**Task 1: Various types of Network Topology.**

Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.

## BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.

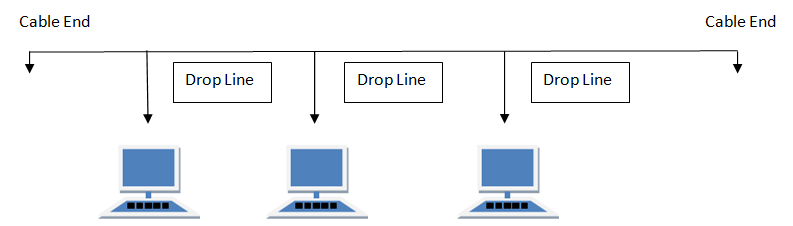


Fig No. 1.1: BUS Topology

#### **Features of Bus Topology**

1. It transmits data only in one direction.
2. Every device is connected to a single cable

#### **Advantages of Bus Topology**

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

#### **Disadvantages of Bus Topology**

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

**RING Topology**

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

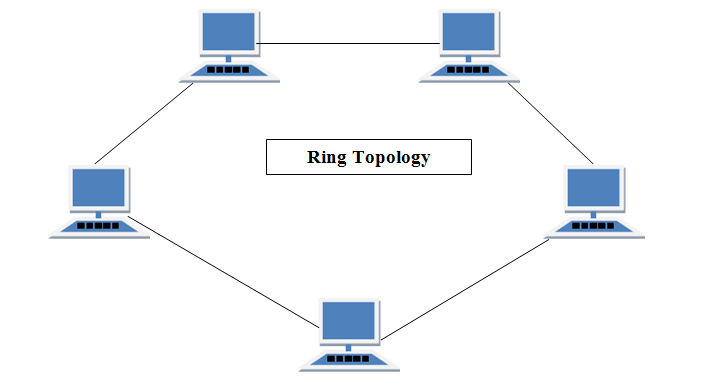


Fig No. 1.2: RING Topology

#### **Features of Ring Topology**

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

#### **Advantages of Ring Topology**

1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

#### **Disadvantages of Ring Topology**

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

**STAR Topology**

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

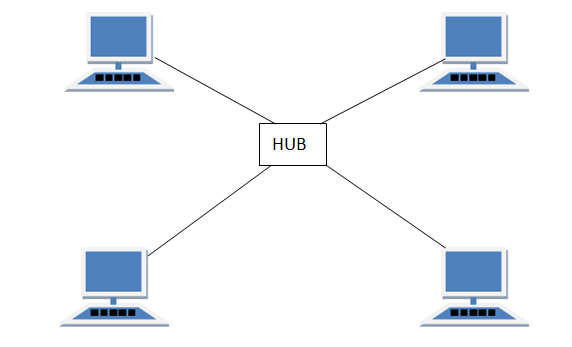


Fig No. 1.3: STAR Topology

#### **Features of Star Topology**

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

#### **Advantages of Star Topology**

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

#### **Disadvantages of Star Topology**

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity.

**MESH Topology**

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

1. Routing
2. Flooding

### **MESH Topology: Routing**

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

### **MESH Topology: Flooding**

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.

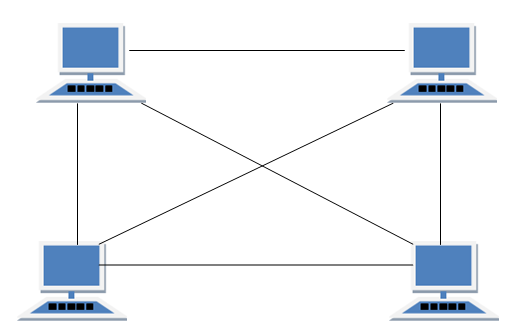


Fig No. 1.4: MESH Topology

#### **Types of Mesh Topology**

1. **Partial Mesh Topology :**In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :**Each and every nodes or devices are connected to each other.

#### **Features of Mesh Topology**

1. Fully connected.
2. Robust.
3. Not flexible.

#### **Advantages of Mesh Topology**

1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

#### **Disadvantages of Mesh Topology**

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

**HYBRID Topology**

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

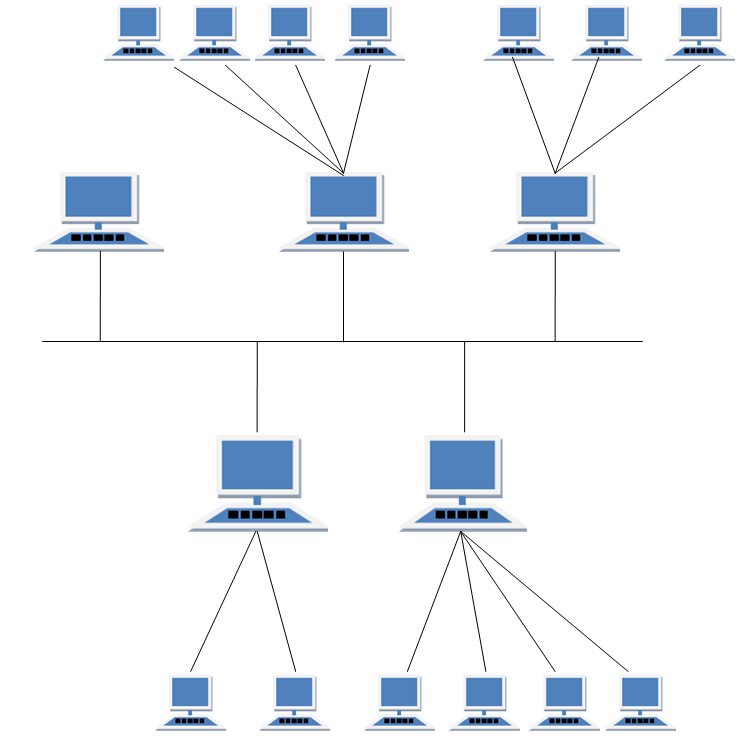


Fig No. 1.5: Hybrid Topology

#### **Features of Hybrid Topology**

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

#### **Advantages of Hybrid Topology**

1. Reliable as Error detecting and troubleshooting is easy.
2. Scalable as size can be increased easily.
3. Flexible.

#### **Disadvantages of Hybrid Topology**

1. Complex in design.
2. Costly.

**Task 2: To Learn the Usage Of Various Basic Tools Used In Establishing a LAN.**

**2.1 Crimping Tool**

A crimping tool is a device used to conjoin two pieces of metal by deforming one or both of them in a way that causes them to hold each other. The result of the tool's work is called a crimp. A good example of crimping is the process of affixing a connector to the end of a cable. For instance, network cables and phone cables are created using a crimping tool (shown below) to join the RJ-45 and RJ-11 connectors to the both ends of either phone or Cat 5 cable.

**2.2 How does it work?**

To use this crimping tool, each wire is first placed into the connector. Once all the wires are in the jack, the connector with wires are placed into the crimping tool, and the handles are squeezed together. Crimping punctures the plastic connector and holds each of the wires, allowing for data to be transmitted through the connector.



Fig 2.1: Crimping Tool

**2.3 Krone Tool**

A punch down tool, also called a krone tool, is a hand tool used to connect telecommunications and network wires to a patch panel, punch down block, keystone module, or surface mount box. The "punch down" part of the name comes from punching a wire into place using an impact action. It consists of a handle, a spring mechanism, and a removable slotted blade. When the punch down tool connects a wire, the blade cuts off the excess wire.

**2.4 How does it work?**

However, the punch down tool blade also is usually used to cut off excess wire, in the same operation as making the connection; this is done with a sharp edge of the punch down tool blade trapping the wire to be cut against the plastic punch block. If this cutoff feature is heavily used, the tool blade must be resharpened or replaced from time to time. Tool blades without the sharp edge are also available; these are used for continuing a wire through a slotted post to make connections with another slotted post. For light-duty use, there are also less-expensive punch down tools with fixed blades and no impact mechanism. These low-cost tools are more time-consuming for making reliable connections, and can cause muscle fatigue when used for large numbers of connections.



Fig 2.2: Krone Tool

**Task 3: To Make A Certain Copper Cable Using Different Standards.**

**3.1 Straight Through & Cross Over Cable**

Before you get started, make sure you have the necessary tools, and decide whether you're going to use Cat 5e or Cat 6 network cables. What you'll need:

* Unshielded twisted pair (UTP) patch cable
* Modular connector (8P8C plug, aka RJ45)
* Crimping tool
* Cable tester (optional, but recommended)

There are four pairs of wires in an Ethernet cable, and an Ethernet connector has eight pin slots. Each pin is identified by a number, starting from left to right, with the clip facing away from you. The two standards for wiring Ethernet cables are T568A and T568B. T568B is the most common and is what we'll be using for our straight Ethernet cable. The tables below show the proper orientation of the colored wires to the pins.

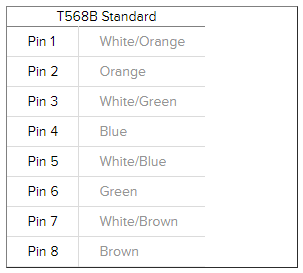
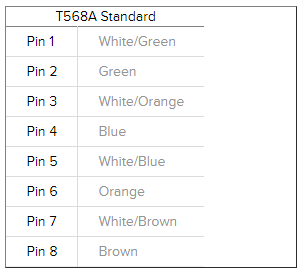


Fig 3.1: T568A And T568B Standards

* Steps to make a straight through cable are as follows:

1. Strip the cable jacket about 1.5 inch down from the end.



Fig 3.2: Striping The Cable

1. Spread the four pairs of twisted wire apart. For Cat 5e, you can use the pull string to strip the jacket farther down if you need to, then cut the pull string. Cat 6 cables have a spine that will also need to be cut.

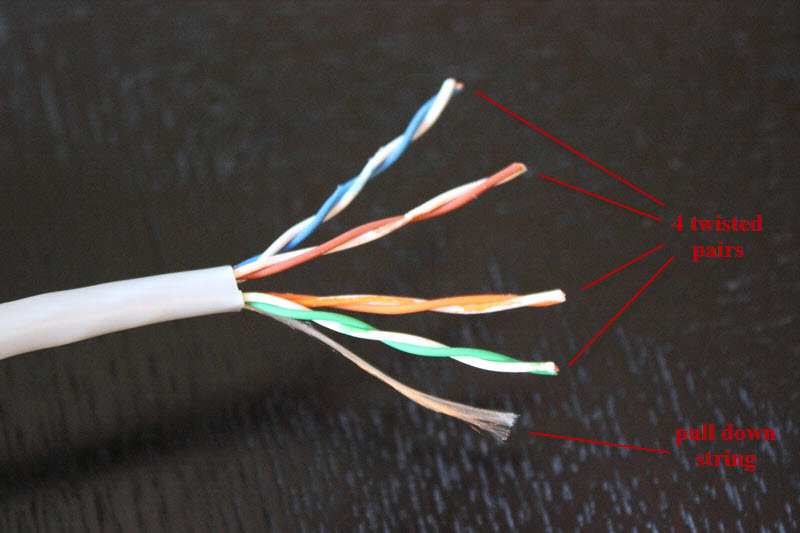


Fig 3.3: Spreading The Cable

1. Untwist the wire pairs and neatly align them in the T568B orientation. Be sure not to untwist them any farther down the cable than where the jacket begins; we want to leave as much of the cable twisted as possible.

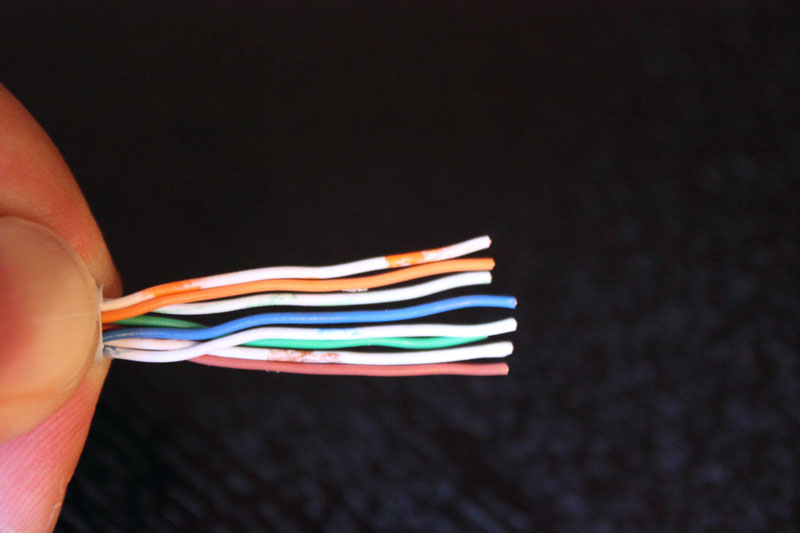


Fig 3.4: Untwisting the Cable

1. Cut the wires as straight as possible, about 0.5 inch above the end of the jacket.
2. Carefully insert the wires all the way into the modular connector, making sure that each wire passes through the appropriate guides inside the connector.

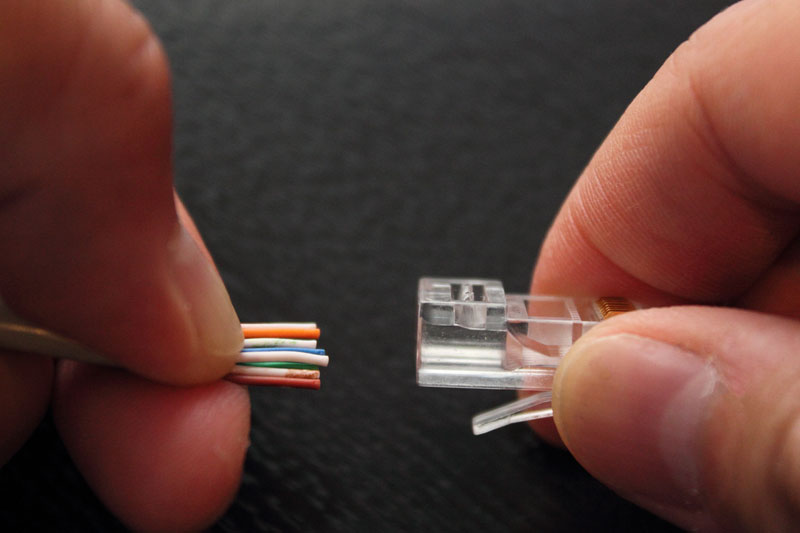


Fig 3.5: Inserting the Wires

1. Push the connector inside the crimping tool and squeeze the crimper all the way down.

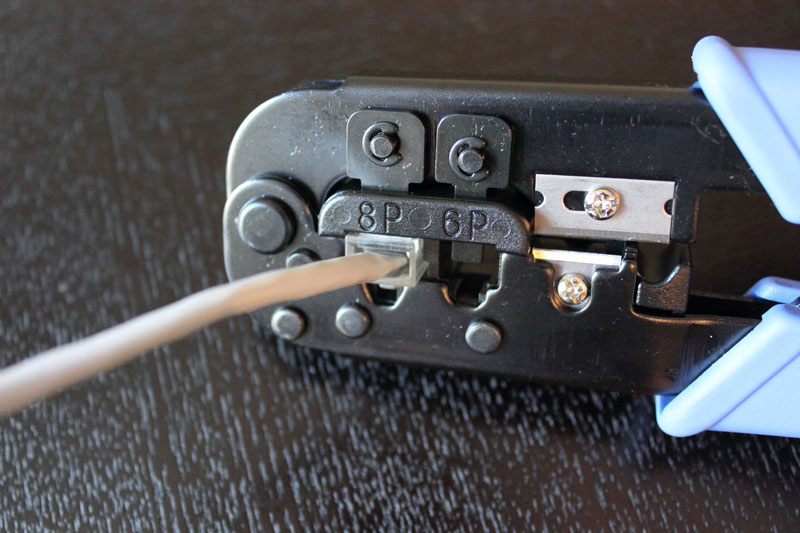


Fig 3.6: Crimping the Wire

1. Repeat steps 1-6 for the other end of the cable.
2. To make sure you've successfully terminated each end of the cable, use a cable tester to test each pin.



Fig 3.7: Testing the Wire

1. When you're all done, the connectors should look like this:

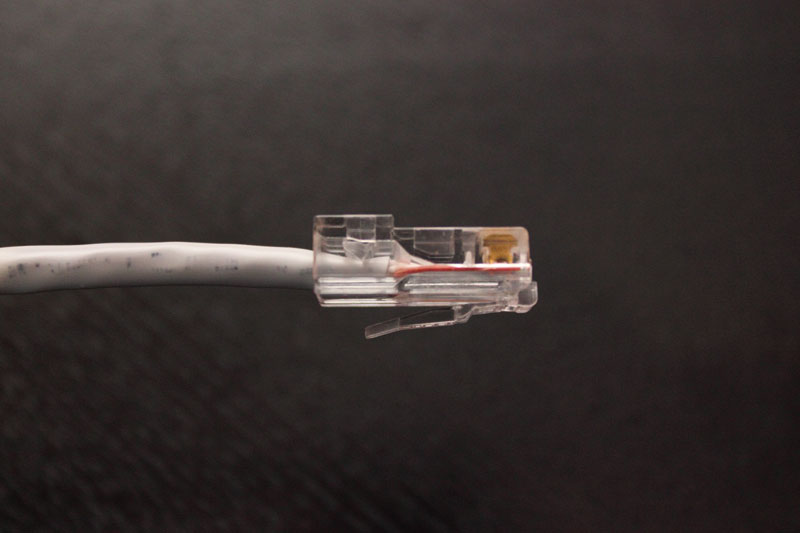


Fig 3.8: Complete LAN Wire

**3.2 Categories for Ethernet cables**

A variety of different cables are available for Ethernet and other telecommunications and networking applications. These cables that are described by their different categories, e.g. Cat 5 cables, Cat-6 cables, etc, which are often recognised by the TIA (telecommunications Industries Association) and they are summarised below:

* Cat-1: This is not recognised by the TIA/EIA. It is the form of wiring that is used for standard telephone (POTS) wiring, or for ISDN.
* Cat-2: This is not recognised by theTIA/EIA. It was the form of wiring that was used for 4Mbit/s token ring networks.
* Cat-3: This cable is defined in TIA/EIA-568-B. It is used for data networks employing frequencies up to 16 MHz. It was popular for use with 10 Mbps Ethernet networks (100Base-T), but has now been superseded by Cat-5 cable.
* Cat-4: This cable is not recognised by the TIA/EIA. However it can be used for networks carrying frequencies up to 20 MHz. It was often used on 16Mbps token ring networks.
* Cat-5: This is not recognised by the TIA/EIA. It is the cable that is widely used for 100Base-T and 1000Base-T networks as it provides performance to allow data at 100 Mbps and slightly more (125 MHz for 1000Base-T) Ethernet. Cat 5 cable is now obsolete and therefore it is not recommended for new installations.
* Cat-5e: This form of cable is recognised by the TIA/EIA and is defined in TIA/EIA-568-B.. It has a slightly higher frequency specification that Cat-5 cable as the performance extends up to 125 Mbps. It can be used for 100Base-T and 1000Base-t (Gigabit Ethernet). Cat 5e or enhanced is a form of Cat 5 cable manufactured t0 higher specifications although physically the same as Cat 5. It is tested to a higher specification.
* Cat-6: This cable is defined in TIA/EIA-568-B provides a significant improvement in performance over Cat5 and Cat 5e. During manufacture Cat 6 cables are more tightly wound than either Cat 5 or Cat 5e and they often have an outer foil or braided shielding. The shielding protects the twisted pairs of wires inside the Ethernet cable, helping to prevent crosstalk and noise interference. Cat-6 cables can technically support speeds up to 10 Gbps, but can only do so for up to 55 metres.
* Cat-6a: The “a” in Cat 6a stands for “Augmented.” The Cat 6a cables are able to support twice the maximum bandwidth, and are capable of maintaining higher transmission speeds over longer cable lengths. Cat 6a cables utilise shielded which is sufficient to all but eliminate crosstalk. However this makes them less flexible than Cat 6 cable.
* Cat-7: This is an informal number for ISO/IEC 11801 Class F cabling. It comprises four individually shielded pairs inside an overall shield. It is aimed at applications where transmission of frequencies up to 600 Mbps is required.

**3.3 Color Coding of Ethernet Cables**

There are two basic ethernet cable pin outs. A straight through ethernet cable, which is used to connect to a hub or switch, and a crossover ethernet cable used to operate in a peer-to-peer fashion without a hub/switch. Generally all fixed wiring should be run as straight through. Some ethernet interfaces can cross and un-cross a cable automatically as needed, a handy feature.

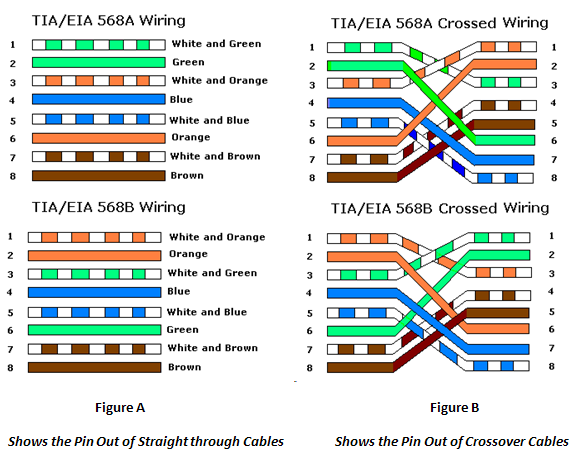


Fig 3.9: Color Coding of Ethernet Cables

**Task 4: To Learn the Usage of Connecters and Cables Used in Networks.**

**4.1 Cables**

Networking cables are networking hardware used to connect one network device to other network devices or to connect two or more computers to share printers, scanners etc. Different types of network cables, such as coaxial cable, optical fiber cable, and twisted pair cables, are used depending on the network's physical layer, topology, and size. The devices can be separated by a few meters or nearly unlimited distances. There are several technologies used for network connections. Patch cables are used for short distances in offices and wiring closets. Electrical connections using twisted pair or coaxial cable are used within a building. Optical fiber cable is used for long distances or for applications requiring high bandwidth or electrical isolation. Many installations use structured cabling practices to improve reliability and maintainability. In some home and industrial applications power lines are used as network cabling.

**4.1.1 Coaxial Cable**

Coaxial cable, is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a transmission line.

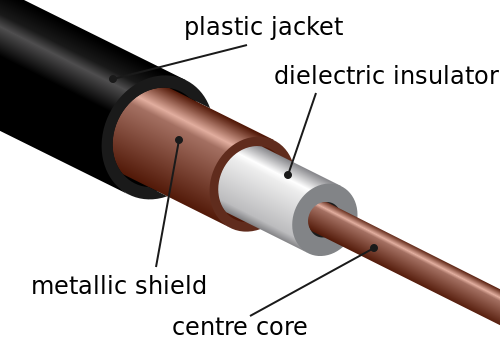


Fig 4.1: Internal View of Coaxial Cable

Coaxial cable conducts electrical signal using an inner conductor (usually a solid copper, stranded copper or copper plated steel wire) surrounded by an insulating layer and all enclosed by a shield, typically one to four layers of woven metallic braid and metallic tape. The cable is protected by an outer insulating jacket. Normally, the shield is kept at ground potential and a signal carrying voltage is applied to the center conductor.



Fig 4.2: Coaxial Cable

The advantage of coaxial design is that electric and magnetic fields are restricted to the dielectric with little leakage outside the shield. Conversely, electric and magnetic fields outside the cable are largely kept from interfering with signals inside the cable. Larger diameter cables and cables with multiple shields have less leakage. This property makes coaxial cable a good choice for carrying weak signals that cannot tolerate interference from the environment or for stronger electrical signals that must not be allowed to radiate or couple into adjacent structures or circuits. Common applications of coaxial cable include video and CATV distribution, RF and microwave transmission, and computer and instrumentation data connections.

**4.1.2 Twisted Pair Cable**

Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources; for instance, electromagnetic radiation from unshielded twisted pair (UTP) cables, and crosstalk between neighboring pairs. It was invented by Alexander Graham Bell. There are two twisted pair types:

* Shielded Twisted Pair Cable (Stp): It has a fine wire mesh surrounding the wires to protect the transmission. This shielding can be applied to individual pairs or quads, or to the collection of pairs. Individual pairs are foiled, while overall cable may use braided screen, foil, or braiding with foil. Because the shielding is made of metal, it may also serve as a ground. Usually a shielded twisted pair cable has a special grounding wire added called a drain wire which is electrically connected to the shield or screen. The drain wire simplifies connection to ground at the connectors. Shielded cable is used in older telephone networks, as well as network and data communications to reduce outside interference.

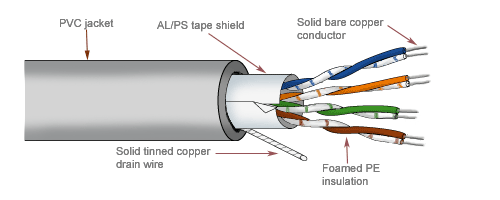


Fig 4.3: Shielded Twisted Pair Cable

* Unshielded Twisted Pair Cable (Utp): These are found in many Ethernet networks and telephone systems. For indoor telephone applications, UTP is often grouped into sets of 25 pairs according to a standard 25-pair color code originally developed by AT&T Corporation. A typical subset of these colors (white/blue, blue/white, white/orange, orange/white) shows up in most UTP cables. For urban outdoor telephone ocables containing hundreds or thousands of pairs, the cable is divided into small but identical bundles.

Each bundle consists of twisted pairs that have different twist rates. The bundles are in turn twisted together to make up the cable. Pairs having the same twist rate within the cable can still experience some degree of crosstalk. Wire pairs are selected carefully to minimize crosstalk within a large cable. UTP cable is also the most common cable used in computer networking. Modern Ethernet, the most common data networking standard, can use UTP cables. Twisted pair cabling is often used in data networks for short and medium length connections because of its relatively lower costs compared to optical fiber and coaxial cable.

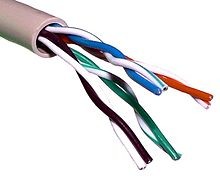
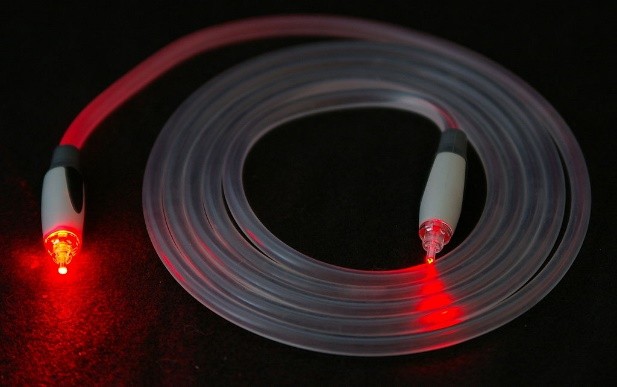


Fig 4.4: Unshielded twisted pair cable

**4.1.3 Optical Fibre**

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.



**Fig 4.5:** Optical Fibre Cable

Optical fiber consists of a core and a cladding layer, selected for total internal reflection due to the difference in the refractive index between the two. In practical fibers, the cladding is usually coated with a layer of acrylate polymer or polyimide. This coating protects the fiber from damage but does not contribute to its optical waveguide properties. Individual coated fibers (or fibers formed into ribbons or bundles) then have a tough resin buffer layer and/or core tube(s) extruded around them to form the cable core. Several layers of protective sheathing, depending on the application, are added to form the cable. Rigid fiber assemblies sometimes put light-absorbing ("dark") glass between the fibers, to prevent light that leaks out of one fiber from entering another. This reduces cross-talk between the fibers, or reduces flare in fiber bundle imaging applications.

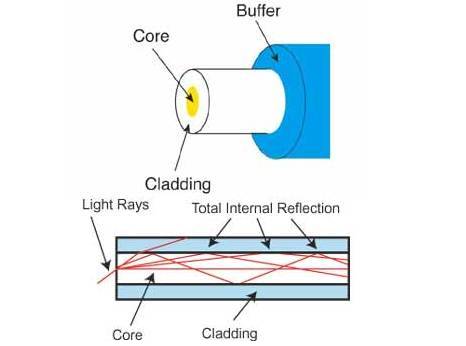


Fig 4.6: Internal View of Optical Fibre Cable

Optical fibers are very strong, but the strength is drastically reduced by unavoidable microscopic surface flaws inherent in the manufacturing process. The initial fiber strength, as well as its change with time, must be considered relative to the stress imposed on the fiber during handling, cabling, and installation for a given set of environmental conditions. There are three basic scenarios that can lead to strength degradation and failure by inducing flaw growth: dynamic fatigue, static fatigues, and zero-stress aging.

**4.2 CONNECTORS**

In information science, connectors, normally called "input-output connectors" (or I/O for short), are interfaces for linking devices by using cables. They generally have a male end with pins protruding from it. This plug is meant to be inserted into a female part (also called a socket), which includes holes for accommodating the pins. However, there are "hermaphroditic" plugs which can act as either male or female plugs, and can be inserted into either one.

**4.2.1 BNC Connector**

The BNC (Bayonet Neill–Concelman) connector used with coaxial cables such as the RG-58 A/U cable used with the 10Base-2 Ethernet system. The basic BNC connector is a male type mounted at each end of a cable. This connector has a center pin connected to the center cable conductor and a metal tube connected to the outer cable shield. A rotating ring outside the tube locks the cable to any female connector.

It is a miniature quick connect/disconnect radio frequency connector used for coaxial cable. It features two bayonet lugs on the female connector; mating is fully achieved with a quarter turn of the coupling nut. BNC connectors are used with miniature-to-subminiature coaxial cable in radio, television, and other radio-frequency electronic equipment, test instruments, and video signals. BNC connectors can also be used to connect some monitors, which increases the accuracy of the signals sent from the video adapter.

BNC T-connectors (used with the 10Base-2 system) are female devices for connecting two cables to a network interface card (NIC).



Fig 4.7: BNC Connector

**4.2.2 RJ Connector**

A family of push-and-click connectors for twisted-pair wiring in telephone and network wiring. RJ stands for Registered Jack. RJ types define both a jack or receptacle (female) and a plug (male) type of connector. The most common types of RJ connectors are as follows:

* RJ-11 Connector: A 4-wire or 6-wire telephone-type connector that connects telephones to wall plates. RJ-11 supports up to six wires, but usually only four are used with the two-pair twisted-pair cabling commonly found in telephone cabling.

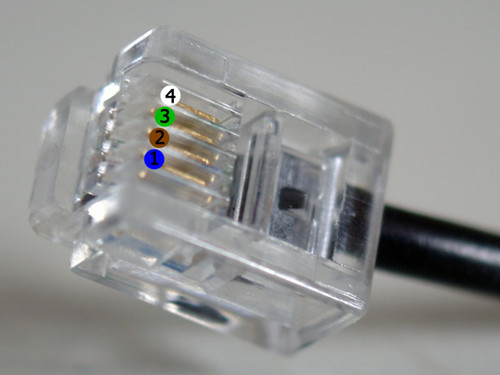


Fig 4.8: RJ 11 Connector

* RJ-45 Connector: An 8-wire telephone-type connector used with twisted-pair cabling for connecting computers, wall plates, patch panels, and other networking components. RJ-45 is the standard type of connector for both unshielded twisted-pair (UTP) and shielded twisted-pair (STP) cabling in star-topology Ethernet networks such as 10BaseT and 100BaseT4. RJ-45 is defined in International Organization for Standardization (ISO) standard 8877.
* RJ-48 Connector: An 8-wire telephone-type connector used with twisted-pair cabling for connecting T1 and 56-KB digital data service (DDS) lines. RJ-48 uses the same jack as RJ-45 but uses a different pinning, with one pair of wires to transmit signals, one pair to receive signals, one pair for drain, and one unused pair (reserved for future use). RJ-48 connectors come in three varieties: RJ-48C and RJ-48X for connecting T1 lines, and RJ-48S for connecting 56-KB DDS lines.

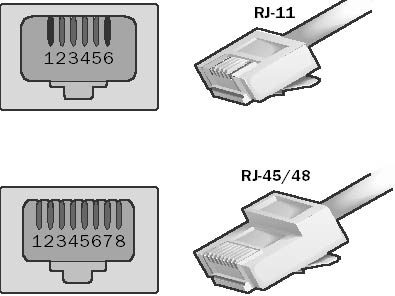


Fig 4.9: RJ 45/48 Connector

**4.2.3 ST Connector**

ST stands for Straight Tip - a quick release bayonet style Connector developed by AT&T. ST Connectors are among the most commonly used Fiber optic connectors in networking applications. They are cylindrical with twist lock coupling, 2.5mm keyed ferrule. ST Connectors are used both short distance applications and long line systems. The ST connector has a bayonet mount and a long cylindrical Ferrule to hold the fiber. Because they are spring-loaded, you have to make sure they are seated properly. They are easily inserted and removed due to their design. If you experience high Light loss, try reconnecting. ST connectors come in two versions: ST and ST-II. These are keyed and spring-loaded. They are push-in and twist types. They are rated for 500 mating cycles. The typical Insertion Loss for matched ST connectors is 0.25 dB. View all Fiber Optic Connectors.

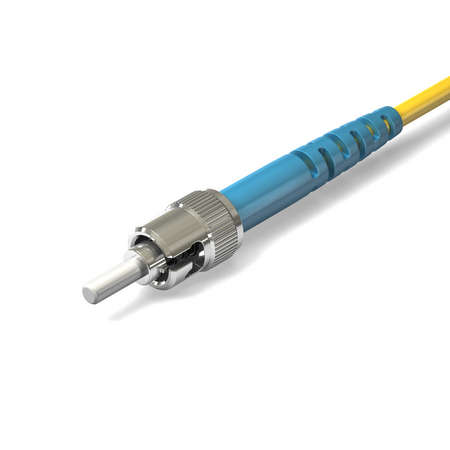


Fig 4.10: ST Connector

**4.2.4 SC Connector**

SC stands for Subscriber Connector- a general purpose push/pull style Connector developed by NTT. SC has an advantage in keyed duplexibility to support send/receive channels. SC Connectors are frequently used for newer Network applications. The SC is a snap-in connector that is widely used in singlemode systems for its performance. The SC connector is also available in a Duplex configuration. They offer low cost, simplicity, and durability. SC connectors provide for accurate alignment via their ceramic ferrules.



Fig 4.11: SC Connector

**Task 5: Comparison of Twisted Pair Cables.**

Comparison of Twisted Pair Cables

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Attribute/Cable Types | Year of Launch | Bandwidth | Distance | Data Speed | Shielded/Unshielded | Applications |
| CAT 1 | 1983 | 0.4 MHz | \_ | 1 Mbps | Unshielded | Telephone and modem lines |
| CAT 2 | 1984 | 4 MHz | \_ | 4 Mbps | Unshielded | Older Terminal System |
| CAT 3 | 1985 | 16 MHz | 100m | 10 Mbps | Unshielded | 10 BASE-T and 100 BASE-T4 Ethernet |
| CAT 4 | 1991 | 20 MHz | 100m | 16 Mbps | Unshielded | Token Ring |
| CAT 5 | 1991 | 100 MHz | 100m | 100 Mbps | Unshielded | 100 BASE-TX & 1000 BASE-T Ethernet |
| CAT 5e | 1999 | 100 MHz | 100m | 1 Gbps | Unshielded | 100 BASE-TX & 1000 BASE-T Ethernet |
| CAT 6 | 2002 | 250 MHz | 100m | 10 Gbps | Unshielded | 10 GBASE Ethernet |
| CAT 6a | 2008 | 500 MHz | 100m | 10 Gbps | Unshielded | 10 GBASE Ethernet |
| CAT 7 | 2010 | 600 MHZ | 100m | 10 Gbps | Shielded | 10 GBASE-TX & Ethernet or 1000 BASE-T over single cable |
| CAT 7a | 2010 | 1000 MHz | 100m | 10 Gbps | Shielded | 10 GBASE-TX & Ethernet or 1000 BASE-T over single cable |
| CAT 8/8.1 | 2013 | 1600-2000  MHz | 30m | 40 Gbps | Shielded | 40 GBASE-TX & Ethernet or 1000 BASE-T over single cable |
| CAT 8.2 | 2013 | 1600-2000  MHz | 30m | 40 Gbps | Shielded | 40 GBASE-TX & Ethernet or 1000 BASE-T over single cable |

**Task 6: Study and familiarization with various network devices.**

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2-port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

* Active Hub: - These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.
* Passive Hub: - These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.

3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2-port device.

Types of Bridges

* Transparent Bridges: - These are the bridge in which the stations are completely unaware of the  
  bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of  
  the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
* Source Routing Bridges: - In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

4. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

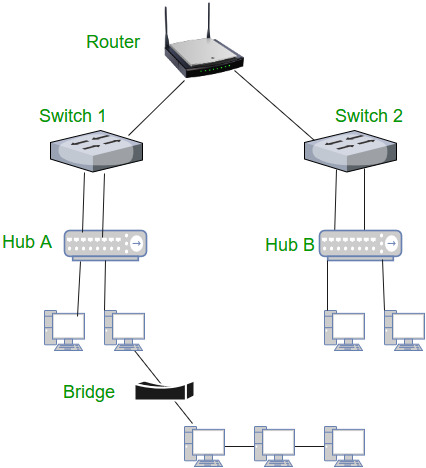


Fig No. 6.1: Devices working at different levels.

6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

7. Brouter – It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.

**Task 7: Familiarization with Network Tracer Tool (Cisco Packet Tracer).**

Packet Tracer is virtual networking simulation software developed by Cisco, to learn and understand various concepts in computer networks. Networking devices appear in packet tracer as they look in reality and a student can interact with various networking devices, by customizing the configurations, by turning them on and off etc. Packet Tracer is teaching and learning software and a tool, easy to work with, thus after working with virtual environment, a student gains lot of confidence, when it comes to working in real-time environment. We can track the path of a packet, when it moves from source to destination, and also learn and understand, how to troubleshoot a network, when a packet doesn’t reach the destination. Packet Tracer can be used to learn concepts more clearly by creating different scenarios. Since Networking is all about imagination and it’s difficult to track movement of packets in a real-time environment, thus various networking concepts can be explained by creating a virtual environment, showing the moment of packets, exactly as it would happen in real-time. Packet tracer can be used to understand the working of various networking devices, their use, what makes them different and their appropriate use in a designing a network. Packet tracer is a user-friendly tool, with various options, where a user can customize and design a network. Various tests can be run, to understand various network failures and how to troubleshoot them in real-time.

**Features of Packet Tracer: -**

**Workspaces:** There are two types of work space:

* **Logical Work-space:** It allows users to build logical network topologies and various devices can be dragged and dropped to logical workspace.
* **Physical work-space**: It allows a user to create a network, the way as it would look in real world, and has the capability of geographical representation, where different networking devices can be shown as connected at different locations of the city.

**Modes**: There are two types of Modes:

* **Real-time Mode:** The devices in a network behave as real devices do and look similar to real devices.
* **Simulation Mode:** In this mode, a student can see and control time intervals, to learn how to troubleshoot network failures.

**Networking Devices:** There are various networking devices which can be used to create different networking lab scenarios. E.g. Routers, Switches, Hubs, Wireless Devices, Connections, End Devices, WAN Emulation, Custom Made Devices, Multi-user Connection, Personal Computer, Laptops, Servers, Printers, IP Phones, VOIP Devices, Analog-Phones, TVs, Wireless-Tablets, PDAs, Wireless End Devices, Wired End Devices etc.

**Connections:** Various types of cables which can be used to connect various networking devices in a packet tracer are Console cable, Copper straight-through cable, Copper Cross-over Cable, Fibre Cable, Phone Cable, Coaxial Cable, Serial DTE, Serial DCE, and Octal Cable.

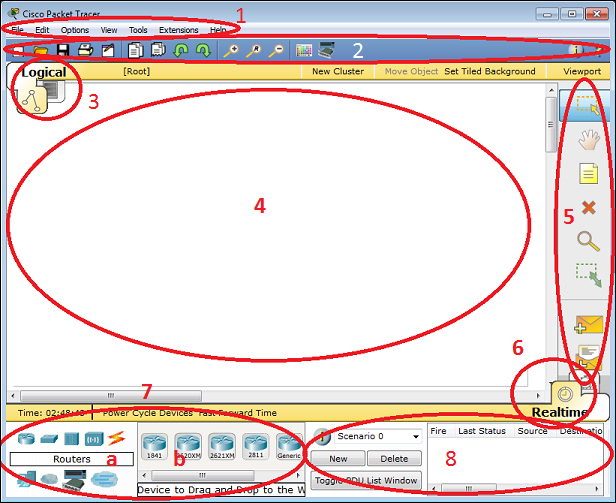


Fig No. 7.1: Cisco Packet Tracer

**The components of the Packet Tracer interface are as follows:**

* **Area 1: Menu bar** – This is a common menu found in all software applications; it is used to open, save, print, change preferences, and so on.
* **Area 2: Main toolbar** – This bar provides shortcut icons to menu options that are commonly accessed, such as open, save, zoom, undo, and redo, and on the right-hand side is an icon for entering network information for the current network.
* **Area 3: Logical/Physical workspace tabs** – These tabs allow you to toggle between the Logical and Physical work areas.
* **Area 4: Workspace** – This is the area where topologies are created and simulations are displayed.
* **Area 5: Common tools bar** – This toolbar provides controls for manipulating topologies, such as select, move layout, place note, delete, inspect, resize shape, and add simple/complex PDU.
* **Area 6: Realtime/Simulation tabs** – These tabs are used to toggle between the real and simulation modes. Buttons are also provided to control the time, and to capture the packets.
* **Area 7: Network component box** – This component contains all of the network and end devices available with Packet Tracer, and is further divided into two areas:
* **Area 7a: Device-type selection box** – This area contains device categories
* **Area 7b: Device-specific selection box** – When a device category is selected, this selection box displays the different device models within that category
* **Area 8: User-created packet box** – Users can create highly-customized packets to test their topology from this area, and the results are displayed as a list.

**Task 8: Creating topology with Layer 2 devices (Switch).**

**Steps:**

1. Take a Switch and connect four PCs with it using Copper Straight-Through cable.
2. Assign IP addresses to all the PCs by going to Desktop > IP Configuration.
3. Now go to any PC and then head over to Desktop > Command Prompt.
4. Type command – **ping 192.168.10.5** (IP address of any PC you want to ping).

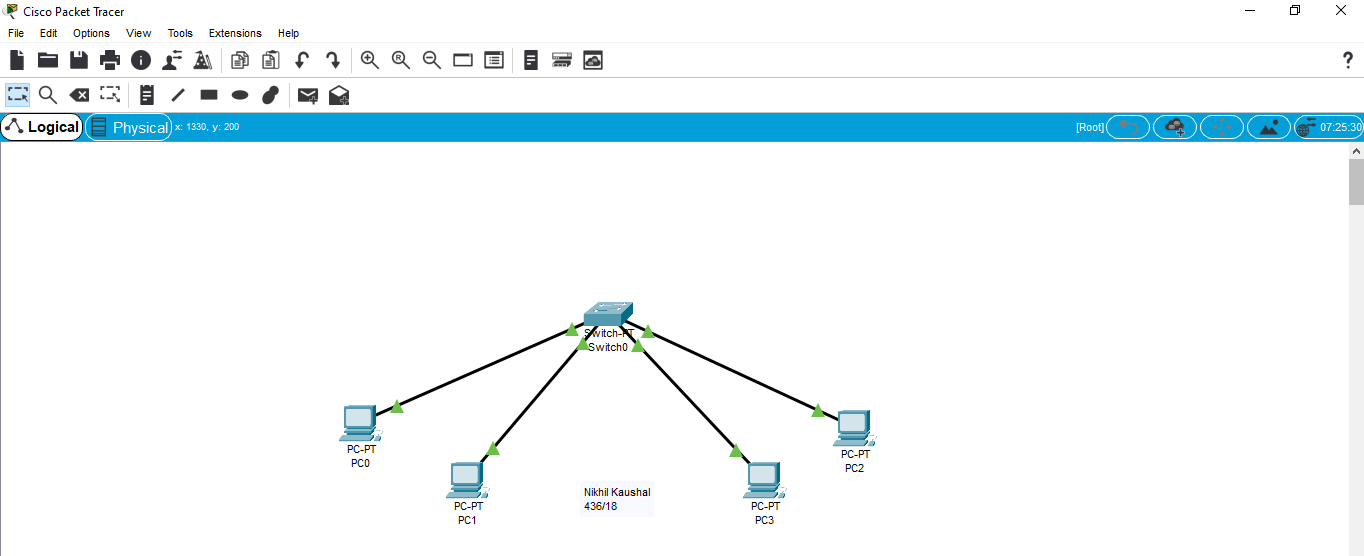


Fig No. 8.1: Topology with Layer-2 device (Switch)

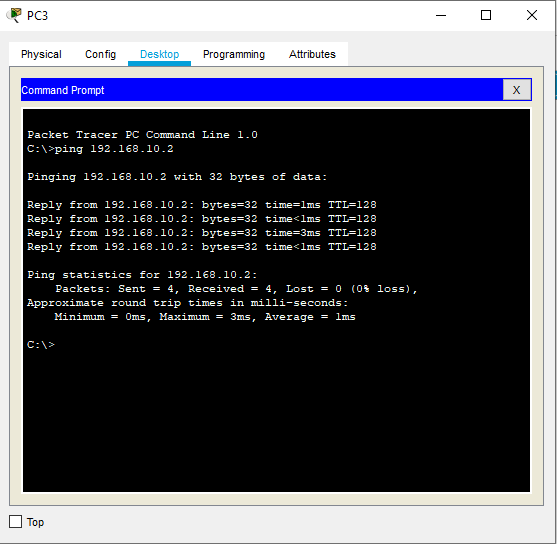


Fig No. 8.2: Ping command

**Task 9: Analysis of Ping command in Simulation mode.**

**Steps:**

1. Switch to Simulation Mode.
2. Go to Event List Filters and select ICMP.
3. Head over to any PC and go to Desktop > Command Prompt.
4. Type the command – **ping 192.168.10.2** (IP address of any PC you want to ping).
5. Carefully observe the movement of packet in Simulation Mode.

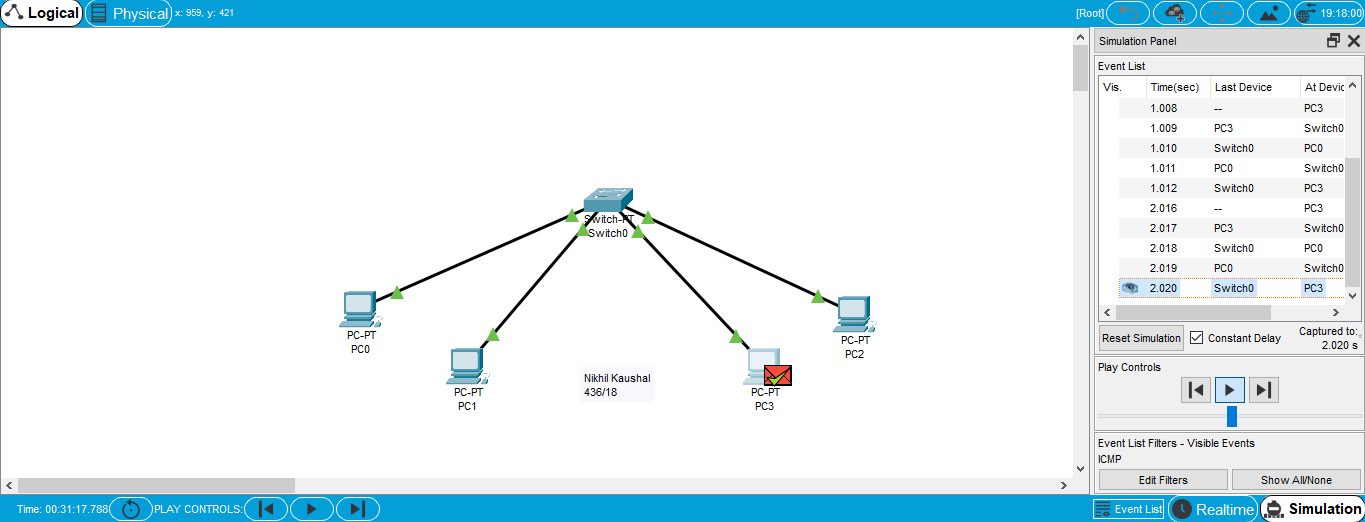


Fig No. 9.1: Ping command in Simulation Mode

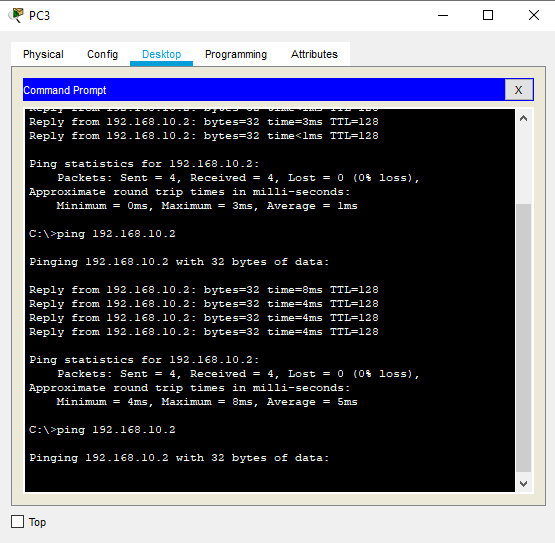


Fig No. 9.2: Ping command from PC 3 to PC 0

**Task 10: Analysis of ARP protocol in Simulation mode.**

**Steps:**

1. Go to any PC. Head over to Desktop > Command Prompt.
2. Type the command – **arp -a**.
3. Check if any ARP entries found.
4. Now, switch to Simulation Mode.
5. Go to any PC and head over to Desktop > Command Prompt.
6. Type the command – **ping 192.168.10.5** (IP Address of any PC you want to ping)
7. Now, observe the simulation of ARP carefully.
8. Head over to PC where you used the ping command and type – **arp -a**.
9. As, you can see now there will be a new entry with Internet Address and Physical Address.

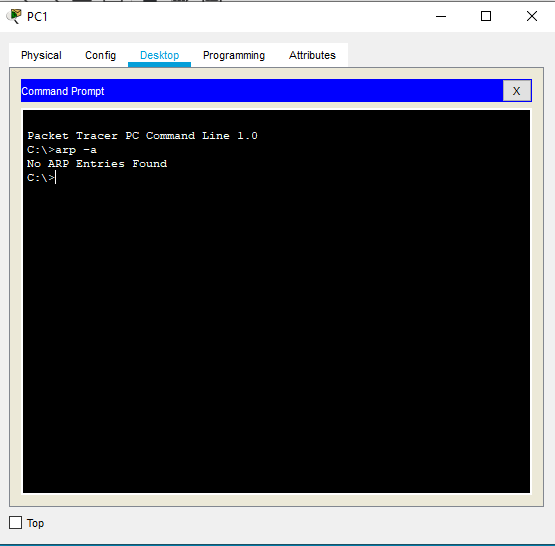


Fig No. 10.1: Check if there is any previous ARP entry

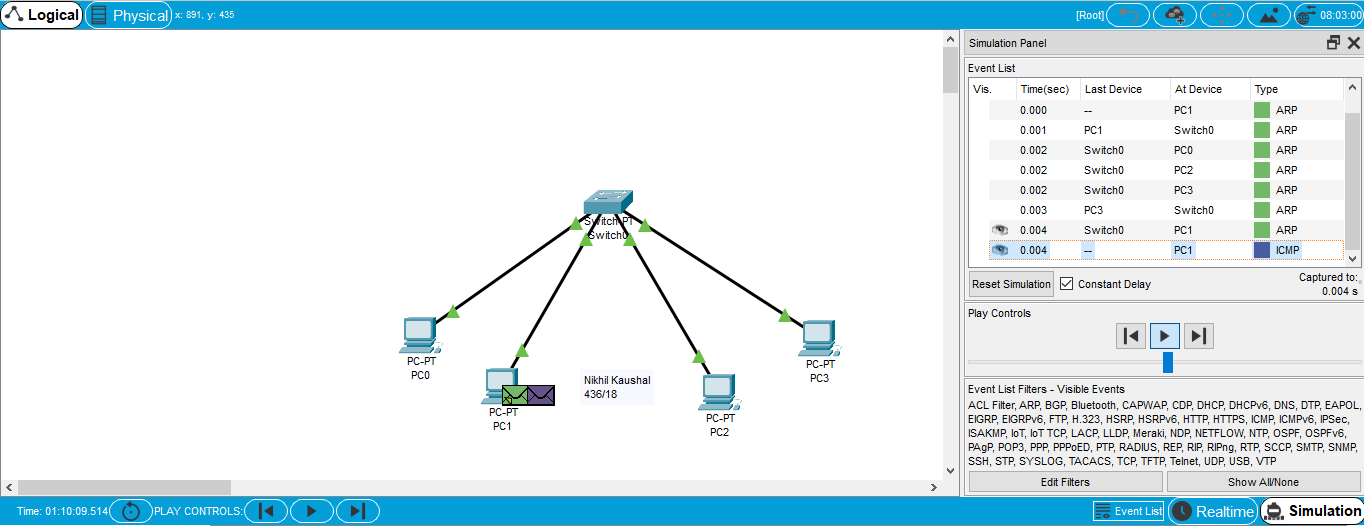


Fig No. 10.2: ARP simulation in Simulation Mode

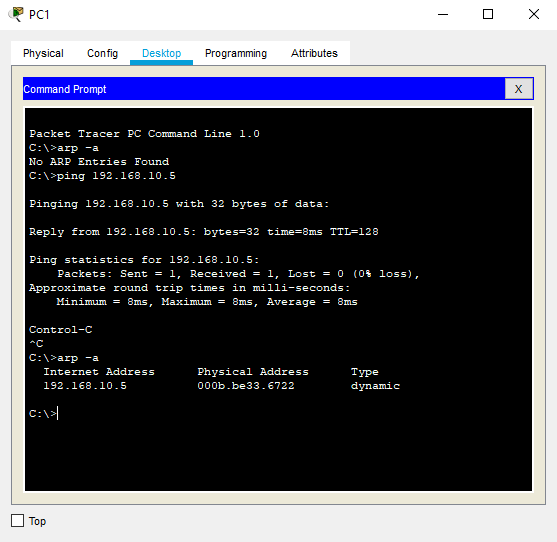
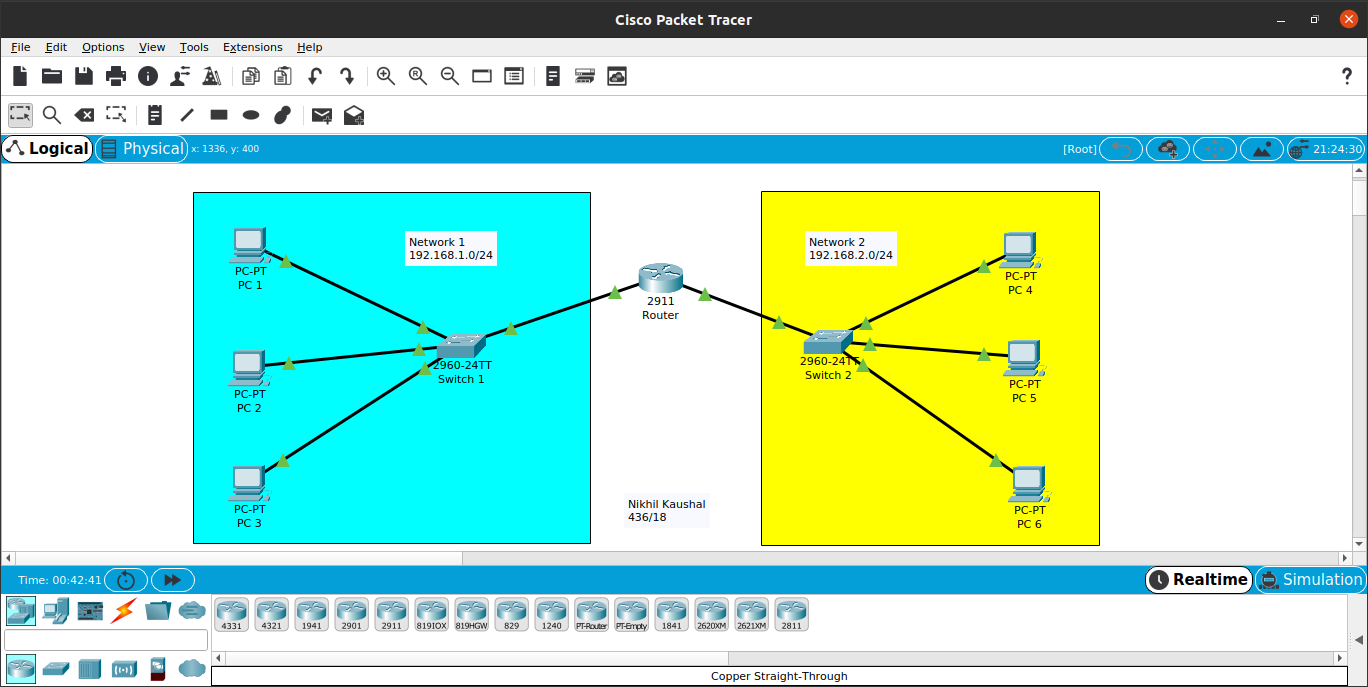


Fig No. 10.3: New ARP entry after successful pinging.

**Task 11: Connecting two networks using router.**

**Steps: -**

1. Take a router, two switches and four PCs.
2. With help of copper straight through cable, make connections between the switches and router and between the PCs and switches.
3. Assign ip address all four PCs and respective default gateway.
4. Go to router’s CLI and type commands to assign ip.
5. Firstly, type enable command (this will get us to privileged mode).
6. Then type configure terminal command (this command gets us to appropriate global configuration mode).
7. Then type interface (It can be Gigabit Ethernet, Fast Ethernet) and type desired ip address with subnet mask and a no shutdown command.
8. And type exit command and close the CLI.
9. Do assign these IP addresses as the default gateway to their particular networks.
10. Go to any PC and head over to Desktop > Command Prompt.
11. Type the command – **ping 192.168.2.11** (IP Address of any PC from other network you want to ping).
12. And observe the output shown in command prompt.

Fig No. 11.1: Connecting two networks using router topology

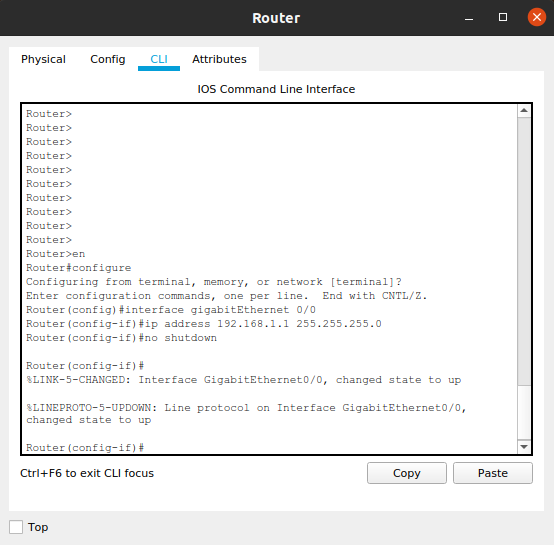
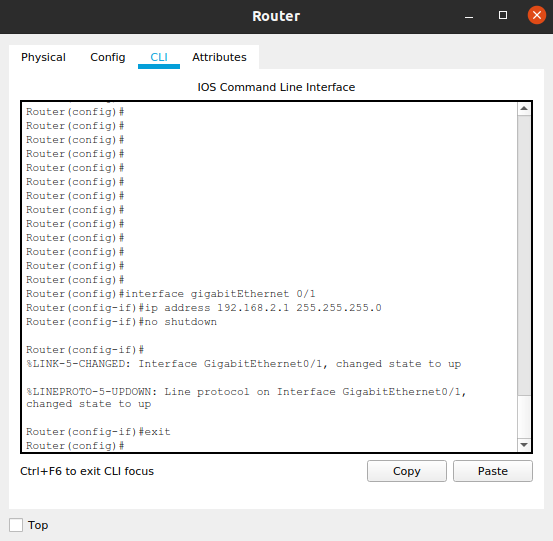
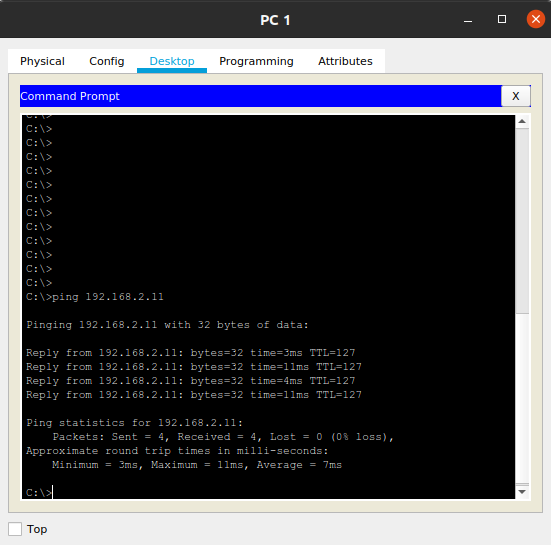


Fig No. 11.2: Router commands for configuring Switch 1

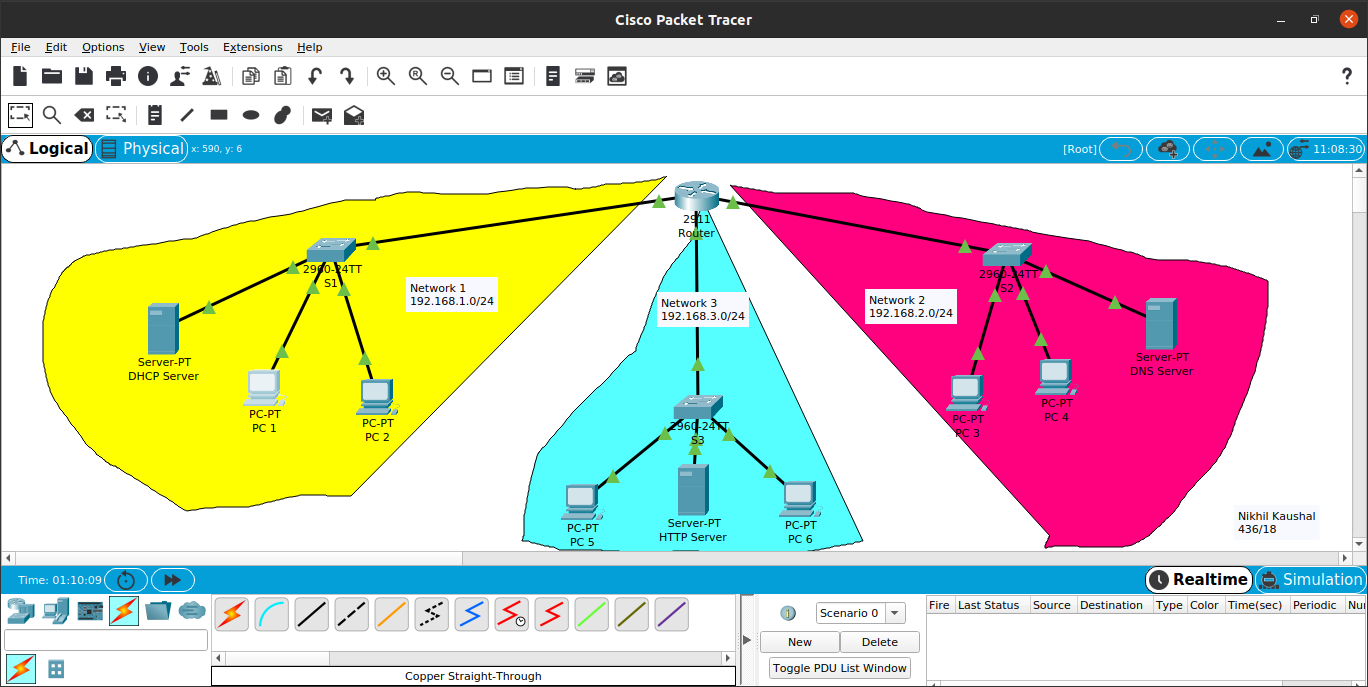
Fig No. 11.3: Router commands for configuring Switch 2

Fig No. 11.4: Ping command from PC 1 to PC 4

**Task 12: Create a network topology to configure and analyse DHCP , HTTP and DNS Server.**

**Steps: -**

1. Take a router, three switches, three servers and six PCs.
2. With help of copper straight through cable, make connections between the switches and router, between the PCs and switches and between the servers and switches.
3. Assign IP address through router’s CLI.
4. Go to router’s CLI and type commands to assign IP addresses.
5. Firstly, type enable command (this will get us to privileged mode).
6. Then type configure terminal command (this command gets us to appropriate global configuration mode).
7. Then type interface (It can be Gigabit Ethernet, fast Ethernet) and type desired Ip address with subnet mask and a no shutdown command.
8. After no shutdown command type exit so that to go back to privileged mode and type the command copy running-config startup-config. This saves the current runningconfiguration to the start-upconfiguration in the NVRAM.
9. And type exit command and close the CLI.
10. Now go to DHCP server, click on service On option and then add server pools with default gateway, DNS server, starting IP address, subnet mask and maximum number of users.
11. Now go to every PC’s of all the server and change the option of static ip to DHCP.
12. Observe the IP addresses.
13. By default, the services of HTTP server are ON. If we go to any PC and open the browser and try to put IP address of the HTTP Server, a default web page is shown.
14. We can access this web page by a particular URL by making an entry with IP address of the HTTP Server with a particular URL in DNS Server by turning its services ON.

Fig No. 12.1: Topology with DHCP, HTTP and DNS Server.

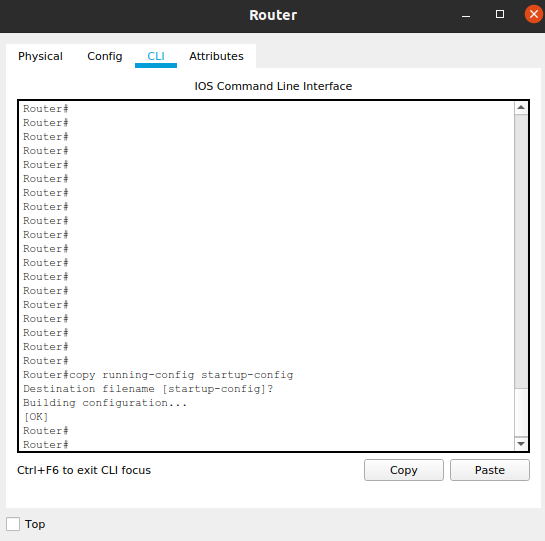
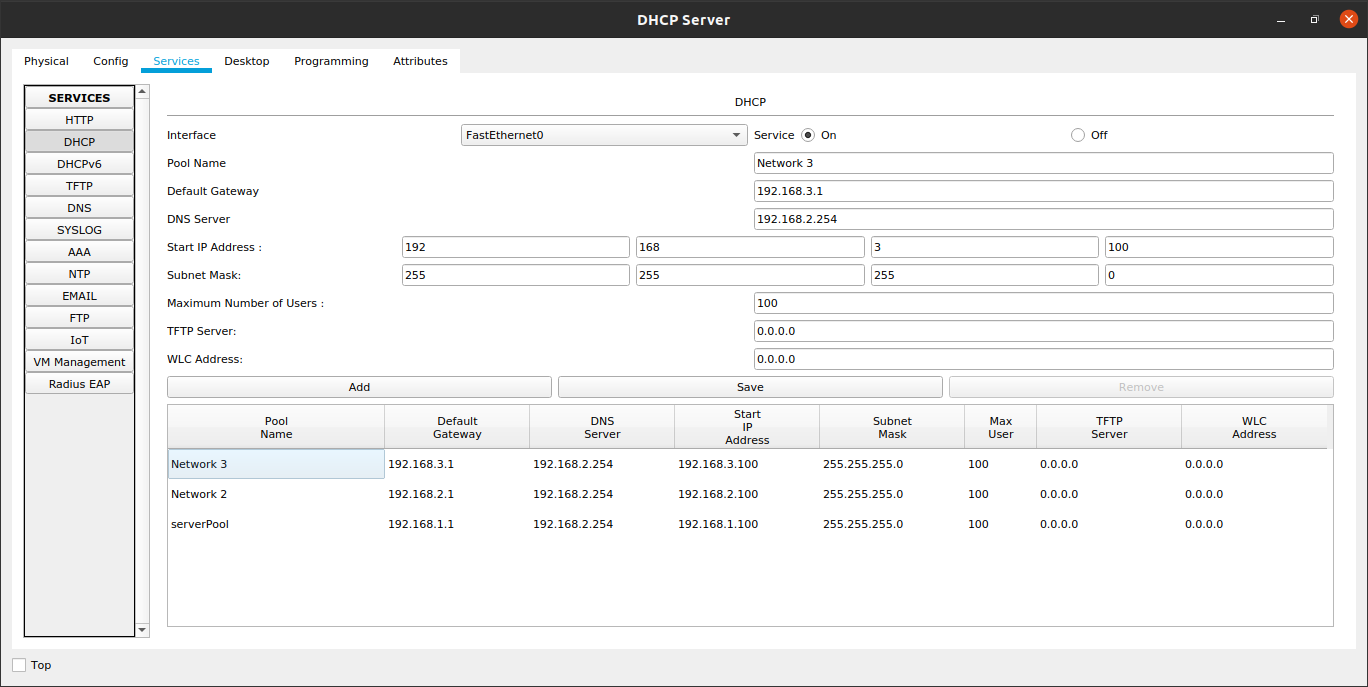
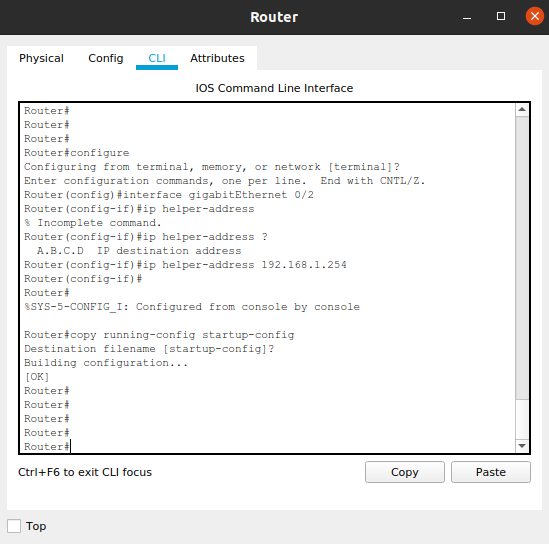
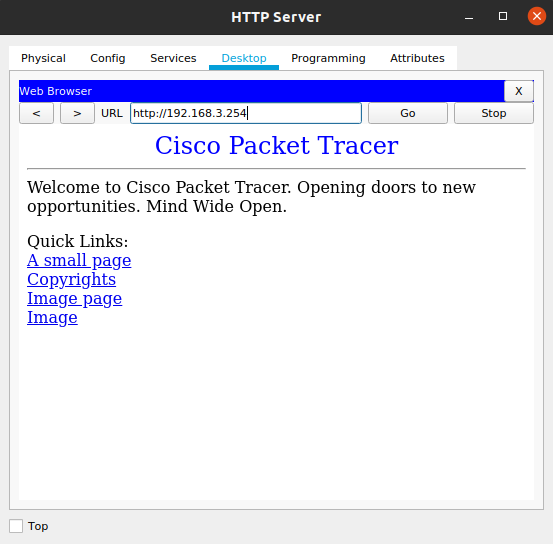
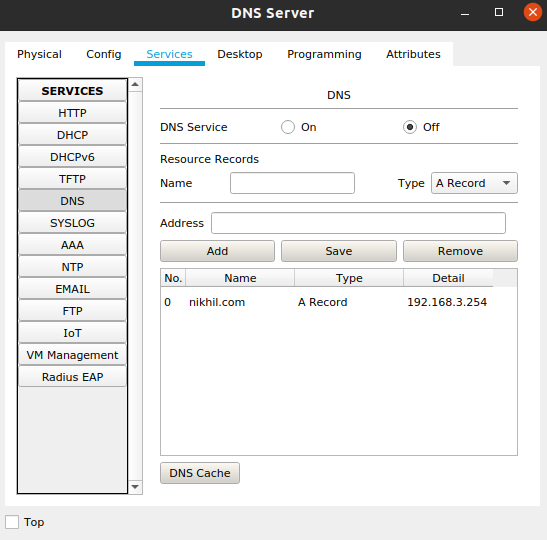


Fig No. 12.2: Saving the current runningconfiguration to the startupconfiguration.

Fig No. 12.3: Making DHCP Pool entries.

Fig No. 12.4: Router CLI commands for accessing the DHCP services in other networks.

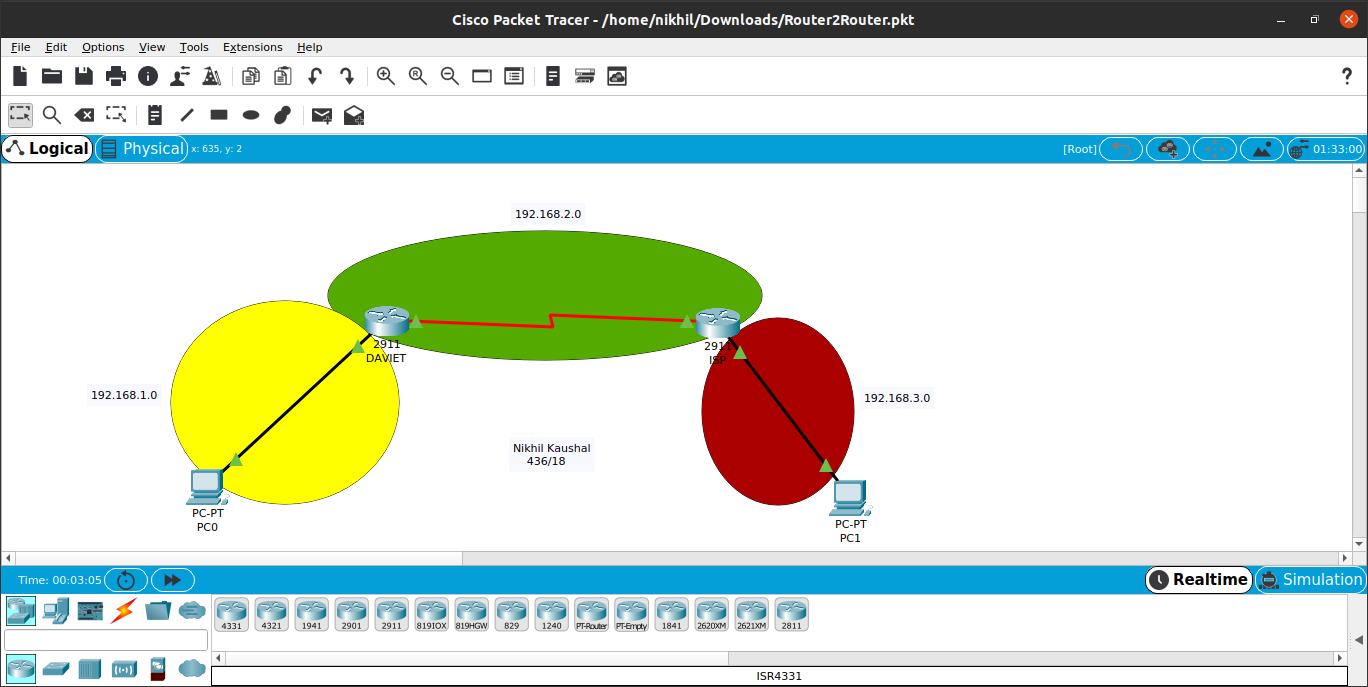
Fig No. 12.5: Using Web browser on HTTP Server

Fig No. 12.6: Adding a resource record on DNS Server.

**Task 13: Router to Router Communication.**

**Steps:**

1. Take two routers and two PCs.
2. With help of copper straight through cable, make connections between the PC’s and router and with help of serial connecting wires make connection between two routers.
3. Change the name of both the routers to DAVIET and Host
4. Assign IP address through both router’s CLI.
5. Go to router’s CLI and type commands to assign IP.
6. Firstly, type enable command (this will get us to privileged mode).
7. Then type configure terminal command (this command gets us to appropriate global configuration mode).
8. Then type interface (it can be gigabit Ethernet, fast Ethernet) and type desired ip address with subnet mask and a no shutdown command.
9. And type exit command and close the CLI.
10. Go to any PC and head over to Desktop > Command Prompt.
11. Type the command – **ping 192.168.3.2** (IP Address of any PC you want to ping) and observe output.

Fig No. 13.1: - Router to Router Communication Topology.

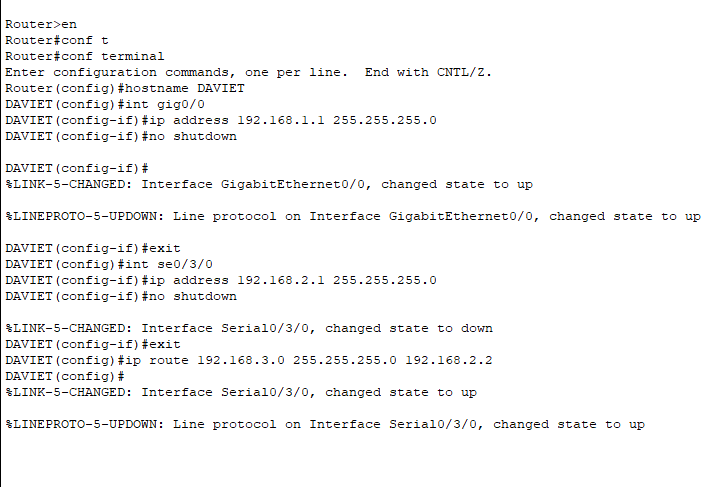


Fig No. 13.2: - Commands to DAVIET Router.

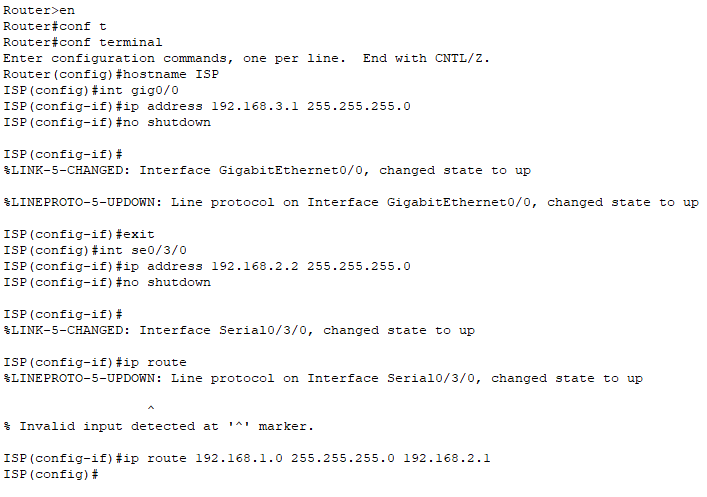
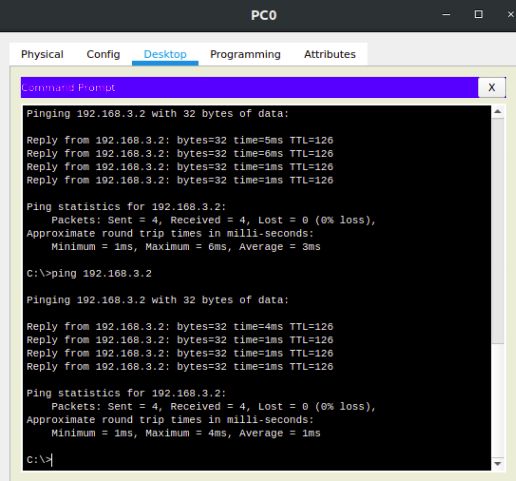
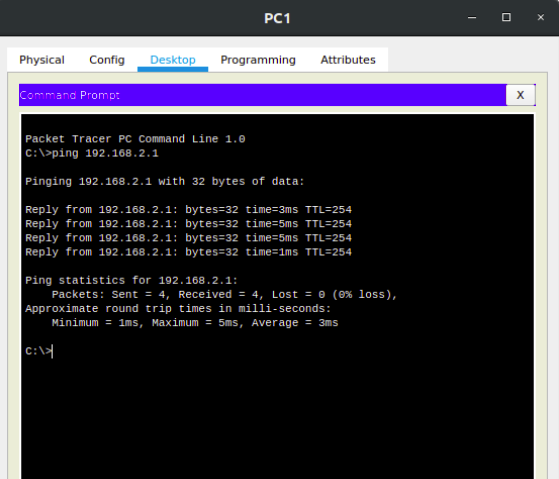


Fig No. 13.3: - Commands to ISP Router.

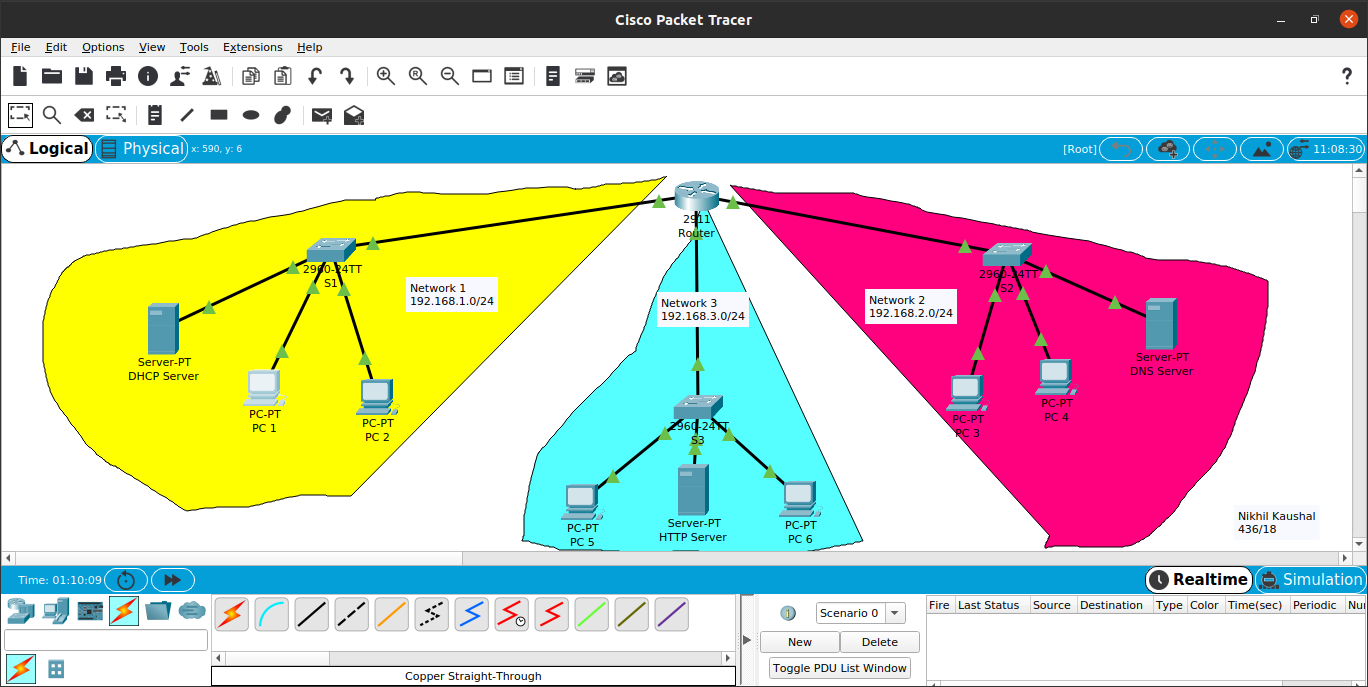
Fig No. 13.4: Ping Command (PC0→PC1)

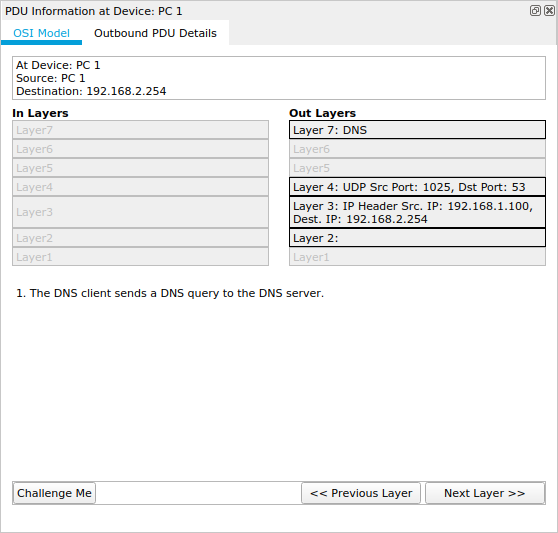
Fig No. 13.5: Ping Command (PC1→PC0)

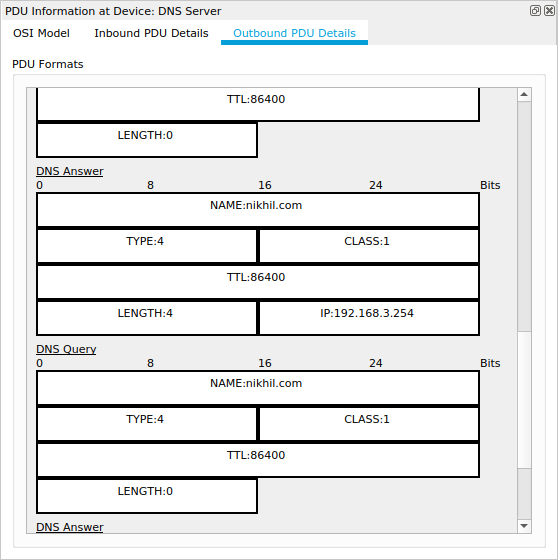
**Task 14:** **Simulation of UDP and TCP Protocols.**

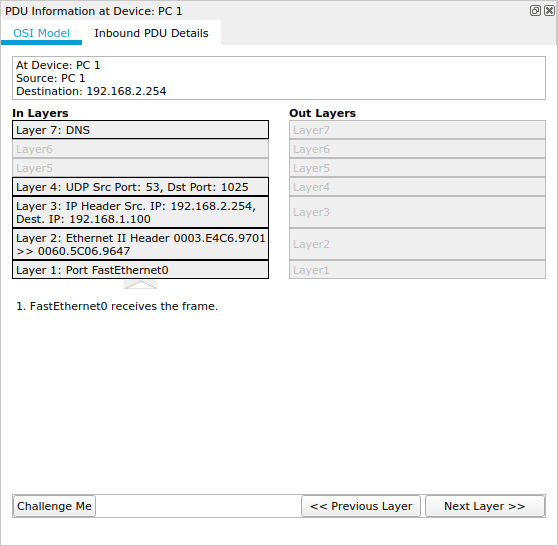
**Steps: -**

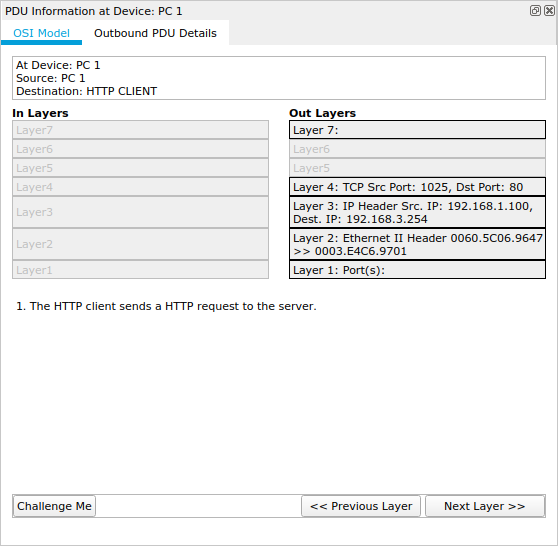
1. Use the topology with six PCs, two switches and three servers i.e. DHCP, DNS and HTTP Server.
2. Go to Simulation Mode and on any PC, go to web browser and type the website URL.
3. Go step-by-step in Simulation Mode and we can see that PC will send a DNS request to DNS Server.
4. Carefully observe the PDU information at each layer.
5. As the packet will reach at DNS Server, we can see that now it has DNS answer.
6. After the packet reaches the way back it came from, then check the PDU information and observe that it uses UDP.
7. Move to the next step, and now we can see that the HTTP works on TCP.
8. Continue to run the simulation and observe the PDU information carefully.

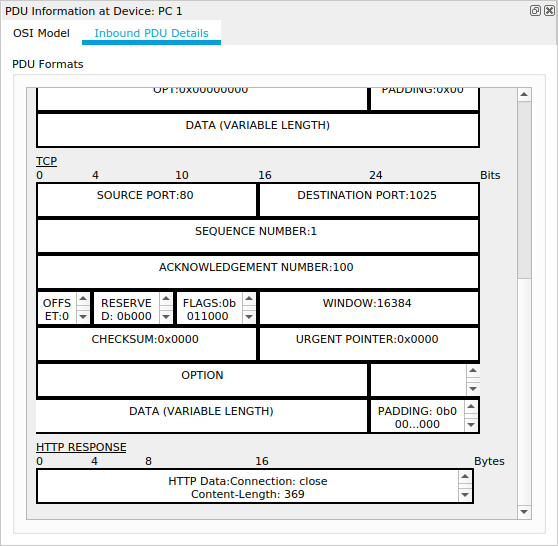
Fig No. 14.1: Topology with DHCP, HTTP and DNS Server.

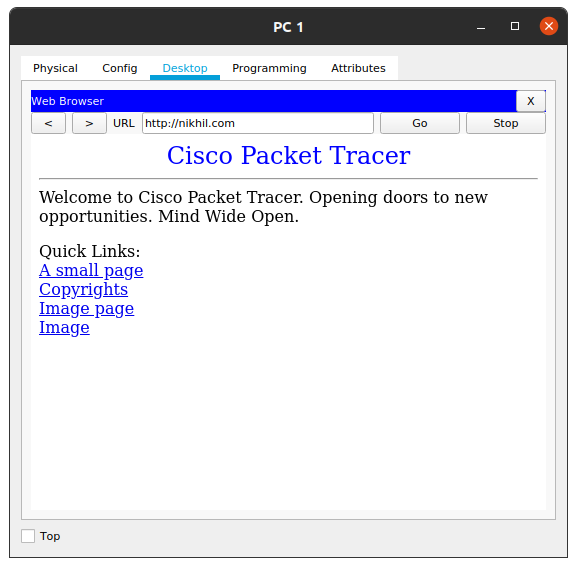
Fig No. 14.2: DNS client sending a DNS query to the DNS Server

Fig No. 14.3: DNS reply (DNS query and DNS answer)

Fig No. 14.4: Packet after reaching the DNS client PC

Fig No. 14.5: HTTP client sending a HTTP request to the server.

Fig No. 14.6: Packet after reaching HTTP client.

Fig No. 14.7: After successful response from HTTP Server.