SSMRV College®

RV INSTITUTIONS
SSMRV COLLEGE, JAYANAGAR
DEPARTMENT OF BCA
COMPUTER NETWORKS (24BCA33P) LAB MANUAL

---

1. **Execute the following commands: arp, ipconfig, hostname, netdiag, netstat, nslookup, pathping, ping route, tracert**
2. **Study of different types of network cables.**
3. **Practically implement the cross-wired cable and straight wired cable using crimping tool.**
4. **Study of network IP address configuration: (Classification of address, static and dynamic address)**
5. **Study of network IP address configuration: (IPv4 and IPv6 , Subnet, Supernet)**
6. **Study of network devices: (Switch, Router, Bridge)**
7. **Configure and Connect the computer in LAN.**
8. **Block the website using "Windows Defender Firewall" in windows 8**
9. **Share the folder in a system and access the files of that folder from other system using IP address.**
10. **Share the printer in Network, and take print from other PC.**
11. **Configuration of wifi hotspot, and connect other devices (mobile / laptop).**
12. **Configuration of switches.**
13. **Configuration of VLAN using Packet Tracer/ GNS3.**
14. **Configuration of VPN using Packet Tracer/ GNS3**

Program 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:\>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:\>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

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.

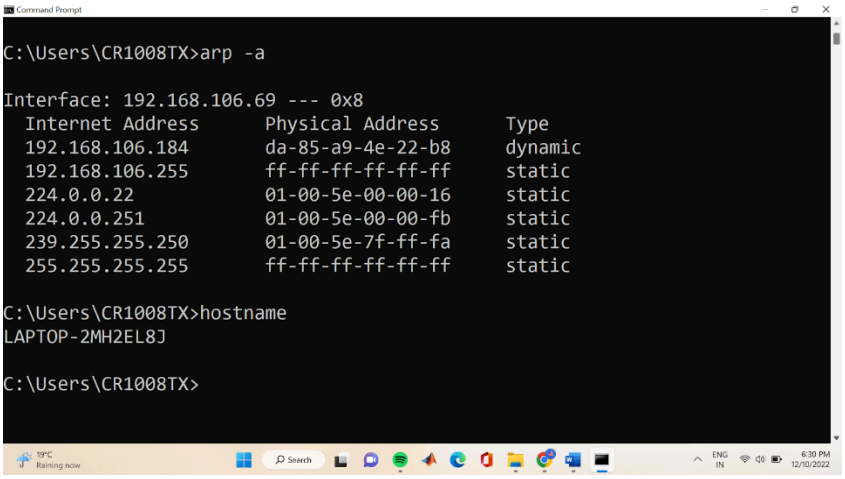
C:\>pathping: Pathping is unique to Window's, and is basically a combination of the Ping and Tracert commands. Pathping traces the route to the destination address then launches a 25 second test of each router along the way, gathering statistics on the rate of data loss along each hop.

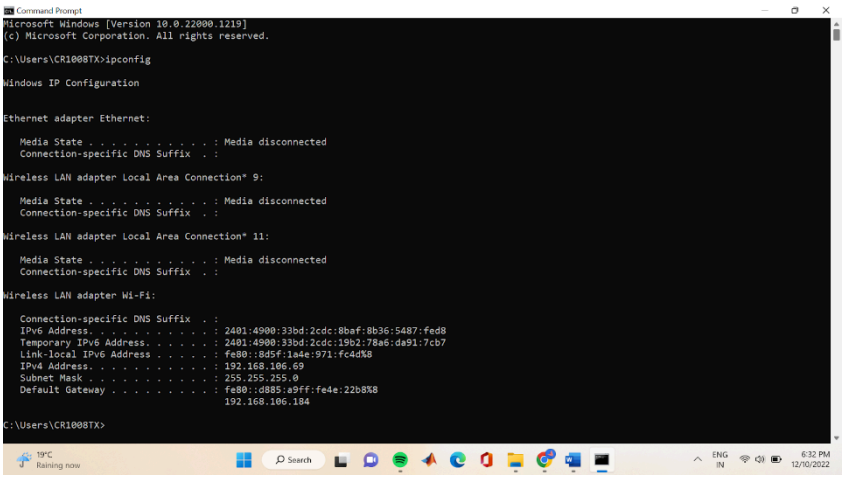
C:\>ping: Computers make phone calls to each other over a network by using a Ping command. The Ping commands main purpose is to place a phone call to another computer on the network, and request an answer. Ping has 2 options it can use to place a phone call to another computer on the network. It can use the computers name or IP address.

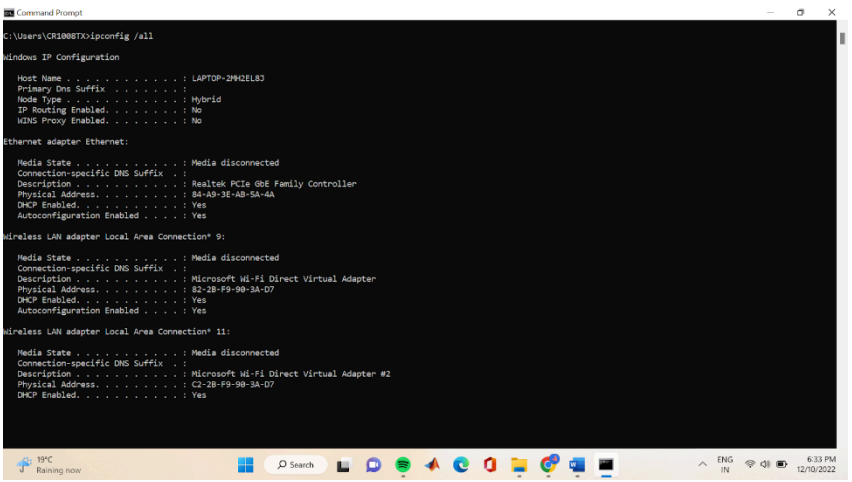
C:\>route: The route command displays the computers routing table. A typical computer, with a single network interface, connected to a LAN, with a router is fairly simple and generally doesn't pose any network problems.

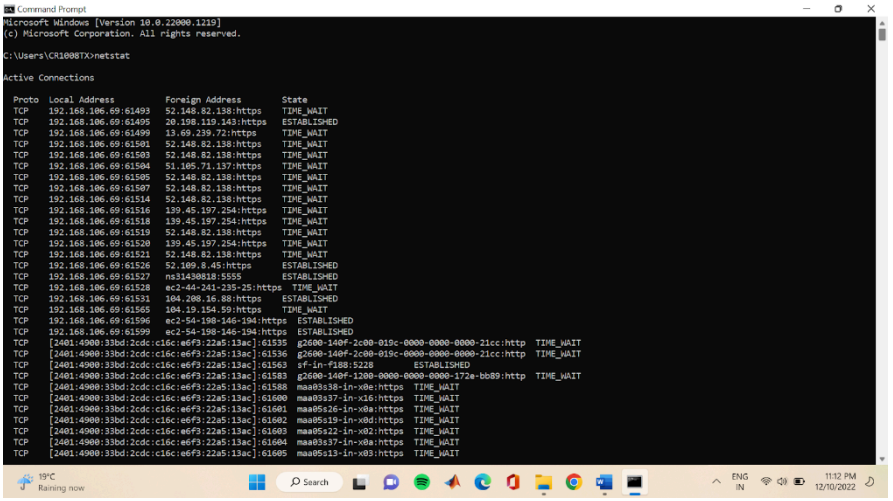
C:\>tracert: The tracert command displays a list of all the routers that a packet has to go through to get from the computer where tracert is run to any other computer on the internet.

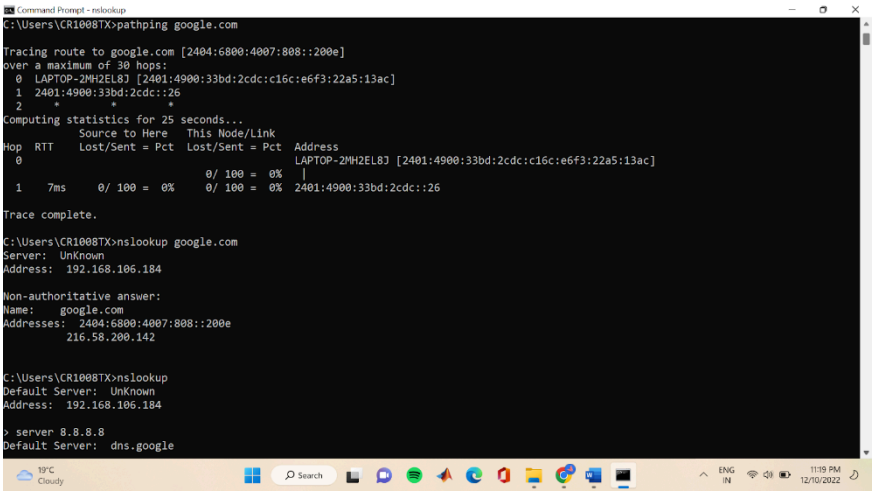
Output:

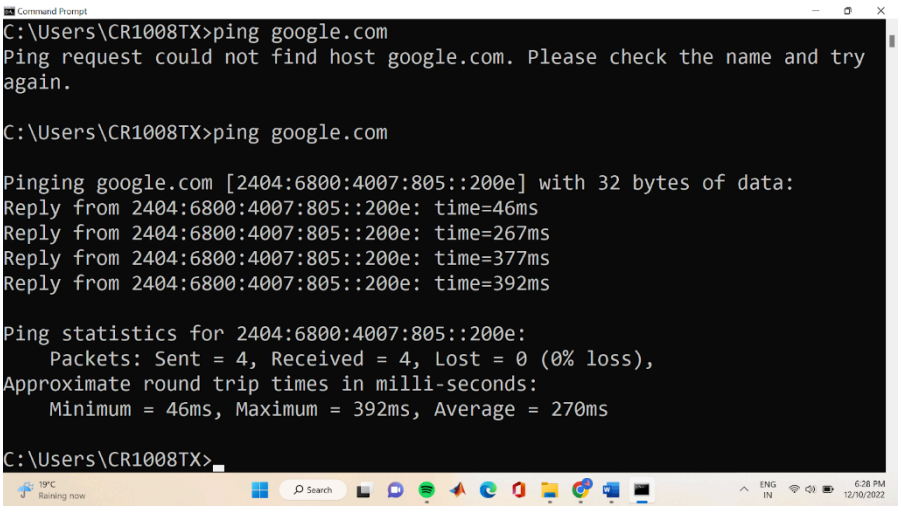

Command Prompt
C:\Users\CR1008TX>arp -a
Interface: 192.168.106.69 --- 0x8
Internet Address Physical Address Type
192.168.106.184 da-85-a9-4e-22-b8 dynamic
192.168.106.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Users\CR1008TX>hostname
LAPTOP-2MH2EL8J
C:\Users\CR1008TX>

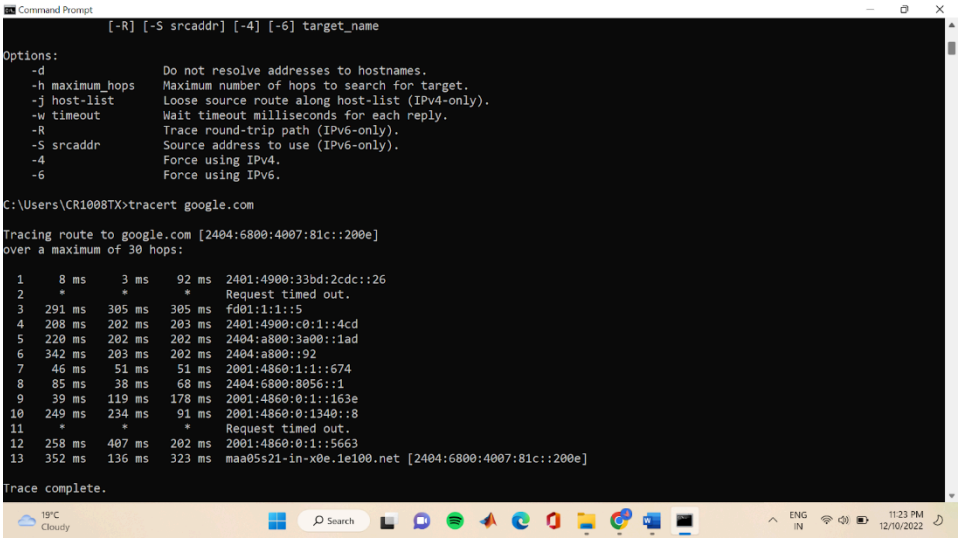

Command Prompt
Microsoft Windows [Version 10.0.22000.1219]
(c) Microsoft Corporation. All rights reserved.
C:\Users\CR1008TX>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 9:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 11:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2401:4900:33bd:2cdc:8baf:8b36:5487:fed8
Temporary IPv6 Address. . . . . : 2401:4900:33bd:2cdc:19b2:78a6:da91:7cb7
Link-local IPv6 Address . . . . . : fe80::8d5f:1a4e:971:fc4d%8
IPv4 Address. . . . . : 192.168.106.69
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::d885:a9ff:fe4e:22b8%8
192.168.106.184
C:\Users\CR1008TX>


Command Prompt
C:\Users\CR1008TX>ipconfig /all
Windows IP Configuration
Host Name . . . . . : LAPTOP-2MH2EL8J
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : 84-A9-3E-AB-5A-4A
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Local Area Connection* 9:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 82-2B-F9-90-3A-D7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Local Area Connection* 11:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : C2-2B-F9-90-3A-D7
DHCP Enabled. . . . . : Yes


Command Prompt
Microsoft Windows [Version 10.0.22000.1219]
(c) Microsoft Corporation. All rights reserved.
C:\Users\CR1008TX>netstat
Active Connections
Proto Local Address Foreign Address State
TCP 192.168.106.69:61493 52.148.82.138:https TIME_WAIT
TCP 192.168.106.69:61495 20.198.119.143:https ESTABLISHED
TCP 192.168.106.69:61499 13.69.239.72:https TIME_WAIT
TCP 192.168.106.69:61501 52.148.82.138:https TIME_WAIT
TCP 192.168.106.69:61503 52.148.82.138:https TIME_WAIT
TCP 192.168.106.69:61504 51.105.71.137:https TIME_WAIT
TCP 192.168.106.69:61505 52.148.82.138:https TIME_WAIT
TCP 192.168.106.69:61507 52.148.82.138:https TIME_WAIT
TCP 192.168.106.69:61514 52.148.82.138:https TIME_WAIT
TCP 192.168.106.69:61516 139.45.197.254:https TIME_WAIT
TCP 192.168.106.69:61518 139.45.197.254:https TIME_WAIT
TCP 192.168.106.69:61519 52.148.82.138:https TIME_WAIT
TCP 192.168.106.69:61520 139.45.197.254:https TIME_WAIT
TCP 192.168.106.69:61521 52.148.82.138:https TIME_WAIT
TCP 192.168.106.69:61526 52.109.8.45:https ESTABLISHED
TCP 192.168.106.69:61527 ns31430818:5555 ESTABLISHED
TCP 192.168.106.69:61528 ec2-44-241-235-25:https TIME_WAIT
TCP 192.168.106.69:61531 104.208.16.88:https ESTABLISHED
TCP 192.168.106.69:61565 104.19.154.59:https TIME_WAIT
TCP 192.168.106.69:61596 ec2-54-198-146-194:https ESTABLISHED
TCP 192.168.106.69:61599 ec2-54-198-146-194:https ESTABLISHED
TCP [2401:4900:33bd:2cdc:c16c:e6f3:22a5:13ac]:61535 g2600-140f-2c00-019c-0000-0000-0000-21cc:http TIME_WAIT
TCP [2401:4900:33bd:2cdc:c16c:e6f3:22a5:13ac]:61536 g2600-140f-2c00-019c-0000-0000-0000-21cc:http TIME_WAIT
TCP [2401:4900:33bd:2cdc:c16c:e6f3:22a5:13ac]:61563 sf-in-f188:5228 ESTABLISHED
TCP [2401:4900:33bd:2cdc:c16c:e6f3:22a5:13ac]:61583 g2600-140f-1200-0000-0000-0000-172a-bb89:http TIME_WAIT
TCP [2401:4900:33bd:2cdc:c16c:e6f3:22a5:13ac]:61588 maa03s38-in-x0e:https TIME_WAIT
TCP [2401:4900:33bd:2cdc:c16c:e6f3:22a5:13ac]:61600 maa03s37-in-x16:https TIME_WAIT
TCP [2401:4900:33bd:2cdc:c16c:e6f3:22a5:13ac]:61601 maa05s26-in-x0a:https TIME_WAIT
TCP [2401:4900:33bd:2cdc:c16c:e6f3:22a5:13ac]:61602 maa05s19-in-x0d:https TIME_WAIT
TCP [2401:4900:33bd:2cdc:c16c:e6f3:22a5:13ac]:61603 maa05s22-in-x02:https TIME_WAIT
TCP [2401:4900:33bd:2cdc:c16c:e6f3:22a5:13ac]:61604 maa03s37-in-x0a:https TIME_WAIT
TCP [2401:4900:33bd:2cdc:c16c:e6f3:22a5:13ac]:61605 maa05s13-in-x03:https TIME_WAIT
19°C Raining now
Search
ENG IN
11:12 PM 12/10/2022


Command Prompt - nslookup
C:\Users\CR1008TX>pathping google.com
Tracing route to google.com [2404:6800:4007:808::200e]
over a maximum of 30 hops:
0 LAPTOP-2MH2EL8J [2401:4900:33bd:2cdc:c16c:e6f3:22a5:13ac]
1 2401:4900:33bd:2cdc::26
2 * * *
Computing statistics for 25 seconds...
Source to Here This Node/Link
Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0 LAPTOP-2MH2EL8J [2401:4900:33bd:2cdc:c16c:e6f3:22a5:13ac]
0/ 100 = 0% |
1 7ms 0/ 100 = 0% 0/ 100 = 0% 2401:4900:33bd:2cdc::26
Trace complete.
C:\Users\CR1008TX>nslookup google.com
Server: UnKnown
Address: 192.168.106.184
Non-authoritative answer:
Name: google.com
Addresses: 2404:6800:4007:808::200e
216.58.200.142
C:\Users\CR1008TX>nslookup
Default Server: UnKnown
Address: 192.168.106.184
> server 8.8.8.8
Default Server: dns.google
19°C Cloudy
Search
ENG IN
11:19 PM 12/10/2022

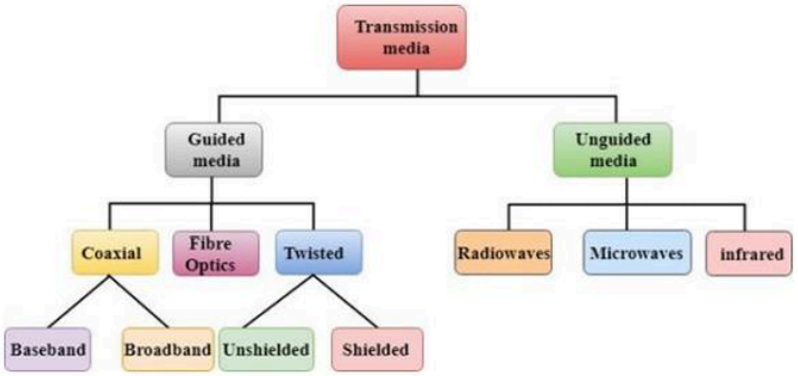

Command Prompt
C:\Users\CR1008TX>ping google.com
Ping request could not find host google.com. Please check the name and try again.
C:\Users\CR1008TX>ping google.com
Pinging google.com [2404:6800:4007:805::200e] with 32 bytes of data:
Reply from 2404:6800:4007:805::200e: time=46ms
Reply from 2404:6800:4007:805::200e: time=267ms
Reply from 2404:6800:4007:805::200e: time=377ms
Reply from 2404:6800:4007:805::200e: time=392ms
Ping statistics for 2404:6800:4007:805::200e:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 46ms, Maximum = 392ms, Average = 270ms
C:\Users\CR1008TX>
19°C Raining now
Search
ENG IN
6:28 PM 12/10/2022


Command Prompt
[-R] [-S srcaddr] [-4] [-6] target_name
Options:
-d Do not resolve addresses to hostnames.
-h maximum_hops Maximum number of hops to search for target.
-j host-list Loose source route along host-list (IPv4-only).
-w timeout Wait timeout milliseconds for each reply.
-R Trace round-trip path (IPv6-only).
-S srcaddr Source address to use (IPv6-only).
-4 Force using IPv4.
-6 Force using IPv6.
C:\Users\CR1008TX>tracert google.com
Tracing route to google.com [2404:6800:4007:81c::200e]
over a maximum of 30 hops:
1 8 ms 3 ms 92 ms 2401:4900:33bd:2cdc::26
2 * * * Request timed out.
3 291 ms 305 ms 305 ms fd01:1:1::5
4 208 ms 202 ms 203 ms 2401:4900:c0:1::4cd
5 220 ms 202 ms 202 ms 2404:a800:3a00::1ad
6 342 ms 203 ms 202 ms 2404:a800::92
7 46 ms 51 ms 51 ms 2001:4860:1:1::674
8 85 ms 38 ms 68 ms 2404:6800:8056::1
9 39 ms 119 ms 178 ms 2001:4860:0:1::163e
10 249 ms 234 ms 91 ms 2001:4860:0:1340::8
11 * * * Request timed out.
12 258 ms 407 ms 202 ms 2001:4860:0:1::5663
13 352 ms 136 ms 323 ms maa05s21-in-x0e.1e100.net [2404:6800:4007:81c::200e]
Trace complete.
19°C
Cloudy
Search
ENG
IN
11:23 PM
12/10/2022

Program 2: Study of different types of network 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 and receiver. The quality as well as characteristics of data transmission, can be determined from the characteristics of medium and 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 and 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 whole cable is protected by a plastic cover.

Advantages:

1. Coaxial cable was widely used for both analog and digital data transmissions.
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.

Advantages:

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:

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:

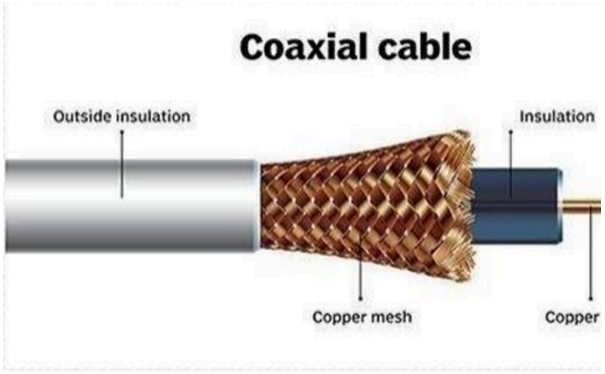
1.It is more expensive as compared to UTP and coaxial cable.
2.It has a higher attenuation rate.

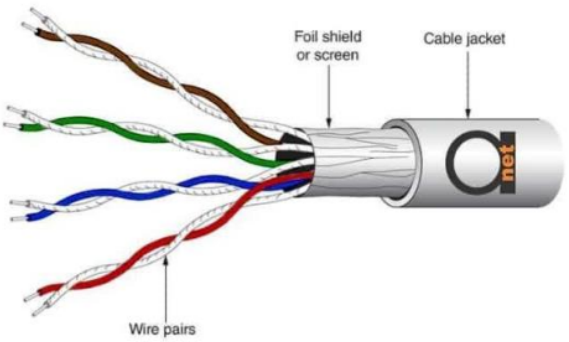
Unshielded twisted pair:

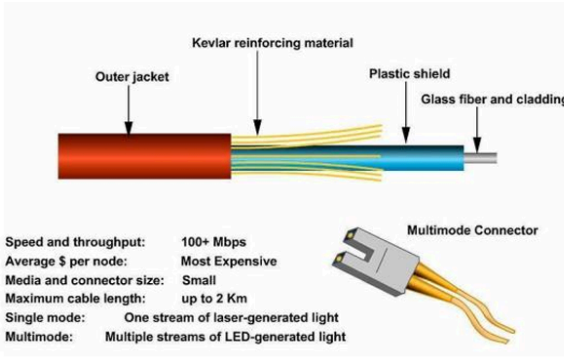
An unshielded twisted pair is widely used in telecommunication. It is most common type when compared with shielded twisted pair cable which consists of two conductors usually copper, each with its own colour plastic insulator.

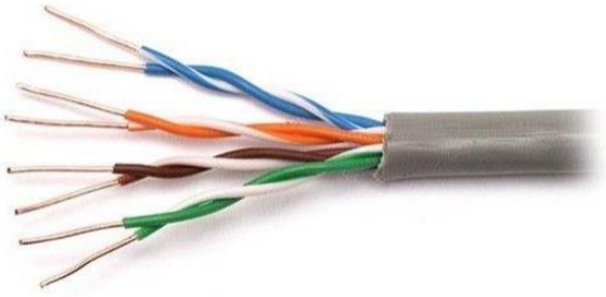
Advantages:
1.It is cheap.
2.Installation of the unshielded twisted pair is easy.
3.It can be used for high-speed LAN.

Disadvantage:
1.This cable can only be used for shorter distances because of attenuation.









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)

Unbounded or 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.
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.

Program-3 Practically implement the Cross – Wired Cable and Straight Wired Cable using Crimping Tool

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

Crimping Tools: A crimping tool is a hand or power tool used to join two pieces of metal, wire, or other materials by deforming one or both of them so that they hold each other. 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.

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

Procedure:

1. Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Be very careful at this point, as to not nick or cut into the wires, which are inside. Doing so could alter the characteristics of your cable, or even worse render is useless. Check the wires, one more time for nicks or cuts. If there are any, just whack the whole end off, and start over.

2. Spread the wires apart, but be sure to hold onto the base of the jacket with your other hand. You do not want the wires to become untwisted down inside the jacket. Category 5 cable must only have 1/2 of an inch of 'untwisted' wire at the end; otherwise it will be 'out of spec'. At this point, you obviously have ALOT more than 1/2 of an inch of un-twisted wire.

3. You have 2 end jacks, which must be installed on your cable. If you are using a pre-made cable, with one of the ends whacked off, you only have one end to install - the crossed over end. Below are two diagrams, which show how you need to arrange the cables for each type of cable end. Decide at this point which end you are making and examine the associated picture below.

Ethernet Cable Tips:

· A straight-thru cable has identical ends.
· A crossover cable has different ends.
· A straight-thru is used as a patch cord in Ethernet connections.
· A crossover is used to connect two Ethernet devices without a hub or for connecting two hubs.
· A crossover has one end with the Orange set of wires switched with the Green set.
· Odd numbered pins are always striped; even numbered pins are always solid coloured.
· Looking at the RJ-45 with the clip facing away from you, Brown is always on the right, and pin 1 is on the left.
· No more than 1/2" of the Ethernet cable should be untwisted otherwise it will be susceptible to crosstalk.
· Do not deform, do not bend, do not stretch, do not staple, do not run parallel with power cables, and do not run Ethernet cables near noise inducing components.

Diagram shows you how to prepare straight through wired connection

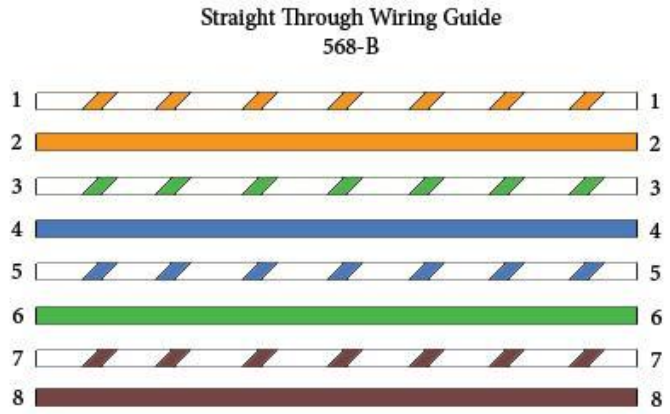
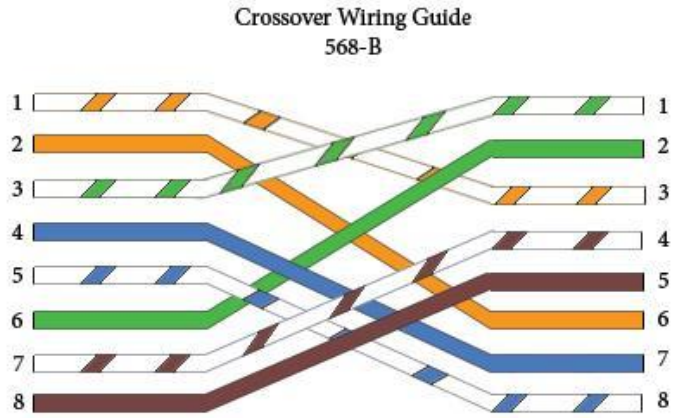
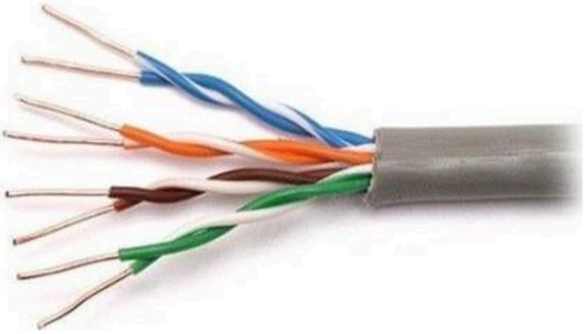


Diagram shows you how to prepare Cross wired connection


Crossover Wiring Guide
568-B
1
2
3
4
5
6
7
8
1
2
3
4
5
6
7
8


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




CABLE TESTER
RJ45+RJ11
RJ11+ RJ45
MASTER
NSHL468
REMOTE
NSHL468

Program-4 Study the Network IP Address Configuration (Classification of Address, Static and Dynamic Address)

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.

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.

Configuration:

Step 1. To access Control Panel

A. **On your keyboard, press the "Windows" and "R" keys at the same time.**

A. **Enter "ncpa.cpl" in the window that pops up.**

Step 2: Right click on the network adapter that is currently connected to the device that you are trying to configure

Step 3: Select "Properties" from the drop-down menu.

Step 4: Double-click on "Internet Protocol Version 4 (TCP/IPv4)".

Step 5: Manually enter IP address and subnet mask.

Step 6: Click the ok button

Dynamic IP addresses 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 a temporary dynamic IP address.

Configuration:

Step 1. To access Control Panel

A. **On your keyboard, press the "Windows" and "R" keys at the same time.**

A. **Enter "ncpa.cpl" in the window that pops up.**

Step 2: Right click on the network adapter that is currently connected to the device that you are trying to configure

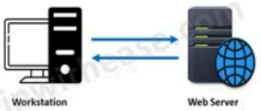
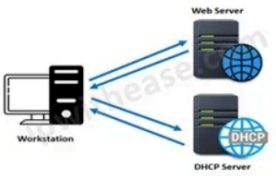
Step 3: Select "Properties" from the drop-down menu.

Step 4: Double-click on "Internet Protocol Version 4 (TCP/IPv4)".

Step 5: Select the Obtain an IP address automatically **option.**

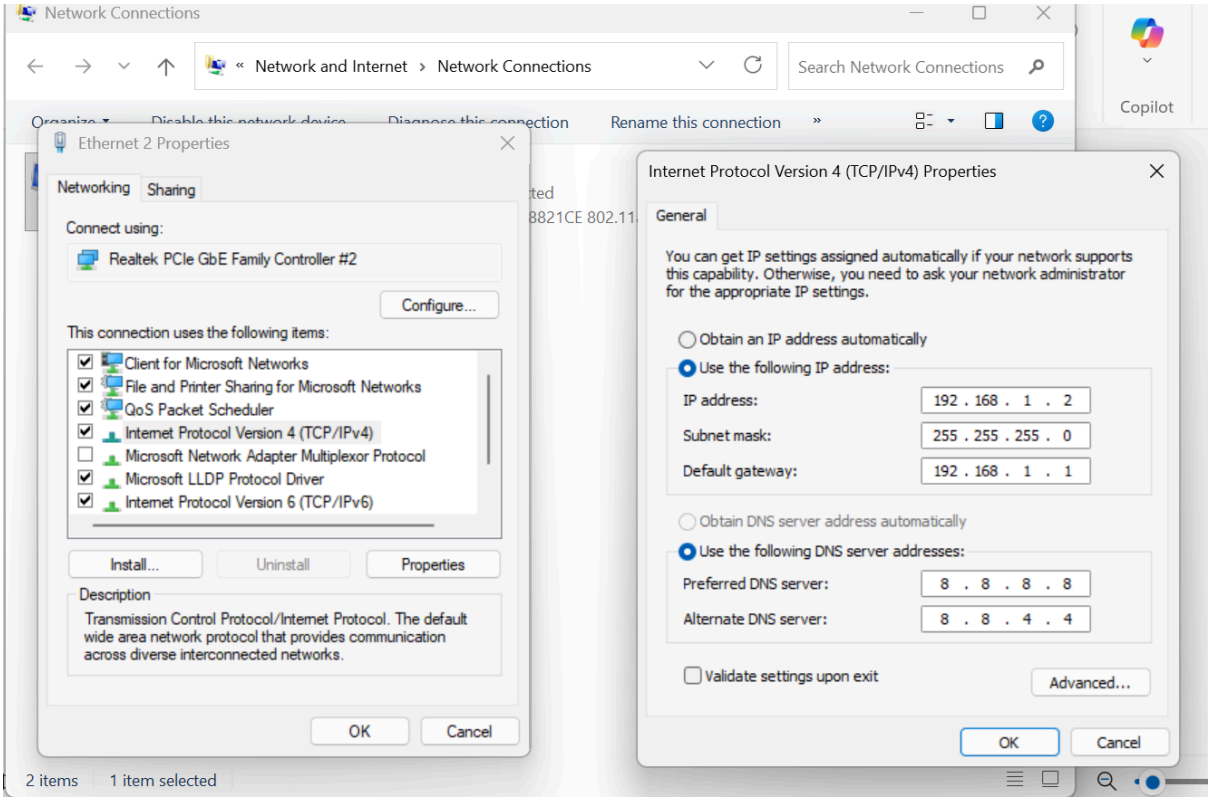
Step 6: Select the Obtain the following DNS server address automatically **option.**

Step 7:Click the ok button

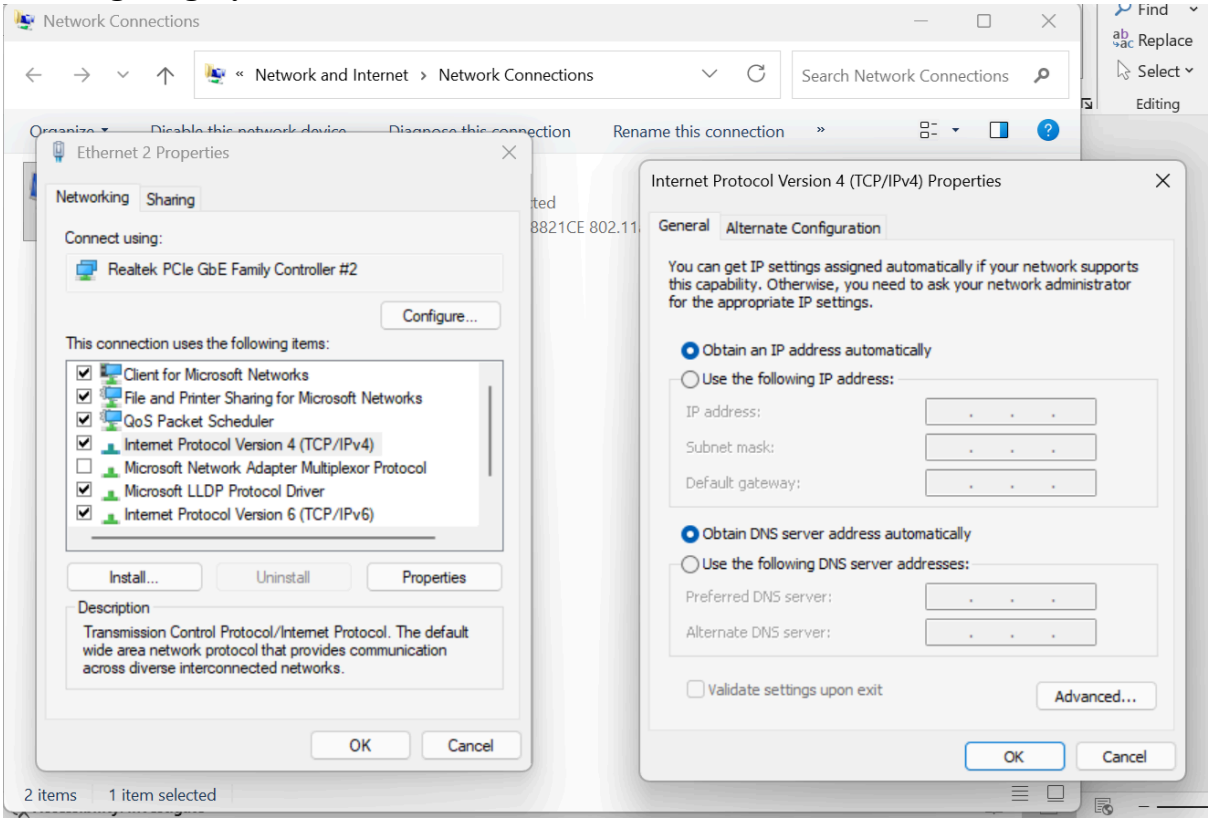
Function	Static IP address	Dynamic IP address
		
Provider	Internet Service Provider	DHCP (Dynamic Host Configuration Protocol)
Nature	Constant	Not constant
Security	Less secure	More secure
Traceability	Easily traceable	Difficult to trace
Stability	Stability is higher	Less stable
Costs	Costly	No direct cost Cost associated to setup initial infrastructure DHCP server
Confidentiality	Not so confidential	Higher security
Troubleshooting	Easy	Complex

Output:

a. Configuring Static IP Address



b. Configuring Dynamic IP Address



Program 5: Study of network IP address configuration: (IPv4 and IPv6 , Subnet, Supernet)

IP Address :

An IP address is a unique identifier for devices that access the internet or devices on a local area network. It uses a string of numbers and/or letters with periods or colons. It is

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.
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:

Subnetting is a technique of partitioning an individual physical network into several small-sized logical sub-networks. These subnetworks are known as subnets.

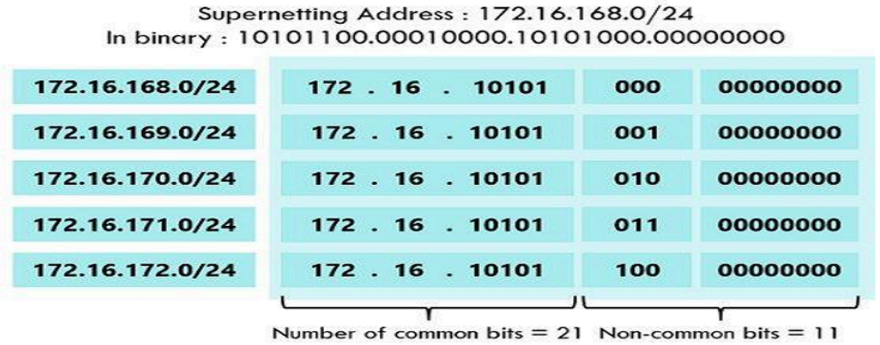
An IP address is made up of the combination of the network segment and a host segment. A subnet is constructed by accepting the bits from the IP address host portion which are then used to assign a number of small-sized sub-networks in the original network. The Subnetting basically convert the host bits into the network bits.

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).

Supernetting:

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 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.



Program 6: Study of network devices: (Switch, Router, Bridge)

1. Switch

A switch is a network device that operates at the Data Link Layer (Layer 2) of the OSI model.

It is used to connect multiple devices (computers, printers, servers) in a LAN and forward data intelligently.

Functions:

- **MAC Address Learning: Maintains a MAC address table to remember which device is on which port.**
- **Frame Forwarding: Sends data only to the specific port where the destination device is connected (unlike a hub which sends data to all ports).**
- **Collision Reduction: Creates a separate collision domain per port, reducing network congestion.**

Advantages:

- **Faster than hubs (no unnecessary traffic).**
- **Improves security (data not broadcast to all).**
- **Full-duplex communication (simultaneous send/receive).**

2. Bridge

A bridge is a network device that also works at the Data Link Layer (Layer 2) and is used to divide a network into segments.

Functions

- **Traffic Filtering: Checks the MAC address of incoming frames and decides whether to forward or block them.**
- **Collision Domain Separation: Reduces network traffic by isolating segments.**
- **Protocol Transparency: Works regardless of higher-layer protocols (TCP/IP, etc.).**

Advantages

- **Connects two LAN segments.**
- **Reduces collisions and improves performance.**
- **Works as a primitive version of a switch (in fact, switches are multiport bridges with more intelligence).**

Limitations

- **Slower than switches (software-based processing).**
- **Mostly outdated, switches have replaced bridges in modern networks.**

3. Router

A router operates at the Network Layer (Layer 3) of the OSI model.

Its main job is to connect different networks together and forward data packets between them.

Functions

- **IP Addressing: Uses IP addresses (not MAC) to determine best path for data.**
- **Routing Table: Maintains information about available networks and routes.**
- **Packet Forwarding: Chooses the most efficient path for each data packet.**
- **Traffic Management: Can apply policies like QoS, access control lists (ACLs).**

Advantages

- **Connects multiple networks (LAN to WAN).**
- **Reduces broadcast traffic by dividing broadcast domains.**
- **Provides security with firewalls and NAT (Network Address Translation).**

Differences:

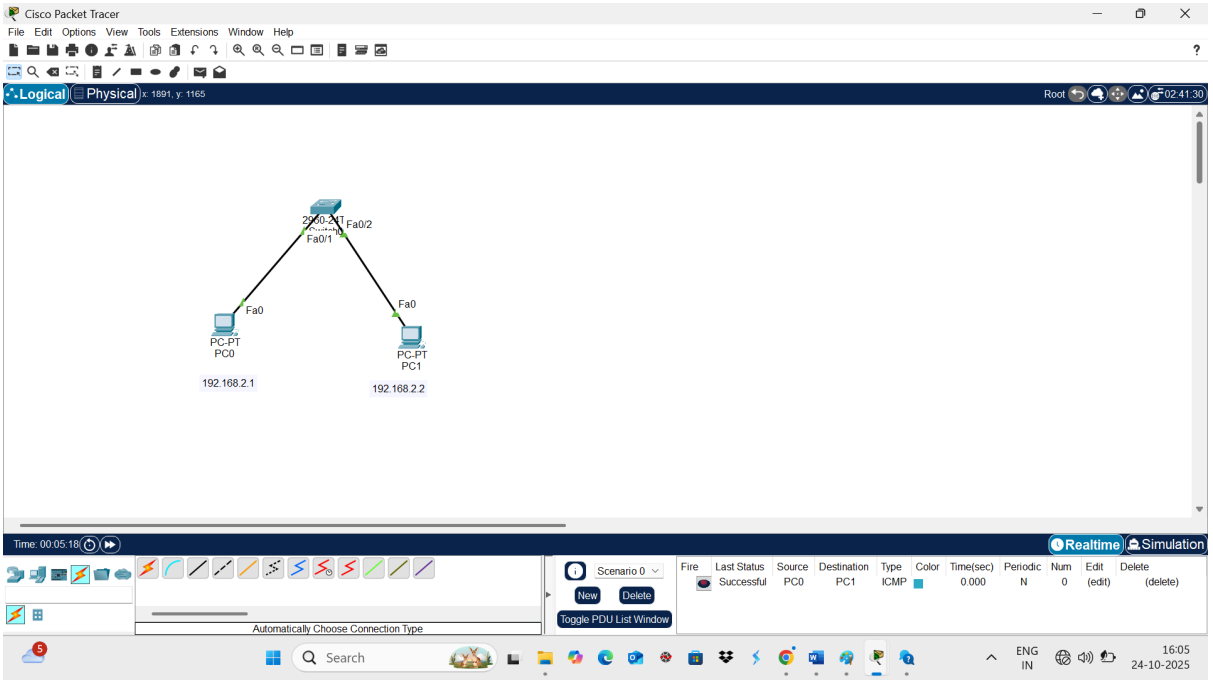
Feature	Switch	Bridge	Router
OSI Layer	Layer 2 (Data Link)	Layer 2 (Data Link)	Layer 3 (Network)
Uses	Connects devices in LAN	Connects network segments	Connects multiple networks
Forwarding Basis	MAC Address	MAC Address	IP Address
Collision Domain	Per Port	Per Segment	Per Interface (separate network)
Broadcast Domain	Same for all ports (unless VLANs)	Same for all segments	Each interface = separate domain
Speed	High (hardware-based)	Moderate (software-based)	Slightly slower (routing overhead)
Modern Use	Very common (LAN backbone)	Rarely used (replaced by switches)	Essential (LAN-WAN connection)

Program 7: Configure and Connect the computer in LAN.

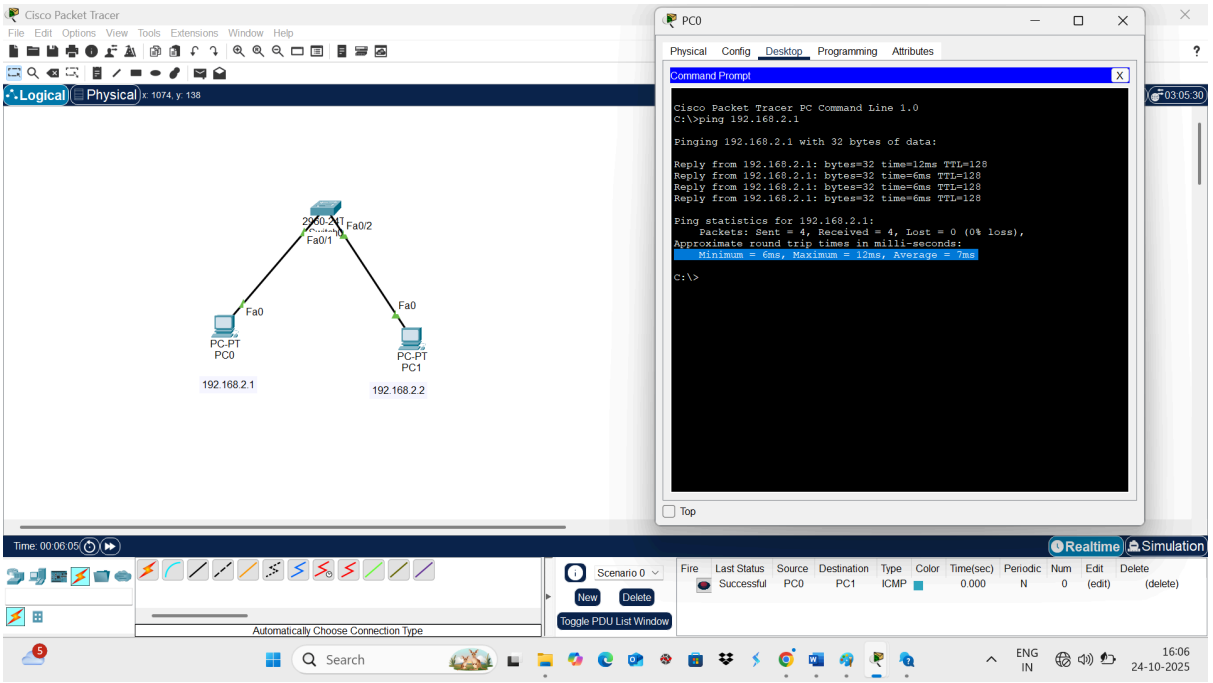
LAN: A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school. A LAN comprises cables, access points, switches, routers, and other components that enable devices to connect to internal servers, web servers, and other LANs via wide area networks.
The advantages of a LAN are the same as those for any group of devices networked together. The devices can use a single Internet connection, share files with one another, print to shared printers, and be accessed and even controlled by one another.

Procedure:
Step 1 : Select the 02 - PCs, 01- Switch by using Drag and Drop
Step 2: Connect all 02 PCs to switch using Straight Through cable and configure IP address as 192.168.1.1 and 192.168.1.2
Step3 : Click in any one PC, Click on Desktop, Click on Command Prompt and ping pc1 to pc2 by giving command - ping IP address(ex 192.168.1.1)

Network Topology:


Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical Physical
Root
2950-24T
Fa0/1
Fa0/2
Fa0
Fa0
PC-PT
PC0
PC-PT
PC1
192.168.2.1
192.168.2.2
Time: 00:05:18
Realtime Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
Successful
PC0
PC1
ICMP
0.000
N
0
(edit)
(delete)
Search
ENG
IN
16:05
24-10-2025

Output:

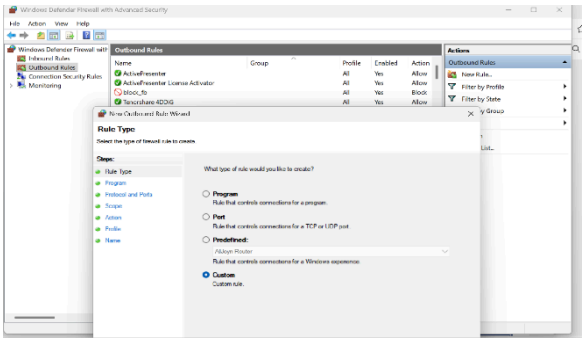

Cisco Packet Tracer
PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=12ms TTL=128
Reply from 192.168.2.1: bytes=32 time=6ms TTL=128
Reply from 192.168.2.1: bytes=32 time=6ms TTL=128
Reply from 192.168.2.1: bytes=32 time=6ms TTL=128
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 12ms, Average = 7ms
C:\>
Top
Logical Physical
2950-24T
Fa0/1
Fa0/2
Fa0
Fa0
PC-PT
PC0
PC-PT
PC1
192.168.2.1
192.168.2.2
Time: 00:06:05
Realtime Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type
Search
ENG
IN
16:06
24-10-2025

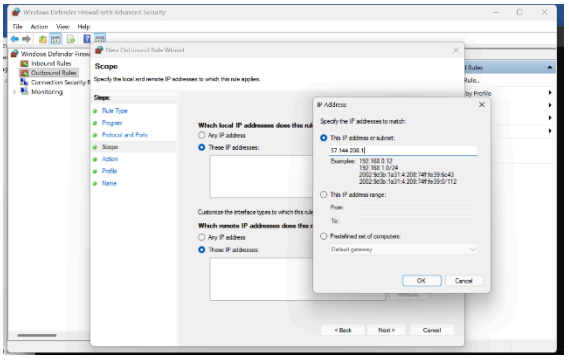
Program 8 : Block the website using “Windows Defender Firewall” in windows 8

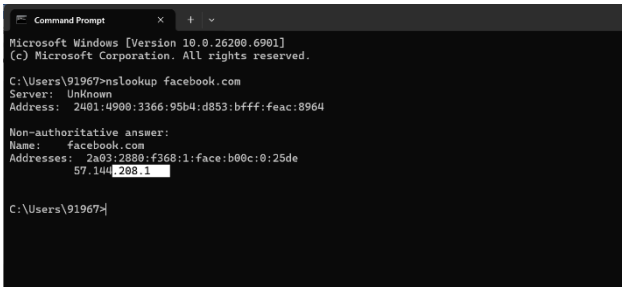
Procedure:

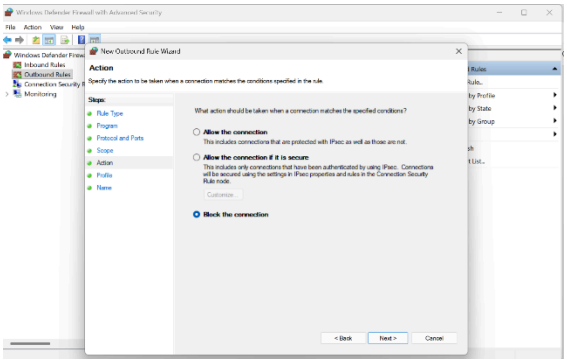
Step 1: Launch the Control Panel on your computer.
Step 2: Select “Windows Defender Firewall” followed by “Advanced Settings” on the left side pane.
Step 3: Right-click on “Outbound Rules” from the menu on the left and select “New Rule.”
Step 4: When a new window pops up, select the “Custom” option followed by “Next.”
Step 5: On the next window, select “All programs” and again select “Next.”
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.
Step 9: Click on “Add” and enter the IP addresses you want to block. Then select “Next.” Step 10 : Make sure to choose the “Block the connection” option and click on “Next.” Step 11: Choose whether the rule applies to Domain, Private, or Public. You can also select all three.

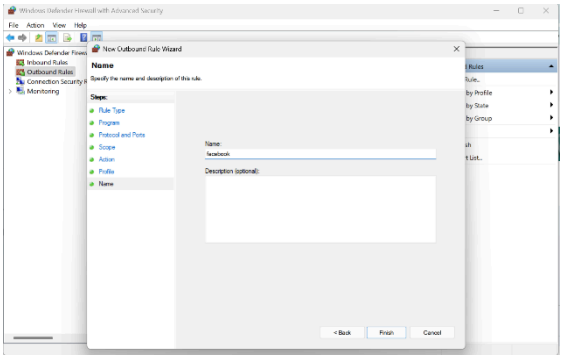
Step 12 : Select “Next,” add a name or description for this rule, and select “Finish” to complete the action.
Step 13: Finish and Check for Blocked website



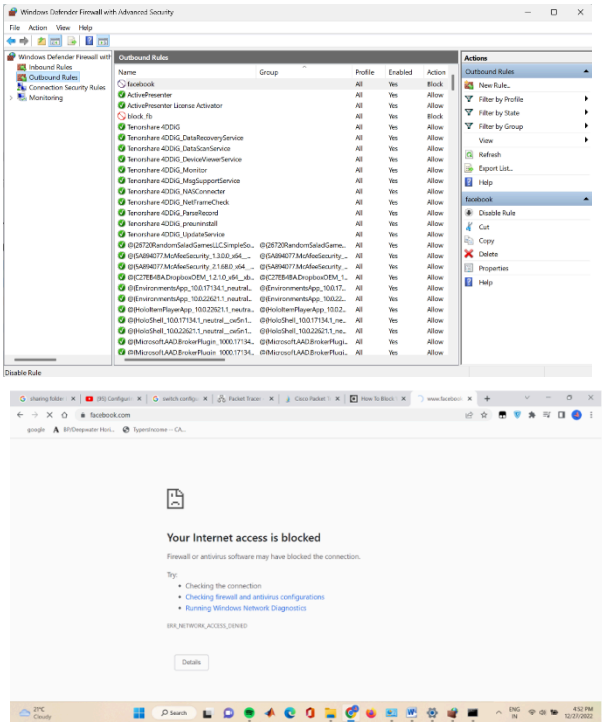



Command Prompt
Microsoft Windows [Version 10.0.26200.6901]
(c) Microsoft Corporation. All rights reserved.
C:\Users\91967>nslookup facebook.com
Server: UnKnown
Address: 2401:4900:3366:95b4:d853:bfff:feac:8964
Non-authoritative answer:
Name: facebook.com
Addresses: 2a03:2880:f368:1:face:b00c:0:25de
57.144.208.1
C:\Users\91967>


New Outbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
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.
Customize...
Block the connection
< Back
Next >
Cancel


New Outbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Name:
facebook
Description (optional):
< Back
Finish
Cancel

Output:



Program 9 : Share the folder in a system and access the files of that folder from other system using IP address.

Procedure:

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

Step -2 IP Address Configuration for DNS Server (192.168.1.4) and PC's (192.168.1.2 and 192.168.1.3)

Step -3 For both PC give the DNS server IP (192.168.1.4)

Step -4 Click on Server - Services - FTP

a) **Give the User name and Password (username is – admin, password – admin)**

b) **Give the permission for admin (Write, Read, Delete, Rename, List) Next Click on add**

Step -5 From PC1

a) **Create text file (double click on PC)**

b) **Click on Desktop**

c) **Click on Text Editor**

d) **Click on File > New Type text (Share the file in a system and access the files from other system or server using IP address)**

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

Step -6 In the same PC click on command prompt

a) **Check the file by entering C: \> dir C:\> ftp 192.168.1.1 (Enter the IP address of Server to connect Server)**

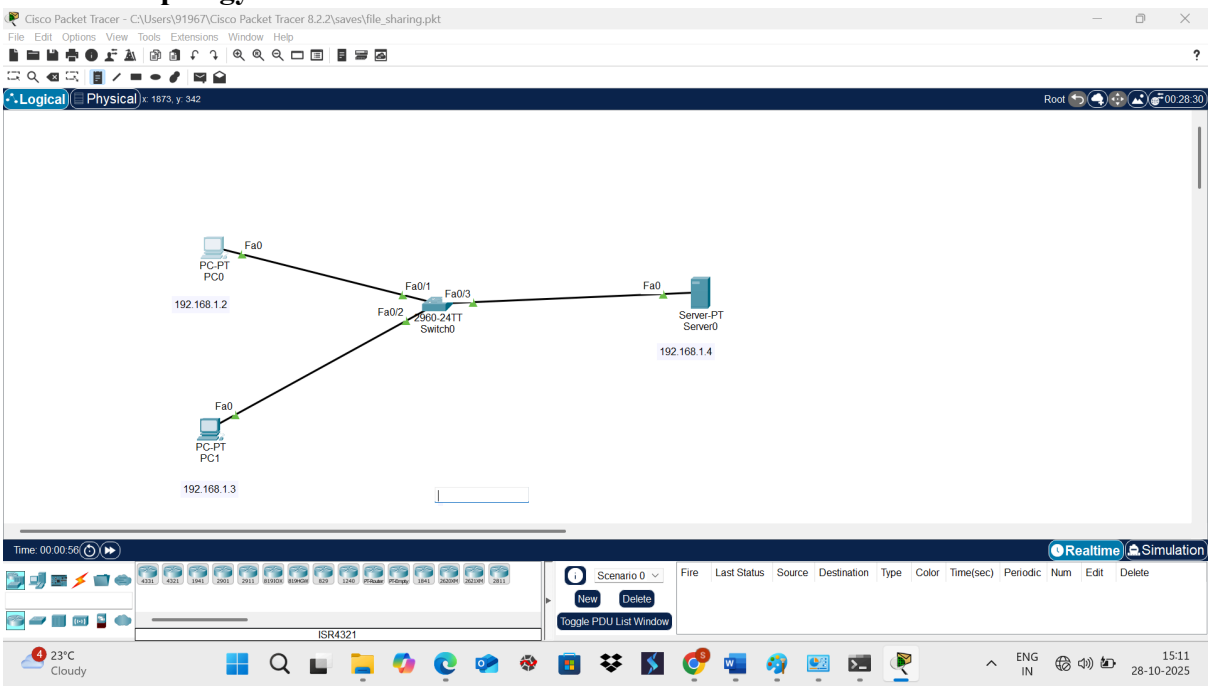
b) **Give Username and Password**

c) **ftp> put test1.txt (File transferred from PC1 to Server)**
d) **ftp> dir (Check the file is transferred to server by giving dir command) test1.txt**

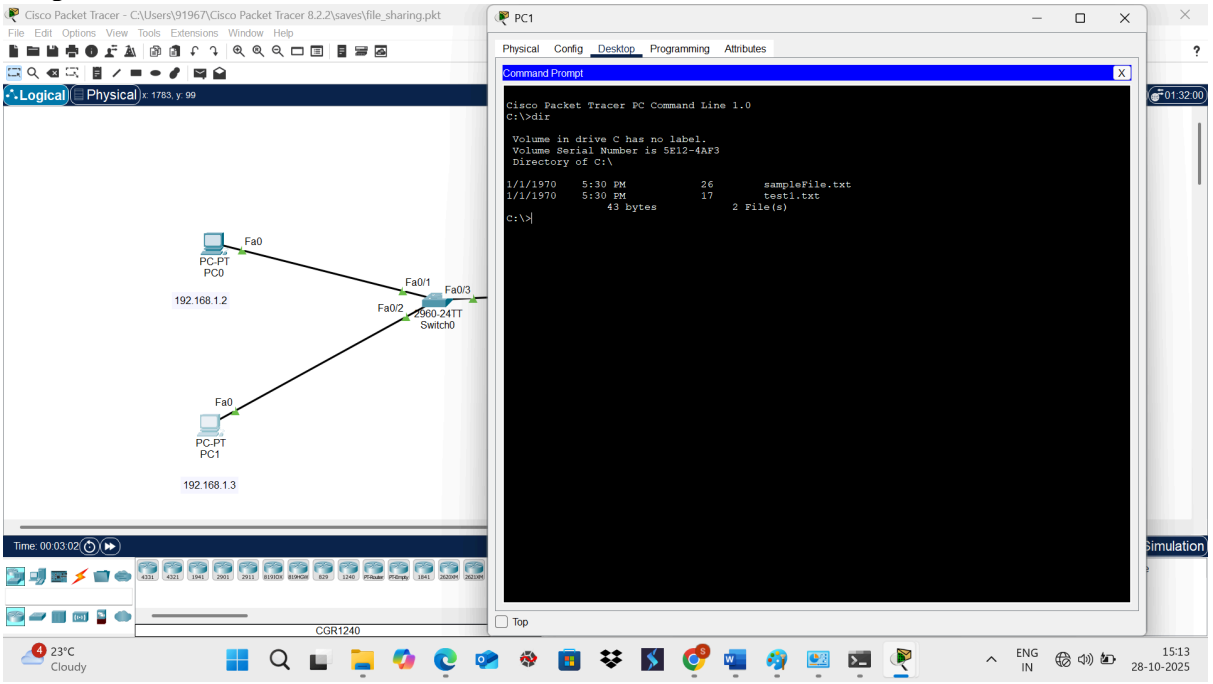
Step -7 Select PC2

a) **Click on Desktop**
b) **Click on Command Prompt C:\> dir Test1.txt no such file will be there in PC2**
c) **C:\> ftp 192.168.1.1 (Enter the IP address of Server to connect Server)**
d) **Give Username and Password**
e) **ftp> get test1.txt (File transferred from Server to PC2)**
f) **ftp> dir (Check the file is transferred to PC2) test1.txt**

Network Topology



Output

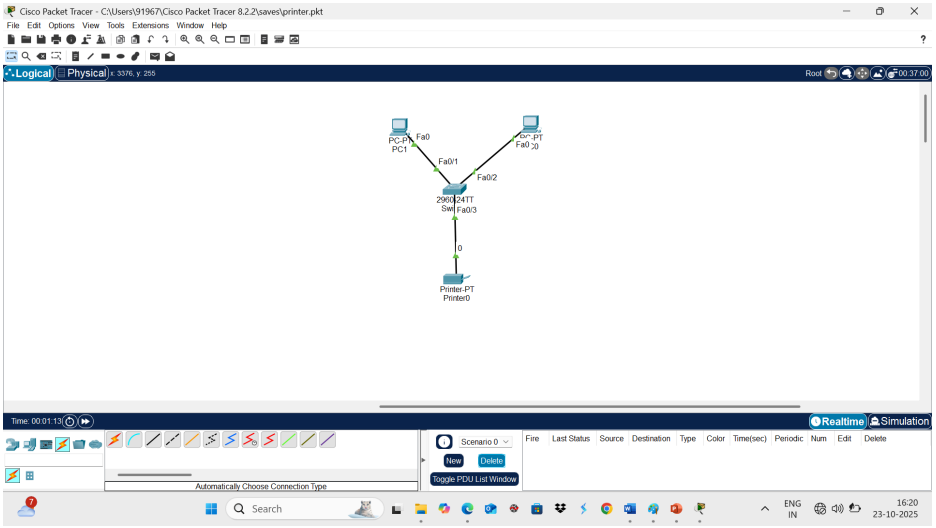


Program 10 : Share the printer in Network, and take print from other PC.

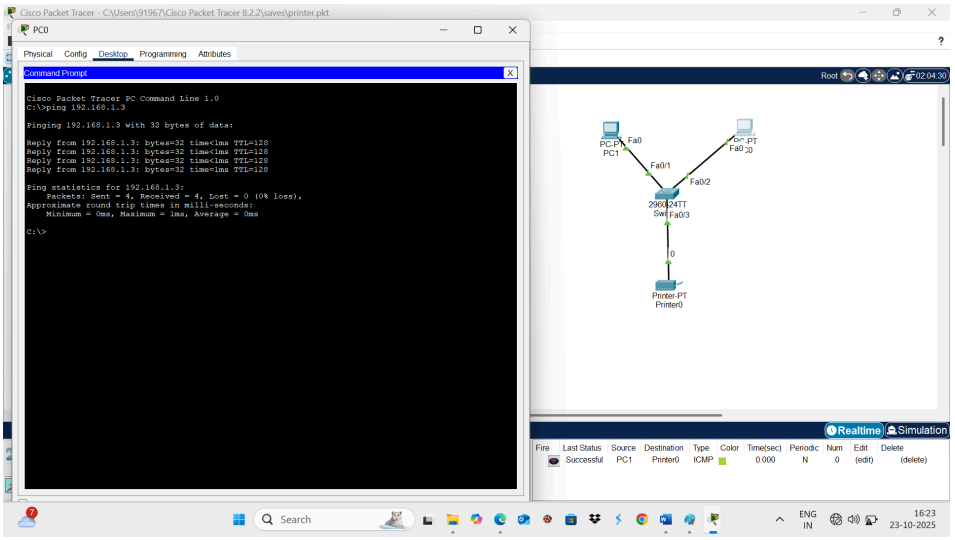
Procedure:

Step -1 Select the 02 - PCs, 01- Printer, 01- Switch by using Drag and Drop
Step -2 Connect all 02 PCs to switch using Straight Through cable and configure IP address as 192.168.1.1 and 192.168.1.2
Step -3 Configure Printer IP 192.168.1.3 and connect to switch using Straight Through cable.
Step -7 Click in any one PC, Click on Desktop, Click on Command Prompt and ping any pc to printer By giving command - > ping IP address(ex 192.168.1.1)

Network Topology:



Output:



Program 11 : Configuration of wifi hotspot, and connect other devices (mobile / laptop).

Procedure:

Step -1 Select 02 - PCs, 01- Printer, 01- Laptop, 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 SSMRV**

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**

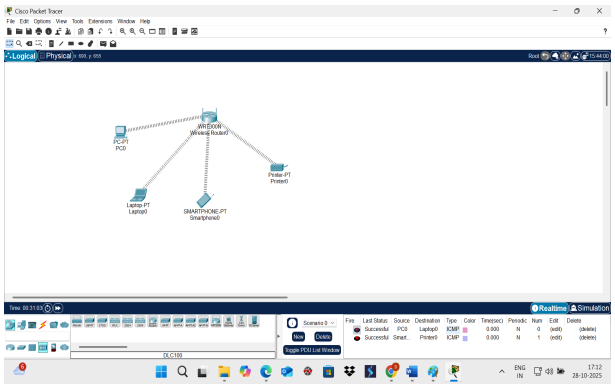
Step - 4 Configure wireless PC

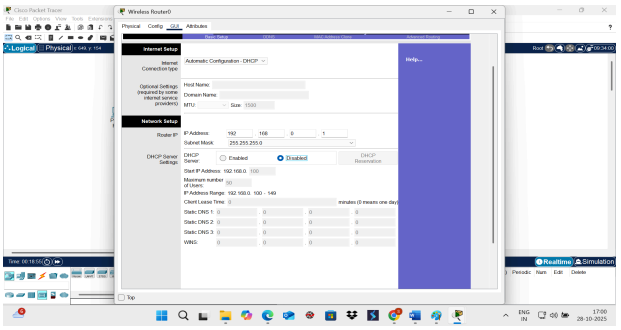
- **Click on desktop**
- **Click on DHCP**
- **Next click on config**
- **Click on wireless0**
- **Click on WPA-PSK and give PSK PASS Phrase (12345678)**
- **Change SSID default to SSMRV**

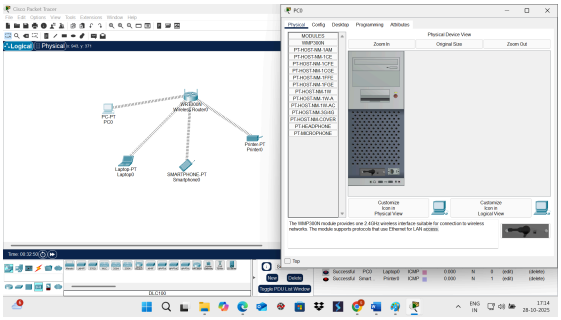
Step -5 Repeat Step 3rd to make Laptop, Printer, Server and Smartphone wireless

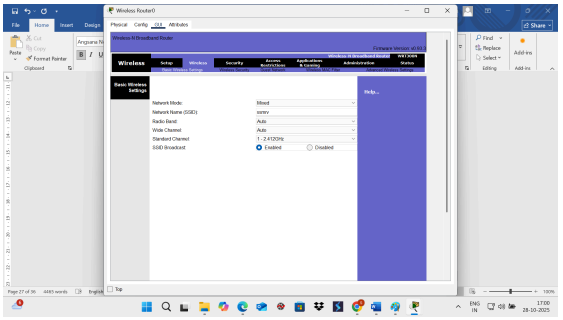
- **Now Wifi connection is ready to ping**

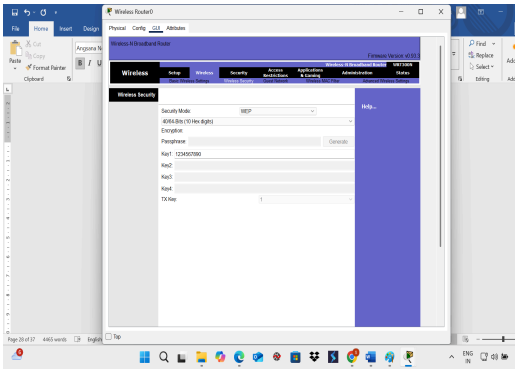
Step - 6 Ping Printer from any Devices Click in any device, Click on Desktop, Click on Command Prompt and ping any pc from printer
By giving command - > Ping IP address
OR
Ping By Realtime or Simulation

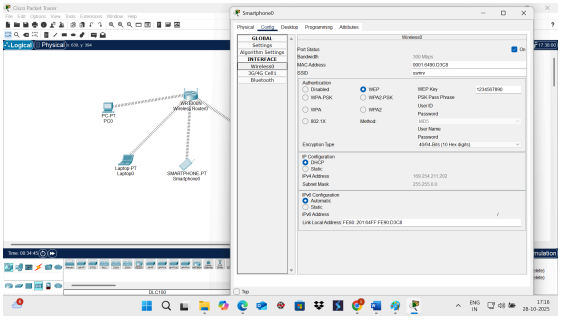




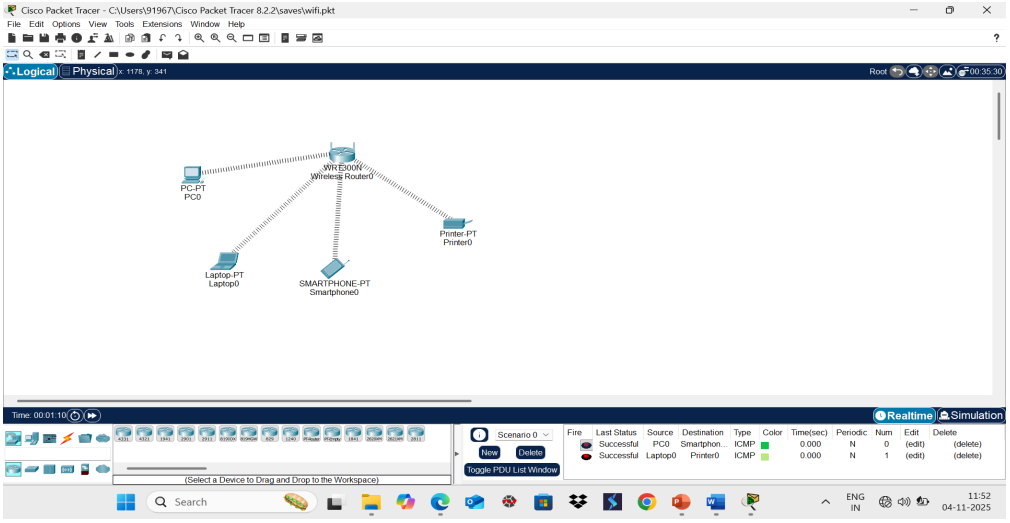








Output:



Program 12: Configuration of switches.

Procedure:

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

3. Configure Switch hostname as SSMRV

Step -1 Switch# configure t

Step -2 Switch(config)# hostname SSMRV

Step -3 SSMRV(config)#

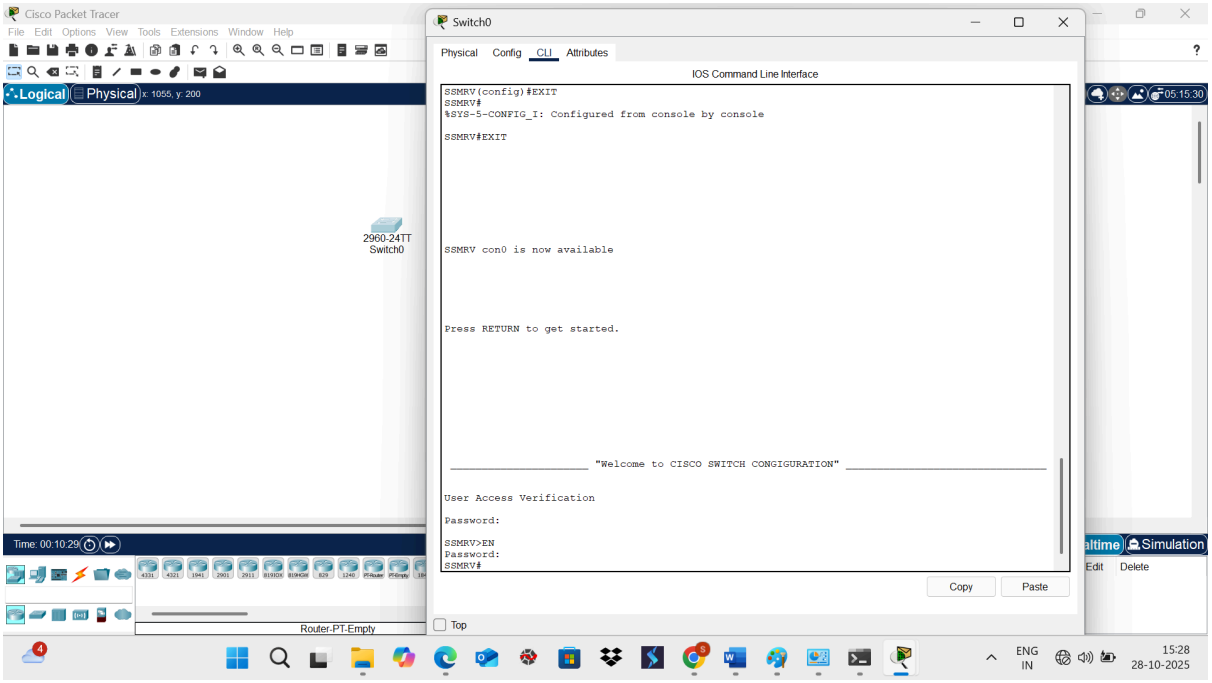
4. Configure the message of the day as

----------"Well Come to CISCO Switch Configuration" ----------

Step -1 SSMRV(config)#banner motd #

---------- "Well Come to CISCO Switch Configuration" ----------

Output:



Program 13 : Configuration of VLAN using Packet Tracer/ GNS3.

Procedure:

Step1: Create Network Topology with 2 Switches and 4 PCs

Step2: Configure IP Address for PC0(192.168.1.5), PC2(192.168.1.2), PC1(10.10.1.1) and PC3(10.10.1.3)

Step3: Click Switch0 -> Click CLI mode

Switch>enable

Switch#configure terminal

Switch(config)#vlan 10

Switch(config-vlan)#exit

Switch(config)#vlan 20

Switch(config-vlan)#exit

Switch(config)#interface fastethernet 0/1

Switch(config-if)#switchport access vlan 10

Switch(config-vlan)#exit

Switch(config)#interface fastethernet 0/2

Switch(config-if)#switchport access vlan 20

Switch(config-vlan)#exit

Switch(config)#interface fastethernet 0/3

Switch(config-if)#switchport mode trunk

Switch(config-if)#exit

Step4: Click Switch1 -> Click CLI mode

Switch>enable

Switch#configure terminal

Switch(config)#vlan 10

Switch(config-vlan)#exit

Switch(config)#vlan 20

Switch(config-vlan)#exit

Switch(config)#interface fastethernet 0/3

Switch(config-if)#switchport access vlan 10

Switch(config-vlan)#exit

Switch(config)#interface fastethernet 0/2

Switch(config-if)#switchport access vlan 20

Switch(config-vlan)#exit

Switch(config)#interface fastethernet 0/1

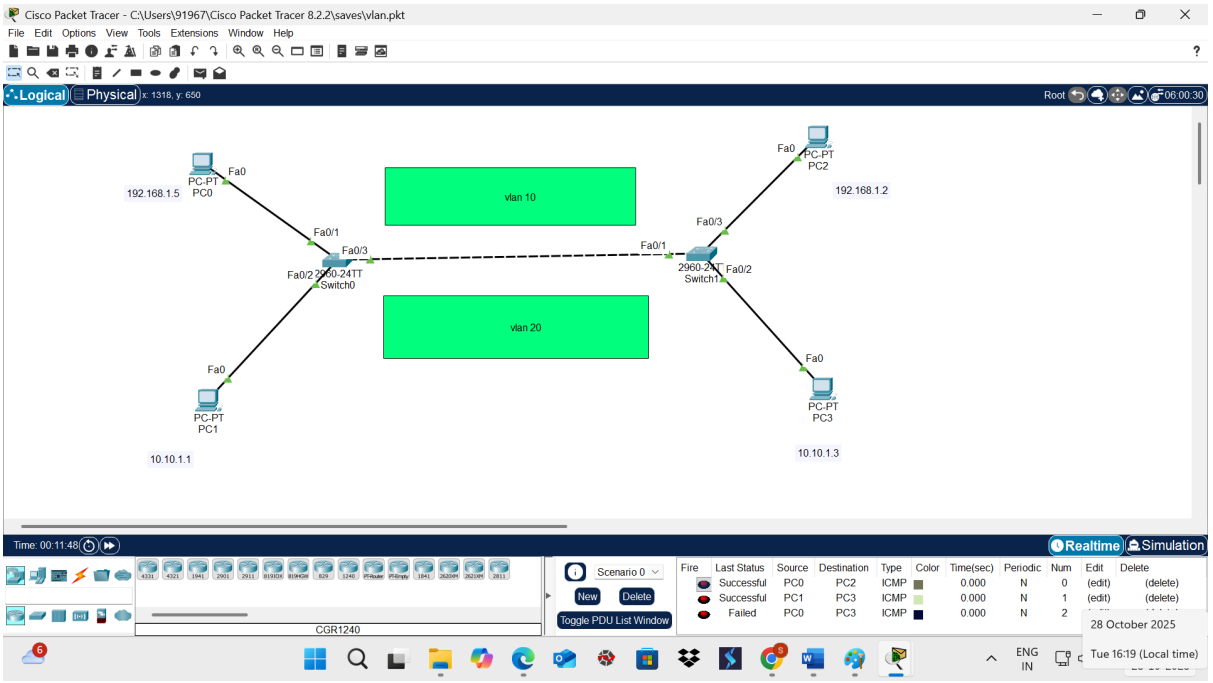
Switch(config-if)#switchport mode trunk

Switch(config-if)#exit

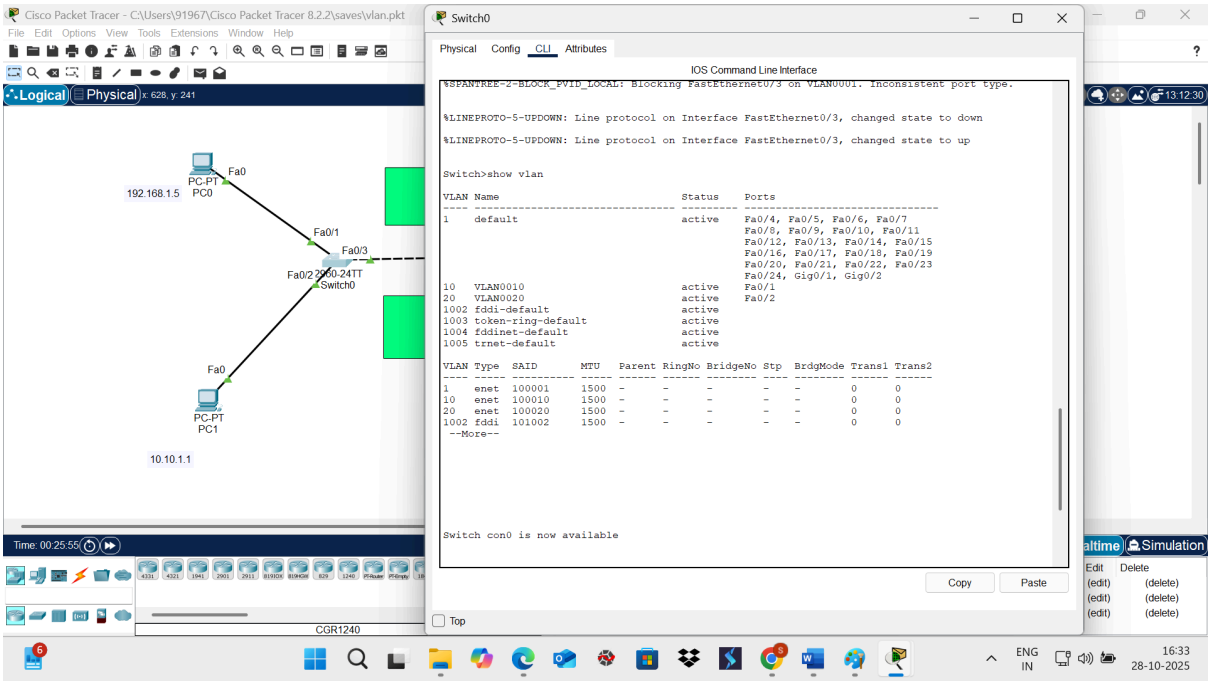
Step5: check vlan configuration using **show vlan** command

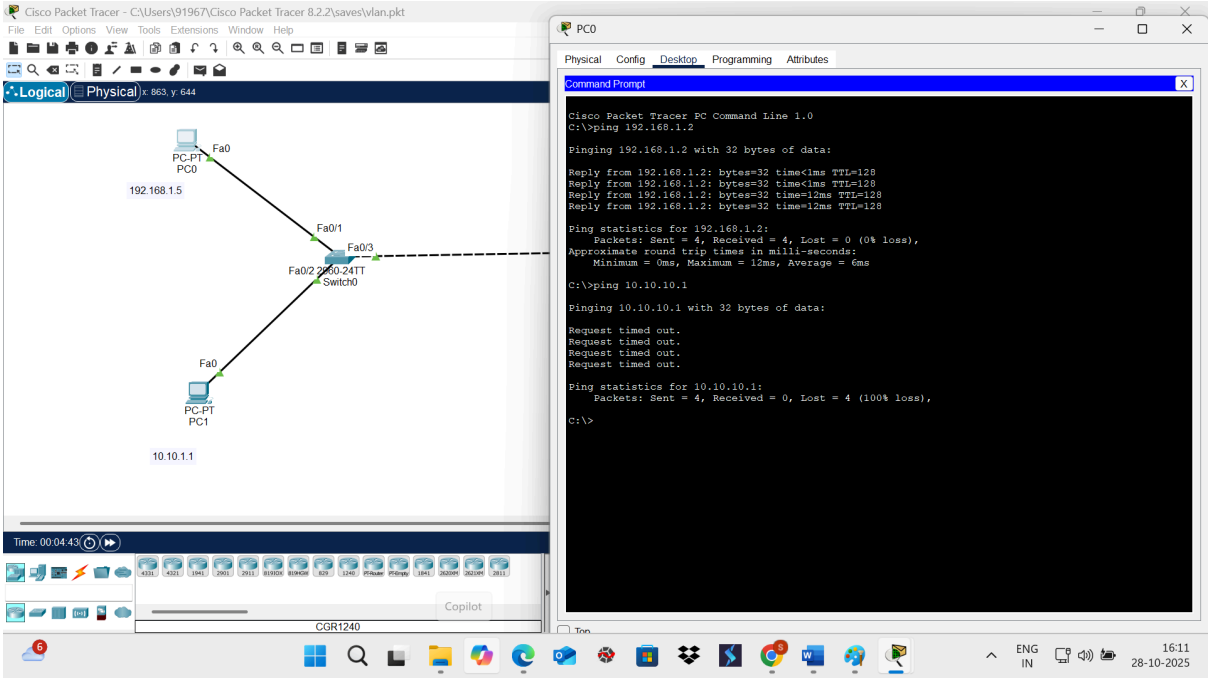
Step6: Check the output using ping command from pc1-pc3 and pc0-pc2

Network Topology:



Output:


Switch0
Physical Config CLI Attributes
IOS Command Line Interface
%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/3 on VLAN0001. Inconsistent port type.
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
Switch>show vlan
VLAN Name Status Ports
1 default active 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
10 VLAN0010 active Fa0/1
20 VLAN0020 active Fa0/2
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
1 enet 100001 1500 - - - - - 0 0
10 enet 100010 1500 - - - - - 0 0
20 enet 100020 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
--More--
Switch con0 is now available
Copy
Paste
Top
192.168.1.5
PC-PT PC0
Fa0
Fa0/1
Fa0/3
Fa0/2 2950-24TT Switch0
PC-PT PC1
10.10.1.1
Time: 00:25:55
CGR1240
Edit Delete
(edit) (delete)
(edit) (delete)
(edit) (delete)
ENG IN
16:33
28-10-2025


PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=12ms TTL=128
Reply from 192.168.1.2: bytes=32 time=12ms TTL=128
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 12ms, Average = 6ms
C:\>ping 10.10.10.1
Pinging 10.10.10.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.10.10.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top
192.168.1.5
PC-PT PC0
Fa0
Fa0/1
Fa0/3
Fa0/2 2950-24TT Switch0
PC-PT PC1
10.10.1.1
Time: 00:04:43
CGR1240
Copilot
ENG IN
16:11
28-10-2025

Program 14 : Configuration of VPN using Packet Tracer/ GNS3

Procedure:

Step 1: Create Network Topology with 2 PCS and 3 Routers

Step 2: Configure IP Address for all devices

Device	Interface	IP Address	Default Gateway
PC0	Fa0	192.168.1.2	192.168.1.1
PC1	Fa0	192.168.2.2	192.168.2.1
Router0	Gig0/0	192.168.1.1	-
	Gig0/1	1.1.1.1	-
Router3	Gig0/0	1.1.1.2	-
	Gig0/1	2.2.2.2	-
Router2	Gig0/0	2.2.2.1	-
	Gig0/1	192.168.2.1	-

Step 3: Click on Router 0

Router# config t

Router(config)#interface tunnel 1

Router(config-if)#ip address 50.50.50.1 255.0.0.0

Router(config-if)#tunnel source Gig0/1

Router(config-if)#tunnel destination 2.2.2.1

Router(config-if)no shut

Step 4: Click on Router 2

Router# config t

Router(config)#interface tunnel 1

Router(config-if)#ip address 50.50.50.2 255.0.0.0

Router(config-if)#tunnel source Gig0/0

Router(config-if)#tunnel destination 1.1.1.1

Router(config-if)no shut

Step -5 Router 0

Click on Config - > Click on Static - > Add

Network - 0.0.0.0

Mask - 0.0.0.0

Next Hop - 1.1.1.2

Click on Config - > Click on Static - > Add

Network - 192.168.2.0

Mask - 255.255.255.0

Next Hop – 50.50.50.2

Step -6 Router 2

Click on Config - > Click on Static - > Add

Network - 0.0.0.0

Mask - 0.0.0.0

Next Hop – 2.2.2.2

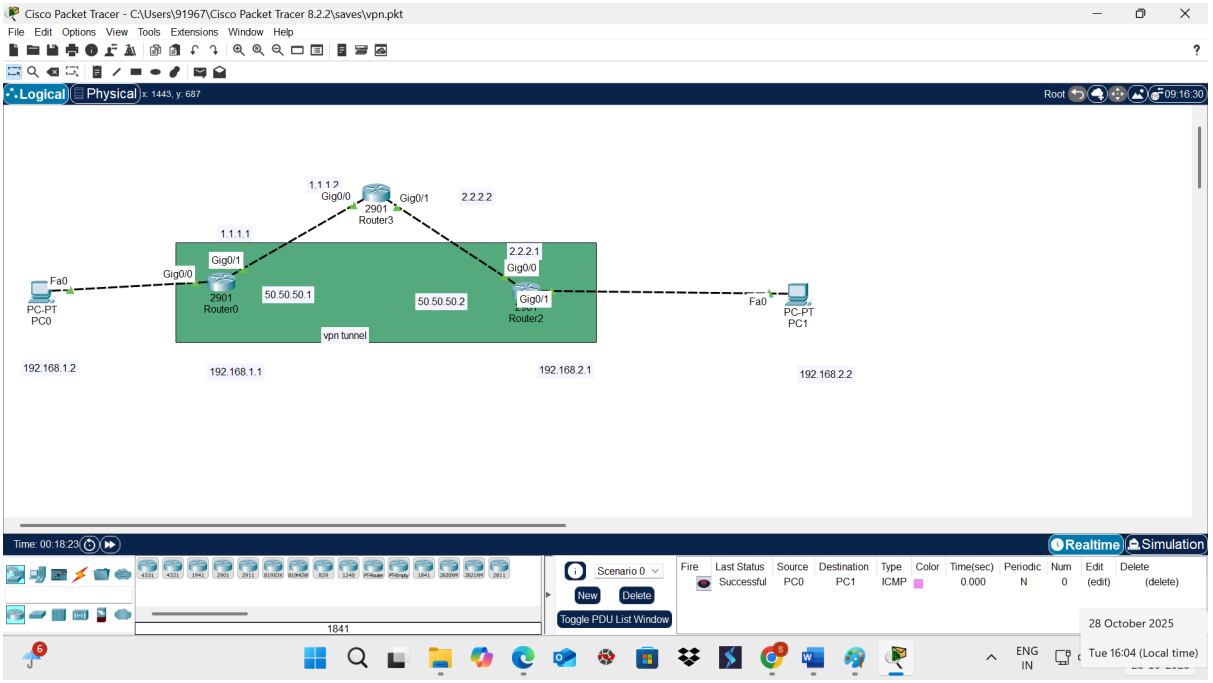
Click on Config - > Click on Static - > Add

Network - 192.168.1.0

Mask - 255.255.255.0

Next Hop – 50.50.50.1

Network Topology



Output