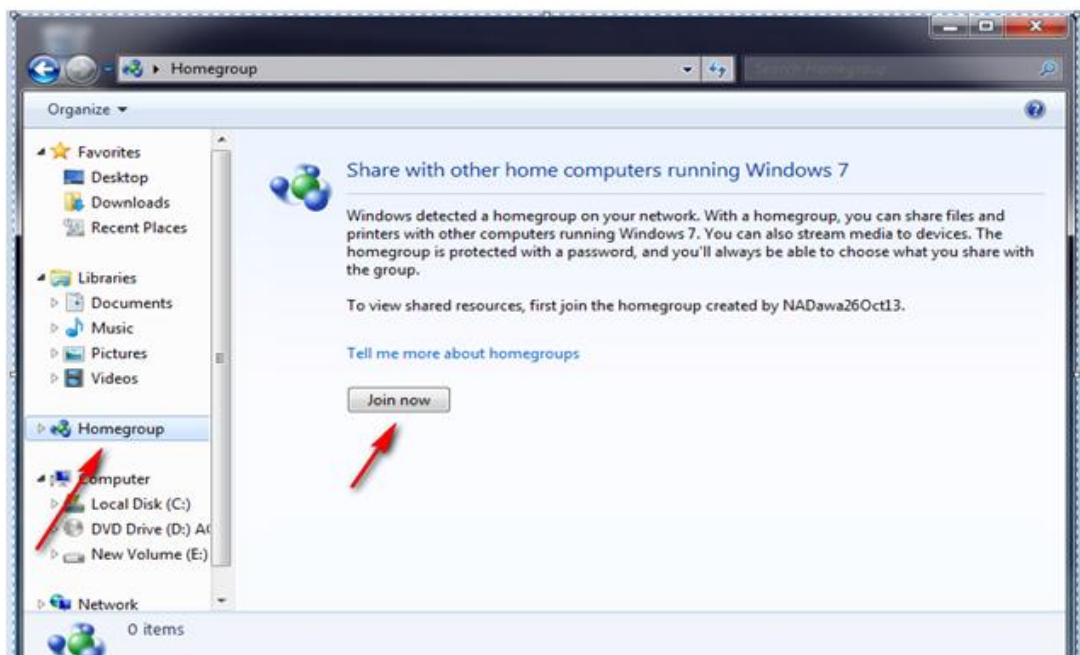


# Password protected

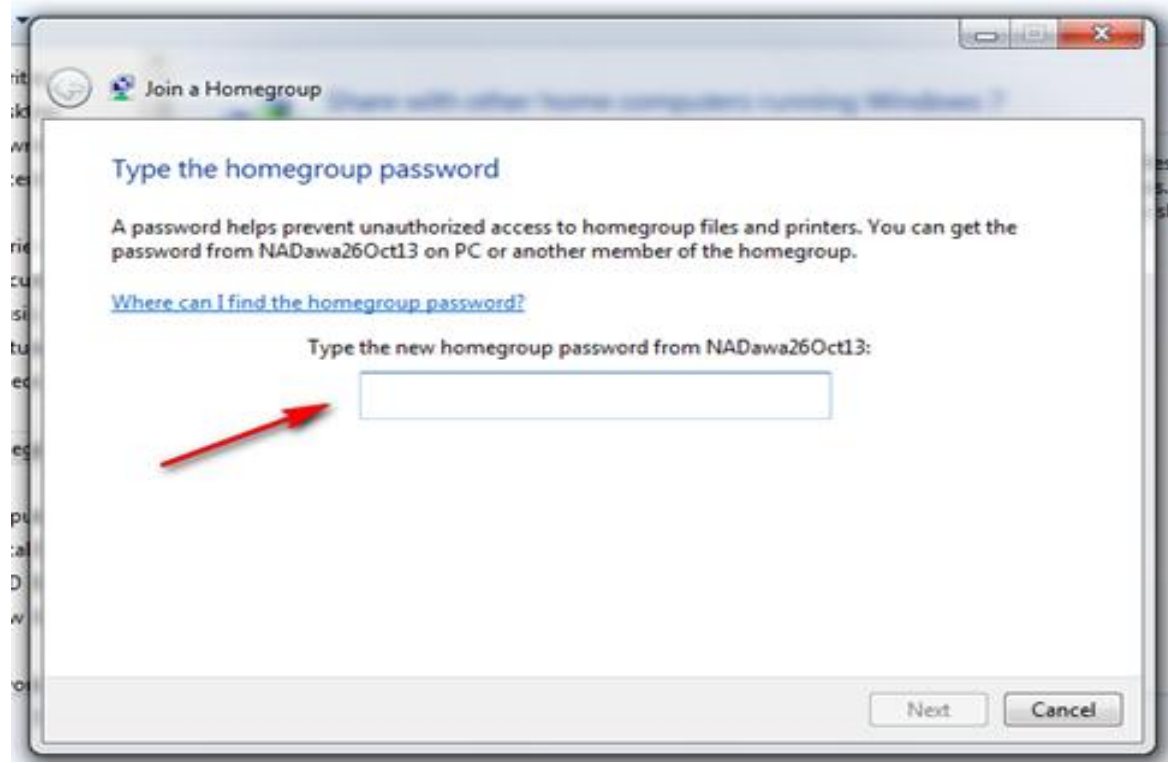


## Join to homegroup (cont)

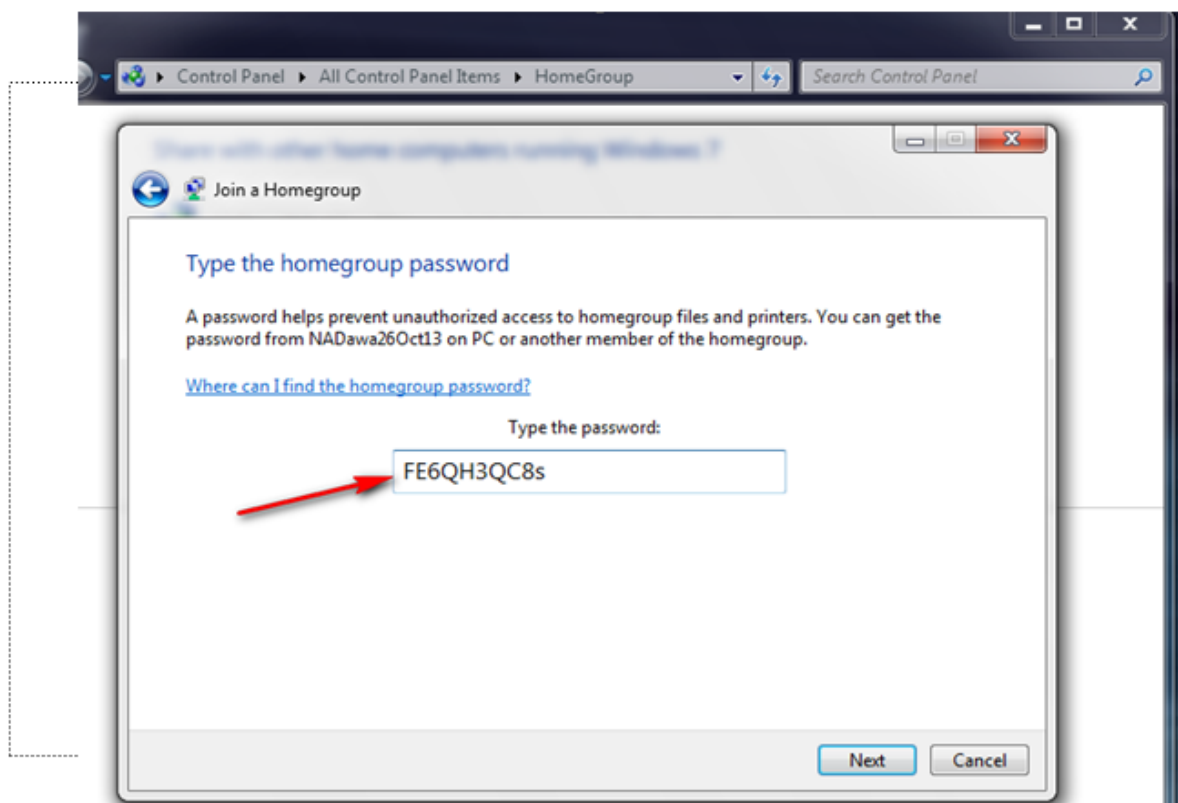
Computer then homegroup then join now



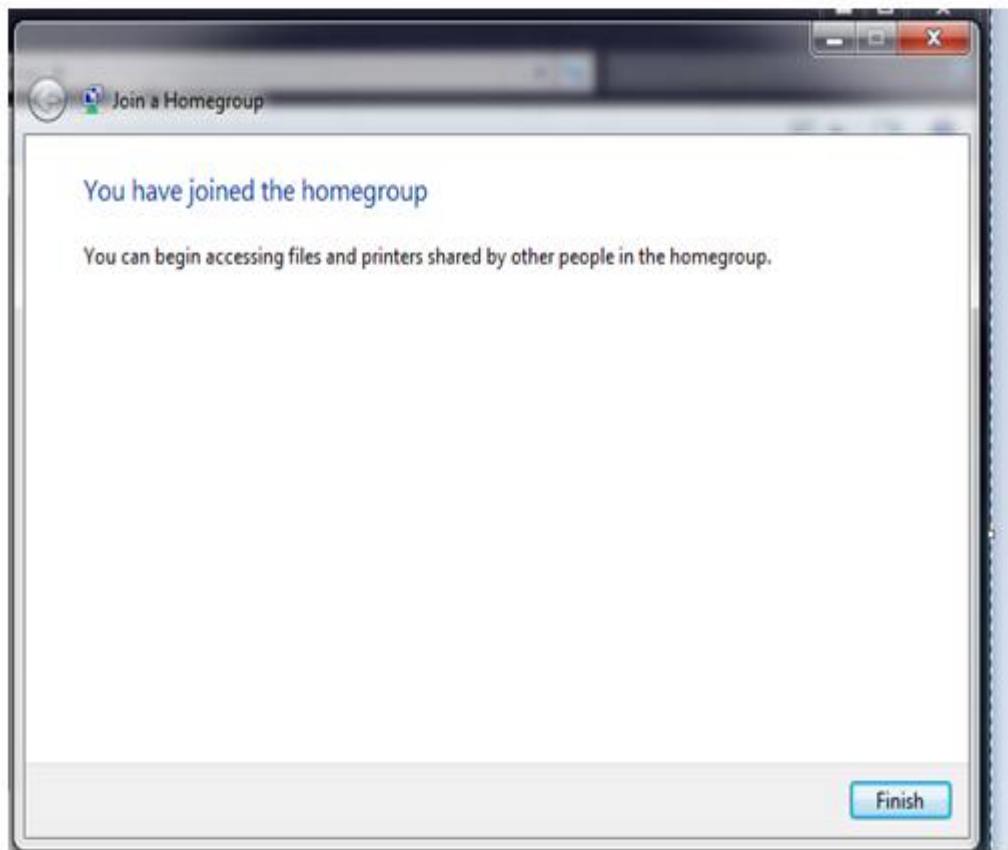
# Join to homegroup



## Type a password



## Now join to homegroup





# Chapter 3 ☺✍

---

## *Network media*

ABDELSALAM SALEH ELRASHDI

Networking fundamentals



## Chapter 3 ☺✍

### Outlines



- Define a network media
- The Purpose of media
- Types of cables
- Coaxial cable
- Twisted pair cable
- Fiber optical cable
- Console cable

---

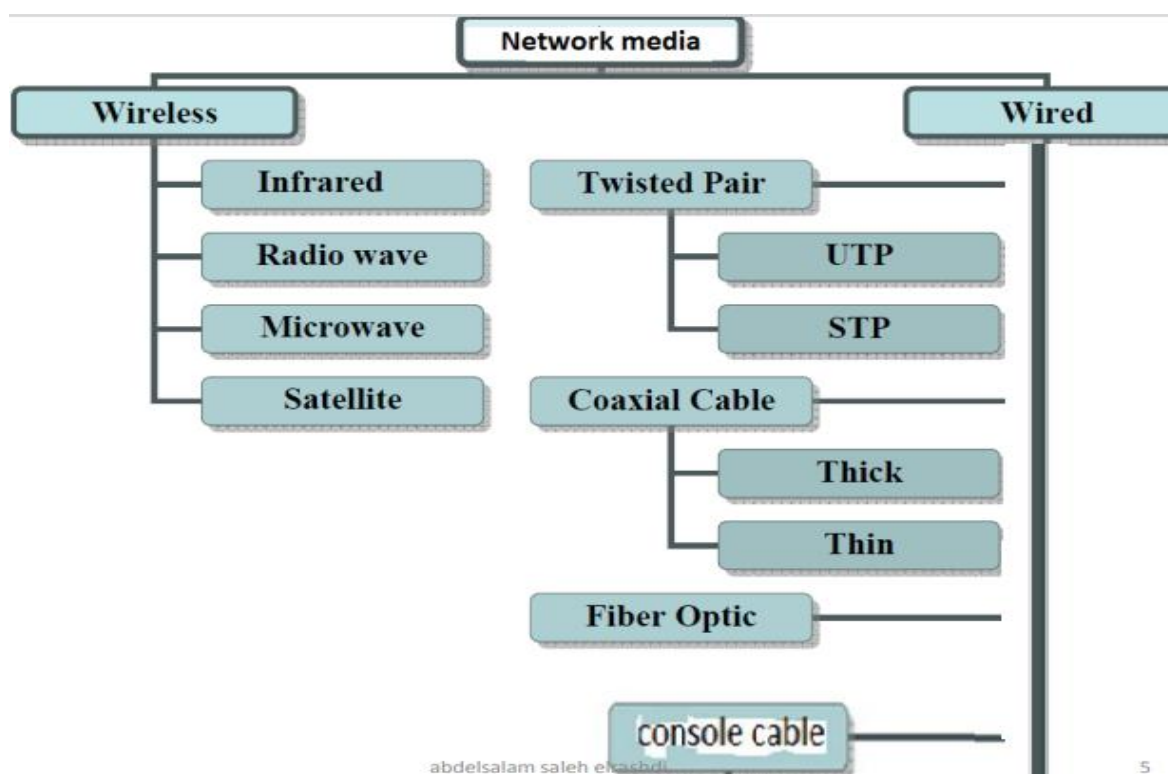
### Objectives

*By end of this lecture the student will be able :*

- Describe the types of media used in networking.
- Describe the characteristics and uses of each one.
- Describe the types of network cables
- Explain the coaxial cable, twisted pair, fiber optical cable.
- Describe advantages and disadvantages of cables.
- Comparison of the different types of cables

# Network media

- Network media refers to the communication channels used to interconnect nodes on a computer network. Typical examples of network media include copper coaxial cable, copper twisted pair cables and optical fiber cables used in wired networks, and radio waves used in wireless data communications networks.
- The media might be physical, such as a copper or fiber-optic cable. Alternatively, the media might be the air, through which radio waves propagate (as is the case with wireless networking technologies). This section contrasts various media types, including physical media



abdelsalam saleh elrahbani

5

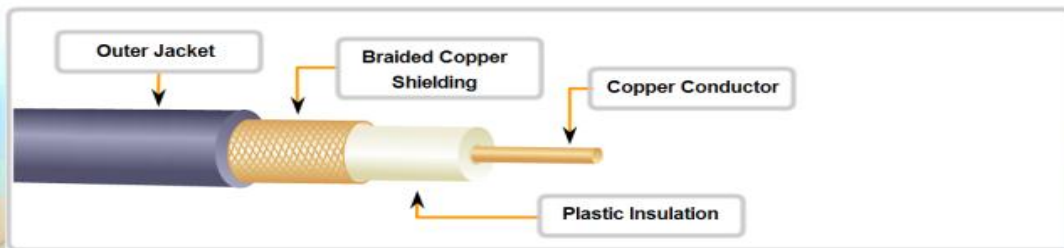
## *Coaxial cable*

- Coaxial cable (commonly referred to as coax ) is composed of two conductors, one of the conductors is an inner insulated conductor. This inner conductor is surrounded by another conductor. This second conductor is sometimes made of a metallic foil or woven wire.
- Because the inner conductor is shielded by the metallic outer conductor, coaxial cable is resistant to electromagnetic interference (EMI). For example, EMI occurs when an external signal is received on a wire and might result in a corrupted data transmission.
- As another example, EMI occurs when a wire acts as an antenna and radiates electromagnetic waves, which might interfere with data transmission on another cable. Coaxial cables have an associated characteristic impedance that needs to be balanced with the device (or terminator) with which the cable connects.
- **Coaxial lines** confine the electromagnetic wave to area inside the cable, between the center conductor and the shield. The transmission of energy in the line occurs totally through the dielectric inside the cable between the conductors.
- The most common use for coaxial cables is for television and other signals with bandwidth of multiple megahertz. Although in most homes coaxial cables have been installed for transmission of TV signals, new technologies
- There are two type of coaxial cable
- Thin Coaxial cable 185m (10base2)
- Thick Coaxial cable 500m (10base5)
- It is not used much this day.



# Coaxial Cable

## Coaxial Cable Design

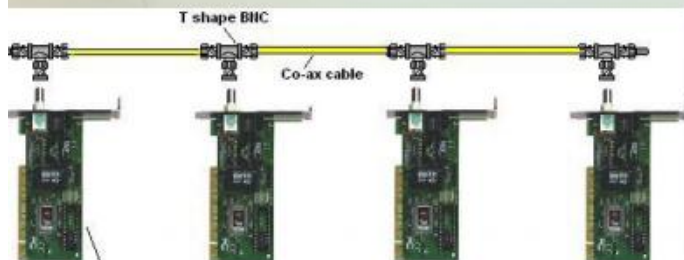
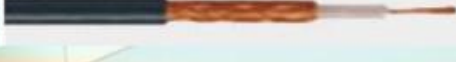


# Coaxial cable

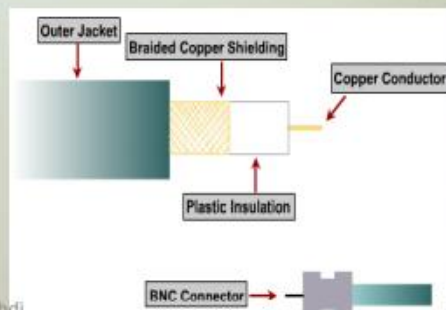
10BASE5 - "Thicknet"



10BASE2 - "Thinnet"



Network Interface Card (NIC) with BNC



abdeisalam saleh elrashdi

10

## *Types of coaxial cables*

- RG-59:
  - Typically used for short-distance applications, such as carrying composite video between two nearby devices. This cable type has loss characteristics such that it is not appropriate for longdistance applications. RG-59 cable has a characteristic impedance of 75 Ohms.
  - Where RG (for radio guide)
- 
- 

### *RG-6*

- Commonly used by local cable companies to connect individual homes to the cable company's distribution network. Like RG-59 cable, RG-6 cable has a characteristic impedance of 75 Ohms.
- 
- 

### *RG-58*

- Has loss characteristics and distance imitations similar to those of RG-59. However, the characteristic impedance of RG-58 is 50 ohms, and this type of coax was popular with early 10BASE2 Ethernet networks.
- 
- 

## *Common connectors used on coaxial cables*

- **BNC:** A Bayonet Neill-Concelman (BNC) (also referred to as British Naval - Connector in some literature) connector can be used for a variety of applications, including being used as a connector in a 10BASE2 Ethernet network.
  - A **BNC** coupler could be used to connect two coaxial cables together back to back.
  - **F-connector:** An F-connector is often used for cable TV (including cable modem) connections.
- 
- 

## *Twisted-Pair Cable*

- Twisted-pair cable consists of multiple individually insulated wires that are twisted together in pairs. Sometimes a metallic shield is placed around them; hence the name shielded twisted pair (STP).

- Today's most popular LAN media type is twisted-pair cable, where individually insulated copper strands are intertwined into a twisted-pair cable. Two categories of twisted-pair cable include shielded twisted pair (STP) and unshielded twisted pair (UTP).
  - There are two type of Twisted-pair unshielded twisted-pair (UTP). shielded twisted pair (STP).
  - It's easy to work with.
  - It allows transmission rates that were impossible 10 years ago.
  - most popular.
  - maximum length 100 M.
  - prone to noise.
- 

### ► *Unshielded Twisted-Pair*

- Unshielded Twisted Pair (UTP) cable is most certainly by far the most popular cable around the world. UTP cable is used not only for networking but also for the traditional telephone (UTP-Cat 1) • Unshielded twisted-pair cable (UTP) is a four-pair wire medium used in a variety of networks.
  - Each of the 8 individual copper wires in the UTP cable is covered by insulating material.
  - In addition, each pair of wires is twisted around each other.
  - This type of cable relies solely on the cancellation effect produced by the twisted wire pairs, to limit signal degradation caused by EM I and RFI.
  - CAT 5,CAT6, CAT 6A are the one most frequently recommended and implemented in installations today.
- 

### *UTP*

- Unshielded twisted-pair cable has many advantages.
- It is easy to install and is less expensive than other types of networking media.
- However, the real advantage is the size. Since it has such a small external diameter, UTP does not fill up wiring ducts as rapidly as other types of cable.

### *Common categories of UTP*

## Common categories of UTP

UTP Categories - Copper Cable				
UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

## Common categories of UTP cont

Category	Standard	Data rate	Frequency	# of Conductors
Cat 5	100BASE-TX	100 Mbit	100 MHz	4 or 8
Cat 5e	1000BASE-TX	1 Gbit	100 MHz Duplex	8
Cat 6	EIA/TIA 568B2.1	1-10 Gbit*	250 MHz	8
Cat 6A	10GBASE-T	10 Gbit	500 MHz	8
Cat 7	10GBASE-T	10 Gbit	600 MHz	8
Cat 7A	10GBASE-T	10 Gbit	1000 MHz	8
Cat 8	40GBASE-T	40 Gbit	1600-2000 MHz	8

\* Depends on length and cable type

## Common categories of UTP cont

Balanced Twisted-Pair Copper Cabling (4-pair)		
Application	Distance (meters)	Media - Components
10BASE-T	100 m	Categories 3, 5e, 6, 6A, and 7A
100BASE-T	100 m	Categories 3, 5e, 6, 6A, and 7A
1000BASE-T	100 m	Categories 5e, 6, 6A, and 7A
2.5GBASE-T <sup>1</sup>	100 m	Categories 6A and 7A
5GBASE-T <sup>1</sup>	100 m	Categories 6A and 7A
10GBASE-T	100 m	Categories 6A and 7A
25GBASE-T <sup>2</sup>	30 m	Categories 8, 8.1 and 8.2 <sup>3</sup>
40GBASE-T <sup>2</sup>	30 m	Categories 8, 8.1 and 8.2 <sup>3</sup>

<sup>1</sup> May operate over some configurations of installed categories 5e and 6.  
<sup>2</sup> Targeted for data center deployments only.  
<sup>3</sup> Category 8 defined by TIA. Categories 8.1 and 8.2 defined by ISO/IEC.

---

---

## Ethernet standards

- Defined in the IEEE 802.3 standard in 1983
- IEEE = Institute of Electrical and Electronics Engineers



# IEEE



## Ethernet standards (copper)

### Ethernet Standards (copper)

Speed	Common Name	IEEE Standard	Informal Name	Maximum Length
10 Mbps	Ethernet	802.3i	10BASE-T	100 m
100 Mbps	Fast Ethernet	802.3u	100BASE-T	100 m
1 Gbps	Gigabit Ethernet	802.3ab	1000BASE-T	100 m
10 Gbps	10 Gig Ethernet	802.3an	10GBASE-T	100 m

## Ethernet Local Area Networks (LANs)

Standard	Maximum Cable Length in Meters
10Base5	500
10Base2	185
10BaseT	100
100Base-TX	100
100Base-FX	400

# What's in a Name?

Ethernet naming rules:

## 10 Base T

Transmission Rate

Copper unshielded twisted pair

Baseband signaling

Uses the entire bandwidth of the transmission medium

# UTP Implementation Straight-through

Cable 10BaseT/  
100BaseT Straight-through



Hub/Switch



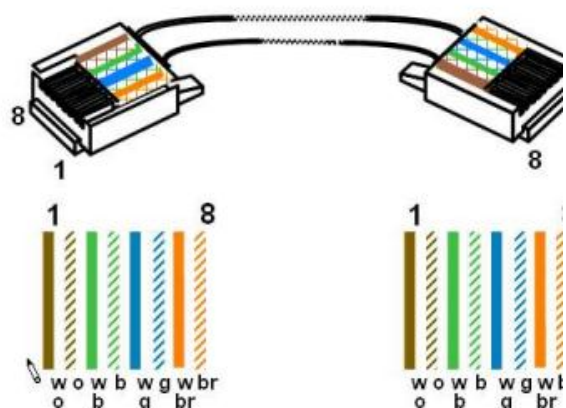
Server/Router

Pin Label

Pin Label	Pin Label
1 RD+	1 TD+
2 RD-	2 TD-
3 TD+	3 RD+
4 NC	4 NC
5 NC	5 NC
6 TD-	6 RD-
7 NC	7 NC
8 NC	8 NC

This just for 10base-t and 100 base-t

Straight-through Cable



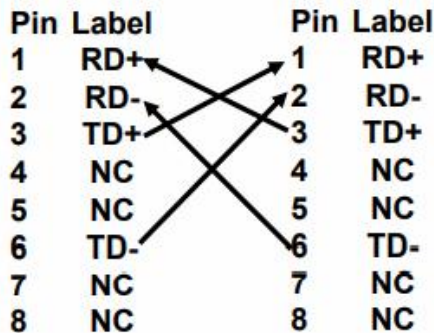
Wires on cable ends  
are in same order

26

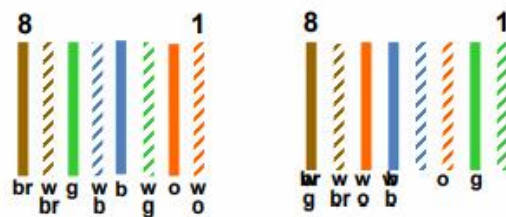
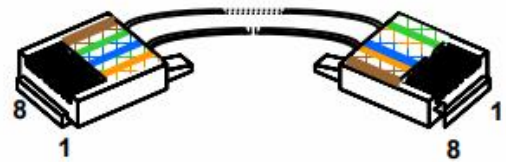


# UTP Implementation Crossover

## Cable 10BaseT/ 100BaseT Crossover



## Crossover Cable



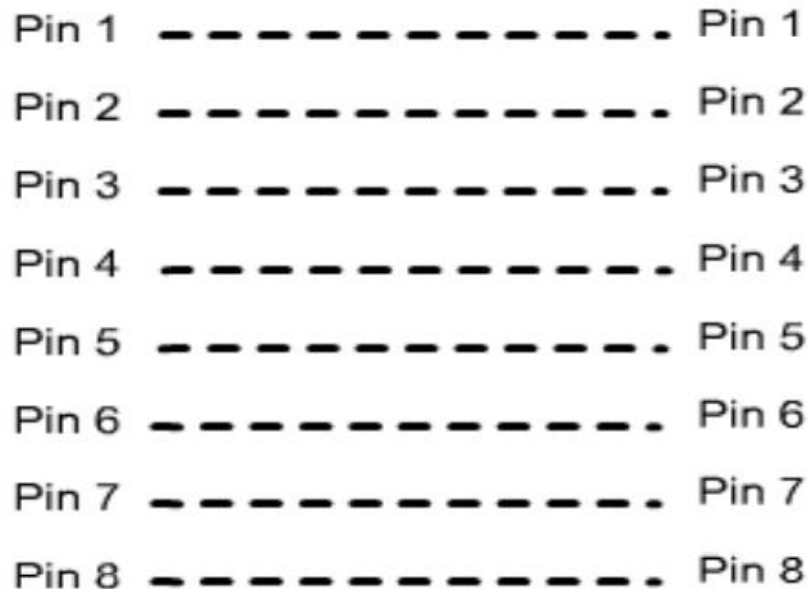
Some wires on cable ends are crossed

This just for 10base-t and 100 base-t

abdelsalam saleh elrashdi

27

## Straight cable



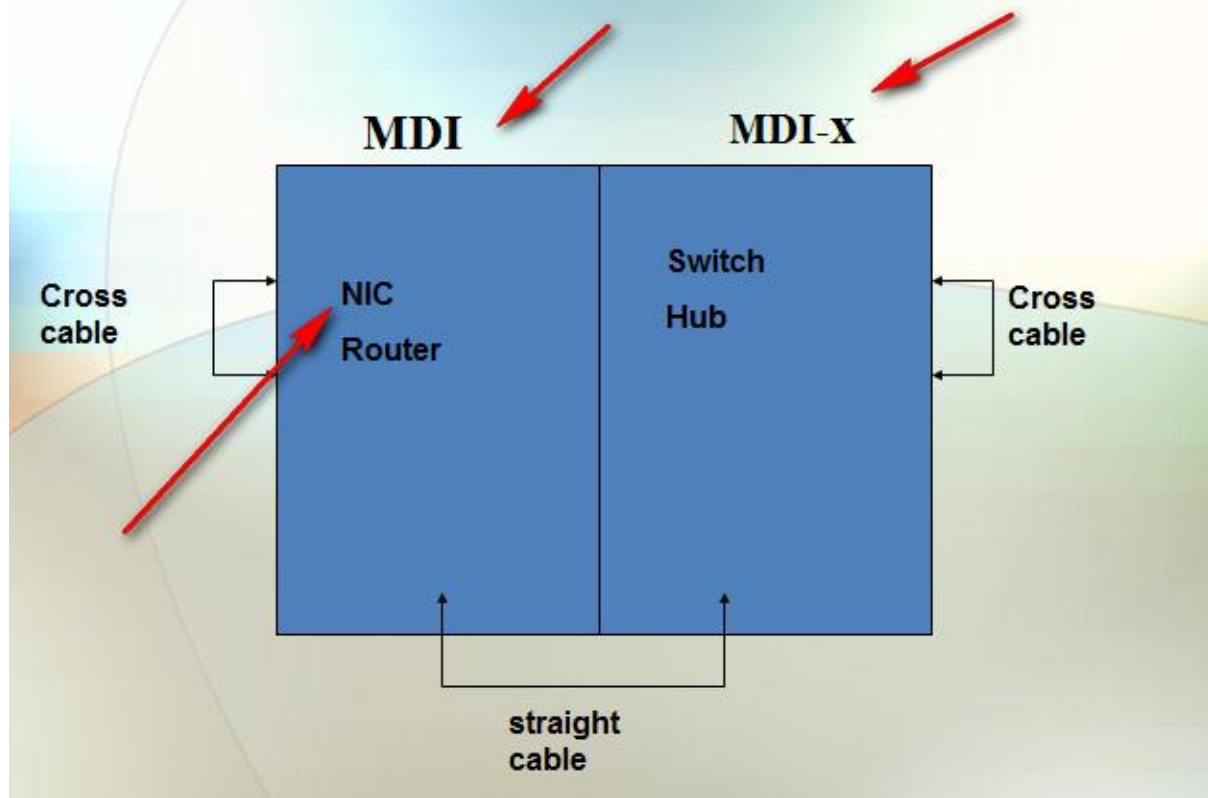
abdelsalam saleh elrashdi

2

## Crossover cable

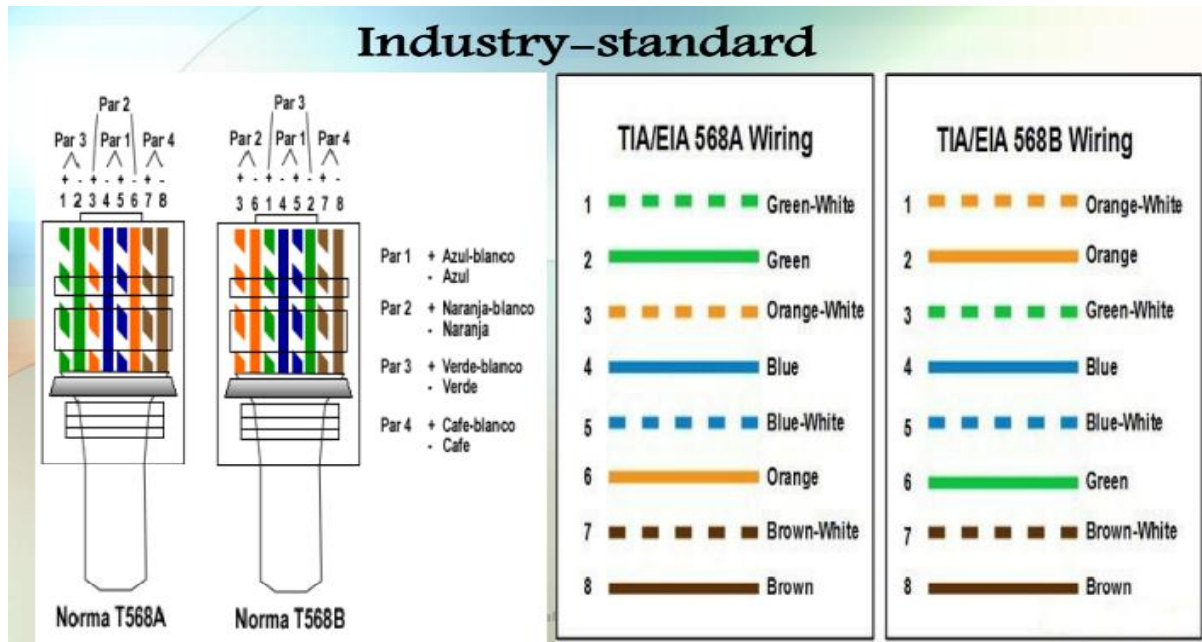
From	To
1	3
2	6
3	1
4	none
5	none
6	2
7	none
8	none

## Straight-Through or Crossover cables

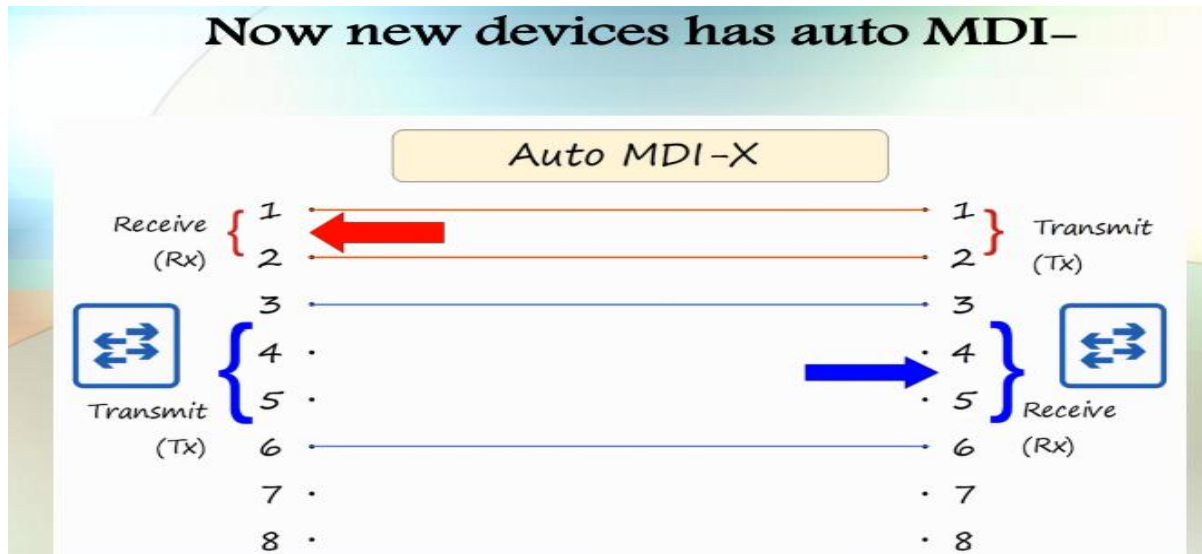


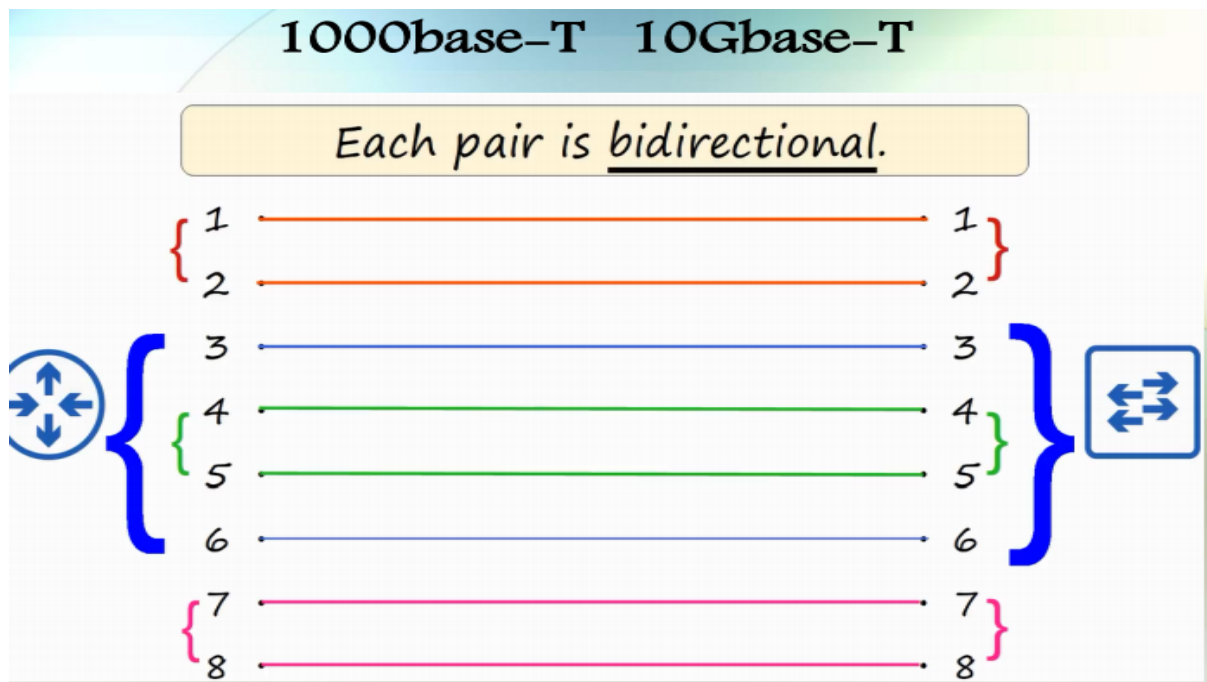
# Industry-standard

- To define industry-standard pinouts and color coding for twisted-pair cabling, the TIA/EIA-568 standard was developed.
- The first iteration of the TIA/EIA-568 standard has come to be known as the TIA/EIA-568-A standard, which was released in 1991.
- NOTE The TIA/EIA acronym comes from Telecommunications Industry Association/ Electronic Industries Alliance.
- In 2001, an updated standard was released, which became known as TIA/EIA-568-B . Interestingly, the pin out of these two standards is the same. However, the color coding of the wiring is different.



## Now new devices has auto MDI-





## Shielded Twisted-Pair

- Shielded twisted pair (STP) cable was originally designed by IBM for token ring networks that include two individual wires covered with a foil shielding, which prevents electromagnetic interference, thereby transporting data faster.
- Shielded twisted-pair cable (STP) combines the techniques of shielding, cancellation, and twisting of wires.
  - Each pair of wires is wrapped in metallic foil.
  - The four pairs of wires are wrapped in an overall metallic braid or foil.
  - STP affords greater protection from all types of external interference, but is more expensive and difficult to install than UTP.
  - The metallic shielding materials in STP need to be grounded at both ends.





## *Comparison Between UTP and STP*

- UTP VS. STP • Technology — STP is shield while UTP is unshield. The shield technique could enhance the the confidentiality of STP. Thus, STP has a higher fidelity than UTP.
- Transmission speed — UTP is faster than STP based on the same type of copper wires on data transferring.
- Applications — UTP is widely used for data transmission within short distance, and is very popular for home networking connecting. STP is mainly applicable to connections among enterprises over longer distance.
- Cost — It is universally acknowledged that UTP has a nice price. The cost of STP is much higher than UTP.



## *Common connectors used on twisted-pair cables :-*

- We have three types (RJ45,RJ11 and DB-9 (RS-232))
- RJ-45: A type 45 registered jack (RJ-45) is an eight-pin connector found in most Ethernet networks. However, most Ethernet implementations only use four of the eight pins.

### **RJ 45 Connector**



## Rj 45

- RJ45 is a type of connector commonly used for Ethernet networking. It looks similar to a telephone jack, but is slightly wider. Since Ethernet cables have an RJ45 connector on each end, Ethernet cables are sometimes also called RJ45 cables.

- The "RJ" in RJ45 stands for "registered jack," since it is a standardized networking interface. The "45" simply refers to the number of the interface standard. Each RJ45 connector has eight pins, which means an RJ45 cable contains eight separate wires. If you look closely at the end of an Ethernet cable, you can actually see the eight wires, which are each a different color. Four of them are solid colors, while the other four are striped

---

## RJ-11

- A type 11 registered jack (RJ-11) has the capacity to be a sixpin connector. However, most RJ-11 connectors have only two or four conductors. An RJ-11 connector is found in most home telephone networks. However, most home phones only use two of the six pins.

---

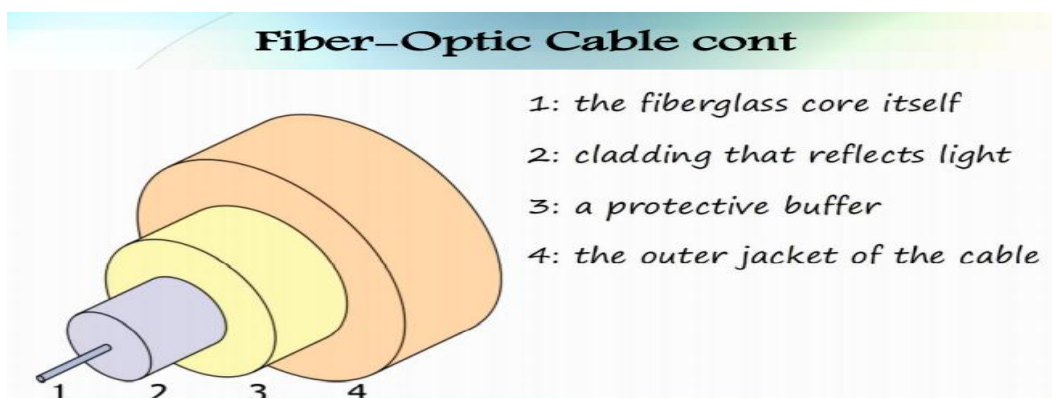
## Fiber-Optic Cable

- An alternative to copper cabling is fiber-optic cabling, which sends light (instead of electricity) through an optical fiber (typically made of glass). Using light instead of electricity makes fiber optics immune to EMI. Also, depending on the Layer 1 technology being used, fiber-optic cables typically have greater range (that is, a greater maximum distance between networked devices) and greater data-carrying capacity.

- The part of an optical fiber through which light rays travel is called the core of the fiber.

- If the diameter of the core of the fiber is large enough so that there are many paths that light can take through the fiber, the fiber is called "multimode" fiber.

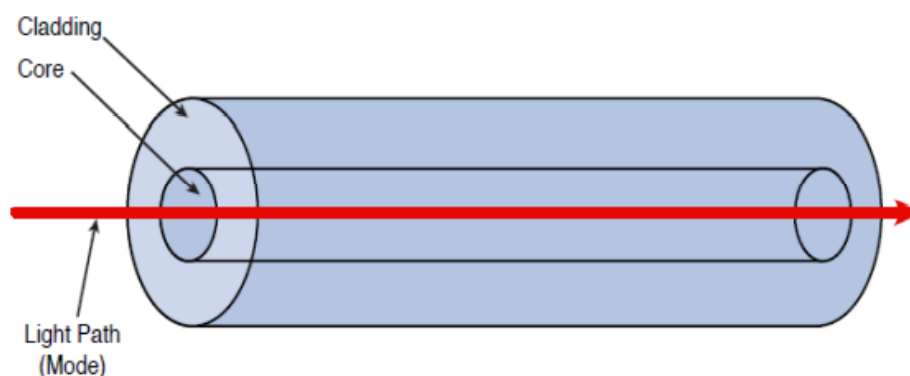
- Single-mode fiber has a much smaller core that only allows light rays to travel along one mode inside the fiber.



## ► Single-Mode Fiber

- SMF eliminates the issue of multimode delay distortion by having a core with a diameter so small that it only permits one mode (that is, one path) of propagation. With the issue of multimode delay distortion mitigated, SMF typically has longer distance limitations than MMF.
- A potential downside to SMF, however, is cost. Because SMF has to be manufactured to very exacting tolerances, you usually pay more for a given length of fiber optic
- cabling. However, for some implementations, where greater distances are required, the cost is an acceptable trade-off to reach greater distances.
- Single-mode fiber-optic cable (SMF) is a very high-speed, long-distance media that consists of a single strand— sometimes two strands—of fiber glass that carries the signals. Light emitting diodes (LEDs) and laser are the light sources used with SMF

### Single-Mode Fiber cont

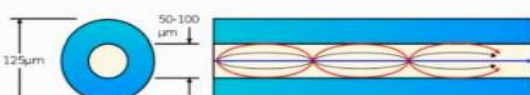
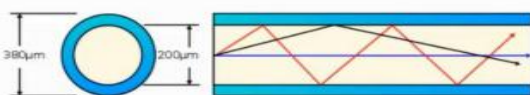


Light Propagation in Single-Mode Fiber

### Single mode fiber optical



Mrzeon ([https://commons.wikimedia.org/wiki/File:Optical\\_fiber\\_types.svg](https://commons.wikimedia.org/wiki/File:Optical_fiber_types.svg)), „Optical fiber types”, edited, <https://creativecommons.org/licenses/by-sa/3.0/legalcode>



- Core diameter is narrower than multimode fiber.
- Light enters at a single angle (mode) from a laser-based transmitter.
- Allows longer cables than both UTP and multimode fiber.
- More expensive than multimode fiber (due to more expensive laser-based SFP transmitters)



## Single-Mode Fiber cont

Singlemode Optical Fiber Cabling (operation requires 2 fibers unless otherwise specified)	
Application	OS1 and OS2 Distance (kilometers)
1000BASE-LX	5 km
10GBASE-LX4	10 km
10GBASE-E	40 km
10GBASE-L	10 km
25GBASE-LR	10 km
25GBASE-ER	40 km <sup>1</sup>
40GBASE-LR4	10 km
40GBASE-ER4 <sup>1</sup>	40 km <sup>1</sup>
50GBASE-FR	2 km
50GBASE-LR	10 km
100GBASE-DR	0.5 km
100GBASE-LR4	10 km
100GBASE-ER4 <sup>1</sup>	40 km <sup>1</sup>
200GBASE-DR4 <sup>2</sup>	0.5 km
200GBASE-FR4	2 km
200GBASE-LR4	10 km
400GBASE-DR4 <sup>2</sup>	0.5 km
400GBASE-FR8	2 km
400GBASE-LR8	10 km

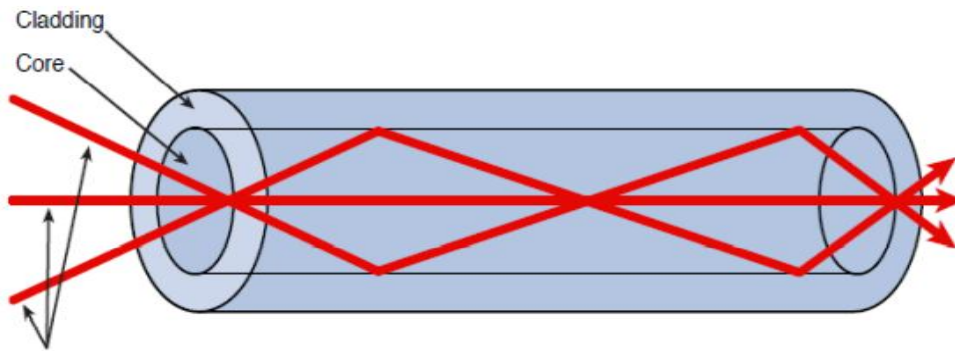
<sup>1</sup> Links longer than 30 km (98,400 ft) are considered engineered links. Consult IEEE Std 802.3-2018 for additional information.

<sup>2</sup> 8 fibers required for transmission

### ► *Multimode Fiber*

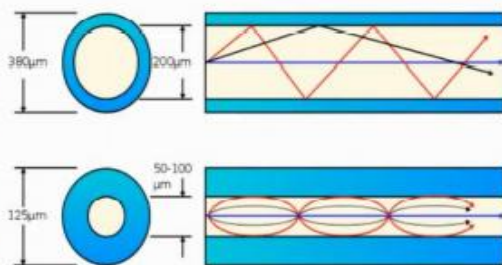
- When a light source, such as a laser, sends light pulses into a fiber-optic cable, what keeps the light from simply passing through the glass and being dispersed into the surrounding air? The trick is that fiber-optic cables use two different types of glass. • There is an inner strand of glass (that is, a core ) surrounded by an outer cladding of glass, similar to the construction of the previously mentioned coaxial cable.
  - The light injected by a laser (or LED) enters the core, and the light is prevented from leaving that inner strand and going into the outer cladding of glass. Specifically,
    - the indices of refraction of these two different types of glass are so different that if the light attempts to leave the inner strand, it hits the outer cladding and
    - bends back on itself.
  - Multimode fiber-optic cable (MMF) also uses light to communicate a signal; but with it, the light is dispersed on numerous paths as it travels through the core and is reflected back. A special material called cladding is used to line the core and focus the light back onto it

## Multimode Fiber cont



Light Propagation in Multimode Fiber

## Multimode fiber optical



- Core diameter is wider than single-mode fiber.
- Allows multiple angles (modes) of light waves to enter the fiberglass core.
- Allows longer cables than UTP, but shorter cables than single-mode fiber.
- Cheaper than single-mode fiber (due to cheaper LED-based SFP transmitters).

## Multimode Fiber cont

Multimode Optical Fiber Cabling (operation requires 2 fibers unless otherwise specified)					
Application	OM1	OM2	OM3	OM4	OM5
	Distance (meters)				
10/100BASE-SX	300 m	300 m	300 m	300 m	300 m
100BASE-FX	2,000 m	2,000 m	2,000 m	2,000 m	2,000 m
1000BASE-SX	275 m	550 m	1,000 m	1,100 m	1,100 m
1000BASE-LX	550 m	550 m	550 m	550 m	550 m
10GBASE-S	33 m	82 m	300 m	400 m	400 m
10GBASE-LX4	300 m	300 m	300 m	300 m	300 m
10GBASE-LRM	220 m	220 m	220 m	220 m	220 m
25GBASE-SR	-	-	70 m	100 m	100 m
40GBASE-SR4 <sup>2</sup>	-	-	100 m	150 m	150 m
50GBASE-SR	-	-	70 m	100 m	100 m
100GBASE-SR2 <sup>1</sup>	-	-	70 m	100 m	100 m
100GBASE-SR4 <sup>2</sup>	-	-	70 m	100 m	100 m
100GBASE-SR10 <sup>4</sup>	-	-	100 m	150 m	150 m
200GBASE-SR4 <sup>2</sup>	-	-	70 m	100 m	100 m
400GBASE-SR4 2 <sup>2,6</sup>	-	-	70 m	100 m	150 m
400GBASE-SR8 <sup>3,6</sup>	-	-	70 m	100 m	100 m
400GBASE-SR16 <sup>5</sup>	-	-	70 m	100 m	100 m

# Multi-mode fiber optic cable standards

Minimum reach of Ethernet variants over multi-mode fiber

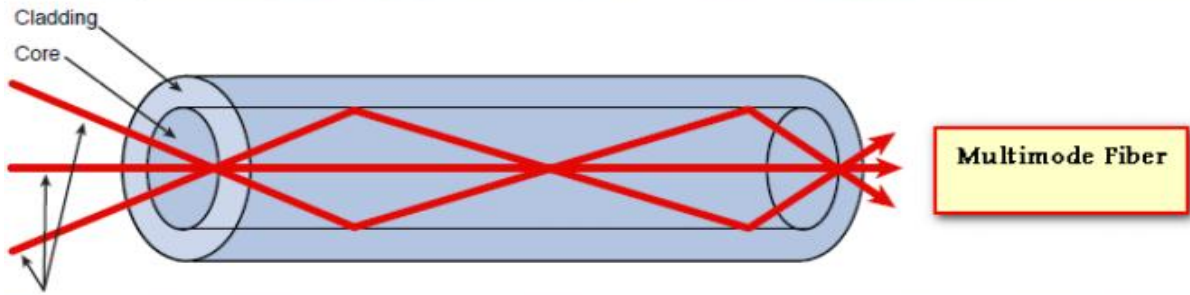
Category	Minimum modal bandwidth 850 / 953 / 1300 nm <sup>(8)</sup>	Fast Ethernet 100BASE-FX	1 Gb (1000 Mb) Ethernet 1000BASE-SX	1 Gb (1000 Mb) Ethernet 1000BASE-LX	10 Gb Ethernet 10GBASE-SR	10 Gb Ethernet 10GBASE-LRM (requires EDC)	25 Gb Ethernet 25GBASE-SR	40 Gb Ethernet 40GBASE-SWDM4	40 Gb Ethernet 40GBASE-SR4	100 Gb Ethernet 100GBASE-SR10
FDDI (62.5/125)	160 / - / 500 MHz km	2000 m <sup>(10)</sup>	220 m <sup>(11)</sup>	550 m <sup>(12)</sup> (mode-conditioning patch cord required) <sup>(13)(14)</sup>	26 m <sup>(15)</sup>	220 m <sup>(16)</sup>	Not Supported	Not Supported	Not supported	Not supported
OM1 (62.5/125)	200 / - / 500 MHz km		275 m <sup>(11)</sup>		33 m <sup>(10)</sup>	220 m	Not Supported	Not supported	Not supported	Not supported
OM2 (50/125)	500 / - / 500 MHz km		82 m <sup>(2)</sup>		220 m	Not Supported	Not Supported	Not supported	Not supported	
OM3 (50/125) *Laser Optimized*	1500 / - / 500 MHz km		550 m <sup>(2)</sup>	550 m (no mode-conditioning patch cord should be used) <sup>(17)</sup>	300 m <sup>(10)</sup>	220 m	70 m	240m <sup>(18)</sup> Duplex LC	100 m <sup>(2)</sup> (330 m QSFP+ eSR4 <sup>(19)</sup> )	100 m <sup>(2)</sup>
OM4 (50/125) *Laser Optimized*	3500 / - / 500 MHz km		>220 m		100 m	350m <sup>(18)</sup> Duplex LC	150 m <sup>(2)</sup> (550 m QSFP+ eSR4 <sup>(19)</sup> )	150 m <sup>(2)</sup>		
OM5 (50/125) *Wideband multi-mode* for short-wave WDM <sup>(21)</sup>	3500 / 1850 / 500 MHz km		>220 m		100 m	400 m <sup>(20)</sup>	>220 m	100 m	350m <sup>(18)</sup> Duplex LC	150 m <sup>(2)</sup>

## Fiber –optical cable standards

Informal Name	IEEE Standard	Speed	Cable Type	Maximum Length
1000BASE-LX	802.3z	1 Gbps	Multimode or Single-Mode	550 m (MM) 5 km (SM)
10GBASE-SR	802.3ae	10 Gbps	Multimode	400 m
10GBASE-LR	802.3ae	10 Gbps	Single-Mode	10 km
10GBASE-ER	802.3ae	10 Gbps	Single-Mode	30 km

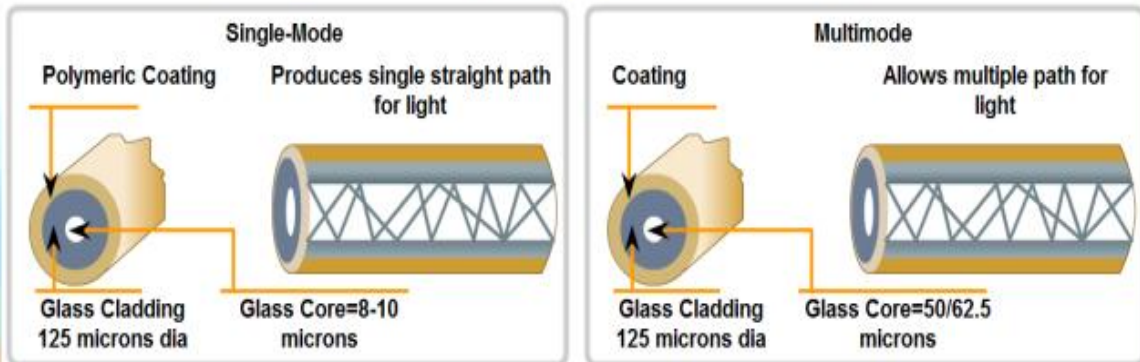


# Single and multi mode



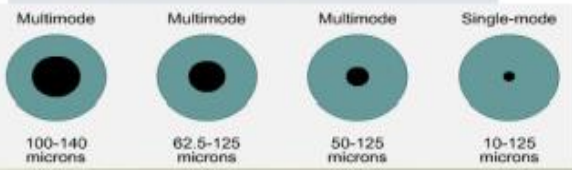
# Single and multi mode

## Fiber Media Modes



- Small Core
- Less Dispersion
- Suited for long distance applications (up to 100 km, 62,14 mi.)
- Uses lasers as the light source often within campus backbones for distance of several thousand meters

- Larger core than single-mode cable (50 microns or greater)
- Allows greater dispersion and therefore, loss of signal
- Used for long distance application, but shorter than single-mode (up to ~2km, 6560 ft)
- Uses LEDs as the light source often within LANs or distances of couple hundred meters within a campus network



## • *Pros and cons Fiber Optic*

- Pros • Fiber can transfer lots of data quickly with very little latency (delays in data processing), making it the fastest internet available. The data flows over long distances without degrading like it does with cable, so the information gets from one place to another quickly and intact. Even better, fiber optic internet does not have bandwidth caps, so you can theoretically use as much as you need.
  - In addition, fiber optic internet has the scalability, stability, and security that a business needs. Fiber optic wavelengths can be turned on and off on demand, and extra fiber infrastructure can be placed to accommodate growth, which means a growing business can easily customize and scale their services if needed
- 
- Fiber also is more reliable in that it is more resistant to electromagnetic, corrosive, and lightning-related damage, and it is less likely to go down during a power outage; thus, it tends to be a more stable option.
  - Furthermore, this form of internet service is also harder to hack, and it does not radiate signals the way cable internet does. Breaches are easier to identify as soon as they occur as well, meaning that your data is more secure with fiber internet vs. cable. Plus, the fire hazard associated with traditional copper wiring is also absent with fiber, as it does not use electricity.

## ▶ *Cons*

- While there are significant advantages to fiber, it is far from a perfect replacement for traditional technology. While fiber is thinner and lighter than copper cable, it is also more delicate, making it more susceptible to physical damage from construction mishaps, wildlife, radiation, or chemicals. It is also sensitive to bending, so maneuvering and laying fiber cabling is a challenge. Fiber optic threads are also potentially harmed by what is known as “fiber fuse.” This occurs when there is an imperfection in the fiber and, when too much light meets the anomaly, it causes permanent damage to the fiber.
- Another major drawback to fiber internet vs. cable is the high short-term costs. Fiber optic internet requires a whole new infrastructure to be implemented for use, which is very expensive. It requires trained specialists and special equipment to install. Repairs are also very costly if the fiber is damaged.
- An additional issue with fiber is its limited availability. As it is a relatively

new technology, fiber optic internet is not yet as widely available as cable or DSL.

## *Pros and cons Fiber Optic*

pros:-

- Can transmit up to long kilometers
- High speed cons:-
- Is difficult to install
- Is more expensive than twisted-pair
  - Troubleshooting equipment is more expensive than twisted-pair test equipment
- Is harder to troubleshoot

## **Comparison table UTP and fiber optic**

### *UTP*

- Lower cost than fiber-optic.
- Shorter maximum distance than fiber-optic (~100m).
- Can be vulnerable to EMI (Electromagnetic Interference).
- RJ45 ports used with UTP are cheaper than SFP ports.
- Emit (leak) a faint signal outside of the cable, which can be copied (=security risk)

### *Fiber-Optic*

- Higher cost than UTP.
- Longer maximum distance than UTP.
- No vulnerability to EMI.
- SFP ports are more expensive than RJ45 ports (single-mode is more expensive than multimode).
- Does not emit any signal outside of the cable (=no security risk).

## Comparison table UTP and fiber optic cont

Comparisons Between UTP, MM, and SM Ethernet Cabling

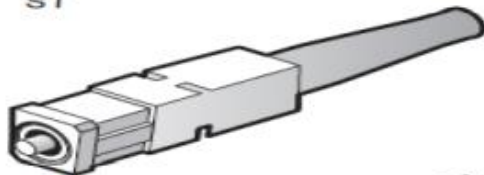
Criteria	UTP	Multimode	Single-Mode
Relative Cost of Cabling	Low	Medium	Medium
Relative Cost of a Switch Port	Low	Medium	High
Approximate Max Distance	100m	500m	40km
Relative Susceptibility to Interference	Some	None	None
Relative Risk of Copying from Cable Emissions	Some	None	None

## Common connectors used on fiber-optic cables



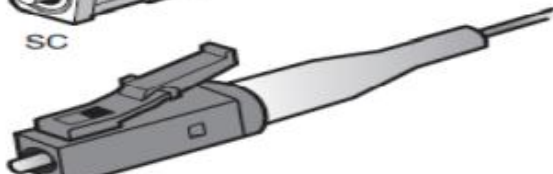
ST

The ST connector uses a half-twist bayonet type of lock.



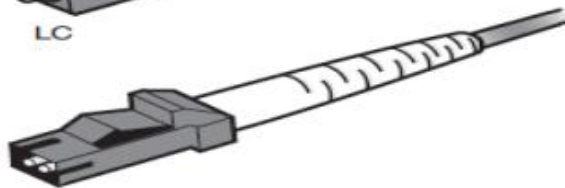
SC

The SC uses a push-pull connector similar to common audio and video plugs and sockets.



LC

LC connectors have a flange on top, similar to an RJ-45 connector, that aids secure connection.



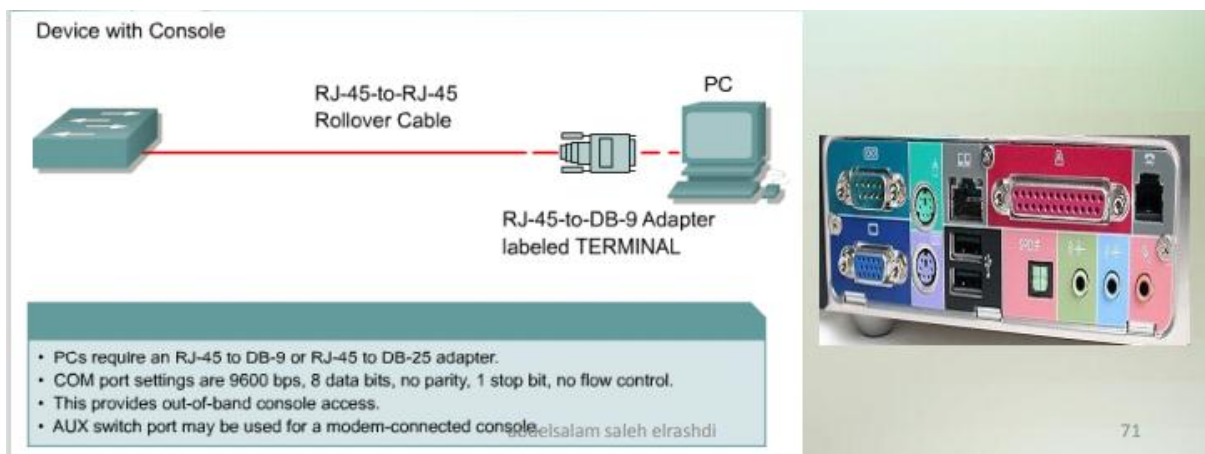
MT-RJ

MT-RJ is a popular connector for two fibers in a very small form factor.

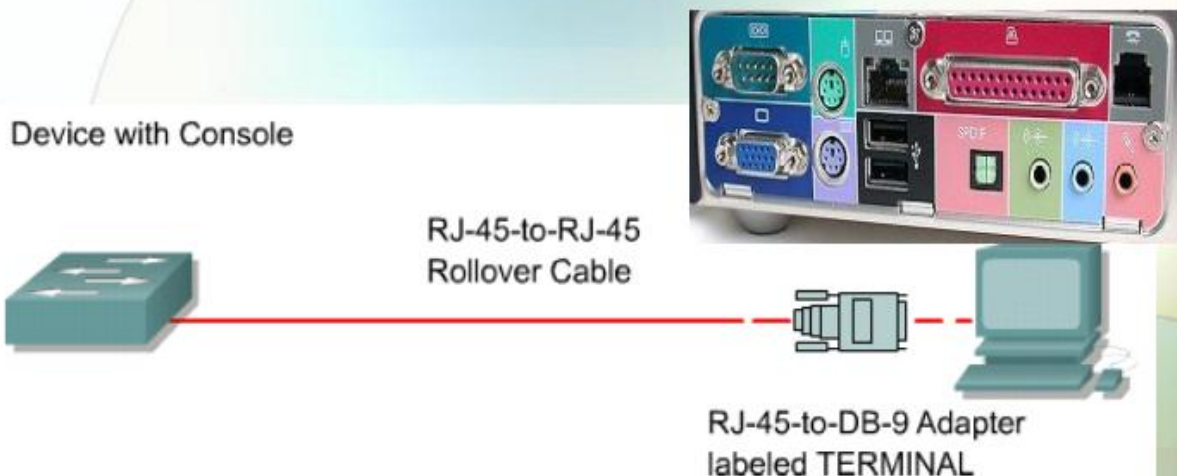


# Console (Rollover) cable

- a rolled Ethernet cable to connect a host to a router console serial communication (com) port.
- If you have a Cisco router or switch, you would use this cable to connect your PC running HyperTerminal to the Cisco hardware.
- Eight wires are used in this cable to connect serial devices, although not all eight are used to send information, just as in



# Console (Rollover) cable



- PCs require an RJ-45 to DB-9 or RJ-45 to DB-25 adapter.
- COM port settings are 9600 bps, 8 data bits, no parity, 1 stop bit, no flow control.
- This provides out-of-band console access.
- AUX switch port may be used for a modem-connected console.

## *DB-9 (RS-232)*

- A 9-pin D-subminiature (DB-9) connector is commonly used as a connector for asynchronous serial communications. One of the more popular uses of a DB-9 connector is to connect the serial port on a computer with an external modem.



DB-9 (RS-232)





# Chapter 4 ☺ ✍️

---

*Ip address version 4*

**ABDELSALAM SALEH ELRASHDI**

**Networking fundamentals**



## Chapter 4 ☺✍

### Outlines

- Introduction to IPv4 address
- Purpose of IPv4
- IP Address Classes
- Reserved Ip V4 Address
- Public and Private Addresses
- Network address translation (NAT)



---

### Objectives

- Define IP address v4
- Explain the purpose of IPV4
- List of IPV4 classes .
- Identify reserved IP address
- Distinguished between private and public IP
- Importance of network address translation (NAT).

# *IPv4*

Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks. IPv4 was the first version deployed for production in the ARPANET in 1983. It still routes most Internet traffic today,[1] despite the ongoing deployment of a successor protocol, IPv6. IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980).

---

## *IP V4 addressing*

- IP (Internet Protocol) determines where we are going to send packets to by looking at the destination IP address
  - IPv4 uses a 32-bit address space which provides 4,294,967,296 (2<sup>32</sup>) unique addresses, but large blocks are reserved for special networking methods.
  - Consist of 32bit( four octets)
    - *Octet=8bits*
    - *Octet=0-255*
    - *Octet1.Octet2.Octet3.Octet4*
    - *Example of 192.168.20.50*
    - *10.0.0.50 200.58.12.45*
    - *172.16.4.20 20.10.1.40*

---

## *Purpose of IPv4*

- The Internet Protocol is the protocol that defines and enables internetworking at the internet layer of the Internet Protocol Suite. In essence it forms the
- Internet. It uses a logical addressing system and performs routing, which is the forwarding of packets from a source host to the next router that is one hop closer to the intended destination host on another network.
- without IP address we can't access to other devices in network

## *IP Address Classes*

Bits:	1	8	9	16	17	24	25	32							
<b>Class A</b>	<b>0NNNNNNN</b>			Host		Host		Host							
	Range (1-126)														
<b>Class B</b>	1	8		9		16		17		24		25		32	
	<b>10NNNNNN</b>			Network				Host				Host			
	Range (128-191)														
<b>Class C</b>	1	8		9		16		17		24		25		32	
	<b>110NNNNN</b>			Network				Network				Host			
	Range (192-223)														
<b>Class D</b>	1	8		9		16		17		24		25		32	
	<b>1110MMMM</b>			Multicast Group				Multicast Group				Multicast Group			
	Range (224-239)														

ICND20GR\_22

### *Examples of IP Addressing :*

- 1- 200.10.200.4
- 2- 10.20.56.100
- 3- 192.168.0.20
- 4- 192.169.200.30
- 4- 172.35.20.241
- 5- 200.10.30.6
- 6- 172.30.20.200
- 7- 265.20.100.5

#### *1. Class A :*

$$\text{No of network} = 2^7 - 2 = 126$$

$$\text{No of host} = 2^{24} - 2 = 16,777,214$$



## 2. Class B :

No of network =  $2^{14}-2 = 16,382$

No of host =  $2^{16}-2 = 65,534$

---

## 3. Class C

No of network =  $2^{21}-2 = 2,097,152$

No of host =  $2^8-2 = 254$

---

## Default Subnet Masks

<b>Class A</b>	Network	Host	Host	Host
Subnet Mask	255	0	0	0

<b>Class B</b>	Network	Network	Host	Host
Subnet Mask	255	255	0	0

<b>Class C</b>	Network	Network	Network	Host
Subnet Mask	255	255	255	0

Address Class	Value in First Octet	Classful Mask (Dotted Decimal)	Classful Mask (Prefix Notation)
Class A	1–126	255.0.0.0	/8
Class B	128–191	255.255.0.0	/16
Class C	192–223	255.255.255.0	/24
Class D	224–239	—	—
Class E	240–255	—	—

## *IP Address Classes*

<i>Class</i>	<i>Range of Class</i>	<i>Network Portion</i>	<i>Host Portion</i>	<i>Number of Networks</i>	<i>Hosts per Network</i>	<i>Default Subnet Mask</i>
<i>Class A</i>	<i>1 - 126</i>	<i>8</i>	<i>24</i>	<i>128</i>	<i>16,777,214</i>	<i>255.0.0.0</i>
<i>Class B</i>	<i>128 - 191</i>	<i>16</i>	<i>16</i>	<i>16,384</i>	<i>65,534</i>	<i>255.255.0.0</i>
<i>Class C</i>	<i>192 - 223</i>	<i>24</i>	<i>8</i>	<i>2,097,152</i>	<i>254</i>	<i>255.255.255.0</i>
<i>Class D (multicast)</i>	<i>224 - 239</i>	<i>Not defined</i>	<i>Not defined</i>	<i>Not defined</i>	<i>Not defined</i>	<i>Not defined</i>
<i>Class E (reserved)</i>	<i>240 - 254</i>	<i>Not defined</i>	<i>Not defined</i>	<i>Not defined</i>	<i>Not defined</i>	<i>Not defined</i>

## *Reserved Ip V4 Address*

- ✓ Network Address
- ✓ Broadcast Address
- ✓ Default Route (0.0.0.0)
- ✓ Loopback (127.0.0.1)
- ✓ Link-Local Addresses “Automatic Private IP Addressing (APIPA)” (169.254.x.x)
- ✓ Reserved Ip V4 Address

---

### *Public IP address*

- Public IP address of a system is the IP address which is used to communicate outside the network. Public IP address is basically assigned by the ISP (Internet Service Provider).

• It is public global addresses that are used in the Internet. A public IP address is an IP address that is used to access the Internet. Public (global) IP addresses are routed on the Internet, unlike private addresses.

---

## *Private IP address*

• Private IP address of a system is the IP address which is used to communicate within the same network. Using private IP data or information can be sent or received within the same network. • Private internal addresses are not routed on the Internet and no traffic cannot be sent to them from the Internet, they only supposed to work within the local network. • Private addresses include IP addresses from the following subnets:

---

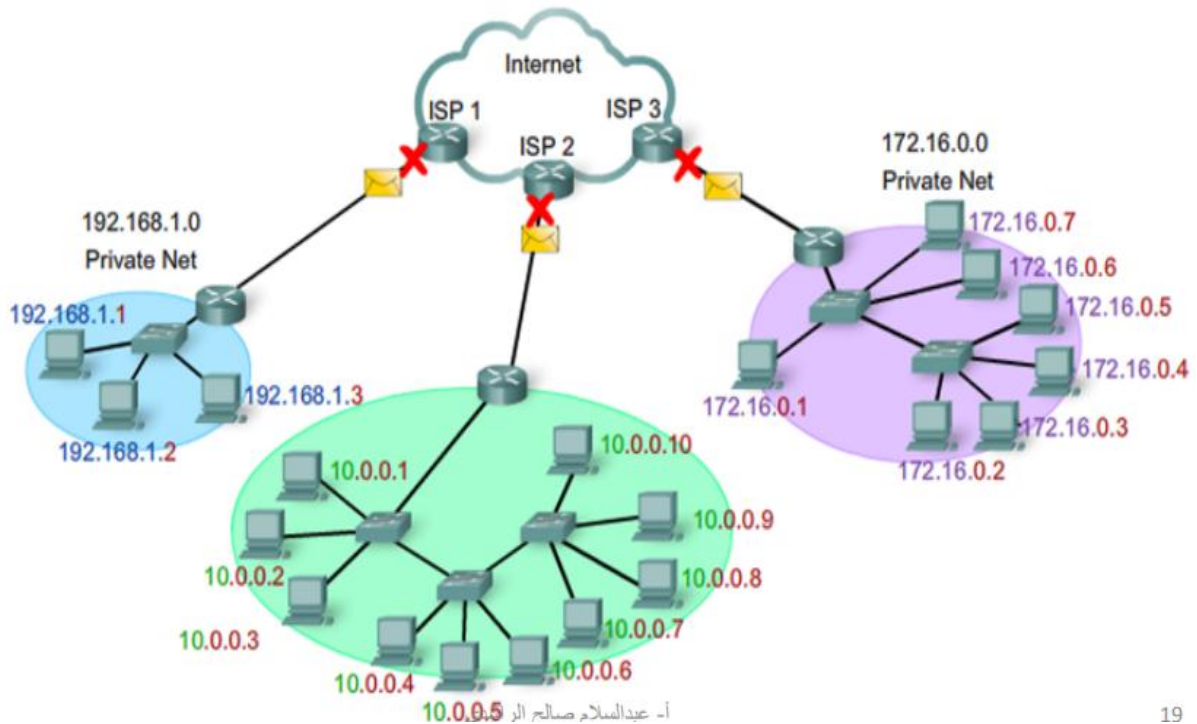
## *Private Addressing*

Address Class	Reserved Address Space
Class A	10.0.0.1 through 10.255.255.254
Class B	172.16.0.1 through 172.31.255.254
Class C	192.168.0.1 through 192.168.255.254

## *Examples of IP Addressing :*

- 1- 200.10.200.4
- 2- 10.20.56.100
- 3- 192.168.0.20
- 4- 192.169.200.30
- 5- 172.35.20.241
- 6- 200.10.30.6
- 7- 172.30.20.200
- 8- 265.20.100.50

# Private Addressing



19

## Private V public IP address

PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
Scope is local.	Scope is global.
It is used to communicate within the network.	It is used to communicate outside the network.
Private IP addresses of the systems connected in a network differ in a uniform manner.	Public IP may differ in uniform or non-uniform manner.
It works only in LAN.	It is used to get internet service.
It is used to load network operating system.	It is controlled by ISP.
It is available in free of cost.	It is not free of cost.
Private IP can be known by entering "ipconfig" on command prompt.	Public IP can be known by searching "what is my ip" on google.
Range: 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0 - 192.168.255.255	Range: Besides private IP addresses, rest are public.

## *Network address translation (NAT)*

- NAT has many uses, but its key use is to save IP addresses by allowing networks to use private IP addresses there are three types of NAT :-
  - ✓ Static NAT (from one to one )uses a one-to-one mapping of local and global addresses, and these mappings remain constant.
  - ✓ Dynamic NAT (from one to multi) uses a pool of public addresses and assigns them on a first-come, first-served basis
  - ✓ PAT NAT overloading (sometimes called Port Address Translation) (from one to all) maps multiple private IP addresses to a single public IP address or a few addresses.

---

### *NAT*

#### *• Static NAT*

- 192.168.1.20 ----11.20.30.23
- 10.0.0.5 -----20.14.25.30
- 172.16.0.20 ----200.50.10.20

---

#### *Dynamic NAT*

- 10.0.0.5 ----205.10.20.3
- 10.0.0.6 ----205.10.20.3
- 10.0.0.7 ----205.10.20.3
- 10.0.0.8-----200.0.0.20
- 10.0.0.9-----200.0.0.20
- 10.0.0.10-----200.0.0.20

---

### *PAT*

- 10.0.0.5 ----205.10.20.3
- 10.0.0.6 ----205.10.20.3
- 10.0.0.7 ----205.10.20.3

# *The subnetting*

---

## *What is sub netting?*

- Sub netting is to get many network IPs from one network IP by changing in the network portion and the host portion in the original network IP.
  - The following examples illustrates how we can make subnetting for a certain IP address.
- 

## *Example :-*

- Ex:192.168.1.65
  - I want 30 computers
- 1- Network ID
  - 2- first valid ip address
  - 3- last valid ip address
  - 4- Broadcast ip address
  - 5-CIDR
- 

## *Classless Inter-Domain Routing (CIDR)*

Used to allocate an amount of IP address space to a given entity (company, home, customer, etc).

Example: 192.168.10.32/28

The slash notation (/) means how many bits are turned on (1s) and tells you what your subnet mask is.

<http://www.subnet-calculator.com/>

---



# CIDR Values

Subnet Mask	CIDR Value	Subnet Mask	CIDR Value
255.0.0.0	/8	255.255.240.0	/20
255.128.0.0	/9	255.255.248.0	/21
255.192.0.0	/10	255.255.252.0	/22
255.224.0.0	/11	255.255.254.0	/23
255.240.0.0	/12	255.255.255.0	/24
255.248.0.0	/13	255.255.255.128	/25
255.252.0.0	/14	255.255.255.192	/26
255.254.0.0	/15	255.255.255.224	/27
255.255.0.0	/16	255.255.255.240	/28
255.255.128.0	/17	255.255.255.248	/29
255.255.192.0	/18	255.255.255.252	/30
255.255.224.0	/19		

## Ex:192.168.1.65

- No of host 30 then  $2^n - 2 \leq 30$
  - N is number of 0 = 5 = 32
- 11111111.11111111.11111111.11100000
- 255 255 255 224
  - How 11100000 = 224 by
  - 128 64 32 16 8 4 3 2 1
  - 1 1 1 0 0 0 0 0 128+64+32 = 224
  - Now I will find fix addition between each network 256 - 224 = 32 then
  - First network is
  - 1 192.168.1.0
  - 2 192.168.1.32
  - 3 192.168.1.64
  - 4 192.168.1.96
- 1- so Network ID 192.168.1.64  
 2- first valid ip address 192.168.1.65

- 3- last valid ip address 192.168.1.94
  - 4- Broadcast ip address 192.168.1.95
  - 5-CIDR is number of ones 27 28
- 

### **Ex 172.16.101.100**

- No of host 500 then  $2^n - 2 \leq 500$
  - N is number of 0 = 9 = 32
  - 11111111.11111111.11111110.00000000
  - 255 255 254 0
  - How 11100000 = 254 by
  - 128 64 32 16 8 4 3 2 1
  - 1 1 1 1 1 1 1 0 128+64+32+16+8+4+2 = 254
  - Now I will find fix addition between each network 256 -254=2 then
  - First network is
  - 1 172.16.0.0
  - 2 172.16.2.0
  - 3 172.16.4.0
  - N 172.16.100.0
  - N 172.16.102.0
  - 1- so Network ID 172.16.100.0
  - 2- first valid ip address 172.16.100.1
  - 3- last valid ip address 172.16.101.254
  - 4- Broadcast ip address 172.16.101.255
  - 5-CIDR is number of ones 23
- 

### **Ex 10.50.50.50**

- 10.75.50.50 /10
- 11111111.11000000.00000000.00000000
- 255 192 0 0
- How 11000000 = 192by
- 128 64 32 16 8 4 3 2 1
- 1 1 0 0 0 0 0 0 128+64+0+0+0+0+0 = 192
- Now I will find fix addition between each network 256 -192=64then
- First network is
- 1 10.0.0.0
- 2 10.64.0.0
- 3 10.128.0.0

- 4 172.16.192.0
  - N .....
- 1- so Network ID 10.64.0.0
  - 2- first valid ip address 10.64.0.1
  - 3- last valid ip address 10.127.255.254
  - 4- Broadcast ip address 10.127.255.255
  - 5- CIDR is number of ones 10 30
- 

## *Subnetting Class Addresses*

In a Class C address, only 8 bits are available for defining the hosts. Remember that subnet bits start at the left and go to the right, without skipping bits. This means that the only Class C subnet masks can be the following:

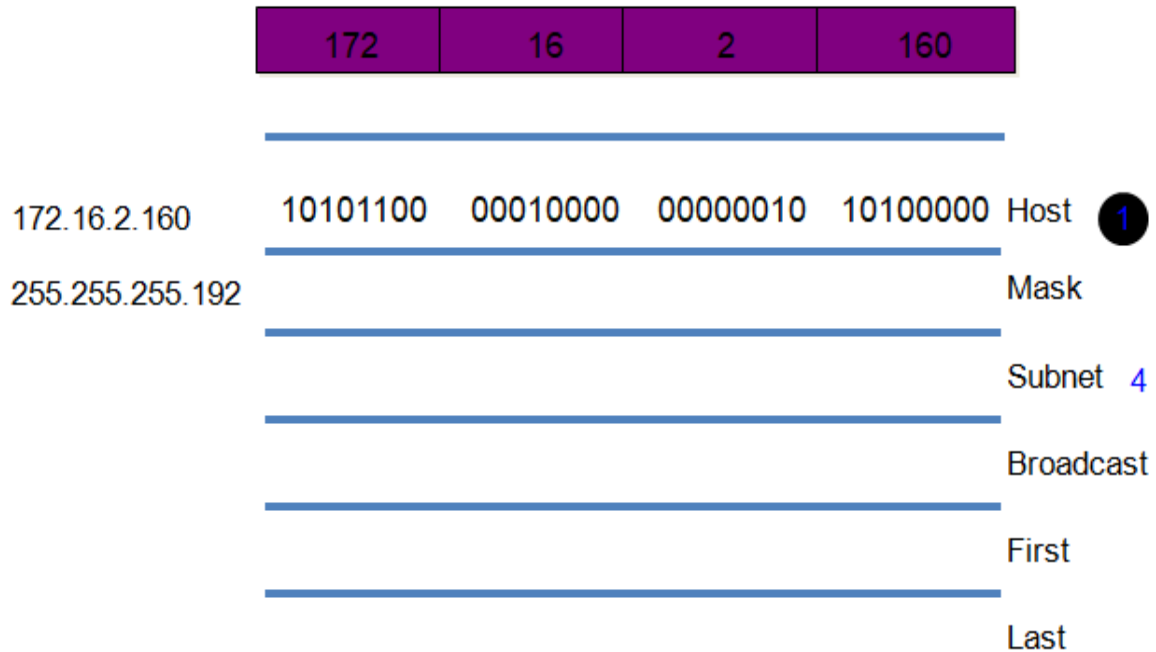
Binary    Decimal    CIDR

---

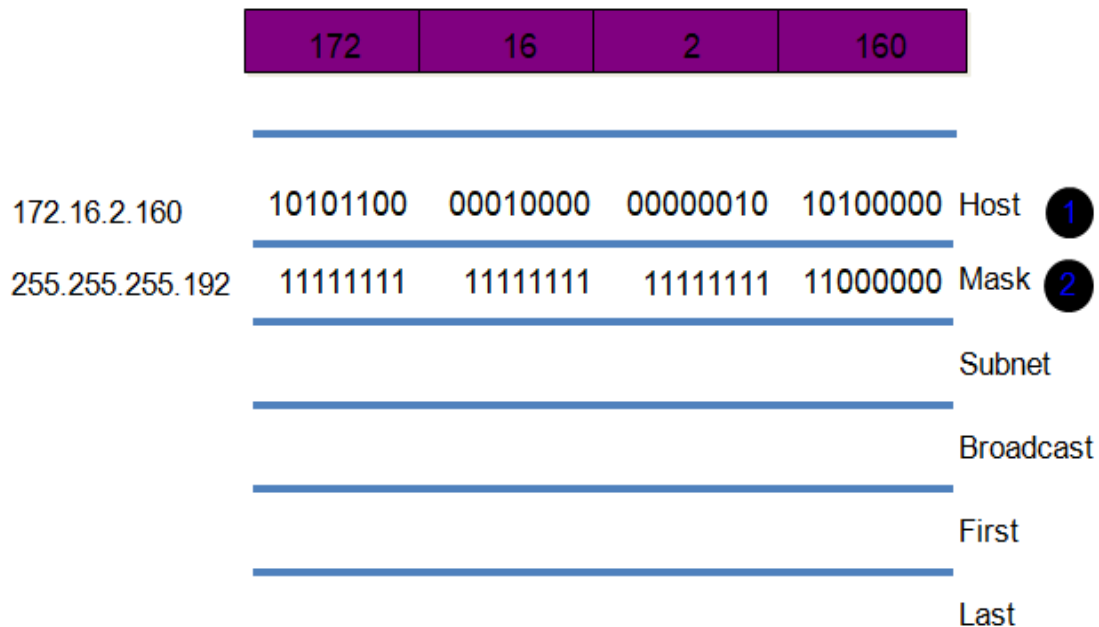
Binary	Decimal	CIDR
10000000	= 128	/25
11000000	= 192	/26
11100000	= 224	/27
11110000	= 240	/28
11111000	= 248	/29
11111100	= 252	/30



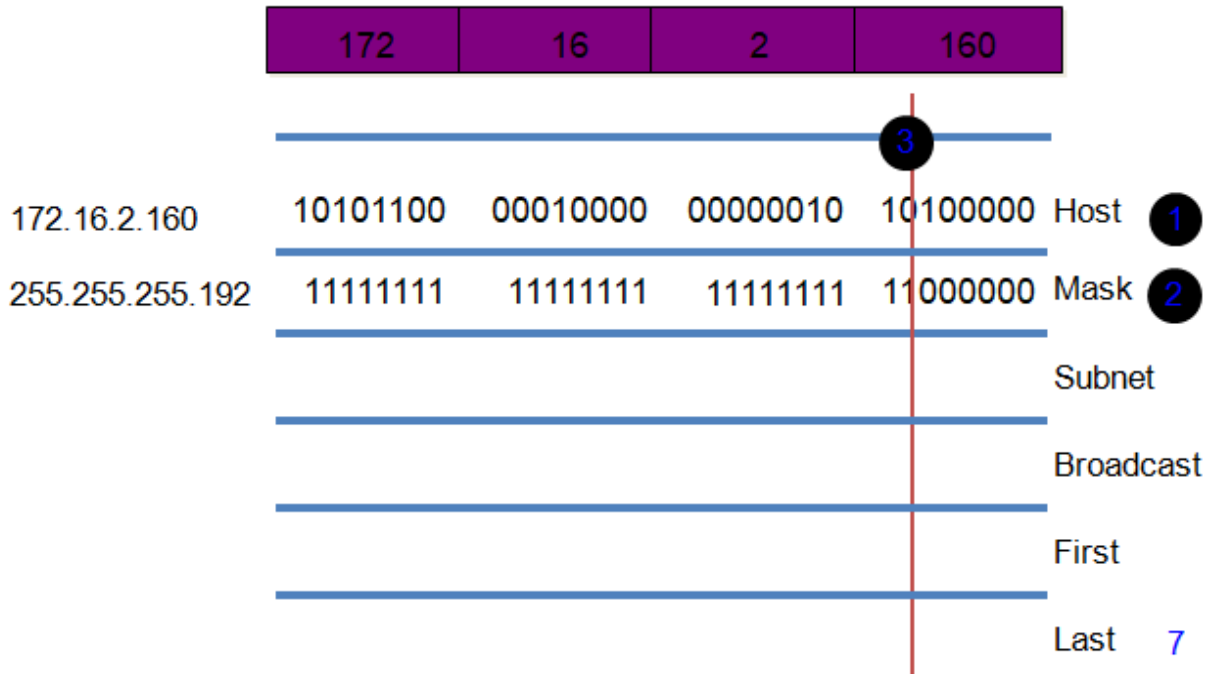
# Addressing Summary Example



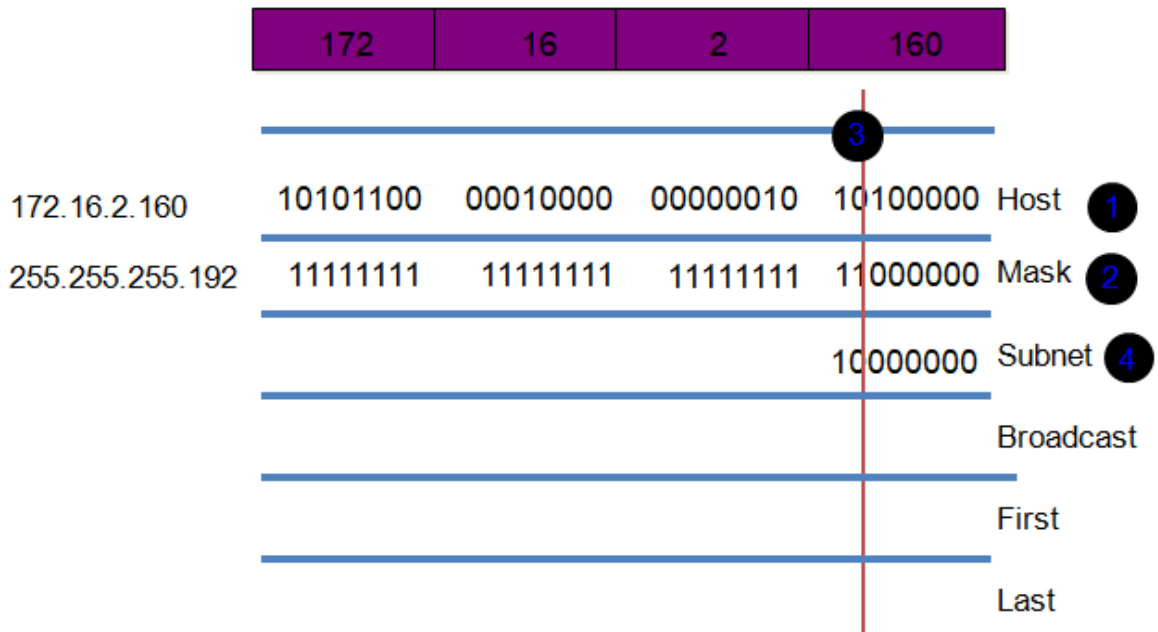
# Addressing Summary Example



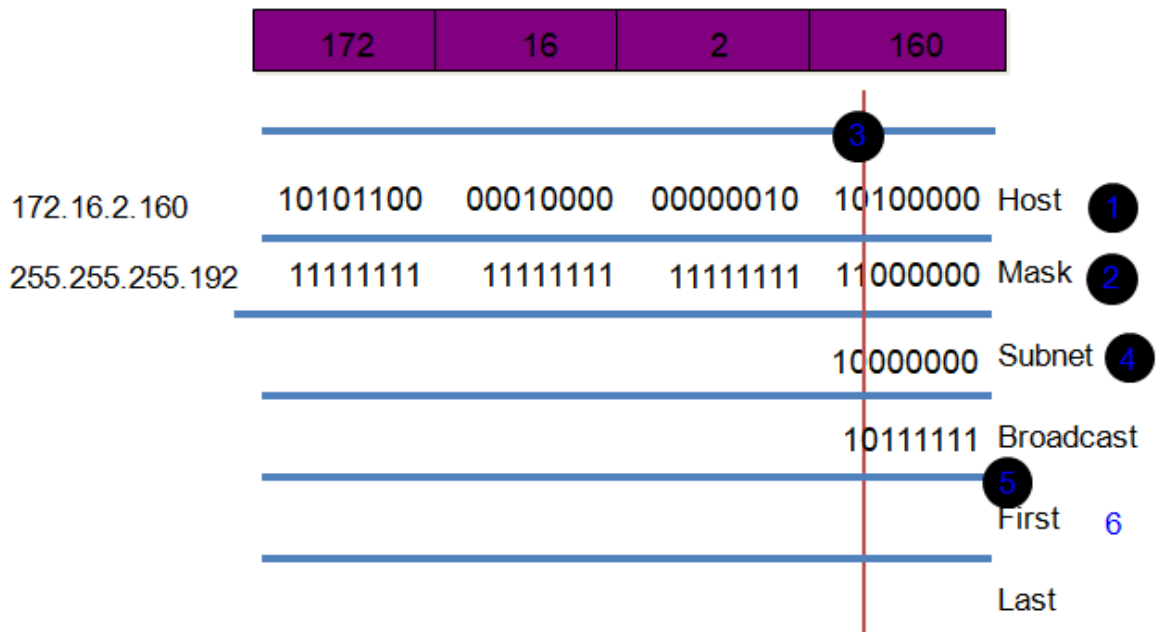
# Addressing Summary Example



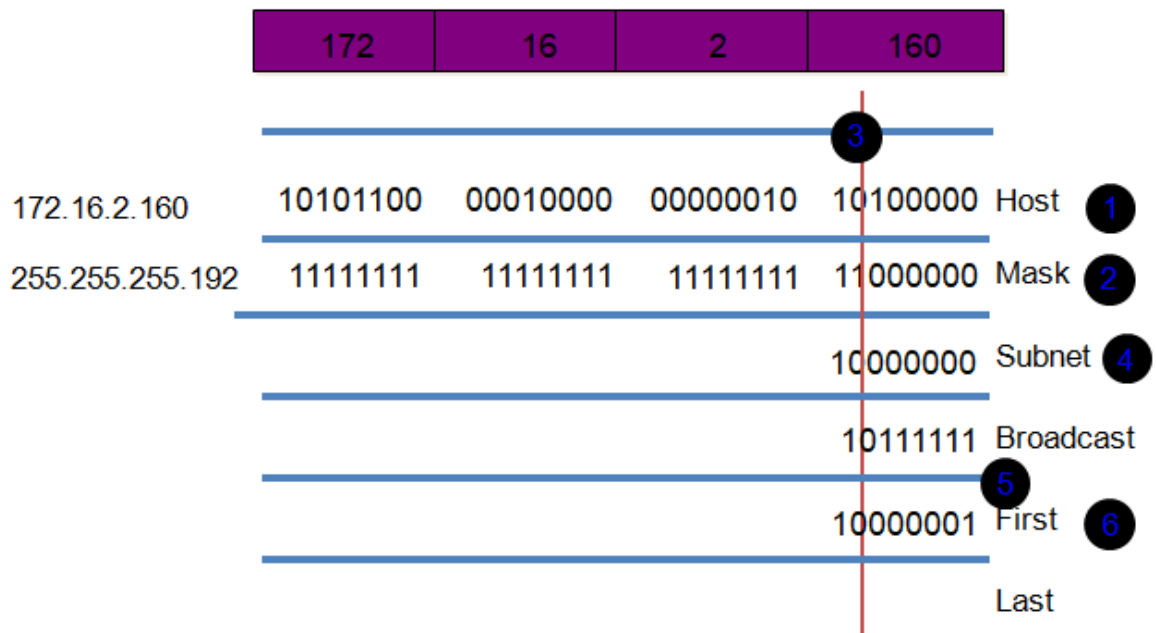
# Addressing Summary Example



# Addressing Summary Example

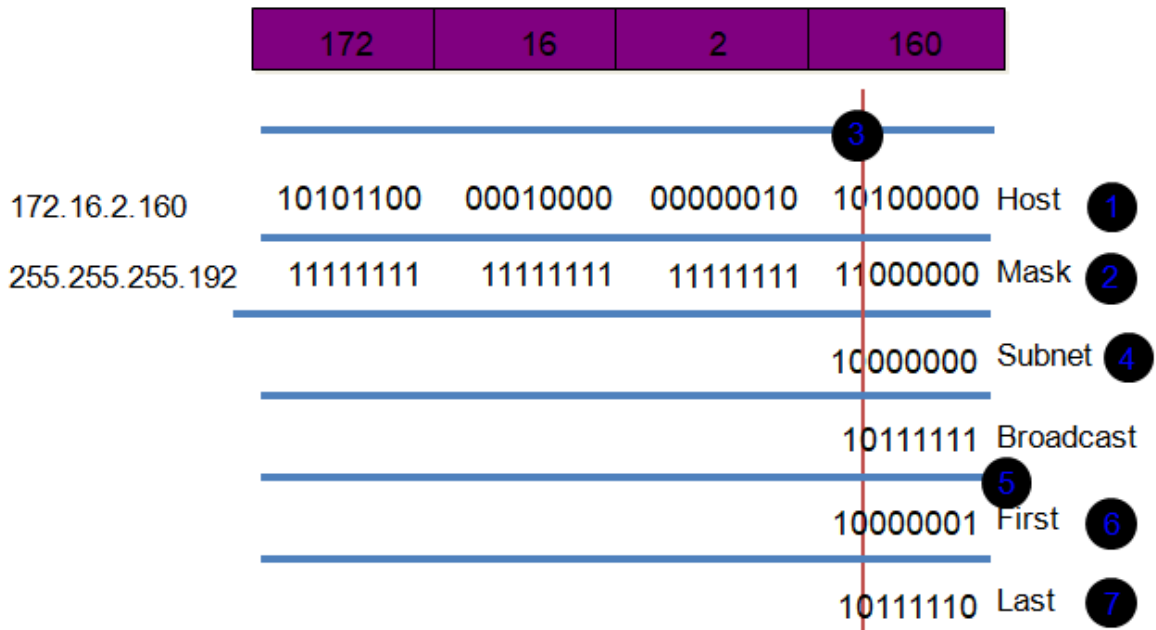


# Addressing Summary Example

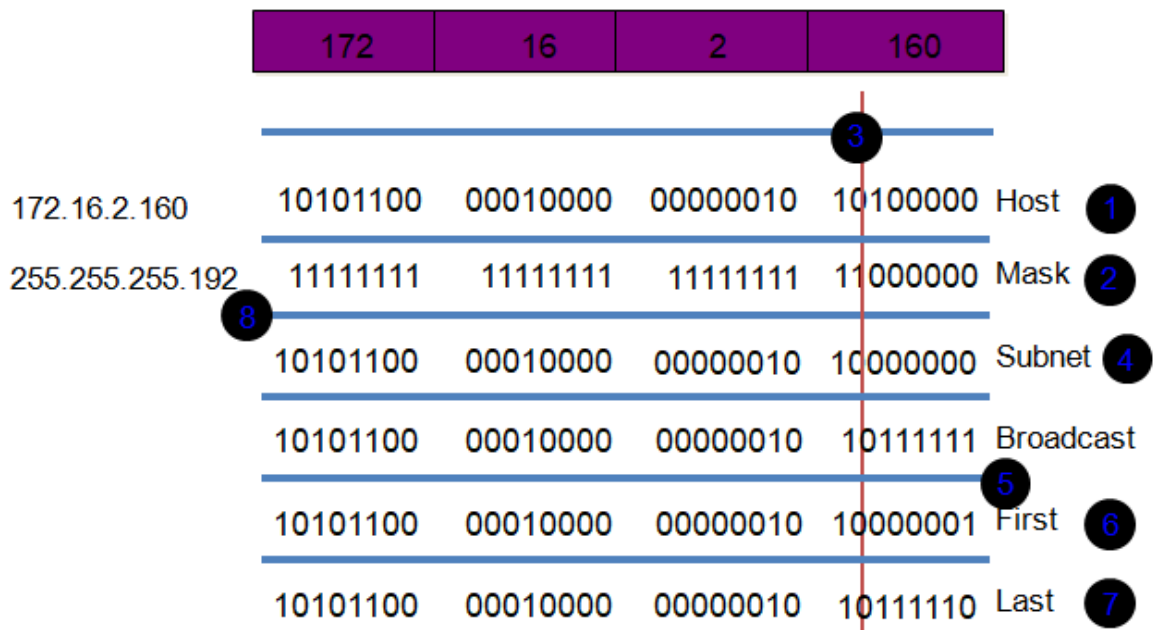




# Addressing Summary Example



# Addressing Summary Example



# Addressing Summary Example

	172	16	2	160	
172.16.2.160	10101100	00010000	00000010	10100000	Host 1
255.255.255.192	11111111	11111111	11111111	11000000	Mask 2
172.16.2.128	10101100	00010000	00000010	10000000	Subnet 4
172.16.2.191	10101100	00010000	00000010	10111111	Broadcast 5
172.16.2.129	10101100	00010000	00000010	10000001	First 6
172.16.2.190	10101100	00010000	00000010	10111110	Last 7



# Chapter 5 ☺✍

---

## *Open system interconnection model (OSI)*

ABDELSALAM SALEH ELRASHDI

Networking fundamentals



## Chapter 5 ☺✍

### Outlines

- OSI model
- International Organization for Standardization
- Purpose OSI model
- Application layer
- Presentation layer
- Session layer
- Transport layer
- Network layer
- Data link layer
- Physical layer
- Windowing and flow control
- Protocol data unit



---

### Objectives

*By end of this lecture the student will be able :*

- Define the open system interconnection model (OSI model ).
- Describe the purpose of OSI model.
- Explain the functions of the three upper layers of the OSI model.
- List and describe the protocols at each layer.
- Explain the functions of the transport layer.
- Explain the functions of the network layer.
- Describe the flow control process.
- Explain how network layer protocols and services support communications across data networks
- Explain the functions of data link and physical layer.
- Identified the components of the data link layer.
- Identified and purpose of each sub layer .
- Describe the purpose and characteristics of the Ethernet MAC address

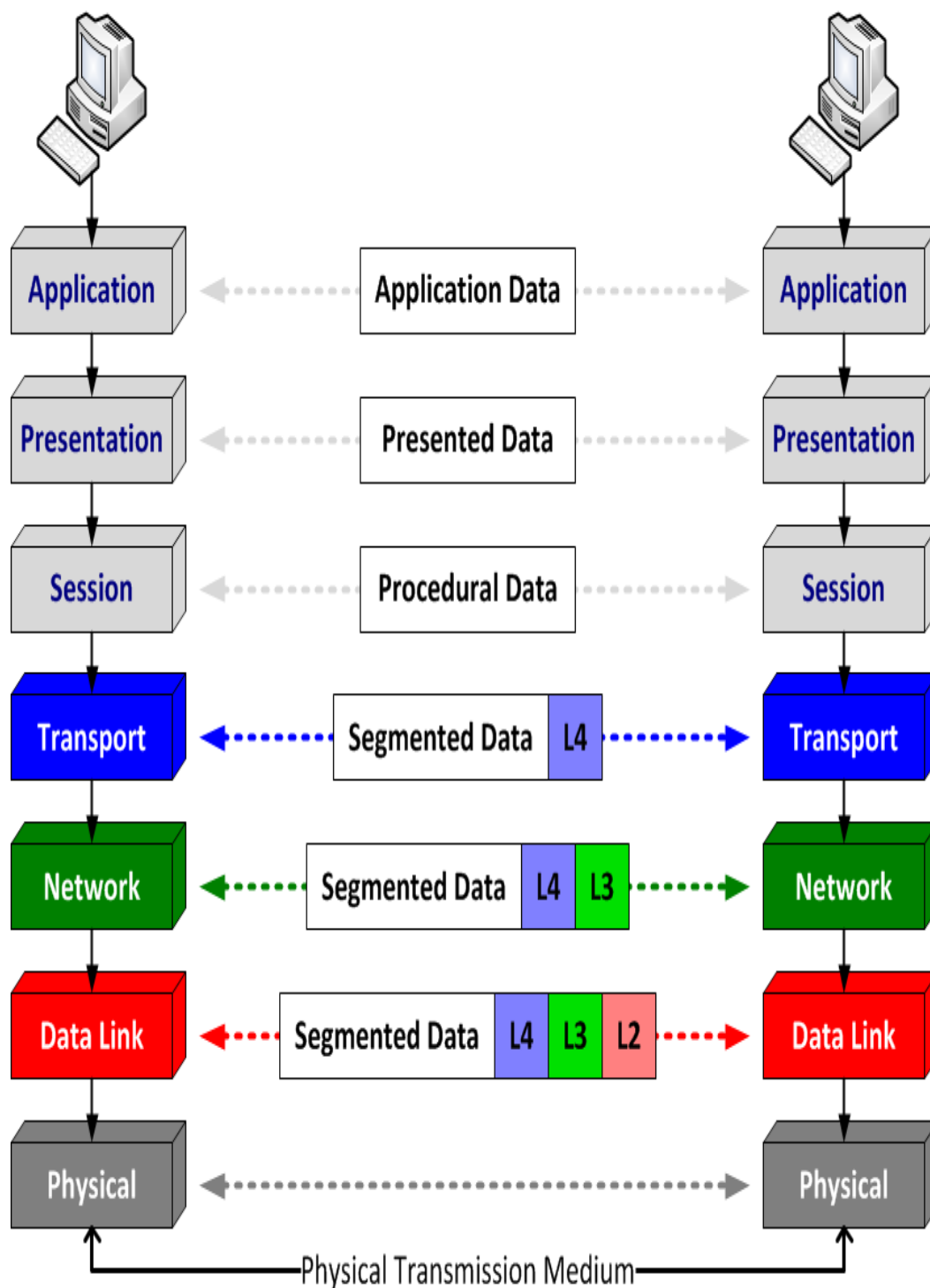
## ► *Open System Interconnection Model (OSI)*

- When networks first came into being, computers could usually communicate only with computers from the same manufacturer.  
For example, companies ran either a Microsoft or an IBM not both together.
- In the late 1970s, the Open Systems Interconnection (OSI) reference model was created by the International Organization for Standardization (ISO) to break through this barrier.
- The OSI model was meant to help vendors create interoperable network devices and software in the form of protocols so that different vendor networks could work with each other.
- The OSI model is the primary architectural model for networks. It describes how data and network information are communicated from an application on one computer through the network media to an application on another computer. The OSI reference model breaks this approach into layers.
- The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software. In the OSI reference model, the communications between a computing system are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.
- Created at a time when network computing was in its infancy, the OSI was published in 1984 by the International Organization for Standardization (ISO). Though it does not always map directly to specific systems, the OSI Model is still used today as a means to describe Network Architecture.

---

### ■ *OSI 7 layer*

- OSI Open System Interconnection We want the system to be standard to can any one use it
- ISO International Standard Organization Make standardization to main task for operation ( IEEE) The Institute of Electrical and Electronics Engineers



# L A Y E R S



## *IEEE*

- 38 societies
  - 130 journals
  - 1,300 conferences each year
  - 1,300 standards and projects
  - 400,000 members
  - 160 countries
  - IEEE 802.3
  - IEEE 802.11
- 

### ▪ *The Purpose of Reference Models*

- It divides the network communication process into smaller and simpler components, thus aiding component development, design, and troubleshooting.
  - It allows multiple-vendor development through standardization of network components.
  - It encourages industry standardization by defining what functions occur at each layer of the model.
  - It allows various types of network hardware and software to communicate.
  - It prevents changes in one layer from affecting other layers, so it does not hamper development.
  - you can better determine whether one device is going to be able to communicate with another device,
- 

### *Protocol Suites and Industry Standards*

	TCP/IP	ISO	AppleTalk	Novell Netware
7	HTTP	ACSE		
6	DNS	ROSE	AFP	NDS
5	DHCP	TRSE		
	FTP	SESE		
4	TCP	TP0 TP1 TP2	ATP AEP	SPX
	UDP	TP3 TP4	NBP RTMP	
3	IPV4 IPV6	CONP/CMNS	AFP	IPX
	ICMPV4	CLNP/CLNS		
	ICMPV6			
2	Ethernet PPP Frame Relay ATM WLAN			
1				

## Network Protocols and Standards Organizations

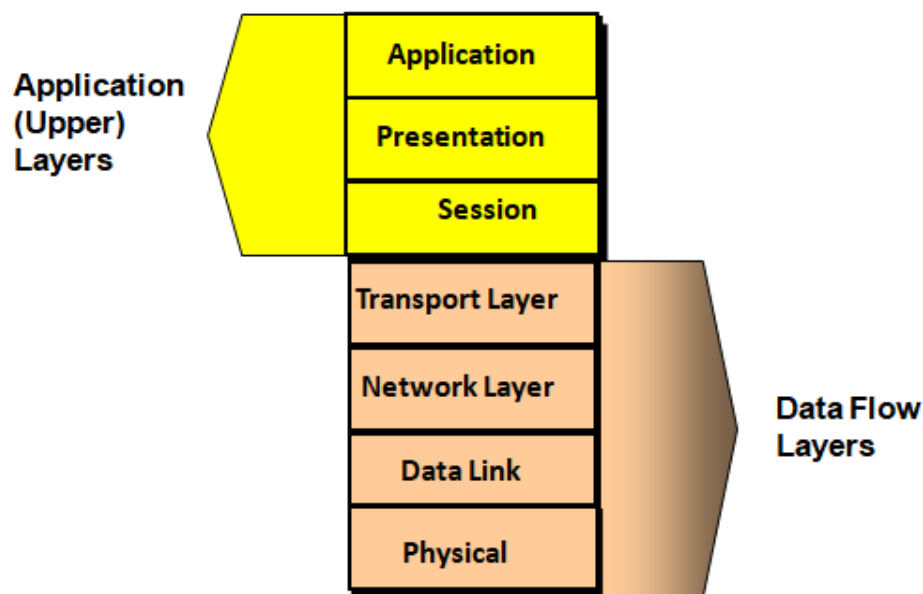
### Network Protocols and Standards Standards Organizations



## *Standards Organizations Other Standards Organization*

- The Electronic Industries Alliance (EIA)
  - The Telecommunications Industry Association (TIA)
  - The International Telecommunications Union –Telecommunications Standardization Sector (ITU-T)
  - The Internet Corporation for Assigned Names and Numbers (ICANN)
  - The Internet Assigned Numbers Authority (IANA)
- 

## **OSI Model Overview**



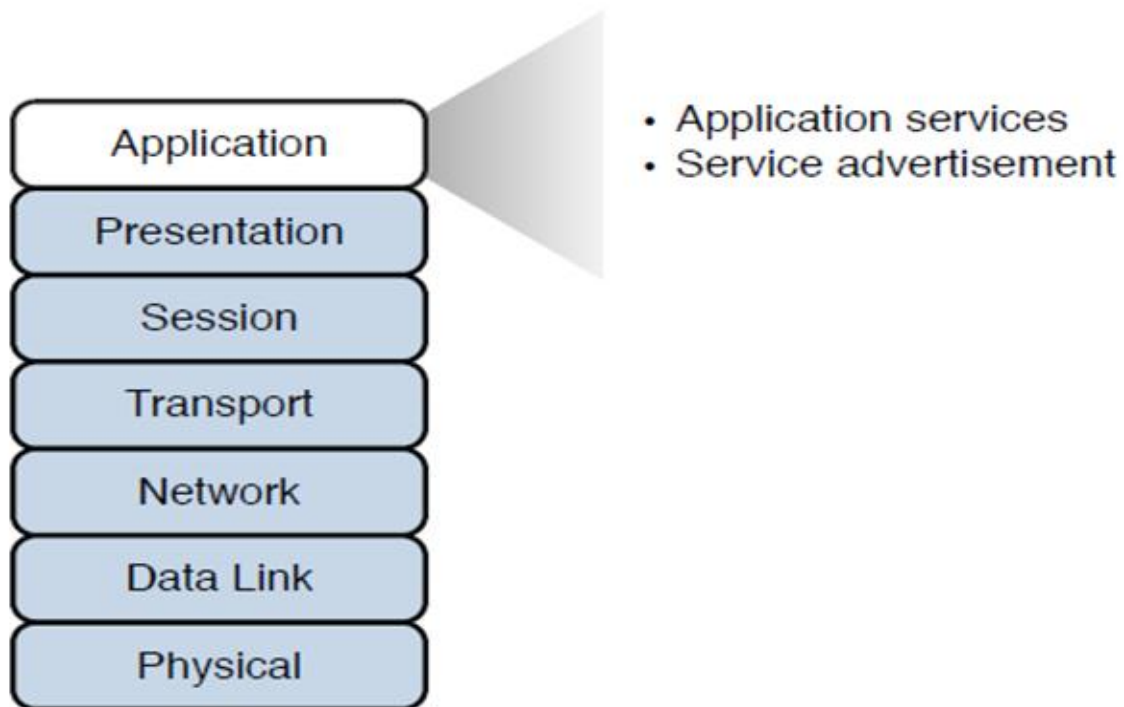
### *The Application Layer (Layer 7)*

The application layer provides services for an application program to ensure that effective communication with another application program on a network is possible. The application layer should not be thought of as an application as most people understand it. Instead, the application layer is a component within an application that controls the communication method to other devices. It's an abstraction layer service that masks the rest of the application from the transmission process. The application layer relies on all the layers below it to complete its process. At this stage, the data, or the application, is presented in a

visual form the user can understand. For example, e-mail is an application layer service that does reside at the application layer

---

## The Application Layer(Layer 7) cont



---

### *Functions of the application layer*

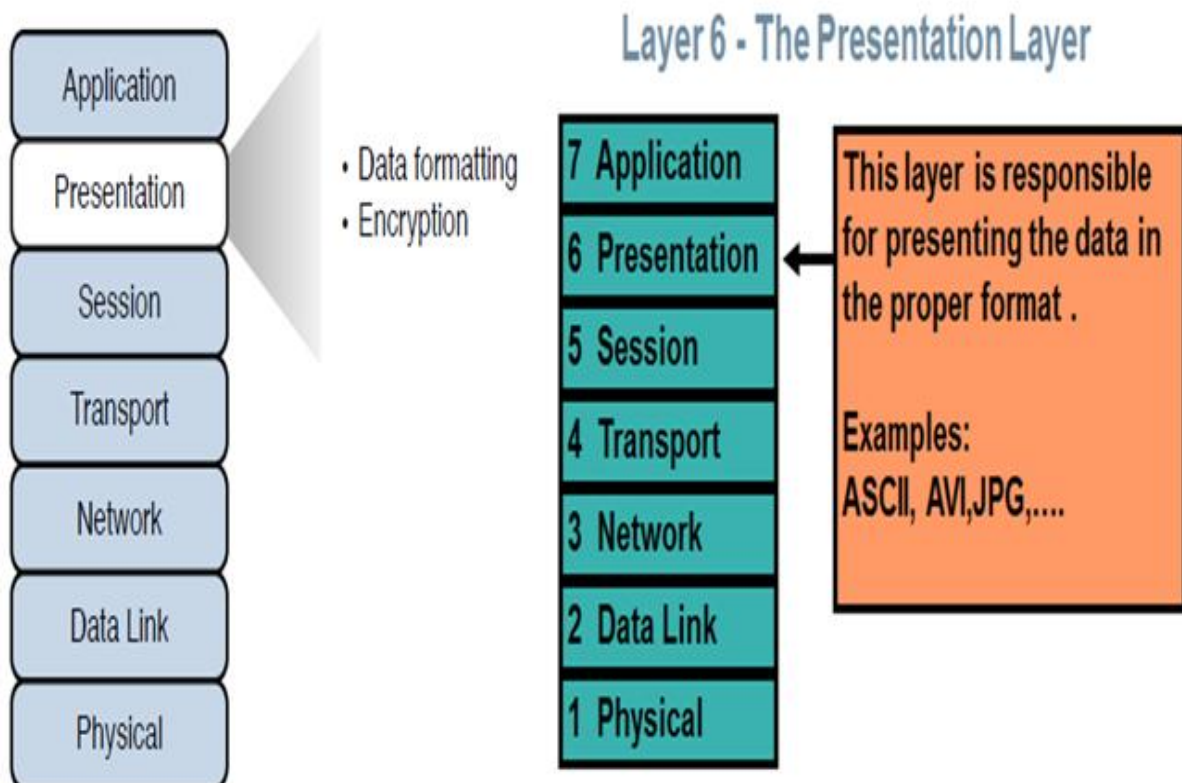
- Application services: Examples of the application services residing at the application layer include file sharing and e-mail.
  - Service advertisement: Some applications' services (for example, some networked printers) periodically send out advertisements, making the availability of their service known to other devices on the network. Other services, however, register themselves and their services with a centralized directory services.
- 

### ▪ *The Presentation Layer (layer 6)*

- The presentation layer is responsible for the formatting of data being exchanged and securing that data with encryption.

- The presentation layer (Layer 6) ensures that the message is presented to the upper layer in a standardized format. It deals with the syntax and the semantics of the messages.
  - The main functions of the presentation layer are as follows :
    - 1- It encodes the messages from the user dependent format to the common format and vice versa, for communication among dissimilar systems.
    - 2- It is responsible for data encryption and decryption of sensitive data before they are transmitted over common channels.
    - 3- It is also responsible for data compression. Data compression is done at the source to reduce the number of bits to be transmitted. It reduces the storage space and increases the file transfer rate. It is particularly useful for transmission of large multimedia files.
    - 4-Data formatting (extension) like (PDF,JPG,MP3,MP4..Etc)
- 

## The Presentation Layer (cont)



## ▪ *The Session Layer(layer 5)*

- The session layer is responsible for setting up, maintaining, and tearing down sessions. A session can be thought of as a conversation that needs to be treated separately from other sessions to avoid intermingling of data from different conversations.
- The Session Layer allows users on different machines to establish active communication sessions between them.
- It's main aim is to establish, maintain and synchronize the interaction between communicating systems. Session layer manages and synchronize the conversation between two different applications. In Session layer, streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

---

## *The Session Layer(layer 5) cont*

- This layer also provides dialogue control between devices, or nodes. It coordinates communication between systems and serves to organize their communication by offering three different modes:

---

### *✓ simplex, half duplex, and full duplex.*

- Set a logical connection ( session) between different application
- Specifies communication mode

( simple - Half duplex – full duplex )

Simple duplex:- device send or receive the data.

half duplex:- :- device send and receive the data but not same time.

full duplex:- device send and receive the data in same time

## *Functions of session layer*

---

### *1. Setting up a session: -*

- Checking user credentials (for example, username and password).
- Assigning numbers to a session's communications flows to uniquely identify each flow.



- Negotiating services required during the session.
  - Negotiating which device begins sending data.
- 

## ***2- Maintaining a session:-***

- Transferring data.
- Reestablishing a disconnected session.
- Acknowledging receipt of data.

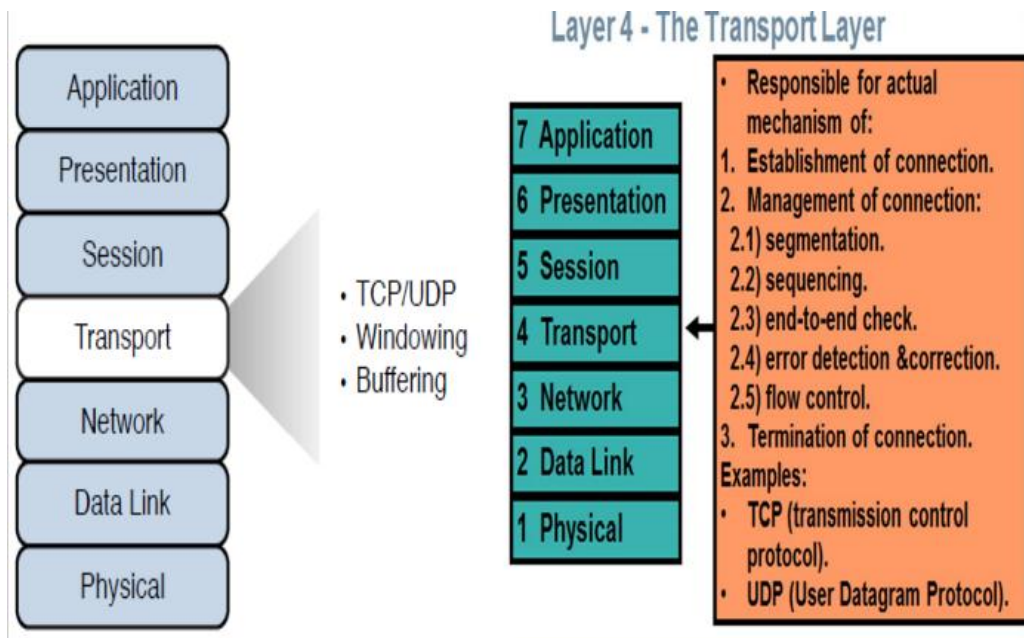
## ***3- Tearing down a session:***

A session can be disconnected based on mutual agreement of the devices in the session. Alternatively, a session might be torn down because one party disconnects (either intentionally or because of an error condition). In the event that one party disconnects, the other party can detect a loss of communication with that party and tear down its side of the session.

---

## ***▪ The Transport Layer***

- The transport layer acts as a dividing line between the upper layers and lower layers of the OSI model. Specifically, messages are taken from upper layers (Layers 5–7) and are encapsulated into segments for transmission to the lower layers (Layers 1–3). Similarly, data streams coming from lower layers are decapsulated and sent to Layer 5 (the session layer), or some other upper layer, depending on the protocol.
  - The Transport layer segments and reassembles data into a data stream.
  - They provide end-to-end data transport services and can establish a logical connection between the sending host and destination host on an internetwork.
  - Flow control ,Acknowledgments and Error recovery are used in this layer.
  - Port number is used in this layer
-



## *Transport layer*

- Flow control
- Error recovery

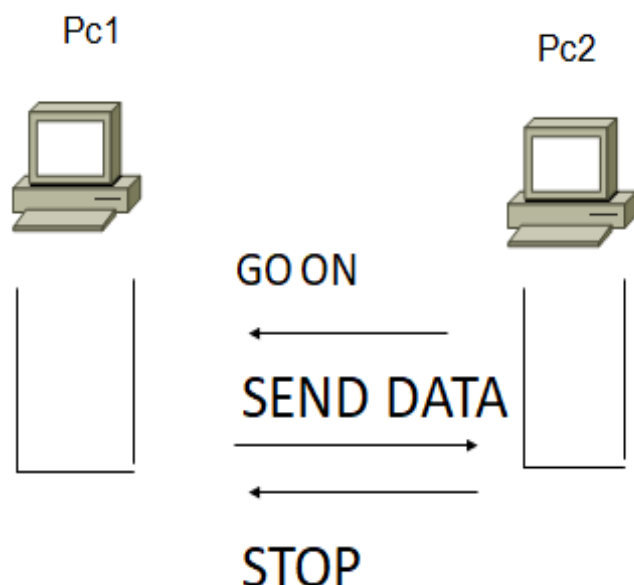
*Flow control* provides a means for the receiver to govern the amount of data sent by the sender. It prevents a sending host on one side of the connection from overflowing the buffers in the receiving host—an event that can result in lost data. Reliable data transport employs a connection-oriented communications session between systems, and the protocols involved ensure that the following will be achieved:

### **Flow control :-**

- Buffering .
- Congestion avoidance.
- **Error recovery**

### **•Acknowledgments:-**

Reliable data delivery ensures the integrity of a stream of data sent from one machine to the other through a fully functional



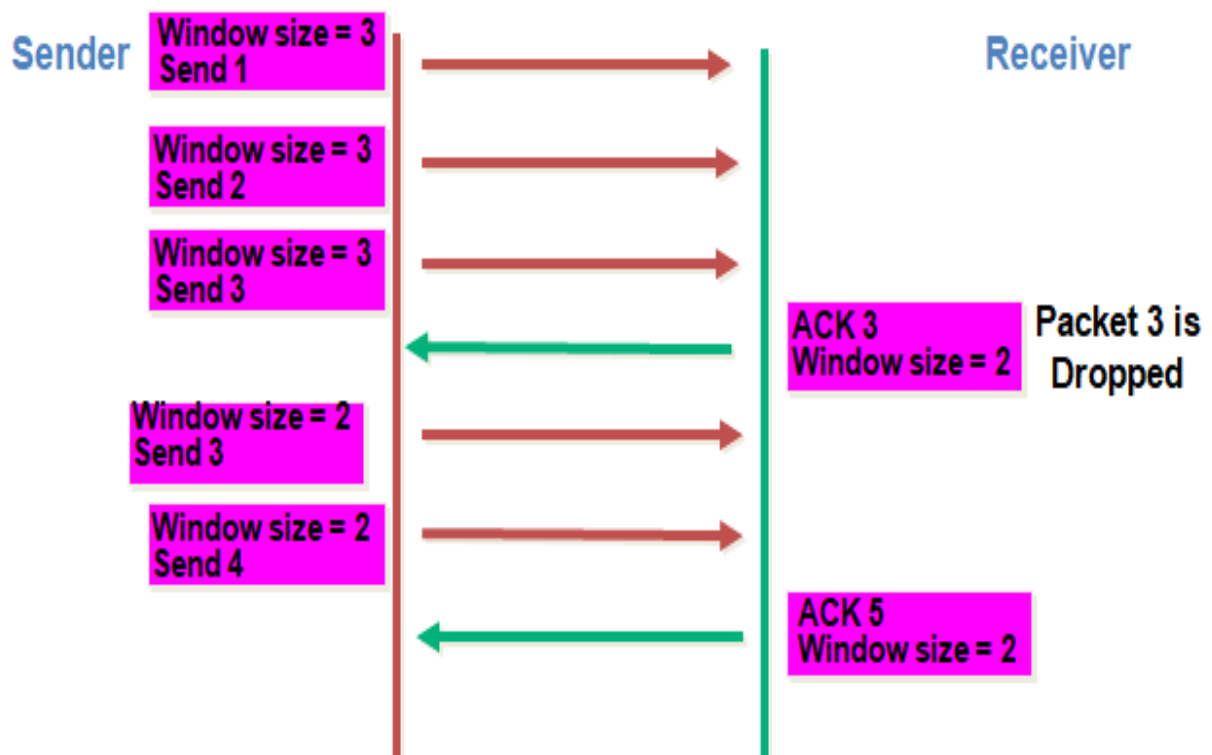
data link. It guarantees that the data won't be duplicated or lost.

The receiver sending an acknowledgment message back to the sender when it receives data.

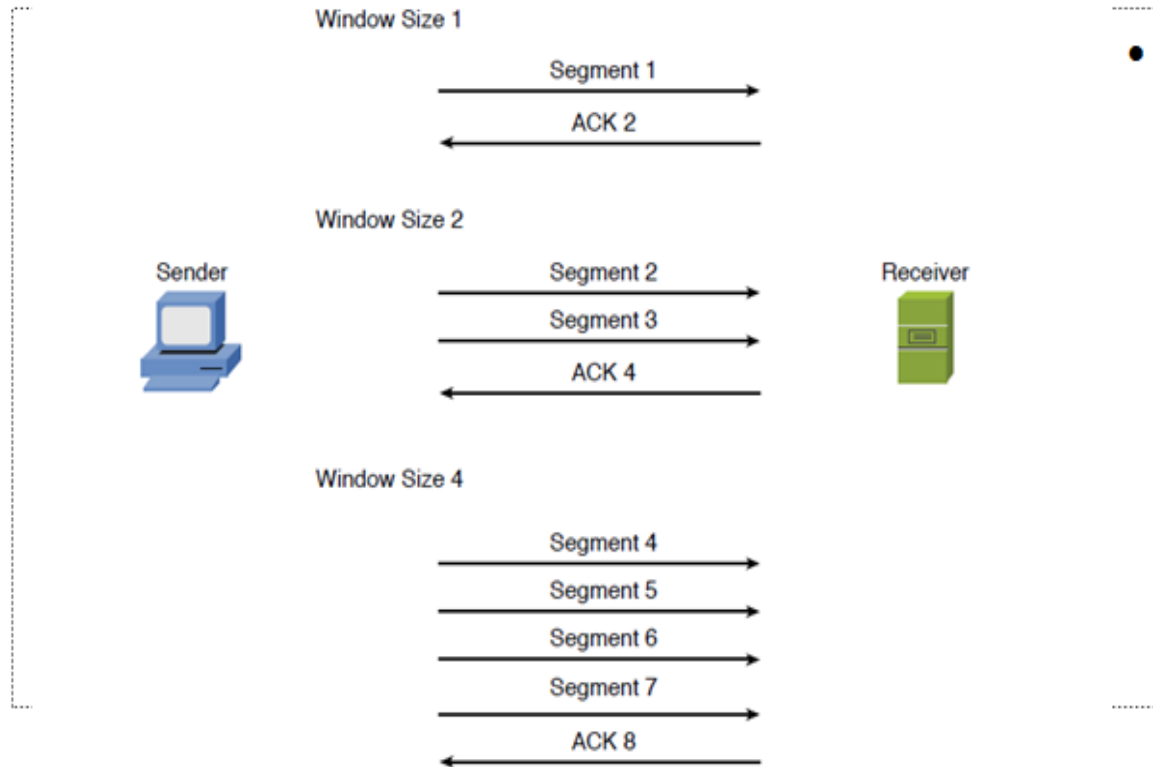
- **Windowing** :- because time is available after the sender transmits the data segment and before it finishes processing acknowledgments from the receiving machine, the sender uses the break as an opportunity to transmit more data. The quantity of data segments (measured in bytes) that the transmitting machine is allowed to send without receiving an acknowledgment for them is called a window.

- **Segmentation**:- is dividing the data to small parts to help to send them

## Windowing



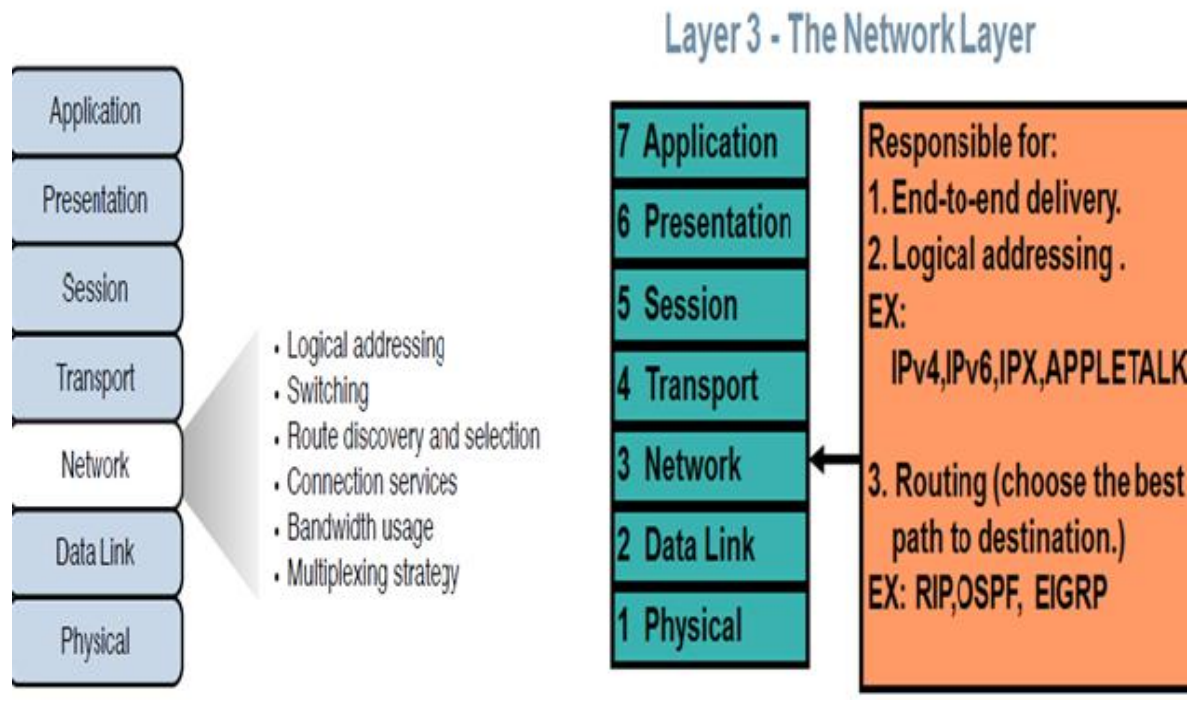
# TCP Sliding Window



## ▪ The Network Layer (Layer 3)

- The network layer is primarily concerned with forwarding data based on logical addresses.
- The Network layer manages device addressing, tracks the location of devices on the network, and determines the best way to move data, which means that the Network layer must transport traffic between devices that aren't locally attached.
- Routers and switch L3 (Layer 3 devices) are specified at the Network layer and provide the routing services within an internetwork.
- Although many network administrators immediately think of routing and IP addressing when they hear about the network layer.
- Ip address, IPX and APF

## The Network Layer (cont)



### ▪ *This layer is actually responsible*

**1- Logical addressing:** - Although the data link layer uses physical addresses to make forwarding decisions, the network layer uses logical addressing to make forwarding decisions. A variety of routed protocols (for example, AppleTalk and IPX) have their own logical addressing schemes, but by far, the most widely deployed routed protocol is Internet Protocol (IP).

**2- Route discovery and selection:-** Because Layer 3 devices make forwarding decisions based on logical network addresses, a Layer 3 device might need to know how to reach various network addresses. For example, a common Layer 3 device is a router. A router can maintain a routing table indicating how to forward a packet based on the packet's destination network address via a dynamic routing protocol (for example, RIP, OSPF, or EIGRP).

▪ *Logical addressing and Route discovery and selection*

---

▪ **This layer is actually responsible cont**

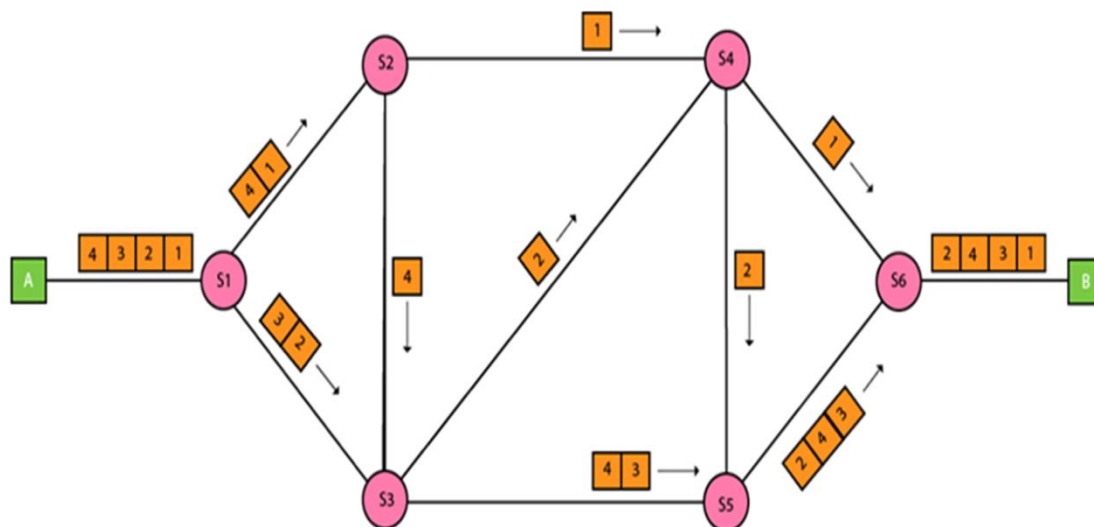
**3- Switching** : The term switching is often associated with Layer 2 technologies; however, the concept of switching also exists at Layer 3. Switching, at its essence, is making decisions about how data should be forwarded. At Layer 3, three common switching techniques exist:

- **Packet switching**: With packet switching, a data stream is divided into packets. Each packet has a Layer 3 header, which includes a source and destination Layer 3 address.

- **Circuit switching**: Circuit switching dynamically brings up a dedicated communication link between two parties for those parties to communicate.

As a simple example of circuit switching, think of making a phone call from your home to a business. Assuming you have a traditional landline servicing your phone, the telephone company's switching equipment interconnects your home phone with the phone system of the business you are calling. This interconnection (that is, circuit ) only exists for the duration of the phone call.

- **Message switching**: Unlike packet switching and circuit switching technologies, message switching is usually not well suited for real-time applications because of the delay involved. Specifically, with message switching, a data stream is divided into messages. Each message is tagged with a destination address, and the messages travel from one network device to another network device on the way to their destination





Circuit Switching	Packet Switching(Datagram type)	Packet Switching(Virtual Circuit type)
Dedicated path	No Dedicated path	No Dedicated path
Path is established for entire conversation	Route is established for each packet	Route is established for entire conversation
Call setup delay	packet transmission delay	call setup delay as well as packet transmission delay
Overload may block call setup	Overload increases packet delay	Overload may block call setup and increases packet delay
Fixed bandwidth	Dynamic bandwidth	Dynamic bandwidth
No overhead bits after call setup	overhead bits in each packet	overhead bits in each packet

## Difference between Circuit Switching and Packet Switching

Circuit Switching	Packet Switching
A circuit needs to be established to make sure that data transmission takes place.	Each packet containing the information that needs to be processed goes through the dynamic route.
A uniform path is followed throughout the session.	There is no uniform path that is followed end to end through the session.
It is most ideal for voice communication, while also keeping the delay uniform.	It is used mainly for data transmission as the delay is not uniform.
Without a connection, it cannot exist, as the connection needs to be present on a physical layer.	A connection is not necessary, as it can exist without one too. It needs to be present on a network layer.
Data to be transmitted is processed at the source itself.	Data is processed and transmitted at the source as well as at each switching station.

▪ *this layer is actually responsible cont*

**4- Connection services:** Just as the data link layer provided connection services for flow control and error control, connection services also exist at the network layer. Connection services at the network layer can improve the communication reliability, in the event that the data link's LLC sublayer is not performing connection services.

The following functions are performed by connection services at the network layer:

■ **Flow control** (also known as congestion control): Helps prevent a sender from sending data more rapidly than the receiver is capable of receiving the data.

■ **Packet reordering:** Allows packets to be placed in the appropriate sequence as they are sent to the receiver. This might be necessary because some networks support load balancing, where multiple links are used to send packets between two devices. Because multiple links are used, packets might arrive out of order.

---

## ▪ *The Data Link Layer (Layer 2)*

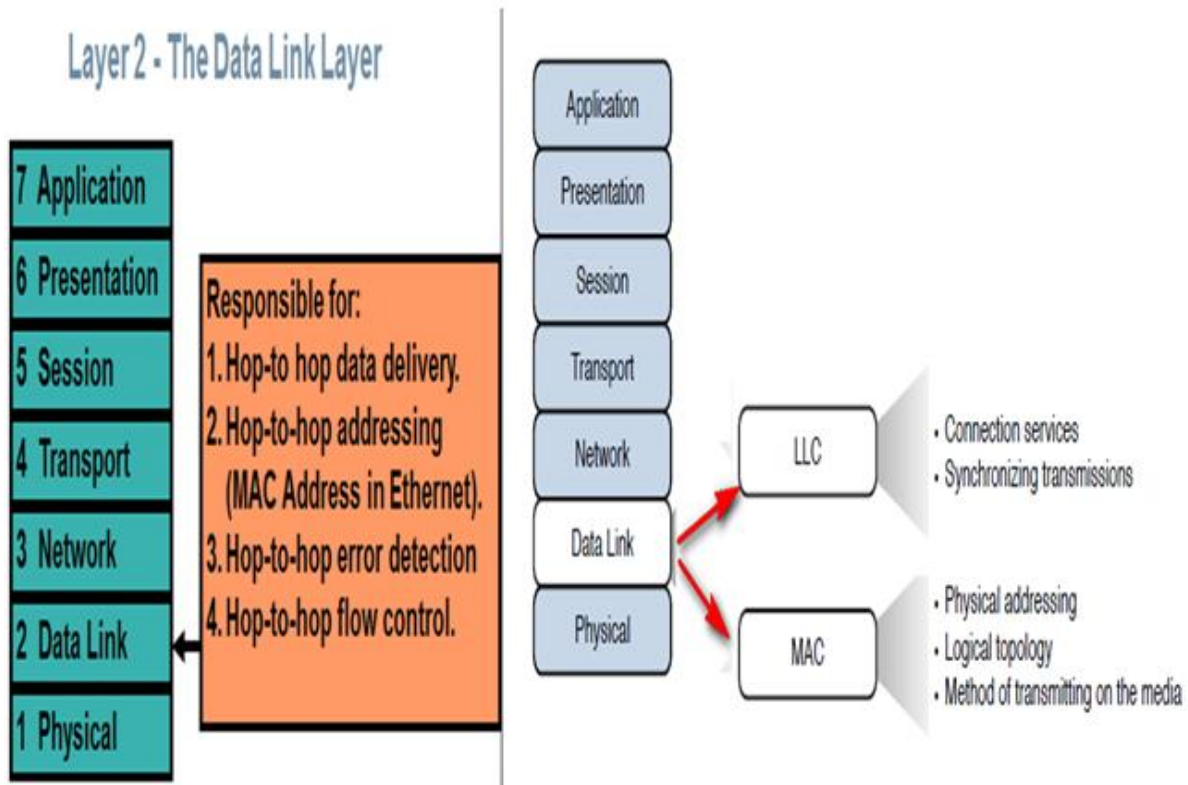
• The data link layer ensures that all packets of information are passed on free of errors. It makes sure the appropriate physical protocol is assigned to the data.

• The data link layer is concerned with packaging data into frames and transmitting those frames on the network, performing error detection/correction, uniquely identifying network devices with an address, and handling flow control. These processes are collectively referred to as data-link control (DLC).

• The data link layer is responsible for the exchange of frames between nodes over a physical network media. It allows the upper layers to access the media and controls how data is placed and received on the media.

• Switch, bridge most common device in this layer • The data link layer is unique from the other layers in that it has two sublayers of its own: MAC and LLC.

## The Data Link Layer (Layer 2) cont



---

### ▪ *Media Access Control*

*Characteristics of the Media Access Control (MAC) sublayer include the following:*

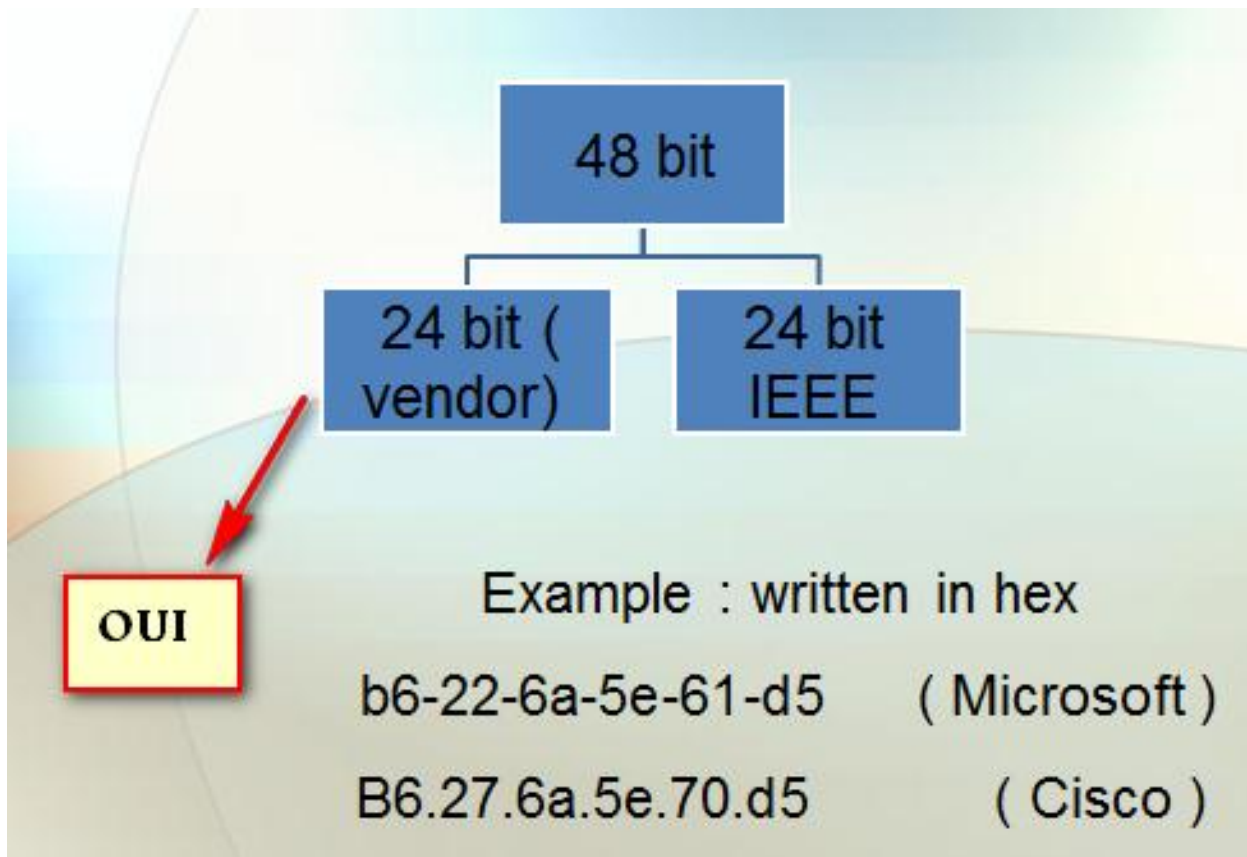
---

**1- Physical addressing :** - A MAC address is a unique identifier for network interfaces. It is a 48-bit number (12 hexadecimal characters). They can either be written in either of these formats:

- A common example of a Layer 2 address is a MAC address, which is a 48-bit address assigned to a device's network interface card (NIC).
- The address is commonly written in hexadecimal notation (for example, 58:55:ca:eb:27:83). The first 24 bits of the 48-bit address are collectively referred to as the vendor code .
- Vendors of networking equipment are assigned one or more unique vendor codes.

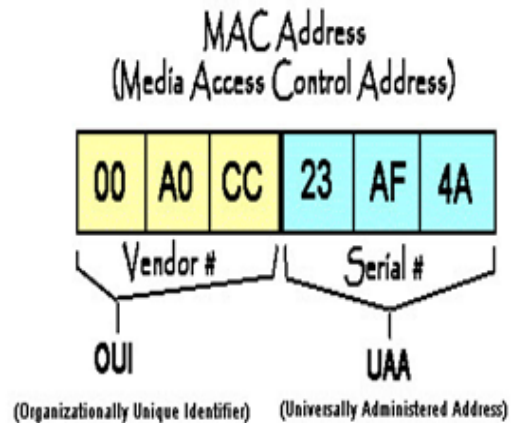
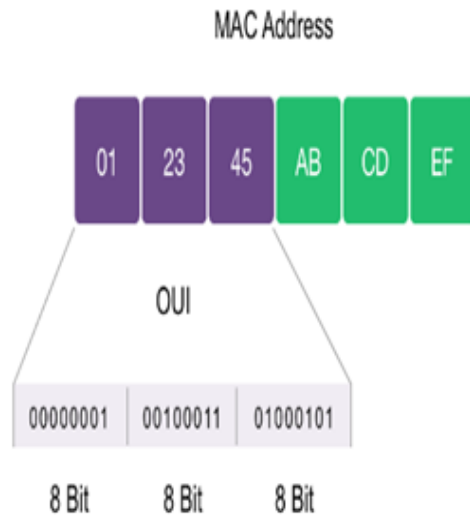
You can use the list of vendor codes at <http://standards.ieee.org/develop/regauth/oui/oui.txt> to determine the manufacturer of a networking device, based on the first half of the device's MAC address. Because each vendor is responsible for using unique values in the last 24 bits of a MAC address, and because each vendor has a unique vendor code, no two MAC addresses in the world should have the same value.

**MAC address** : hardware address



### ▪ *OUI {Organizationally Unique Identifier}*

An OUI {Organizationally Unique Identifier} is a 24-bit number that uniquely identifies a vendor or manufacturer. They are purchased and assigned by the IEEE. The OUI is basically the first three octets of a MAC address.



## ▪ *Media Access Control*

2- Logical topology:- Layer 2 devices view a network as a logical topology. Examples of a logical topology include bus and ring topologies.

3- Method of transmitting on the media:- With several devices connected to a network, there needs to be some strategy for determining when a device is allowed to transmit on the media. Otherwise, multiple devices might transmit at the same time, and interfere with one another's transmissions.

## ▪ *Logical Link Control*

**Characteristics of the Logical Link Control (LLC) sublayer include the following:-**

**1- Connection services:-** When a device on a network receives a message from another device on the network, that recipient device can provide feedback to the sender in the form of an acknowledgment message. The two main functions provided by these acknowledgment messages are as follows:

- **Flow control:** Limits the amount of data a sender can send at one time; this prevents the receiver from being overwhelmed with too much information.
- **Error control:** Allows the recipient of data to let the sender know whether the expected data frame was not received or whether it was received but is corrupted. The recipient determines whether the data frame is corrupted by mathematically calculating a checksum of the data received. If the calculated

checksum does not match the checksum received with the data frame, the recipient of the data draws the conclusion that the data frame is corrupted and can then notify the sender via an acknowledgment message.

## ▪ *Logical Link Control (cont)*

**2- Synchronizing transmissions:-** Senders and receivers of data frames need to coordinate when a data frame is being transmitted and should be received.

Three methods of performing this synchronization are as follows:

- **Asynchronous:-** With asynchronous transmission, network devices reference their own internal clocks, and network devices do not need to synchronize their clocks. Instead, the sender places a start bit at the beginning of each data frame and a stop bit at the end of each data frame.

These start and stop bits tell the receiver when to monitor the medium for the presence of bits.

An additional bit, called the parity bit (0,1) odd or even, might also be added to the end of each byte in a frame to detect an error in the frame.

- **Synchronous:** With synchronous transmission, two network devices that want to communicate between themselves must agree on a clocking method to indicate the beginning and ending of data frames. One approach to providing this clocking is to use a separate communications channel over which a clock signal is sent.

However, rather than using parity bits, synchronous communication runs a mathematical algorithm on the data to create a cyclic redundancy check (CRC).

---

## ▪ *The Physical Layer (Layer)*

- Physical layer in the OSI model plays the role of interacting with actual hardware and signaling mechanism. Physical layer is the only layer of OSI network model which actually deals with the physical connectivity of two different stations. This layer defines the hardware equipment, cabling, wiring, frequencies, pulses used to represent binary signals etc.

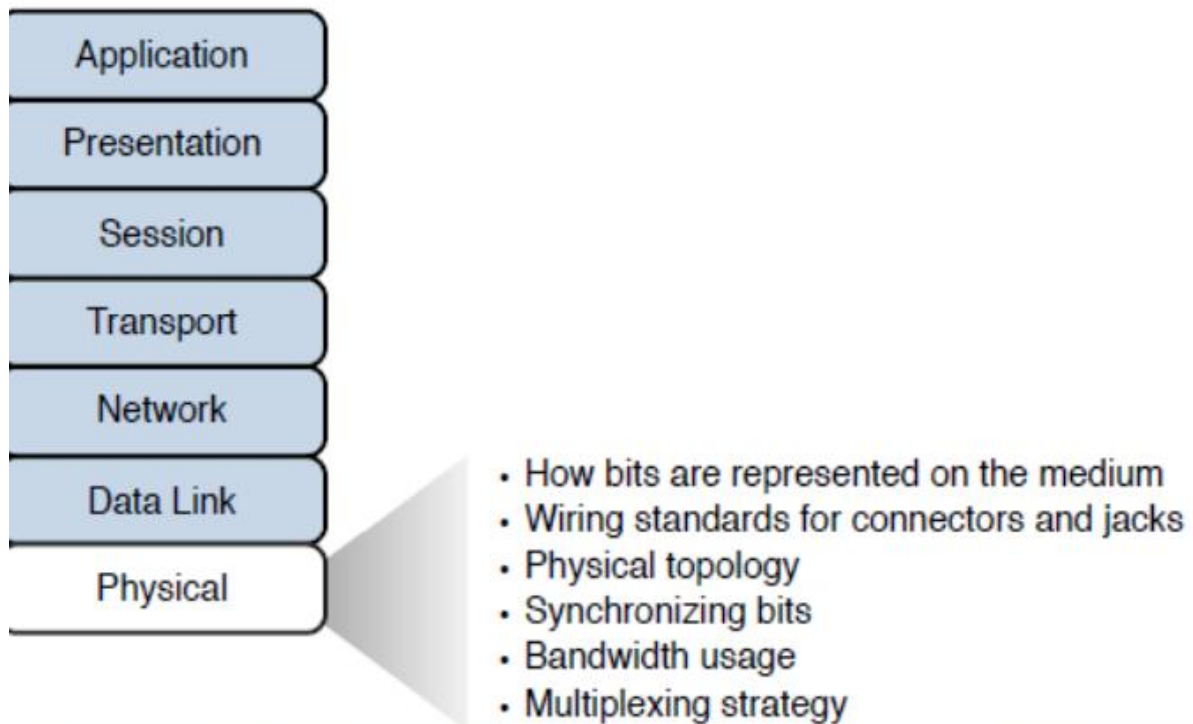
- Physical layer provides its services to Data-link layer. Data-link layer hands over frames to physical layer. Physical layer converts them to electrical pulses, which represent binary data. The binary data is then sent over the wired or wireless media.

- The physical layer is concerned with the transmission of bits on the network along with the physical and electrical characteristics of the network.



- Examples of devices defined by physical layer standards include hubs, wireless access points, and network cabling.

## ▪ The Physical Layer (Layer) cont



## ▪ *The physical layer defines*

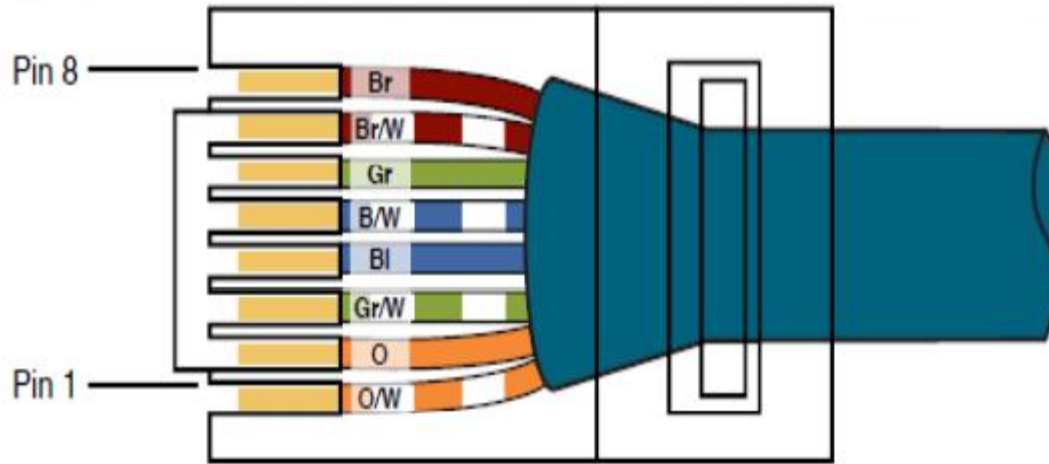
**1- How bits are represented on the medium:** Data on a computer network is represented as a binary expression.

Electrical voltage (on copper wiring) or light (carried via fiber-optic cabling) can represent these 1s and 0s. For example, the presence or the absence of voltage on a wire can represent a binary 1 or a binary 0, respectively, as illustrated in Figure 2-5 . Similarly, the presence or absence of light on a fiber-optic cable can represent a 1 or 0 in binary. This type of approach is called current state modulation



Current State Modulation

2- Wiring standards for connectors and jacks: Several standards for network For example however, the TIA/EIA-568-B standard describes how an RJ-45 connector should be wired for use on a 100BASE-TX Ethernet network.



TIA/EIA-568-B Wiring Standard for an RJ-45 Connector

3- **Synchronizing bits:** For two networked devices to successfully communicate

at the physical layer, they must agree on when one bit stops and another bit starts. Specifically, what is needed is a method to synchronize the bits. Two basic approaches to bit synchronization include asynchronous and synchronous synchronization:

■ **Asynchronous:** With this approach, a sender indicates that it is about to start transmitting by sending a start bit to the receiver. When the receiver sees this, it starts its own internal clock to measure the subsequent bits. After the sender transmits its data, it sends a stop bit to indicate that it has finished its transmission.

■ **Synchronous:** This approach synchronizes the internal clocks of both the sender and the receiver to ensure that they agree on when bits begin and end. A common approach to make this synchronization happen is to use an external clock (for example, a clock provided by a service provider), which is referenced by both the sender and the receiver.

4- **Physical topology:** Layer 1 devices view a network as a physical topology (as opposed to a logical topology). Examples of a physical topology include bus,

ring, and star topologies

**5- Bandwidth usage:** The two fundamental approaches to bandwidth usage on a network are broadband and baseband :

■ **Broadband:** Broadband technologies divide the bandwidth available on a medium (for example, copper or fiber-optic cabling) into different channels. Different communication streams are then transmitted over the various channels. For example, consider frequency-division multiplexing (FDM) used by a cable modem. Specifically, a cable modem uses certain ranges of frequencies on the cable coming into your home from the local cable company to carry incoming data, another range of frequencies for outgoing data, and several other frequency ranges for various TV stations.

■ **Baseband:** Baseband technologies, in contrast, use all the available frequencies on a medium to transmit data. Ethernet is an example of a networking technology that uses baseband.

**6- Multiplexing strategy:** Multiplexing allows multiple communications sessions to share the same physical medium. Cable TV, as previously mentioned, allows you to receive multiple channels over a single physical medium (for example, a coaxial cable plugged into the back of your television).

**Here are some of the more common approaches to multiplexing:**

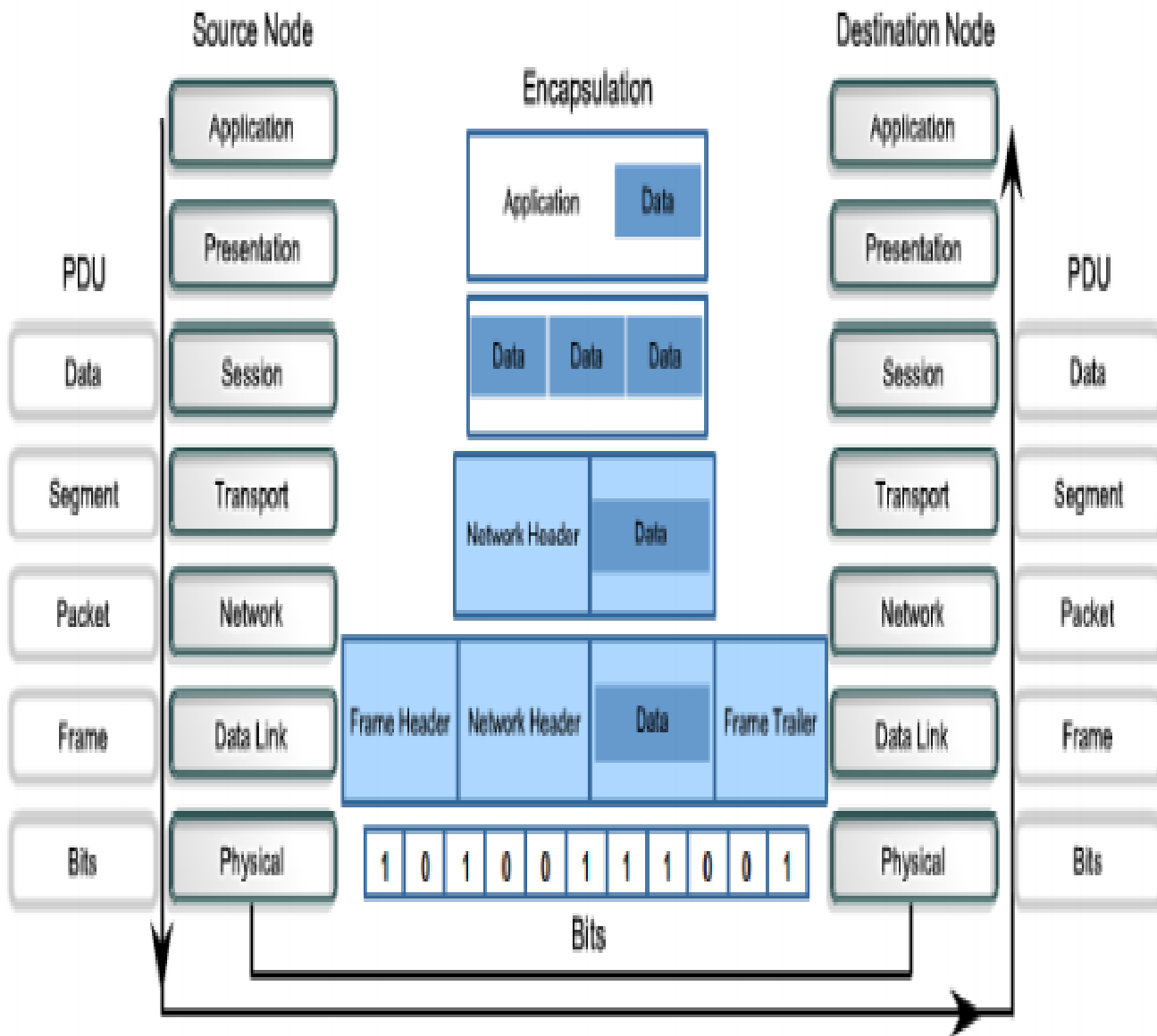
-----  
■ **Time-division multiplexing (TDM):** TDM supports different communication sessions (for example, different telephone conversations in a telephony network) on the same physical medium by causing the sessions to take turns. For a brief period of time, defined as a time slot, data from the first session will be sent, followed by data from the second session. This continues until all sessions have had a turn, and the process repeats itself.

■ **Statistical time-division multiplexing (StatTDM):** A downside to TDM is that each communication session receives its own time slot, even if one of the sessions does not have any data to transmit at the moment. To make a more efficient use of available bandwidth, StatTDM dynamically assigns time slots to communications sessions on an as-needed basis.

■ **Frequency-division multiplexing (FDM):** FDM divides a medium's frequency range into channels, and different communication sessions transmit their data over different channels. As previously described, this approach to bandwidth usage is called broadband .

-----

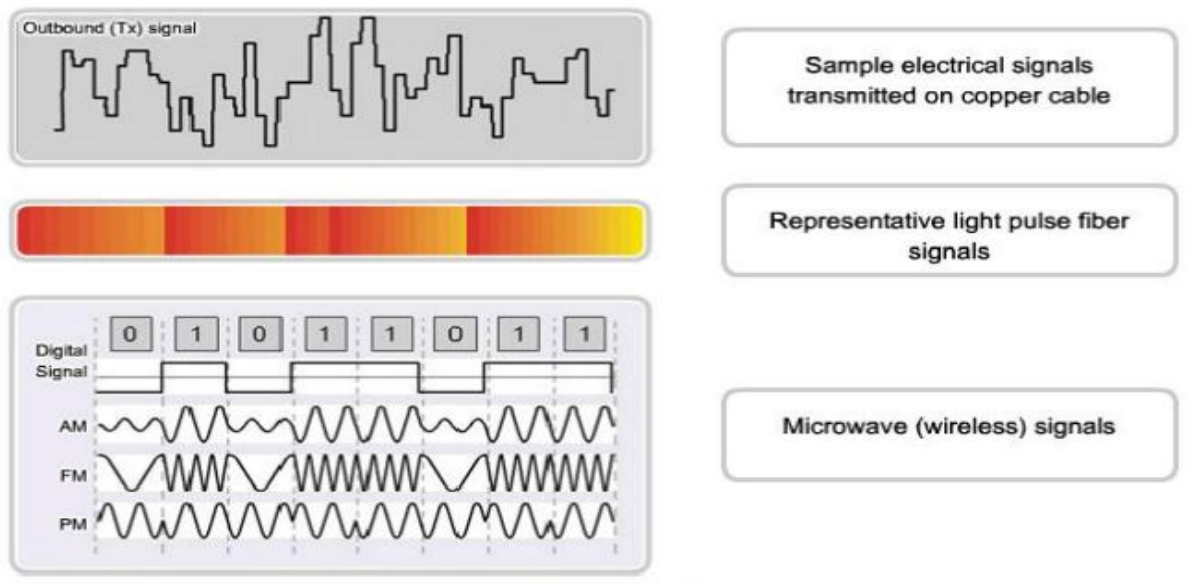
# The Physical Layer



In diagrams, signals on the physical media are depicted by this line symbol.

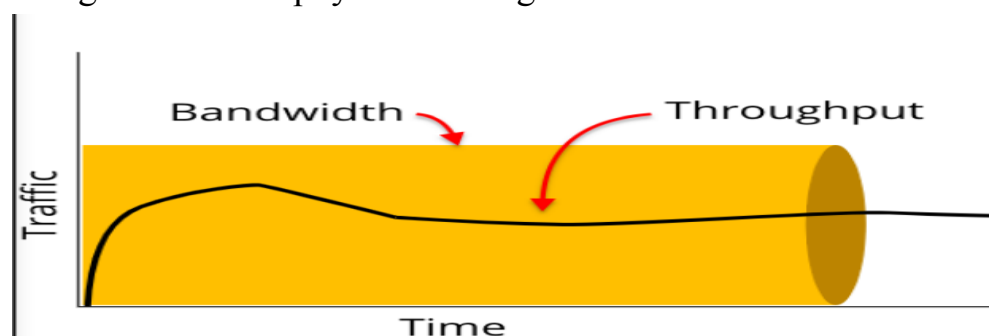


## ▪ *Physical Layer Media*

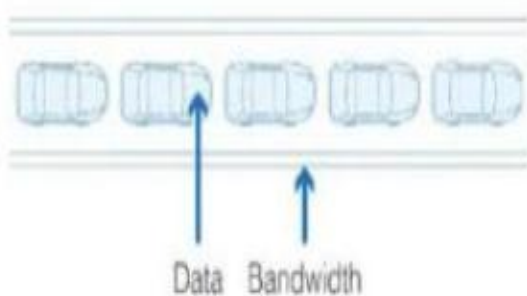


## ▪ *Speed and bandwidth*

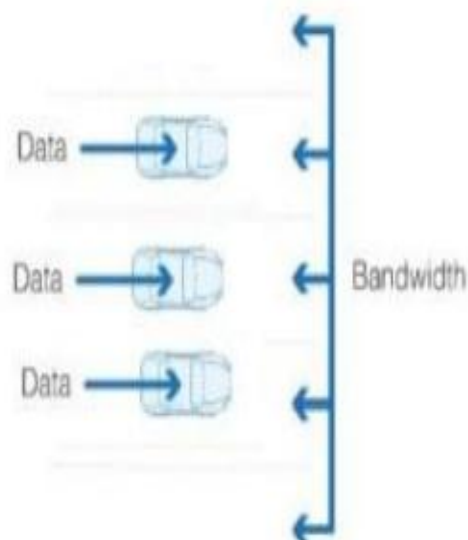
- Bandwidth is the capacity available and has nothing to do with speed. For example, a stadium that can hold 75,000 fans doesn't improve the running speed of an athlete on the field. How fast that athlete can run is determined on a variety of factors— including training, health and natural aptitude. In the same way, the speed of the athlete isn't determined by the size of the stadium.
- When ISPs advertise “blazing-fast speeds” and make other such claims, it could seem like purchasing the highest-bandwidth plan will provide those top speeds. This simply isn't true.
- Bandwidth doesn't necessarily affect any single computer, and certainly won't affect connection speed. If each computer takes up one “lane,” bandwidth is how many lanes are available. The speed of each lane is completely independent of the amount of lanes.
- Where bandwidth will limit you is with data limits. Bandwidth itself is how much data can be transferred and processed at any given moment. It's restricted by cabling and laws of physics— though it shouldn't be confused with data caps.



**Throughput:**  
One data packet arrives  
within one second.



**Throughput:**  
Five data packets  
arrive within one second



Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	kbps	1 kbps = 1,000 bps = $10^3$ bps
Megabits per second	Mbps	1 Mbps = 1,000,000 bps = $10^6$ bps
Gigabits per second	Gbps	1 Gbps = 1,000,000,000 bps = $10^9$ bps
Terabits per second	Tbps	1 Tbps = 1,000,000,000,000 bps = $10^{12}$ bps

Prefix	Symbol	$1000^m$	$10^n$	Decimal	Short scale	Long scale	Since
yotta	Y	$1000^8$	$10^{24}$	1 000 000 000 000 000 000 000 000	Septillion	Quadrillion	1991
zetta	Z	$1000^7$	$10^{21}$	1 000 000 000 000 000 000 000	Sextillion	Trilliard	1991
exa	E	$1000^6$	$10^{18}$	1 000 000 000 000 000 000	Quintillion	Trillion	1975
peta	P	$1000^5$	$10^{15}$	1 000 000 000 000 000	Quadrillion	Billiard	1975
tera	T	$1000^4$	$10^{12}$	1 000 000 000 000	Trillion	Billion	1960
giga	G	$1000^3$	$10^9$	1 000 000 000	Billion	Milliard	1960
mega	M	$1000^2$	$10^6$	1 000 000		Million	1960
kilo	k	$1000^1$	$10^3$	1 000		Thousand	1795
hecto	h	$1000^{2/3}$	$10^2$	100		Hundred	1795
deca	da	$1000^{1/3}$	$10^1$	10		Ten	1795

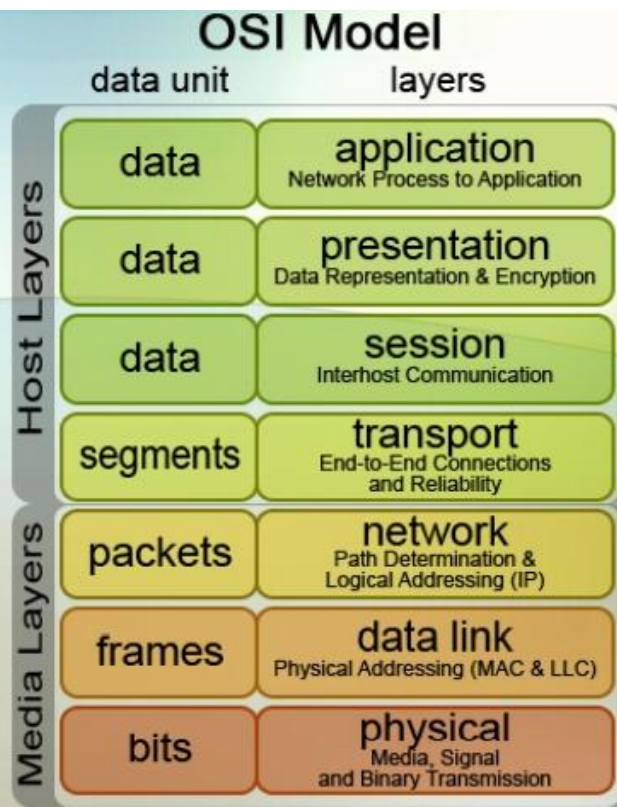


## Summary of OSI layers

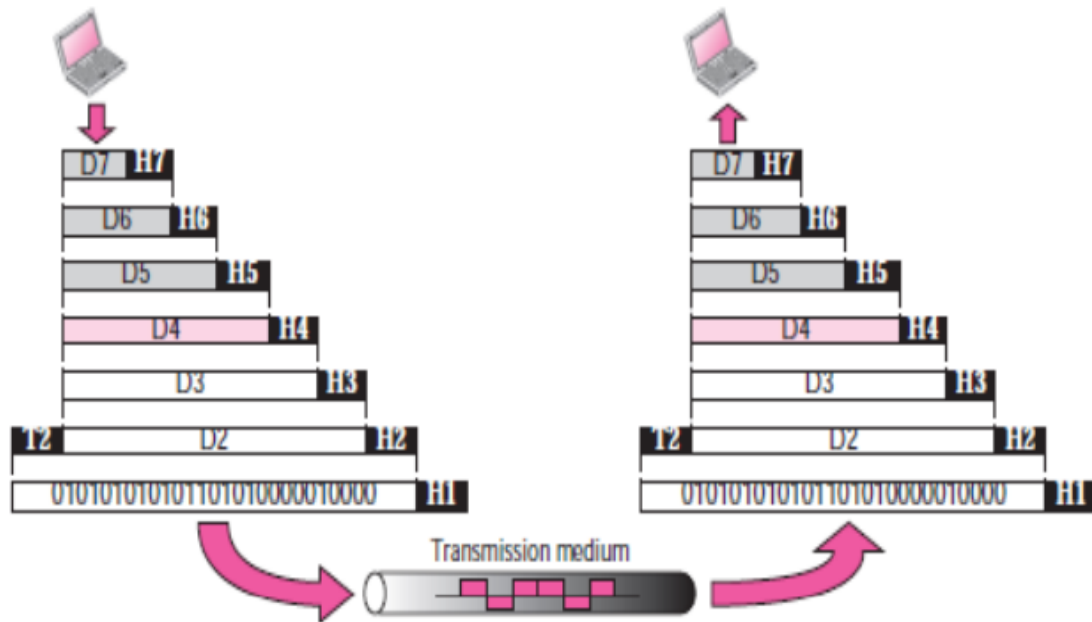
Application	To allow access to network resources	7
Presentation	To translate, encrypt, and compress data	6
Session	To establish, manage, and terminate sessions	5
Transport	To provide reliable process-to-process message delivery and error recovery	4
Network	To move packets from source to destination; to provide internetworking	3
Data link	To organize bits into frames; to provide hop-to-hop delivery	2
Physical	To transmit bits over a medium; to provide mechanical and electrical specifications	1

## Protocol Data Units (PDUs)

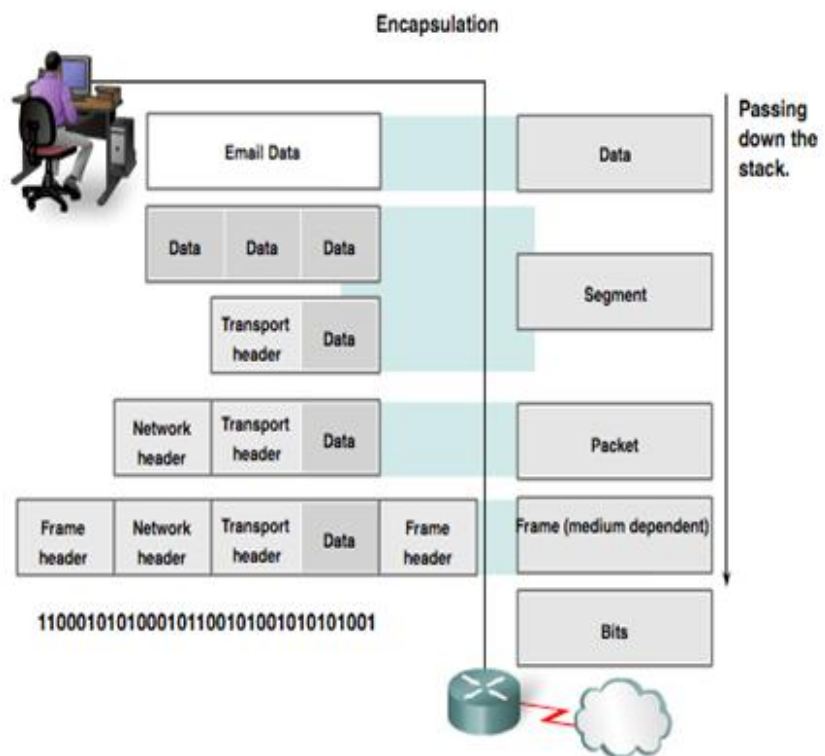
At the physical layer, binary expressions (that is, a series of 1s and 0s) represent data. However, bits are grouped together, into what is known as a protocol data unit (PDU) or a data service unit. However, PDUs might have an additional name, depending on their OSI layer. A Figure illustrates these PDU names.



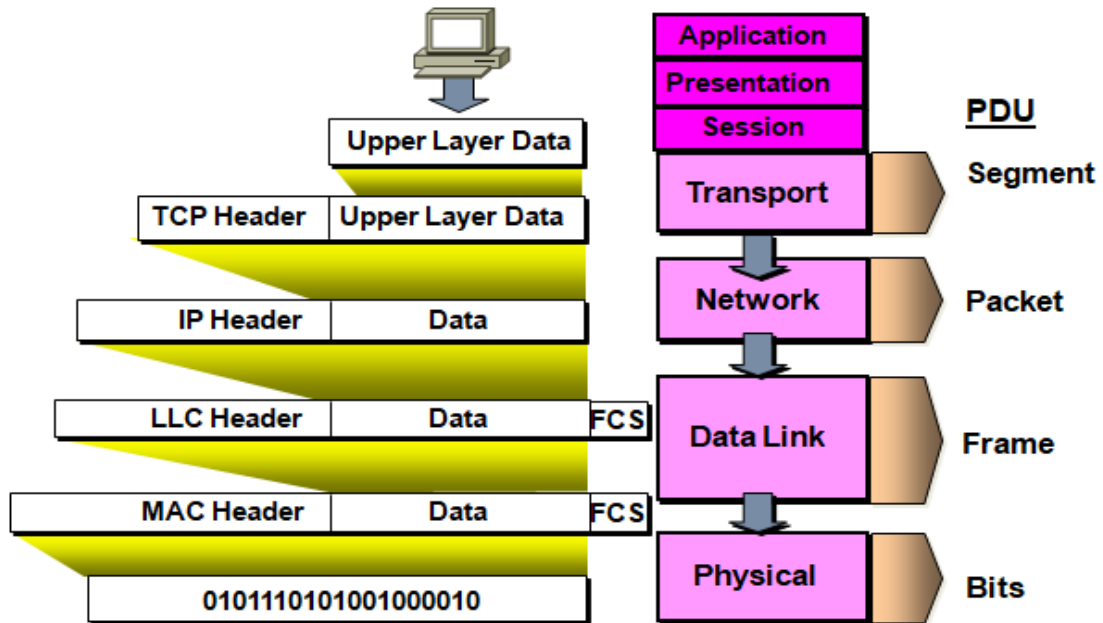
# Protocol data unit (PDU) cont



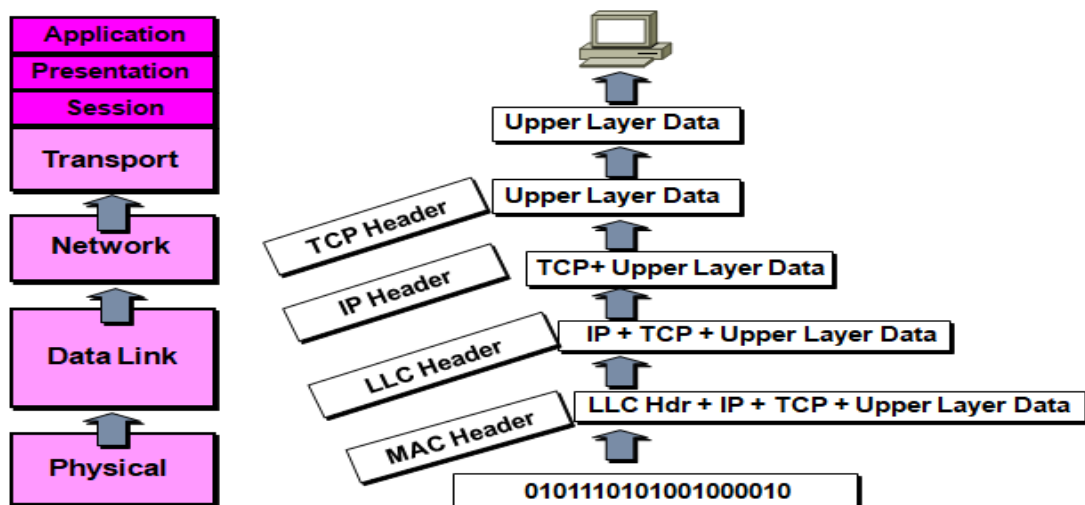
## Data Encapsulation Protocol Data Units (PDUs)



# Encapsulating Data



# De-encapsulating Data





# Chapter 6 ☺✍

## *TCP/IP model*

ABDELSALAM SALEH ELRASHDI

Networking fundamentals



## Chapter 6 ☺✍

### Outlines



- TCP/IP model
- Application layer
- Application protocols
- Types of server services
- TCP and UDP header
- Similarities between TCP/IP model and OSI model
- Differences between OSI model and TCP/IP model
- Ip header
- Broadcast and collision domain

---

### Objectives

*By end of this lecture the student will be able :*

- Define the TCP/IP model
- Similarities between TCP/IP model and OSI model
- Explain the functions of the TCP and UDP.
- List and describe the protocols at application layer.
- Explain the functions of application, transport and network layer.
- ARP and RARP protocol
- ICMP
- Identified broadcast and collision

## *The Transmission Control Protocol/Internet*

Protocol (TCP/IP) TCP/IP Suite was created by the Department of Defense (DoD) to ensure and preserve data integrity, as well as to maintain communications in the event of catastrophic war. So it follows that if designed and implemented correctly, a TCP/IP network can truly be a solid, dependable, and resilient network solution. • TCP/IP first came on the scene in 1973. Later, in 1978, it was divided into two distinct protocols: TCP and IP. Then, back in 1983, TCP/IP replaced the Network Control Protocol. • In March 1982, the US Department of Defense declared TCP/IP as the standard for all military computer networking In the same year, NORSAR and Peter Kirstein's research group at University College London adopted the protocol. The migration of the ARPANET to TCP/IP was officially completed on flag day January 1, 1983, when the new protocols were permanently activated.

---

### *History of TCP/IP*

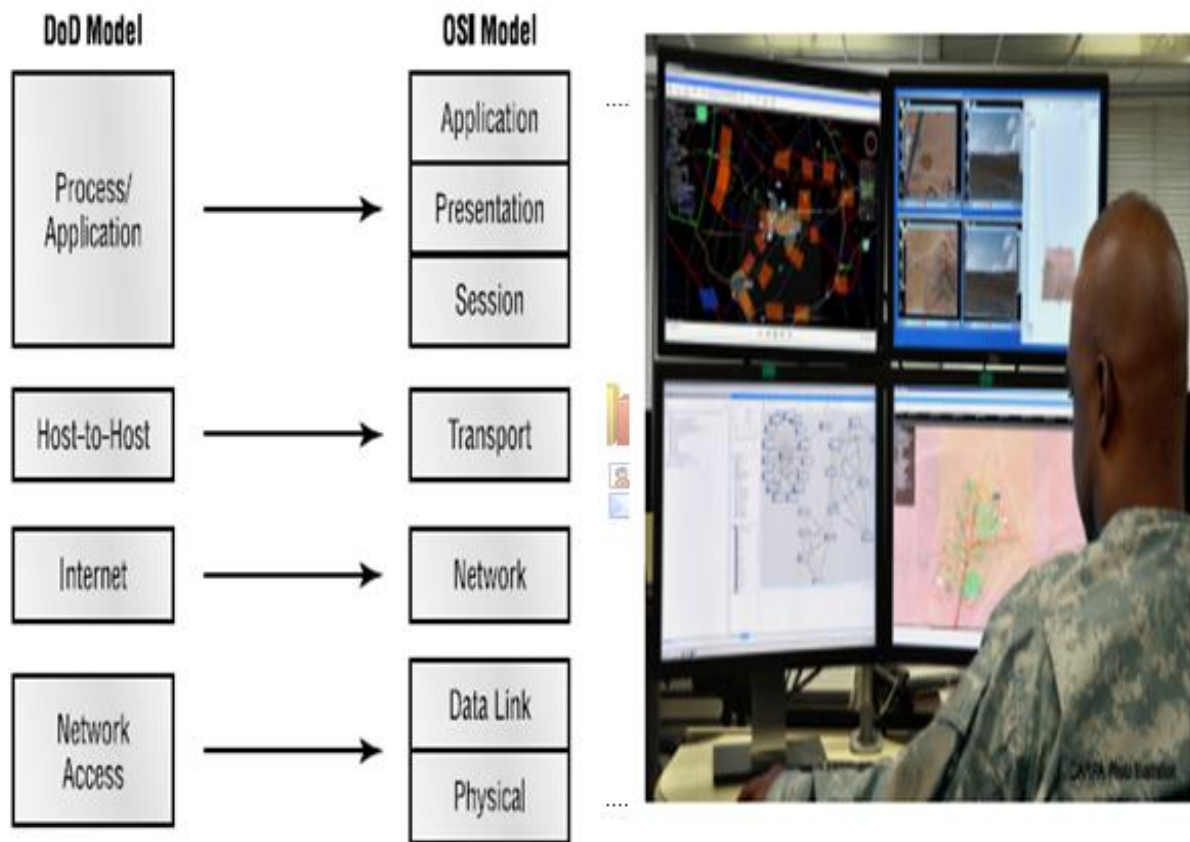
The Internet protocol suite is the conceptual model and set of communications protocols used in the Internet and similar computer networks. It is commonly known as TCP/IP because the foundational protocols in the suite are the Transmission Control Protocol (TCP) and the Internet Protocol (IP). During its development, versions of it were known as the Department of Defense (DoD) model because the development of the networking method was funded by the United States Department of Defense through DARPA " Defense Advanced Research Projects Agency". Its implementation is a protocol stack. he Defense Advanced Research Projects Agency is a US Department of Defense agency responsible for developing emerging technologies for military use. The agency was originally known as the Advanced Research Projects Agency, and was established by President Dwight Eisenhower in February 1958 in response to the Soviet launch of the Sputnik 1 satellite in 1957.



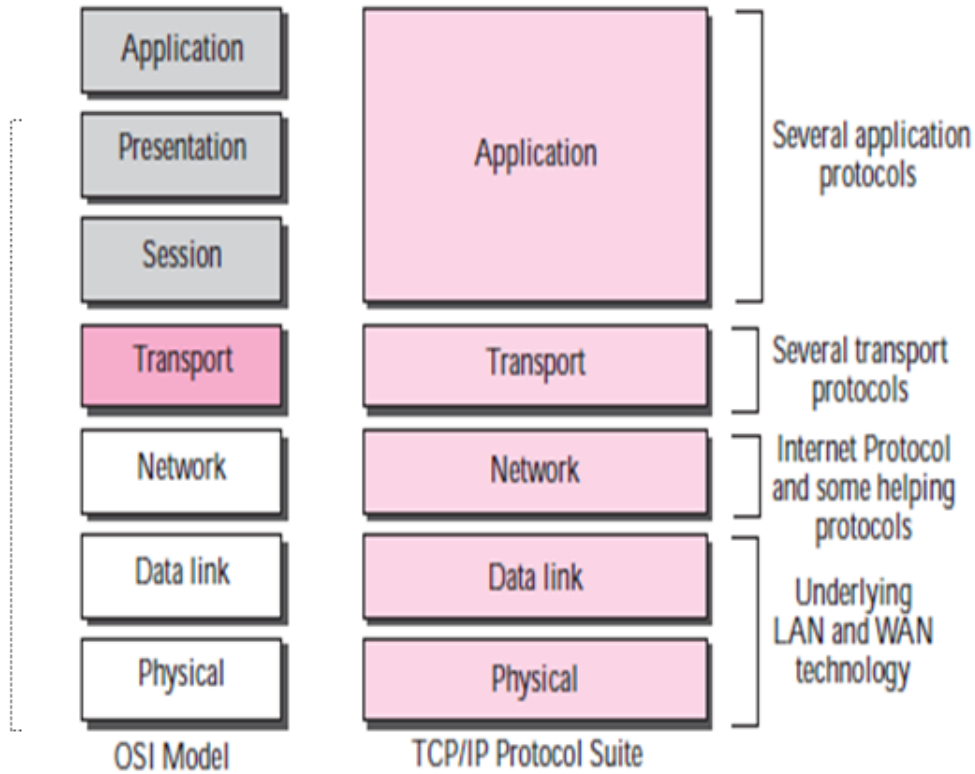
# History of TCP/IP

• The Internet protocol suite resulted from research and development conducted by the (DARPA) in the late 1960s After initiating the pioneering ARPANET in 1969, DARPA started work on a number of other data transmission technologies. In 1972, Robert E. Kahn joined the DARPA Information Processing Technology Office, where he worked on both satellite packet networks and ground-based radio packet networks, and recognized the value of being able to communicate across both. In the spring of 1973, Vinton Cerf, who helped develop the existing ARPANET Network Control Program (NCP) protocol, joined Kahn to work on open-architecture interconnection models with the goal of designing the next protocol generation for the ARPANET, in full Advanced Research Projects Agency Network • In March 1982, the US Department of Defense declared TCP/IP as the standard for all military computer networking.

## The DoD Model



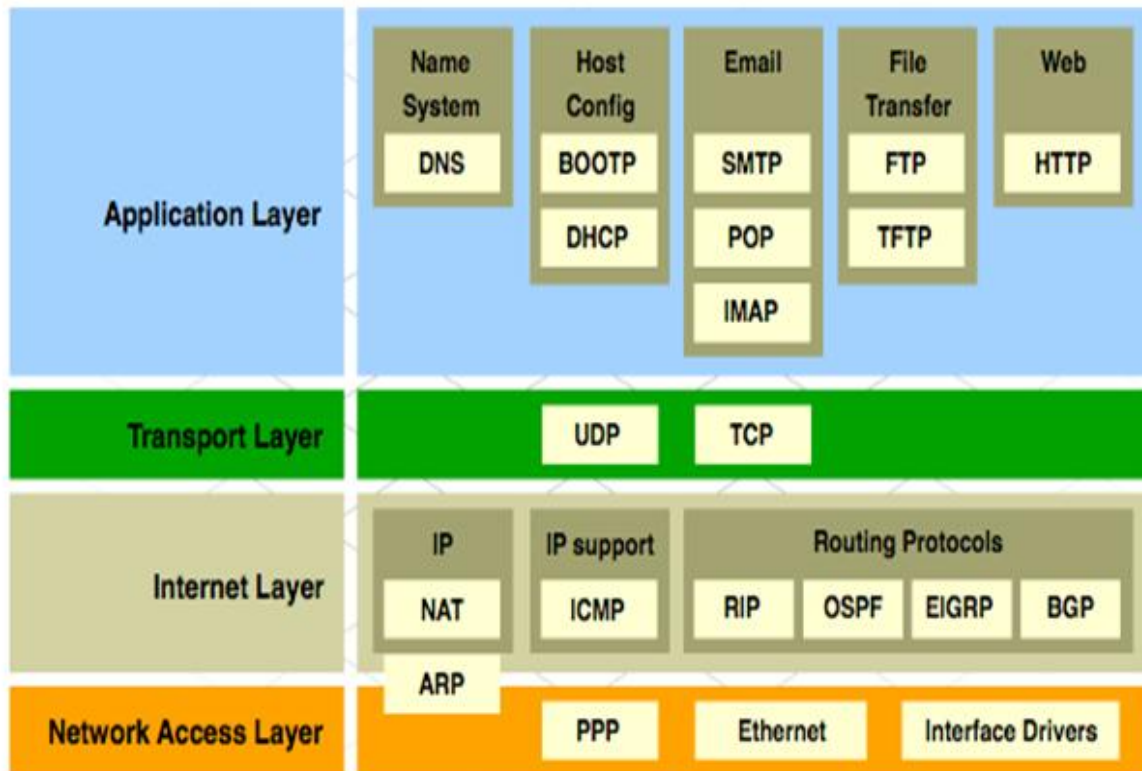
# TCP/IP Protocol Stack last update



## TCP/IP suite

<a href="#">RFC 1122</a> , Internet STD 3 (1989)	Cisco Academy <sup>[31]</sup>	Kurose, <sup>[32]</sup> Forouzan <sup>[33]</sup>	Comer, <sup>[34]</sup> Kozierok <sup>[35]</sup>	Stallings <sup>[36]</sup>	Tanenbaum <sup>[37]</sup>	Arpanet Reference Model (RFC 871)	OSI model
Four layers	Four layers	Five layers	Four+one layers	Five layers	Five layers	Three layers	Seven layers
"Internet model"	"Internet model"	"Five-layer Internet model" or "TCP/IP protocol suite"	"TCP/IP 5- layer reference model"	"TCP/IP model"	"TCP/IP 5-layer reference model"	"Arpanet reference model"	OSI model
Application	Application	Application	Application	Application	Application	Application/Process	Application Presentation Session
Transport	Transport	Transport	Transport	Host-to-host or transport	Transport	Host-to-host	Transport
Internet	Internetwork	Network	Internet	Internet	Internet		Network
Link	Network interface	Data link	Data link (Network interface)	Network access	Data link	Network interface	Data link
		Physical	(Hardware)	Physical	Physical		Physical

## TCP/IP Protocol Suite and Communication



### *OSI Model vs TCP/IP Model (which one is better and why TCP/IP is used instead of the OSI Both TCP/IP and OSI :=*

are networking reference models. Development of both models was started in early 1970s. Both were published in 1980s. Manufacturers added support for one or both in their devices in 1990s. By the end of 1990s, TCP/IP model became common choice and OSI model rejected due to slower formal standardization process in comparison of TCP/IP model. Leading manufacturers discarded their proprietary networking models in favor of TCP/IP model in 2000s. Nowadays the world of computer networking uses only one networking model and that is the TCP/IP model.

✓ *Why OSI model is still taught in networking courses?* OSI model is one of the best explained and well-documented models ever created in computer networking world. It describes complex networking concepts, protocols and terms in such a manner that is not only

easy to understand but also easier to remember. By learning one model, you can easily learn the other model. For this reason, even OSI model is no longer supported and used by hardware manufacturers, still it is taught in almost all networking courses. Since they have been already learned the foundation topics and layered approach from OSI model, learning TCP/IP model becomes much easier for them

---

### *Similarities between TCP/IP model and OSI model :=*

- Both are the logical models.
- Both define standards for networking.
- Both provide a framework for creating and implementing networking standards and devices.
- Both divide the network communication process in layers.
- In both models, a single layer defines a particular functionality and set standards for that functionality only.
- Both models allow a manufacturer to make devices and network components that can coexist and work with the devices and components made by other manufacturers.
- Both models simplify troubleshooting process by dividing complex functions into simpler components.

---

### *Differences between OSI model and TCP/IP model 13 :-*

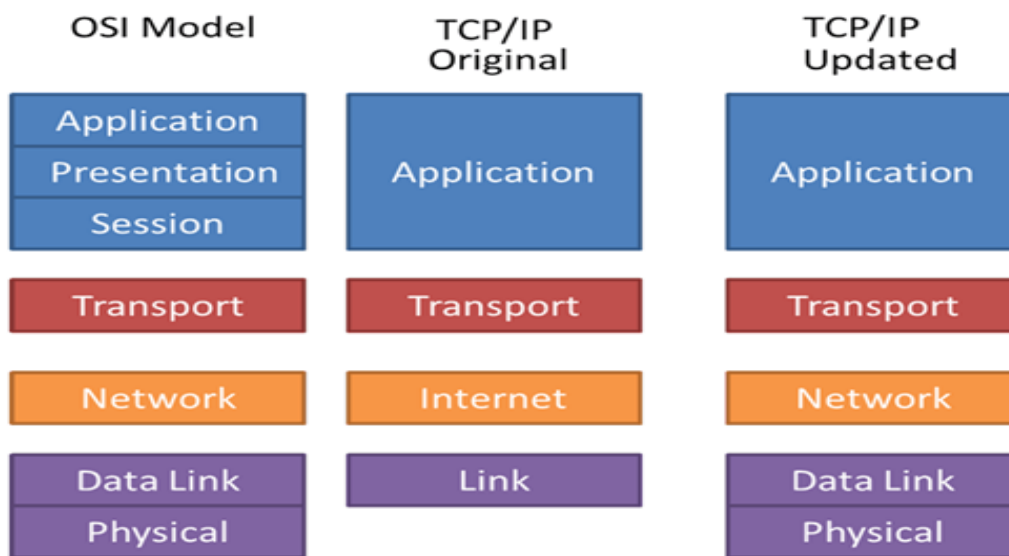
- OSI Layer model has seven layers while TCP/IP model has four layers.
- OSI Layer model is no longer used while TCP/IP is still used in computer networking.
- To define the functionality of upper layers, OSI uses three separate layers (application, presentation and session) while TCP/IP uses a single layer (application).
- Just like upper layers, OSI uses two separate layers (Physical and Data link) to define the functionality of bottom layers while TCP/IP uses a single layer (Link) for the same.
- To define the routing protocols and standards, OSI uses Network layer while TCP/IP uses Internet layer.
- In comparison of TCP/IP model, OSI model is well documented and explains standards and protocols in more details

---

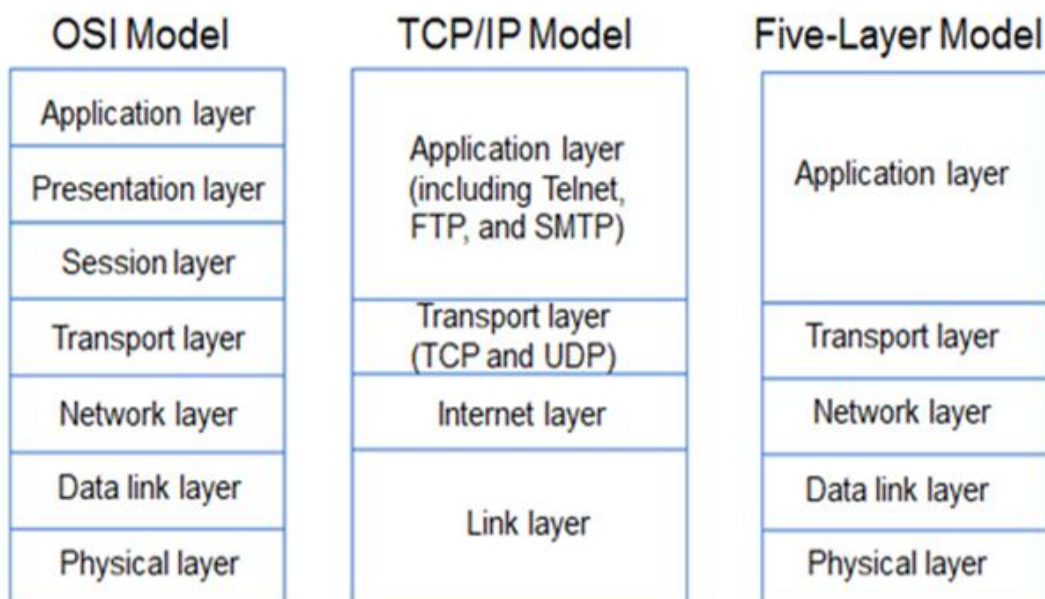
### *Differences between TCP/IP original model and TCP/IP updated model 14*

- The original TCP/IP model has four layers while the updated TCP/IP model has five layers.
- The original version uses a single layer (Link layer) to define the functionality and components which are responsible for data transmission.
- The update version uses two layers (Data Link and Physical) for this.
- The updated version divides the original Link layer based on the functionality.
- In updated version, the name of Internet layer is changed to the Network layer.

**Compares OSI Reference model with both TCP/IP original and TCP/IP updated models.**



**Compares OSI Reference model with both TCP/IP original and TCP/IP updated models cont**





## Application Layer

- It is closest layer to end user which means that both the OSI application layer and user interact directly with software application .
  - It's important to remember that the Application layer acts as an interface between application programs. this means that it deal with some applications like Microsoft Word, IE, and shard folders .
- *The Application-layer includes some protocols like :-*

**HTTP : Browsing protocol.**

**FTP : File Transfer Protocol .**

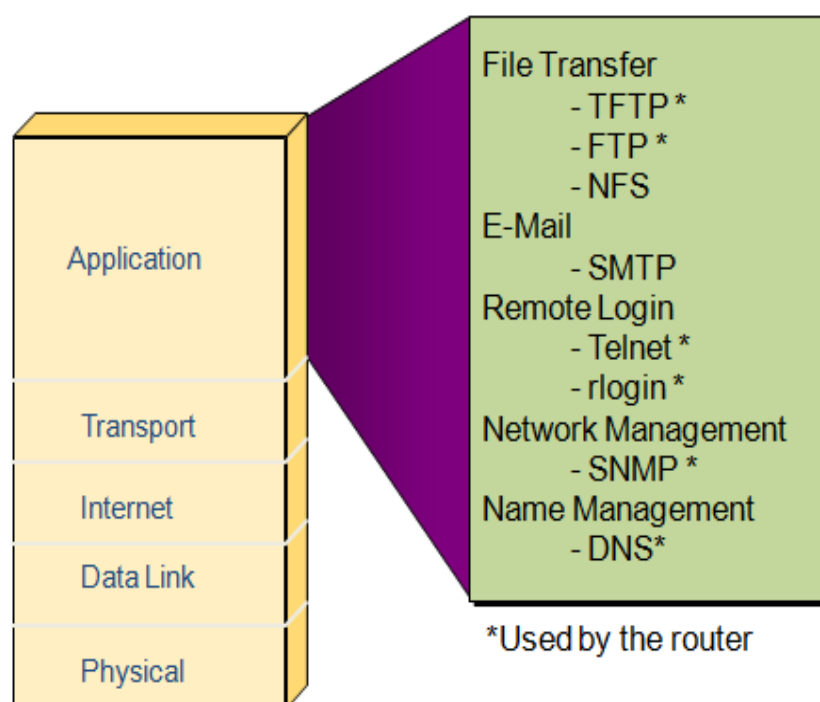
**TFTP : Trivial**

**FTP. Telnet : Remote access protocol.**

**SMTP : Simple Mail Transfer protocol .**

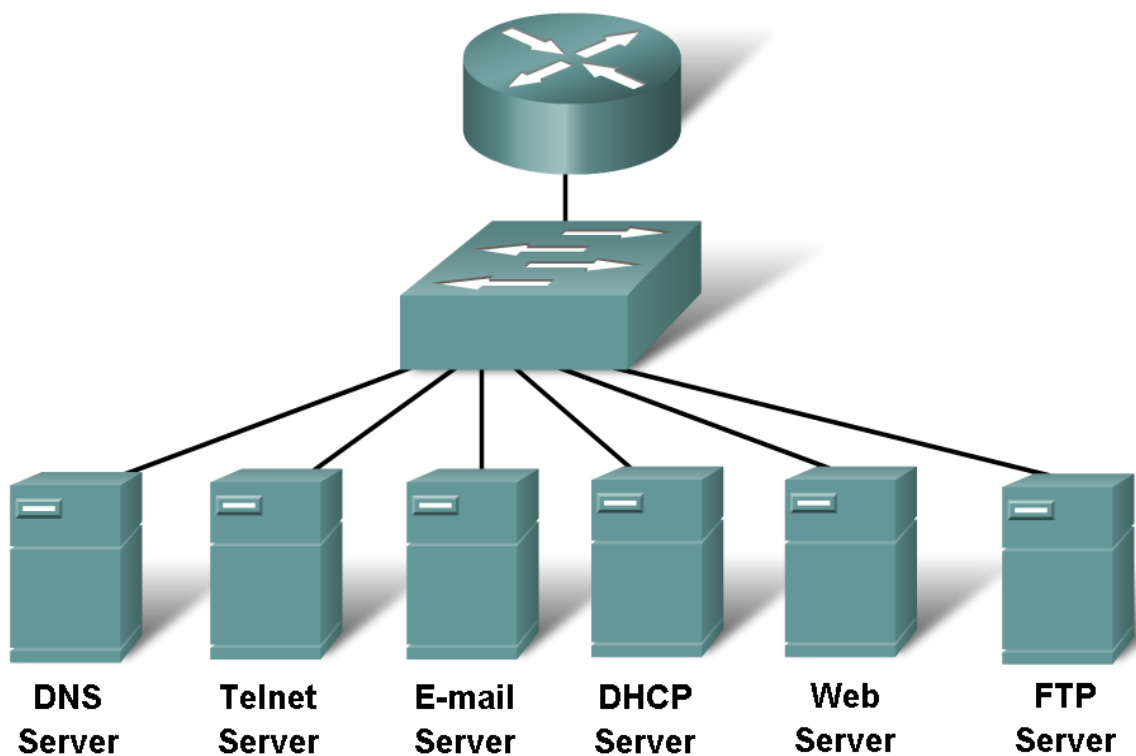
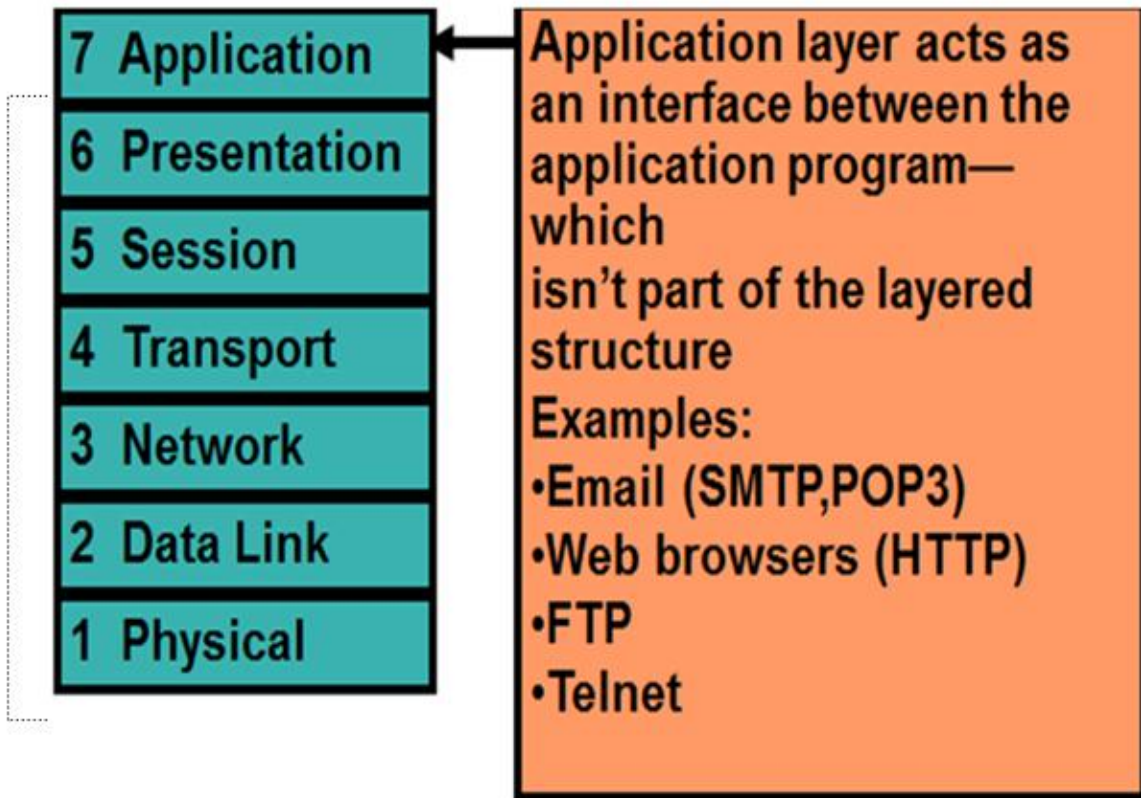
**SNMP : Simple Network Management Protocol. DNS :Domain name system DHCP :Dynamic host configuration protocol**

## Application Layer Overview





# Application Layer

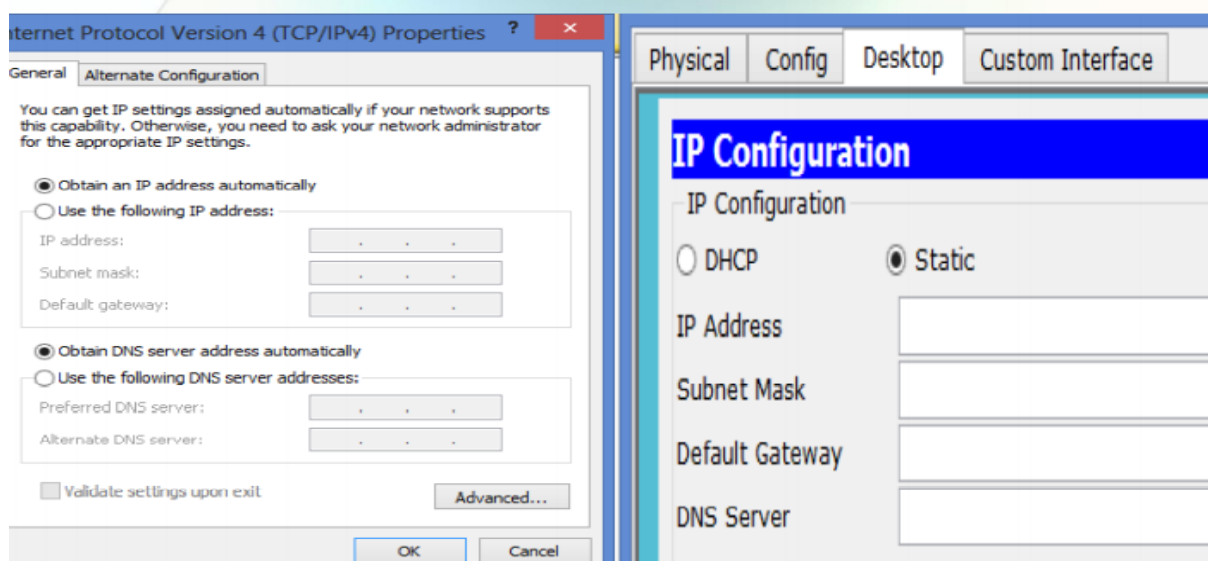
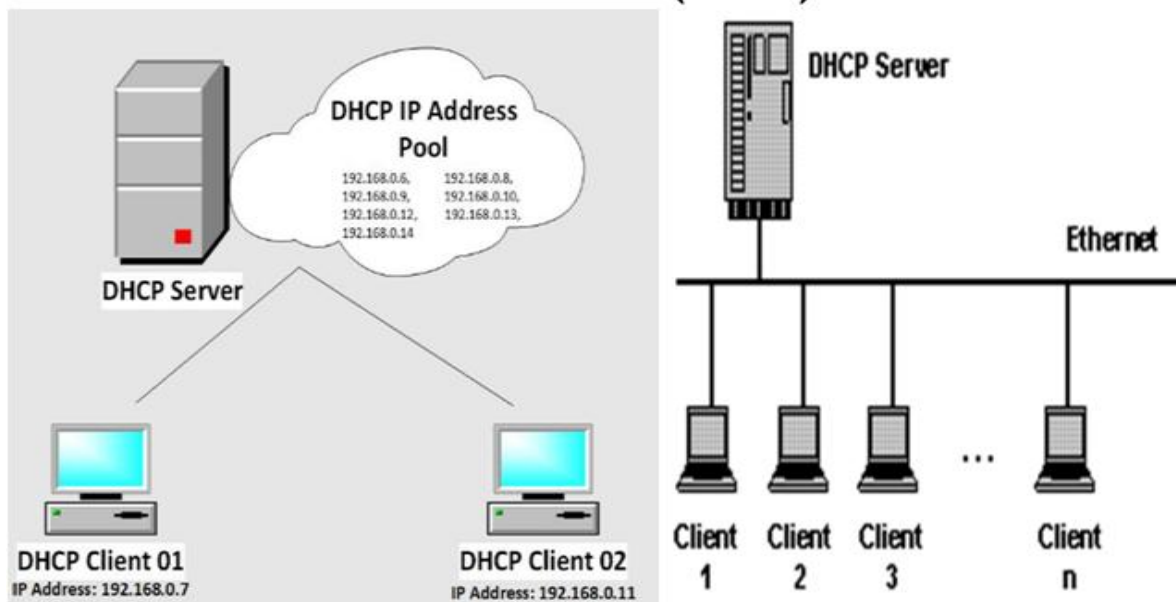


Server Farm

## DHCP server

- A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol also DHCP to respond to broadcast queries by clients.
- A DHCP server automatically sends the required network parameters for clients to properly communicate on the network. Without it, the network administrator has to manually set up every client that joins the network, which can be cumbersome, especially in large networks. DHCP servers usually assign each client with a unique dynamic IP address, which changes when the client's lease for that IP address has expired.

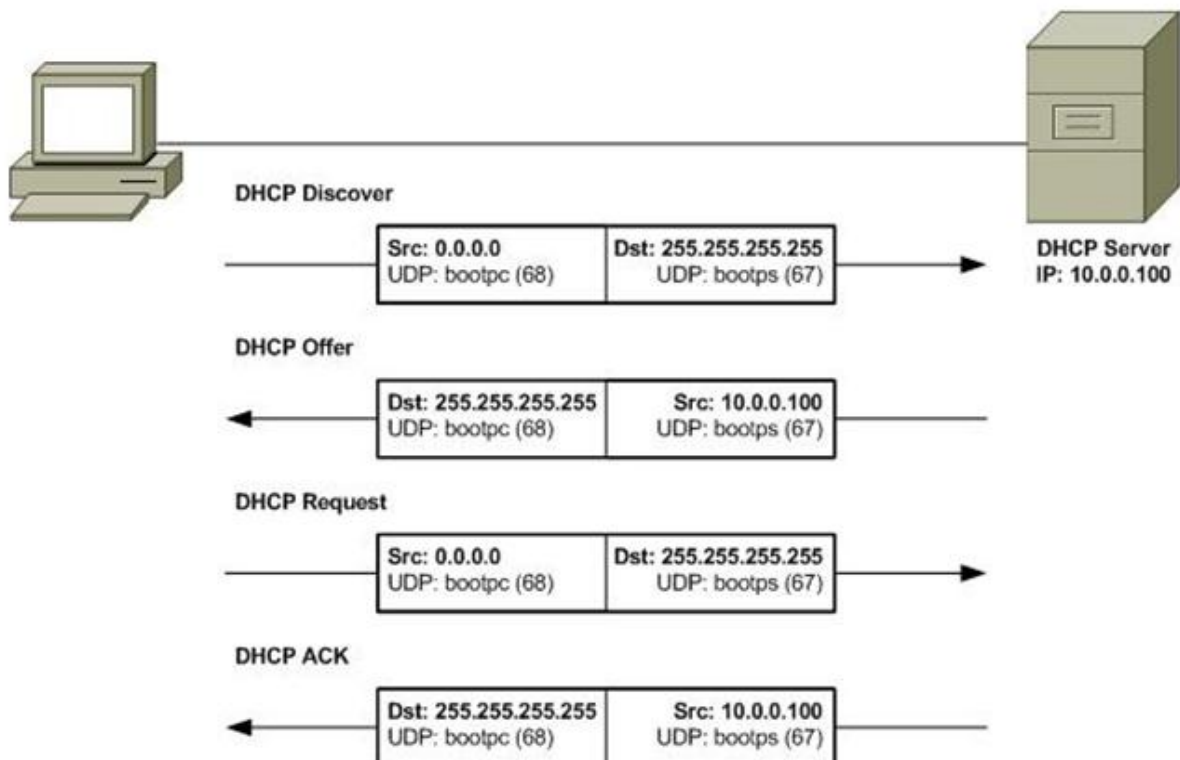
### DHCP server (cont)



# DHCP messages



## DHCP messages(cont)



## *File Transfer Protocol (FTP) And TFTP*

- File Transfer Protocol (FTP) is the protocol that actually lets you transfer files across an IP network, and it can accomplish this between any two machines using it. But FTP isn't just a protocol; it's also a program

- Trivial File Transfer Protocol (TFTP) Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it—plus it's easy to use, and it's fast too! It doesn't give you the abundance of functions that FTP does,

---

## *File Server*

- a file server is a server that provides access to files. It acts as a central file storage location that can be accessed by multiple systems.

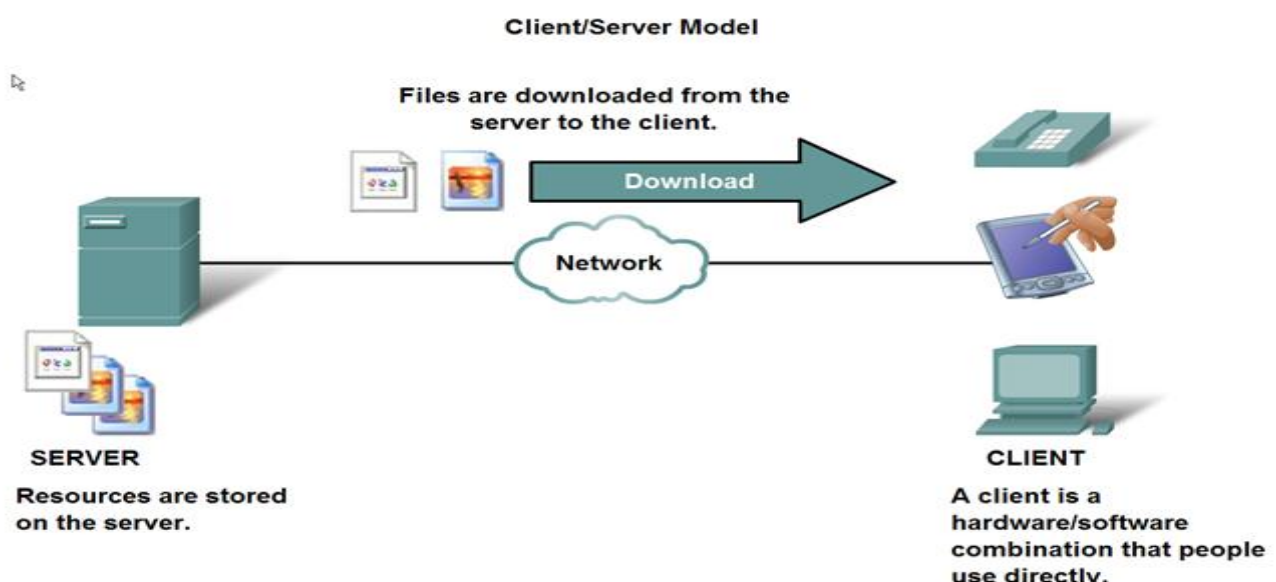
- File servers are commonly found in enterprise settings, such as company networks, but they are also used in schools, small organizations, and even home networks.

- FTP : File Transfer Protocol used to share, upload and download files.

- A file server may be a dedicated system, such as network attached storage (NAS) device, or it may simply be a computer that hosts shared files. Dedicated file servers are typically used for enterprise applications, since they provide faster data access and offer more storage capacity than non-dedicated systems. In home networks, personal computers are often used as file servers. However, personal NAS devices are also available for home users that require more storage capacity and faster performance than a non-dedicated file server would allow.

---

## **File Transfer Protocol (FTP)**

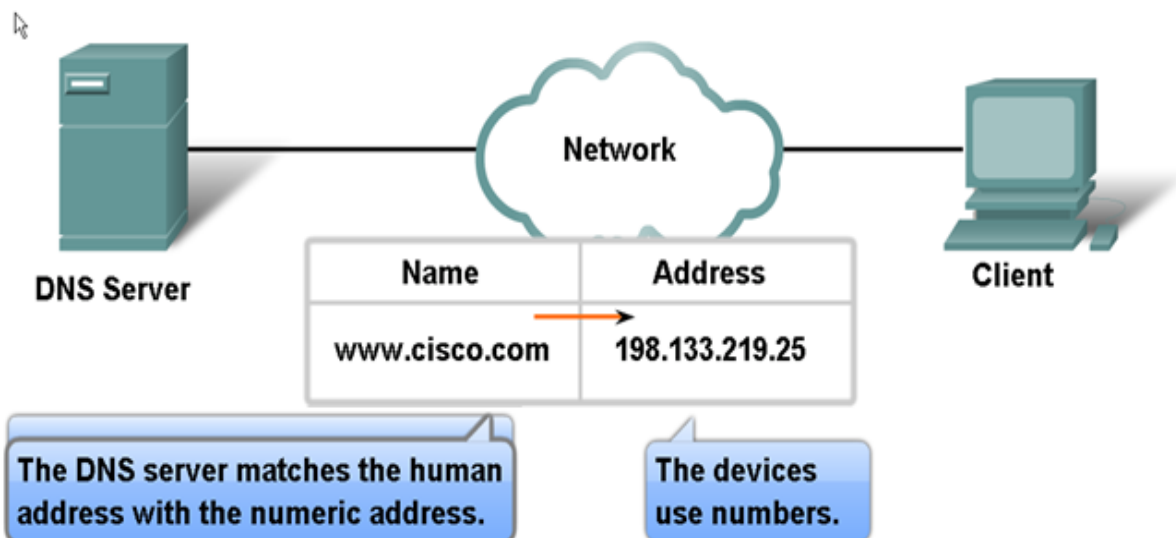


## Domain name system (DNS) server

- The Domain Name System (DNS) is the phonebook of the Internet. When users type domain names such as —google.com‖ or —LIMU.edu‖ into web browsers, DNS is responsible for finding the correct IP address for those sites. Browsers then use those addresses to communicate with origin servers. This all happens thanks to DNS servers: machines dedicated to answering DNS queries.
- A DNS server stores a database of different domain names, network names, Internet hosts, DNS records and other related data.
- The most basic function of a DNS server is to translate a domain name into its respective IP address. During a domain name resolution query, DNS records are searched, and if found, the domain name record is returned. If the domain name is not registered or added to that DNS server, the query is then passed to other DNS servers until the domain name record is found.

## Domain Name Service (DNS)

### Resolving DNS Addresses

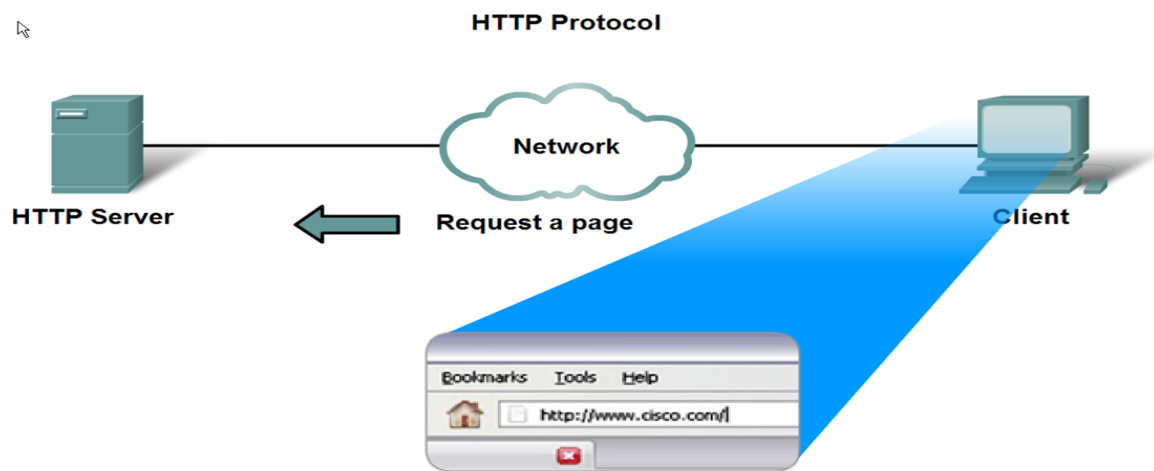


## *Hypertext Transfer Protocol (HTTP) And HTTPS*

- It's used to manage communications between web browsers and clients and opens the right resource when you click a link, wherever that resource may actually reside

### *Hypertext Transfer Protocol Secure (HTTPS)*

The Hypertext Transfer Protocol Secure (HTTPS) is also known as Secure Hypertext Transfer Protocol. Sometimes you'll see it referred to as SHTTP or S-HTTP, but no matter—as indicated, it's a secure version of HTTP that arms you with a whole bunch of security tools for keeping transactions between a web browser and a server secure

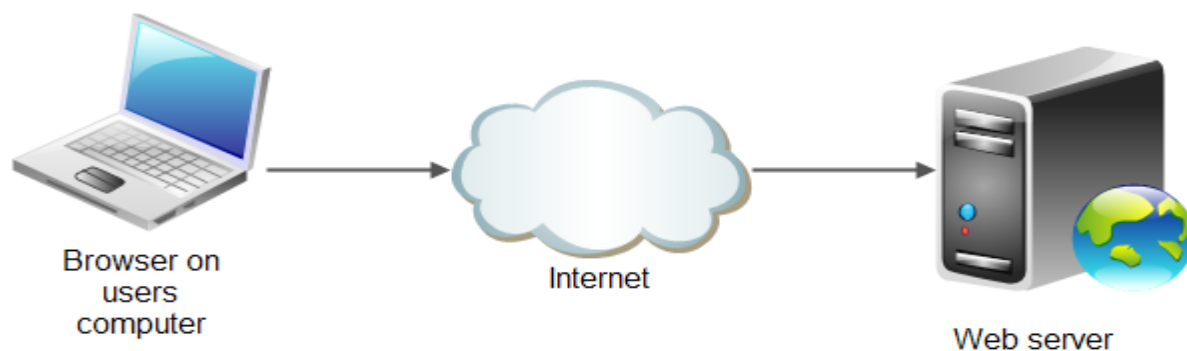


## *Web server*

- A web server is a computer that runs websites. It's a computer program that distributes web pages as they are requisition. The basic objective of the web server is to store, process and deliver web pages to the users. This intercommunication is done using Hypertext Transfer Protocol (HTTP). These web pages are mostly static content that includes HTML documents, images, style sheets, test etc. Apart from HTTP, a web server also supports SMTP (Simple Mail transfer Protocol) and FTP (File Transfer Protocol) protocol for emailing and for file transfer and storage

- A web server stores and delivers the content for a website – such as text, images, video, and application data – to clients that request it. The most common type of client is a web browser program, which requests data from your website when a user clicks on a link or downloads a document on a page displayed in the browser.





---

## *Telnet and SSH*

Telnet is the chameleon of protocols—its specialty is terminal emulation. It allows a user on a remote client machine, called the Telnet client, to access the resources of another machine, the Telnet server.

- Telnet achieves this by pulling a fast one on the Telnet server and making the client machine appear as though it were a terminal directly attached to the local network.
- This projection is actually a software image—a virtual terminal that can interact with the chosen remote host. Secure Shell (SSH)

*Secure Shell host (SSH)* protocol sets up a secure Telnet session over a standard TCP/IP connection and is employed for doing things like logging into other systems, running programs on remote systems, and moving files from one system to another.

---

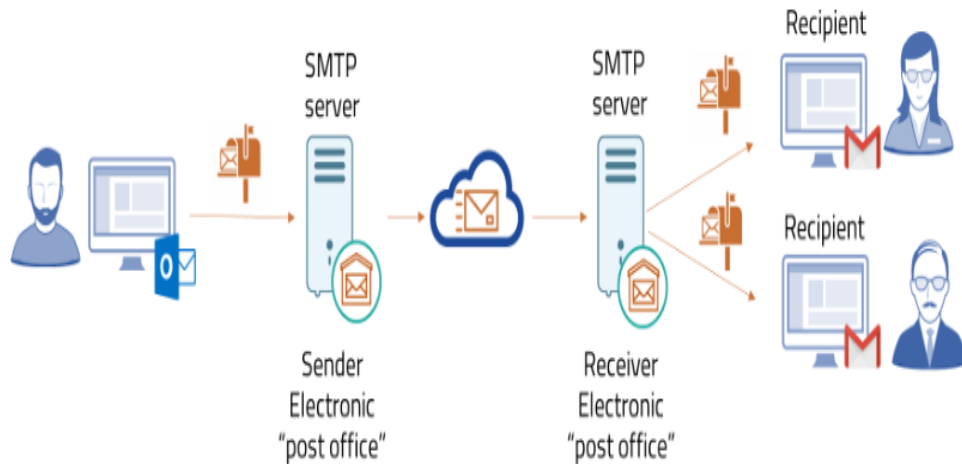
## *Simple Mail Transfer Protocol (SMTP)*

And Post Office Protocol (POP)

- Simple Mail Transfer Protocol (SMTP) , answering our ubiquitous call to email, uses a spooled, or queued, method of mail delivery. Once a message has been sent to a destination, the message is spooled to a device—usually a disk. The server software at the destination posts a vigil, regularly checking the queue for messages. When it detects them, it proceeds to deliver them to their destination.

- SMTP is used to send mail; POP3 is used to receive mail.

- Post Office Protocol (POP) gives us a storage facility for incoming mail, and the latest version is called POP3 (sound familiar?). Basically, how this protocol works is when a client device connects to a POP3 server, messages addressed to that client are released for downloading. It doesn't allow messages to be downloaded selectively

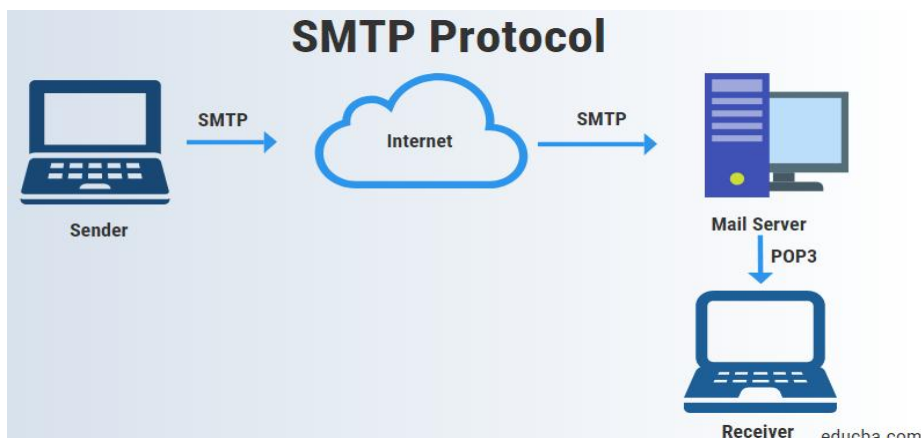


### *E-mail server*

- A remote or central computer that holds electronic mail (e-mail) messages for clients on a network is called a mail server. A mail server is similar to the post office, where mail is stored and sorted before being sent to its final destination. When the user requests his or her e-mail, contact is established with the mail server, which then delivers all stored to the client's computer.

## *Simple Network Management Protocol (SNMP) :-*

Simple Network Management Protocol (SNMP) collects and manipulates valuable network information. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information

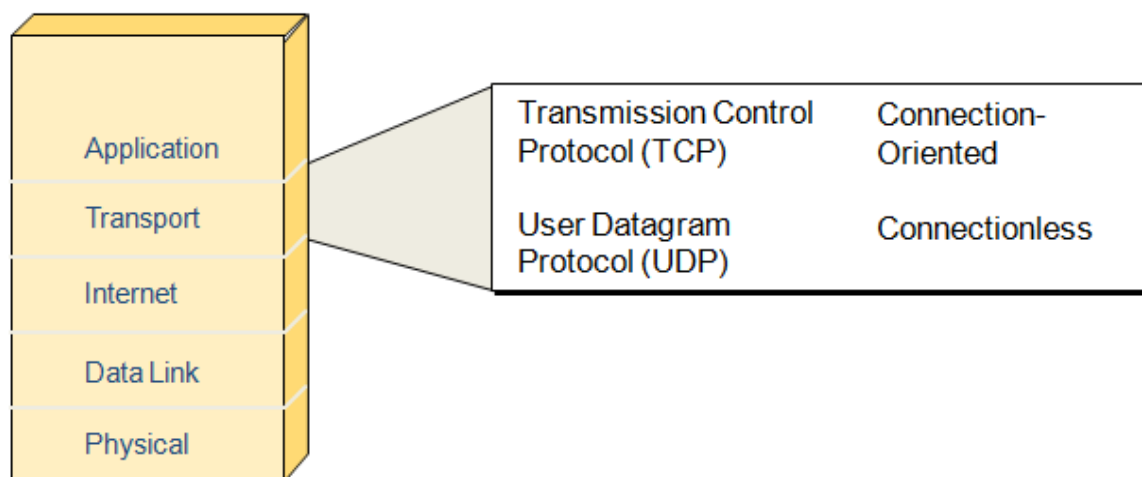


## *Transport layer or host to host Layer*

The main purpose of the Host-to-Host layer is to shield the upper-layer applications from the complexities of the network. This layer says to the upper layer, “Just give me your data stream, with any instructions, and I’ll begin the process of getting your information ready to send.” The following sections describe the two protocols at this layer:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

## Transport Layer Overview



---

## *TCP And UDP*

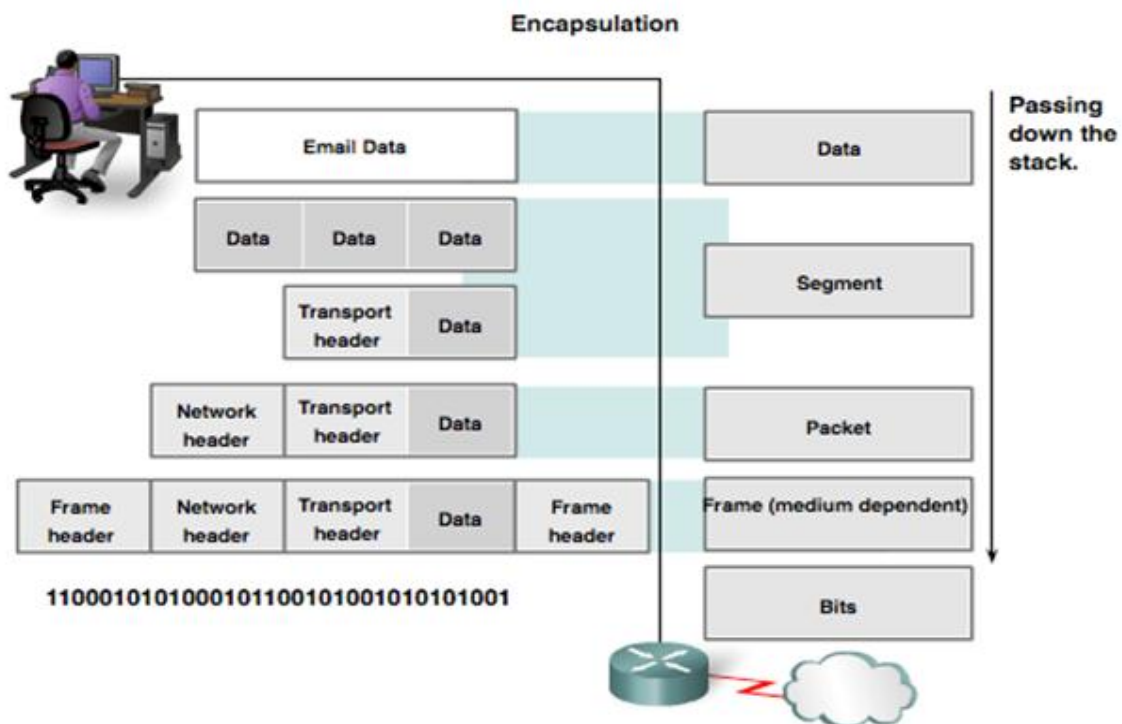
Transmission Control Protocol (TCP) the sender’s TCP process contacts the destination’s TCP process to establish a connection. What is created is known as a virtual circuit.

- This type of communication is called connection-oriented.
  - It must establish session before transmit the data , make recovery&control
- User Datagram Protocol (UDP)
- UDP doesn’t create a virtual circuit, nor does it contact the destination before delivering information to it.
  - this, type of communication is called considered a connectionless protocol.
  - UDP connectionless protocol no session,no recovery&no control
-

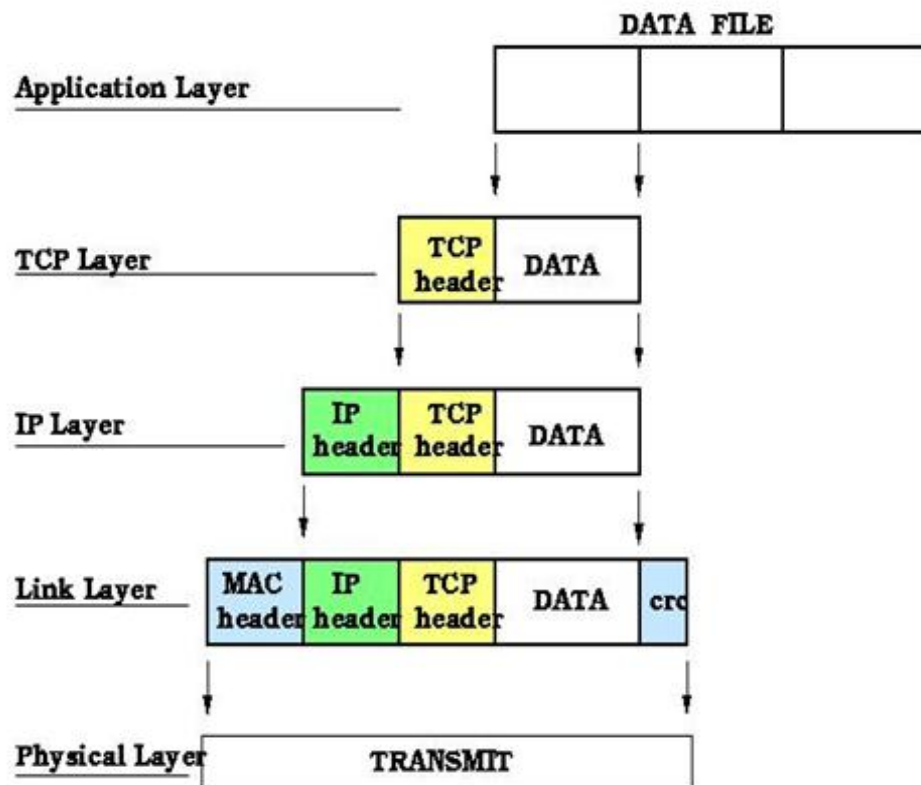
# TCP And UDP

TCP	UDP
Sequenced	Unsequenced
Reliable	Unreliable
Connection-oriented	Connectionless
Virtual circuit	Low overhead
Acknowledgments	No acknowledgment
Windowing flow control	No windowing or flow control

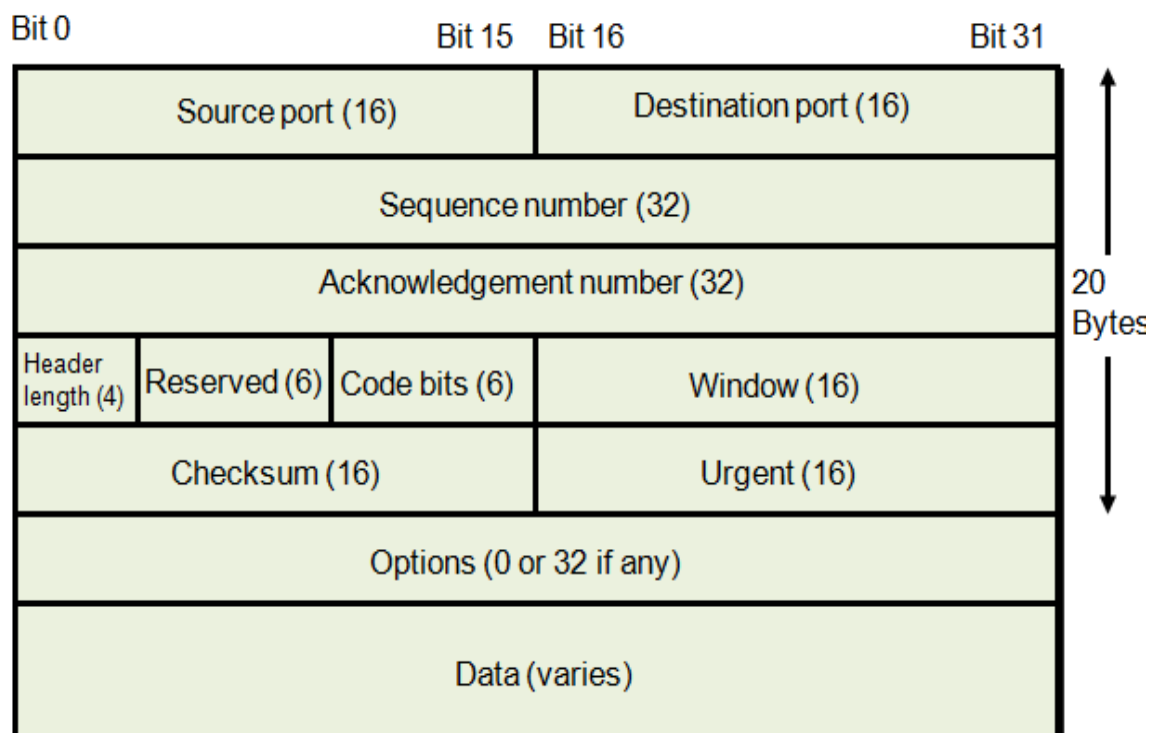
## Data Encapsulation



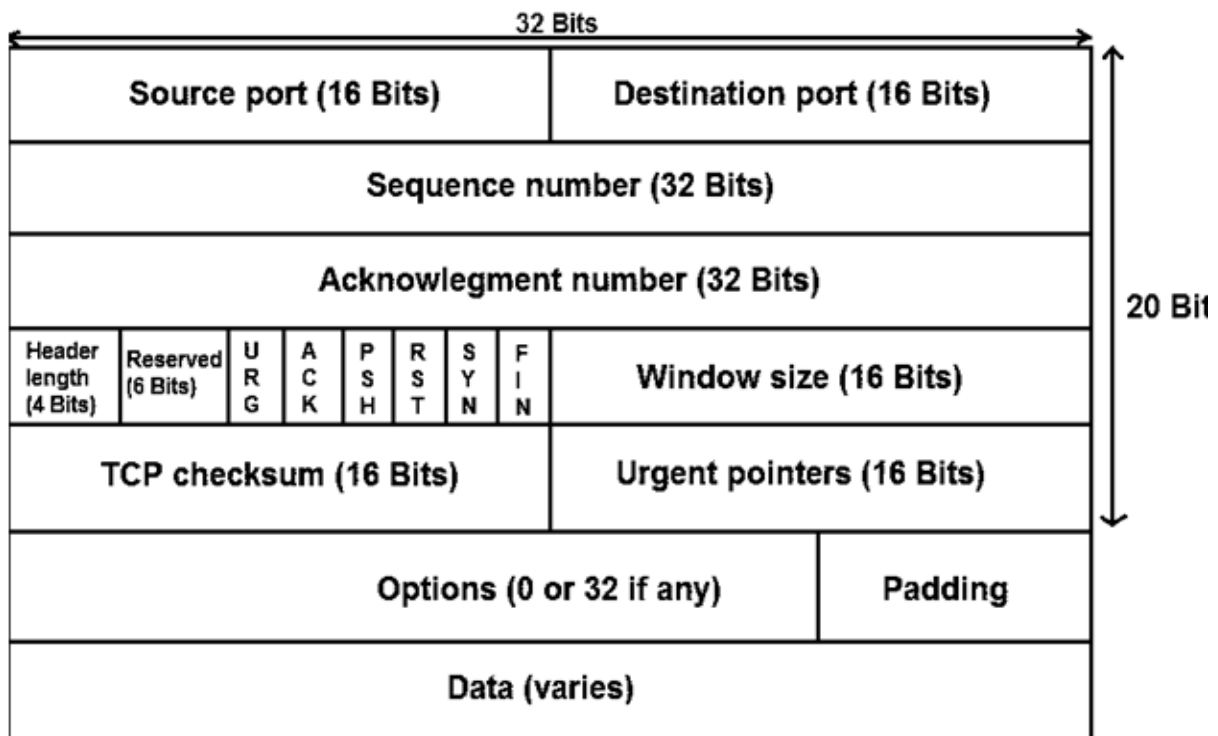
# Data Encapsulation cont



## TCP Segment Format



## TCP Segment Format



### *TCP Header*

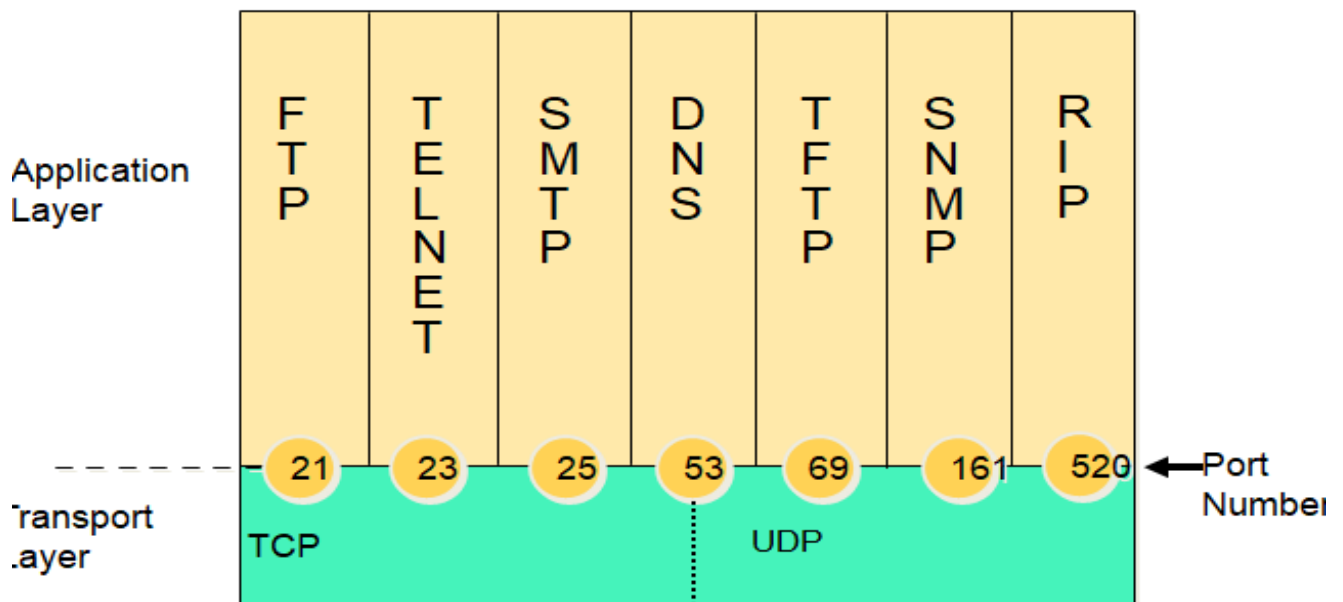
- Source port The port number of the application on the host sending the data. (Port numbers will be explained a little later in this section.)
- Destination port The port number of the application requested on the destination host.
- Sequence number A number used by TCP that puts the data back in the correct order or retransmits missing or damaged data, a process called sequencing.
- Acknowledgment number The TCP octet that is expected next.
- Header length The number of 32-bit words in the TCP header. This indicates where the data begins. The TCP header (even one including options) is an integral number of 32 bits in length.
- Reserved Always set to zero.
- Code bits Control functions used to set up and terminate a session.
- Window The window size the sender is willing to accept, in octets.
- Checksum The cyclic redundancy check (CRC), because TCP doesn't trust the lower layers and checks everything. The CRC checks the header and data fields.
- Urgent A valid field only if the Urgent pointer in the code bits is set. If so, this



value indicates the offset from the current sequence number, in octets, where the first segment of non-urgent data begins.

- Options May be 0 or a multiple of 32 bits, if any. What this means is that no options have to be present (option size of 0). However, if any options are used that do not cause the option field to total a multiple of 32 bits, padding of 0s must be used to make sure the data begins on a 32-bit boundary. Data Handed down to the TCP protocol at the Transport layer, which includes the upperlayer headers.

## Port Numbers

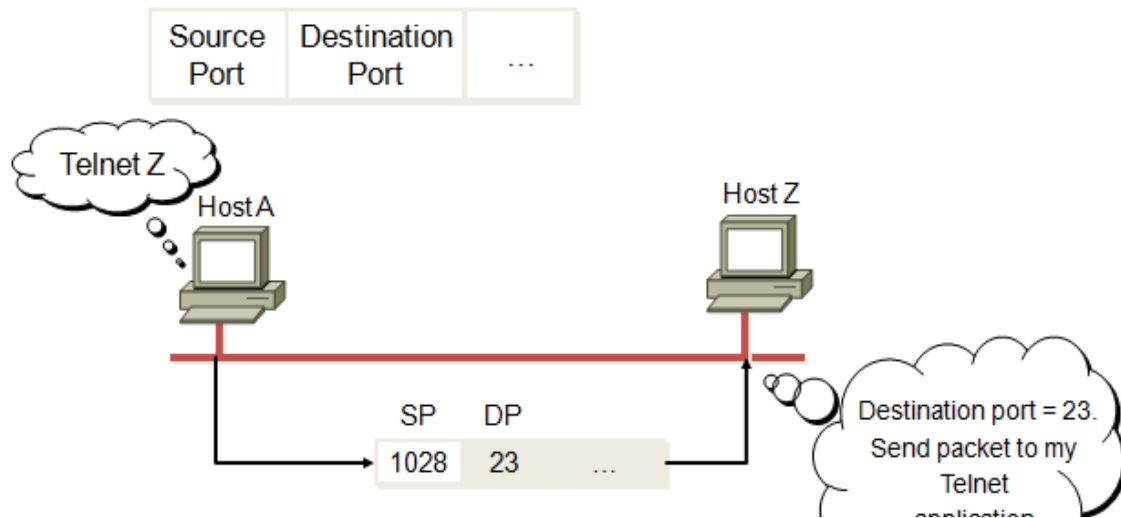


### Port Numbers

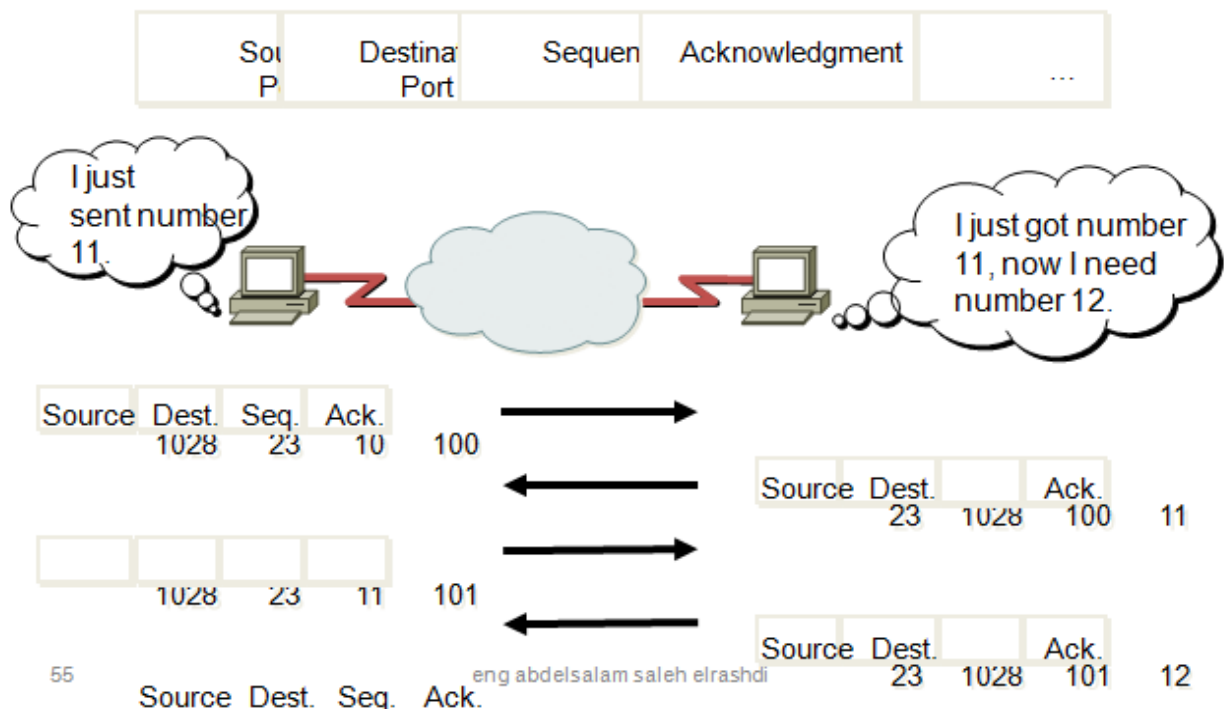
- TCP and UDP must use port numbers to communicate with the upper layers because they're what keep track of different conversations crossing the network simultaneously. Originating source. The port number divided into three ranges:
  - 1-The well known ports those in the ranges 0 –1023
  - 2-Used defined included
    - the registered port range 1024 ---49151
    - the dynamic and/or private ports range 49152---65535
- randomly chosen port numbers out of this range called Ephemeral port . These ports are not permanently assigned to any public defined application
- There are 65535 port number in computer 16 bit.

- port numbers are dynamically assigned by the source host and will equal some number starting at 1024.
- 1023 and below are defined in RFC 3232 (or just see [www.iana.org](http://www.iana.org)), which discusses what are called well-known port numbers.

## TCP Port Numbers

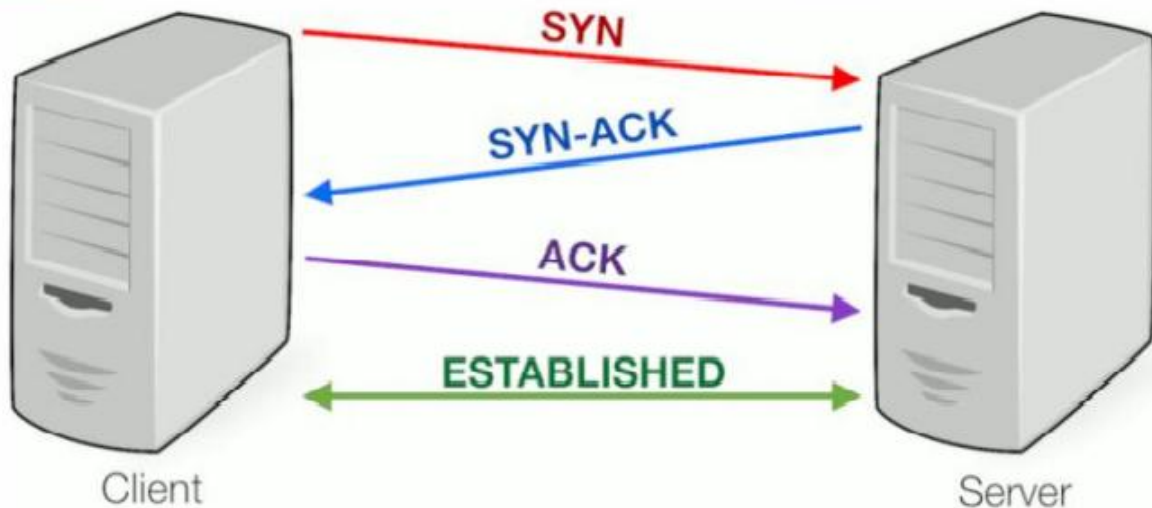


## TCP Sequence and Acknowledgment Numbers

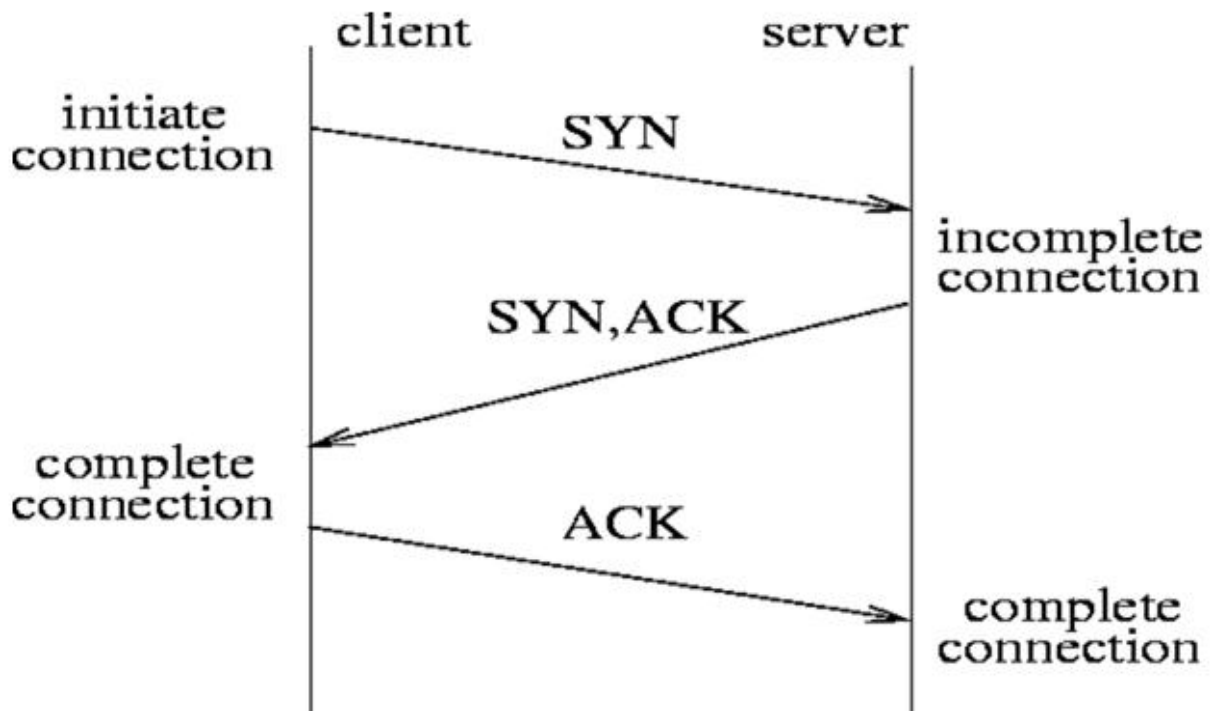


## Three way handshake

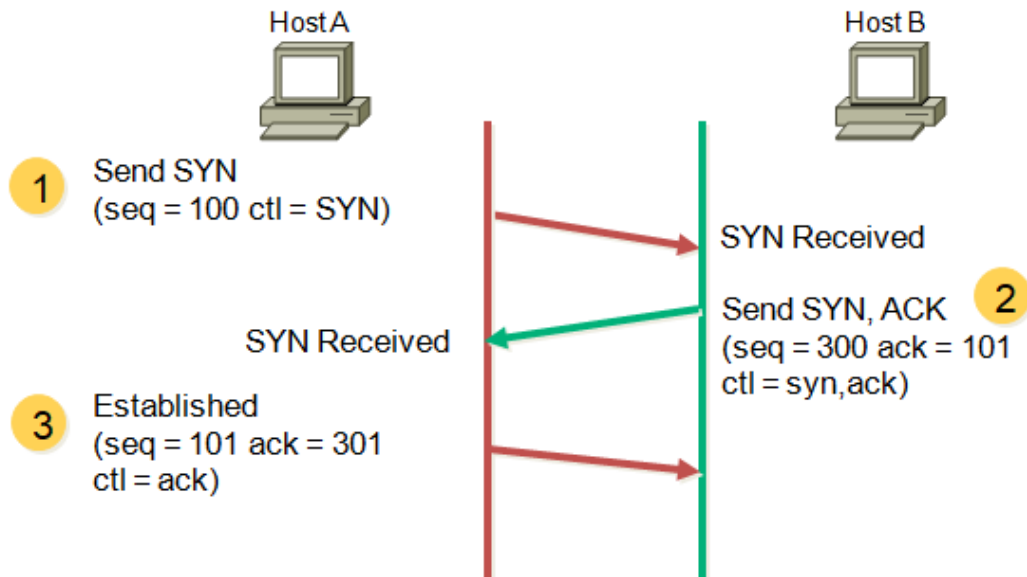
A three-way handshake (or TCP handshake) is a method used in a TCP/IP network to create a connection between a local host/client and server. It is a three-step method that requires both the client and server to exchange SYN and ACK (acknowledgment) packets before actual data communication begins.



## TCP Three-Way Handshake/Open Connection cont



## TCP Three-Way Handshake/Open Connection

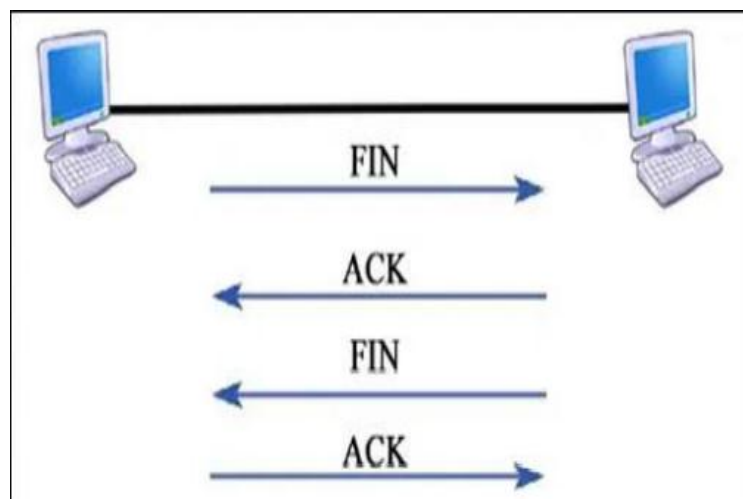


### *This is how the TCP 3-way handshake works:*

- A client node sends a SYN data packet over an IP network to a server on the same or an external network. The objective of this packet is to ask/infer if the server is open for new connections.
- The target server must have open ports that can accept and initiate new connections. When the server receives the SYN packet from the client node, it responds and returns a confirmation receipt – the ACK packet or SYN/ACK packet
- The client node receives the SYN/ACK from the server and responds with an ACK packet.

### *Four way handshake*

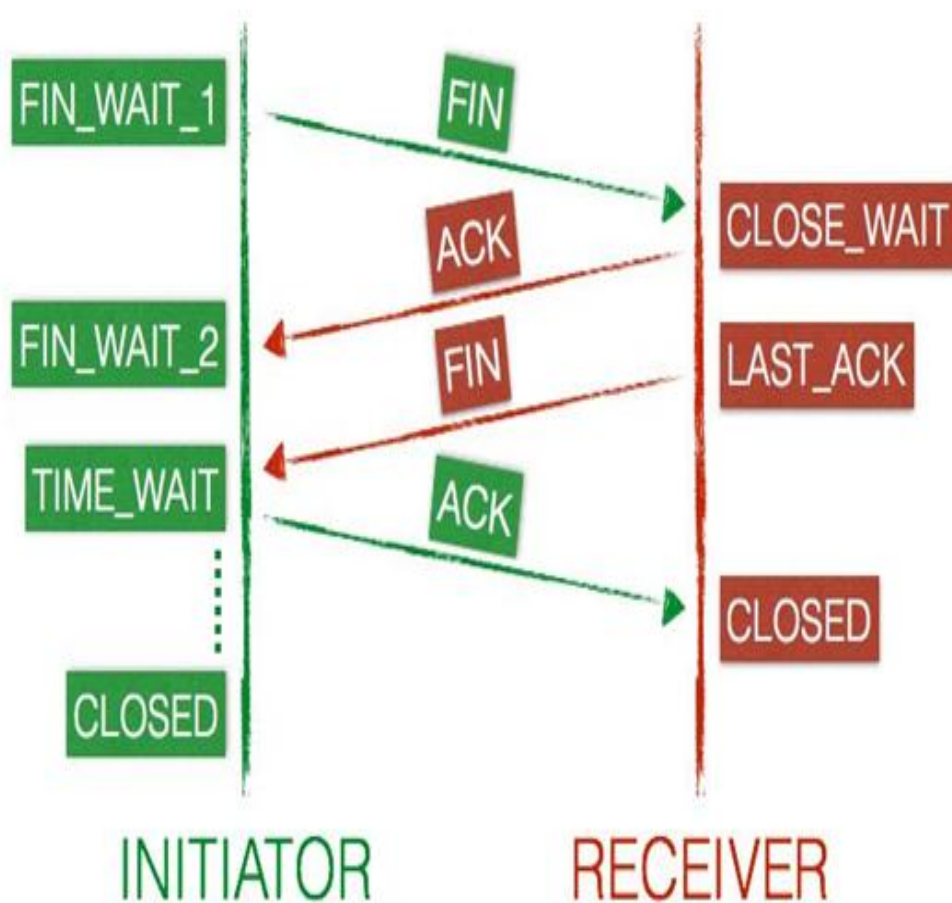
- The four-way disconnect is the method used in a TCP/IP network to close the connection between a client and a server.



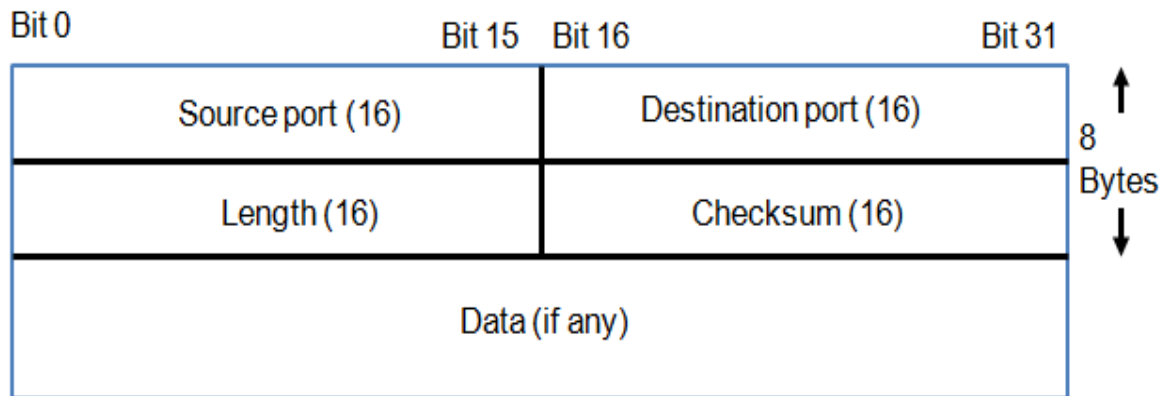
This is how the TCP 4-way disconnect works:

- The client sends a FIN packet to the server and updates its state to FIN\_WAIT\_1
- The server receives the termination request from the client, responds with ACK and moves to CLOSE\_WAIT
- The client receives the reply from the server and will go to FIN\_WAIT\_2
- The server is in CLOSE\_WAIT and will follow up with FIN, which updates the state to LAST\_ACK
- The client receives the termination request and replies with an ACK, which results in a TIME\_WAIT state
- The server is finished and sets connection to CLOSED
- The client stays in TIME\_WAIT for a maximum of 4 minutes before setting the connection to CLOSED

## Four way handshake

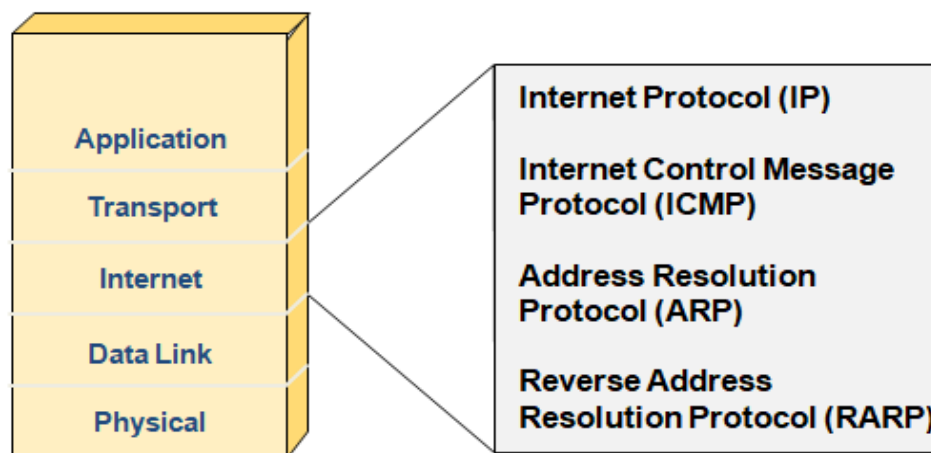


# UDP Segment Format



No sequence or acknowledgment fields •

## Internet Layer Overview



OSI network layer corresponds to the •  
TCP/IP internet layer



## *Address Resolution Protocol (ARP)*

- Address Resolution Protocol (ARP) finds the hardware address of a host from a known IP address. Here's how it works: When IP has a datagram to send, it must inform a Network Access protocol, such as Ethernet or Token Ring, of the destination's hardware address on the local network. (It has already been informed by upper-layer protocols of the destination's IP address.) If IP doesn't find the destination host's hardware address in the ARP cache, it uses ARP to find this information

---

## *Reverse Address Resolution Protocol (RARP)*

- When an IP machine happens to be a diskless machine, it has no way of initially knowing its IP address. But it does know its MAC address. Reverse Address Resolution Protocol (RARP) discovers the identity of the IP address for diskless machines by sending out a packet that includes its MAC address and a request for the IP address assigned to that MAC address.

---

## *Internet Control Message Protocol (ICMP)*

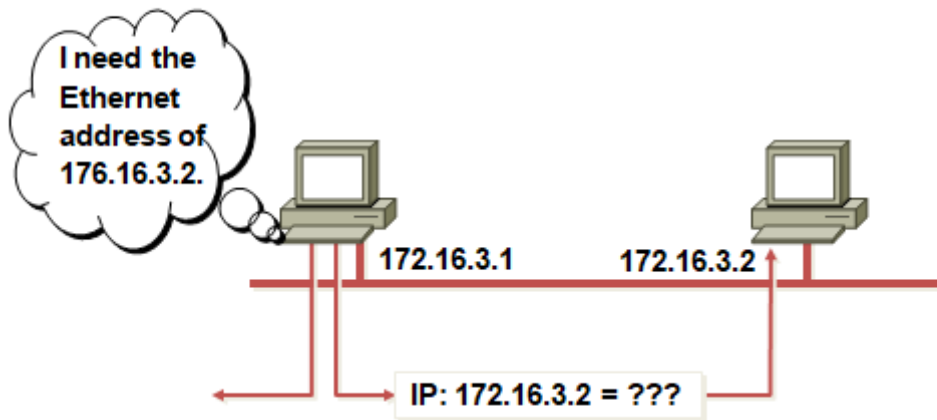
- Internet Control Message Protocol (ICMP) works at the Network layer and is used by IP for many different services. ICMP is a management protocol and messaging service provider for IP. Its messages are carried as IP datagrams.
- RFC 1256 is an annex to ICMP, ICMP packets have the following characteristics:
  - They can provide hosts with information about network problems.
  - They are encapsulated within IP datagrams.

---

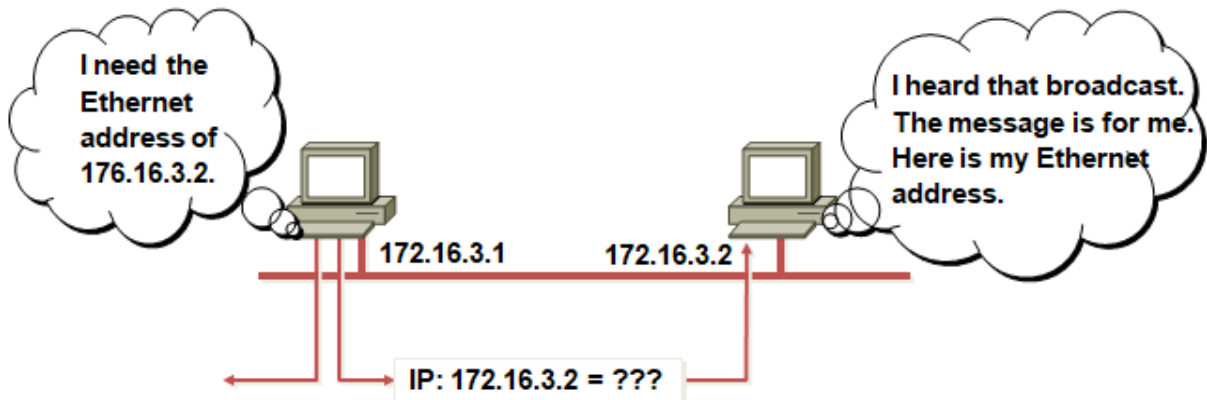
## *Internet Control Message Protocol (ICMP)*

- Ping Packet Internet Groper (Ping) uses ICMP echo request and reply messages to check the
  - physical and logical connectivity of machines on an internetwork.
  - Traceroute Using ICMP time-outs, Traceroute is used to discover the path a packet takes as
    - it traverses an internetwork.

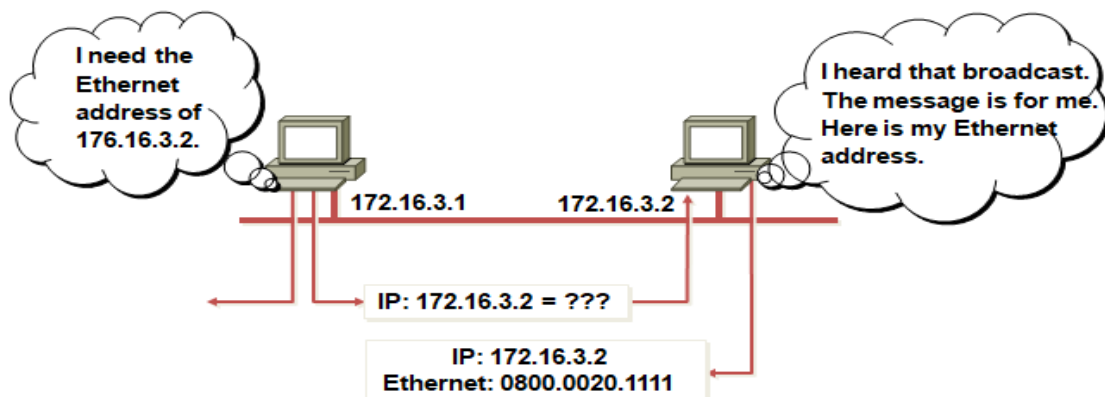
# Address Resolution Protocol



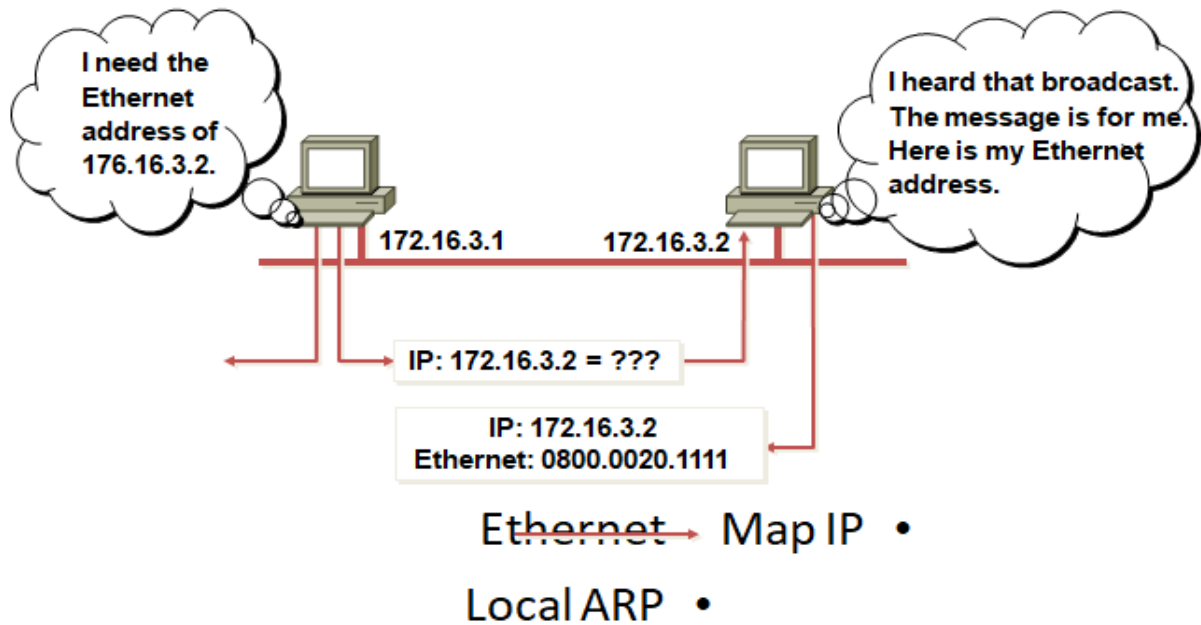
# Address Resolution Protocol



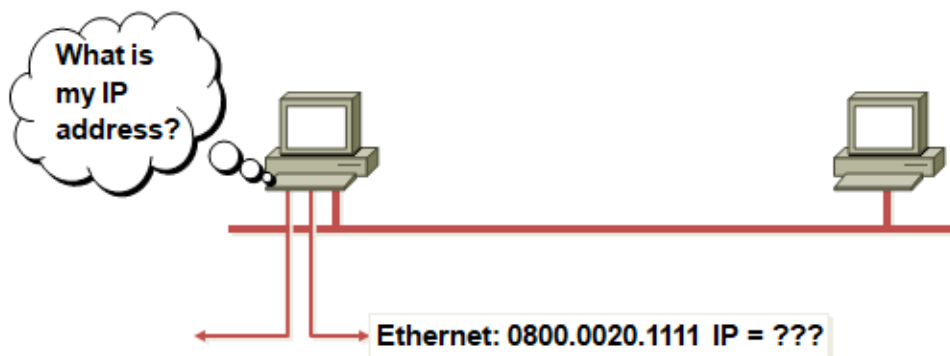
# Address Resolution Protocol



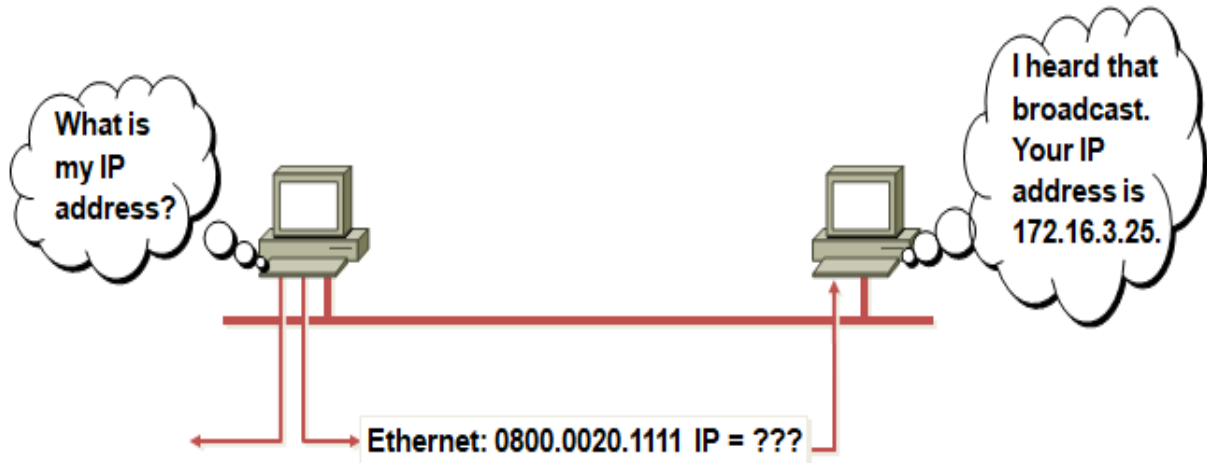
# Address Resolution Protocol



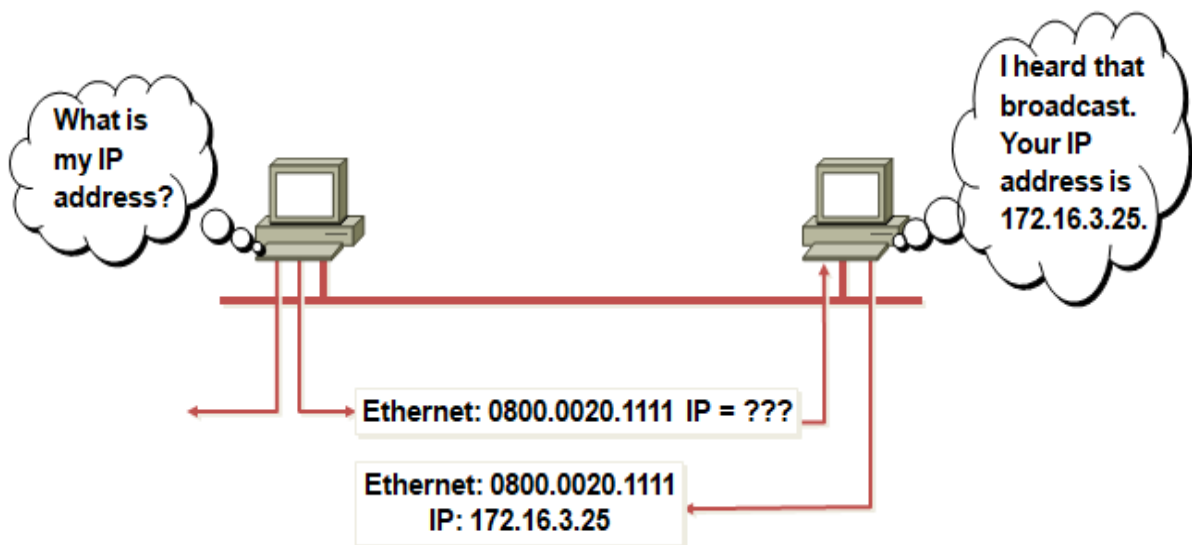
# Reverse ARP



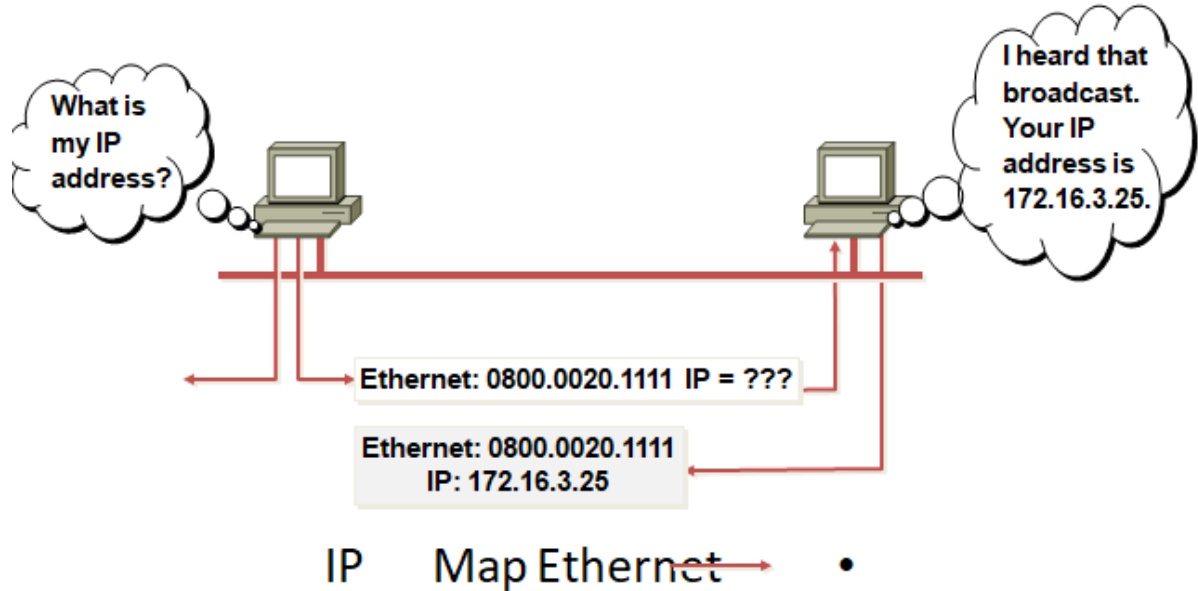
# Reverse ARP



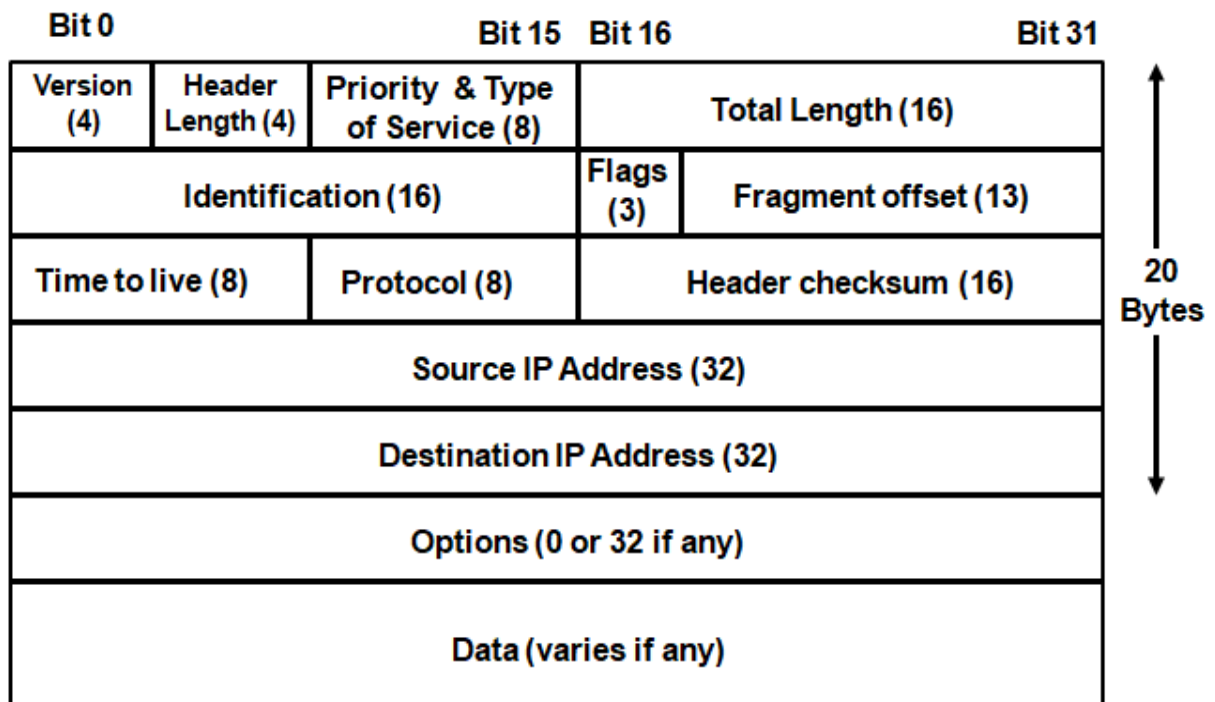
# Reverse ARP



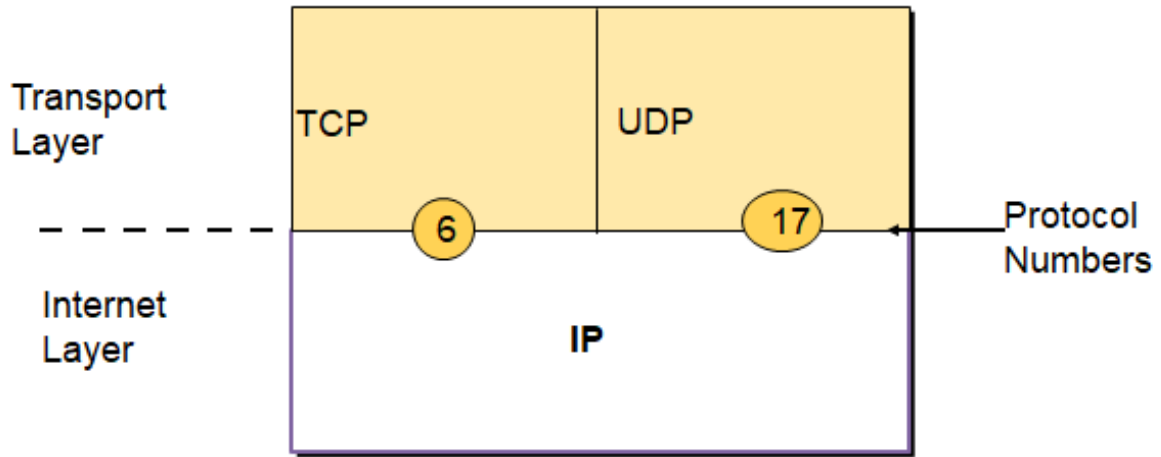
# Reverse ARP



# IP Datagram



# Protocol Field



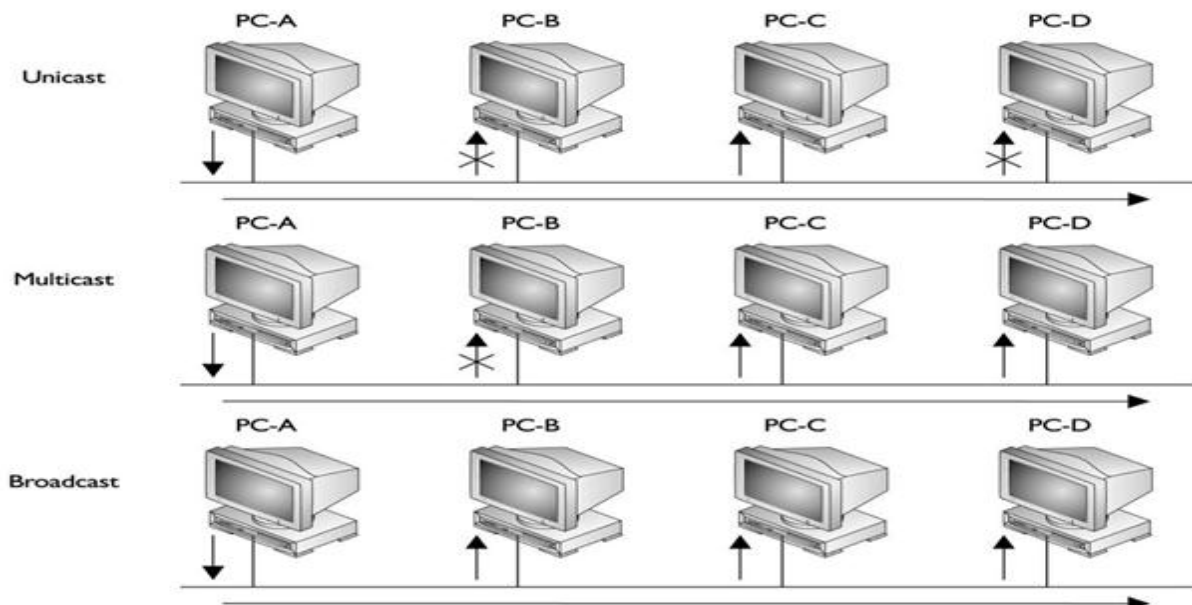
Determines destination upper-layer protocol •

## Types of addresses

### Unicast One

- to - One Multicast One
- to - Group Broadcast One
- to - All

## Type of Transmission





## Broadcast Domain

- A group of devices receiving broadcast frames $\theta$  initiating from any device within the group
- Routers do not forward broadcast frames, broadcast $\theta$  domains are not forwarded from one broadcast to another

## Collision

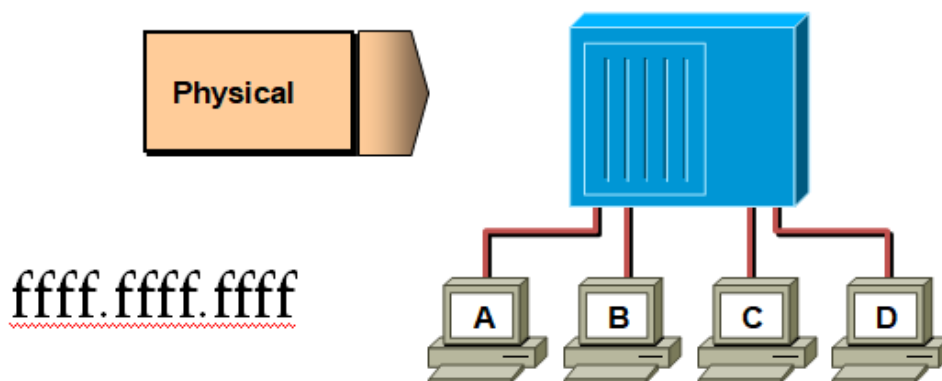
. The effect of two nodes sending transmissions simultaneously $\theta$  in Ethernet. When they meet on the physical media, the frames from each node collide and are damaged

- Collision Domain

The network area in Ethernet over which frames $\theta$  that have collided will be detected.

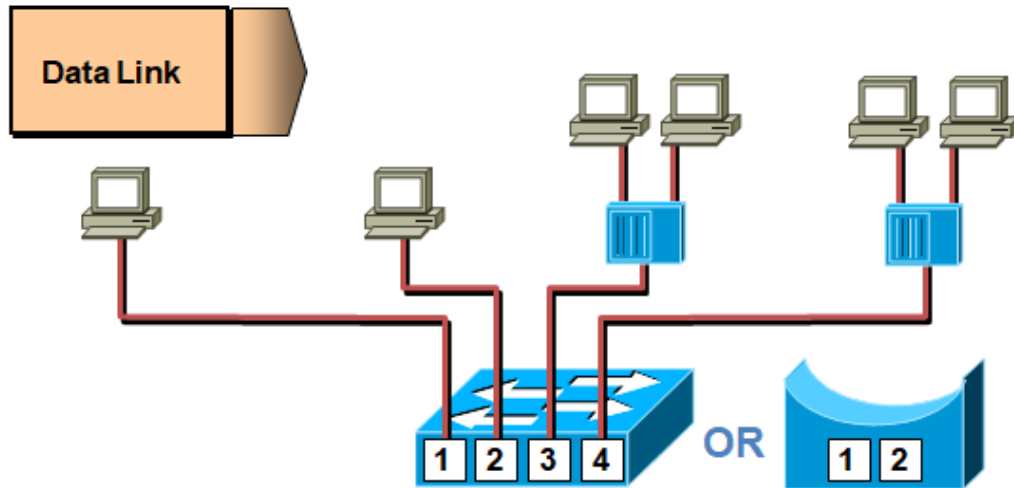
- Collisions are propagated by hubs and repeaters $\theta$
- Collisions are Not propagated by switches, routers, $\theta$  or bridges

## Hubs Operate at Physical layer



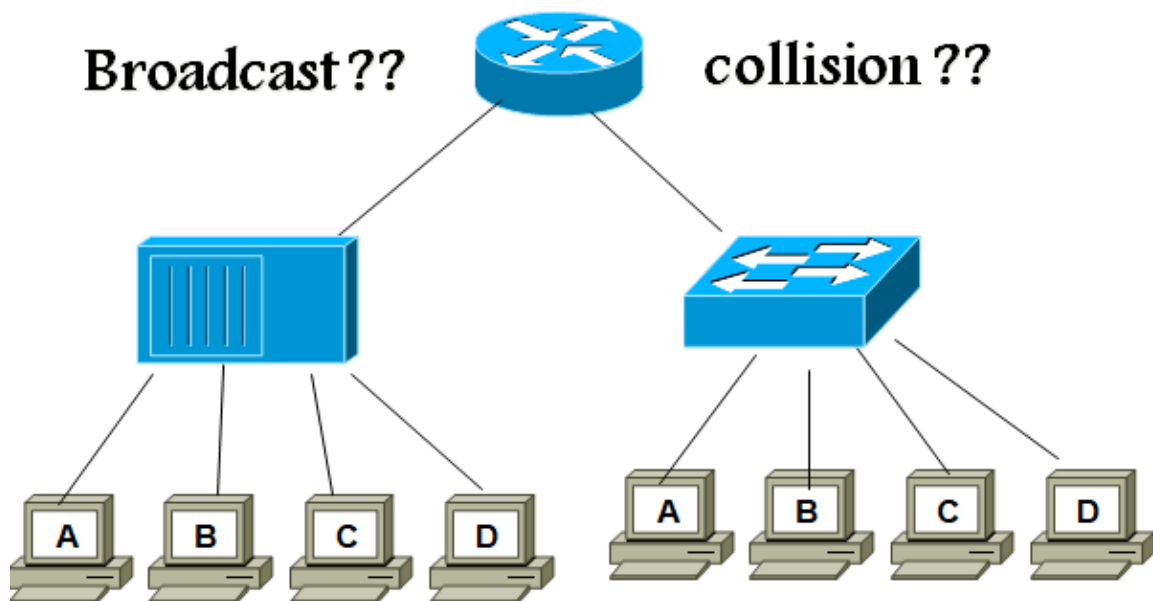
- All devices in the same collision domain
- All devices in the same broadcast domain
- Devices share the same bandwidth

## Switches and Bridges Operate at Data Link Layer

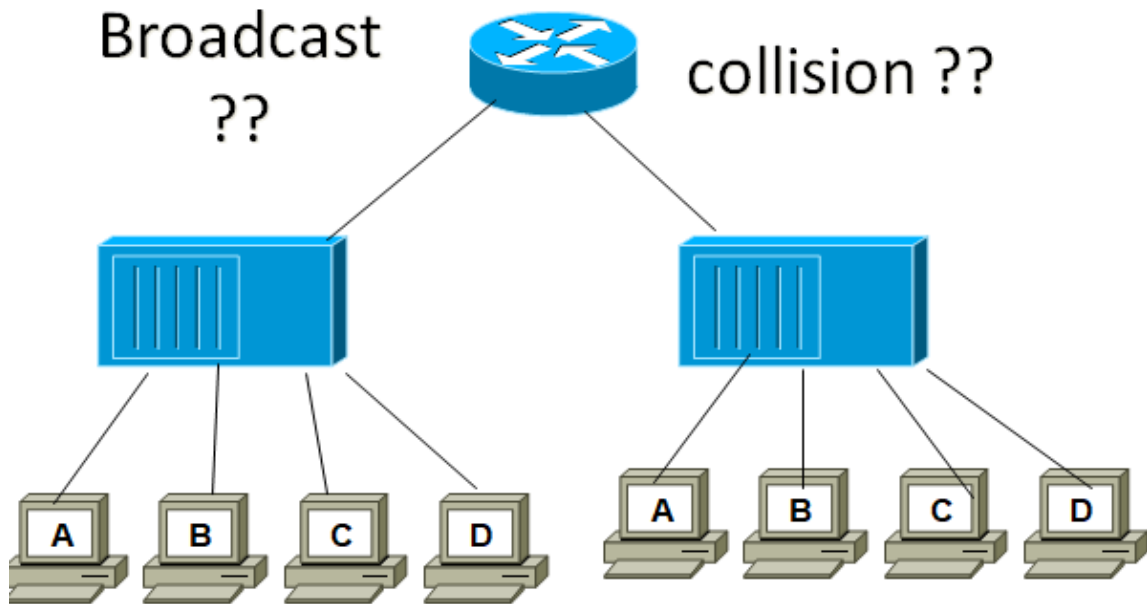


- Each segment has its own collision domain
- All segments are in the same broadcast domain

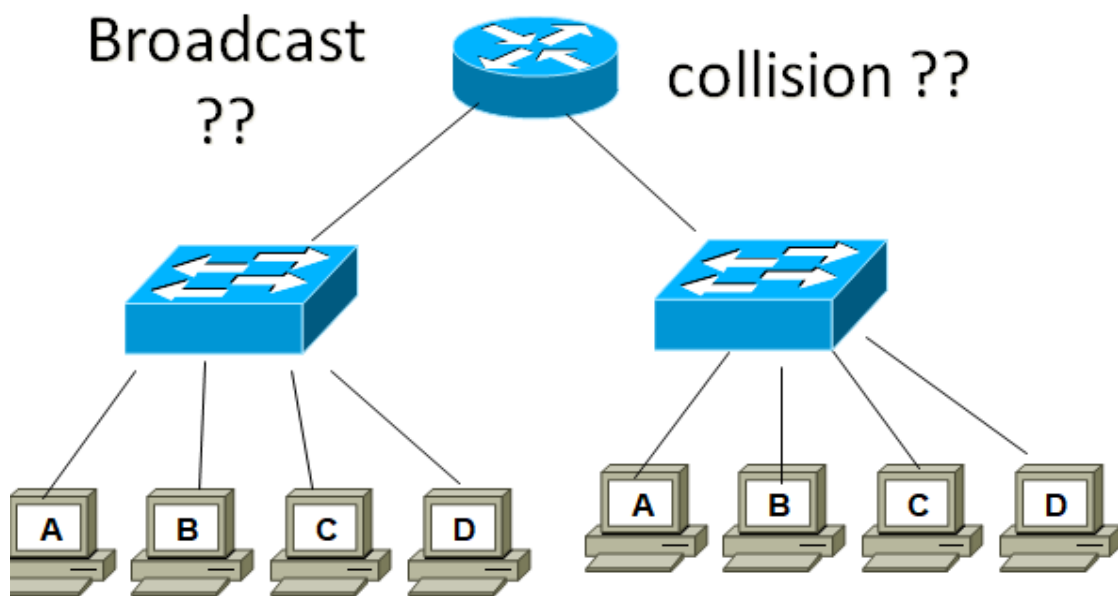
## Question



## Question



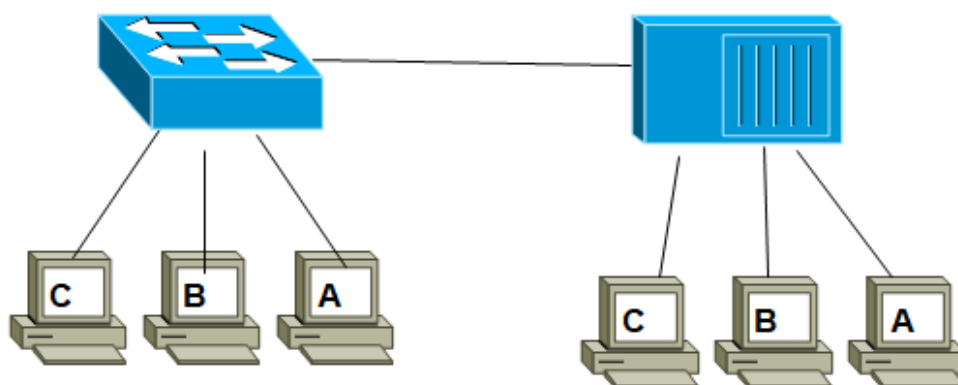
## Question



# Question

Broadcast  
??

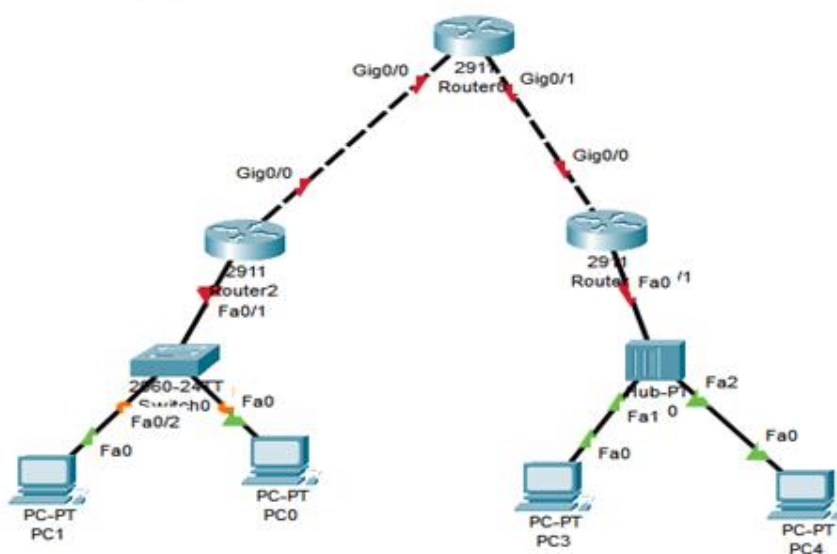
collision ??



# Question

Broadcast  
??

collision ??





# Chapter 7 ☺✍

---

## *IP address version 6*

ABDELSALAM SALEH ELRASHDI

Networking fundamentals



## Chapter 7 ☺✍

### Outlines

- Internet protocol Version 6
- Purpose IP address
- Types of IPV6
- Advantages of IPV6
- Migration to IPv6
- IPv6 Subnetting



---

### Objectives

*By end of this lecture the student will be able :*

- By end of this lecture the student will be able :
- Define IP address V6 .
- Explain the functions of IPV6 address.
- Describe the purpose IPV6 address.
- The differences of IPv6
- Describe the Migration to IPv6
- Explain sub netting in IPv6



# IP address version 6

## IPv4 address space as of October 18, 2010

■ Used
 ■ Free
 ■ Unusable

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

IPv4 was a 32 bit address , and it is suffering from shortage !

Ipv6 is a 128 bit address . Meaning total number of addresses are :

$$2^{128} = 3.4 \times 10^{38}$$

consider the fact that the Earth currently has less than  $10^{10}$  people

The 128-bit IPv6 address is written in hexadecimal notation, with colons between each quartet of symbols

For example : 23D0:1E51:A48A:0001:12B4:5678:9ABC:1234

0	0000	4	0100	8	1000	C	1100
1	0001	5	0101	9	1001	D	1101
2	0010	6	0110	A	1010	E	1110
3	0011	7	0111	B	1011	F	1111

Some IPv6 Advantages are :

- 1- Address assignment features.
- 2- IPsec is Built in
- 3- Simpler Header improvements
- 4- Transition tools

## IPv6

### how to write it

23D0:1E51:A48A:0001:12B4:5678:9ABC:1234

seems along address to write

But the creators of IPv6 made some helping ways to write it down

#### 1- Zero compression :

Any consecutive “all zeros ” quartets can be compressed

23D0:0000:0000:0000:0000:5678:9ABC:1234

Can be written :

23D0::5678:9ABC:1234

But it should only be used once in each address , for example :

23D0:0000:0000:A234:0000:0000:0000:1234

23D0::A234::1234 = wrong way to write it

---

#### 2- Leading Zero Compression :

Any leading zero “in each quartet” can be compressed

For example :

00D0:002A:1000:0000:000E:00B4:0000:0034

D0:2A:1000:0:E:B4:0:34

And you can use both rules together :

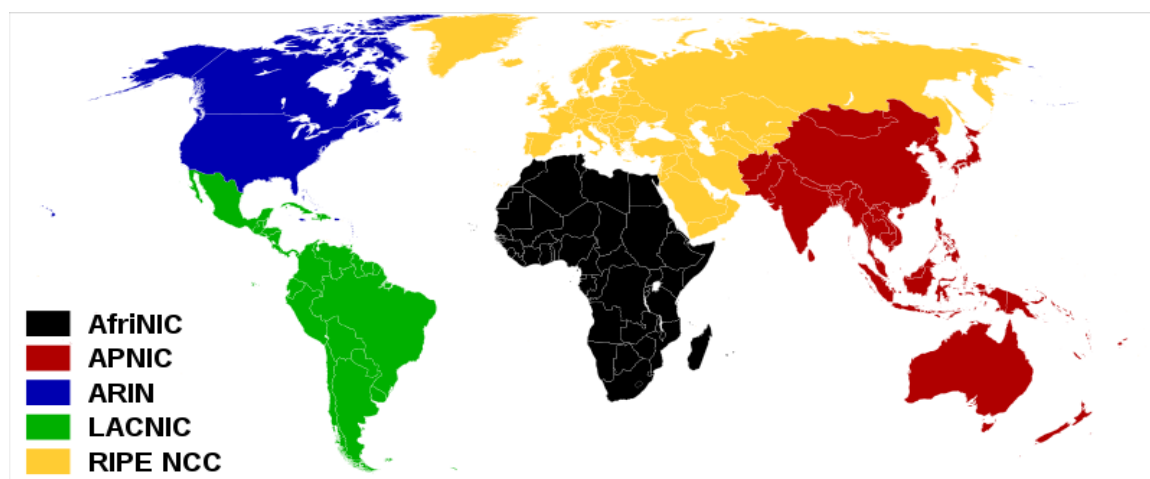
00D4:0000:0000:0000:0000:009C:0000:0004

D4::9C:0:4

---

## Types

IPv6 implementation depends on the facts the ICANN divided the world in to 5 (RIR) Regional Internet Registry each with its own IPv6 allocation , That's called hierarchy design ,each RIR has its own address space



## Address Types :

- 1- UniCast : one to one  
global  
unique Local  
link local
- 2- MultiCast one to group
- 3- AnyCast one to nearest

Note :Each interface can have more than one address

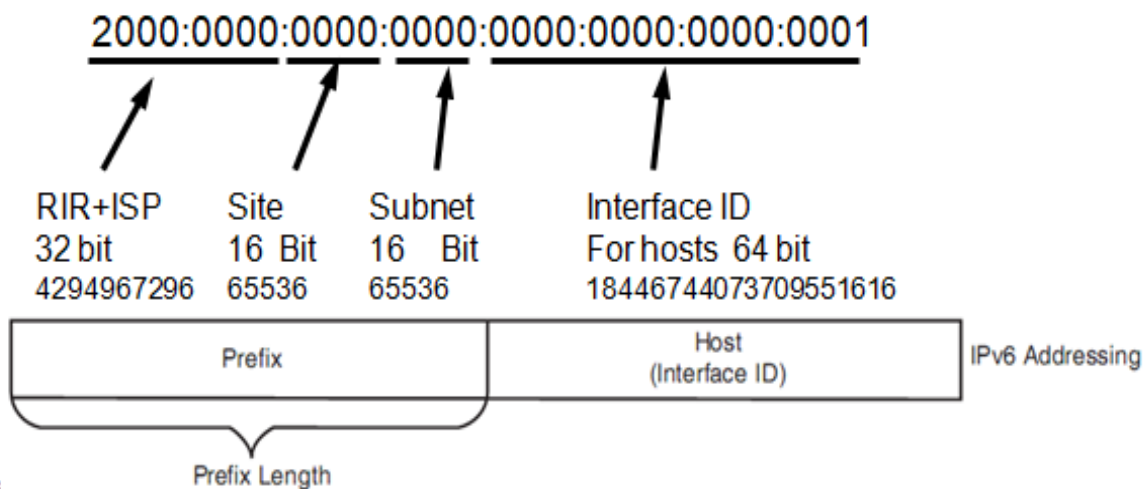


## UniCast addresses

- 1- Global  $\equiv$  public "ipv4 " used on the internet  
address start with 001 binary  
2000 or 2001

Example : 2000:0000:0000:0000:0000:0000:0000:0001

Global address are usually divided like this:

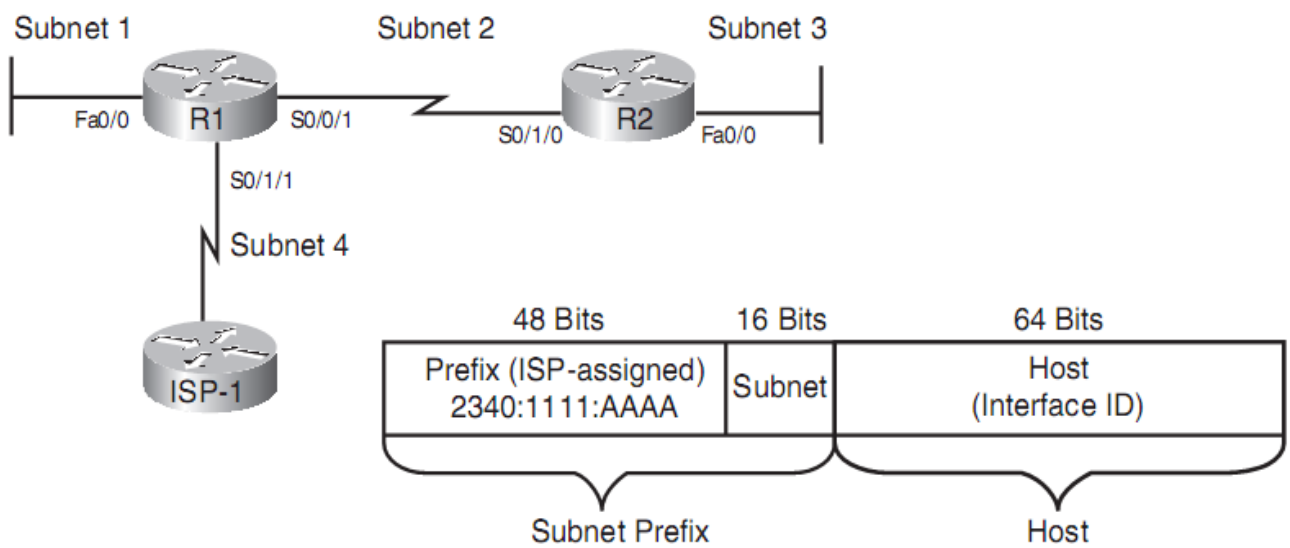
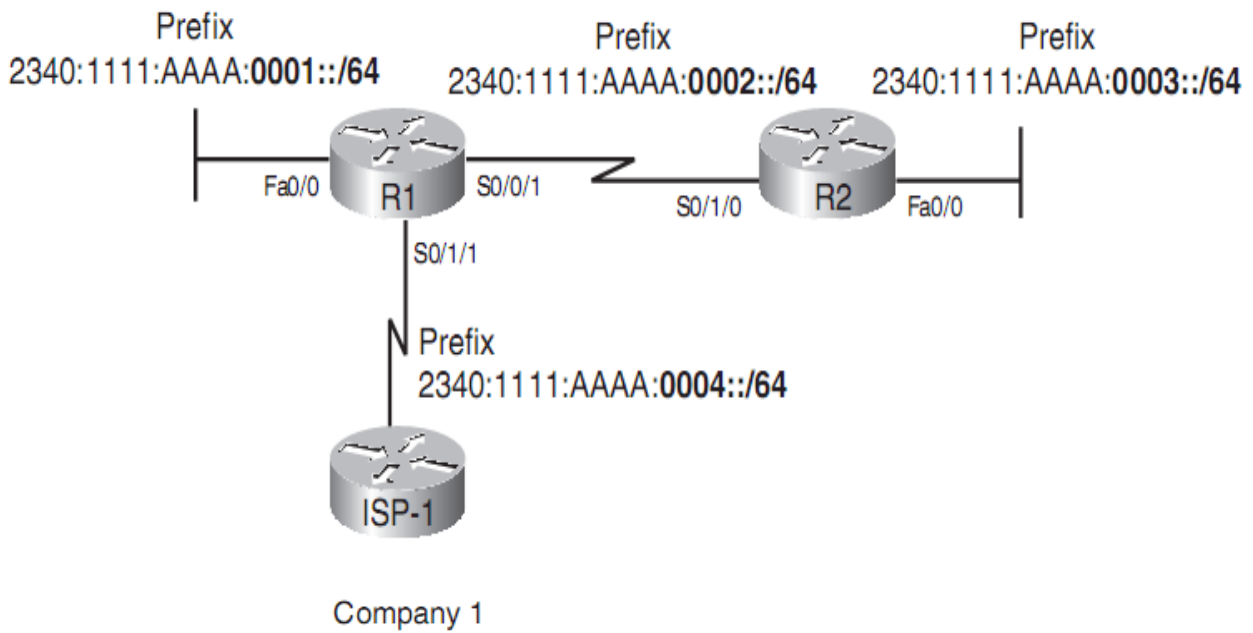


## Subnetting ?

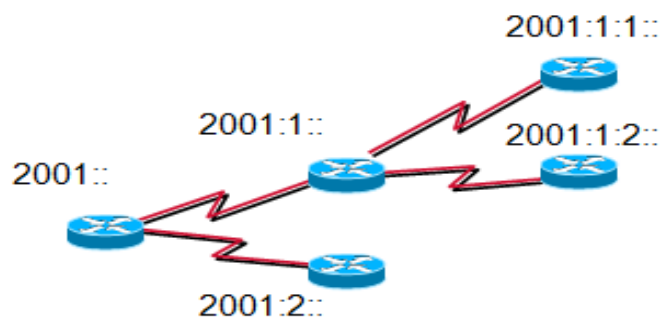
23D0:1E51:A48A:0001:12B4:5678:9ABC:1234/64

/64 = the prefix , it shows how many bits are for the Network portion ,

Remember each character in HEX is 4 bits ! So each quartet is 16 bits



## UniCast addresses



# *UniCast addresses*

2- Local  $\equiv$  Private “ipv4 “

address start with FD00:/8

3- site Local  $\equiv$  Private “ipv4 “ special purpose

address start with FE80:/10

Assigned to each device automatically by EUI-64

Routers never forward data from that address , its only for inside network communication

And it is used by the devices to communicate with the router to get a proper address

---

## *EUI-64*

MAC address =48 bit example: A3B5:5424:DE40

IPv6 = 128 bit , 64 bit for the network “prefix”, 64 bit for the interface ID

EUI-64 derives an IPv6 address from the device’s MAC address by inserting FFFE between the two halve of the MAC address

The 64 bit of the Network will be FE80:0000:0000:0000

And the 64 but of the interface id will be A3B5:54FF:FE24:DE40

The address will be FE80:0000:0000:0000:A3B5:54FF:FE24:DE40

And it will be assigned automatically

---

Multicast:

start with “ FF “

Loopback :

127.0.0.1 in IPv4:::1 in IPv6 or 0:0:0:0:0:0:1

Any network :

0.0.0.0 in IPv4                    ::/128 in IPv6

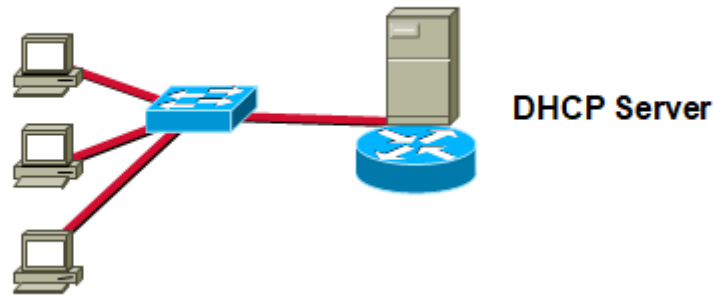
---

## *Assignment*

In IPv4 , if a host needs to communicate with outside of the network it needs an IP , Default Gateway , and DNS !

In IPv6 the same requirements above are needed too

In Ipv6 address assignment can be provided Manually or by DHCP server , to provide the requirements mentioned above ,



### Manual "Static "

EUI64 "only 64bit of Prefix "

```
-config t
-ipv6 unicast-routing
-int fa0/0
-ipv6 add 2001:983A:7BD3:0900::/64 EUI-64
```

Provide only half of the IPv6

The whole 128 bit

```
-config t
-ipv6 unicast-routing

-int fa0/0
-ipv6 add 2001:983A:7BD3:0900::1/64
```

### Dynamic

- Stateless auto configuration  
Gives only 64 bit of Prefix

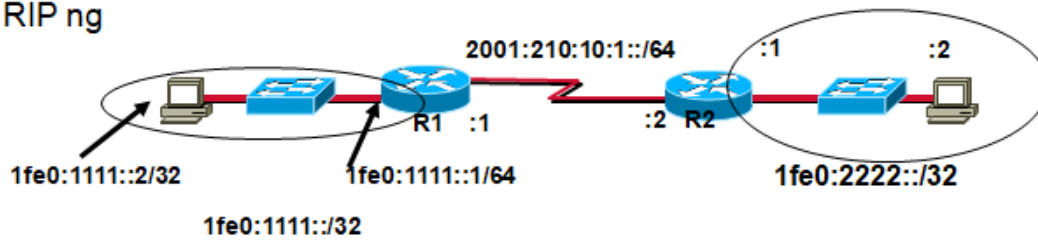
-Stateful DHCP

Gives entire 128 bit

## *stateless autoconfiguration*

Using NDP (Neighbor Discovery Protocol) each host can know it's address , default gateway , and other options relying on NDP's RS and RA "Router Solicitation " and "Router Advertisement "

## RIP ng



RIPng : R1

Config t

Ipv6 unicast-Routing

Ipv6 router rip tag

Int fa0/0

Ipv6 RIP tag enable

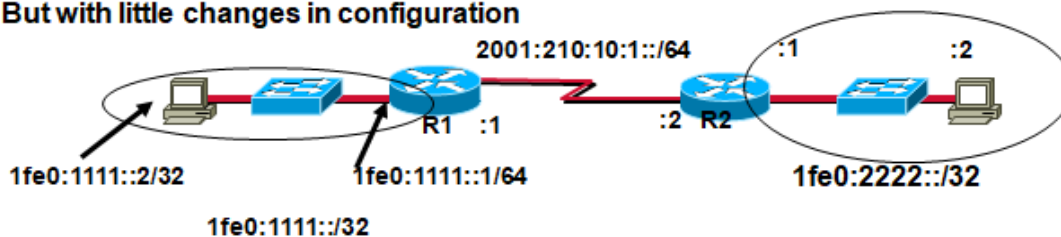
Int s0/0/0

Ipv6 RIP tag enable

## IPv6 Routing

Same Protocols are used in IPv4: static , Dynamic “ RIPng, OSPFv3 , EIGRPv6 “ But with little changes in configuration

Same Protocols are used in IPv4: static , Dynamic “ RIPng, OSPFv3 , EIGRPv6 “  
But with little changes in configuration



Static : R1

Config t

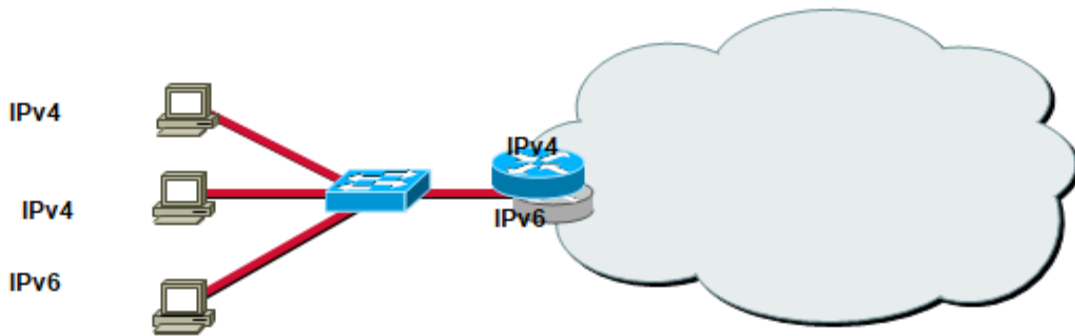
Ipv6 unicast-Routing

Ipv6 route 1fe0:2222::/32 s0/0/0 ( or ) Ipv6 route 1fe0:2222::/32 2001:210:10:1::2



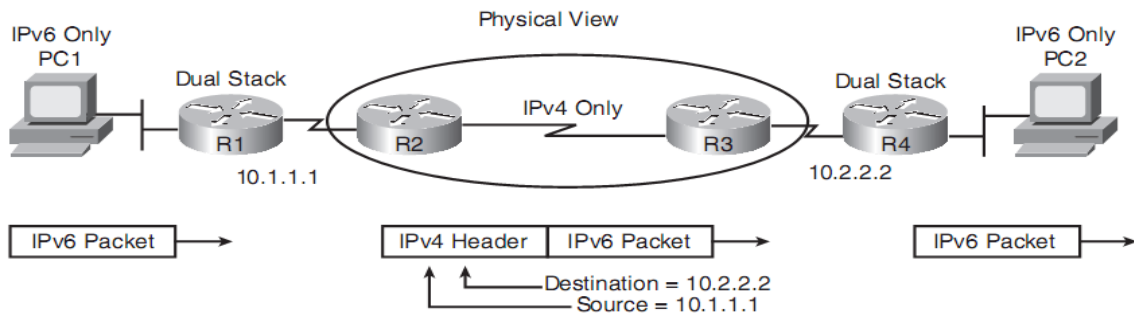
## Migration to IPv6

- 1- IPv4/IPv6 Dual Stacks : router uses both IPv4 and IPv6 at the same time .



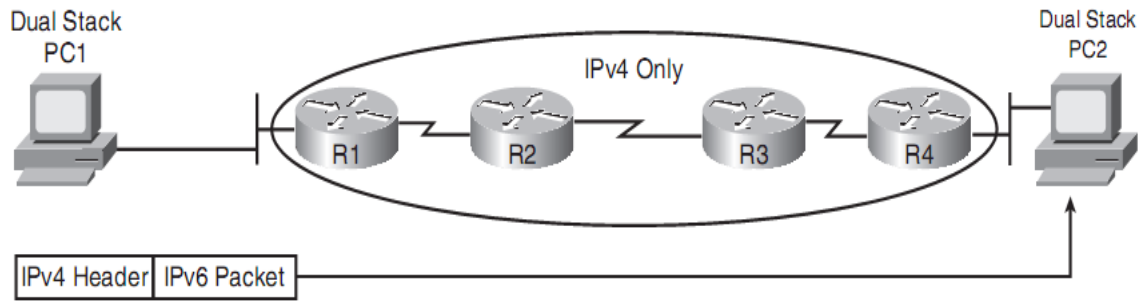
## Migration to IPv6

- 2- Tunneling : the tunnel function typically takes an IPv6 packet sent by a host and encapsulates it inside an IPv4 packet. The IPv4 packet can then be forwarded over an existing IPv4 internetwork .



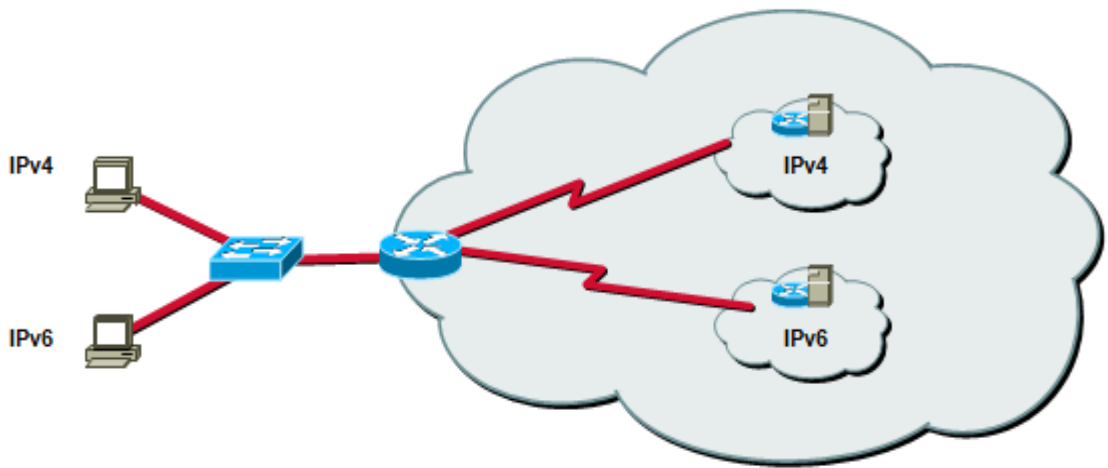
Types Of Tunneling : “ only Teredo tunneling is for Hosts ”

- 1-Manually configured tunnels (MCT)
- 2-Dynamic 6to4 tunnels
- 3-Intra-site Automatic Tunnel Addressing Protocol (ISATAP)
- 4- Teredo tunneling

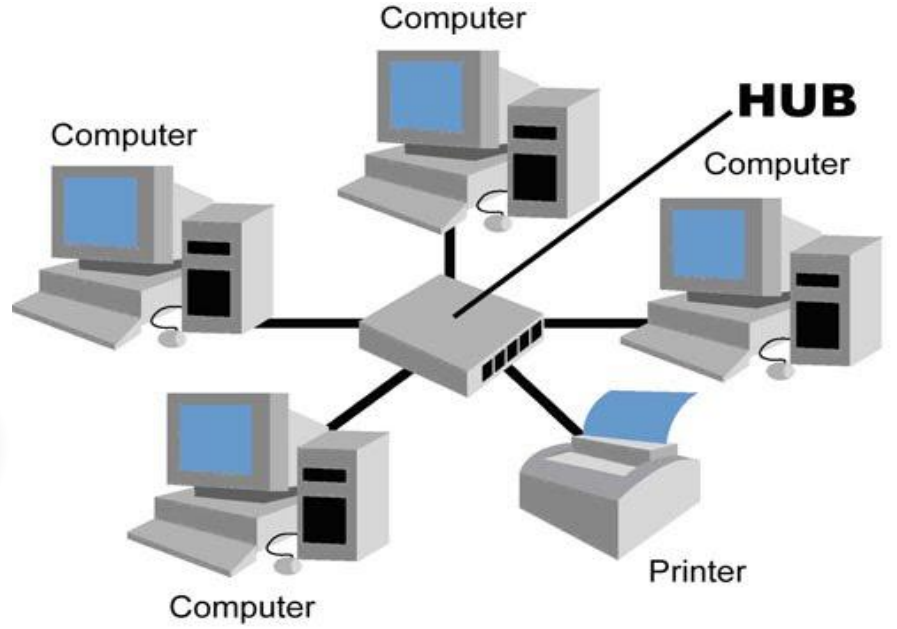


## MIGRATION TO IPv6

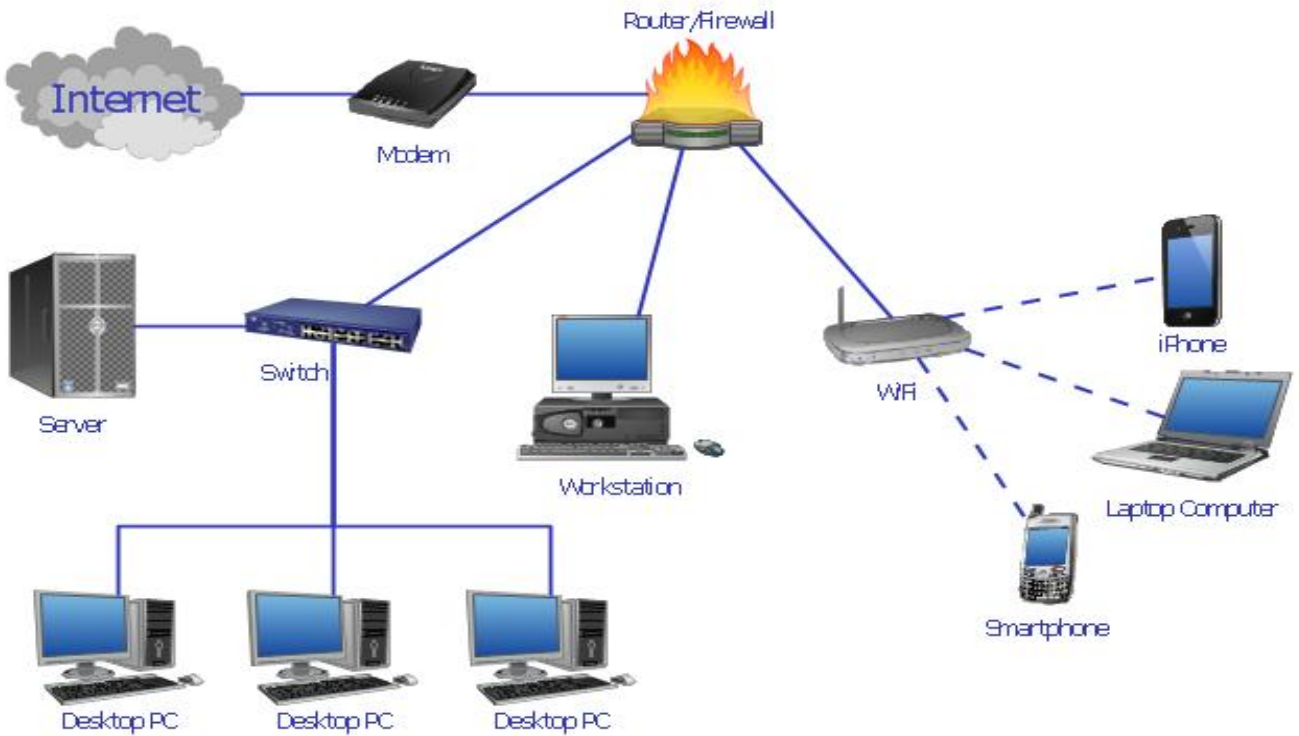
### 3- NAT pt : Protocol Translation



☺👉 The End



# اجزاء العملي ✓



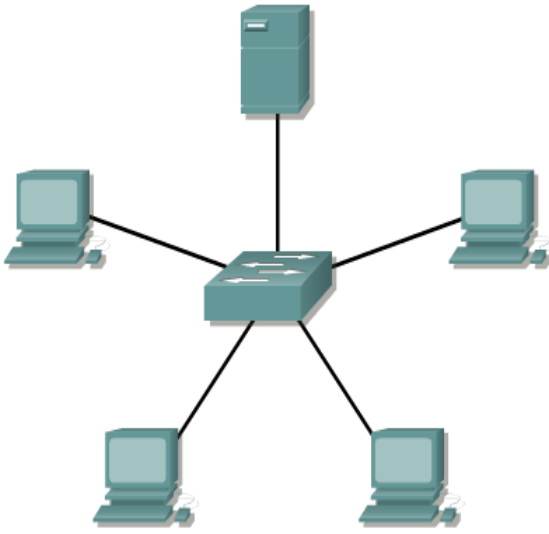


# *Contents*

- ✓ **LAB 1 :-** Make LAN Network
- ✓ **LAB 2 :-** Make Wireless LAN Network
- ✓ **LAB 3 :-** Make password on switch ( Telnet+console+enable mode)
- ✓ **LAB 4 :-** Connect two difference networks by router
- ✓ **LAB 5 :-** Cerate VIANS.
- ✓ **LAB 6 :-** Make Port Security on Switch



• ربط شبكة محلية LAN (سلكية )

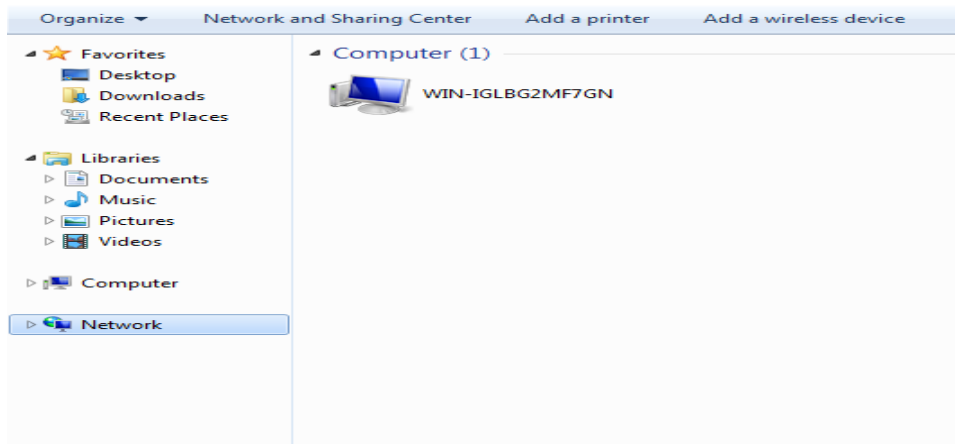


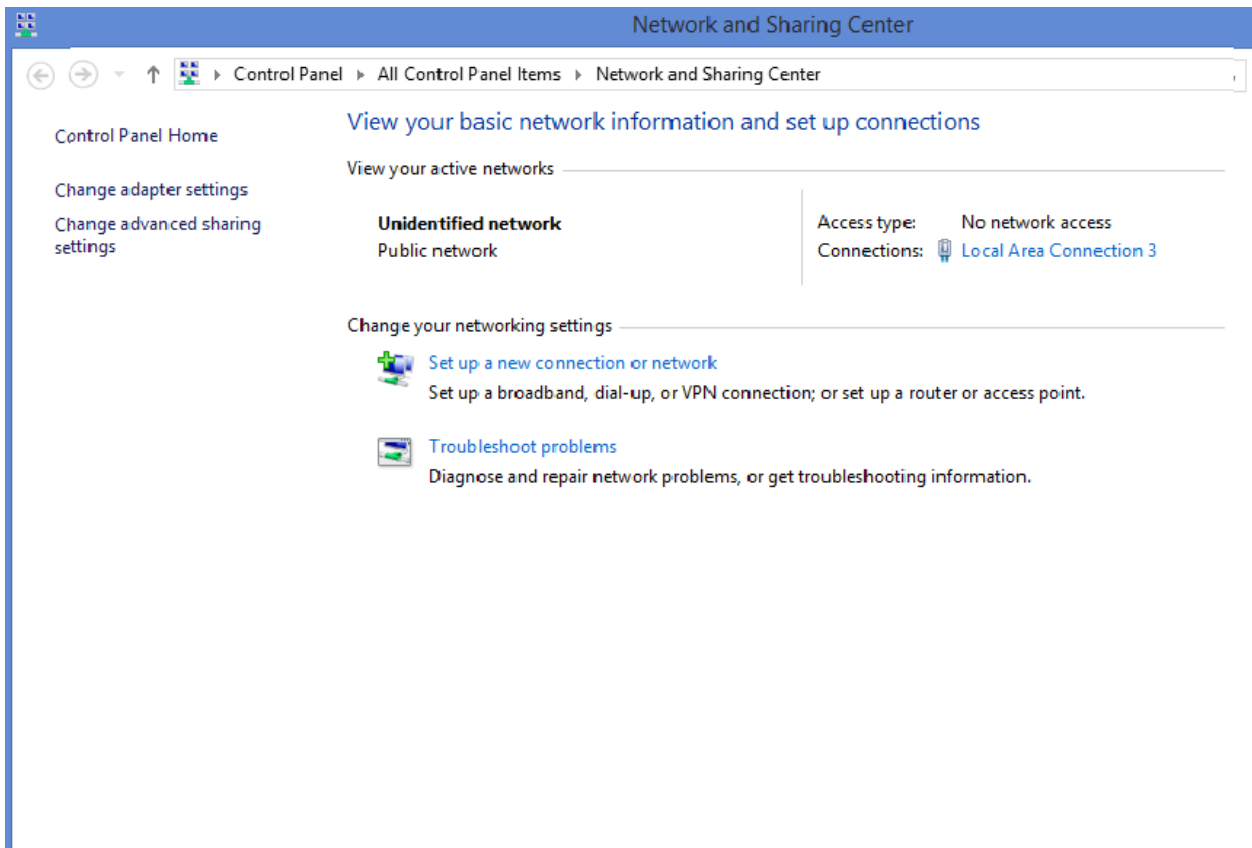
لكي يتم ربط شبكة محلية يجب توفر الاتي :-

- 1- اجهزه (كمبيوتر، طابعة ، موبيل ....).
- 2- كوابل (coaxial ,twisted pair).
- 3- جهاز مركزي (Switch,Hub).
- 4- address لكل جهاز.

بعد توفر كل من الاجهزه والكوابل والجهاز المركز نحتاج لاعطاء IP address لكل جهاز حيث هناك طريقتين لاعطاء عنوان لكل جهاز ، اما تلقائي عن طريق بروتوكول DHCP او يدوي اي بمعنى الدخول علي كل جهاز واعطائه IP address وهذا الاختيار يكون ذات جدوي اذا كان عدد الاجهزة قليل ولكن اذ كان العدد كبير ففي هذي الحال يجب اعطاء العنوان تلقائي ، ولكي يتم اعطاء IP address بشكل يدوي نقوم بالاتي :-

نقوم بدخول علي جهاز ← computer Network  
 Network and sharing center ↙

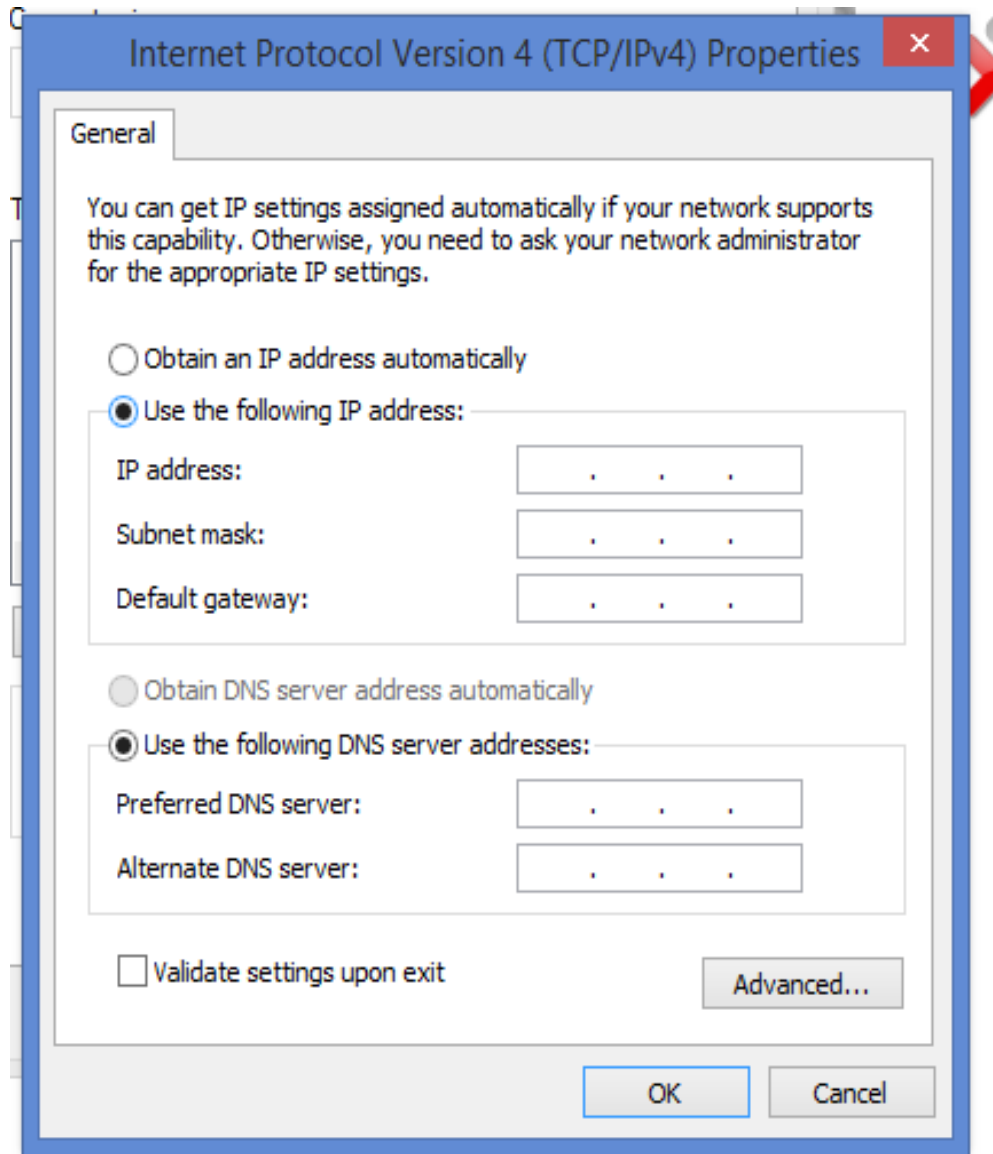




وبعد ذلك نقوم باختيار change adapter setting تم نقوم بعمل زر الايمن علي كرت الشبكة LAN او Ethernet ثم خصائص ثم اختيار V4 Internet protocol كالاتي :-

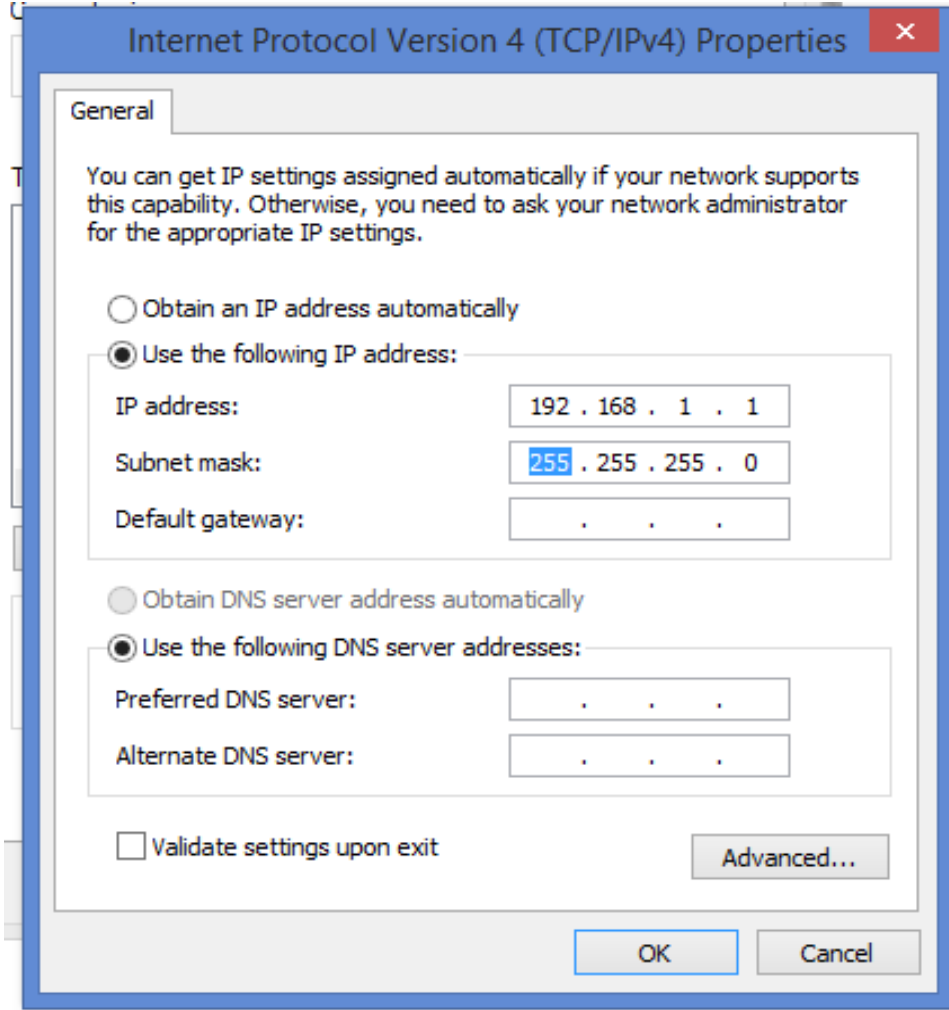


بعد ذلك تظهر الرسالة توجد به اختيار الاول الحصول علي العنوان عن طريق DHCP  
والتاني الحصول علي يدوي



في هذ الشبكة سوف نقوم باعطاء IP يدوي وسوف نستخدم Private IP address لكلاس C كالاتي :-





معا مراعات ان باقي الاجهزي يجب ان تبدأ 192.168.1 ويتم تغيير اخر خانة في العنوان لان  
الخانات الثلاثة الاولى خاصة برقم الشبكة اي ان باقي الاجهزة ستكون كالاتي :-

192.168.1.2 •

192.168.1.3 •

192.168.1.4 •

بعد ربط جميع الاجهزه مع بعضها البعض يجب ان يتم التحقق من ان هناك اتصال ما بين  
الاجهزه عن طريق امر PING ثم عنوان الجهاز كالاتي  
192.168.1.2 PING حيث يتم ارسال اربع بيانات حجم كل واحد منها 32 بيت وللتأكد من  
الاتصال يجب ان يرد الجهاز اربع مرات كالاتي

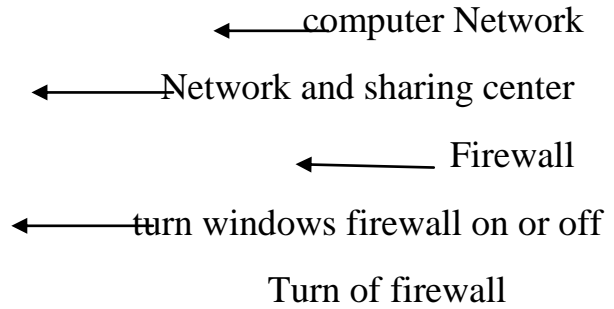
Replay from 192.168.1.2

Replay from 192.168.1.2

Replay from 192.168.1.2

Replay from 192.168.1.2

مع ملاحظة انا في بعض الحالات يقوم جدار الحماية بمنع هذا الاتصال ولايقاف جدار  
الحماية نقوم بالاتي



Network and Sharing Center

Control Panel > All Control Panel Items > Network and Sharing Center

Control Panel Home

Change adapter settings


Change advanced sharing settings


View your basic network information and set up your network

View your active networks

Unidentified network	A
Public network	C

Change your networking settings

 [Set up a new connection or network](#)  
Set up a broadband, dial-up, or VPN connection; connect to a wireless network

 [Troubleshoot problems](#)  
Diagnose and repair network problems, or get troubleshooting help



See also

- HomeGroup
- Intel® PROSet/Wireless Tools
- Internet Options
- Windows Firewall**



## Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

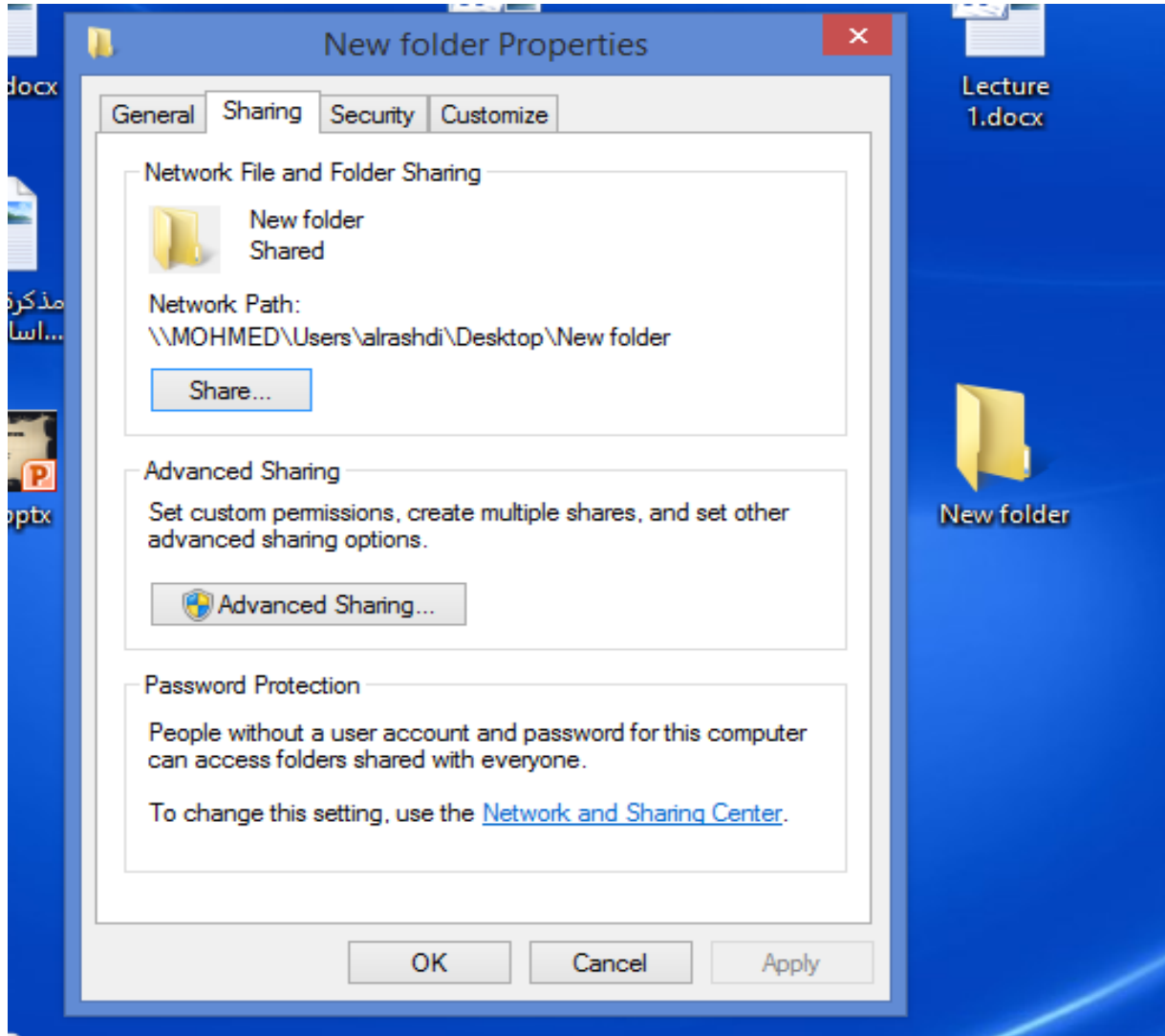
### Private network settings

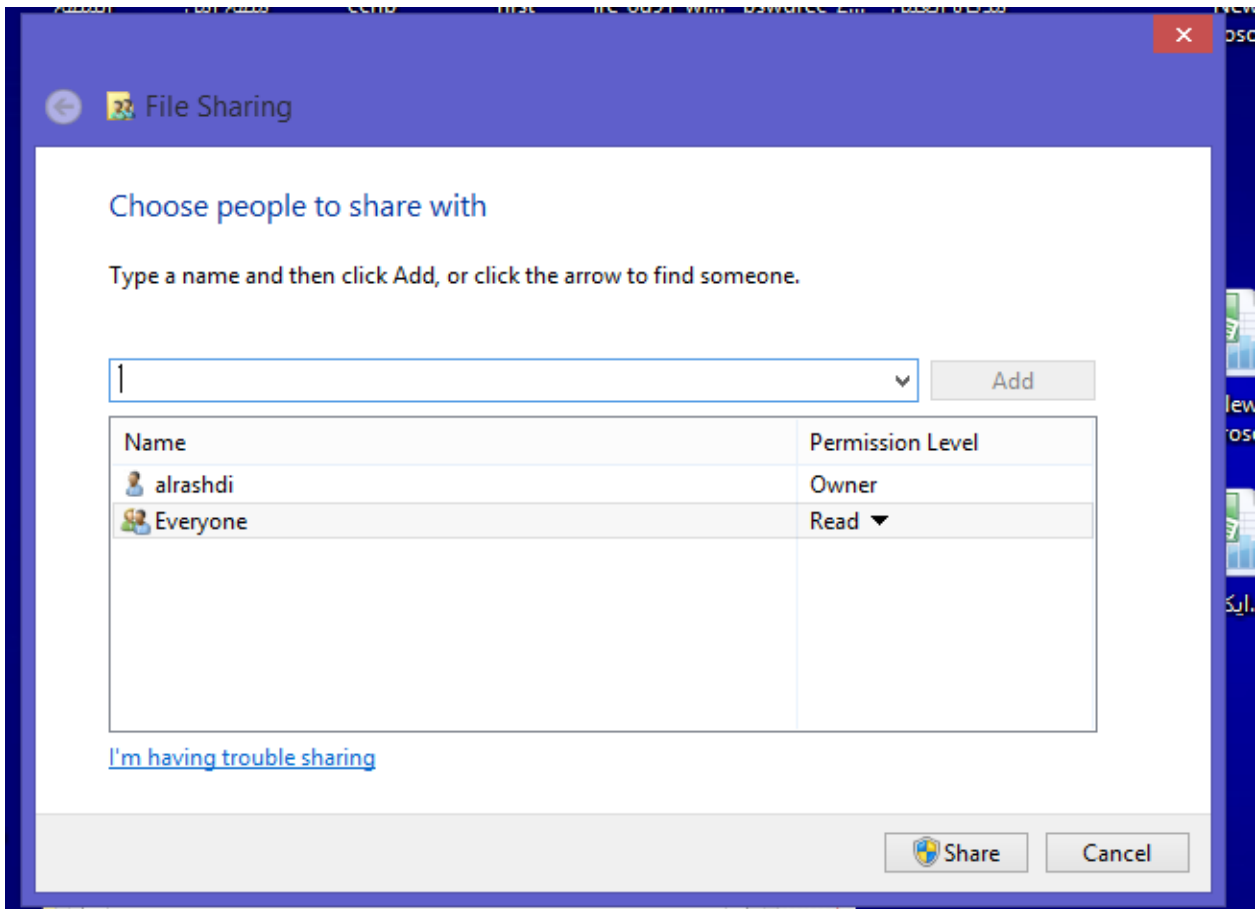
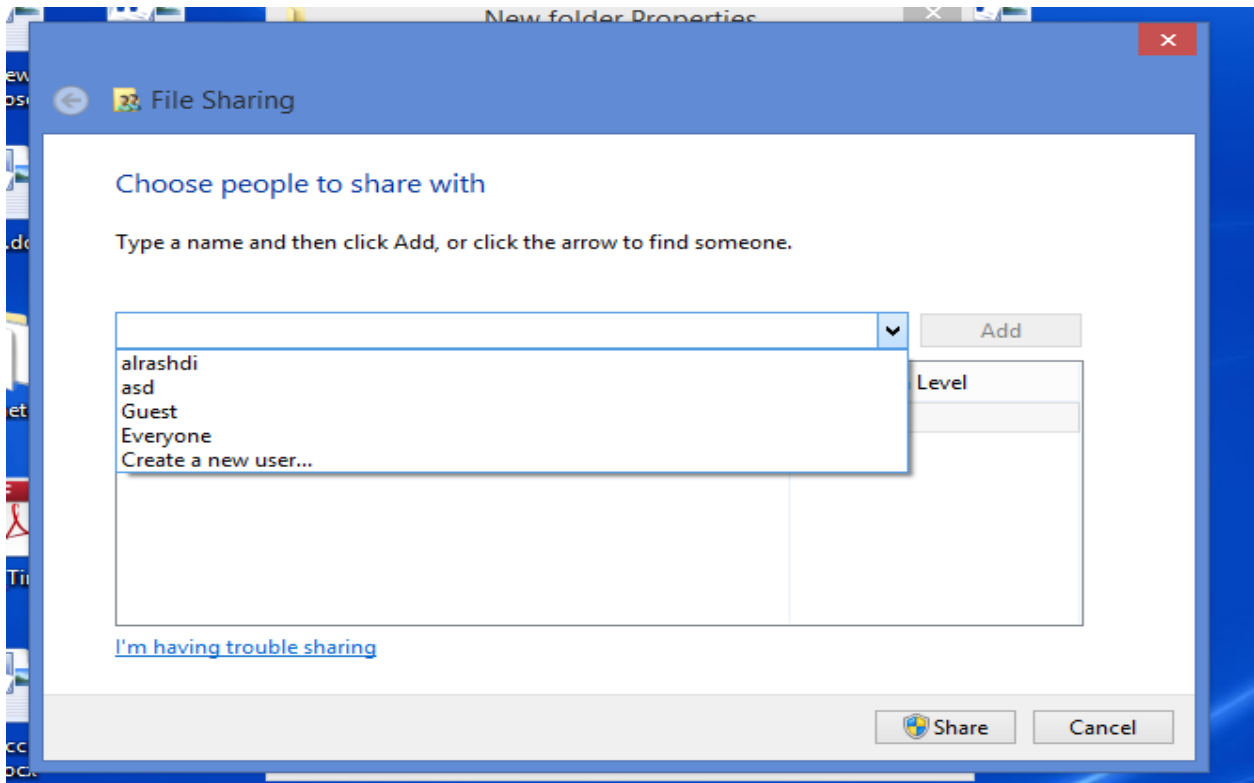
-   Turn on Windows Firewall
- Block all incoming connections, including those in the list of allowed apps
  - Notify me when Windows Firewall blocks a new app
-   Turn off Windows Firewall (not recommended)

### Public network settings

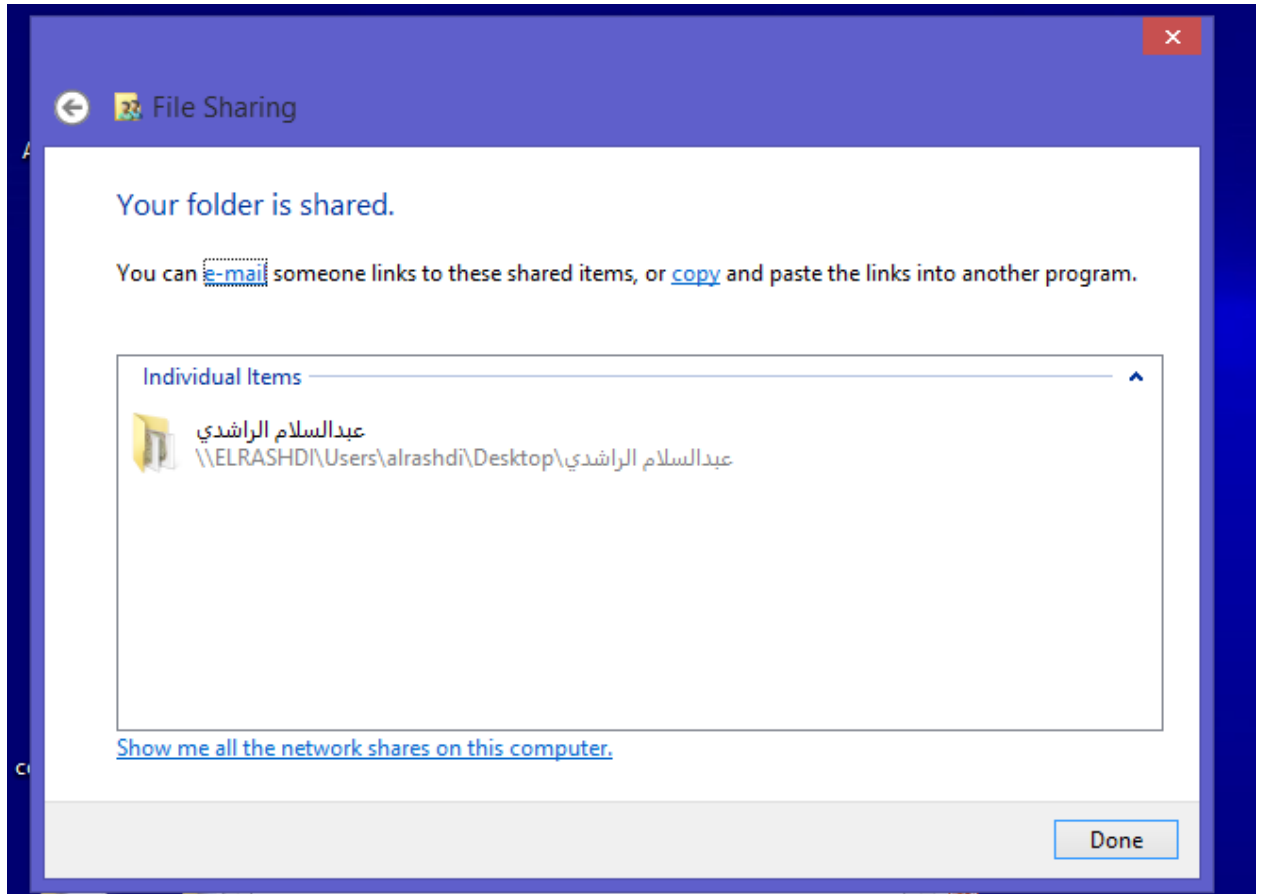
-   Turn on Windows Firewall
- Block all incoming connections, including those in the list of allowed apps
  - Notify me when Windows Firewall blocks a new app
-   Turn off Windows Firewall (not recommended)

الآن نقوم بعمليات تبادل بيانات وملفات ولكي يتم ذلك نقوم بالاتي نقوم باختيار المجلد المراد مشاركتهم مع باقي الاجهزه زر الايمن وبتالي نختار مشاركة ويتم اختيار الاشخاص المراد مشاركتهم او اختيار everyone اي جميع الموجودين ثم اختيار Add اخيرا نقوم باختيار الصلاحيات قراء واو قراء وكتابه كالاتي :-

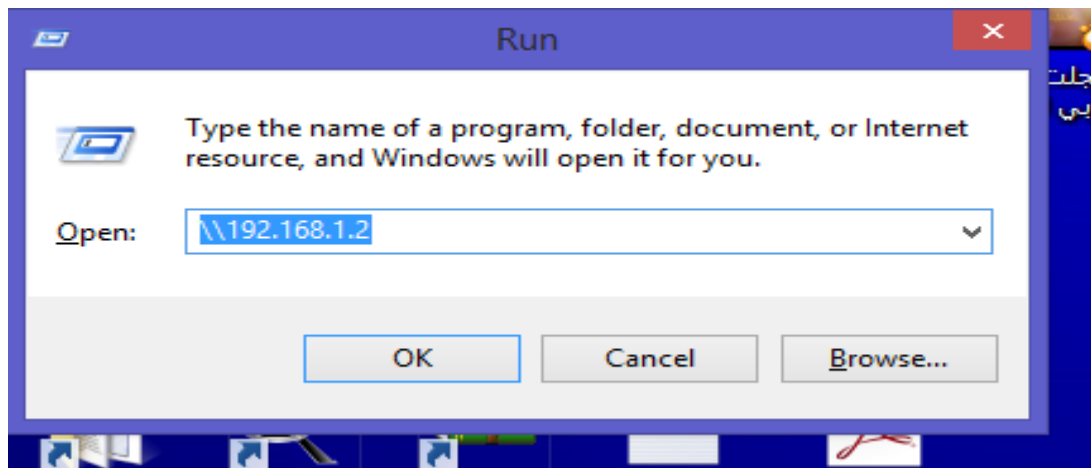




ثم نقر علي share ثم done



وللدخول علي الجهاز للحصول علي الملفات التي تم مشاركتها نكتب رقم ip address او اسم الجهاز المستهدف داخل شاشة التشغيل (run) كالآتي :-



## 2- ربط شبكة محلية Wireless LAN (لاسلكية)

الآن سوف نتعلم سويا كيفية ربط مجموعه أجهزه لاسلكية عن طريق Access point

وسوف نستخدم في هذا Lab Access point

من نوع Linksys من شركة Cisco كما في

الشكل التالي

يتم عمل اعدادات للاكس بيونت بطريقتين

:-

الاولي:- عن طريق توصيل الكابل مباشرة

بالاكسس بيونت (Console) عن طريق

كابل الشبكات RJ45 وهو الأصح والأفضل

كما في الشكل التالي



معا ملاحظة ان هناك اخطاء يقع فيها الكثير فعندما يريدون الدخول علي الاعدادات

الاكسس بيونت يضع الكابل علي بورت WAN او internet وهذا خطأ كبير كما في

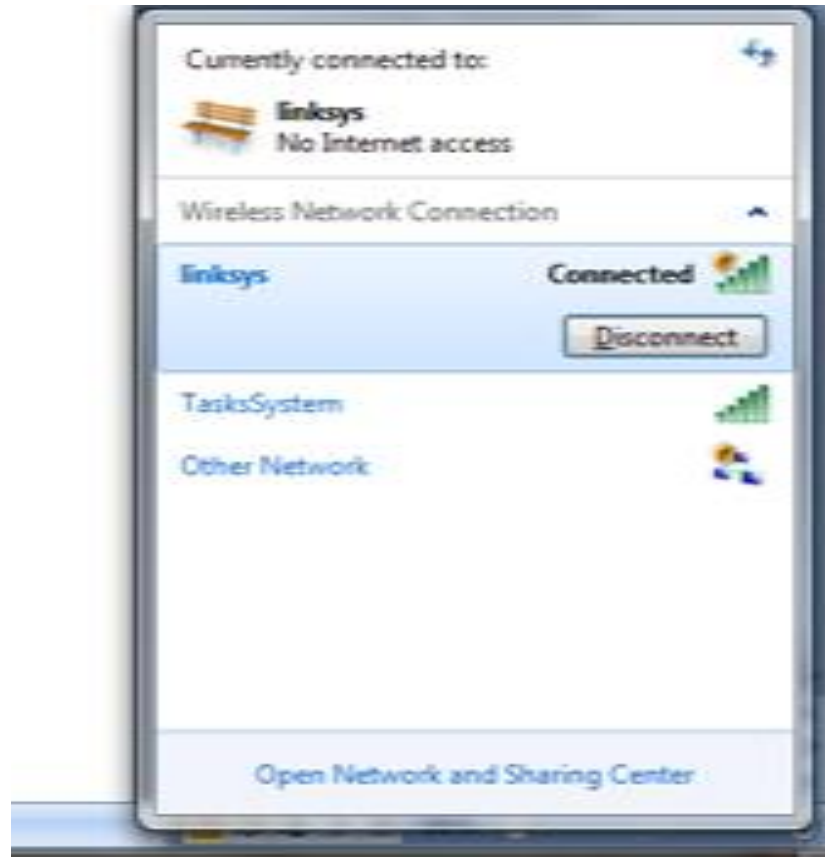
الشكل التالي





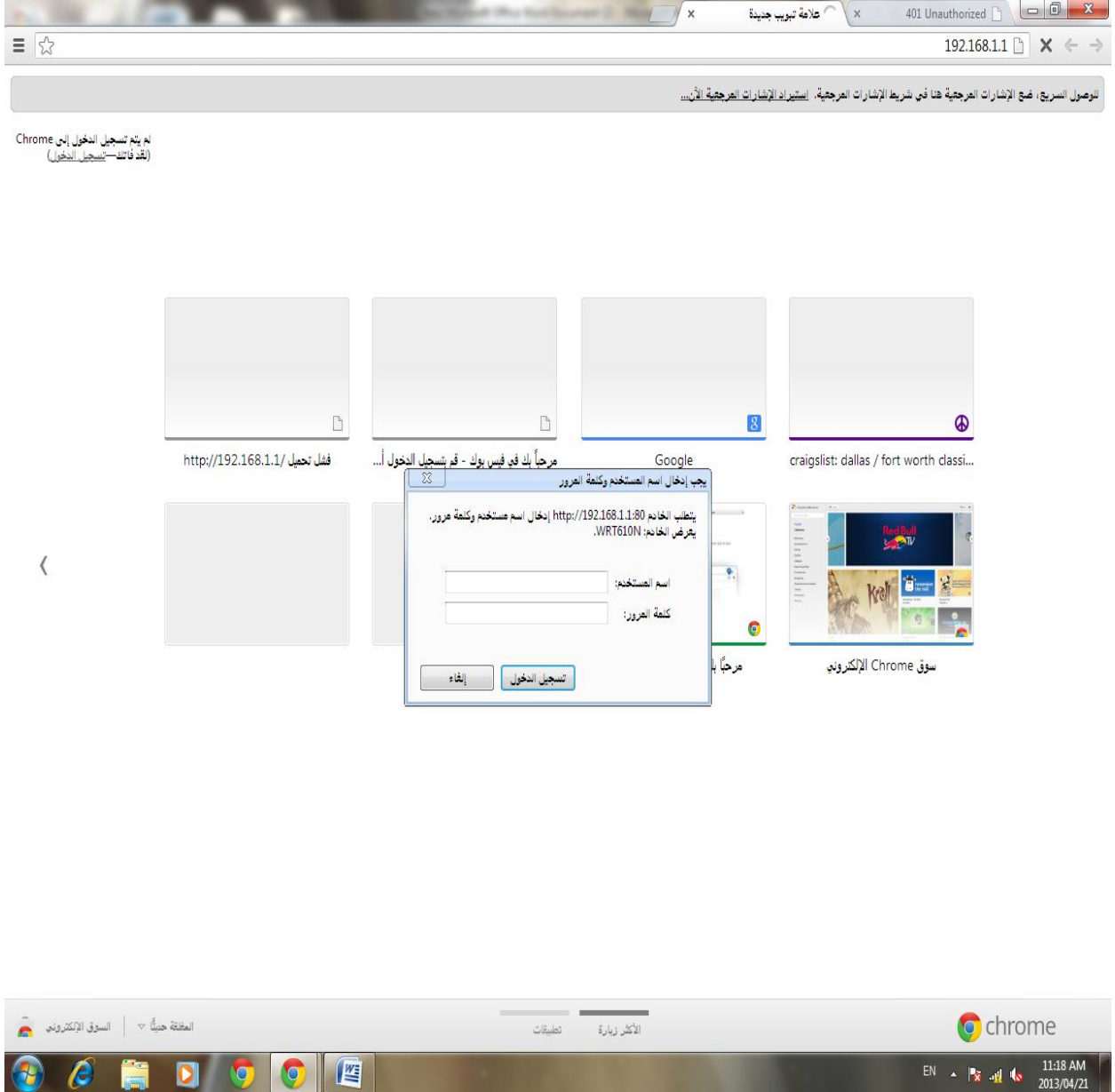


ثانيا :-وهو الدخول علي الإعدادات للاكسس بيونت عن طريق جهاز غير متصل مباشرة  
بالاكسس بيونت (Telnet)  
وللدخول على إعدادات الاكسس بيونت يجب علينا اولا الاتصال بالاكسس بيونت حيث

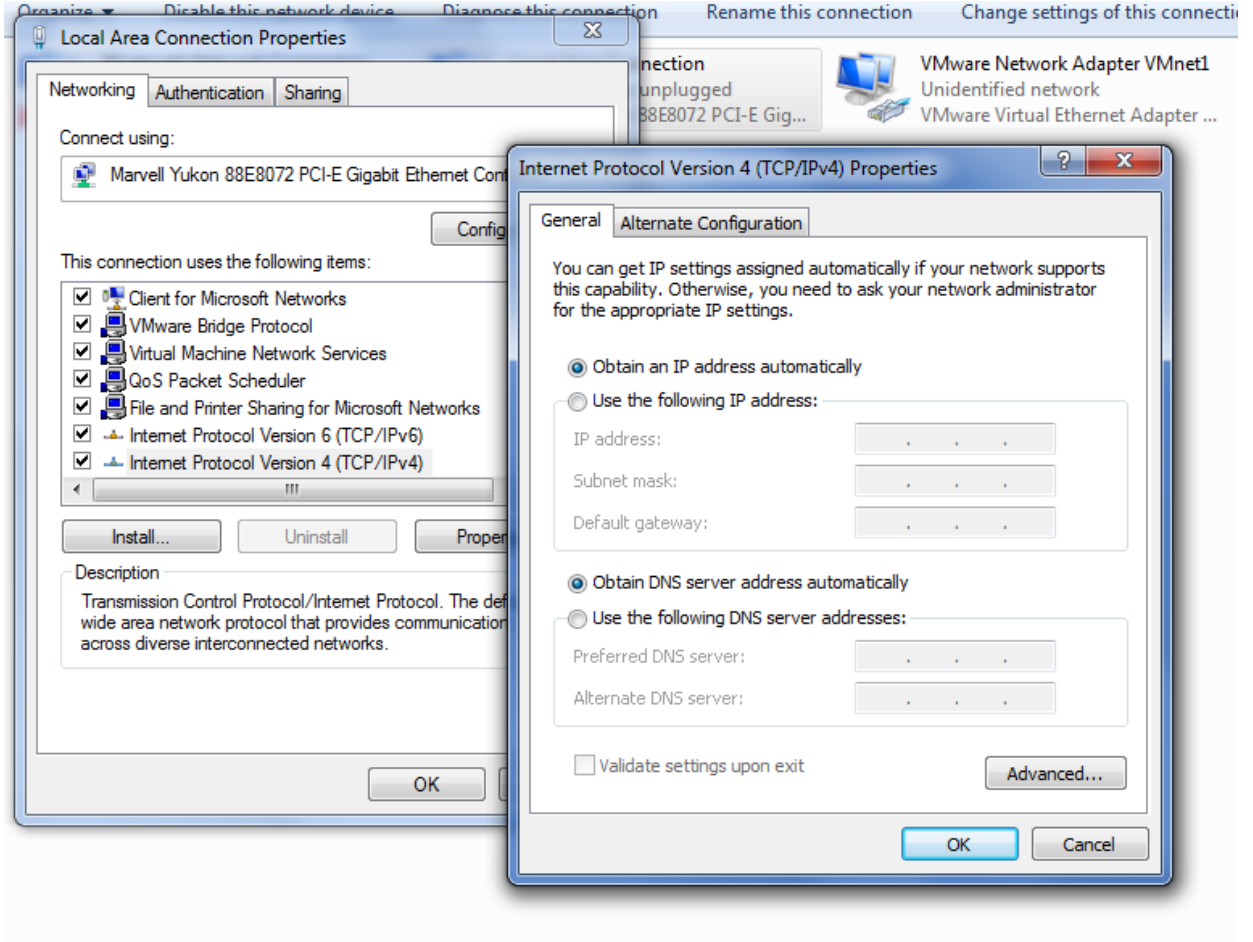


يظهر اسم الاكسس البيونت الافتراضي وهو نفس اسم الشركة Linksys كما في الشكل التالي

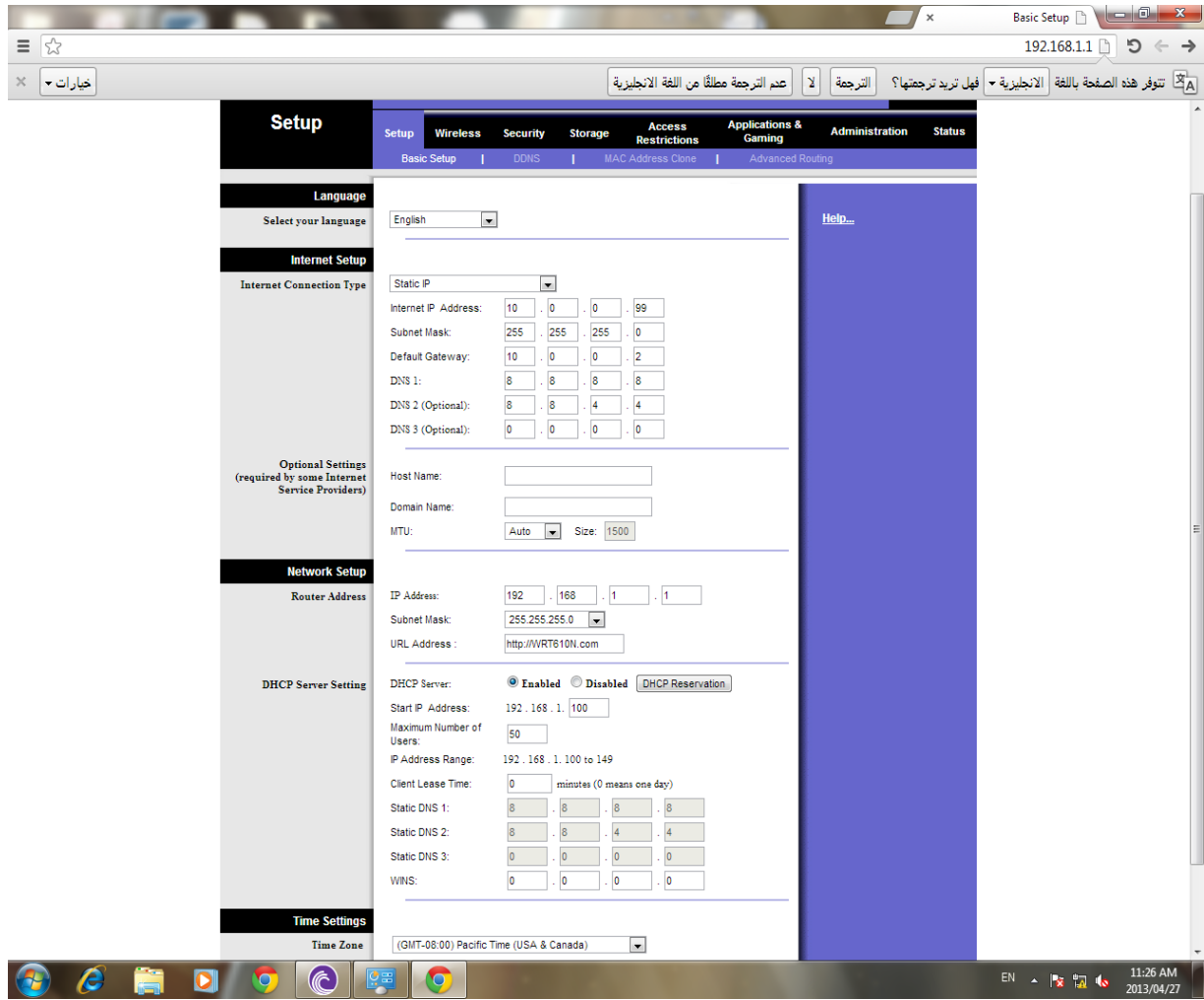
ثانياً يجب معرفة IP Address وعادة يتم كتابته في الاسفل ويبدأ مثلاً 192.168.1.1 أو 192.168.0.1 فنقوم بدخول علي أي Internet explorer كما في الشكل الآتي



## معا ملاحظة ان نجعل كرت الشبكات يأخذ IP من DHCP



وبعد ذلك يطلب منك إدخال اسم المستخدم وكلمه المرور بالنسبه لأسم المستخدم في الغالب تكون admin اما بالنسبة للكلمة المرور فأحيانا 1234 وأحيانا كلمة admin في هذا الاكسس بوينت كلمة المرور admin بعد كتابة واسم المستخدم admin كلمة المرور admin تظهر لنا النافذة التالي :-



سوف تظهر عدة قوائم كما في الشكل السابق سوف نتكلم على القوائم التي سوف نحتاج اليها في تكوين هذا الشبكة والقوائم هي

## Setup :

تحتوي على عدة قوائم من أهمه basic setup التي من أهمه

Internet setup إذا كان لديك انترنت وتريد جميع الاجهازه المتصل بالاكسس بينت تدخل على انترنت فتقوم بكتابه IP Address الجهاز الذي سوف يدخل على النت اما يدويا او عن طريق DHCP

## ► Network setup

فهي Ip Address امتاع الاكسس بيونت وتستطيع تغييره

## ► DHCP Server setup

وفيه يتم تفعيل او عدم تفعيل خدمة الحصول علي IP Address من DHCP ايضا يتم

تحديد المدى IP

Address الذي سوف

يخده الاجهازه أي مثلا

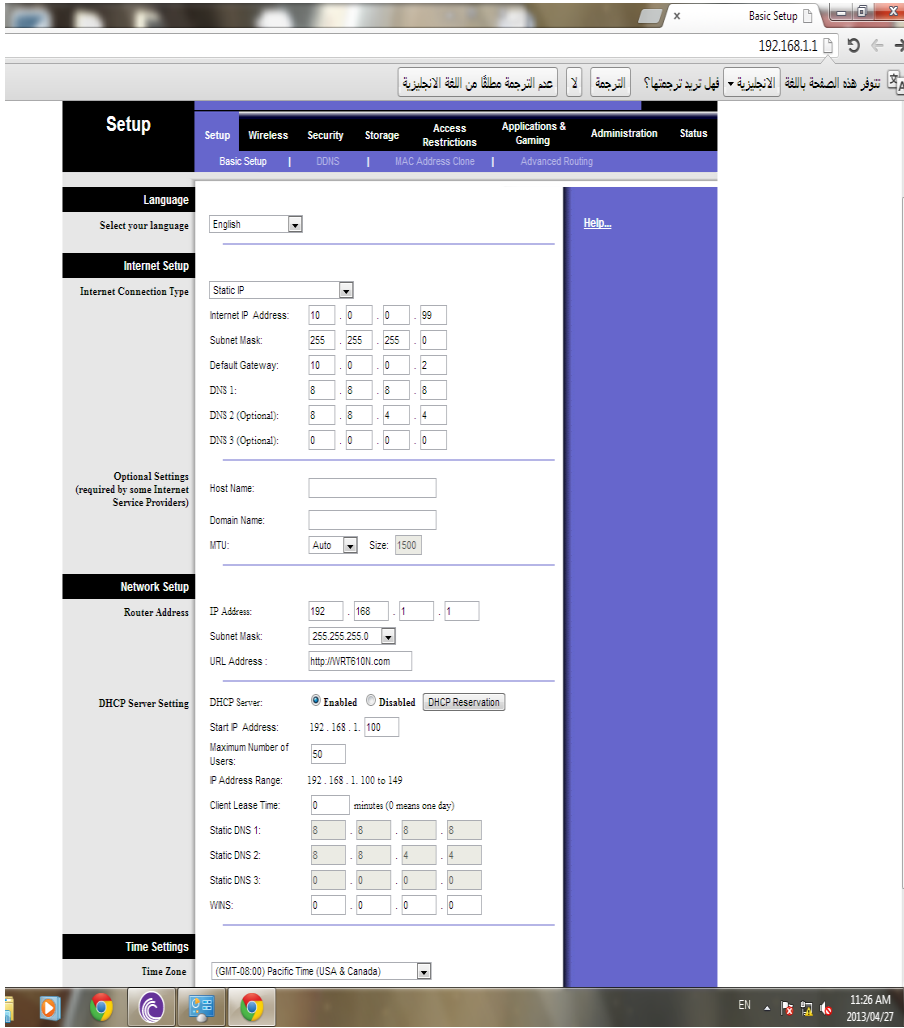
سوف يقوم بتحديد

المدى IP Address يبدأ

مثلا من

192.168.1.50 وينتهي

192.168.1.200



أما القوائم الثانية فهي Wireless وفيها مجموعة قوائم أيضا منها

## Basic setup wireless

تتكون من جزأين جزءاً خاصاً IEE 802.11 A التي تستخدم كما ذكرنا سابقاً تردد 5 GHz

The screenshot shows the Linksys wireless configuration interface. The top navigation bar includes 'Wireless', 'Setup', 'Security', 'Storage', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. The 'Wireless' section is active, showing 'Basic Wireless Settings', 'Wireless Security', 'Wireless MAC Filter', and 'Advanced Wireless Settings'. The '2.4GHz Wireless Settings' section is expanded, showing the following configuration: Network Mode: Mixed, Network Name (SSID): TaskSystem, Radio Band: Standard - 20MHz Channel, Wide Channel: Auto, Standard Channel: Auto, and SSD Broadcast: Enabled. A red arrow points to the 'TaskSystem' SSID field. The '5GHz Wireless Settings' section is collapsed. At the bottom, there are 'Save Settings' and 'Cancel Changes' buttons.

أما الجزء الثاني وهو الذي سوف نركز عليه فيخصص IEE 802.11 G,B والذي يستخدم تردد 2.4 GHz

نستطيع من هذا القوائم تغيير اسم الاكسس بيونت من الاسم الافتراضي الي أي اسم نريده

أيضا نستطيع الغاء خاصية broadcast للاكسس بيونت حيث لن تظهر اسم الاكسس بيونت للاجهازه المحيطة والشكل التالي بوضوح الصورة أكثر

## Wireless security

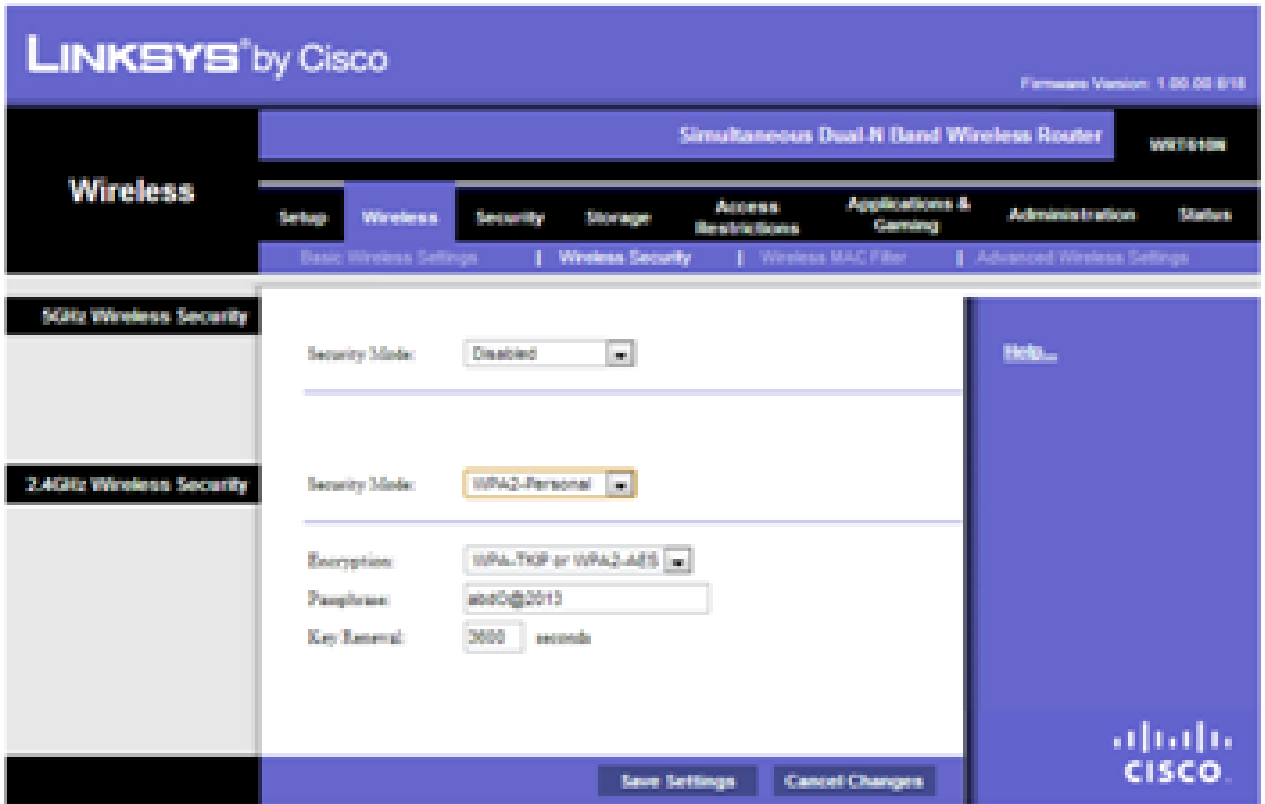
حيث يعتبر من أهم الأشياء التي يجب علينا القيام بها وهي حماية الاكسس بيونت من الدخول الغير مسرح بهو باختيار نظام التشفير والحماية حيث كل شي شخص يريد الدخول علي الاكسس بيونت يجب التحقق منه عن طريق كلمة السر وبالتالي حماية الشبكة من الدخول الغير مصرحة بيه

أيضا يتم فيها اختيار نوع التشفير مثلا WPA WPA2 WPA security Wep , personal WPA enterprise

وسوف نختار في هذا المثال WPA 2 personal

حيث يتم ادخال كلمة المرور التي من الافضل ان تكون معقدة وصعبه التخمين

## Wireless Mac filter



The screenshot displays the Linksys by Cisco wireless security configuration interface. The main heading is 'LINKSYS<sup>®</sup> by Cisco'. The page is titled 'Simultaneous Dual-Band Wireless Router' with the model number 'WRT54GL'. The navigation menu includes 'Setup', 'Wireless', 'Security', 'Storage', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. The 'Wireless Security' section is active, showing settings for both 5GHz and 2.4GHz bands. The 5GHz band is currently disabled. The 2.4GHz band is configured with 'Security Mode' set to 'WPA2-Personal', 'Encryption' set to 'WPA-TKIP or WPA2-AES', a 'Passphrase' of 'a040@2013', and a 'Key Interval' of '3000 seconds'. A 'Help...' link is available on the right side. At the bottom, there are 'Save Settings' and 'Cancel Changes' buttons, along with the Cisco logo.



حيث تعتبر أكثر أنواع الحماية وثوقا حيث يسمح فقط للأجهزة التيتم تخزين MAC Address امتاعها في الاكسس بيونت بدخول والاتصال بالشبكة اللاسلكية فقل ان يتم الاتصال بالاكسس بيونت فان الاكسس بيونت تقوم بالبحث علي MAC Address الجهاز

الذي يريد

الاتصال به

فاذا وجدا هذا

MAC فسوف

يسمح له

بالاتصال

بالشبكة. لمن لا

يعرف MAC

Address فهو

عنوان فريد

للكرت

الشبكات

بحيث لا يتكرر

هذا الرقم في

جميع انواع

كراوات

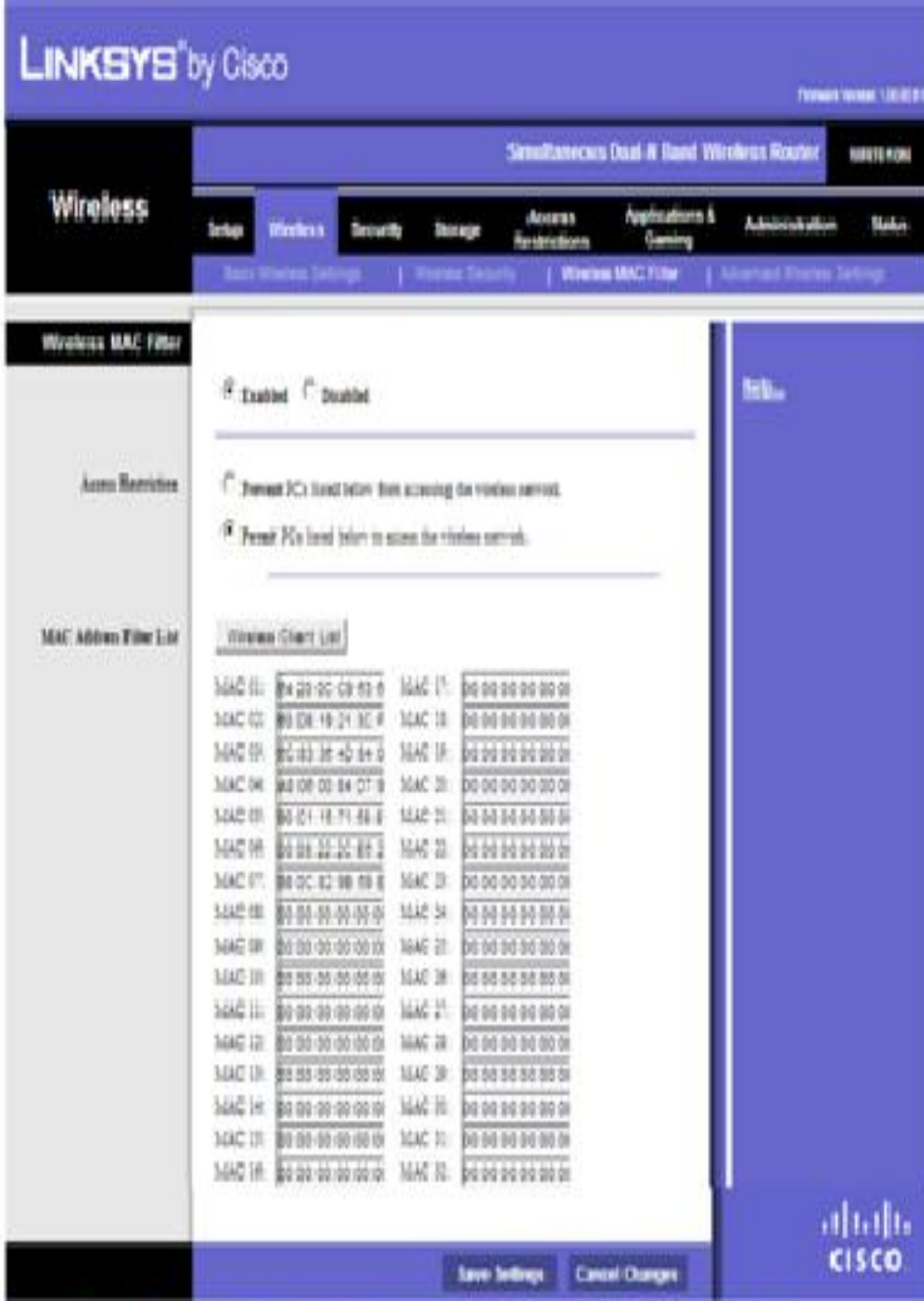
الشبكات في

العالم ويتكون

من 24 bit 48

للشركة المصنع

IEEE تعطي 24



# Administrations

ومن أهم قوائمها Management حيث نستطيع من خلالها تغيير اسم المستخدم وكلمة المرور حيث من المهم تغييرهم حتي لا يتسني لاحد الدخول علي الاكسس بيونت وتغيير اعدادتها لان كلمة المرور واسم المستخدم معلومة لجميع لأنها افتراضية

The screenshot displays the Linksys WRT610N router administration interface. The browser address bar shows the URL 192.168.1.1/Management.asp. The interface is titled "LINKSYS by Cisco" and "Firmware Version: 1.00.00 B18". The main navigation menu includes "Administration", "Setup", "Wireless", "Security", "Storage", "Access Restrictions", "Applications & Gaming", and "Status". The "Administration" section is expanded, showing "Management", "Log", "Diagnostics", "Factory Defaults", and "Firmware Upgrade". The "Management" section is further expanded, showing "Router Access", "Local Management Access", "Remote Management Access", "Upnp", and "Backup and Restore". The "Router Access" section is active, showing fields for "Router Password" and "Re-Enter to Confirm". The "Local Management Access" section shows "Access via" (HTTP checked, HTTPS unchecked) and "Access via Wireless" (Enabled selected, Disabled unselected). The "Remote Management Access" section shows "Remote Management" (Enabled unselected, Disabled selected), "Access via" (HTTP unchecked, HTTPS unchecked), "Remote Upgrade" (Enabled unselected, Disabled selected), "Allowed Remote IP Address" (Any IP Address selected), and "Remote Management Port" (8080). The "Upnp" section shows "Upnp" (Enabled selected, Disabled unselected), "Allow Users to Configure" (Enabled selected, Disabled unselected), and "Allow Users to Disable Internet Access" (Enabled unselected, Disabled selected). The "Backup and Restore" section shows "Backup Configurations" and "Restore Configurations" buttons. The interface also includes a "Help..." link and "Save Settings" and "Cancel Changes" buttons at the bottom.

آخر القوائم التي سوف نتكلم عليها هي status

وهي لا يتم فيها تكون أعداد ولكن تكون خاصة بعرض حالة ووضع الاكسس بيونت وتتكون من 3 قوائم

## Router

وتعرض معلومات عن Router من حيث MAC Address الوقت الحالي لاكسس بيونت معلومات عن IP Address من حيث

- Internet IP address
- Subnet mask
- Default gateway
- DNS S

The screenshot shows the Linksys router status page. The top navigation bar includes 'Status', 'Setup', 'Wireless', 'Security', 'Storage', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. The 'Status' page is divided into two main sections: 'Router Information' and 'Internet Connection'.

**Router Information:**

Firmware Version:	1.00.00 B18 Aug. 16, 2008
Firmware Verification:	6777e43f6991f668cd263824683acc
Current Time:	Mon, 29 Apr 2013 03:43:24
Internet MAC Address:	00:23:69:14:C9:2F
Server Name:	WRT610N
Host Name:	
Domain Name:	

**Internet Connection:**

Connection Type:	Static
Internet IP Address:	10.0.0.99
Subnet Mask:	255.255.255.0
Default Gateway:	10.0.0.1
DNS1:	8.8.8.8
DNS2:	8.8.4.4
DNS3:	
MTU:	1500

A 'Refresh' button is located at the bottom right of the Internet Connection section. The Cisco logo is visible in the bottom right corner of the page.

## Local network

وتحوى بيانات على Ip Address الاكسس بيونت و subnet mask و Mac Address  
ايضا تحوى بيانات على DHCP من حيث التفعيل وعدم التفعيل وبداية ونهاية رنج IP Address

The screenshot displays the Linksys by Cisco web interface. At the top, it shows the logo and the firmware version: 1.00.00 B18. The main navigation bar includes 'Status', 'Setup', 'Wireless', 'Security', 'Storage', 'Access Restrictions', 'Applications & Gaming', and 'Administration'. The 'Status' page is selected, and the 'Local Network' tab is active. The 'Local Network' section displays the following information:

Local MAC Address:	00-21-49-14-C9-2E
Router IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0

The 'DHCP Server' section shows:

DHCP Server:	Enabled
Start IP Address:	192.168.1.100
End IP Address:	192.168.1.149

A 'DHCP Client Table' button is visible below the DHCP Server information. The Cisco logo is present in the bottom right corner of the interface.

# wireless network

وتحوي بيانات علي كل من Mode ,Access point ,Mac Address ,Name

نوع واسم وعنوان الاكسس بيونيت ورقم القناة المستخدمة في عملية الاتصال

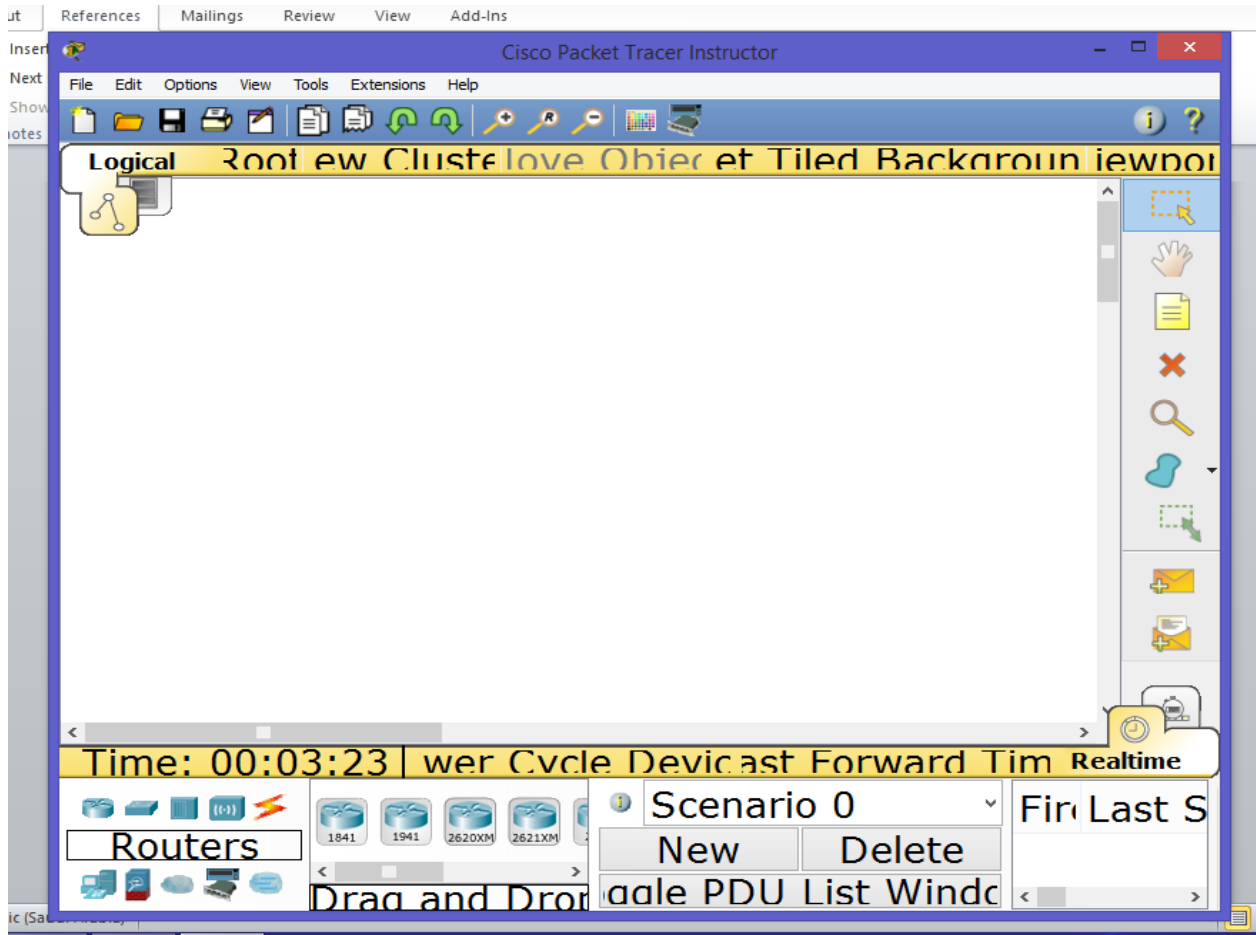
The screenshot displays the Linksys by Cisco web interface for a 'Simultaneous Dual-Band Wireless Router'. The interface is divided into a top navigation bar and a main content area. The top bar includes the Linksys logo, the router model, and the firmware version (1.00.00.019). The main content area is organized into a 'Status' sidebar and a central configuration table. The table lists settings for two wireless networks: 5G and 2.4G. The 5G network is configured with a MAC address of 00:23:49:14:C9:31, Mode: Mixed, Network Name (SSID): Suleym\_media, Radio Band: Wide - 40MHz Channel, Wide Channel: 36, Standard Channel: 36, Security: Disabled, and SSID Broadcast: Disabled. The 2.4G network is configured with a MAC address of 00:23:49:14:C9:30, Mode: Mixed, Network Name (SSID): LAB, Radio Band: Standard - 20MHz Channel, Wide Channel: N/A, Standard Channel: 1, Security: WPA2-Personal, and SSID Broadcast: Enabled. The Cisco logo is visible in the bottom right corner of the interface.

Network Type	MAC Address	Mode	Network Name (SSID)	Radio Band	Wide Channel	Standard Channel	Security	SSID Broadcast
5G Wireless Network	00:23:49:14:C9:31	Mixed	Suleym_media	Wide - 40MHz Channel	36	36	Disabled	Disabled
2.4G Wireless Network	00:23:49:14:C9:30	Mixed	LAB	Standard - 20MHz Channel	N/A	1	WPA2-Personal	Enabled

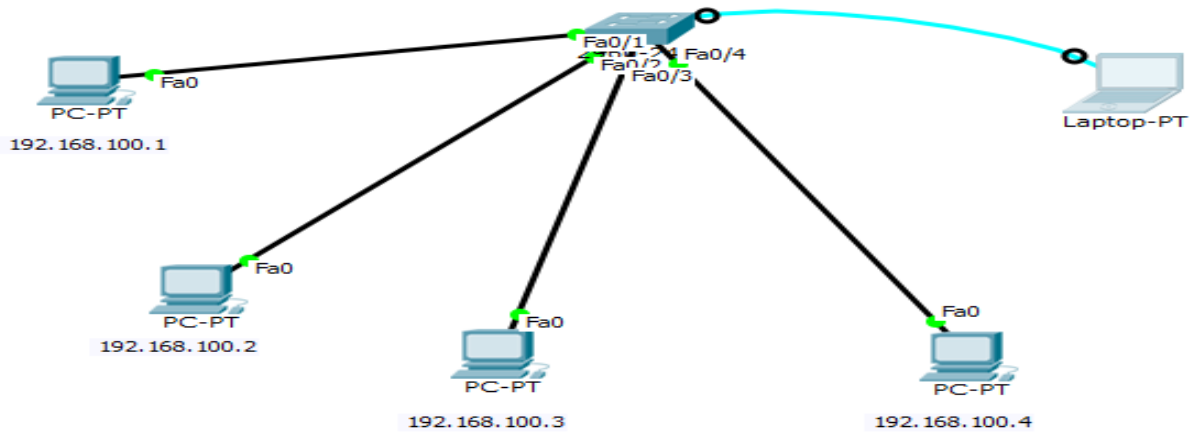
## LAB (3) make password on switch (Telnet+console+enable mode)

اعدادات كلمات المرور لل (Telnet+console+enable mode) لكل من switch أو router  
سوف نستخدم برنامج محاكاة للشبكات الخاصة بشركة Cisco Packet Tracer 6.1.1  
لان نقوم بشرح كيفية عمل البرنامج ولكن هناك مجموعة من الفيديوات توضح بشكل  
مفصل كيفية عمله

والشكل التالي يوضح شكل البرنامج



سوف نقوم بربط شبكة تتكون من اربع اجهزة ثم نقوم بإنشاء كلمات المرور



```
Switch>enable
Switch#config t
```

```
Switch(config)#line console 0 (make password on user mode or console mode)
```

```
Switch(config-line)#password 123456
Switch(config-line)#login
Switch(config-line)#exit
```

```
Switch(config)#enable password 123456789 (make password on enable password without encryption)
```

```
Switch(config)#enable secret 123 (make password on enable password with encryption)
```

```
Switch(config)#line vty0 4 (make password on telnet password)
```

```
Switch(config-line)#password 0000
```

```
Switch(config-line)#login
Switch(config-line)#exit
```

```
Switch(config)#interface vlan 1
```

```
Switch(config-if)#ip address 192.168.100.100 255.255.255.0
Switch(config-if)#no shutdown
```



Now on one of computer open run then ping the switch to ensure that there is connection

```
PC>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.100: bytes=32 time=0ms TTL=255
Reply from 192.168.100.100: bytes=32 time=0ms TTL=255
Reply from 192.168.100.100: bytes=32 time=0ms TTL=255
```

Then write telnet and Ip address of switch

```
PC>telnet 192.168.100.100
Trying 192.168.100.100 ...Open

User Access Verification

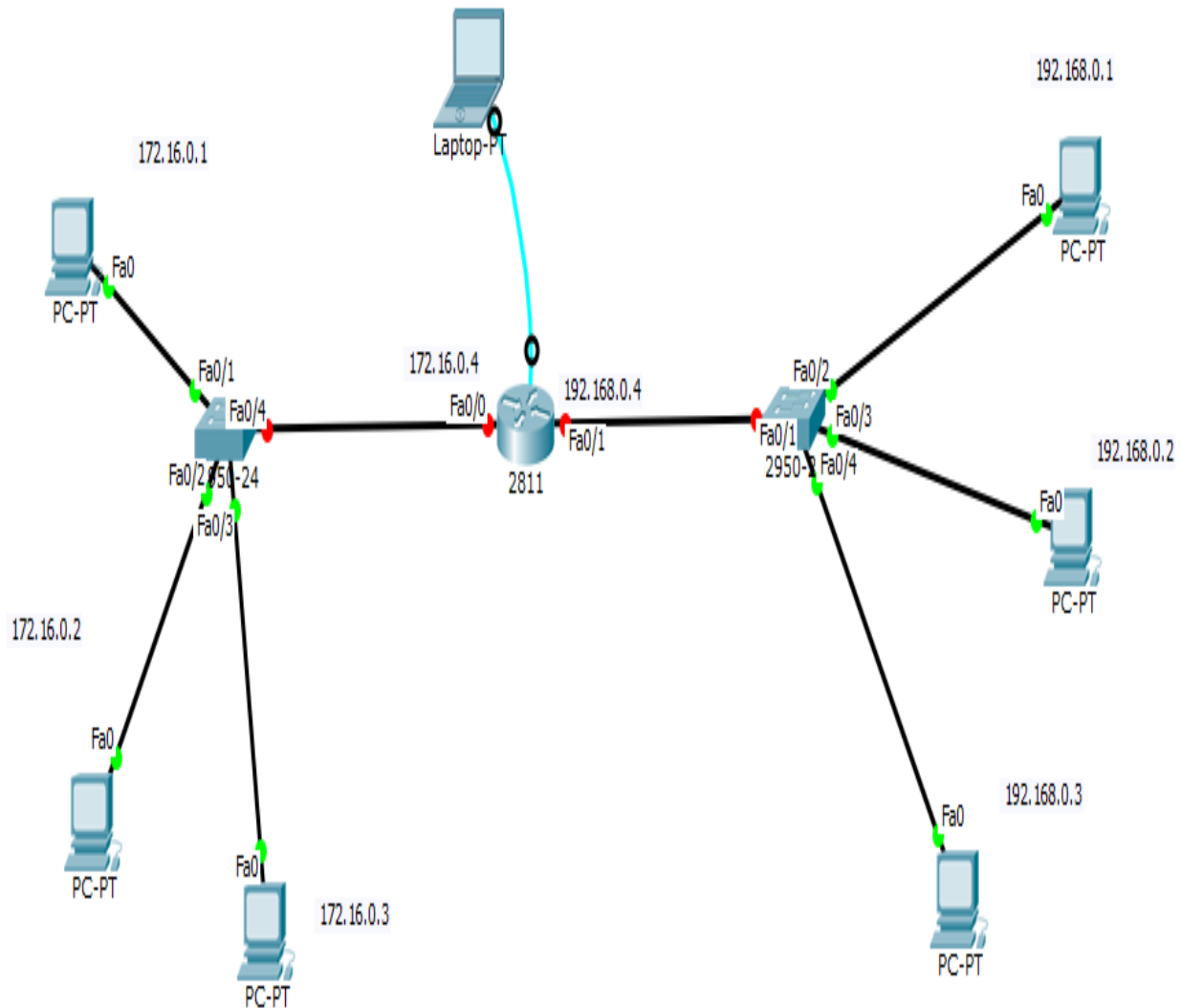
Password:
```

Now type password of telnet 0000 then password enable 123

```
Password:
Switch>ena
Switch>enable
Password:
Password:
Switch#config t
```

## LAB (4) How connect two difference networks by router

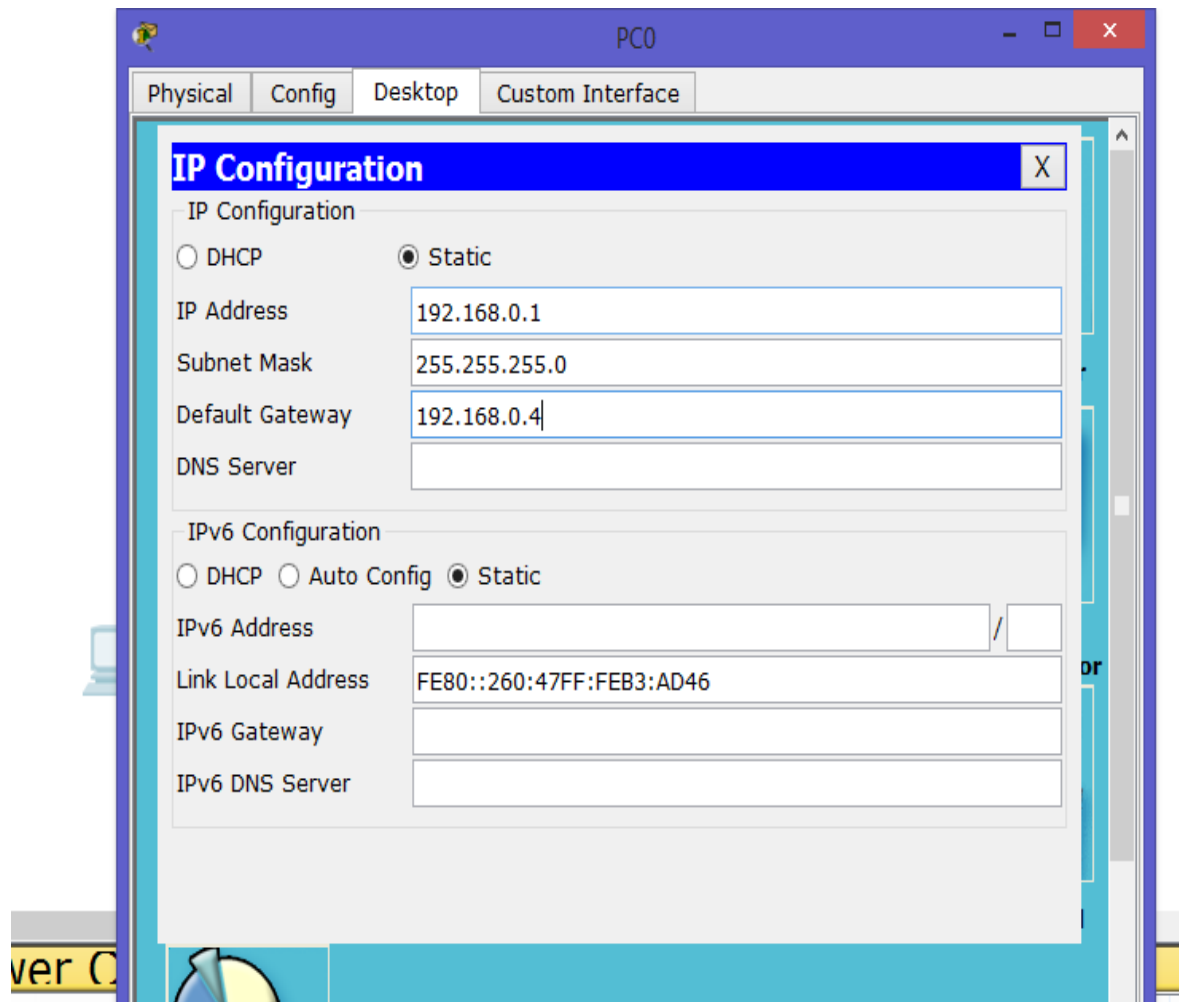
We will use private IP Class C and B as following :-



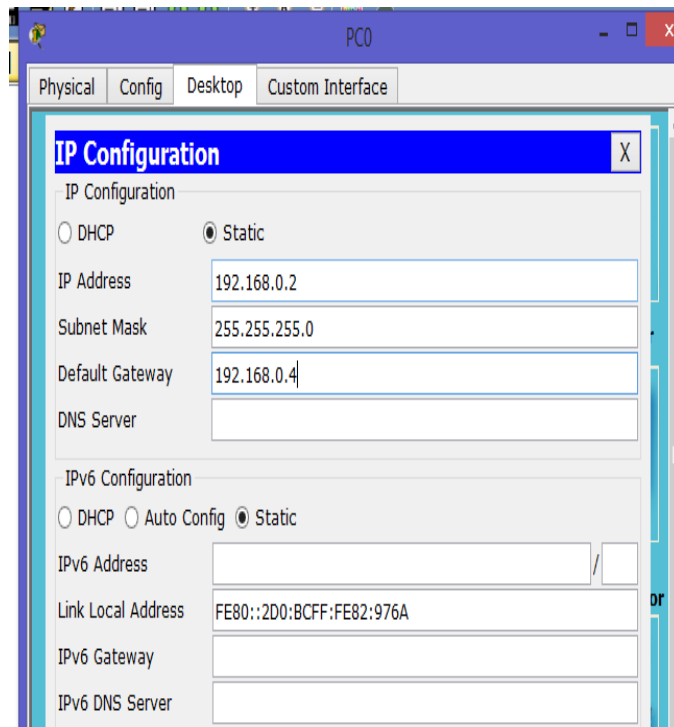
```
Router>enable
Router#config t
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 172.16.0.4 255.255.0.0
Router(config-if)#no shutdown
```

```
Router(config-if)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 192.168.0.4 255.255.255.0
Router(config-if)#no shutdown
```

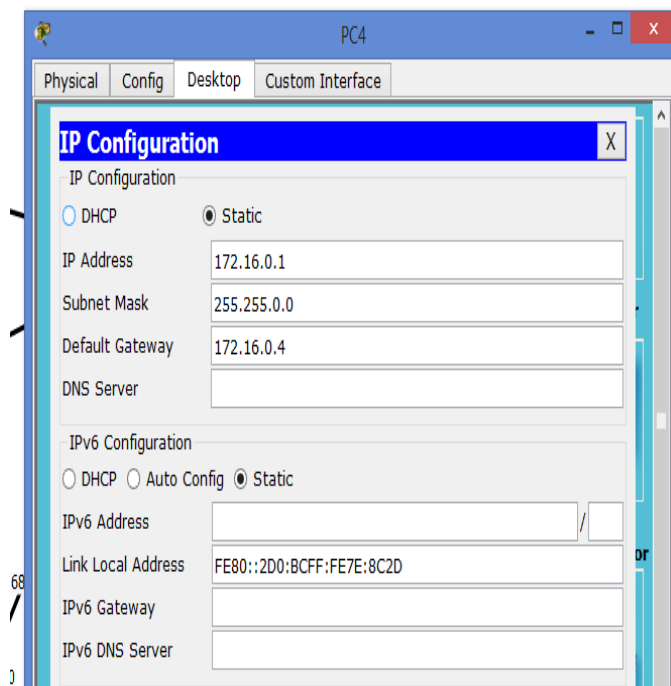
On each computer put default gateway 192.168.0.4



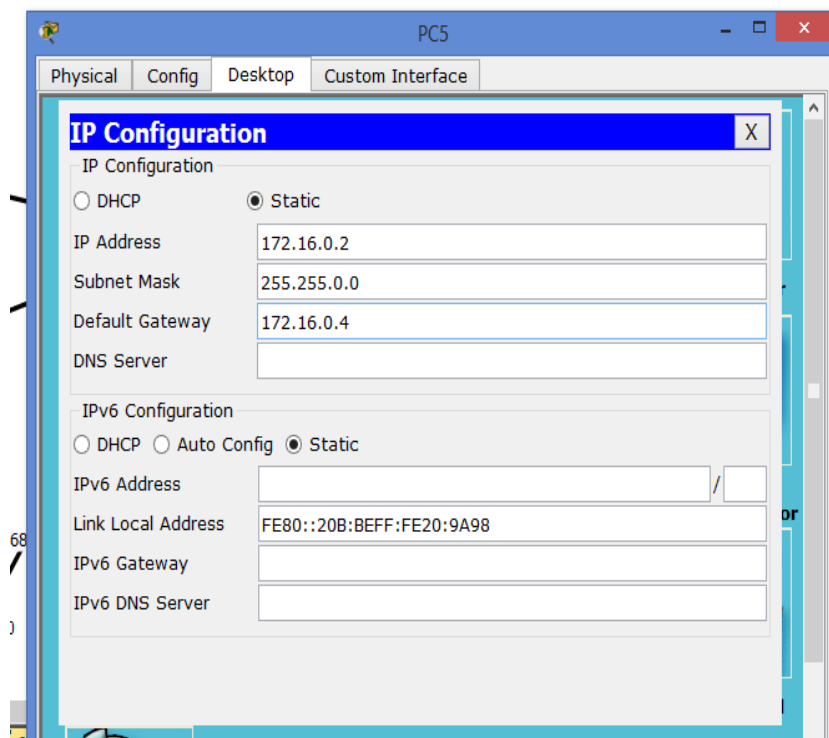
On pc 2



And same thing on all computer on class C  
After that put default gateway on class b



On pc2



Same that on all computer

- الآن نقوم باختبار اتصال من جهاز من شبكة 192.168.0.1 بجهاز من الشبكة الاخرى وليكن 172.16.0.1 كما في الشكل الاتي

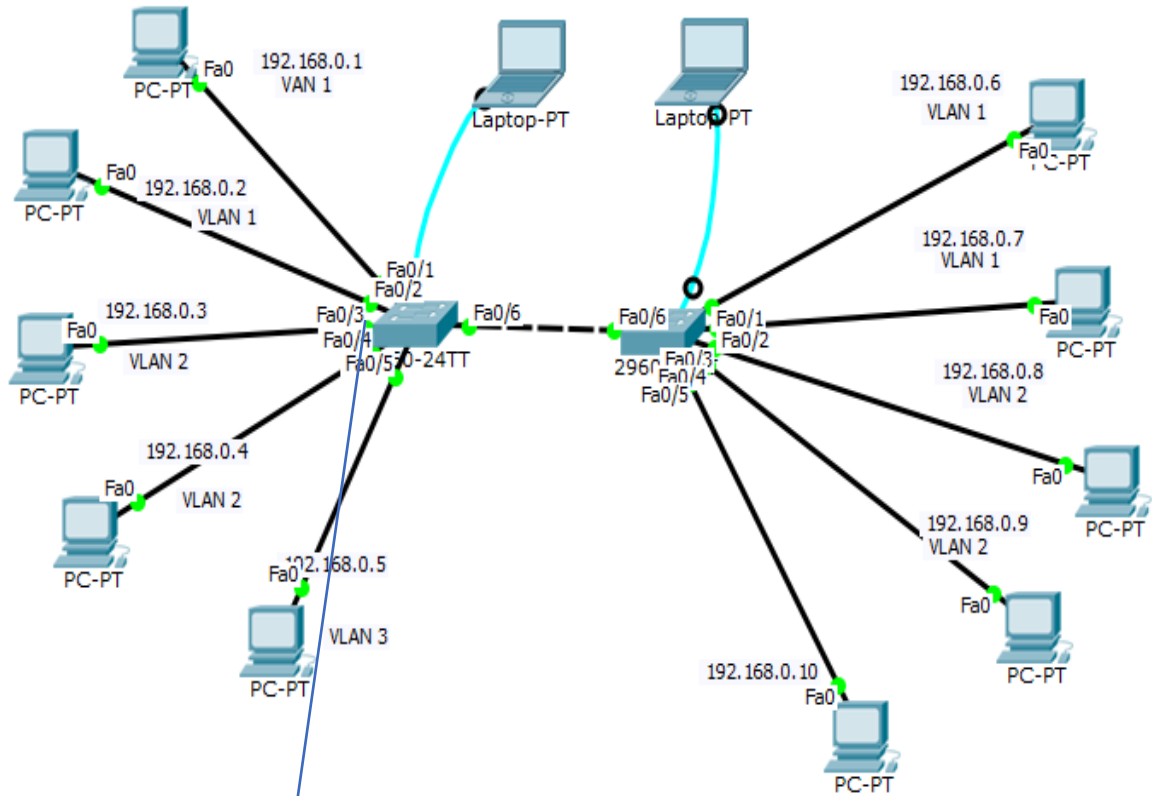
After then we will Ping on another network

Ping 172.16.0.4

```
Pinging 172.16.0.1 with 32 bytes of data:
Reply from 172.16.0.1: bytes=32 time=0ms TTL=127
Reply from 172.16.0.1: bytes=32 time=0ms TTL=127
Reply from 172.16.0.1: bytes=32 time=0ms TTL=127
Reply from 172.16.0.1: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

## *LAB (5) Create VLAN on switch*



Configuration on switch 1

```

Switch>enable
Switch#config t
Switch(config)#interface fastEthernet 0/1          (enter to interface)
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1        (assign interface to vlan )
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1
Switch(config-if)#exit

Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/6
Switch(config-if)#switchport mode trunk

```

---

## Configuration on switch 2

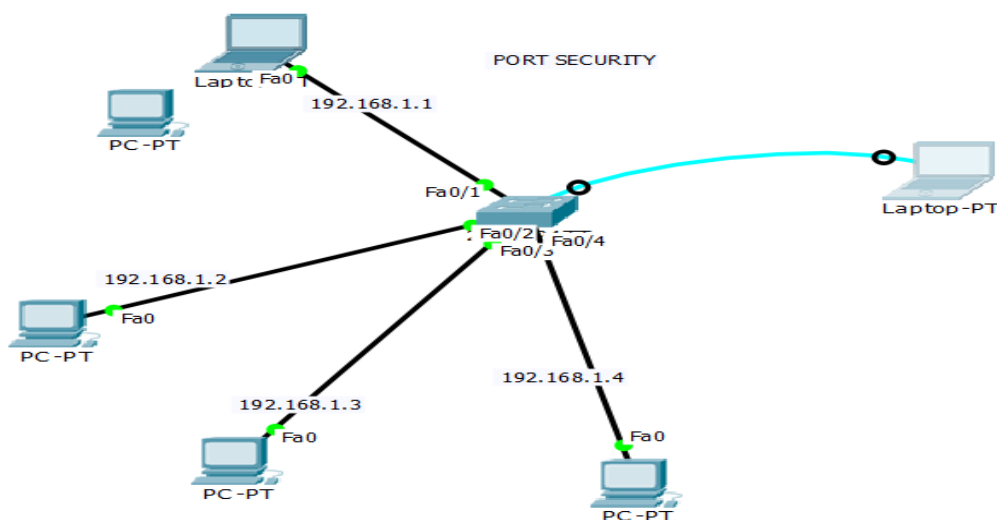
```
Switch>enable
Switch#config t
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1
Switch(config-if)#exit

Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/6
Switch(config-if)#switchport mode trunk
```

(mode of interface trunk to all pass all vlan)

---

## LAB(6) Port Security





```

Switch>
Switch>enable
Switch#config t
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security                (enable security on
interface )
Switch(config-if)#switchport port-security mac-address sticky (assign make address to
switch)
Switch(config-if)#switchport port-security maximum 1      (number of device on
interface )
Switch(config-if)#switchport port-security violation shutdown (shutdown ,protect,restrict)
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown

Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown

Switch(config)#interface fastEthernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown

```



# References



*[1] Available On line :*

- **CompTIA® Network N10-006 Cert Guide,**

*[2] Available On line :*

- **TCP/IP protocol suite / Behrouz A. Forouzan.—4th ed**

*[3] Available Online :*

- **CCENT/CCNA ICDN1-105,**

*[4] Available On line :*

- **" CCNA 200-301 Volume 1 Official Cert Guide,**