**List of CN experiment**

1. Use basic networking commands in Command Prompt

**🧠 Most Useful for Students:**

* ipconfig → Check if you got an IP.
* ping 8.8.8.8 → See if you have internet.
* ping [router IP] → Check local connectivity.
* tracert google.com → Understand how packets travel.
* nslookup google.com → See DNS resolution.
* getmac -> gets mac address of router
* Ipconfig /all, ipconfig /release, ipconfig/renew

1. Build a simple network topology and configure it for static routing protocol using packet tracer. Setup a network and configure IP addressing, subnetting, masking.
2. Use Wire shark to understand the operation of TCP/IPlayers: ● Ethernet Layer: Frame header, Frame size etc. ● Data Link Layer: MAC address, ARP (IP and MAC address binding) ● Network Layer: IP Packet (header, fragmentation),ICMP (Query and Echo) ● Transport Layer: TCP Ports, TCP handshakesegments etc. ● Application Layer: DHCP, FTP, HTTP headerformats
3. Implement the Hamming code using C
4. Perform Remote login using Telnet server using Cisco Packet Tracer

1 Router (or Switch)

1 PC

Straight-through cable (PC ↔ Router/Switch)

Click on Router/Switch → CLI

enable

configure terminal

interface gigabitethernet 0/0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

line vty 0 4

password cisco

login

exit

enable password class

service password-encryption

#Click the PC → Desktop → IP Configuration:

#IP Address: 192.168.1.2

#Subnet Mask: 255.255.255.0

#Default Gateway: 192.168.1.1

On the PC → Desktop → Command Prompt:

telnet 192.168.1.1

1. To perform basic configuration tasks on Cisco routers and switches using the IOS CLI, including setting hostnames, configuring and encrypting enable passwords, verifying configurations, and saving them to startup configuration. (**DAY 4 -LAB YOUTUBE)**

For router

Press enter and type these commands

* en
* ex
* press enter again
* en
* conf t
* hostname R1
* enable password CCNA
* exit
* exit
* note: then type ur password to check if its working (which is CCNA in this case)
* sh run
* conf t
* service password-encryption
* do sh run
* enable secret cisco
* exit
* exit
* then itll ask for ur password again enter it as cisco this time
* sh run

1. To analyze network traffic using Packet Tracer’s simulation mode by observing various protocol data units (PDUs) across different layers of the OSI and TCP/IP models, including STP, OSPF, and DHCP operations. **(DAY 3 -LAB YOUTUBE)**

**Summary Table:**

| **Protocol** | **Purpose** | **Device Used On** | **Key Function** |
| --- | --- | --- | --- |
| **STP** | Avoid switching loops | Switches | Blocks redundant links |
| **DTP** | Auto-negotiates trunk links | Switches | Forms VLAN trunks |
| **OSPF** | Dynamic routing | Routers | Finds best route |
| **DHCP** | Auto IP address assignment | Routers/Servers | Gives IPs to PCs |

1. To analyze ARP and ICMP message flow during network communication, learn MAC address table population in switches, and practice clearing dynamic MAC address entries using simulation and real-time modes in Packet Tracer. (**DAY 6 – LAB YOUTUBE)**

* Send an arp request from PC1 which will be received by all devices and PC3 will send a reply only to Pc1
* Then PC1 will send and ICMP msg to PC3 and PC3 will send an ICMP reply to PC1
* Then u click simulation mode
* Open PC1, go to command prompt and type ping 192.168.1.3
* Then in the sim tab you’ll the outbound PDU details with 0806 which is for arp table and FFFFFFFFFFFFF which is for an outbound message
* Then keep pressing the forward button in simulation showing how the arp request echoes around and ICMP is forwarded and then show the play button
* Then go to SW1->CLI-> type en-> show mac address-table
* Do the same for SW2 as SW1 will show for PC1,2 to which it is attached

1. To design and implement a network topology using appropriate copper (straight-through and crossover) and fiber-optic connections between PCs, switches, and routers, considering transmission standards and cable selection based on device types and distance limitations. (**DAY2 LAB-youtube)**

**PCs transmit data on pins 1 and 2 and receive data on pins 3,6 switches r the opposite**

**U can use a straight cable for pc->switch and crossover cable for switch->switch**

1. Set up multiple IP addresses on a single LAN. Using nestat and route commands of Linux, do the following: • View current routing table • Add and delete routes • Change default gateway Perform packet filtering by enabling IP forwarding using IPtables in Linux.

# Assign 2 IPs to eth0

sudo ip addr add 192.168.1.10/24 dev eth0

sudo ip addr add 192.168.1.11/24 dev eth0

# Show routing table

ip route

# Add and delete a route

sudo ip route add 192.168.2.0/24 via 192.168.1.1

sudo ip route del 192.168.2.0/24

# Change default gateway

sudo ip route replace default via 192.168.1.1

# Enable IP forwarding

sudo sysctl -w net.ipv4.ip\_forward=1

# Basic packet filtering with iptables

sudo iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT

sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

1. Perform File Transfer and Access using FTP.

# Install FTP server

sudo apt update

sudo apt install vsftpd -y

# Start & enable service

sudo systemctl start vsftpd

sudo systemctl enable vsftpd

# Allow FTP through firewall (if UFW is used)

sudo ufw allow 20/tcp

sudo ufw allow 21/tcp

# Create FTP user

sudo useradd -m ftpuser

echo "ftpuser:password" | sudo chpasswd

# Set FTP directory permissions

sudo mkdir -p /home/ftpuser/ftp

sudo chown nobody:nogroup /home/ftpuser/ftp

sudo chmod a-w /home/ftpuser/ftp

# Restart vsftpd

sudo systemctl restart vsftpd

ftp <server\_ip>  
ip addr show eth0 #for finding server ip