SUPRA

Network Security

2024


Cell Phones
Telephone System
Telephone Service Provider
Corporate Web Site Intranet and Extranet
Servers
Internet Service Provider
Internet
Wireless Internet Service Provider
Corporate Wired LAN
Wireless LAN
Mobile Wi-Fi Network

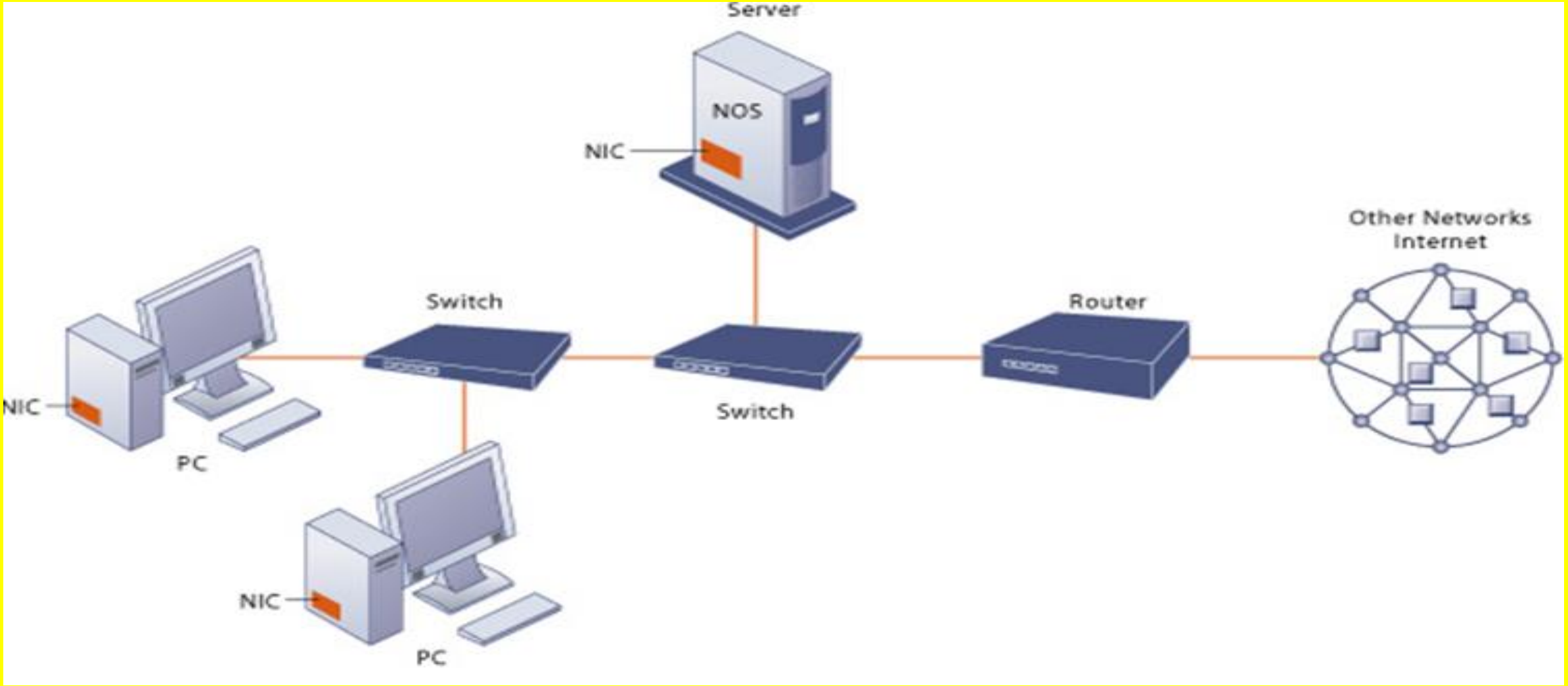
Networking & IT Infrastructure?

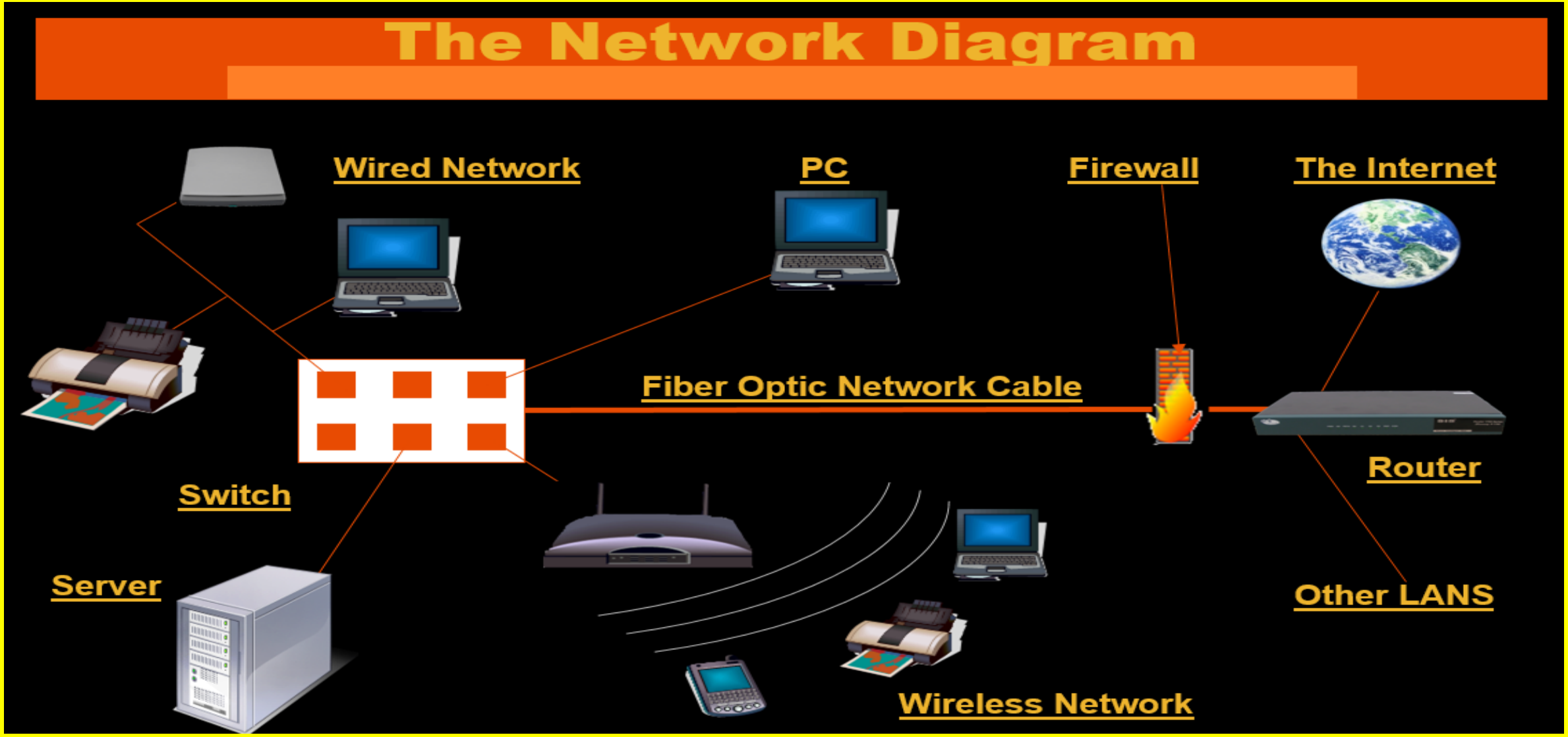
- IT infrastructure refers to the components used to operate and manage enterprise IT environments.
- These components can deploy in a cloud computing system or within the organization's facilities.
- Components include hardware, software, networking, operating system, and data storage. They deliver IT services and solutions.
- IT infrastructure products can be downloadable software or online solutions like IaaS.


What are the COMPONENTS of IT INFRASTRUCTURE
?
Hardware
Software
Networking

Networking

- It involves interconnected components facilitating network operations and communication between internal and external systems.
- This includes internet connectivity, network enablement, firewalls, security measures, routers, switches, and cables.
- computer network may include personal computers, servers, networking hardware, or other specialized or general-purpose hosts.
- A communication protocol (a set of rules) decides the exchange of information over a network.


Server
NOS
NIC
Other Networks
Internet
Switch
Router
Switch
NIC
PC
NIC
PC


The Network Diagram
Wired Network
PC
Firewall
The Internet
Fiber Optic Network Cable
Router
Switch
Server
Other LANS
Wireless Network

The Advantages/Uses of Network

Simultaneous Access

- There are moments in any business when several workers may need to use the same data at the same time.

Shared Peripheral Devices

Personal Communications

- Videoconferencing

- Voice over Internet Protocol (VoIP):-VoIP transmits the sound of voice over a computer network using the Internet Protocol (IP) rather than sending the signal over traditional phone wires

Easier Data Backup

The Networking Devices(Nodes)

- NIC Card
- Repeater
- Hub
- Switch
- Bridge
- Router
- Gateway
- Firewall

Network Interface Card

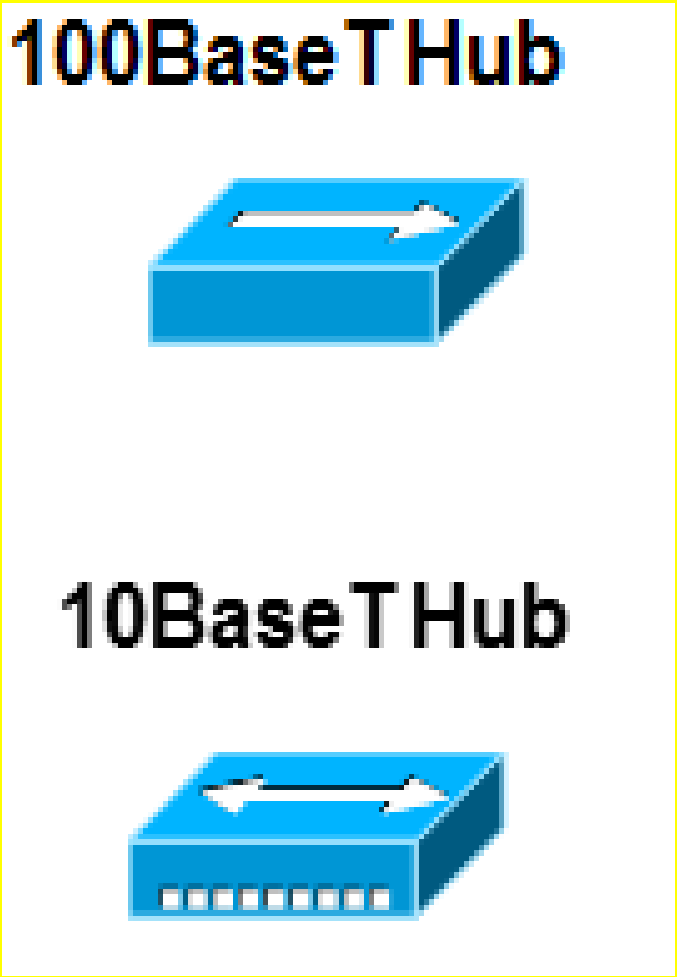
- NIC is used to physically connect host devices to the network media.
- A NIC is a printed circuit board that fits into the expansion slot of a bus on a computer motherboard.
- It can also be a peripheral device. NICs are sometimes called network adapters.
- Each NIC is identified by a unique code called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

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.
- A repeater does not make an intelligent decision concerning forwarding packets

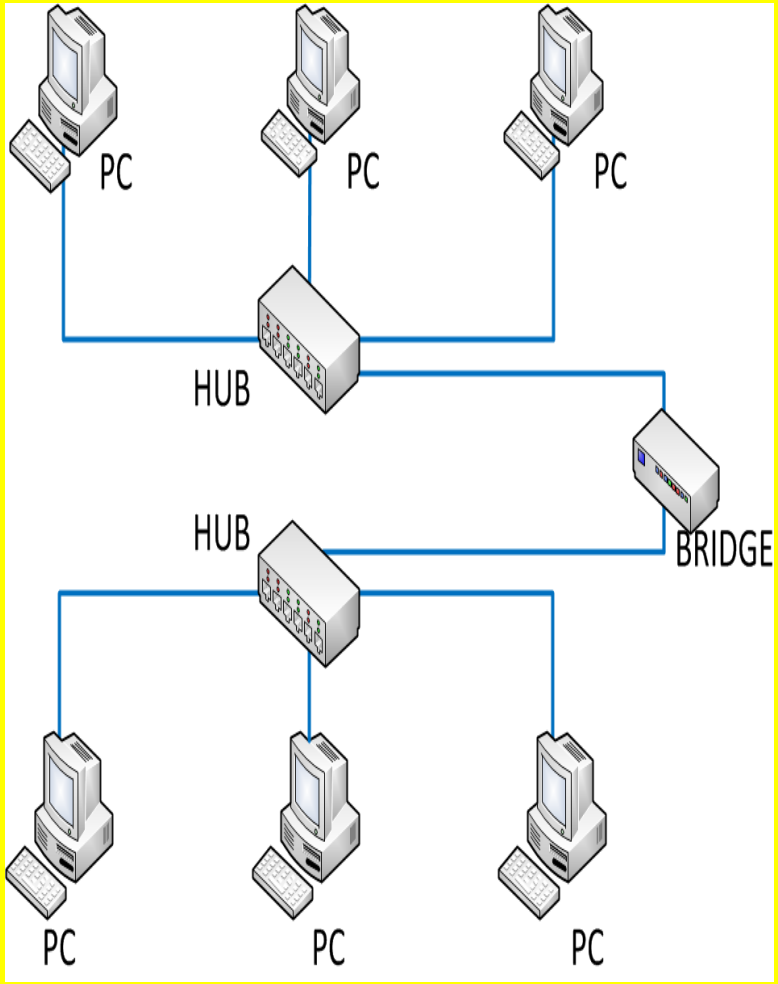
Hubs

- 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.



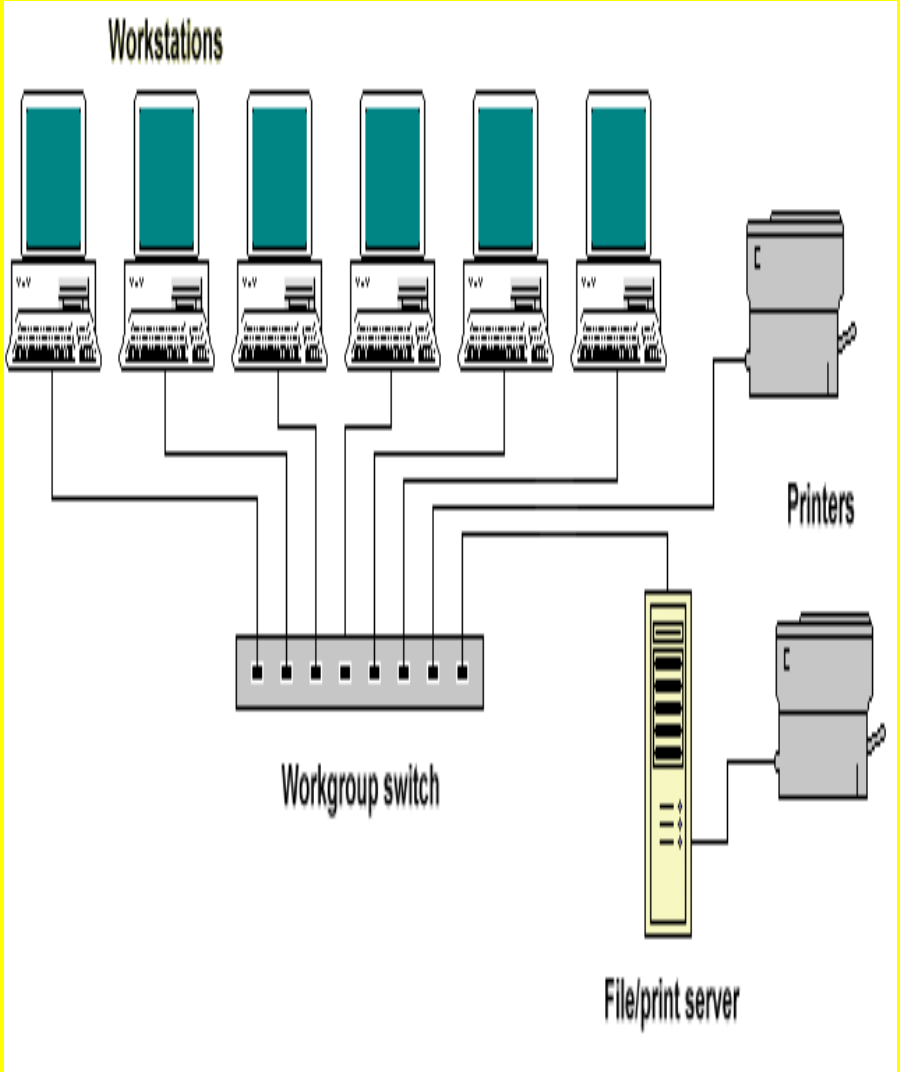
Bridges

- Bridges convert network data formats and perform basic data transmission management.
- Bridges provide connections between LANs.
- They also check data to determine if it should cross the bridge. This makes each part of the network more efficient



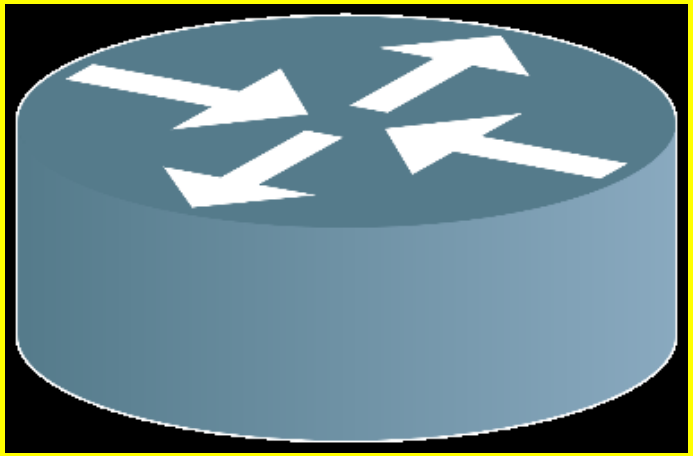
Switches

- 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



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.



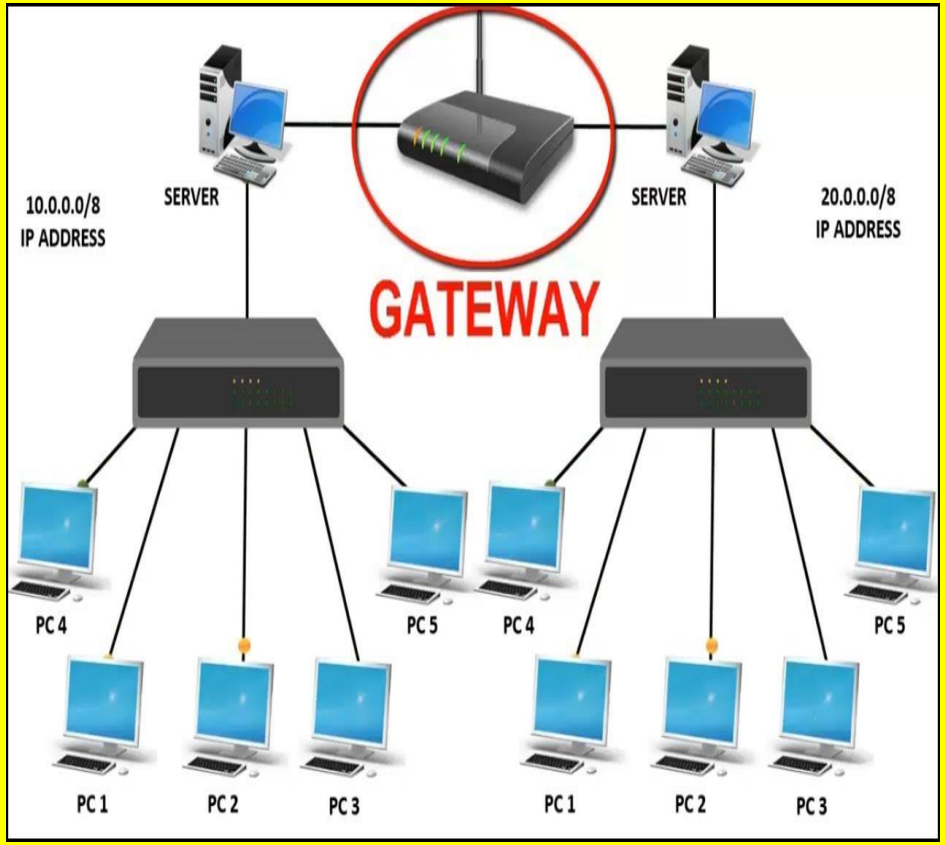
Gateway

- A gateway is a piece of networking hardware used in telecommunications for telecommunications networks that allows data to flow from one discrete network to another.

- Gateways are distinct from routers or switches

in that they communicate using more than one protocol

to connect a bunch of networks



Network Media

The function of the media 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 area network (LAN) technology are collectively known as Ethernet

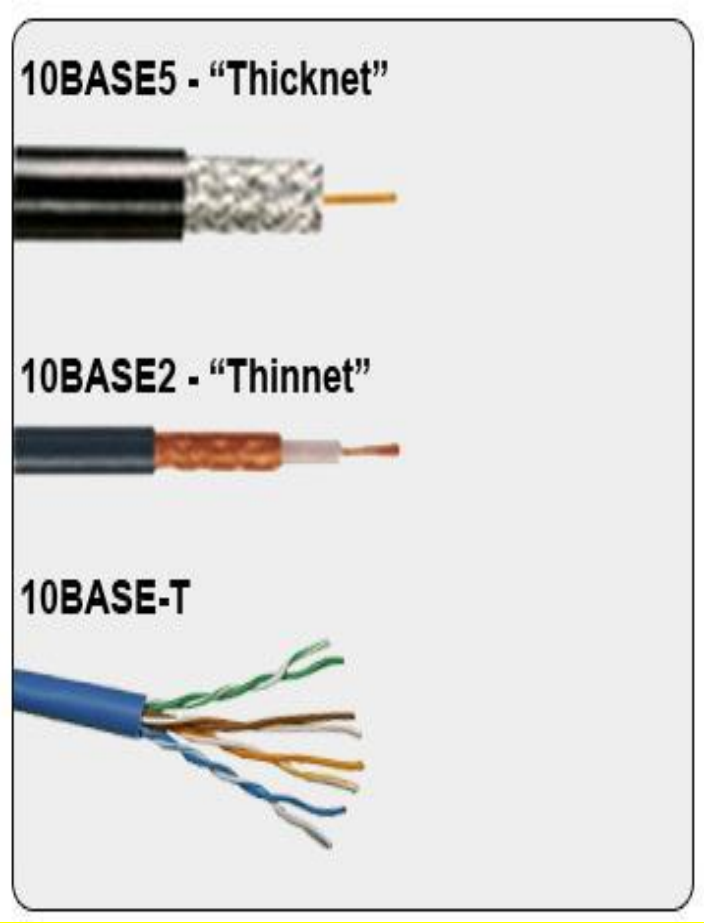
   1. Copper Cable
      a. Coaxial Cables
      b. Shielded Twisted Pair(STP)
      c. Unshielded Twisted Pair

   2. Fibre Optic Cable

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

Copper Cable

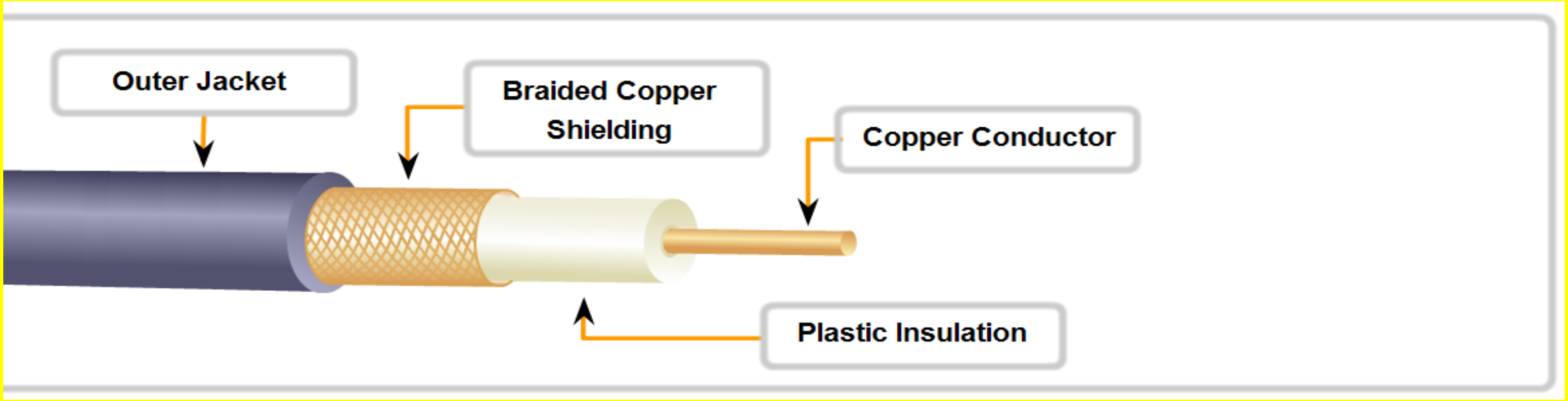
- The most common, easiest, quickest, and cheapest form of network media to install.
- The disadvantage of sending data over copper wire is that the further the signal travels, the weaker it becomes.



Coaxial Cable

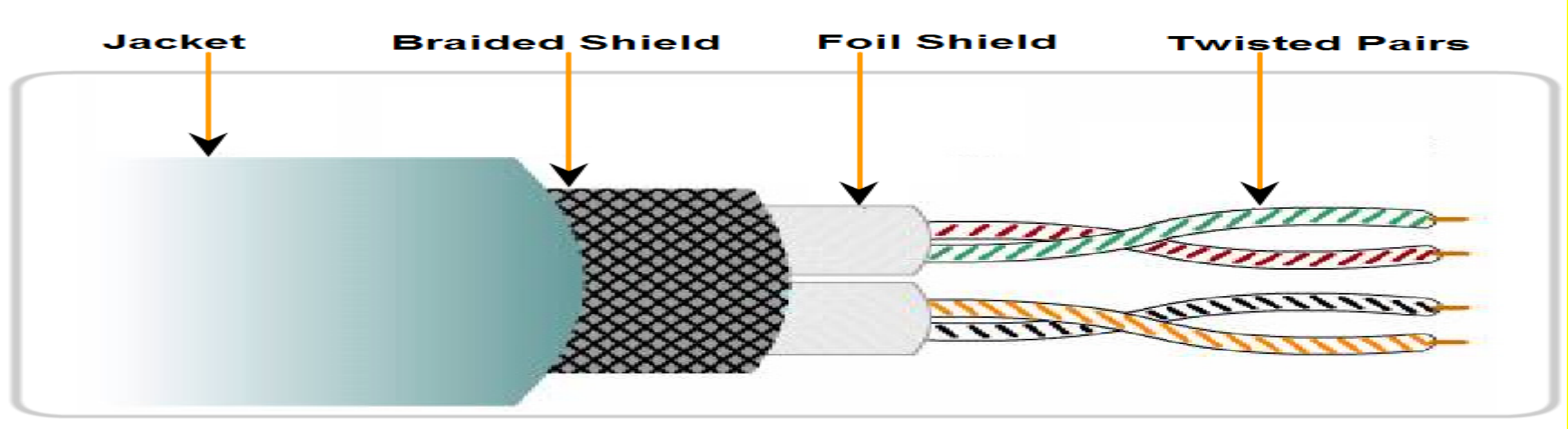
- It can be run longer distances than Twisted pair Cables.

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



Shielded Twisted Pair(STP)

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



Unshielded Twisted Pair

➢UTP is a four-pair wire medium used in a variety of networks.

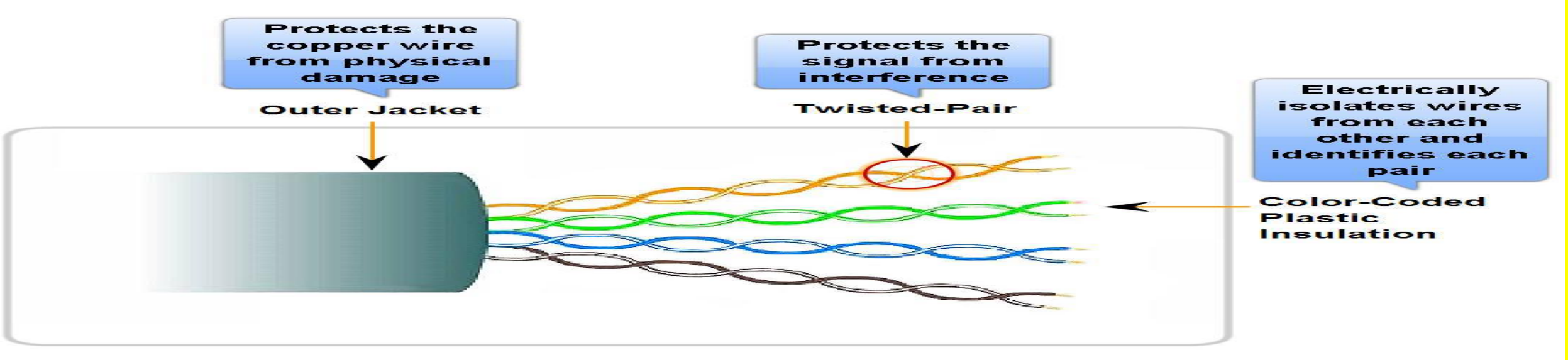
➢ Each of the eight copper wires in the UTP cable is covered by insulating material

Speed: 10-100-1000 Mbps*

Cost: Least Expensive

Media and connector size: Small

Maximum cable length: 100m * (Depending on the quality/category of cable)

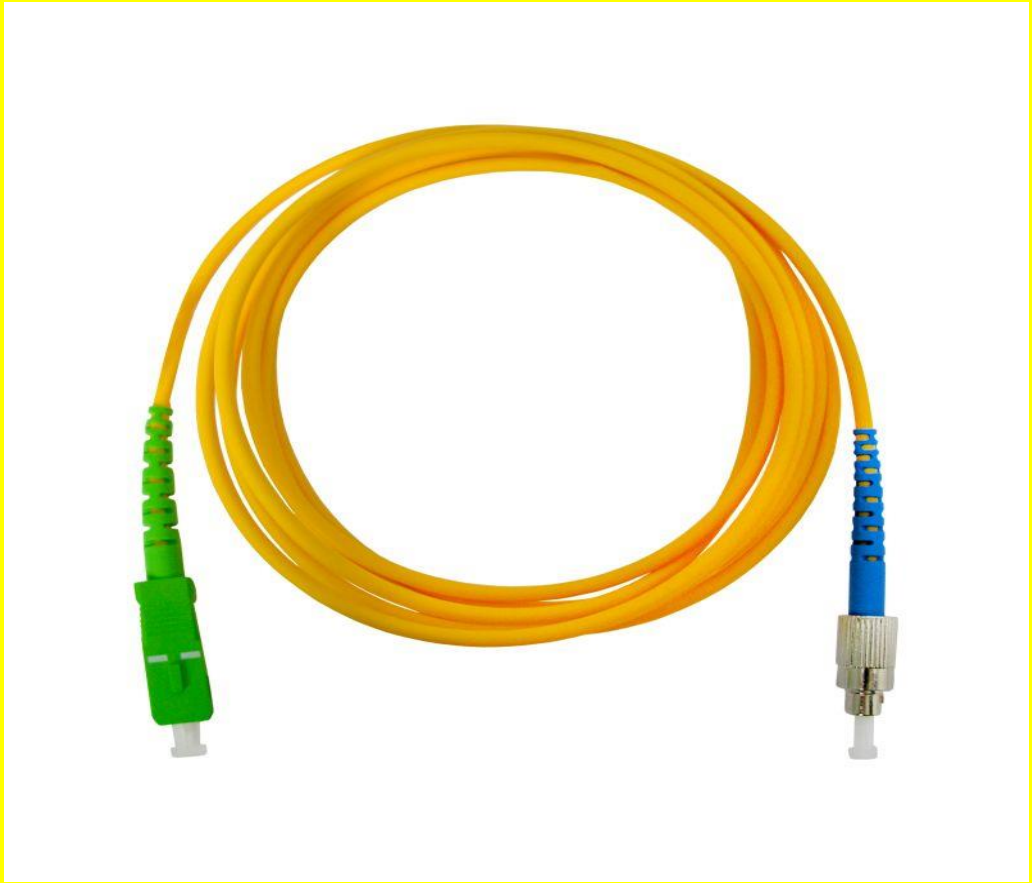


UTP Implementation

- 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



Network Defenses

Firewall — One of the first lines of defense in a network, a firewall isolates one network from another.

Firewalls either can be standalone systems or included in other devices, such as routers or servers. You can find both hardware and software firewall solutions; some firewalls are available as appliances that serve as the primary device separating two networks.

Intrusion detection system (IDS) — An IDS enhances cybersecurity by spotting a hacker or malicious software on a network so you can remove it promptly to prevent a breach or other problems, and use the data logged about the event to better defend against similar intrusion incidents in the future.

Investing in an IDS that enables you respond to attacks quickly can be far less costly than rectifying the damage from an attack and dealing with the subsequent legal issues.

Intrusion prevention system (IPS) — An IPS is a network security solution that can not only detect intruders, but also prevent them from successfully launching any known attack. Intrusion prevention systems combine the abilities of firewalls and intrusion detection systems. However, implementing an IPS on an effective scale can be costly, so businesses should carefully assess their IT risks before making the investment. Moreover, some intrusion prevention systems are not as fast and robust as some firewalls and intrusion detection systems, so it might not be an appropriate solution when speed is an absolute requirement.

Network access control (NAC) involves restricting the availability of network resources to endpoint devices that comply with your security policy. Some NAC solutions can automatically fix non-compliant nodes to ensure it is secure before access is allowed. NAC is most useful when the user environment is fairly static and can be rigidly controlled, such as enterprises and government agencies. It can be less practical in settings with a diverse set of users and devices that are frequently changing, which are common in the education and healthcare sectors.

Web filters are solutions that by preventing users' browsers from loading certain pages from particular websites. There are different web filters designed for individual, family, institutional and enterprise use.

Proxy servers act as negotiators for requests from client software seeking resources from other servers. A client connects to the proxy server, requesting some service (for example, a website); the proxy server evaluates the request and then allows or denies it. In organizations, proxy servers are usually used for traffic filtering and performance improvement.

Anti-DDoS devices detect distributed denial of service (DDoS) attacks in their early stages, absorb the volume of traffic and identify the source of the attack.

Load balancers are physical units that direct computers to individual servers in a network based on factors such as server processor utilization, number of connections to a server or overall server performance. Organizations use load balancers to minimize the chance that any particular server will be overwhelmed and to optimize the bandwidth available to each computer in the network.

Spam filters detect unwanted email and prevent it from getting to a user's mailbox. Spam filters judge emails based on policies or patterns designed by an organization or vendor. More sophisticated filters use a heuristic approach that attempts to identify spam through suspicious word patterns or word frequency.

Understand the OSI Model

The International Standards Organization (ISO) developed the Open Systems Interconnect (OSI) model in 1981. It consists of seven functional layers that provide the basis for communication among computers over networks, as described in the table below.

You can easily remember them using the mnemonic phrase “All people seem to need data processing.”

Understanding this model will help you build a strong network, troubleshoot problems, develop effective applications and evaluate third-party products.

SUPRA

Layer	Function	Protocols or Standards
Layer 7: Application	Provides services such as e-mail, file transfers and file servers	HTTP, FTP, TFTP, DNS, SMTP, SFTP, SNMP, RLogin, BootP, MIME
Layer 6: Presentation	Provides encryption, code conversion and data formatting	MPEG, JPEG, TIFF
Layer 5: Session	Negotiates and establishes a connection with another computer	SQL, X- Window, ASP, DNA, SCP, NFS, RPC
Layer 4: Transport	Supports end-to-end delivery of data	TCP, UDP, SPX
Layer 3: Network	Performs packet routing	IP, OSPF, ICMP, RIP, ARP, RARP
Layer 2: Data link	Provides error checking and transfer of message frames	Ethernet, Token Ring, 802.11
Layer 1: Physical	Physically interfaces with transmission medium and sends data over the network	EIA RS-232, EIA RS-449, IEEE, 802

Segregate Your Network

Network segmentation involves segregating the network into logical or functional units called zones.

For example, you might have a zone for sales, a zone for technical support and another zone for research, each of which has different technical needs. You can separate them using routers or switches or using virtual local area networks (VLANs), which you create by configuring a set of ports on a switch to behave like a separate network.

Segmentation limits the potential damage of a compromise to whatever is in that one zone. Essentially, it divides one target into many, leaving attackers with two choices: Treat each segment as a separate network, or compromise one and attempt to jump the divide. Neither choice is appealing.

Treating each segment as a separate network creates a great deal of additional work, since the attacker must compromise each segment individually; this approach also dramatically increases the attacker's exposure to being discovered.

Attempting to jump from a compromised zone to other zones is difficult. If the segments are designed well, then the network traffic between them can be restricted. There are always exceptions that must be allowed through, such as communication with domain servers for centralized account management, but this limited traffic is easier to characterize.

Segmentation is also useful in data classification and data protection. Each segment can be assigned different data classification rules and then set to an appropriate level of security and monitored accordingly.

An extreme example of segmentation is the air gap — one or more systems are literally not connected to a network. Obviously, this can reduce the usefulness of many systems, so it is not the right solution for every situation.

In some cases, however, a system can be sensitive enough that it needs to not be connected to a network; for example, having an air-gapped backup server is often a good idea. This approach is one certain way of preventing malware infections on a system.

Virtualization is another way to segment a network. Keep in mind that it is much easier to segment virtual systems than it is to segment physical systems. As one simple example, consider a virtual machine on your workstation. You can easily configure it so that the virtual machine is completely isolated from the workstation — it does not share a clipboard, common folders or drives, and literally operates as an isolated system.

Types of Network Segments

Network segments can be classified into the following categories:

Public networks allow accessibility to everyone. The internet is a perfect example of a public network. There is a huge amount of trivial and unsecured data on public networks. Security controls on these networks are weak.

Semi-private networks sit between public networks and private networks. From a security standpoint, a semi-private network may carry confidential information but under some regulations.

Private networks are organizational networks that handle confidential and propriety data. Each organization can own one or more private networks. If the organization is spread over vast geographical distances, the private networks at each location may be interconnected through the internet or other public networks.

Demilitarized zone (DMZ) is a noncritical yet secure region at the periphery of a private network, separated from the public network by a firewall; it might also be separated from the private network by a second firewall. Organizations often use a DMZ as an area where they can place a public server for access by people they might not trust. By isolating a server in a DMZ, you can hide or remove access to other areas of your network. You can still access the server using your network, but others aren't able to access further network resources.

Software-defined networking (SDN) is a relatively recent trend that can be useful both in placing security devices and in segmenting the network. Essentially, in an SDN, the entire network is virtualized, which enables relatively easy segmentation of the network. It also allows administrators to place virtualized security devices wherever they want.

What are the limitations of IPv4?

Common IPv4 flaws:

1. The lack of address space - the number of different devices connected to the Internet grows exponentially, and the size of the address space is quickly depleted;

2. Weak protocol extensibility - the insufficient size of the IPv4 header, which does not accommodate the required number of additional parameters;

3. The problem of security of communications - no means are provided to limit access to information hosted on the network. IPv4 has never been designed for security.

Originally designed as an isolated military network

Then adapted for public education and research network

4. Lack of quality of service support - placement of information about bandwidth, delays required for smooth operation of some network applications are not supported;

5. Geographic limitations - since the Internet was created in the USA, this country is also involved in the distribution of IP addresses. Almost 50% of all addresses are reserved for the United States.

It is impossible to stop the IPv4 depletion and transition to IPv6 is inevitable. Moreover, the growing demand for addresses leads to the appearance of a black market. After the distribution of almost all free addresses, the only way to get addresses will be on the black market and prices will rise significantly. If the survival of your business depends on getting IPv4 addresses, you will be ready to pay for them, even if you must bypass the rules. Fortunately, Carrier Grade Network Address Translation (CGN or CGNAT), also known as Large Scale NAT (LSN) was developed to deal with the IPv4 exhaustion problem and to prevent the appearance of the IP black market.

Use Network Address Translation

Network address translation (NAT) enables organizations to compensate for the address deficiency of IPv4 networking. NAT translates private addresses (internal to a particular organization) into routable addresses on public networks such as the internet. In particular, NAT is a method of connecting multiple computers to the internet (or any other IP network) using one IP address.

NAT complements firewalls to provide an extra measure of security for an organization's internal network. Usually, hosts from inside the protected networks, which have private addresses, are able to communicate with the outside world, but systems that are located outside the protected network have to go through the NAT boxes to reach internal networks. Moreover, NAT enables an organization to use fewer IP addresses, which helps confusing attackers about which particular host they are targeting.

SUPRA

Thank you!!!

PrasannaGuntur@supratech.xyz

Ph: +91 99028 49444