KLE SOCIETY'S

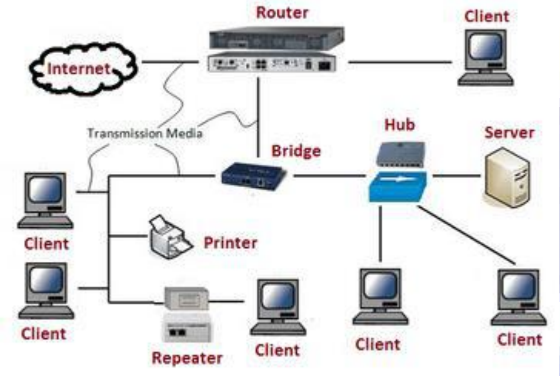
S. NIJALINGAPPA COLLEGE

RAJAJINAGAR, BANGALORE-560010

BACHELOR OF COMPUTER APPLICATION

III Semester

COMPUTER NETWORK LAB MANUAL



Under the guidance of:

PROF. VIJAYKUMAR A S (H.O.D OF COMPUTER SCIENCE DEPARTMENT)

&

PROF. ROOPA H R (ACADEMIC CO-ORDINATOR)

Prepared By

MRS. PRANATEERTHA J ARADHYA &

MS. TEJASWINI

Academic Year

2022-2023

LAB -1 EXECUTE THE FOLLOWING COMMANDS

arp , ipconfig, hostname, netdiag, netstart, nslookup, pathping, ping, route,tracert

AIM
To study the basic networking commands.

C:\>arp –a: ARP is short form of address resolution protocol, It will show the IP address of your computer along with the IP address and MAC address of your router.

C:\>hostname: This is the simplest of all TCP/IP commands. It simply displays the name of your computer.

C:\>ipconfig: The ipconfig command displays information about the host (the computer your sitting at)computer TCP/IP configuration.

C:\>ipconfig /all: This command displays detailed configuration information about your TCP/IP connection including Router, Gateway, DNS, DHCP, and type of Ethernet adapter in your system.

C:\>Ipconfig /renew: Using this command will renew all your IP addresses that you are currently (leasing) borrowing from the DHCP server. This command is a quick problem solver if you are having connection issues, but does not work if you have been configured with a static IP address.

C:\>Ipconifg /release: This command allows you to drop the IP lease from the DHCP server.

C:\>ipconfig /flushdns: This command is only needed if you're having trouble with your networks DNS configuration. The best time to use this command is after network configuration frustration sets in, and you really need the computer to reply with flushed.

C:\>nbtstat –a: This command helps solve problems with NetBIOS name resolution. (Nbt stands for NetBIOS over TCP/IP)

C:\>net diag: Netdiag is a network testing utility that performs a variety of network diagnostic tests, allowing you to pinpoint problems in your network. Netdiag isn't installed by default, but can be installed from the Windows XP CD after saying no to the install. Navigate to the CD ROM drive letter and open the support\tools folder on the XP CD and click the setup.exe icon in the support\tools folder.

C:\>netstat: Netstat displays a variety of statistics about a computers active TCP/IP connections. This tool is most useful when you're having trouble with TCP/IP applications such as HTTP, and FTP.

C:\>nslookup: Nslookup is used for diagnosing DNS problems. If you can access a resource by specifying an IP address but not it's DNS you have a DNS problem.

C:\>pathping: Pathping is unique to Window's, and is basically a combination of the Ping and Tracert commands. Pathping traces the route to the destination address then launches a 25 second test of each router along the way, gathering statistics on the rate of data loss along each hop.

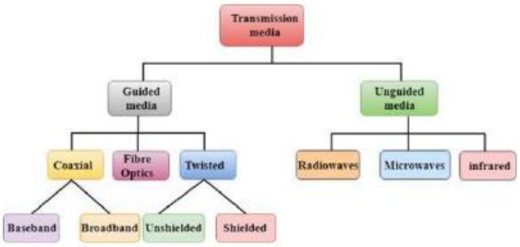
C:\>ping: Ping is the most basic TCP/IP command, and it's the same as placing a phone call to your best friend. You pick up your telephone and dial a number, expecting your best friend to reply with "Hello" on the other end. Computers make phone calls to each other over a network by using a Ping command. The Ping commands main purpose is to place a phone call to another computer on the network, and request an answer. Ping has 2 options it can use to place a phone call to another computer on the network. It can use the computers name or IP address.

C:\>route: The route command displays the computers routing table. A typical computer, with a single network interface, connected to a LAN, with a router is fairly simple and generally doesn't pose any network problems. But if you're having trouble accessing other computers on your network, you can use the route command to make sure the entries in the routing table are correct.

C:\>tracert: The tracert command displays a list of all the routers that a packet has to go through to get from the computer where tracert is run to any other computer on the internet.

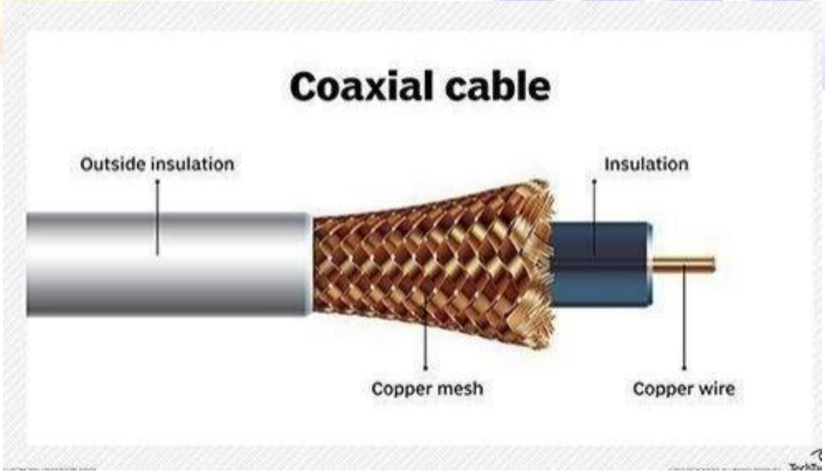
LAB- 2 STUDY OF DIFFERENT TYPES OF CABLES

Transmission Medium:
A communication channel that is used to carry the data from one transmitter to the receiver through the electromagnetic signals . The main function of this is to carry the data in the bits form through the Local Area Network(LAN).In data communication, it works like a physical path between the sender & receiver .For instance ,in a copper cable network the bits in the form of electrical signals whereas in a fiber network ,the bits are available in the form of light pulses. The quality as well as characteristics of data transmission , can be determined from the characteristics of medium &signal. The properties of different transmission media are delay, bandwidth, maintenance, cost and easy installation.



Bounded/Guided Transmission Media:
This kind of transmission media is also known as wired otherwise bounded media. In this type,the signals can be transmitted directly & restricted in a thin path through physical links. The types of Bounded /Guided transmission are discussed below.

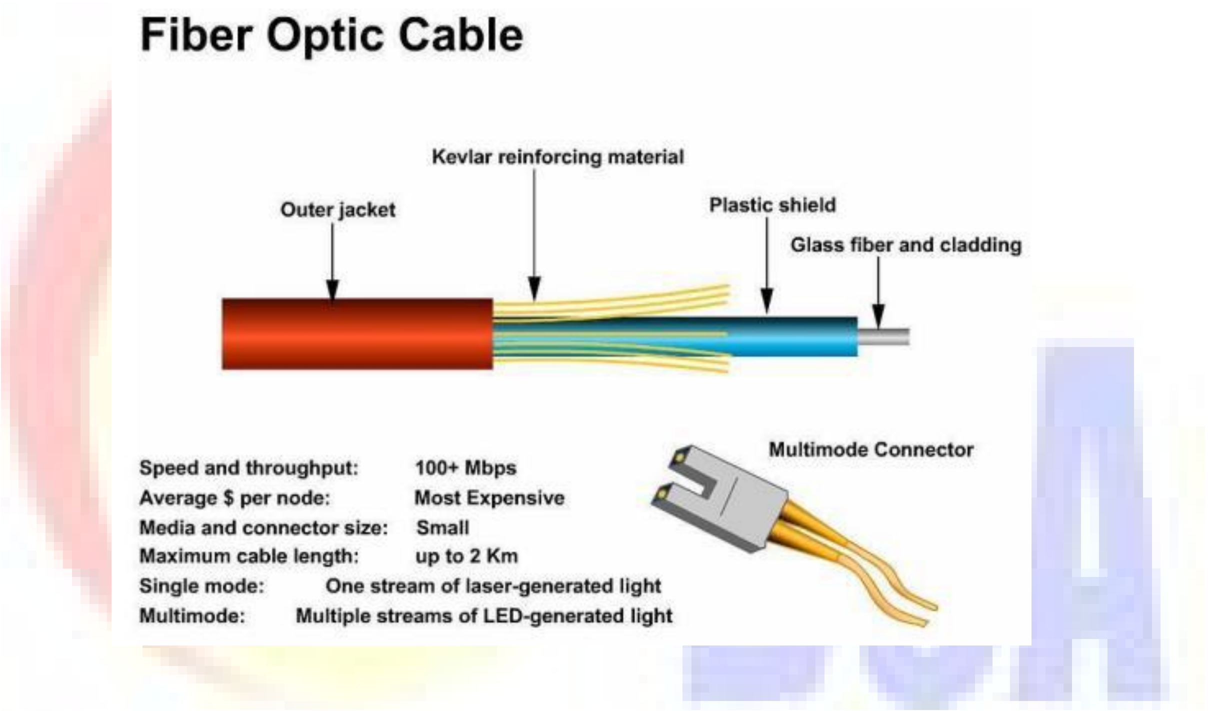
Coaxial Cable:
Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable. It has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer conductor is also enclosed in an insulating sheath, and the jwhole cable is protected by a plastic cover.



Applications:
1. Coaxial cable was widely used for both analog and digital data transmission.
2. It has higher bandwidth.
3.Inexpensive when compared to fiber optical cables.
4. It uses for longer distances at higher data rates.
5. Excellent noise immunity.
6. Used in LAN and Television distribution.

Disadvantage :
1.Single cable failure can fail the entire network.
2.Difficult to install and expensive when compared with twisted pairs.
3.If the shield is imperfect, it can lead to grounded loop.

Fibre Optic Cable:
A fiber optic cable is a network cable that contains strands of glass fibers inside an insulated casing. They're designed for long-distance, high-performance data networking, and telecommunications. Compared to wired cables, fiber optic cables provide higher bandwidth and transmit data over longer distances. Fiber optic cables support much of the world's internet, cable television, and telephone systems.



Speed and throughput:	100+ Mbps
Average $ per node:	Most Expensive
Media and connector size:	Small
Maximum cable length:	up to 2 Km
Single mode:	One stream of laser-generated light
Multimode:	Multiple streams of LED-generated light

Advantages of Fiber Optic Cables:
1.The loss of signal in optical fiber is less than that in copper wire.
2.Opticalfibers usually have a longer life cycle for over 100 years.
Disadvantage:
1.It is expensive.
2.Difficult to install.

Twisted pair cable:
A twisted pair cable is a type of cable made by putting two separate insulated wires together in a twisted pattern and running them parallel to each other. This type of cable is widely used in different kinds of data and voice infrastructures.

Twisted pair is of two types:
1.Shielded Twisted Pair(STP)
2.Unshielded Twisted Pair(UTP)

Shielded Twisted Pair:

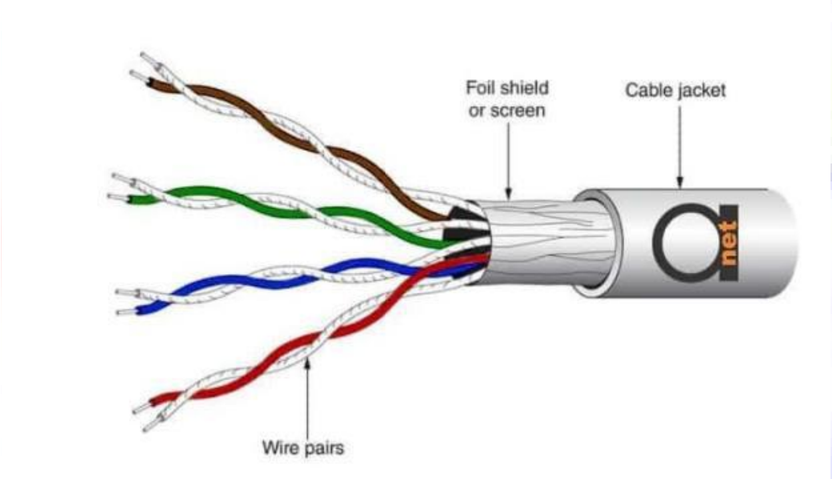
Shielded Twisted Pair (STP) cables additionally have an overall conducting metallic shields covering four twisted pair wires. There may be another conducting metallic shields covering individual twisted pairs also. These metallic shields blocks out electromagnetic interference to prevent unwanted noise from the communication circuit.

Advantage of Shielded Twisted Pair:

1.The cost of the shielded twisted pair cable is not very high and not very low.
2.An installation of STP is easy.
3.It has higher capacity as compared to unshielded twisted pair cable.
4.It has a higher attenuation.
5.It is shielded that provides the higher data transmission rate.

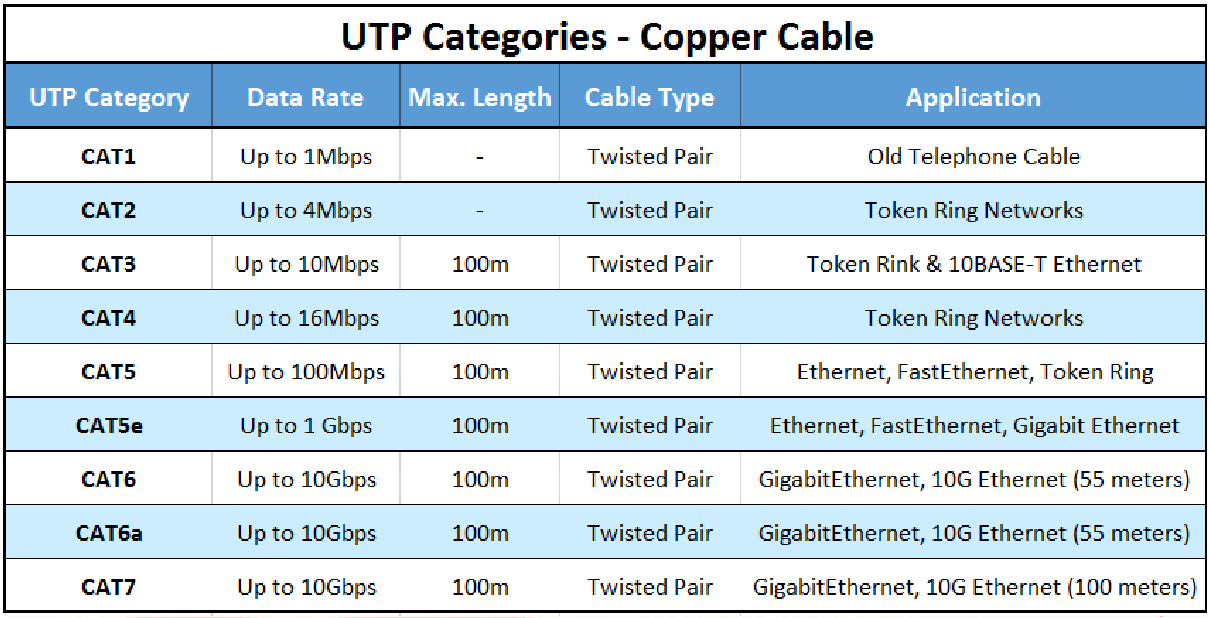
Disadvantages:

1.It is more expensive as compared to UTP and coaxial cable.
2.It has a higher attenuation rate.



Unshielded Twisted Pair(UTP):

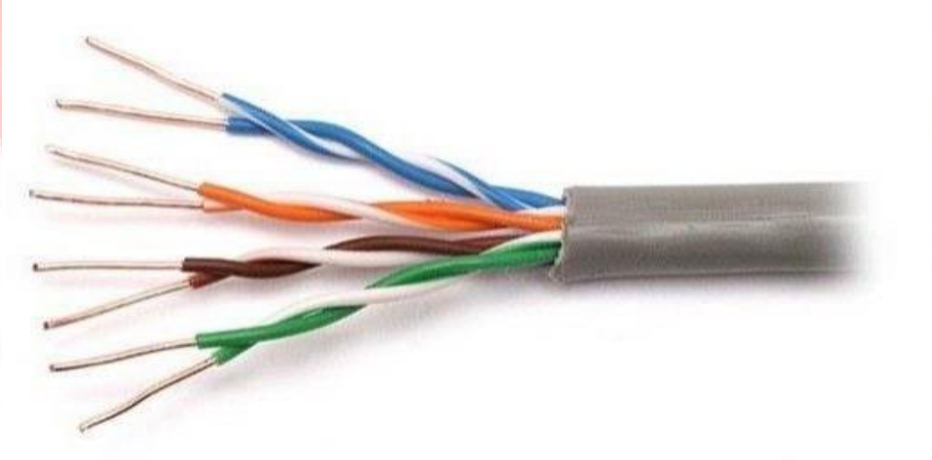
An unshielded twisted pair is widely used in telecommunication. It is most common type when compared with shielded twisted pair cable which consists of two conductors usually copper, each with its own colour plastic insulator



UTP Categories - Copper Cable

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

Advantages Of Unshielded Twisted Pair:
1.It is cheap.
2.Installation of the unshielded twisted pair is easy.
3.It can be used for high-speed LAN.
Disadvantage:
1.This cable can only be used for shorter distances because of attenuation.



Unbounded/Unguided Transmission Media:

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them

Types of unguided Transmission media:

- Radio Transmission:

Its frequency is between 10Khz to 1Ghz. It is simple to install and has high attenuation. These waves are used for multicast communication.

Types of propagation:
1. Troposphere
2. Ionosphere

Microwaves:
It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

Infrared:
Infrared waves are used for very short distance communication. They cannot penetrate through

obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

LAB- 3 PRACTICALLY IMPLEMENT THE CROSS – WIRED CABLE AND STRAIGHT WIRED CABLE USING CRIMPING TOOL

Aim: Study of different types of Network cables and Practically implement the cross-wired cable and straight through cable using clamping tool.

Requirements: Crimping tools, UTP Cable, RJ-45 connector, Cable tester.

Procedure:

Crimping Tools:

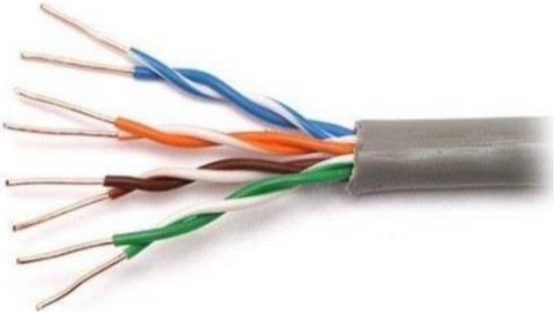
A crimping tool is a device used to conjoin two pieces of metal by deforming one or both of them to hold each other. The result of the tool's work is called a crimp. An example of crimping is affixing a connector to the end of a cable. For instance, network cables and phone cables are created using a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

RJ-11 (6-Pin) and RJ-45 (8-Pin) Crimping Tool

ComputerHope.com

UTP Cables:

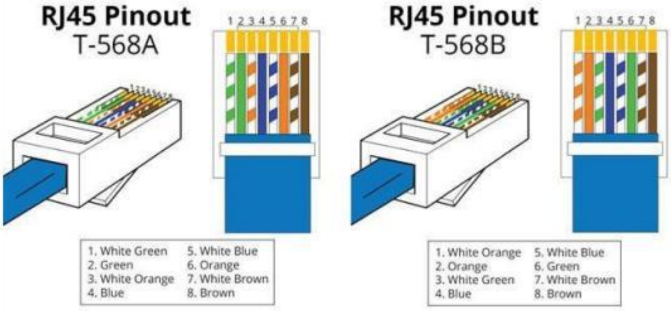
UTP stands for Unshielded Twisted Pair cable. UTP cable is a 100 ohm copper cable that consists of 2 to 1800 unshielded twisted pairs surrounded by an outer jacket. They have no metallic shield. This makes the cable small in diameter but unprotected against electrical interference. The twist helps to improve its immunity to electrical noise and EMI.



RJ-45 Connector:
RJ-45 connector is a tool that we put on the end of the UTP cable. With this we can plug the cable in the LAN port.

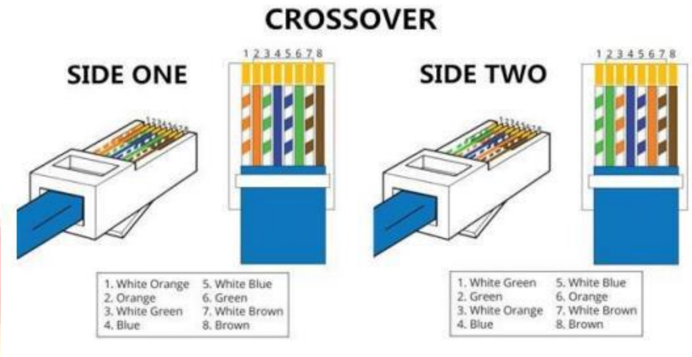
Cable test:
A cable tester is a electronic device used to verify the electrical connections in a signal cable or other wired assembly. Basic cable testers are continuity tester that verify the existence of a conductive path between ends of the cable, and verify the correct wiring of connectors on the cable

Straight cable:
A straight-through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal. On a straight-through cable, the wired pins match. Straightthrough cable use one wiring standard: both ends use T568A wiring standard or both ends use T568B wiring standard. The following figure shows a straight-through cable of which both ends are wired as the T568B standard.



Cross cable:

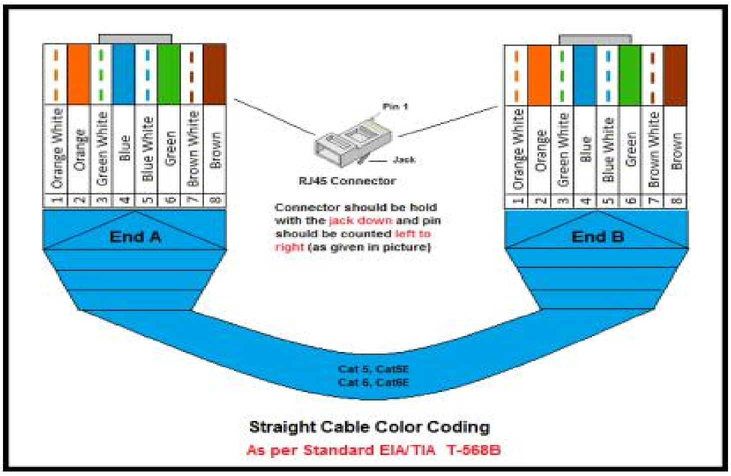
An Ethernet crossover cable is a type of Ethernet cable used to connect computing devices together directly. Unlike straight-through cable, crossover cables use two different wiring standards: one end uses the T568A wiring standard, and the other end uses the T568B wiring standard. The internal wiring of Ethernet crossover cables reverses the transmit and receive signals. It is most often used to connect two devices of the same type: e.g. two computers (via network interface controller) or two switches to each other.



Making Straight UTP Cable:

- Peel the end of the UTP cable , approximately 2 cm.
- Open the cable strands , align and follow the arrangement as standard cable image shown below .
- Once the order is according to the standard , cut and flatten the ends of the cable,
- Put the cable is straight and aligned into the RJ - 45 connector , and make sure all cables are in correct position as follows:

Orange White on no 1
Orange on no 2
Green White on no 3
Blue on no 4
Blue White on no 5
Green on no 6
White Brown on no 7
Brown on no 8



Straight Cable Color Coding
As per Standard EIA/TIA T-568B

- Make crimping using crimp tools , press crimping tool and make sure all the pins (brass) on the RJ - 45 connector has " bite " of each cable . usually when done will sound "click ".

Once finished at the end of this one , do it again at the other end cable.

The final step is to check the cable that you created earlier using the LAN tester , enter each end of the cable (RJ- 45) to each LAN port available on the tester , turn and make sure all of the LEDs light up according to the order of the wires we created.

Creating Cross UTP Cable:-

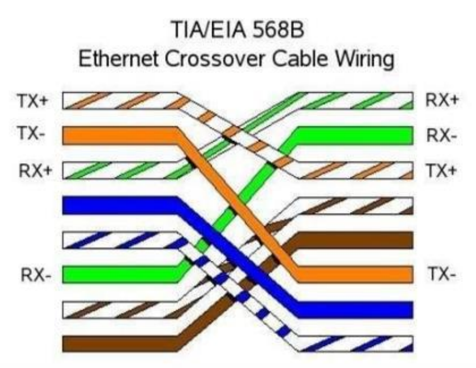
Creating a cross cable has almost the same steps with straight cable , the difference lies only in the colour sequence from both ends of the cable . Unlike the straight cable that has the same colour sequence at both ends of the cable , the cross cable has a different colour sequences at

both ends of the cable.

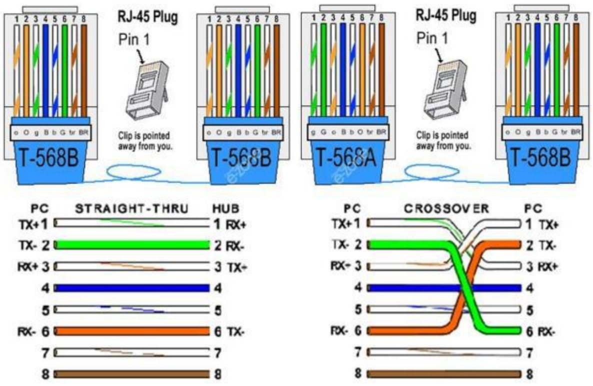
The first ends is same with straight cable :

Orange White on no. 1
Orange on no. 2
Green White on no. 3
Blue on no. 4
Blue White on no. 5
Green on no. 6 .
White chocolate on no. 7
Brown on no. 8

For the second end of the cable, the colour composition is different from the first . The colour arrangement is as follows



Green White on no. 1
Green on no. 2
Orange White on no. 3
Blue on no. 4
Blue White on no. 5
Orange on no. 6
White chocolate no.7
Brown on no.8



LAB - 4 STUDY THE NETWORK IP ADDRESS CONFIGURATION (CLASSIFICATION OF ADDRESS, STATIC AND DYNAMIC ADDRESS)

The IP address stands for Internet Protocol address is also called IP number or internet address. It helps us to specify the technical format of the addressing and packets scheme.
An IP address is a numerical label assigned to the devices connected to a computer network that uses the IP for communication. IP address act as an identifier for a specific machine on a particular network. It also helps us to develop a virtual connection between a source and a destination.

Types of IP address

There are mainly four types of IP addresses:

- Public
- Private
- Static
- Dynamic.

Public IP Addresses

A public IP address is an address where one primary address is associated with the whole network. In this type of IP address, each of the connected devices has the same IP address. This type of public IP address is provided by Internet Service Provider (ISP).

Private IP Addresses

A private IP address is a unique IP number assigned to every device that connects to internet network, which includes devices like computers, tablets, smartphones etc.,

Static IP addresses

A static IP address is an IP address that cannot be changed. These are fixed that are manually assigned to a system device. On the network configuration page, the network administrator manually inputs the IP address for every system. Moreover, the static address is not changed until it is directly updated by the *network administrator* or the *Internet Service Provider*. Furthermore, this address does not change with each network connection. In other words, the device always connects to the internet through the same IP address. The *dynamic IP address* is typically configured on devices via the *DHCP protocol* and regularly updates. The dynamic IP address constantly changes whenever the user links to a network. The Dynamic Host Configuration Protocol(DHCP) server employs a method for tracking and retrieving IP address information associated with active network components. The mechanism utilized for translation in dynamic address is known as *Domain Name Server (DNS)*.

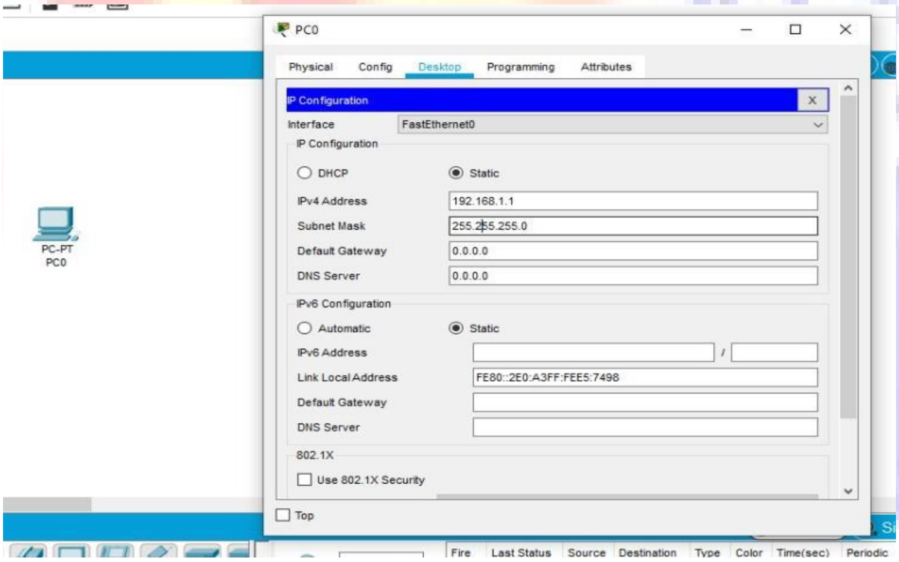
The DHCP and DNS are two protocols that are widely used while accessing the internet. When a user connects to the network, DHCP assigns her a temporary dynamic IP address.

The main differences between Static and Dynamic IP addresses are as follows:

Features	Static IP address	Dynamic IP address
Definition	It is a permanent numeric address that is manually issued to a network device.	It is a temporary IP address allocated to a system when it connects to a network.
Provider	It is provided by Internet Service Provider (ISP).	It is provided by DHCP (Dynamic Host Configuration Protocol).

Changes	It doesn't change with time.	It may be changed at any time.
Device tracking	Devices may be traced easily.	Devices may be difficult to trace.
Cost	It is expensive to utilize and maintain.	It is less expensive to utilize and maintain.
Security	It is less secure than the dynamic IP address.	It offers high security.
Designation	It is complex to assign and reassign.	It is much easy to assign and reassign.
Stability	It is highly stable.	It is less stable.
Usage	These are appropriate for dedicated services like FTP, mail, and VPN servers.	Dynamic IP addresses are appropriate for a large network that needs an internet connection for all devices.

Image for Configuring Static IP Address



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2E0:A3FF:FEE5:7498

Default Gateway:

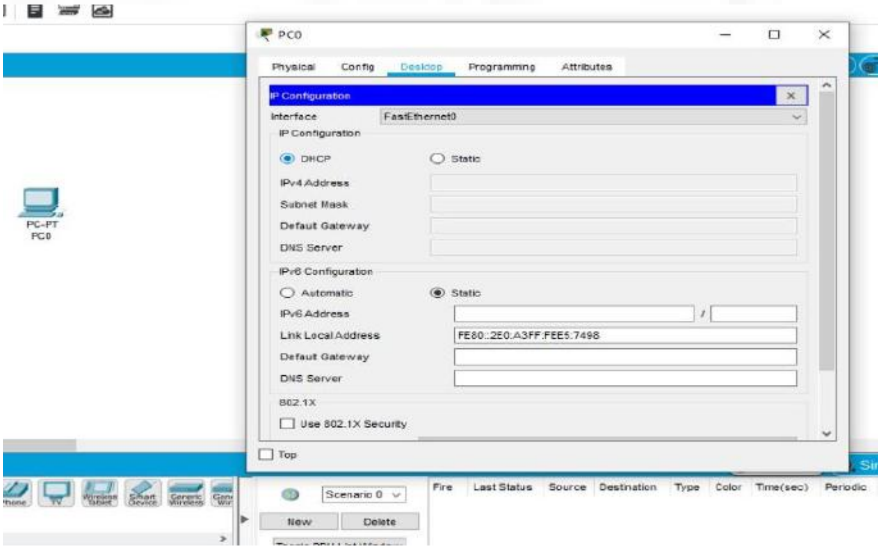
DNS Server:

802.1X

□ Use 802.1X Security

□ Top

Image for Configuring Dynamic IP Address



IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address:

Subnet Mask:

Default Gateway:

DNS Server:

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2E0:A3FF:FEE5:7498

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

□ Top

LAB - 5 STUDY THE NETWORK IP ADDRESS CONFIGURATION (CLASSIFICATION IPV4 AND IPV6, SUBNET, SUPERNET)

The Internet Protocol version 4 (IPv4) is a protocol for use on packet-switched Link Layer networks (e.g. Ethernet). IPv4 provides an addressing capability of approximately 4.3 billion addresses. The Internet Protocol version 6 (IPv6) is more advanced and has better features compared to IPv4.

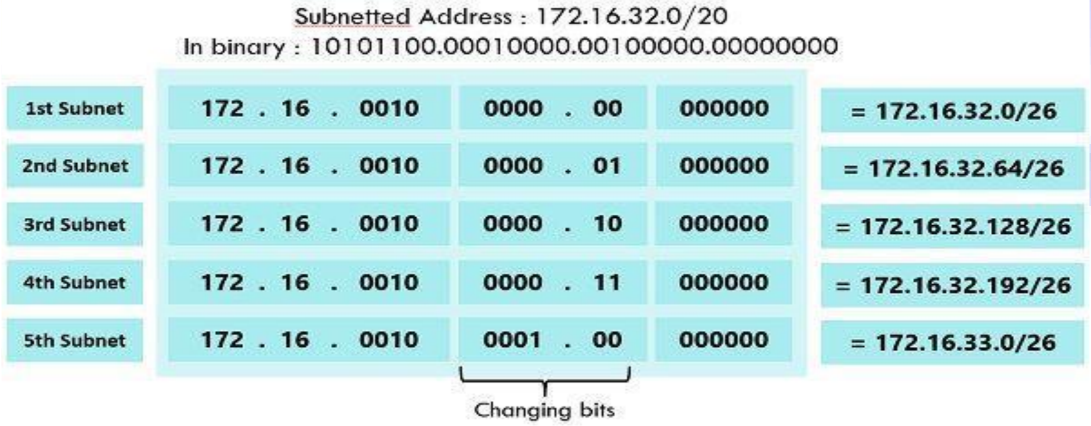
Features	IPv4	IPv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes.	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.

Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.

Subnetting is a technique of partitioning an individual physical network into several small-sized logical sub-networks. These subnetworks are known as ***subnets***. An IP address is made up of the combination of the network segment and a host segment. A subnet is constructed by accepting the bits from the IP address host portion which are then used to assign a number of small-sized sub-networks in the original network.

The Subnetting basically convert the host bits into the network bits. As mentioned above the subnetting strategy was initially devised for slowing down the depletion of the IP addresses.

The subnetting permits the administrator to partition a single class A, class B, class C network into smaller parts. **VLSM (Variable Length Subnet Mask)** is a technique which partitions IP address space into subnets of different sizes and prevent memory wastage. Furthermore, when the number of hosts is same in subnets, that is known as **FLSM (Fixed Length Subnet Mask)**.

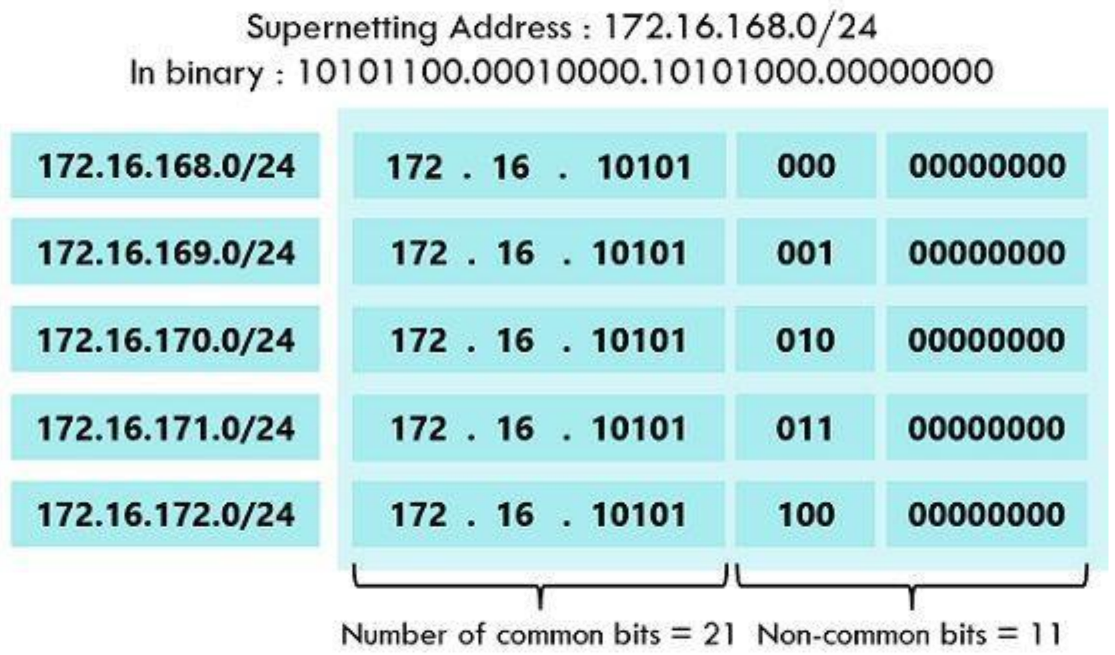


Subnetted Address : 172.16.32.0/20
In binary : 10101100.00010000.00100000.00000000

1st Subnet	172 . 16 . 0010	0000 . 00	000000	= 172.16.32.0/26
2nd Subnet	172 . 16 . 0010	0000 . 01	000000	= 172.16.32.64/26
3rd Subnet	172 . 16 . 0010	0000 . 10	000000	= 172.16.32.128/26
4th Subnet	172 . 16 . 0010	0000 . 11	000000	= 172.16.32.192/26
5th Subnet	172 . 16 . 0010	0001 . 00	000000	= 172.16.33.0/26

Supernetting is inverse process of subnetting, in which several networks are merged into a single network. While performing supernetting, the mask bits are moved toward the left of the default mask. The supernetting is also known as **router summarization** and **aggregation**. It results in the creation of more host addresses at the expense of network addresses, where basically the network bits are converted into host bits.

The supernetting is performed by internet service provider rather than the normal users, to achieve the most efficient IP address allocation. **CIDR (Classless Inter-Domain Routing)** is scheme used to route the network traffic across the internet. CIDR is a supernetting technique where the several subnets are combined together for the network routing. In simpler words, CIDR allows the IP addresses to be organized in the subnetworks independent of the value of the addresses.



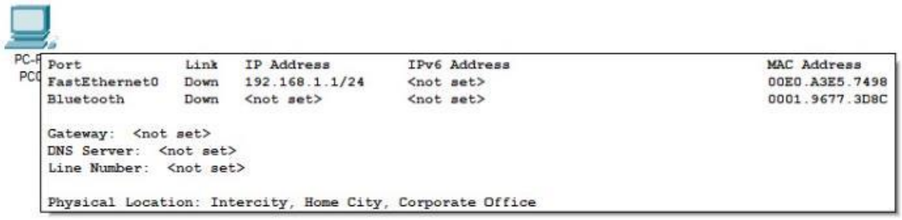
Supernetting Address : 172.16.168.0/24

In binary : 10101100.00010000.10101000.00000000

172.16.168.0/24	172 . 16 . 10101	000	00000000
172.16.169.0/24	172 . 16 . 10101	001	00000000
172.16.170.0/24	172 . 16 . 10101	010	00000000
172.16.171.0/24	172 . 16 . 10101	011	00000000
172.16.172.0/24	172 . 16 . 10101	100	00000000

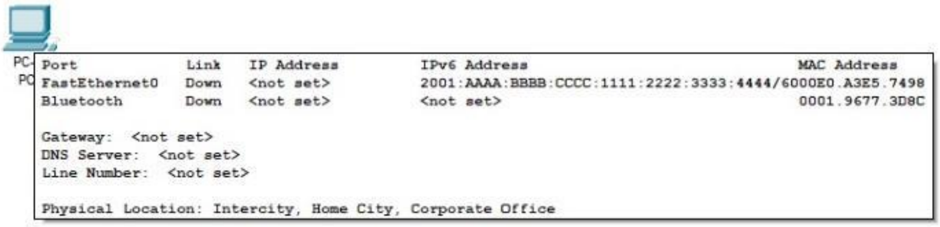
Number of common bits = 21 Non-common bits = 11

IPV4



```
Port           Link   IP Address       IPv6 Address                        MAC Address
FastEthernet0  Down   192.168.1.1/24   <not set>                           00E0.A3E5.7498
Bluetooth      Down   <not set>        <not set>                           0001.9677.3D8C

Gateway:  <not set>
DNS Server:  <not set>
Line Number:  <not set>

Physical Location: Intercity, Home City, Corporate Office
```

IPV6



```
Port           Link   IP Address     IPv6 Address                                  MAC Address
FastEthernet0  Down   <not set>      2001:AAAA:BBBB:CCCC:1111:2222:3333:4444/6000E0.A3E5.7498
Bluetooth      Down   <not set>      <not set>                                     0001.9677.3D8C

Gateway:  <not set>
DNS Server:  <not set>
Line Number:  <not set>

Physical Location: Intercity, Home City, Corporate Office
```

LAB - 6 STUDY OF NETWORK DEVICES (SWITCH, ROUTER BRIDGE)

Aim: Study of following Network Devices in Detail

- Switch
- Bridge
- Router

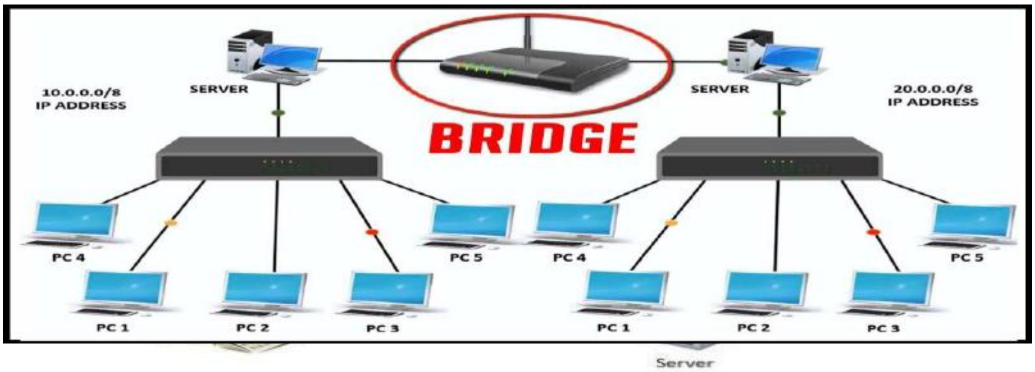
Apparatus (Software): No software or hardware needed.

Procedure: Following should be done to understand this practical.

1. Switch: A network switch or switching hub is a computer networking device that connects network segments. The term commonly refers to a network bridge that processes and routes data at the data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches.

Switch:- A switch is a Networking device in a computer network that connects other devices together. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches manage the flow of data across a network by transmitting a received network packet only to the one or more devices for which the packet is intended

Working of Switch:-Whenever a host sends a frame to any other host, then the source host is stored with the port in the address table of the MAC address switch. A switch always stores the address of the source in the table. Unless a host does send some data, its MAC address and port number will not be stored in the table of the switch. Unless a host does send some data, its MAC address and port number will not be stored in the table of the switch. When you initialize the switch, the switch does not contain any information about any host and its address. In such a situation, when a host frame sends, its MAC address is stored in the table but due to no destination information, the switch sends the frame to all the hosts .When you initialize the switch, the switch does not contain any information about any host and its address. In such a situation, when a host frame sends, its MAC address is stored in the table but due to no destination information, the switch sends the frame to all the hosts. As soon as the second host sends some data, its address also gets stored in the table. As soon as the second host sends some data, its address also gets stored in the table. Whenever a host sends the frames, the switch stores it if its address is not already present in the table. Thus a switch creates its table. When all the hosts' addresses and port numbers come in the switch, the switch delivers the frame to all hosts only, delivering the same host to the host for which the data has been sent.



2. Bridge: A network bridge connects multiple network segments at the data link layer (Layer 2) of the OSI model. In Ethernet networks, the term bridge formally means a device that behaves according to the IEEE 802.1D standard. A bridge and switch are very much alike; a switch being a bridge with numerous ports. Switch or Layer 2 switch is often used interchangeably with bridge. Bridges can analyze incoming data packets to determine if the bridge is able to send the given packet to another segment of the network.

Bridge:-

Bridge is termed as a network device which is helpful in filtering the data load of the traffic by dividing it into segments or packets. They are used to lower the load of traffic on the LAN and other networks. Bridges are passive devices, because there is no interaction between bridged and the paths of bridging. Bridges operate on the second layer of the OSI model that is the data link layer.

Working of Bridge:-

When various network segments are established at the data link layer of the OSI model, we refer to it as bridge. However when the packets of data are transferred along a network , without locating the network addresses this process is termed as bridging. The process of bridging is helpful in locating the addresses of unknown addresses to which it is viable to send data. In bridging the data packets contain a header or a packet header which holds the address to the intended device. Bridge can remember and recall the address of the devices for further transmission. There are two kinds of bridging modes, the transparent bridging and the source routing bridging. When the process of bridging occurs, it makes a bridging table along side where it stores the MAC addresses of the various terminals. This table helps the bridges to send the data packet to the exact location next time. However when a specific address does not meet the contents of the bridging table, the data packet is forwarded further ahead to every attached terminal in LAN except from the computer it is connected to. This type of bridging is called transparent bridging. When the source computer presents pathway information within the packet, this type of bridging is known as source route bridging. It is most commonly used in used on Token Ring networks.

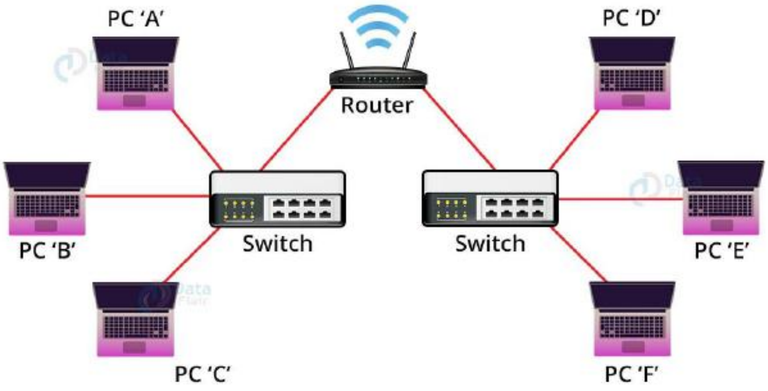
3. Router: A router is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another. Where multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks.

Router:-

Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analyzing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

How a router works:-

A router examines a packet header's destination IP address and compares it against a routing table to determine the packet's best next hop. Routing tables list directions for forwarding data to particular network destinations, sometimes in the context of other variables, like cost. They amount to an algorithmic set of rules that calculate the best way to transmit traffic toward any given IP address. A routing table often specifies a default route, which the router uses whenever it fails to find a better forwarding option for a given packet. For example, the typical home office router directs all outbound traffic along a single default route to its internet service provider (ISP) Routing tables can be static -- i.e., manually configured -- or dynamic. Dynamic routers automatically updated their routing tables based on network activity, exchanging information with other devices via routing protocols.



LAB - 7 CONFIGURE AND CONNECT THE COMPUTER IN LAN

Step -1 Select the 05 - PCs, 01- Printer, 01- Router, 01- Switch and 01-Server

By using Drag and Drop

Step -2 Configure IP address to Router as 192.168.1.100

Double Click on Router and

Select port status check box on . (for which Ethernet switch connected)

Step -3 Configure Server IP address 192.168.1.101 and connect to switch by Straight Through cable.

Click on Server, Select Desktop, Select IP Configuration

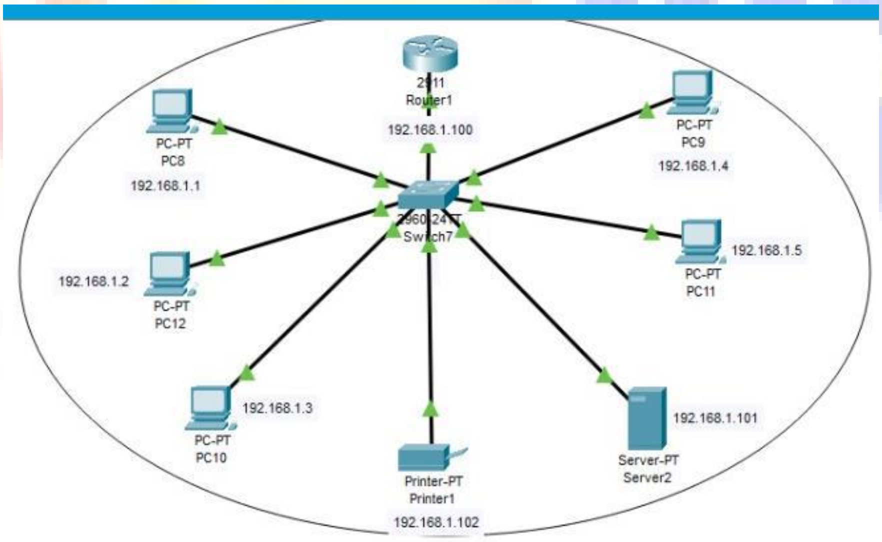
Step -4 Connect all 05 PCs to switch using Straight Through cable and configure IP address as 192.168.1.1 to 192.168.1.5

Step -5 Give gateway IP as 192.168.1.100 and DNS IP 192.168.1.101 for all 05 PCs

Click on PC, Click on Desktop, Click on IP configuration

Step -6 Configure Printer IP 192.168.1.102 and connect to switch using Straight Through cable.

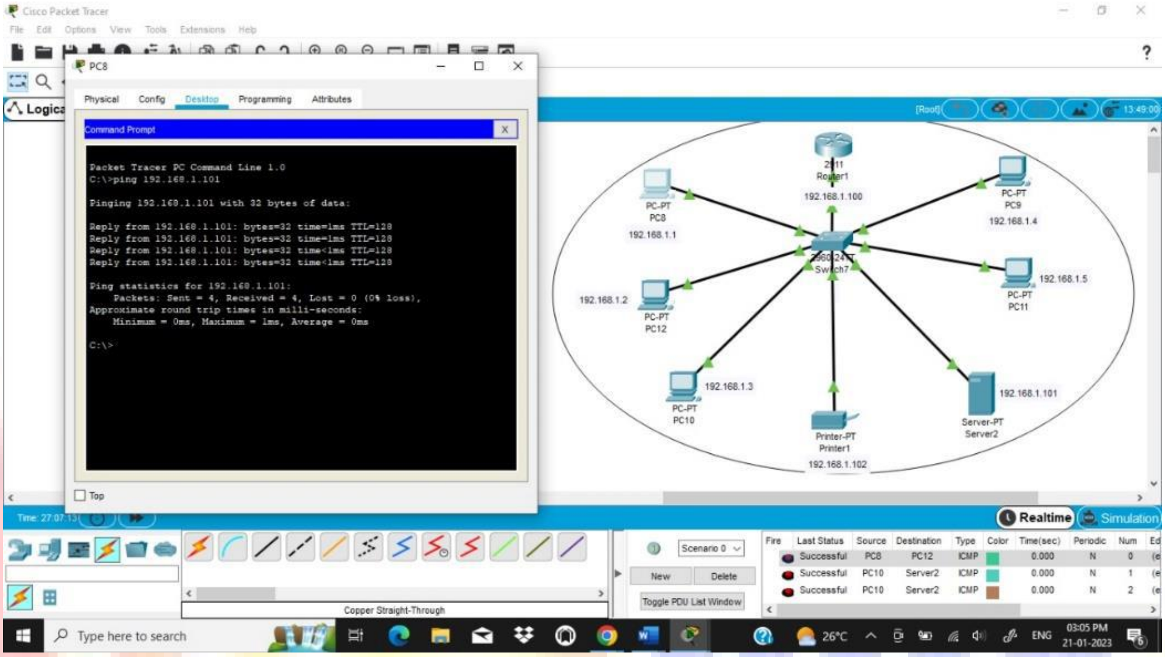
Click on Printer



Step -7 Ping all PCs from Server and Printer

Click in any one PC, Click on Desktop, Click on Command Prompt and ping any pc from this PC

By giving command - > ping IP address(ex 192.168.1.1)



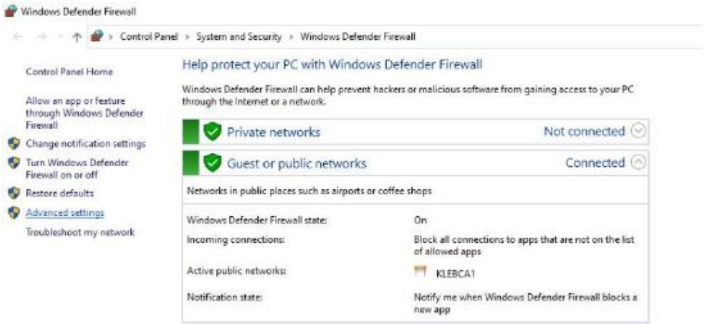
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.101

Pinging 192.168.1.101 with 32 bytes of data:

Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Ed
●	Successful	PC8	PC12	ICMP	🟩	0.000	N	0	(e
●	Successful	PC10	Server2	ICMP	🟩	0.000	N	1	(e
●	Successful	PC10	Server2	ICMP	🟫	0.000	N	2	(e

LAB - 8 BLOCK THE WEBSITE USING “WINDOWS DEFENDER FIREWALL” IN WINDOWS 10

Step 1: Launch the Control Panel on your computer.

Step 2: Select “Windows Defender Firewall” followed by “Advanced Settings” on the left-side pane.


Windows Defender Firewall
Control Panel › System and Security › Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Defender Firewall

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

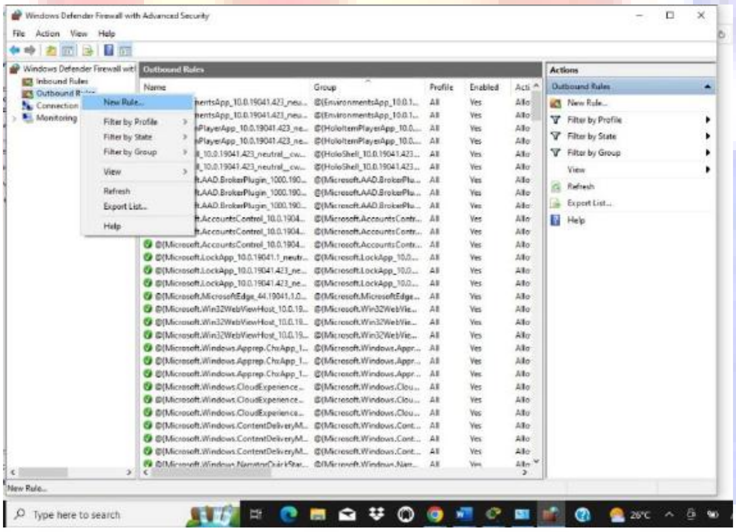
Private networks — Not connected

Guest or public networks — Connected

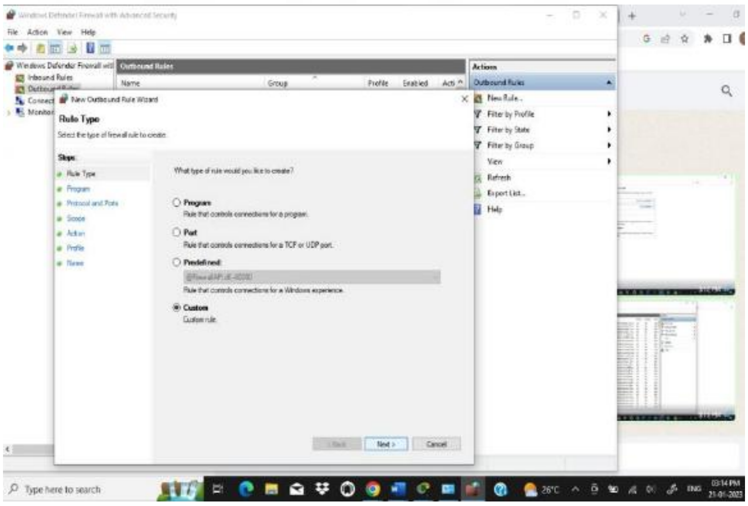
Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	KLEBCA1
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Step 3: Right-click on “Outbound Rules” from the menu on the left and select “New Rule.”



Step 4: When a new window pops up, select the “Custom” option followed by “Next.”



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

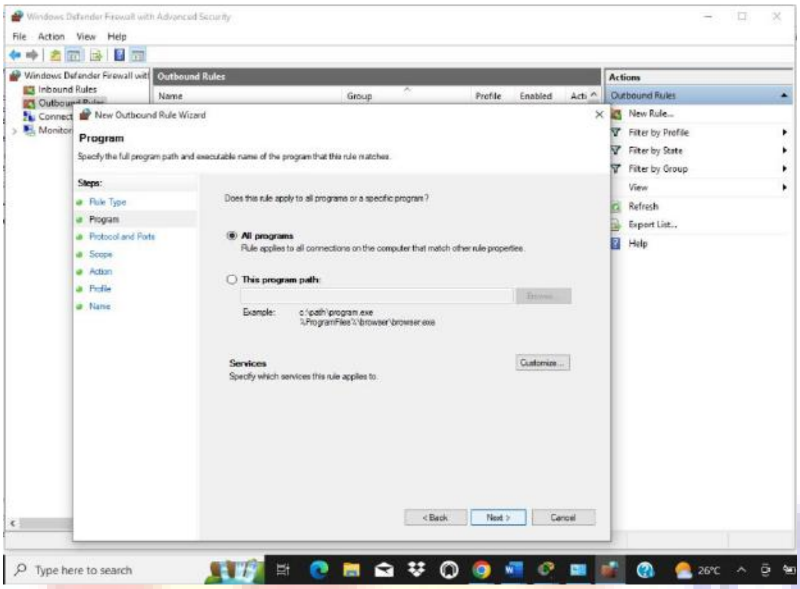
○ Program
Rule that controls connections for a program.

○ Port
Rule that controls connections for a TCP or UDP port.

○ Predefined:
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.

● Custom
Custom rule.

Step 5: On the next window, select “All programs” and again select “Next.”



New Outbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Does this rule apply to all programs or a specific program?

● **All programs**
Rule applies to all connections on the computer that match other rule properties.

○ **This program path:**

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

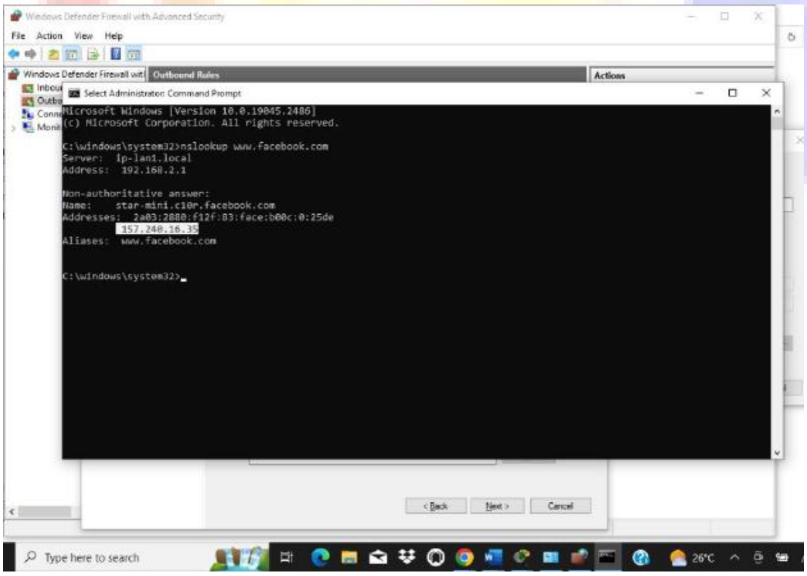
Services
Specify which services this rule applies to.

Step 6: Select the ” These IP addresses ” option under “Which remote IP addresses does this rule apply to?” and

click next

Step 7: Open the Command Prompt as Administrator by entering “CMD” into the search box.

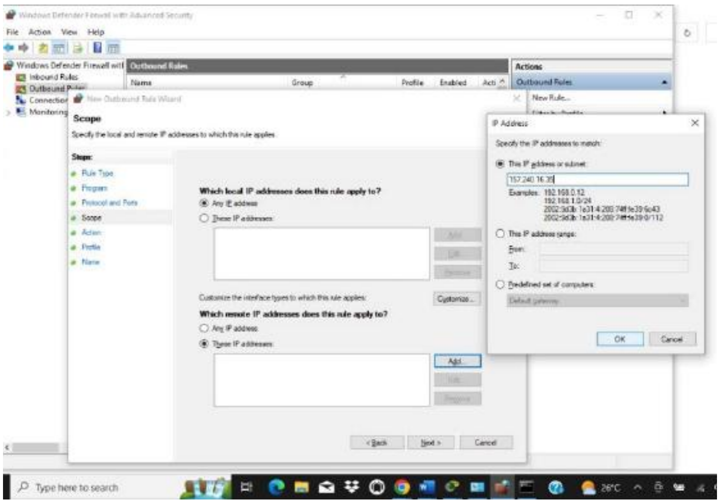
Step 8 : Enter “`nslookup` www.facebook.com” and press the Enter button.



Select Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.19045.2486]
(c) Microsoft Corporation. All rights reserved.

C:\windows\system32>nslookup www.facebook.com
Server:  lp-lan1.local
Address:  192.168.2.1

Non-authoritative answer:
Name:    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f12f:83:face:b00c:0:25de
          157.240.16.35
Aliases:  www.facebook.com


C:\windows\system32>_
```

Step 9: Click on “Add” and enter the IP addresses you want to block. Then select “Next.”



Scope

Specify the local and remote IP addresses to which this rule applies.

Which local IP addresses does this rule apply to?

● Any IP address

○ These IP addresses:

Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

○ Any IP address

● These IP addresses:

IP Address

Specify the IP addresses to match:

● This IP address or subnet:

157.240.16.35

Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

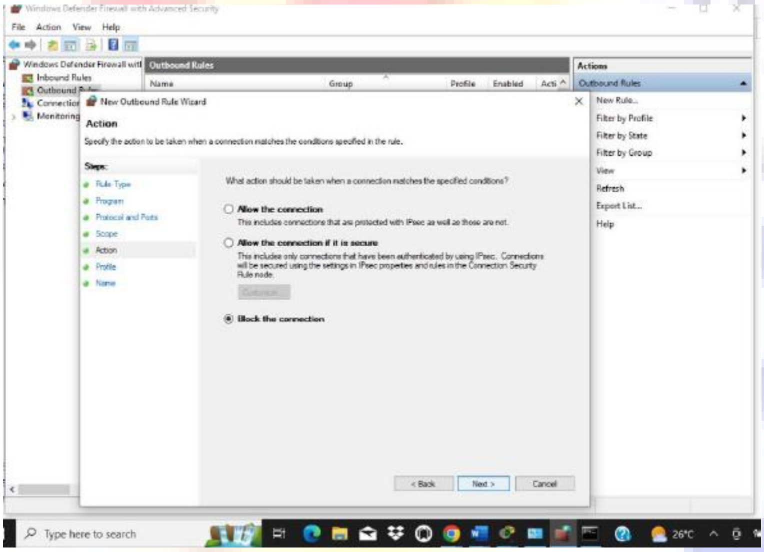
○ This IP address range:

From:

To:

○ Predefined set of computers:

Step 10 : Make sure to choose the “Block the connection” option and click on “Next.”



Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

○ Allow the connection

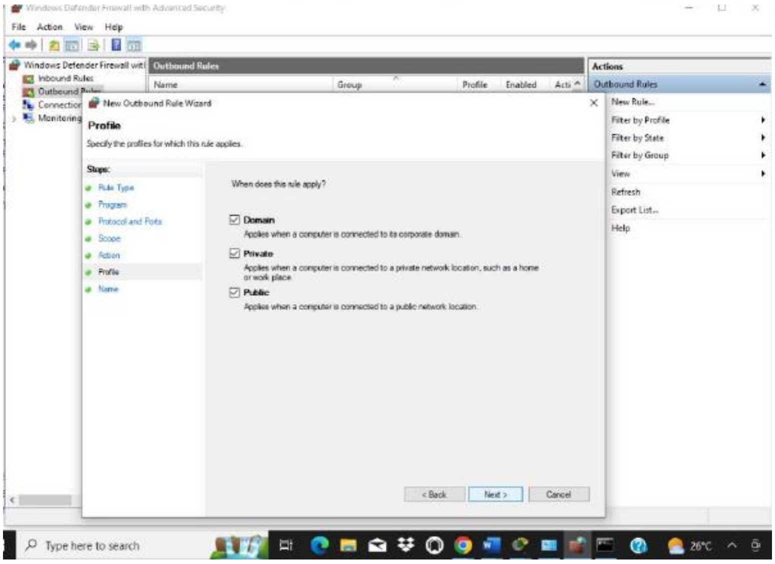
This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● Block the connection

Step 9: Choose whether the rule applies to Domain, Private, or Public. You can also select all three.



Profile

Specify the profiles for which this rule applies.

When does this rule apply?

☑ Domain

Applies when a computer is connected to its corporate domain.

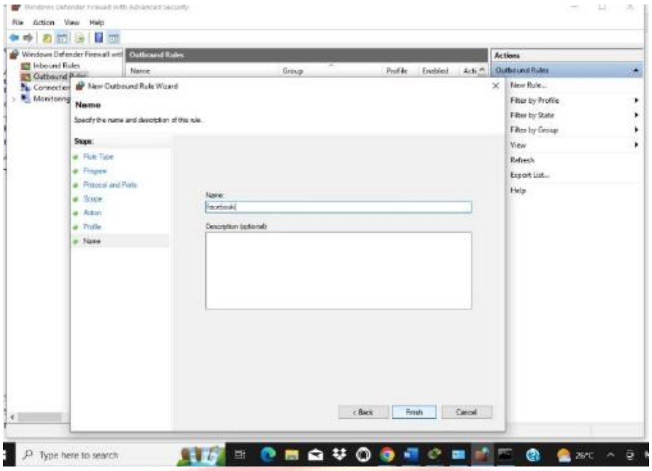
☑ Private

Applies when a computer is connected to a private network location, such as a home or work place.

☑ Public

Applies when a computer is connected to a public network location.

Step 10 : Select “Next,” add a name or description for this rule, and select “Finish” to complete the action.



New Outbound Rule Wizard

Name

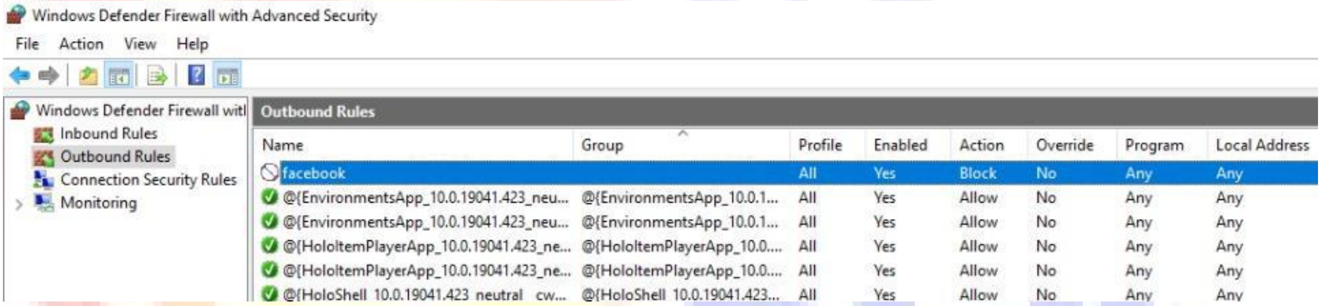
Specify the name and description of this rule.

Name: facebook

Description (optional):

Step 11: Finish

Check for Blocked website



Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

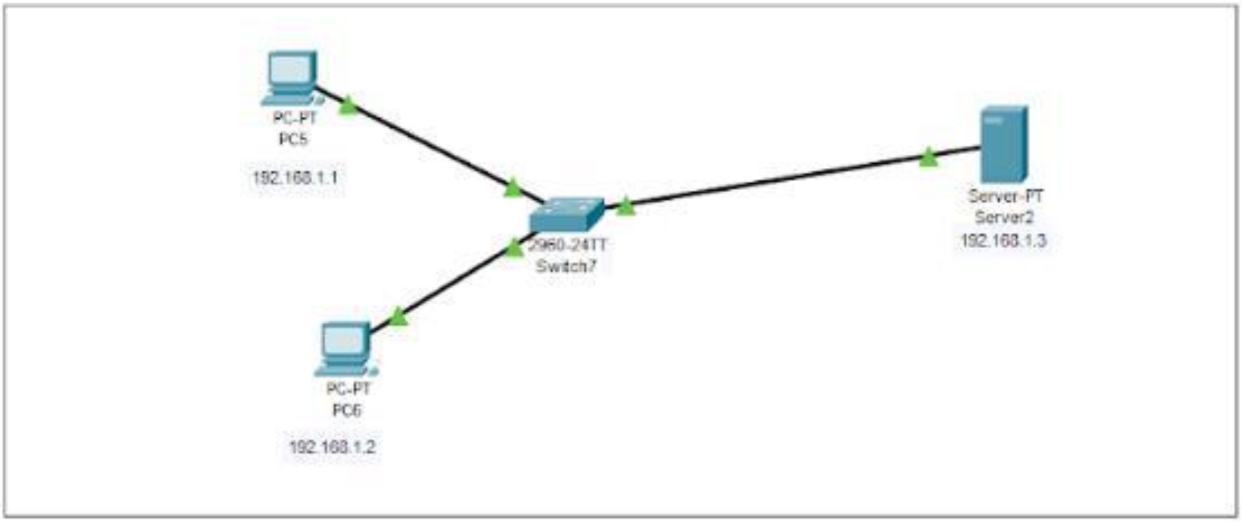
Outbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address
facebook		All	Yes	Block	No	Any	Any
@{EnvironmentsApp_10.0.19041.423_neu...	@{EnvironmentsApp_10.0.1...	All	Yes	Allow	No	Any	Any
@{EnvironmentsApp_10.0.19041.423_neu...	@{EnvironmentsApp_10.0.1...	All	Yes	Allow	No	Any	Any
@{HoloItemPlayerApp_10.0.19041.423_ne...	@{HoloItemPlayerApp_10.0....	All	Yes	Allow	No	Any	Any
@{HoloItemPlayerApp_10.0.19041.423_ne...	@{HoloItemPlayerApp_10.0....	All	Yes	Allow	No	Any	Any
@{HoloShell_10.0.19041.423_neutral__cw...	@{HoloShell_10.0.19041.423...	All	Yes	Allow	No	Any	Any

.

LAB - 9 SHARE THE FOLDER IN A SYSTEM AND ACCESS THE FILES OF THAT FOLDER FROM OTHER SYSTEM USING IP ADDRESS

Step -1 Create Lan Server Configuration (2- PC's, 1- Server, 1- Switch)



Step -2 IP Address Configuration for Server and PC's

Step -3 For both PC give the DNS server IP

Step -4 Click on Server
Click on Services
Click on FTP
Give the User name and Password (username is – admin, password – admin)
Give the permission for admin (Write, Read, Delete, Rename, List)
Next Click on add

Step -5 From PC1 Create text file (double click on PC)
Click on Desktop
Click on Text Editor
Click on File > New

Type text (Share the file in a system and access the files from other system or server using IP address)

Click on Save (Give file name as test1.txt)

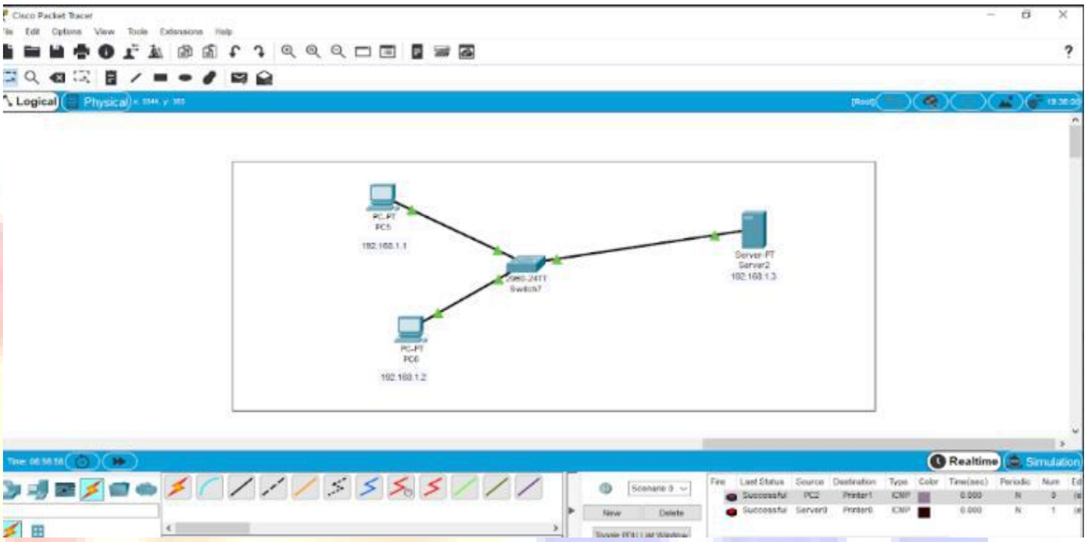
Step -6 In the same PC click on command prompt
Check the file by entering

```
C: \> dir
C:\> ftp 192.168.1.1 ( Enter the IP address of Server to connect Server )
Give Username and Password
ftp> put test1.txt (File transferred from PC1 to Server)
ftp> dir (Check the file is transferred to server by giving dir command)
        test1.txt
```

Step -7 Select PC2

Click on Desktop
Click on Command Prompt

```
C:\> dir
        test.txtsuch file will be there in PC2
C:\> ftp 192.168.1.1 ( Enter the IP address of Server to connect Server )
Give Username and Password
ftp> get test1.txt (File transferred from Server to PC2)
ftp> dir (Check the file is transferred to PC2)
      test1.txt
```



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Ed
●	Successful	PC2	Printer1	ICMP	■	0.000	N	0	
●	Successful	Server0	Printer0	ICMP	■	0.000	N	1	

LAB -10 SHARE THE PRINTER IN A NETWORK , AND TAKE A PRINT FROM OTHER PC

Step -1 Select the 02 - PCs, 01- Printer and 01 -Switch

By using Drag and Drop

Step -2 Configure IP address to Printer as 192.168.1.3

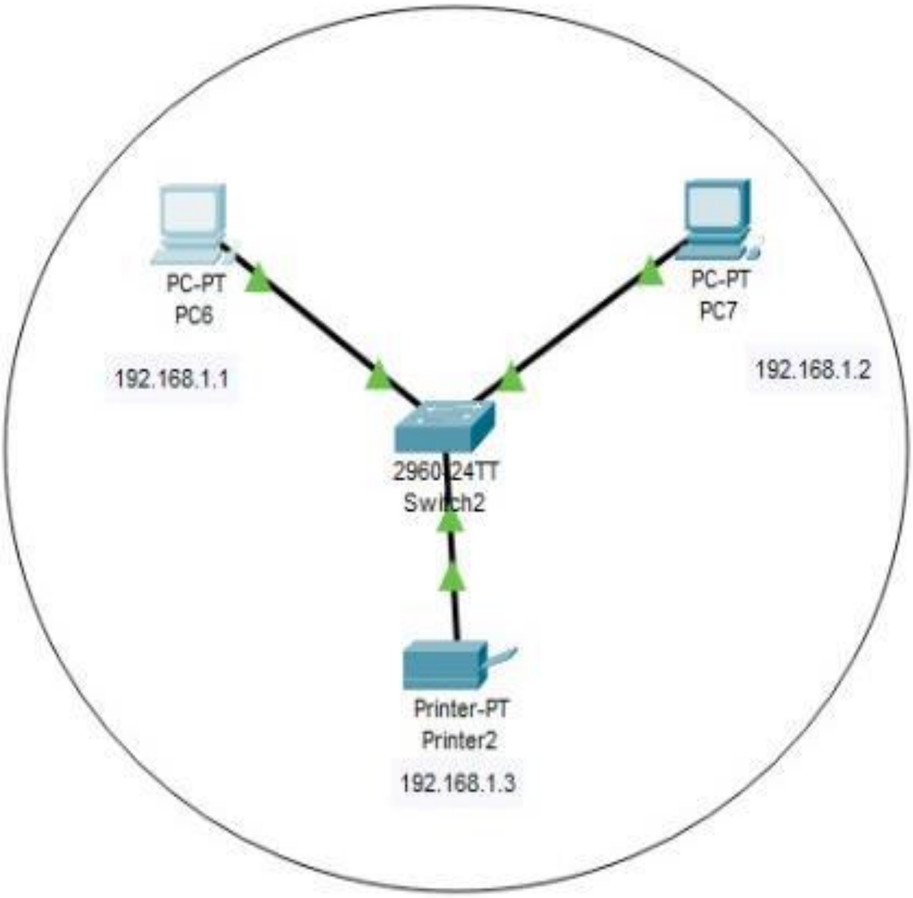
Double click on printer, Click on Config, Select FastEthernet0, Give IPV4 address. And connect to switch using Straight Through cable.

Step -4 Connect all 02 PCs to switch using Straight Through cable and configure IP address as

192.168.1.1 and192.168.1.2

Click on PC, Click on Desktop, Click on IP configuration

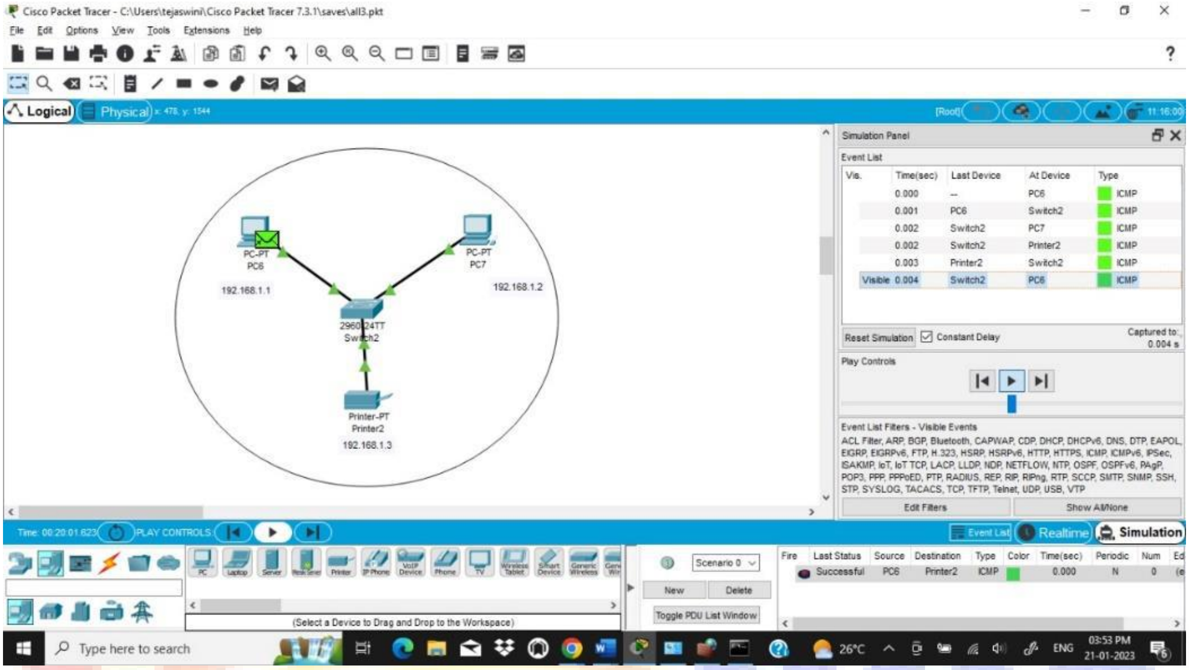
.



Step -7 Ping Printer from any PC

Click in any one PC, Click on Desktop, Click on Command Prompt and ping any pc from printer

By giving command - > ping IP address(ex 192.168.1.3)



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC6	🟩 ICMP
	0.001	PC6	Switch2	🟩 ICMP
	0.002	Switch2	PC7	🟩 ICMP
	0.002	Switch2	Printer2	🟩 ICMP
	0.003	Printer2	Switch2	🟩 ICMP
Visible	0.004	Switch2	PC6	🟩 ICMP

Reset Simulation ☑ Constant Delay Captured to: 0.004 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters | Show All/None

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Ed
●	Successful	PC6	Printer2	ICMP	🟩	0.000	N	0	(e

LAB -11 CONFIGURE OF WIFI HOTSPOT, AND CONNECT OTHER DEVICES (MOBILE / LAPTOP)

Step -1 Select

02 - PCs, 01- Printer, 01- Laptop, 01- server, 01- smart phone and 01- HomeRouter
By using Drag and Drop

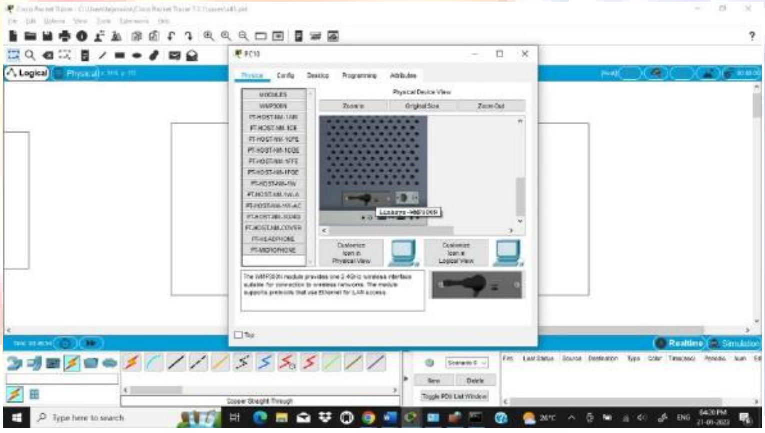
Step -2 Configure IP address to of Router

- Double click on Router
- Click on LAN (give router IP address 192.168.1.10)
- Click on Wireless2.4G
- Click on WPA-PSK
- Give PSK pass Phrase (Password 12345678)
- Change the SSID name default to KLEBCA

Step -3 Make Wired PC to Wireless PC

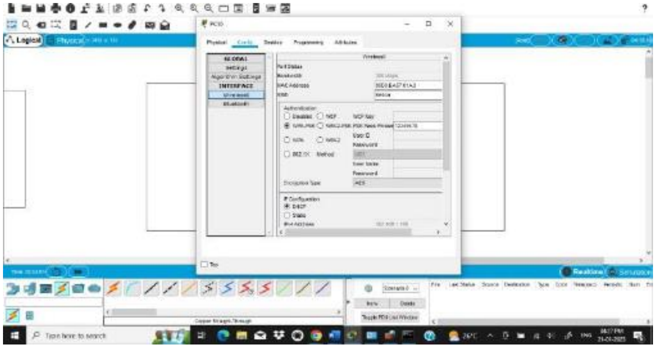
- Double Click on PC select Physical
- Click on WMP300N
- Off the PC

Change Network LAN port to Wireless LAN port by drag and drop
On the PC

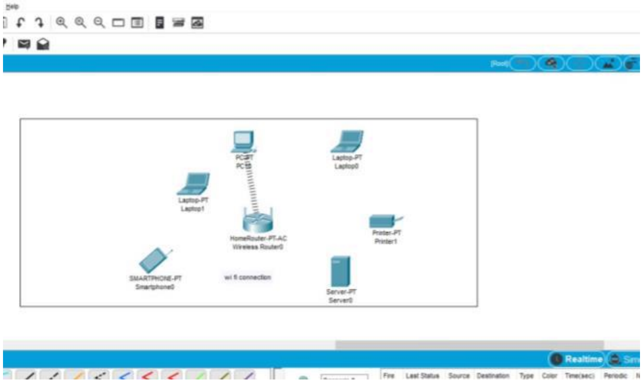


Step -4 Configure wireless PC

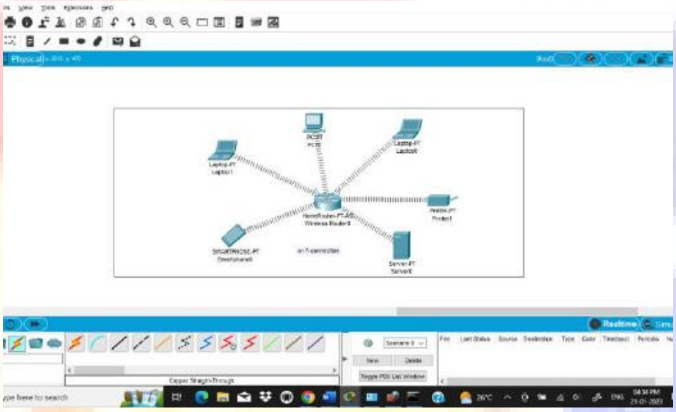
- Click on desktop
- Click on DHCP
- Next click on config
- Click on wireless0
- Click on WPA-PSK and give PSK PASS Phrase (12345678)
- Change SSID default to KLEBCA



PC will get connect to router



Step -4 Repeat Step 3rd to make Laptop, Printer, Server and Smartphone wireless



Now Wifi connection is ready to ping

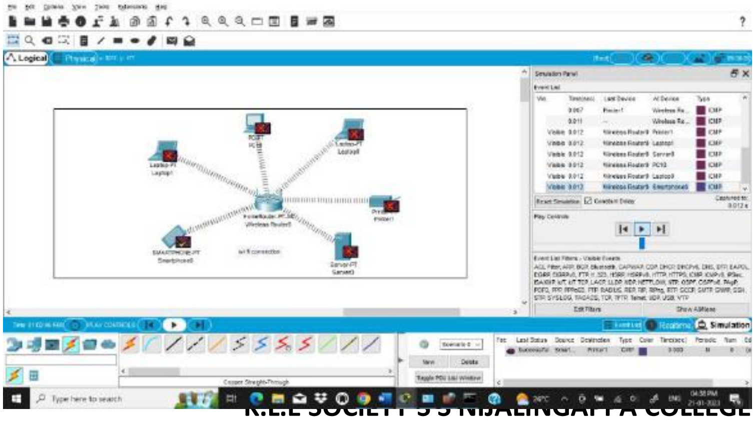
Step – 5 Ping Printer from any Devices

Click in any device, Click on Desktop, Click on Command Prompt and ping any pc from printer

By giving command - > Ping IP address

OR

Ping By Realtime or Simulation



LAB -12 CONFIGURE OF SWITCHES

1. **Configure password (For Login to Switch)**

Enable for switch configuration steps

Step - 1 Switch> EN or Enable

Step - 2 Switch#Config t / configuration terminal

Step -3 Switch(config)#line con 0

Step -4 Switch(config-line)#password 123456

Step -5 Switch(config-line)#login

Step -6 Switch(config-line)# Exit

Step -7 Switch(config)#Exit

Step -8 Switch# Exit

2. **Configure password for configuration switch**

Step - 1 Switch> EN or Enable

Step - 2 Switch# Config t / configuration terminal

Step -3 Switch(config)# enable secret 12345678

Step -4 Switch(config)# Exit

Step -5 Switch# Exit

To check for configuration password (i.e Login to Switch) First need to enter console password

User Access Verification

Password: (Loin password)

Switch> En /Enable

Password: (Configuration password i.e Secrete password)

Switch#

3. **Configure Switch hostname as KLEBCA**

Step -1 Switch# configure t

Step -2 Switch(config)# hostname KLEBCA

Step -3 KLEBCA(config)#

4. **Configure the message of the day as**

--
-

"Well Come to KLEBCA CISCO Switch Configuration"

--
-

Step -1 KLEBCA(config)#banner motd #

"Well Come to KLEBCA CISCO Switch Configuration"

---#

Step - 2 KLEBCA(config)# Exit (To check the message exit from the configuration)

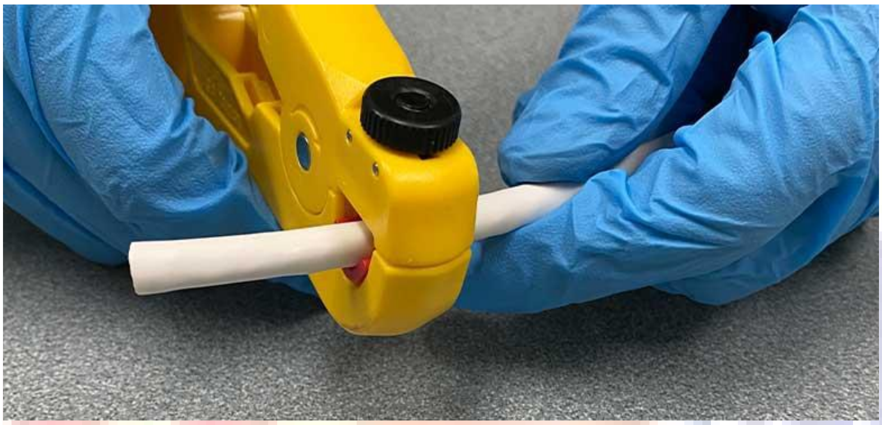
Step - 3 KLEBCA# Exit

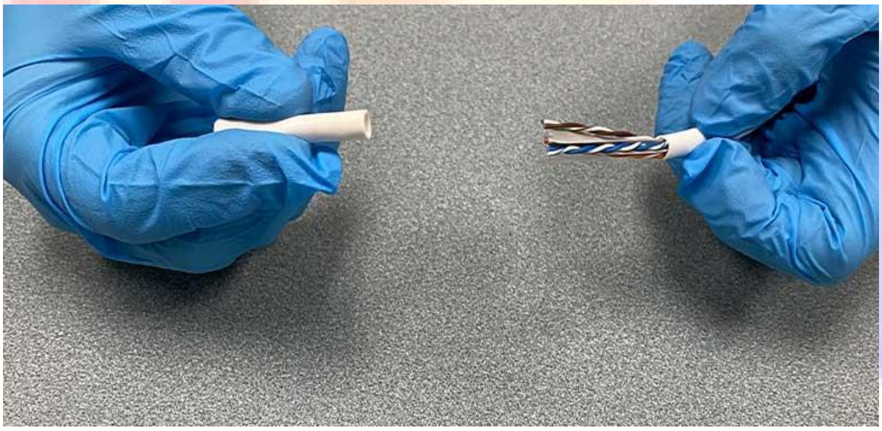
LAB -13 CONFIGURE OF I/O BOX FIXING

Requirements: Crimping tools, Bulk Network Cable, Keystone Jack, Jacket Stripper, Wire Cutter and Punch Down Tool

Procedure:

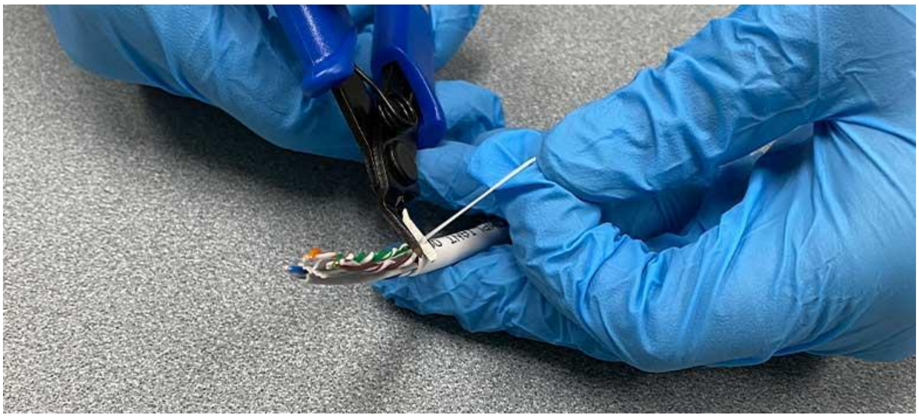
Step -1: 1 inch of jacket with jacket stripper





Using cutting tool cut 1 inch off the jacket from the top of the cable. If using scissors or another cutting device make sure not to cut through the wires in the cable.

Step -2: Cut the pulling string

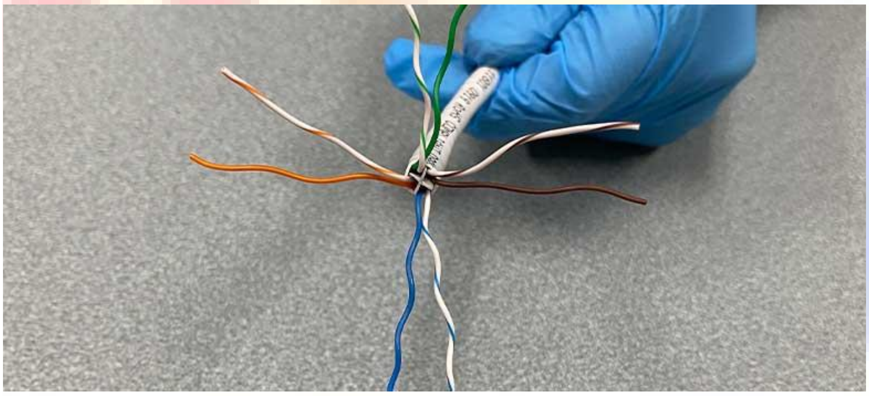


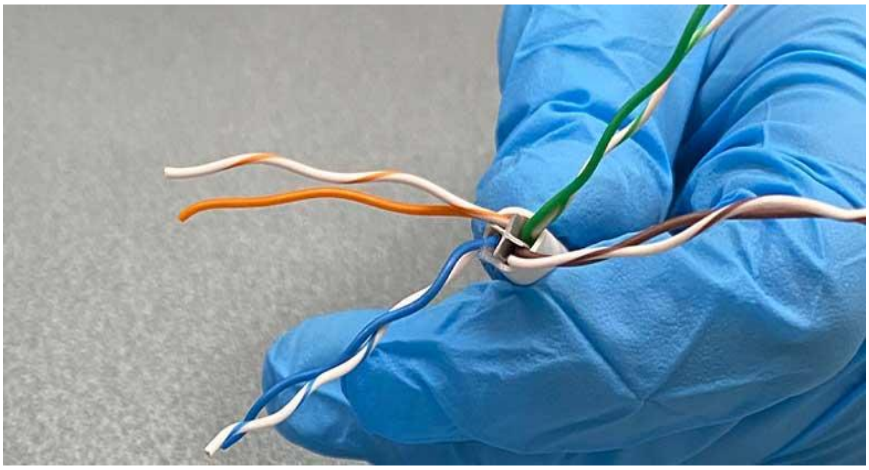
If comes with a pull string inside simply cut off the portion that is showing. The pull string is there to help strip the jack as well so if you need to take a little more jacket off can use it.

Step -3: Cut the spline

If cable also has a spline / cross separator in the cable, then cut off the portion that is showing. Try to cut off the without damaging the wires.

Step -4: Unwrap twisted pairs

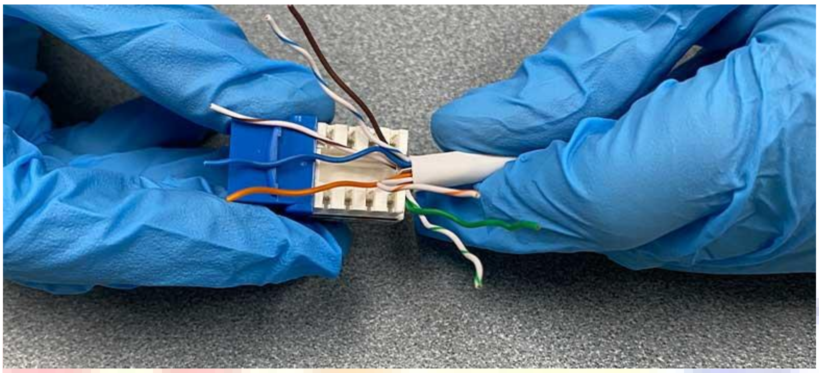




Unwrap the twisted pairs so it's easier to insert on to the 90° keystone jack. The important part to this step is to decide which wiring scheme you want to go with t568b or b.

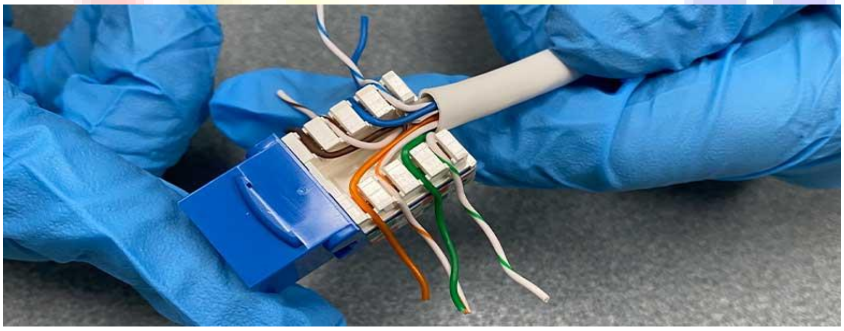
t568b goes in order:

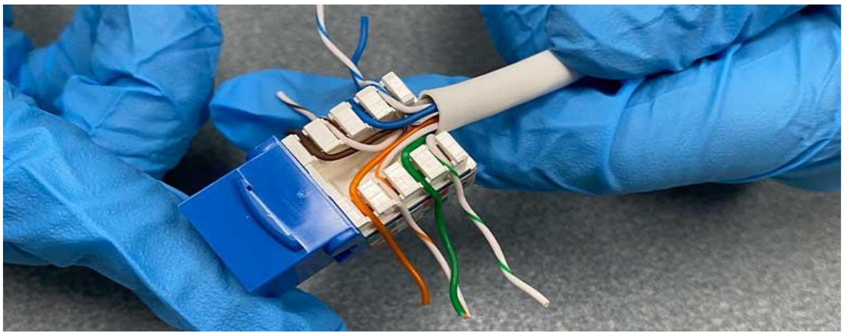
1. Orange stripe
2. Orange
3. Green Stripe
4. Blue
5. Blue stripe
6. Green
7. Brown stripe
8. Brown



Try not to insert the cables jacket too far in to the keystone jack. Try to get the jack just inside or touching the end of the jack. The other important thing to mention here is to not have any wiring exposed from the jack to the jack.

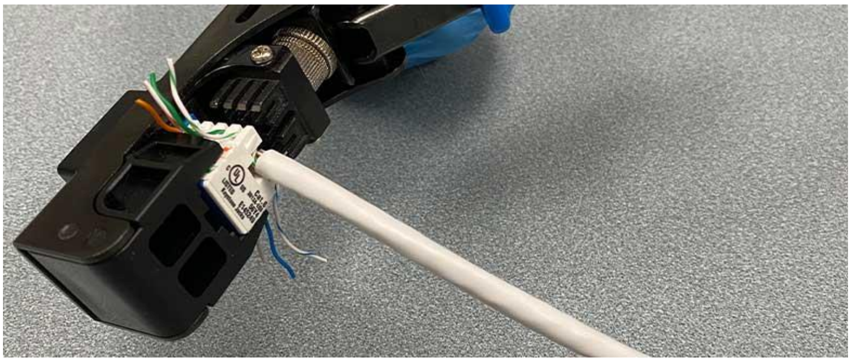
Step -5 Put the wire in the groove





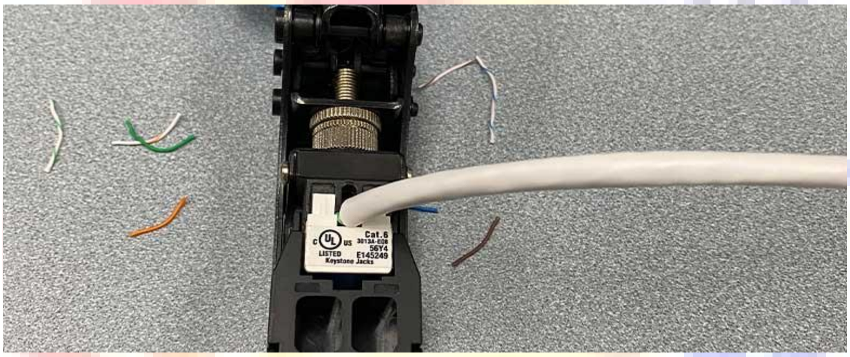
Using the wiring scheme have chosen, lay down the wires in the grooves of the keystone jack.

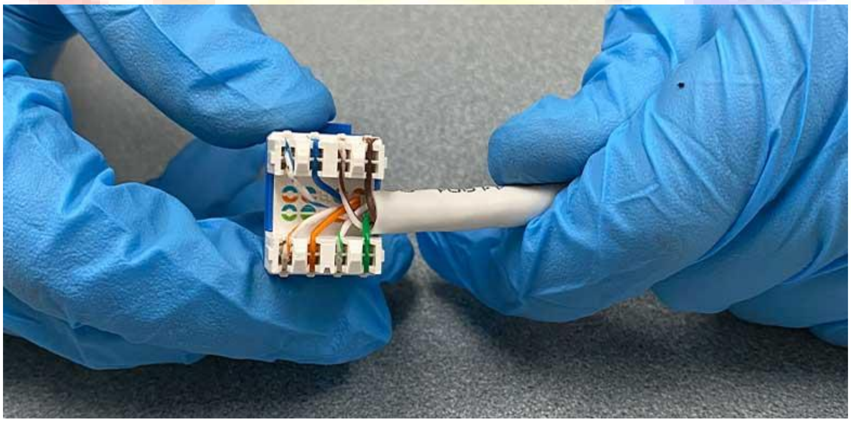
Step -6 Put keystone jack in the 90° punch down tool



Using a punch down tool can now insert the jack in to the punch down area of the tool. Make sure the degree of the punch down tool matches the degree of the keystone jack. Insert with open side facing the grooves of the punch down tool.

Step -7 Squeeze Punch down tool





By squeezing down on the punch down tool wires now firmly inside the contact area of the jack. The wires hanging off the side should also have been cut off. If some weren't cut off that is ok. Simply cut off the remaining portion using a cutting device.

For this step make sure to double check the wires are deep enough in the contact area. If any of the wires are not in the contact area yet try using the tool again to punch them down.

Step -8 Close the cap

LAB - 14 MAKING YOUR OWN PATCH CORD

Requirements: Crimping tools, UTP Cable, RJ-45 connector, Cable tester.

Procedure:

Crimping Tools:

Step -1: take 1/2mtrs or 1 mtrs   cable (cat 5e or cat 6)

Step -2: To Make Straight Through Patch Cord.

Step -3: Do following step

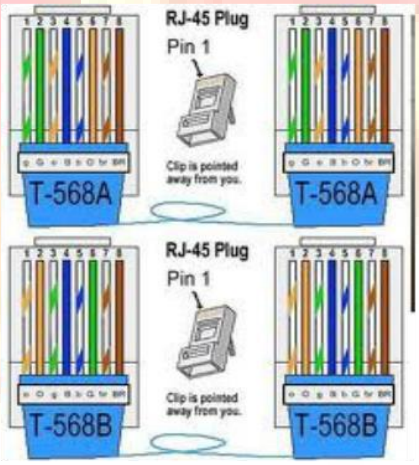
Check both cable end should be either T568A or both ends should be T568B

Step -4 Take RJ45 connector

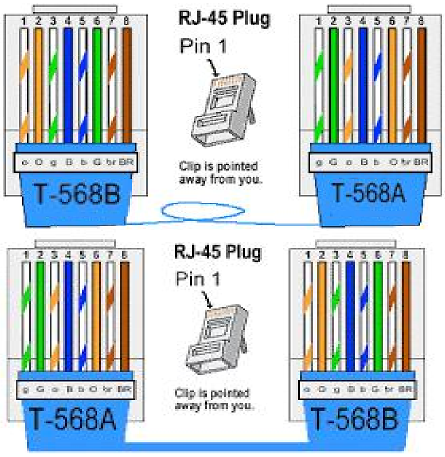
Step -5 Insert cable inside RJ45 connector according to colour code

Step -6 Crimp cable using Crimping Tool for both the ends

Step -7 Check both ends with Cable Tester.



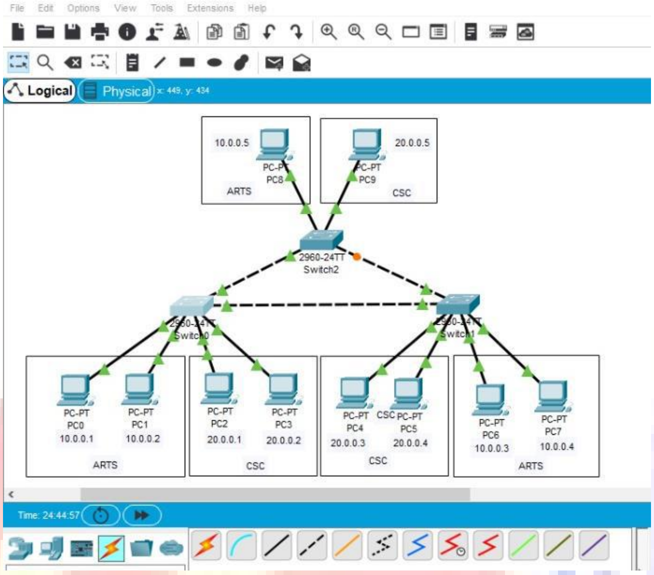
Step -8 Repeat same process for Cross Over cable
(But both the ends of cable should be T568B & T568A   or T568A & T568B)



LAB -15 CONFIGURE OF VLAN USING PACKET TRACER / GNS3

Step -1 : 06 PC's, 03 Switch's

Step -2 : Connect 02 PCs to Computer Science(CSC, Connect 02 PCs to Arts)



Step -3 : Configure IP for all PCS

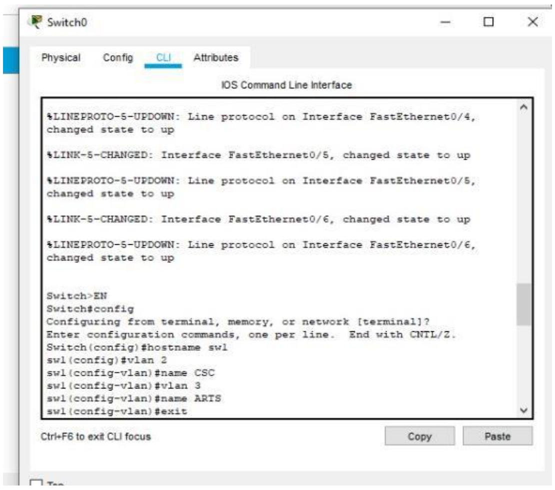
For ARTS - 10.0.0.1 and 10.0.0.5

For CSC - 20.0.0.1 and 20.0.0.5

Step -4 : Configure Switch -1

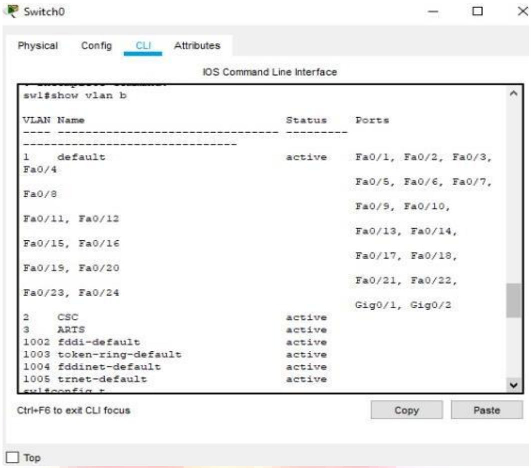
Click on switch, Click on CLI

```
Switch> en
Switch# Config t
Switch(Config)# hostname SW1
SW1(Config)#vlan 2
SW1(Config-vlan)# name CSC
SW1(config-vlan)# vlan 3
SW1(Config-vlan)#name ARTS
SW1(Config-vlan)#exit
SW1(Config)#exit
```



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4,
changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5,
changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6,
changed state to up


Switch>EN
Switch#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname swl
swl(config)#vlan 2
swl(config-vlan)#name CSC
swl(config-vlan)#vlan 3
swl(config-vlan)#name ARTS
swl(config-vlan)#exit
```

SW1#show vlan b /brief



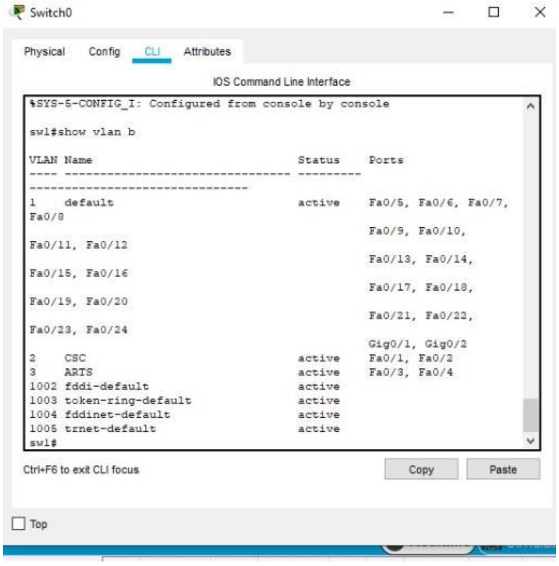
```
sw1#show vlan b

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3,
Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7,
Fa0/8
                                                Fa0/9, Fa0/10,
Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14,
Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18,
Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22,
Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
2    CSC                              active
3    ARTS                             active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
sw1#config t
```

SW1# Config t
SW1(Config)# int fastEthernet 0/1 or fa 0/1
SW1(Config-if)#Switchport access vlan 2
SW1(Config-if)#exit

SW1(Config)#int fastEthernet 0/2
SW1(Config-if)#Switchport access vlan 2
SW1(Config-if)#exit

SW1(Config)# int fastEthernet 0/3 or f1 0/3
SW1(Config-if)#Switchport access vlan 3
SW1(Config-if)# Exit

SW1(Config)#int fastEthernet 0/4
SW1(Config-if)#Switchport access vlan 3
SW1(Config-if)#exit
SW1(Config)#Exit
SW1# show vlan brief

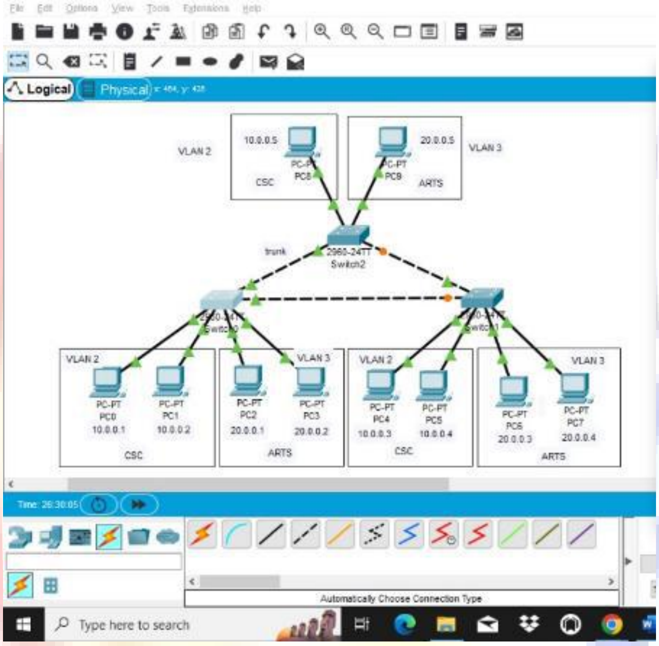


```
%SYS-5-CONFIG_I: Configured from console by console

sw1#show vlan b

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7,
Fa0/8
                                                Fa0/9, Fa0/10,
Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14,
Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18,
Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22,
Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
2    CSC                              active    Fa0/1, Fa0/2
3    ARTS                             active    Fa0/3, Fa0/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
sw1#
```

SWITCH TO SWITCH TRUNK FOR SWITCH1 (same port)

```
SW1(Config)# int fastEthernet 0/5
SW1(Config-if)# Switchport mode trunk
SW1(Config-if)#Exit
SW1(Config)#Exit
```

```
W1(Config)# int fastEthernet 0/6
SW1(Config-if)# Switchport mode trunk
SW1(Config-if)#Exit
SW1(Config)#Exit
SW1#show int trunk
```



```
SW2#Config t
SW2(Config)# int range fa 0/1-2
SW2(Config-if)#switchport access vlan 10
```

```
SW2#Config t
SW2(Config)# int range fa 0/3-4
SW2(Config-if)#switchport access vlan 20
```

SWITCH TO SWITCH TRUNK FOR SWITCH2 (same port)

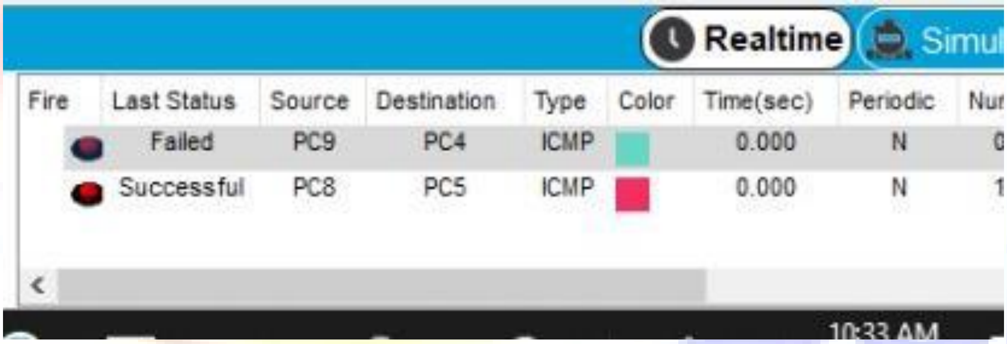
```
SW2(Config)# int fastEthernet 0/5
SW2(Config-if)# Switchport mode trunk
SW2(Config-if)#Exit
SW2(Config)#Exit
```

```
SW2(Config)# int fastEthernet 0/6
SW2(Config-if)# Switchport mode trunk
SW2(Config-if)#Exit
SW2(Config)#Exit
SW2#show int trunk
```

```
SW3#Config t
SW3(Config)# int fa 0/1
SW3(Config-if)#switchport access vlan 10

SW3#Config t
SW3(Config)# int fa 0/3
SW3(Config-if)#switchport access vlan 20
```

SWITCH TO SWITCH TRUNK FOR SWITCH2 (same port)

```
SW3(Config)# int fastEthernet 0/3
SW3(Config-if)# Switchport mode trunk
SW3(Config-if)#Exit
SW3(Config)#Exit

SW3(Config)# int fastEthernet 0/4
SW3(Config-if)# Switchport mode trunk
SW3(Config-if)#Exit
SW3(Config)#Exit
SW3#show int trunk
```



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Nur
●	Failed	PC9	PC4	ICMP	🟩	0.000	N	0
●	Successful	PC8	PC5	ICMP	🟥	0.000	N	1

PC9- (ARTS) to PC4 (CSC) – (VLAN 3 to VLAN 2) Will not send packets
PC8- (CSC) to PC5 (CSC) – (VLAN 3 to VLAN 3) Will send packets