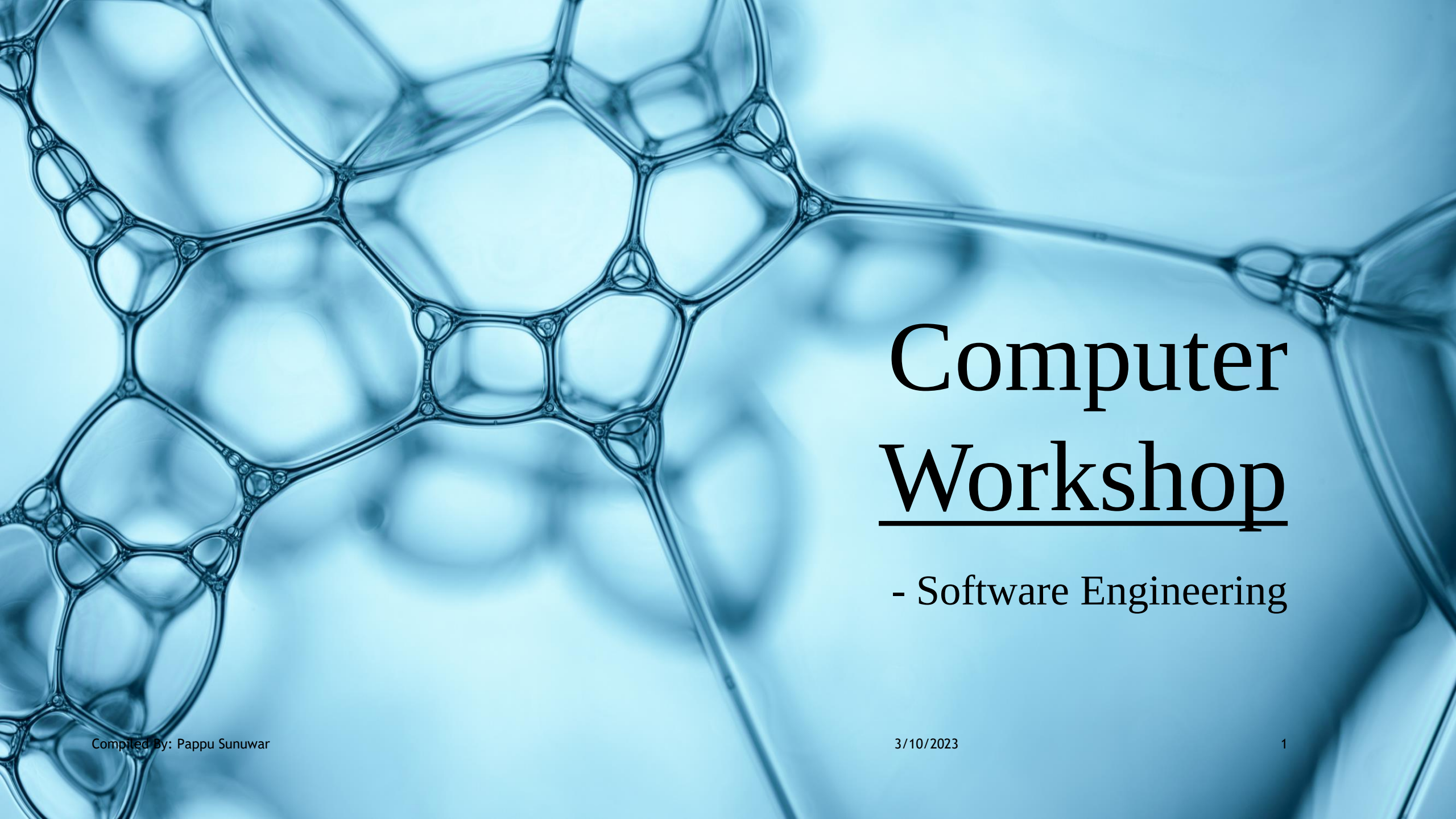
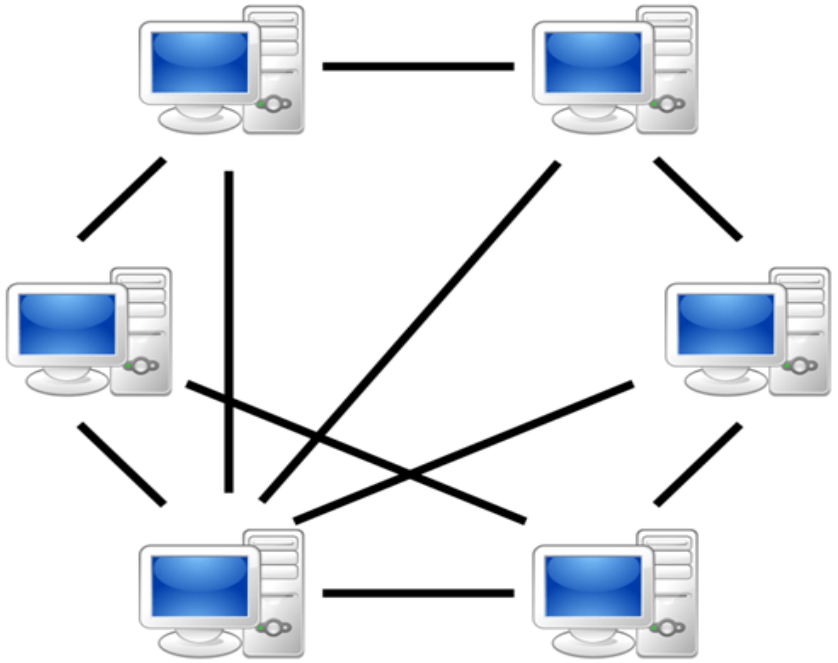


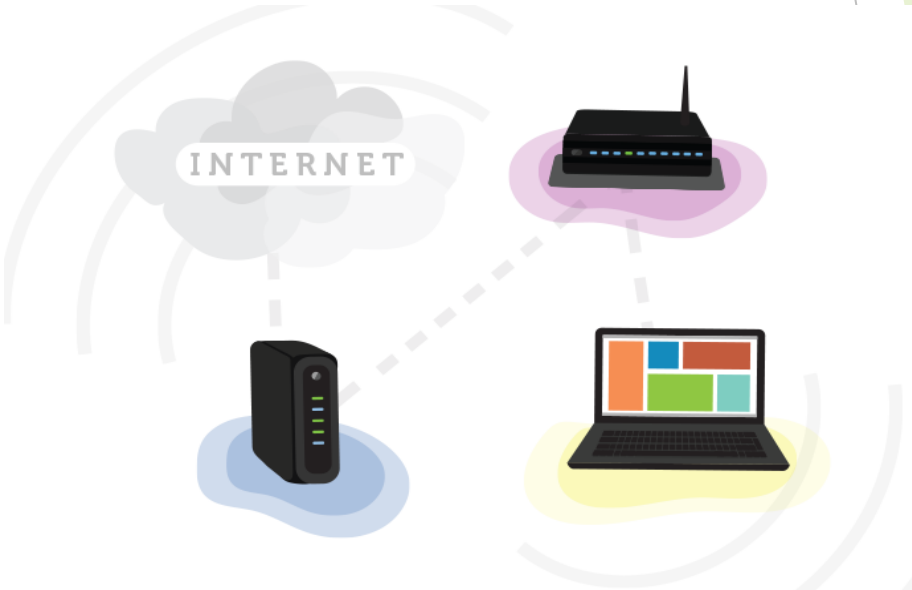
Computer Workshop

- Software Engineering

Unit-05

Networking and Internet Setup



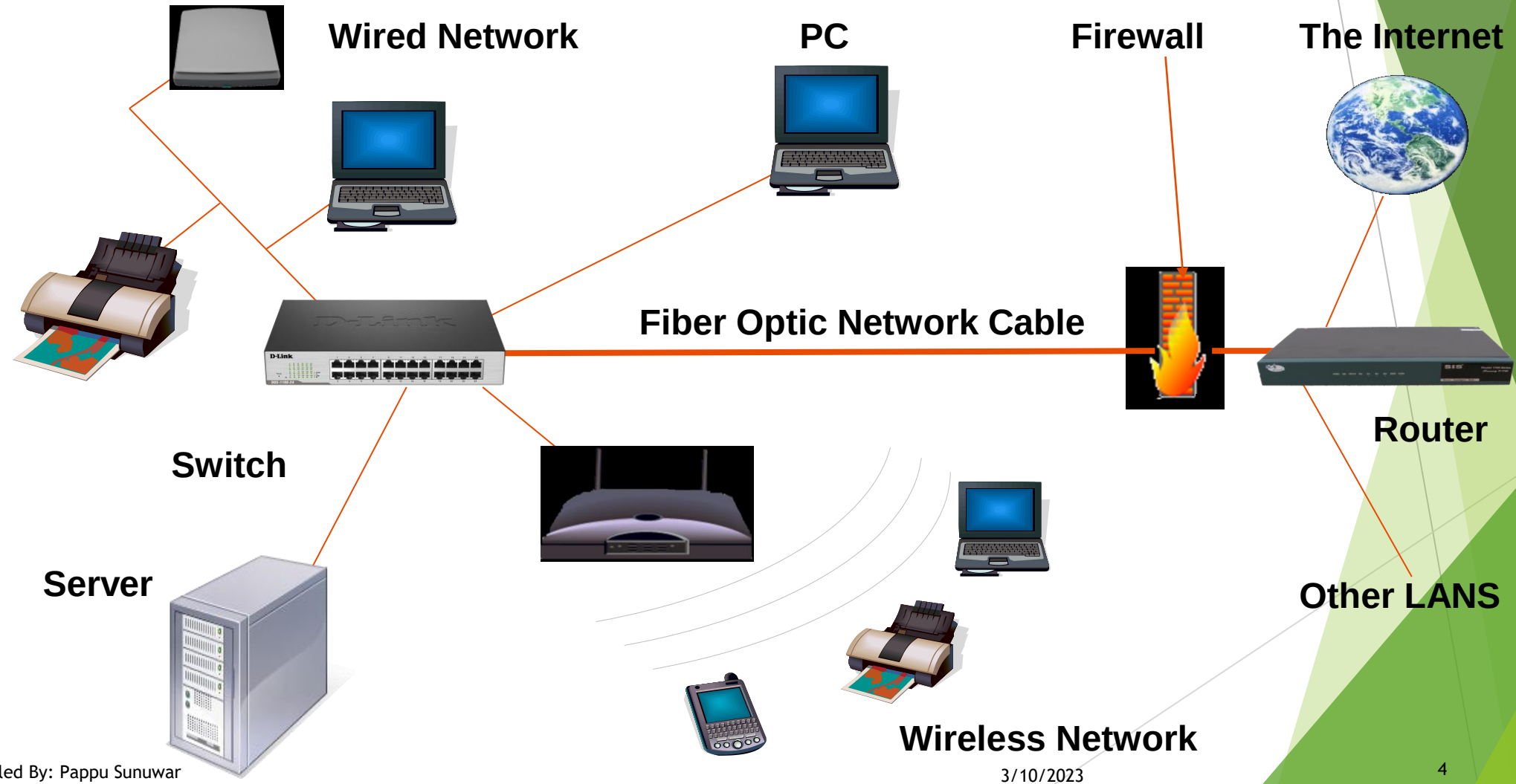


5.1 INTRODUCTION TO COMPUTER NETWORK, NETWORK TOPOLOGIES, WIRED AND WIRELESS NETWORKING MEDIA

What is computer network?

- A computer network is a group of computers/devices(Nodes) that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes.

The Network Diagram



The Networking Devices(Nodes)

1. NIC Card
2. Repeater
3. Hub
4. Switch
5. Router
6. AP
7. Firewall

1. Network Interface Card

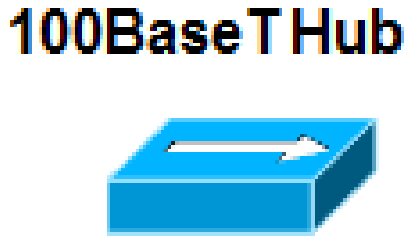
- NIC is used to physically connect host devices to the network media.
- A NIC is a printed circuit board that fits into the expansion slot of a bus on a computer motherboard.
- It can also be a peripheral device. NICs are sometimes called network adapters.
- Each NIC is identified by a unique code called a Media Access Control (MAC) address.
- This address is used to control data communication for the host on the network.

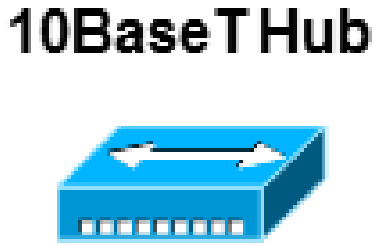
2. Repeaters

- A repeater is a network device used to regenerate a signal.
- Repeaters regenerate analog or digital signals that are distorted by transmission loss due to attenuation(any reduction in the strength of a signal.
- A repeater does not make an intelligent decision concerning forwarding packets

3. Hubs

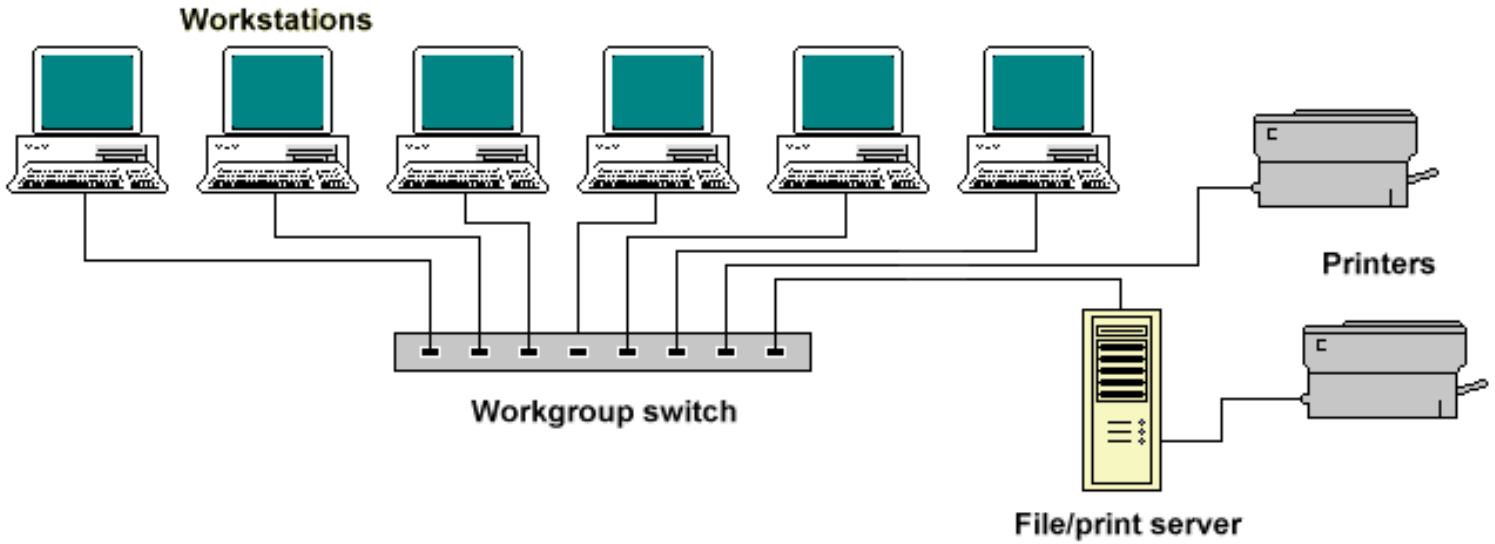
- Hubs concentrate on connections.
- In other words, they take a group of hosts and allow the network to see them as a single unit. This is done passively, without any other effect on the data transmission.
- Active hubs concentrate hosts and also regenerate signals.





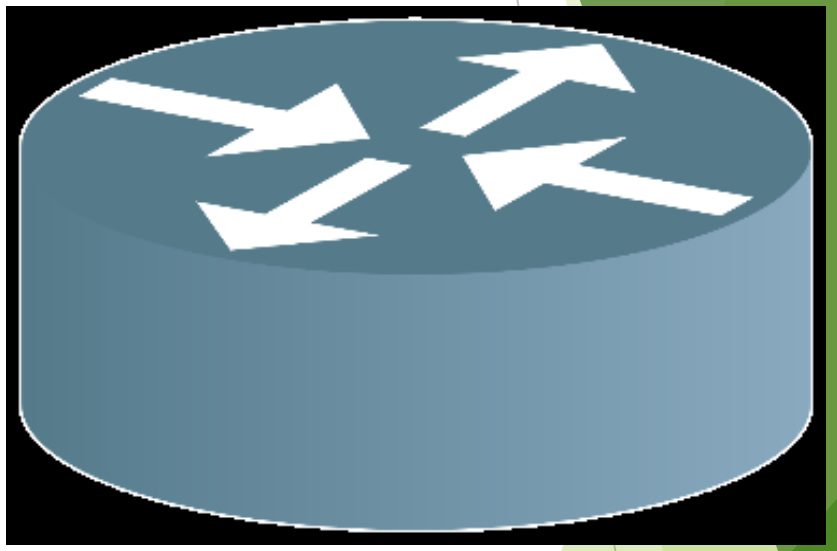
5. Switches

- Switches add more intelligence to data transfer management.
- They can determine if data should remain on a LAN and transfer data only to the connection that needs it.
- Another difference between a bridge and switch is that a switch does not convert data transmission formats



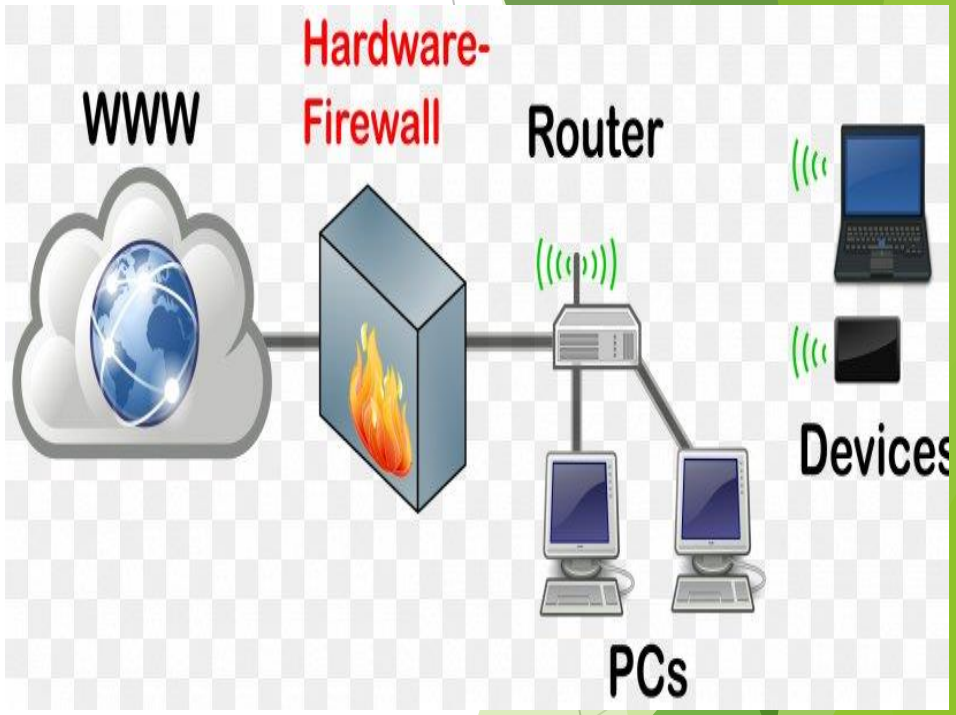
6. Routers

- Routers have all the capabilities listed above.
- Routers can regenerate signals, concentrate multiple connections, convert data transmission formats, and manage data transfers.
- They can also connect to a WAN, which allows them to connect LANs that are separated by great distances.



8. Firewall

- A firewall is a network device or software for controlling network security and access rules.
- Firewalls are inserted in connections between secure internal networks and potentially insecure external networks such as the Internet.
- Firewalls are typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones.
- The vital role firewalls play in network security grows in parallel with the constant increase in cyber attacks.



Network Topologies:

- Network topology refers to the manner in which the links and nodes of a network are arranged to relate to each other.
- It defines the structure of the network.

A. Physical topology:- It define the actual layout of the wire or media.

1. Bus
2. Ring
3. Star
4. Tree(Hierarchical)
5. Mesh

B. Logical topology:- It defines how the hosts access the media to send data.

1. Broadcast
2. Token passing

C. Hybrid Topology

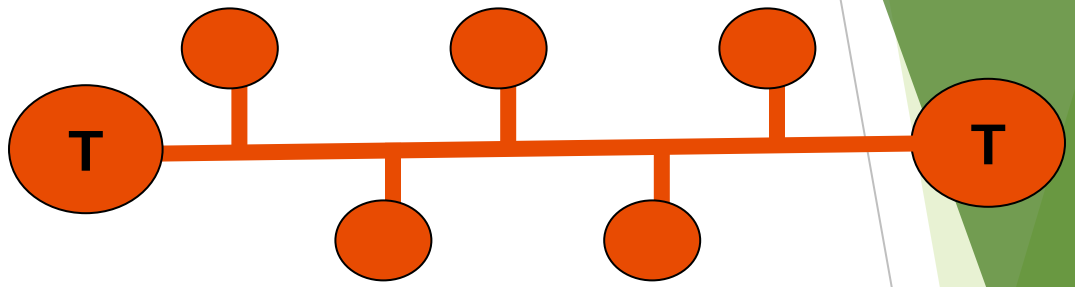
Importance of Network Topology

- The layout of a network has a direct impact on network functionality.
- Selecting the right topology can improve performance and data efficiency, optimize allocation of resources, and reduce operational costs.
- Software-created network topology diagrams are important references for diagnosing network connectivity problems, investigating network slowdowns, and generally troubleshooting issues.
- One of the primary uses of network topology is to define the configuration of various telecommunication networks, including computer networks, command and control radio networks, and industrial field busses.

1. Bus Topology

All devices are connected to a central cable, called bus or backbone.

There are terminators at each end of the bus that stops the signal and keeps it from traveling backwards.



Advantages:

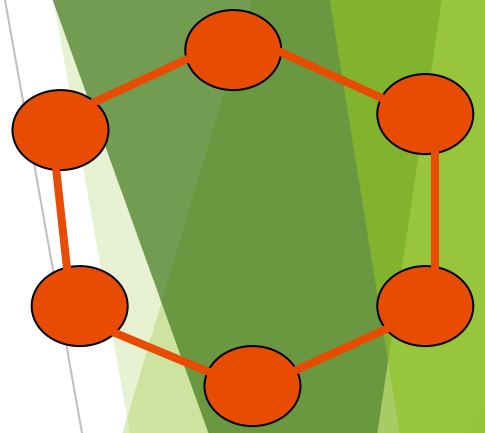
1. There is no central controller.
2. Control resides in each station
3. The less interconnecting wire is required.
4. Ease of installation.
5. Backbone cable can be laid along the most efficient path, and then connected to the nodes by drop lines of various lengths

Disadvantages:

1. It is possible that more than one station may attempt transmission simultaneously (collision or contention).
2. Difficult reconfiguration and fault isolation.
3. A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem.
4. The damaged area reflects signals in the direction of origin, creating noise in both directions

2. Ring Topology

- All devices are connected to one another in the shape of a closed loop.
- Each device is connected directly to two other devices, one on either side of it.



Advantages:

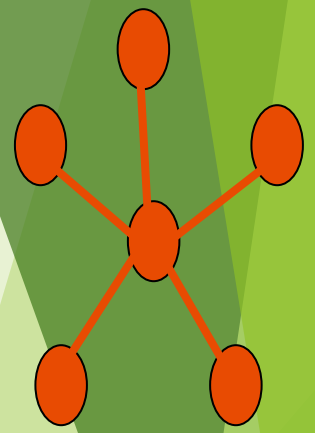
1. Avoids the collisions that are possible in the bus topology.
2. Each pair of stations has a point-to-point connection.
3. A signal is passed along the ring in one direction, from device to another, until it reaches its destination.
4. Relatively easy to install and reconfigure.
5. Fault isolation is simplified.

Disadvantages:

1. A break in the ring (such as station disabled) can disable the entire network.
2. Unidirectional traffic.

3. Star Topology

- All devices are connected to a central hub.
- Nodes communicate across the network by passing data through the hub or switch.



Advantages:

1. Easy to install and reconfigure.
2. Strong, if one link fails; only that link is affected. All other links remain active.
3. Easy fault identification and isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages:

1. The devices are not linked to each other.
2. If one device wants to send data to another, it sends it to the controller, which then relays the data to the other connected device.

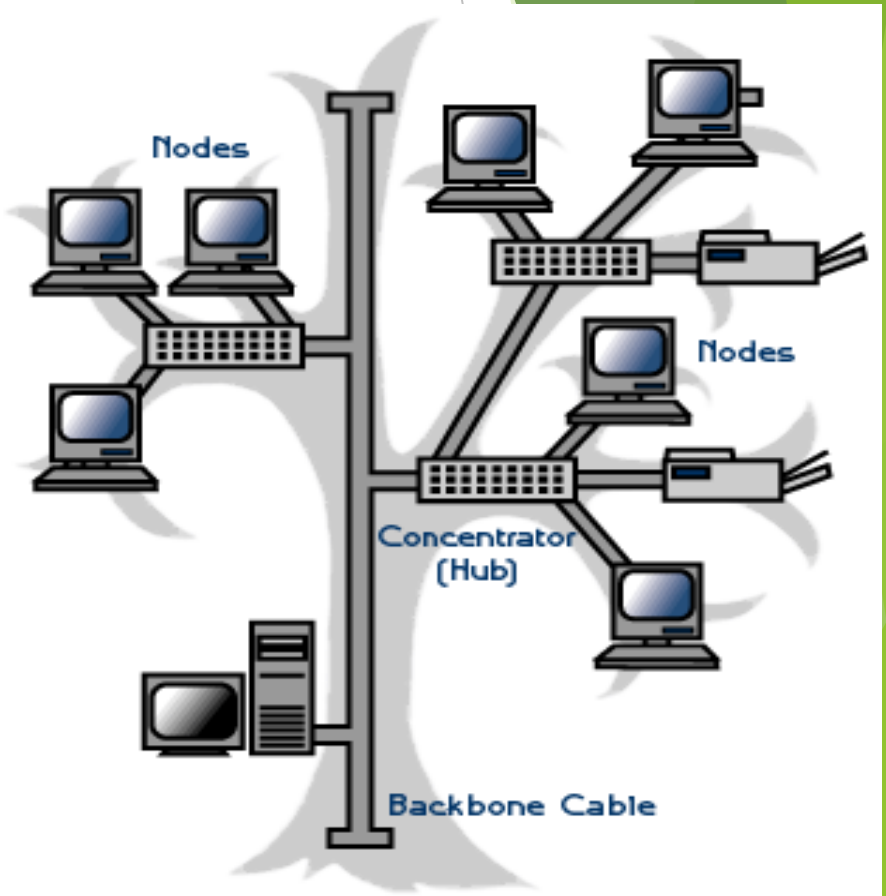
4. Tree/Hierarchical Topology

Advantages:

1. It allows more devices to be attached to a single central hub and can therefore increase the distance a signal can travel between devices.
2. It allows the network to isolate and prioritize communications from different computers.

Disadvantages:

1. The devices are not linked to each other.
2. If one device wants to send data to another, it sends it to the controller, which then relays the data to the other connected device.
3. The addition of secondary hubs brings two further advantages.

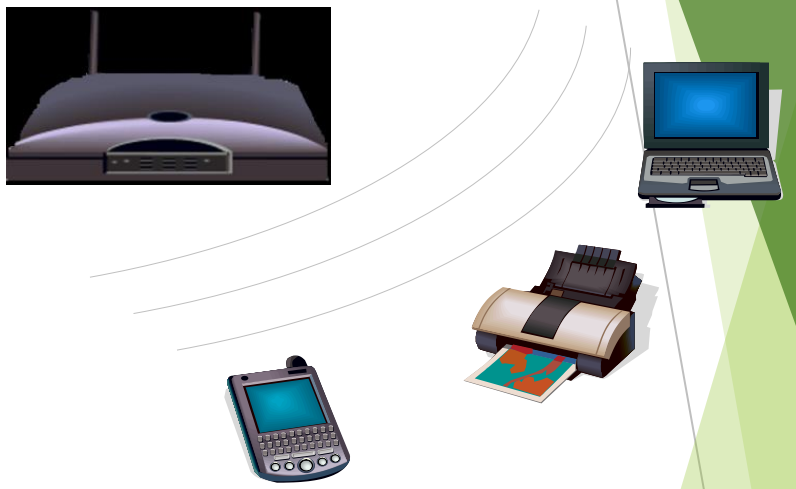


Wireless Networks

Wireless network is a type of computer network that uses wireless data connections for connecting network nodes.

Example

- Bluetooth
- Wi-Fi



Bluetooth

- **Bluetooth** is a short-range wireless technology standard used for exchanging data between fixed and mobile devices over short distances.
- The IEEE standardized Bluetooth as **IEEE 802.15.1**, but no longer maintains the standard.

Wi-Fi

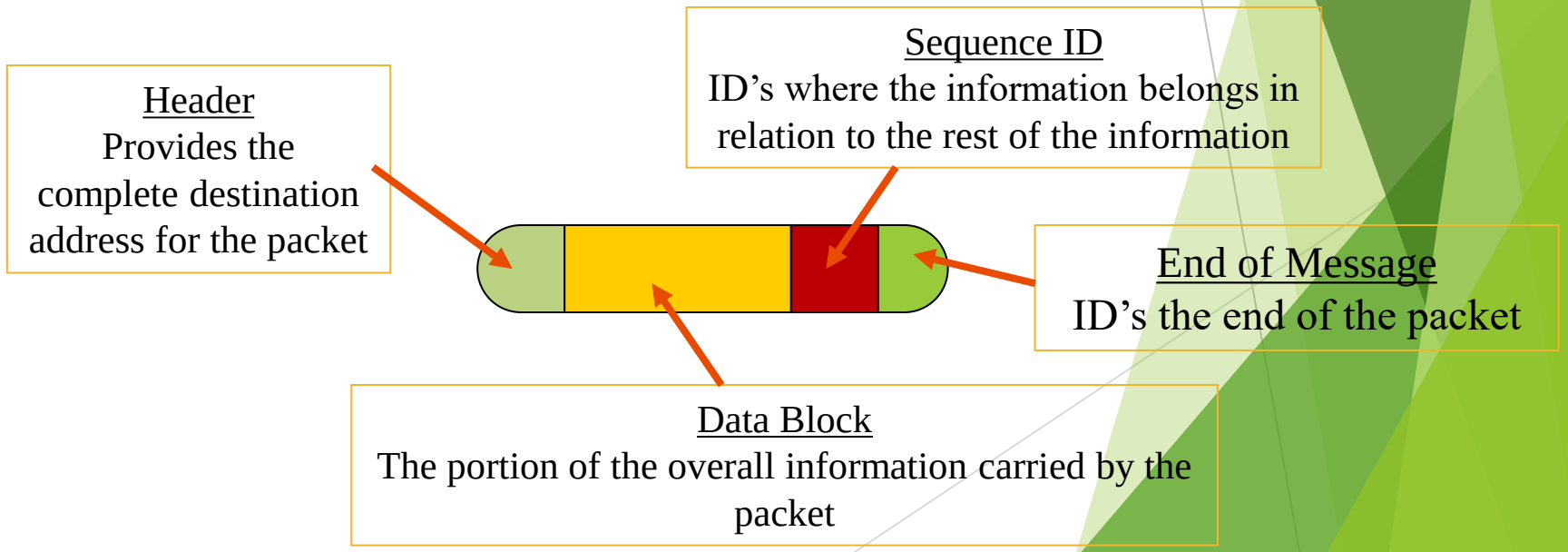
- Wi-Fi Stands for Wireless Fidelity.
- **Wi-Fi**, is a Local Area Wireless technology.
- Wi-Fi networks use radio technologies to transmit and receive data at high speed.
- It is based on the IEEE 802.11 family of standards.
- **Access point:** The access point is a wireless LAN transceiver or " base station" that can connect one or many wireless devices simultaneously to the internet

The Internet

The simplest definition of the Internet is that it's a network of computer networks

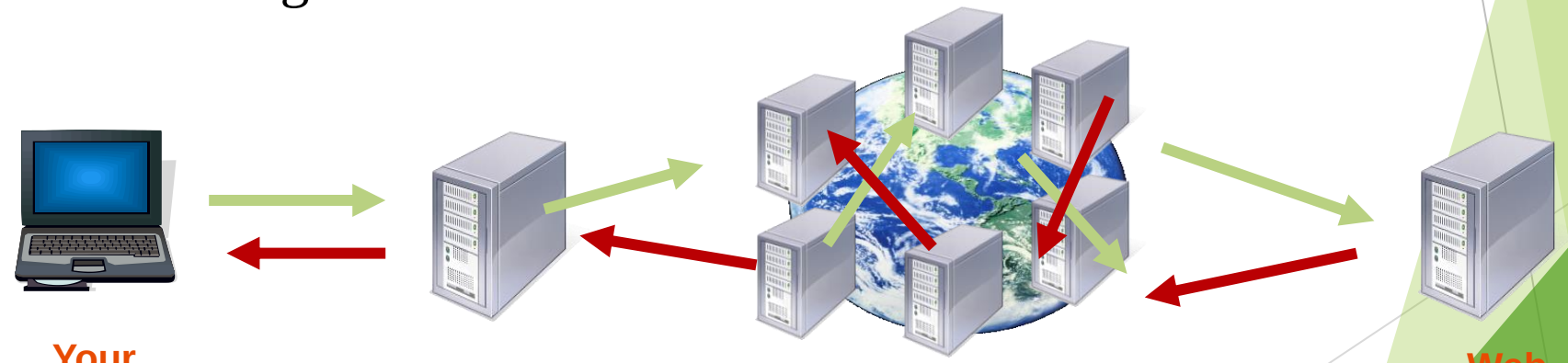
How Information Travel Through the Internet

A page on the Internet—whether it's full of words, images or both—doesn't come to you in one shipment. It's translated into digital information, chopped into 1500 byte pieces called PACKETS, and sent to you like a puzzle that needs to be reassembled. Each part of the packet has a specific function:



How Information Travel Through the Internet

When you connect to a Web site through an ISP and start exchanging information, there isn't a fixed connection between your computer and the Web server computer hosting the Web site. Instead, information is exchanged using the best possible path at that particular time. Special computers called routers determine these paths, avoiding slow links and favoring fast ones.



Cloud Computing

- ✓ Cloud computing is **Internet-based computing**, whereby **shared resources, software, and information** are provided to computers and other devices **on demand**, like the electricity grid.
- ✓ A Cloud is a type of **parallel and distributed system** consisting of a collection of interconnected and **virtualized computers** that are **dynamically provisioned** and presented as one or more unified computing resources based on **service-level agreements** established through negotiation between the service provider and consumers.

5.2 Network Cabling, Cable types and Connectors

The function of the media(cables and connectors) is to carry a flow of information through a LAN.

A. Wired Media:- A widely adopted *family* that uses copper and fibre media in local are network (LAN) technology are collectively known as Ethernet

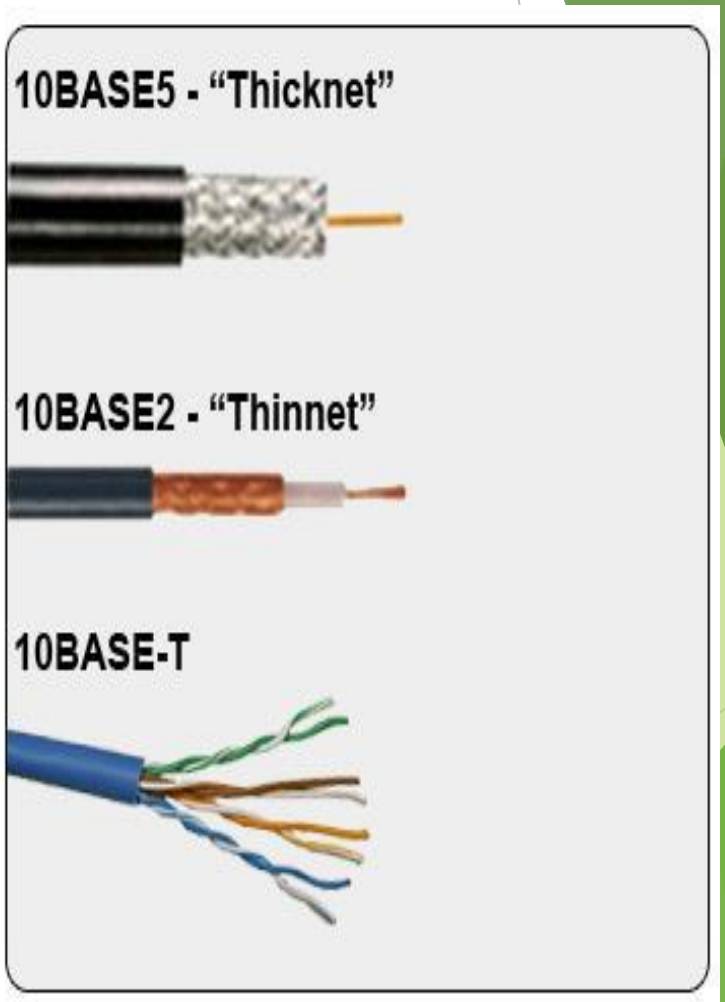
   1. Copper Cable
      a. Coaxial Cables
      b. Shielded Twisted Pair(STP)
      c. Unshielded Twisted Pair

   2. Fibre Optic Cable

B. Wireless Media:- use the atmosphere, or space, as the medium.

1. Copper Cable

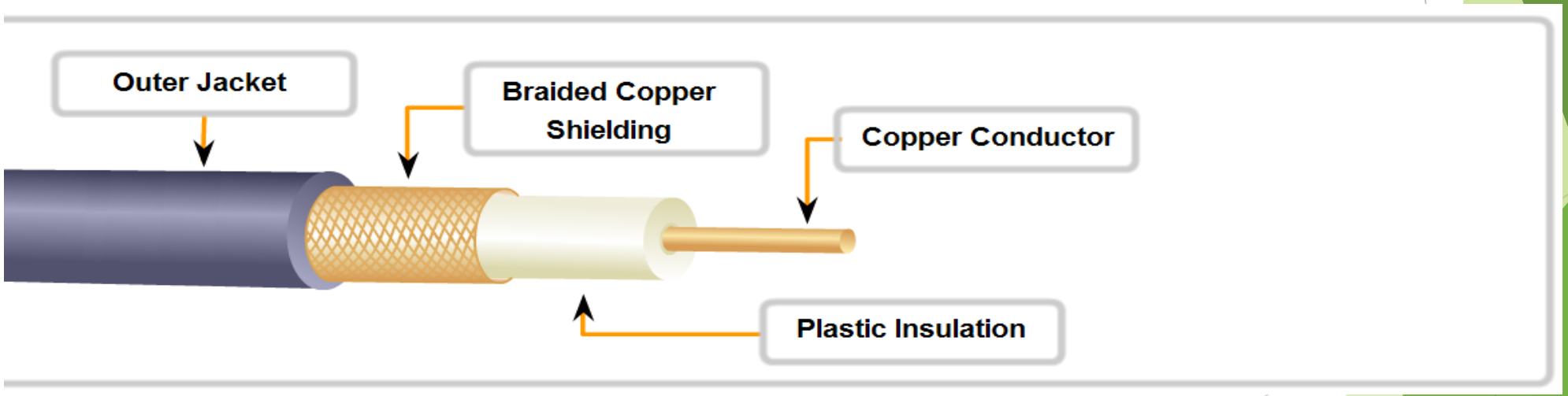
- The most common, easiest, quickest, and cheapest form of network media to install.
- The disadvantage of sending data over copper wire is that the further the signal travels, the weaker it becomes.



a. Coaxial Cable

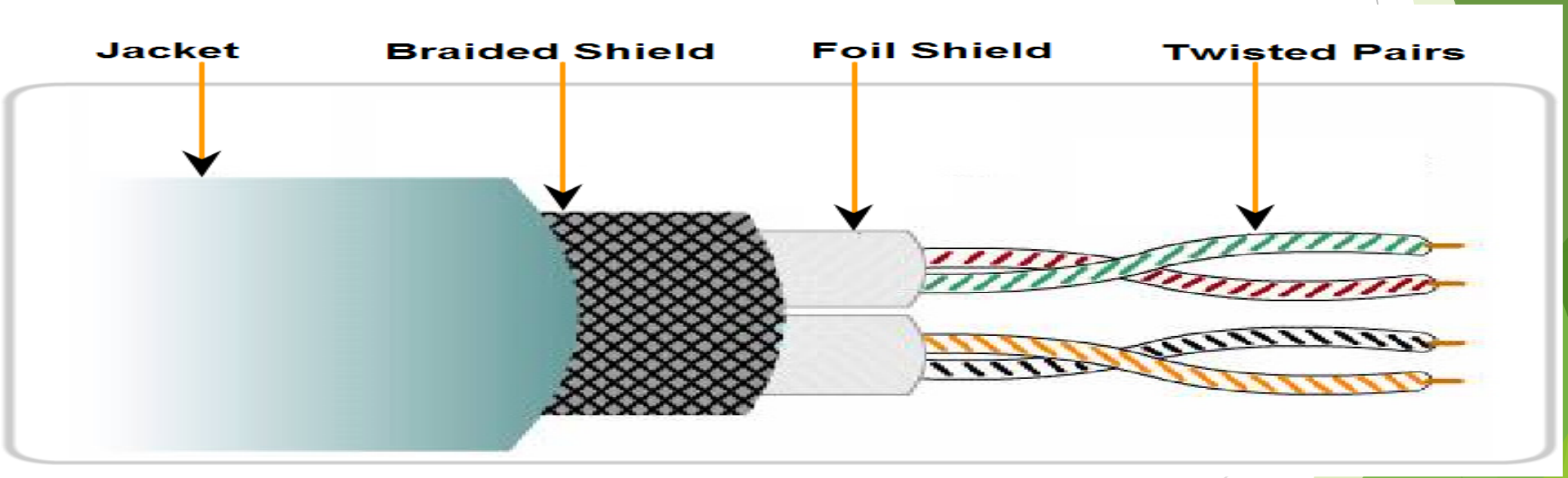
- It can be run longer distances than Twisted pair Cables.

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



b. Shielded Twisted Pair(STP)

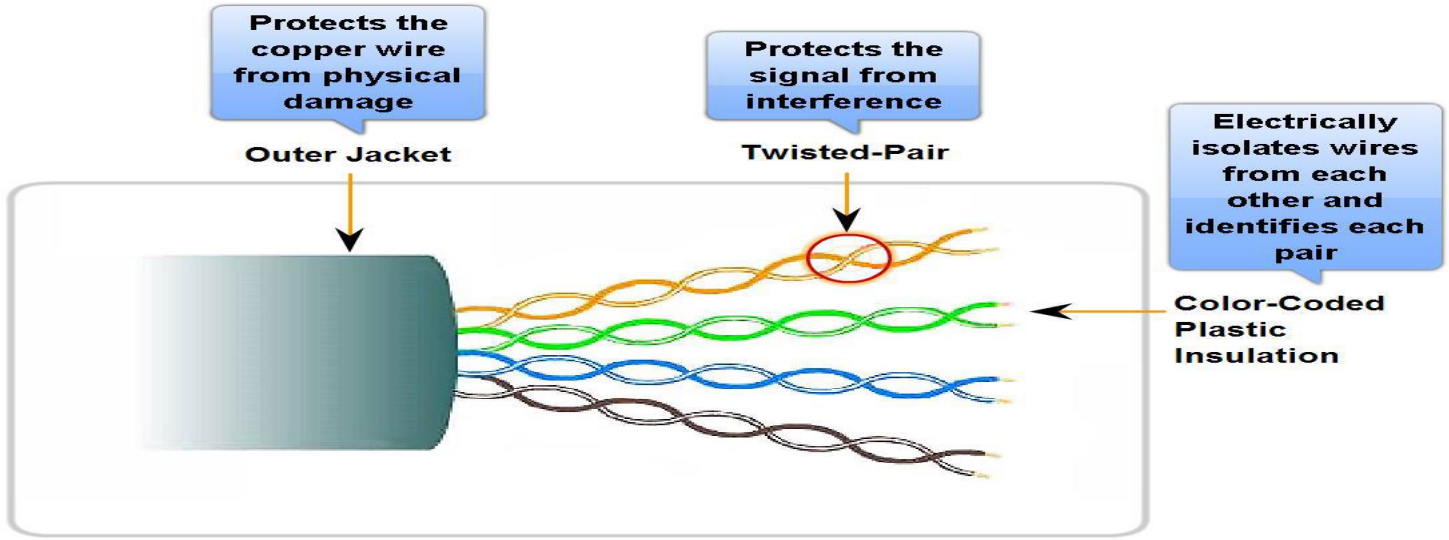
- Speed: 0-100Mbps
- Cost: Moderate
- Media and connector size: Medium to large
- Maximum cable length: 100m



c. Unshielded Twisted Pair

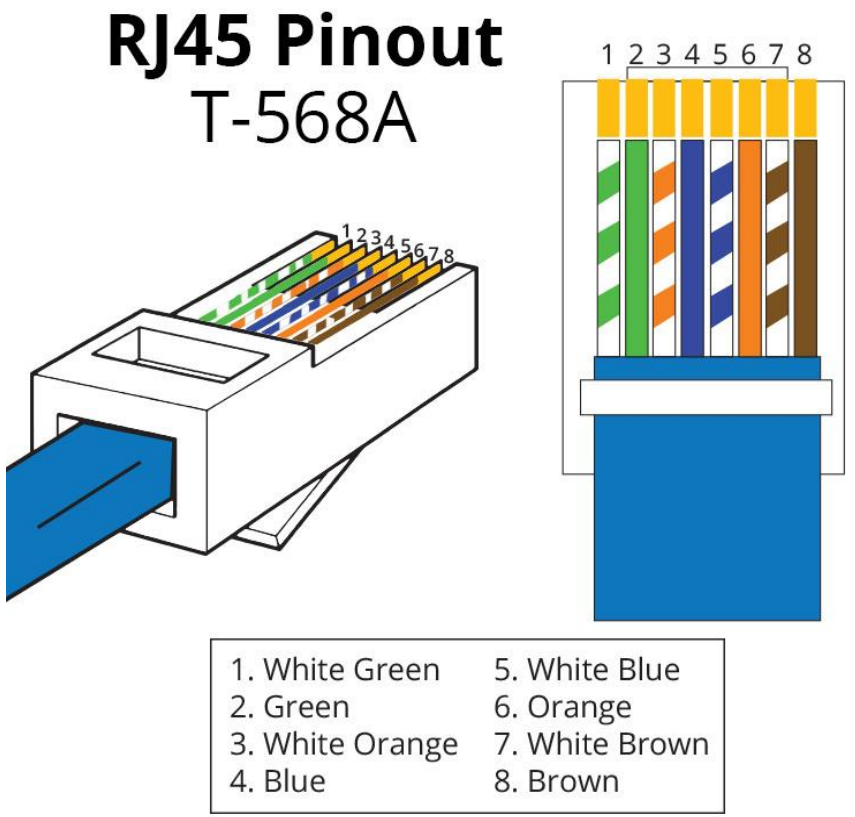
- UTP is a four-pair wire medium used in a variety of networks.
- Each of the eight copper wires in the UTP cable is covered by insulating material

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



UTP Implementation

- EIA/TIA specifies an RJ-45 connector for UTP cable.
- The letters RJ stand for registered jack.



Fiber Optic Cable

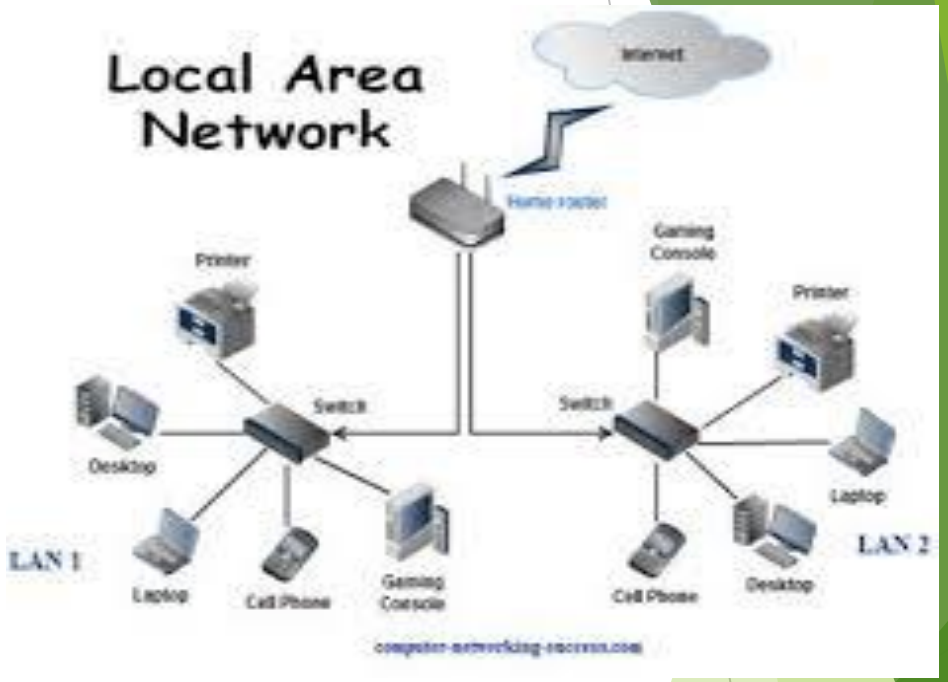
- Glass fiber carrying light pulses, each pulse a bit.
- Based on the Total Internal Reflection of Light.
- High-speed point-to-point transmission 10-100’s Gbps
- low error rate:
  - repeaters spaced far apart
  - immune to electromagnetic noise

Types of Networks

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide Area Network (WAN)
4. Peer to Peer Network (P2P)

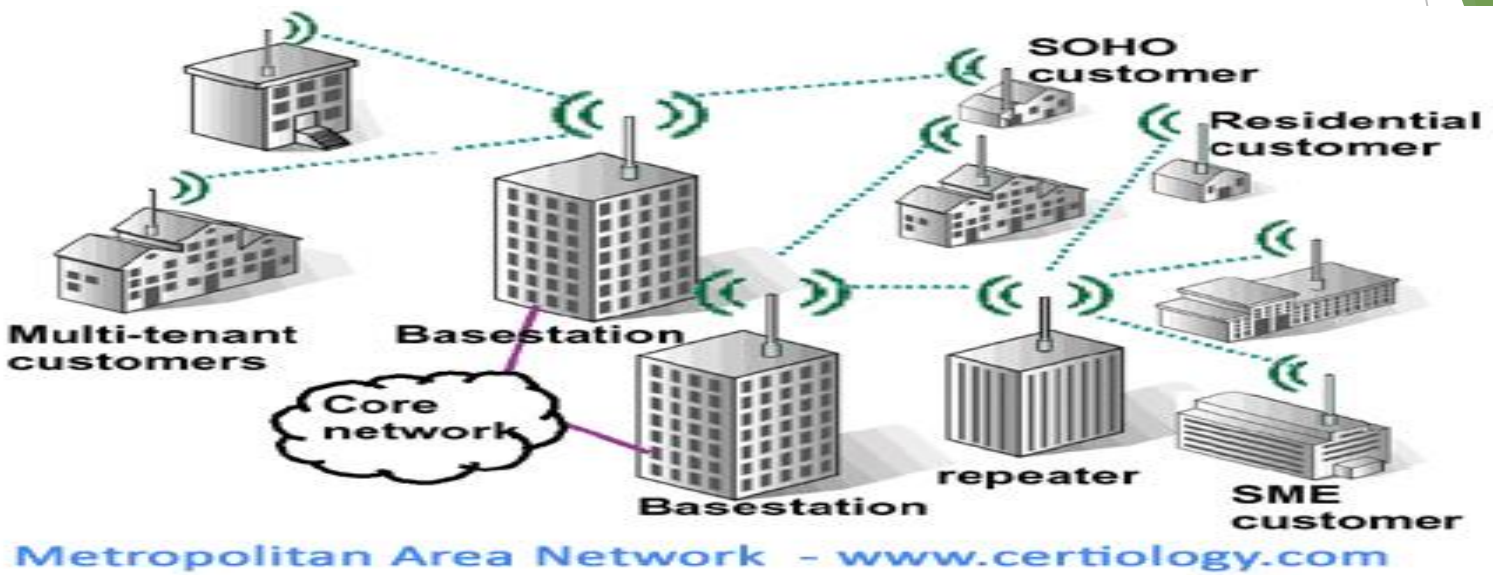
1. Local Area Network

- Xerox Corporation worked in collaboration with DEC and Intel to create Ethernet, which is the most pervasive LAN architecture used today.
- Ethernet has evolved and has seen significant improvements in regard to speed and efficiency.



- An upside of a LAN is fast data transfer with data speed that can reach up to 10Gbps.
- Other significant LAN technologies are Fibre Distributed Data Interface (FDDI) and token ring.

2. Metropolitan Area Network



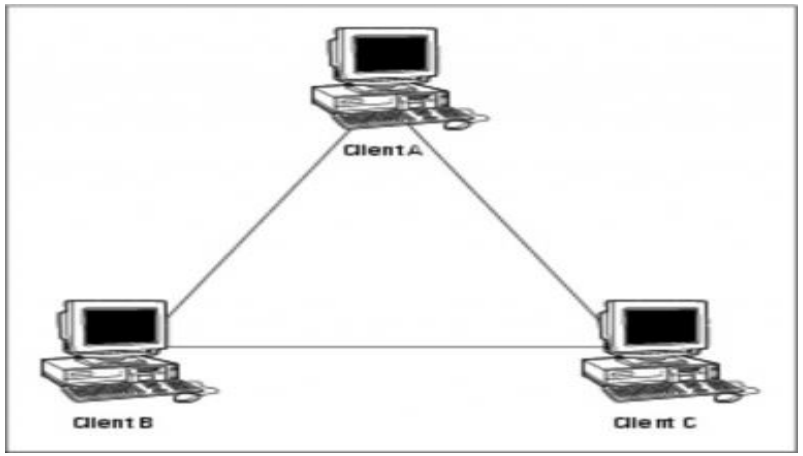
1. A MAN is larger than a LAN but smaller than or equal in size to a WAN.
2. The size range anywhere from 5 to 50km in diameter.
3. MANs are typically owned and managed by a single entity.
4. This could be an ISP or telecommunications company that sells its services to end-users in that metropolitan area.
5. For all intents and purposes, a MAN has the same characteristics as a WAN with distance constraints.

3. Wide Area Network

- A Wide Area Network exist over a large area
- Data travels through telephone or cable lines
- Usually requires a Modem
- The world’s largest Wide Area Network in the Internet

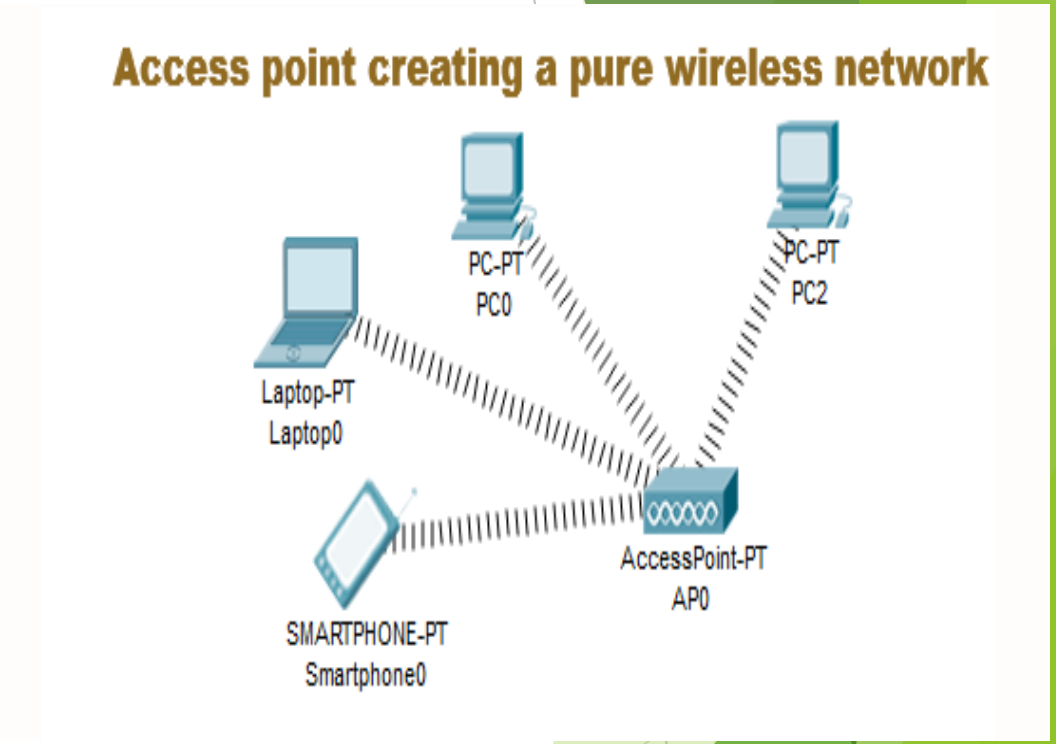
4.Peer to Peer Network

- Usually very small networks
- Each workstation has equivalent capabilities and responsibilities
- Does not require a switch or a hub.
- These types of networks do not perform well under heavy data loads.



5.3 Wireless AP (access point) Configuration

- An access point is the device that allows multiple wireless devices to connect with each other.
- Just like a HUB or switch connects multiple devices together in a single or multiple wired LAN networks, an access point connects multiple wireless devices together in a single wireless or multiple wireless networks.
- An access point can also be used to extend the wired network to the wireless devices.

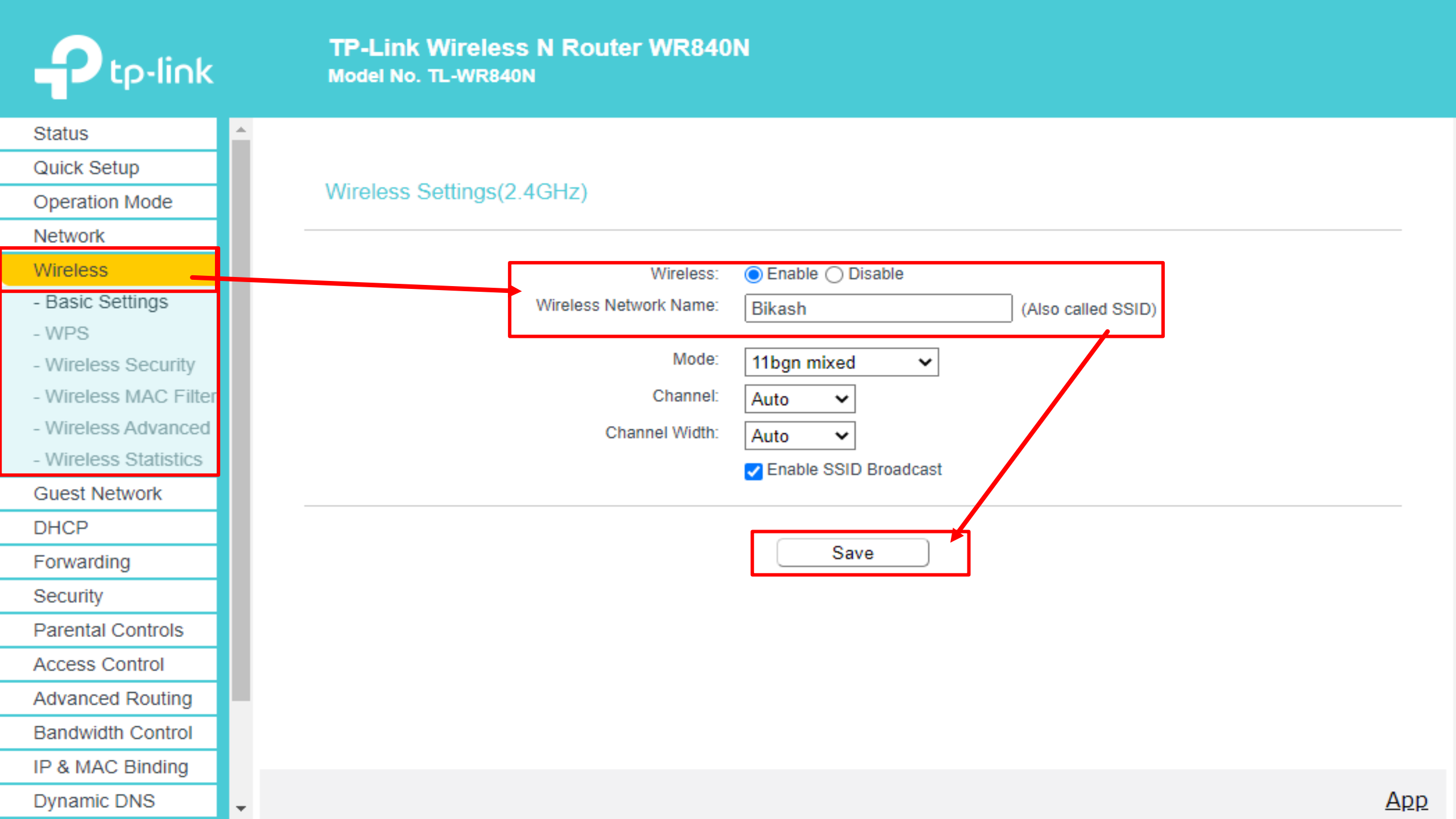


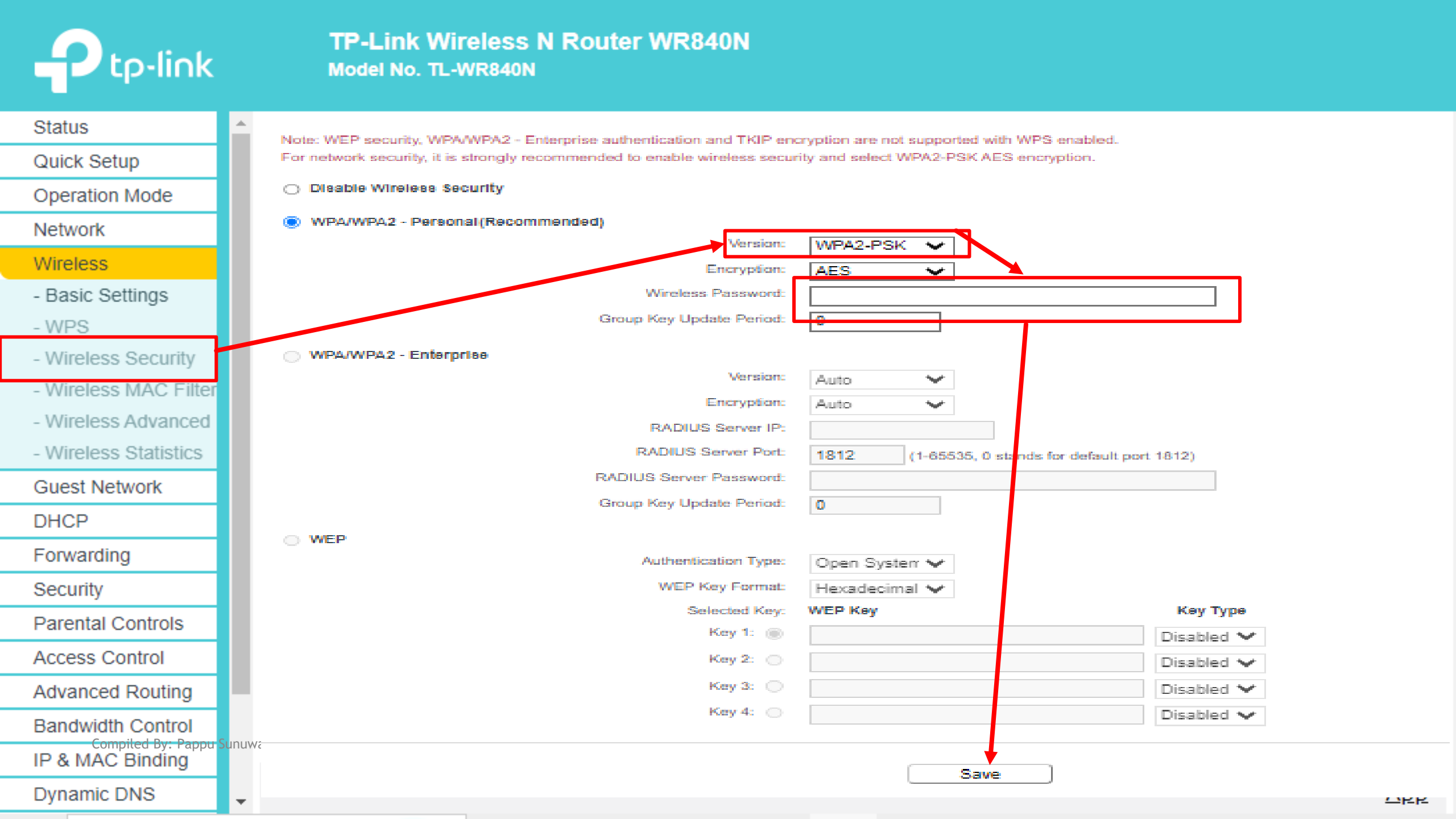
Configuration of AP

- Switch on the AP.
- Go to the Access IP in browser (IP may differ from company)

  Eg .192.168.0.1 (tp-link router)
- Click on ‘Network’ and select ‘WAN’.
- Change the Connection type to ‘Dynamic IP’ (or you may choose ‘Static Ip’ unless you know static ip address.)
- Select ‘Wireless’ and change the SSID name and Save it.
- Go to Wireless security in Wireless tab and select version (WPA2-PSK)
- Then choose suitable password and click on Save.


tp-link
TP-Link Wireless N Router WR840N
Model No. TL-WR840N
Status
Quick Setup
Operation Mode
Network
Wireless
Guest Network
DHCP
Forwarding
Security
Parental Controls
Access Control
Advanced Routing
Bandwidth Control
IP & MAC Binding
Dynamic DNS
IPv6
System Tools
Logout
Status
Network
- WAN
- LAN
- IPTV
- MAC Clone
LAN
Connection Type:
Dynamic IP
Detect
IP Address:
192.168.1.132
Subnet Mask:
255.255.255.0
Gateway:
192.168.1.1
Renew
Release
Advance
Save
Wireless 2.4GHz
Operation Mode:
Router
Wireless Radio:
Enabled
Name(SSID):
Bikash
Mode:
11bgn mixed


TP-Link Wireless N Router WR840N
Model No. TL-WR840N
Status
Quick Setup
Operation Mode
Network
Wireless
- Basic Settings
- WPS
- Wireless Security
- Wireless MAC Filter
- Wireless Advanced
- Wireless Statistics
Guest Network
DHCP
Forwarding
Security
Parental Controls
Access Control
Advanced Routing
Bandwidth Control
IP & MAC Binding
Dynamic DNS
Wireless Settings(2.4GHz)
Wireless: Enable Disable
Wireless Network Name: Bikash (Also called SSID)
Mode: 11bgn mixed
Channel: Auto
Channel Width: Auto
Enable SSID Broadcast
Save
App


TP-Link Wireless N Router WR840N
Model No. TL-WR840N
Status
Quick Setup
Operation Mode
Network
Wireless
- Basic Settings
- WPS
- Wireless Security
- Wireless MAC Filter
- Wireless Advanced
- Wireless Statistics
Guest Network
DHCP
Forwarding
Security
Parental Controls
Access Control
Advanced Routing
Bandwidth Control
IP & MAC Binding
Dynamic DNS
Note: WEP security, WPA/WPA2 - Enterprise authentication and TKIP encryption are not supported with WPS enabled.
For network security, it is strongly recommended to enable wireless security and select WPA2-PSK AES encryption.
Disable Wireless Security
WPA/WPA2 - Personal(Recommended)
Version: WPA2-PSK
Encryption: AES
Wireless Password:
Group Key Update Period: 0
WPA/WPA2 - Enterprise
Version: Auto
Encryption: Auto
RADIUS Server IP:
RADIUS Server Port: 1812 (1-65535, 0 stands for default port 1812)
RADIUS Server Password:
Group Key Update Period: 0
WEP
Authentication Type: Open System
WEP Key Format: Hexadecimal
Selected Key: WEP Key Key Type
Key 1: Disabled
Key 2: Disabled
Key 3: Disabled
Key 4: Disabled
Save
Compiled By: Pappu Sunuwa

Thank You