**Lab Assignment - 2**

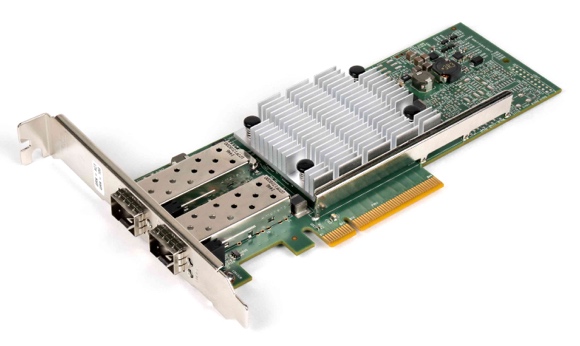
**Name:** Khushi Prasad

**Subgroup:** 2CO20

**Roll No. :** 102183044

Q1. Network Interface Cards - their use, types and working.

Ans. Network Interface Card (NIC) is a hardware unit, which is inbuilt inside a computer provided with a slot, it connects the computer to a[computer network](https://www.elprocus.com/important-of-network-in-embedded-systems-for-beginners/) for communication with other devices via buses. There are many synonyms for network interface card like, network adapter, [local area network](https://www.elprocus.com/what-is-ethernet-and-different-types-of-ethernet-networks/) (LAN) card or physical network interface card, [ethernet](https://www.elprocus.com/what-is-ethernet-and-different-types-of-ethernet-networks/) controller or ethernet adapter, network controller, and connection card.



**Use –**

1. It acts like a translator, which converts data into a digital signal.
2. Communication can be either by using cable wire or by the router which is wireless over the server network
3. To communicate over a long distance a network adapter is used.

### **Types of Network Interface Cards -**

There are the following two types of NICs -

**1. Ethernet NIC**

Ethernet NIC card is a slot for a cable where we have to plug one end of the ethernet cable into the slots of the computer and another end of the cable is plugged into the modem, likewise, various devices are connected to make a communication set up between them.

It is made by ethernet cables. This type of NIC is most widely used in the LAN, MAN, and WAN networks.

Example: TP-LINK TG-3468 Gigabit PCI Express Network Adapter.

2. **Wireless Networks NIC**

Wireless network NIC cards consist of a small [antenna](https://www.elprocus.com/different-types-of-antennas-with-properties-and-thier-working/) integrated onto the card, where the communication between various devices is set up wirelessly using the router and various network protocols. It is a wireless network that allows us to connect the devices without using the cables. These types of NICs are used to design a Wi-Fi connection.

Example: Intel 3160 Dual-Band Wireless Adapter

Q2. Hub Device and its’ working.

Ans. A hub is a common connection point, also known as a network hub, which is used for connection of devices in a network. It works as a central connection for all the devices that are connected through a hub. The hub has numerous ports.

Hub works like an electric wire, it receives data signals from one device in its one port

and forwards them to all the other ports, except the source port. It does not have any

capability to identify any frames to know where it should forward because it does not

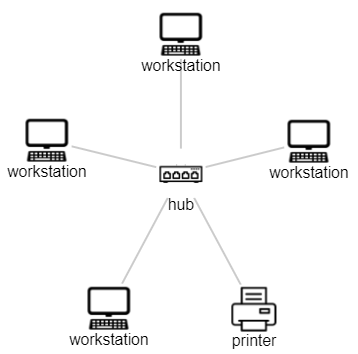
maintain any kind of table like switch. So there is a lot of traffic on the network and

network performance is also very poor, only one device transmits information at a

particular time.

It works on star topology physically because all the devices are connected to the central

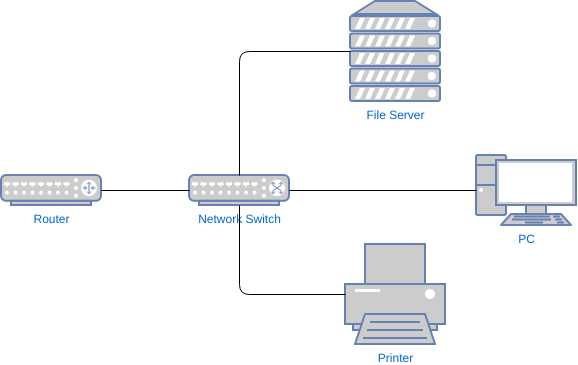
node, but logically it acts as a bus topology.



Q3. Switch Device and its’ working.

Ans. [Switches](https://www.cisco.com/c/en/us/solutions/small-business/networking/switches.html) are key building blocks for any network. They connect multiple devices, such as computers, [wireless access points](https://www.cisco.com/c/en/us/solutions/small-business/networking/wireless.html), printers, and servers; on the same network within a building or campus. A switch enables connected devices to share information and talk to each other.

When a device sends a packet to another device, it enters the switch and the switch reads its header to determine what to do with it. It matches the destination address or addresses and sends the packet out through the appropriate ports that leads to the destination devices.

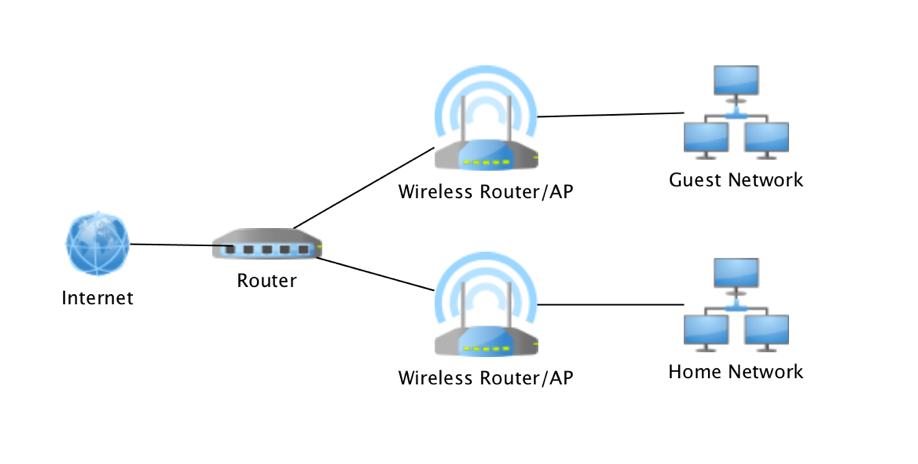


Q4. Router Device and its’ working.

Ans. The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets.

[Routers](https://www.cisco.com/c/en_in/solutions/small-business/networking/routers.html) connect computers and other devices to the Internet. A router acts as a dispatcher, choosing the best route for your information to travel.

Routers connect a modem—like a fiber, cable, or DSL modem—to other devices to allow communication between those devices and the internet. Most routers, including wireless routers, usually feature several network ports to connect numerous devices to the internet simultaneously.

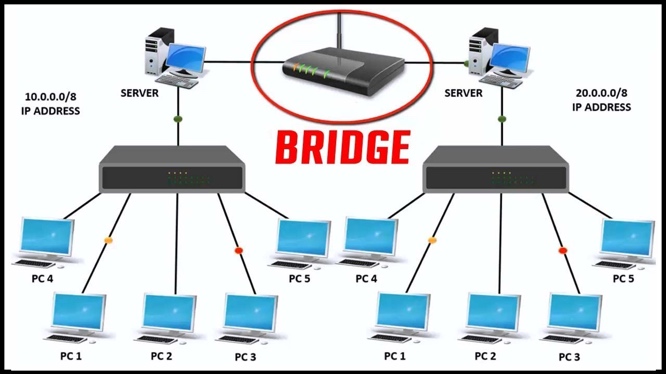


Q5. Bridge device and its’ working.

Ans. A bridge in a computer network is one kind of network device, used to separate a network into sections. Every section in the network represents a collision domain that has separate bandwidth. So that network performance can be improved using a bridge.

In simple words, a bridge in computer networks is defined as, the network device that provides a connection between two local area networks (LANs) or two segments of the same local area network.

The working of the bridge in a[computer](https://www.watelectronics.com/what-is-a-computer-port-types-its-working/) network is similar to the repeater and hub to broadcast the data to every node. The MAC (Media Access Control) address or physical address of the data packet or frame on the segment of the network is utilized by the bridge to perform subsequent transmissions between the source and destination. With the help of MAC address on the particular segment network, the data traffic can be prevented.

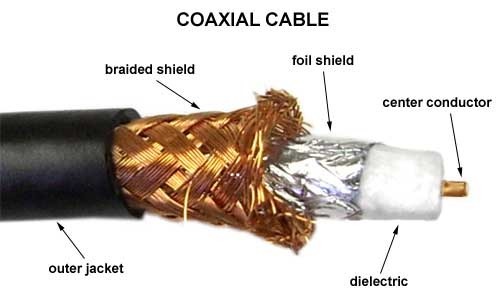


Q6. Types of networking wires and connectors, shapes and specifications.

Ans. To connect two or more computers or networking devices in a network, network cables are used. There are three types of network cables; coaxial, twisted-pair, and fiber-optic.

1. Coaxial cable

This cable contains a conductor, insulator, braiding, and sheath. The sheath covers the braiding, the braiding covers the insulation, and the insulation covers the conductor.



## Twisted-pair cables

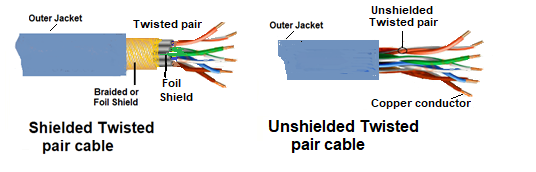
The twisted-pair cable was primarily developed for computer networks. This cable is also known as Ethernet cable. Almost all modern LAN computer networks use this cable.

This cable consists of color-coded pairs of insulated copper wires. Every two wires are twisted around each other to form pair. Usually, there are four pairs. Each pair has one solid color and one stripped color wire. Solid colors are blue, brown, green, and orange. In stripped color, the solid color is mixed with the white color.

Based on how pairs are stripped in the plastic sheath, there are two types of twisted-pair cable; UTP and STP.

In the UTP (*Unshielded twisted-pair*) cable, all pairs are wrapped in a single plastic sheath.

In the STP (*Shielded twisted-pair*) cable, each pair is wrapped with an additional metal shield, then all pairs are wrapped in a single outer plastic sheath.



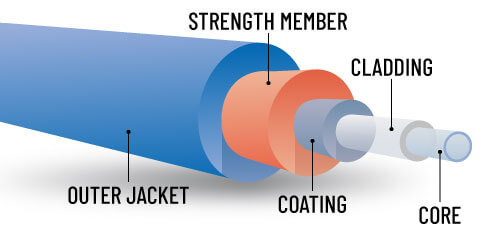
## Fiber optic cable

This cable consists of a core, cladding, buffer, and jacket. The core is made from thin strands of glass or plastic that can carry data over a long distance. The core is wrapped in the cladding; the cladding is wrapped in the buffer, and the buffer is wrapped in the jacket.

* Core carries the data signals in the form of light.
* Cladding reflects light back to the core.
* Buffer protects the light from leaking.
* The jacket protects the cable from physical damage.

Fiber optic cable is completely immune to EMI and RFI. This cable can transmit data over a long distance at the highest speed. It can transmit data up to 40 kilometers at the speed of 100Gbps.

Fiber optic uses light to send data. It reflects light from one endpoint to another. Based on how many beams of light are transmitted at a given time, there are two types of fiber optical cable; SMF and MMF.

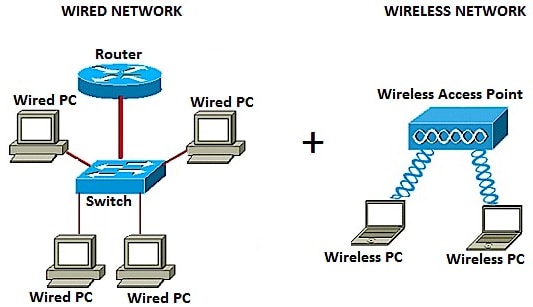


Q7. Wireless Access Points.

Ans. A wireless access point (WAP) is a hardware device or configured node on a local area network (LAN) that allows wireless capable devices and wired networks to connect through a wireless standard, including Wi-Fi or Bluetooth. WAPs feature radio transmitters and antennae, which facilitate connectivity between devices and the Internet or a network.

A WAP is also known as a hotspot.

Wireless access points (WAP) may be used to provide network connectivity in office environments, allowing employees to work anywhere in the office and remain connected to a network. In addition, WAPs provide wireless Internet in public places, like coffee shops, airports and train stations.

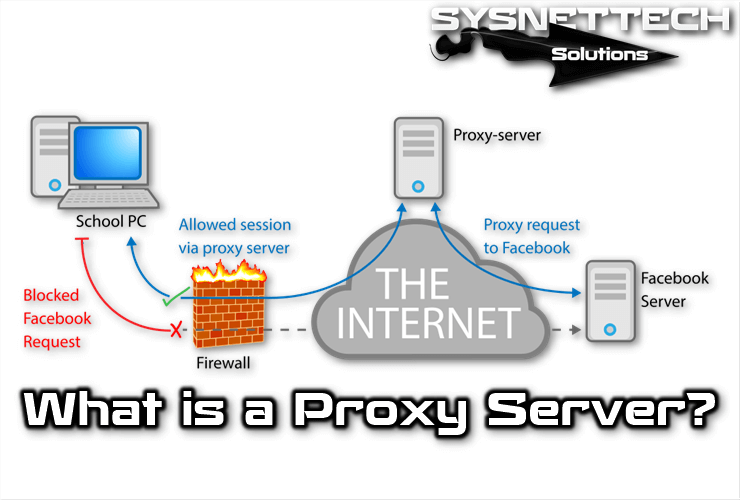


Q8. Proxy Servers and usages.

Ans. A proxy server acts as a gateway between you and the internet. It’s an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.

If you’re using a proxy server, internet traffic flows through the proxy server on its way to the address you requested. The request then comes back through that same proxy server (there are exceptions to this rule), and then the proxy server forwards the data received from the website to you.

Proxy servers act as a firewall and web filter, provide shared network connections, and cache data to speed up common requests. A good proxy server keeps users and the internal network protected from the bad stuff that lives out in the wild internet. Lastly, proxy servers can provide a high level of privacy.



Q9. Firewall and working principle.

Ans. A firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules. In general, the purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate communication to flow freely. In most server infrastructures, firewalls provide an essential layer of security that, combined with other measures, prevent attackers from accessing your servers in malicious ways.

Firewalls analyze each block of data packets entering or leaving the Intranet or the host computer. Based on a defined set of security rules, a firewall can perform three actions:

1. **Accept:** allow the transmission of data packets.
2. **Drop:** block data packets with no reply.
3. **Reject:** Block data packets and send “unreachable error” to the source.
4. 