13/7/24
EX NO: 1

STUDY OF VARIOUS NETWORK COMMANDS IN WINDOWS

Aim:

Study of Various Network Commands used in Linux and windows.

Basic Network Commands:

arp -a: ARP or address resolution protocal reveals the IP address of your Computer alongwith the IP address of your router

output:

Interface: 172.16.75.14 ... 0x12.

Internet Address	Physical Address	Type
172.16.72.1	7C-5a-1C-cf-be-41	dynamic.
172.16.72.133	ac-ac-a3-65-97-f3	dynamic.
172.16.72.195	4c-ae-a3-64-fC-50	dynamic.
172.1675.3	4C-82-a9-78-90-e5	dynamic.

hostname: Simplest of all TCP/IP Commands It Simply display the name.

output:

DESKTOP-C01BH7D.

ip Config/all: This Command display dele Configuration including the router, gateway, DNS, DHCP Settings and the type of ethernet adapter in your System.

output:

Window IP Configuration.

Host name ..... : Desktop-C01BH7D.
Primary Dns Suffix . . .
Node Type ... NO
IP Routing Enabled ..... No
WINS Proxy Enabled ... No

nbtstat -a : This Command helps to solve problems with Net BIOS name, resolutions (Nbt, stands for Net BIOS over TCP/IP)

output :

Display protocal statistics and, current TCP/IP Connections using NBT (Net BIOS over TCP/IP).

NBTSTAT [[-a Remote Name] [-A IP address] [-c] [-n] [-r] [-R].

-a (adapter status) List the remote machines given its name.

-A (adapter status) List the remote machines given IP address

netstat : Netstat is a Command-line tool that displays statistics about a Computer's active TCP/IP Connection, routing tables, and interface statistics

Example : netstat -r.

output :

Interface list

19.....1e ce 51 77 db f8 ... Microsoft wifi VR Adapter

14.....12 ce 51 77 db f8 .... Microsoft wifi direct VR #2

17.....1c ce 51 77 db f8 .... Realtek RT28852BE wifi 6. 802.11ax.

1.....Software loopback Interface 1.

nslookup : nslookup is a linux tool for DNS lookups showing details, like IP address MX records for email servers and it's records for name servers.

output :

Server : unknown.

Address : 2401:4900:50:9:280

Non-authoritative answer.

Name : www.google.com

Address : 2401:6800:4009:819::2004

142.250.195.132.

Pathping : Pathping is a windows command that combines 'ping' and 'tracert'. It traces the route to a destination address and tests each router along the way.

output :

usage : Pathping [-g host-list] [-h maximum] [-P period] [-4] [-6]

options :

-g host-list Loose source route along list
-i address use the specified source address
-n donot resolve addresses.

SOME IMPORTANT LINUX NETWORKING COMMANDS:

1 IP; The 'ip' command is essential for administrators used daily for tasks like seting up systems, assigning IPs, and troubleshooting.

ip <OPTIONS> <OBJECT> <COMMAND>

Some Comman use cases for the ip Command

a) To show the IP address assigned to an interface on your server.

ip address show.

OUTPUT

2: enp250: <BROADCAST, MULTICAST, UP, LOWER, UP>
mtu 1500 qdisc fq-codel state up group default qlen
1000 link/ether 50:9a:4c:35:11 44. brd.

b) To assign an ip to an interface, for example enp:250:

ip address add 192.168.1.254.124 dev enp 250.

c) To delete an ip on an interface

ip address del 192.168.1.254/24 dev

d) Alter the status of the interface by bringing the interface online.

ip link set enp 250 up.

e) Alter the status of the interface by bring the interface offline.

ip link set enp 250 down.

f) [root@ server N] +1 ip link set down The status of an interface is altered by enabling promis on mode.

g) [root @ user N] # ip route add default via 192.168.1.254 dev.

h) [root @ server n] # ip route add 192.168.1.0120 via 192.168.1.254.

i) [root@server] # ip route add 192.168.1.24 dece

A route is added to 192.168.1.0124 that can be reached on the device used

ii) [root@server1 v] # ip route del 192.168.1.0124. Via 192.168.1.254.

The route is deleted for the route 192.168.1 OR

iii) [root@server N] # ip route get 10.10.14.

10.10.1.4 Via 172.16.8.1 dev exp 250 172.16.8.19 cid 0 code.

2; ifconfig:

The ifconfig command was / is a staple in many Sysadmin's tool but for configuring and troubleshooting networks.

OUTPUT:

exp 160: flags = 4163<UP. BROADCAST, RUNNING.)

must 1500 inet 192.168.247.130 netmask 255.255.0

Rx packets 45 bytes 6072 (5.9 KiB)

Rx errors 0 dropped 0 overruns 0 frame 0.

3) mtr;

MTR (Matis traceroute) is a command line tool for network diagnostics, combining the functionality of ping and traceroute.

mtr <options> hostname/IP.

Some common use cases:

a) This basic mtr command shows you the statistics including each hop (hostnames) with time and loss%.

mtr google.com

output:

My traceroute [v0.95].

fedora (192.168.247.130) → google.com (142.250.195.174)

keys: Help display mode restart statistics order of fields quit.

	Packets		Pings	
Host	Loss%	Snt	Last	Avg Best
1. -gateway				
2. (waiting for replay)				
3. (waiting for replay)				
4) (waiting for replay				
5. (waiting for replay)				

b)

mtr: invalid option -- 'g'

usage:

mtr [options] hostname.

-F, --filename FILE.

-4

-6

-u, --udp

-T, --TCP.

4) tcpdump.

The tcpdump command is designed for capturing & displaying packets installing tcpdump.

dnf. install -y tcpdump.

Last metadata expiration check: 0:05:39 ago on Sat 27 Jul 204 23:21:59 IST.

tcpdump -D

output

1, ens1s0 [up, Running, connected]

2, any (Pseudo - device that Captures on all interfaces)

3, lo [up, running, loopback]

4, Bluetooth - monitor

tcpdump -i eth0

output

dropped privs to tcpdump.

tcpdump: Verbose output Suppressed, use for full. Protocol decode listening on ens160 link-type EN10MB (Ethernet), Snapshot length 262144 bytes.

tcpdump -i ethce -c10.

Capture traffic to and from one host you can filter out traffic Coming from Specific host

tcp dump -i eth0 -c10 host 8.8.8.8.

droped privs to tcpdump.

tcp dump: verbose output Suppressed.

use -v[v] ... for full tcpdump: Verbose.

tcpdump -i -eth0 dst host 8.8.8.8.

Capture traffic to and from a network

dropped privs to tcpdump.

tcp dump: verbose output Suppressed, use -v[v]... for full protocal decode listening on ens160, link-type EN10MB.

5, Ping:

Ping is a tool that Verifies IP Connectivity by Sending ICMP echo request message and displ the receipt of echo reply message with rou times.

Ping google.com

Ping google.com (142.250.195.174) 56 (84) bytes of data
64 bytes from maa03s41-in-f14.1e100.net (142.250.195.174)
10 packets transmitted, 10 received, 0% packets time 9016
ms:

Configuring an ethernet Connection by using nmcli

If you Connect a host to the network over ethernet you can manage the connection settings on the Command line by using the nmcli utility.

23/11

Result:
Thus the Study of various network Connections used in linux and windows done and executed successfully

EXNO:2 STUDY OF DIFFERENT KINDS OF NETWORK CABLE.

Aim:

To Study the different types of Cables

a, understand different types of network Cable.

1, unshielded Twisted pair (UTP) Cable

2, Shielded Twisted Pair (STP) Cable

3, Co-axial Cable.

4, Fibre optic Cable.

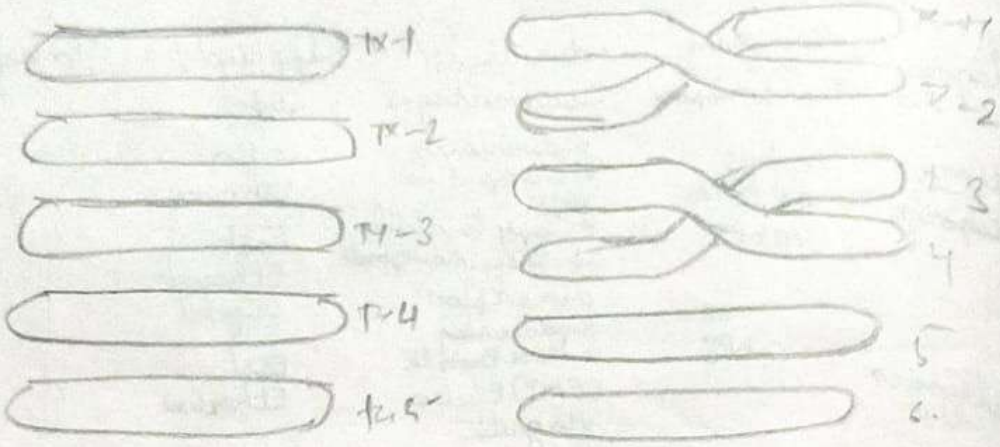
Cable Type	Category	Maximum data transmission	Advantages/ Disadvantages	Applied / use	Image
UTP	Category 3	10 bps	Advantages * Cheapest in cost * Easy to install as they have small dimension Disadvantage * More Prone to (EMI) Electro Magnetic	10 Base-T Ethernet	
	Category 5	up to 100 MbPS.		Fast Ethernet Gigabit-	
	Categoger	1 GbPS		Fast- Ethernet	
STP	Category 6, 6a	10 GbPS	Advantages : * Shielded * Faster than UTP * Less Susceptible	Gigabit Ethernet 10G (55M) widely used in data Centre	
SSTP	Category 7	10 GbPS	Disadvantages * Expensive * Greater installation effort	Gigabit Ethernet 10G Ethernet (100 m)	
Coaxial Cable.	RG-6 RG-59 RG-11	10 - 100 MbPS	Advantages * High Bandwidth * Online to Interface * Versatile Disadvantage * Limited distance * Cost	Speed of signals used in television network High speed interface Connections	
fibre optics Cable	Single Mode	100	Advantages: * High Speed * High bandwidth * Long distance Disadvantages * Expensive * Required	Maximum distance of fibre optics cable is 100 meter	
	Multi Mode	GbPS			

b, Make your own ethernet cross-over cable & Tools and Tests needed

*) Ethernet Cabling - CAT5E is certified for gigabit support but CAT5E is certified for gigabit shorter distance.

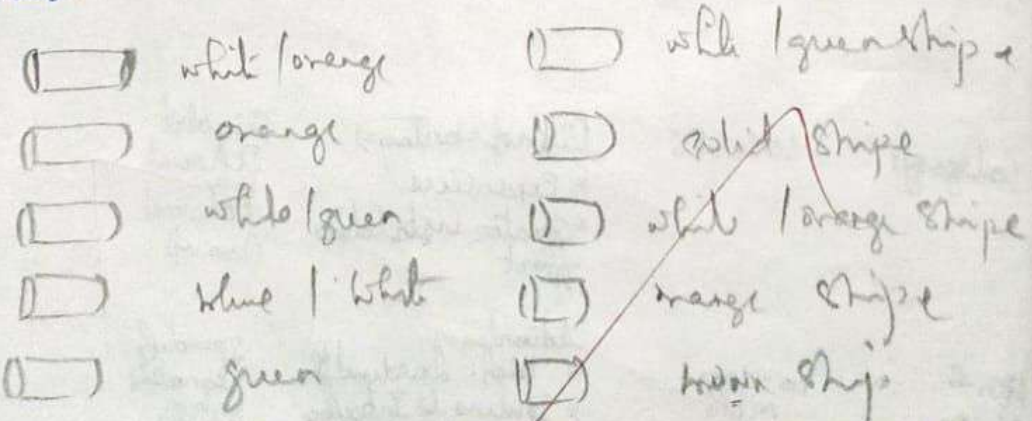
* Two RJ45 plugs.
* optional two plug shields.

Straight thru Cable.



Difference between Crossover cable and Straight Cable

Straight through network Cable both sides should be a cross over cable.



Step 1: To start construction of the device, begin by threading shields on to the cable.

Step 2: Next, strip approximately 1.5 cm of cable shielding from both the ends - The crimping tool has a area to complete this task.

Step 3: After, you will need to the wires there should be four twisted pairs "Reforming Back to the that, arrange them from top to bottom.

Step 4: Next, push the cable right in the at the end of the plug needs to just crence over the Cable sheilding and if it isn't that means that you stripped off too much sheilding

Step 6: After the wires once securely sliding the plug insert it into Crimping tool and push down.

Result

This the study of different type of networking cables once studied and the implement successfully

EX.NO:1

STUDY OF PACKET INTERFACE

Aim: To study the packet tracer tool installation and user interface overview.

c) To understand environment of cisco packets Tracer.

Introduction:

Simulator, as the name suggests simulates network and it's environment Packet Tracer is an existing network design.

1. It allows you to model complex systems without the need for dedicated equipment.
2. It available for both the linux and windows desktop.
3. Both cal is packet tracer and coded towards and behave in same way.

Installing packet Tracer.

To download packet tracer, go to https://www.netacad.com and login is with your CISCO networking Credentials ; then click on the Packet Trace graphic.

WINDOWS:

Installation in windows pretty simple a straight forward the setup comes in a single file named packettracer_setup_6.0.1.exe open file

LINOX:

Linux user with ubuntu/Debia distribute should download .tb file using fedora must download the file

USER INTERFACE OVERVIEW

The layout of packet Tracer is divided into Several Components.

The Components of the packet Tracer interface

1) Menu bar: This is a Common menu found in all Software application, it is used to open

2) Main toolbar: This box provide Shortcut icons to menu option that are Commonly accessed, Such as open, Save, Zoom etc.

3) Logical / Physical workshop tabes: These tabes allow you between logical & physical workshop

4) workshop - this is the area when topologies are created.

5) Common tool -

bar - This tool bar provide Control for manipulating topologies

6) Realtime / Simulation

tabs: These tables are used between the real and Simulation mode.

7) Network Component.

box - This Component Contains all of the network and end devices.

2) Analyse the behaviour of network devices using CISCO PACKET TRACER.

1) From network Component box click and drag and drop the below Components
   a, 6 end to PCs & one HUB.
   b, 4 Enter PCs & one Switch.

2) click on Connections
   a, click on Copper Straight through Cable
   b, Select of PC and Connect HUB with Cable
the link LED should glow in green.

3) click on PCs Connected to hub, go to the desktop tab, click on IP Configuration, and enter IP address and and Subnet mask are only two end devices in the network

4) observe the flow of PDU from source PC to destination PC by selecting the realtime mode

5) Repeat Step 3 to Step 5 for PCs connected to Switch.

6) observe how HUB and Switch the PDU and write your observation and conclusion about the behaviour of Switch & HUB.

Result:
Thus the execution of CISCO packet tracer is verified and implemented Successfully and noted.

Practical - 1

Student observation:

1. which command is used to find the reachability of a host machine from your machine

Command to find the reachability of a host machine from your device

* Ping <hostname or IP address>

2. which command will be given the details of hops take by a packet to reach it's destination?

Command to get the details of taken by a packet to reach it's destination

Track route <hostname or IP address>.

3. which commands display the IP configuration of your machine?

* ifconfig (Linux) · unix, older versions)
* ip addr (Linux (unix, newer versions)
* ip config (windows)

4 which commands displays the TCP port states in your machine.

netstat -tuln

ss -tuln

5. write the modify ip configuration in a MAC machine

using ifconfig (old method)

using ip (Modern method)

Sudo ip addr add 192.168.1.10/24 dev

Sudo ip route add default via 192.168.1.1

Practical - 1

Student observation:

1. which Command is used to find the reachability of a hosh machine from your machine

Command to find the reachability of a host machine from your device

* Ping <hostname or IP address>

2. which Command will be given the details of hops take by a packet to reach it's destination?

Command to get the details of Taken by a packet to reach it's destination

Track route <hostname or IP address>.

3. which Commands display the IP Configuration of your machine?

* ifconfig (Linux). unix, older versions)
* ip addr (Linux (unix, newer versions)
* ip config (windows)

4 which Commands displays the TCP port states in your machine.

netstat -tuls

ss -tuln.

5. write the modify ip Configuration in a MAC machine

using ifconfig (old method)

using ip (Modern method)

Sudo ip addr add 192.168.1.10/24 dev

Sudo ip route add default via 192.168.1.1

Practical - 2

Student observation:

1) What is the difference between cross cable straight cable?

*) All the wires are in the same order on both ends of the cable

*) used to connect different types of devices

cross cable

*) used to connect similar device directly.

2) which type of cable similar device directly router/ switch to your PC?

Straight cable:

*) used to connect a PC to router or switch

3) which type of cable is used to connect two PC cross cable.

*) used for direct PC to PC connection & without a hub switch or router.

4) find out the category of twisted pair cable used in your labe to connect the PC to the network socket

Category 5: Supports upto 10GBPS for short distance

5) write down your understanding challenges faced and output received while making a twisted pair

Straight Cable:

→ used to connect diff type of network devices.

Cross Cable:

→ used to Connect diff. Types of network device

challenges faced:

*) Crimping Issues,
*) wire order
*) Testing.

output recived:

Successfully made Cable

Practical - 3

Student observation:

1) From your observation write down the behaviour of switch and HUB in terms of forwarding the packets received by them.

HUB:

- Broadcasting:
  - → A hub is a basic networking device that operates at the physical layer of the OSI model
  - → This behaviour results in all devices connected to the HUB receiving the packets, even if they are not recipient.
  - → This behaviour result in all devices connected to the HUB receiving the packets, even if they are NOT the intended recipient.

SWITCH:

- Intelligent Forwarding:
  - → A switch operate at the data link layer of the OSI model
  - → when a switch receives a packet it examines the MAC address of the destination device
- collision Domain:
  - → Each port on a switch represent a separate collision Domain.
  - → This Isolation significantly reduce the likelihood of collision. Compared to hub

6. Find out the network topology Implement in your College and draw and label the topology in your notebook.

Star topology -

→ All devices are connected to a Central Switch or hub

→ This is one of the most common and widely used topologies in moden networks due to it's simplicity and efficiency -

Ex No 6

Aim:
Setup and configure a LAN (Local Area Network) using a Switch and ethernet cables in your class.

What is LAN?

A local Area Network refers to a Network that connects devices within a limited area, such as an office building, school or home. It enables users to share resources, including data, printers and internet access.

How to Setup LAN:

① - Plan & Design an appropriate Network topology taking into account Network requirements and equipment location.

② - Take 4 Computers, a Switch with 8, 16 or 24 ports with is sufficient for Network of their sizes and 4 ethernet cables.

③ Connect your Computers to Network Switch via an Ethernet Cable.

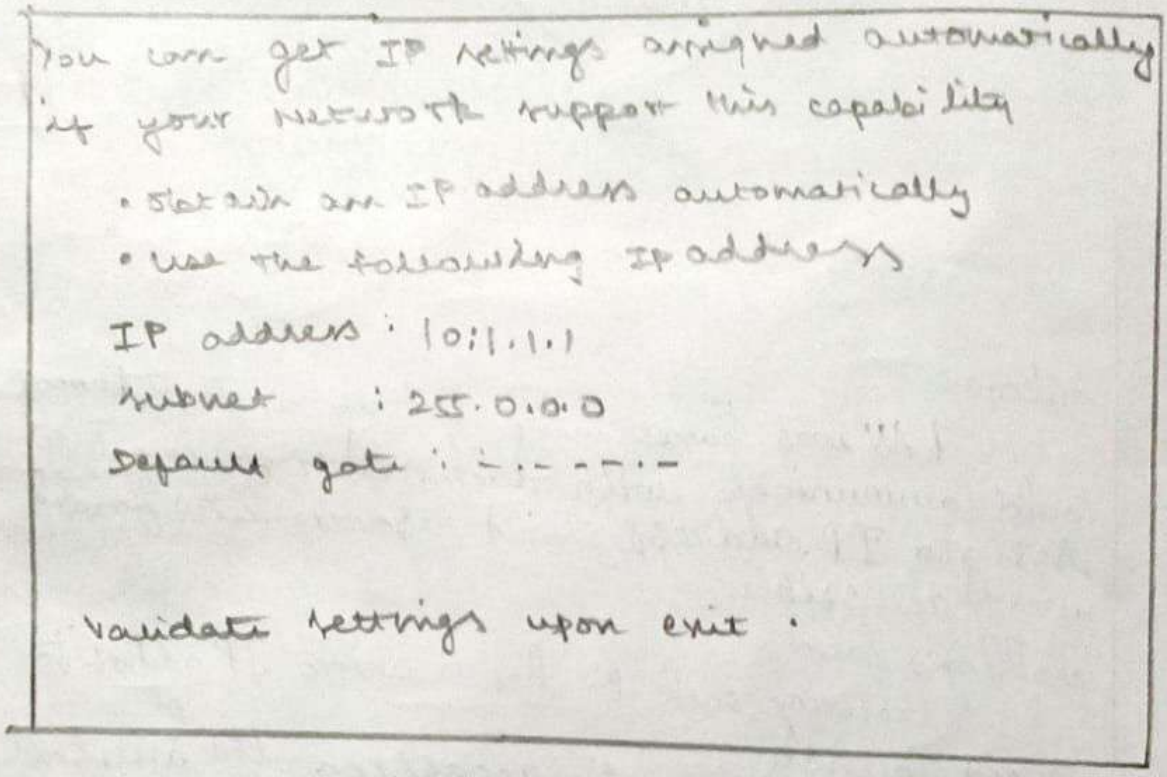
④ Assign IP Address to your PC's
↳ log on to the client computer as admin or as owner
↳ click Network and Internet Connections.
↳ Right click local Area Connection Ethernet's or to properties → Select Internet Protocol (TCP/IPv4)
↳ click on properties → Select use the following IP address option and assign IP address

⑤ - Configure a Network Switch.
↳ Connect your Computer to the Switch to Switch's web Interface, your will need to Connected your Computer to the Switch using an ethernet Cable
↳ Login to the Web Interface.
↳ Configure basic Settings.
↳ Assign IP address as 10.1.1.5; Subnet Mask:

⑥ check the Connectivity between switch and other machine by using ping command in the Command prompt of the device

⑦ - Select a folder → go to properties → click Sharing tab → share it with everyone on the same lan

⑧ Try to a access the shared folder from other Computeress of the Network.



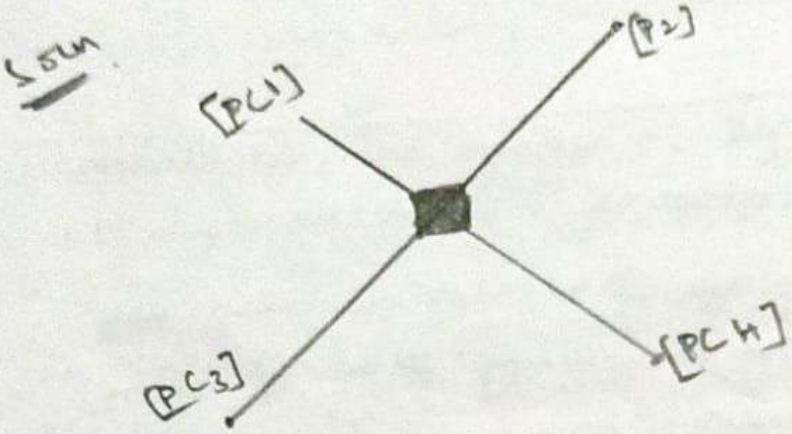
Result:

Thus experiment for Setup and Configuraring a LAN has been Verified.

Student observation

Draw a neat Diagram of LAN in the configuration observation book, that you have Implement in your lab write the IP Config of each & every device with the outcome & challenges faced with Configuring the LAN.

Write IP Configuration of each & every device



outcome:

LAN was successfully set up and all Devices could Communicate with each other using their Assigned IP address. Shared resource like folder were accessible

challenges faced.

→ Measuring each PC has a unique IP address to avoid conflicts

→ Initial Difficulty accessing the Switch Web due to incorrect IP Address.

Lab: 5

Aim:
Experiment on packet Capture tool. wireshark.

Packet Sniffer
→ Sniffs messages being Sent/ recieved from/ by your Computer
→ Store and display the Contents of the various protocal feilds in Managar.
- Never sends packets Shiffs.
- No packets Addressed to it.
- Receives a Copy of all packets
→ Packet Shiffs structure Diagnostic tools
- Tcpdump (eg: tcpdump - enchost 10.129-41.2)
- wire Shark (wireshark -> exex out)

wireshark:
wireshare a Network analysis tool donesly known as Ethernd, capture packet in real time and display them in human readable format.
→ what we Can Do - Capture Network proto 'cols using dissectors
- Analyse problems.
→ used for - People: Learn Networ Protocol meterials
Network administration troubleshoot Network Prolelems.

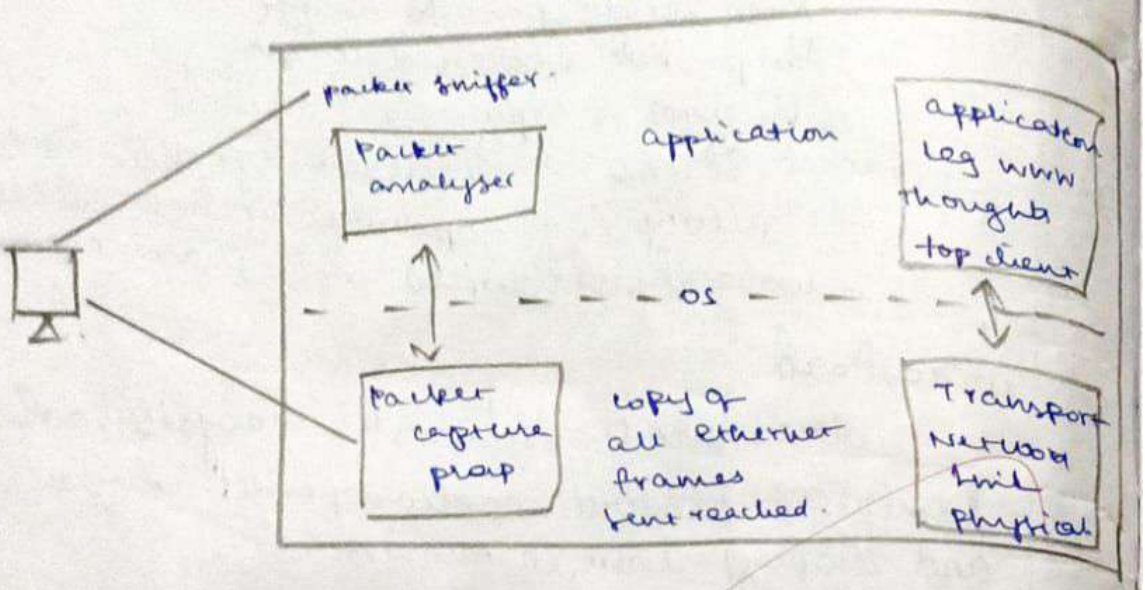
Getting wireshark: wireshark Can be download for windows or Macos from the offecial website Capturing packets
After Downloading and installing wireshark launch it and double check the prans of a Network. interface under Capture to Start Capturing packets
The "Packet Retails" Panel: Shows the Coorent packet in a More detailed,
The "Packet Retails" Panel: Shows the Current Packet in a More detailed.
The 'Packet Bytes' Panel: Shows Rata of Current packet

Colour Coding · Small Captures · Filtering Packets · Inspecting packets · Flow Graph · Gives a better understanding of what is going on

Capturing and Analysing packets using wireshark tool

Procedure:

→ Select LAN in wireshark.
→ Go to Capture Automatically after 100 packets
→ Select Stop Capture Automatically



29/3/24

Implement error detection and Correction using Hamming Code Concepts

Aim: write a program to implement error and Correction using HAMMING Code Code Concept Make a test to input data Stream and Verify error Correction

Error Correction at data link layer.

Hamming Code is a set of error - Corrood Codes that can be used to detect and Correct the errors Corrood Codes that can occur when the data is transitted from the Sender to the receiver.

Creat Sender program with below features.

1. Input to Sender file should be a text of any length should Convert text to Binary
2. Apply hamming Code Concept on the binary data and add bits
3. Save this outputs in a file called channel.

Import numpy as np.

function to Convert text to Binary

```
def text-to-binary (text):
    return "join, format (ord, 'b') '08b')
char in text)
```

```
# function to calculate redundant bits needed
error detection
def calc:
    j = 0
    k = 0
    m = len(data)
    res = ''

# Adding redundant bits at positions that are
    for i in range(1, m+j+1):
        if i == 2**j:
            res = res + '0'
            j += 1
        else:
            res = res + data[k]
            k += 1
    return res

# function to calculate parity bits
def calc_parity_bits(arr, r):
    n = len(arr)
    arr = list(arr)
    for i in range(r):
        parity = 0
        position = 2**i
        for j in range(1, n+1):
            if j & position:
                parity ^= int(arr[j-1])
        arr[position-1] = str(parity)

# function to detect and correct error
def detect_and_correct(data, r):
    n = len(data)
    err = 0
```

```
# Calculate Parity bits
for i in range (r):
    Parity = 0
    Position = 2**i;
for j in range (1, n+1):
    if j & position:
Parity ^= int (data[j-1])
if (Parity != 0):
    res += Position
if res != 0
Print ("error detected at Position: {res}"
data = list (data)
# Correct the error
if res <= n:
    data[res-1] = '0' if data[res-1] == '1'
Print (f"error corrected at position: {res}")
else:
    Print (error position out of bare.
        No Correction performed")
else print (No Correction performed)
else
    original_data += data[i-1]
return original_data
```

```
# function to introduce an error in the data
def introduce_error(data, position):
    if (position < 0 or position > len(data)):
        print("error position is out of range")
    return data

# find the bit at the specified position.
    (1-based index)
    data[position-1] = '0' if data[position-1] == '1' else '1'
    return ''.join(data)

# main program.
    if name == "__main__":
```

Result:

The program for having code is executed successfully

Practical - 7

Aim:
write a progeram to implement flow control at data link layer using SLIDING WINDOW PROTOCOL Simulate the flow of from one node to another.

Create a Sender program with following
1. Input window size from the user.
2. Inputs a text message from the user.
3. Consider 1 character per frame.
4. Create a frame with following fields [frame no DATA].
5. Send the frames.
6. wait for the acknowledgement from the Reciver.
7. Reader a file called Receiver-Buffer
8. Check ACK field for the Acknowledgement number
9. If the Acknowledgement number is as expected Send new set of frames accordingly.

Create a reciver file with following features:
1. Reader a file Called Sender-Buffer
2. check the frame no:
3. If the frame no are as expected. write the appropriate Ack no in the Reciver-Buffer file.

PROGRAM CODE:

```
import Hme.
import random.
class frame:
    def __init__(self, frame_no, data):
        self.frame_no = frame_no
        self.data = data
        self.acknowledged = False
```

```
def send_frames(frames, window_size):
    Print("\n--- Sending frames ...")
    for i in range(window_size):
        if i < len(frames) and not frames[i].acknowledged:
            Print(f"Sent frame {frames[i].frame_no}:
                  {frames[i].data}")
    Print("Frames Sent, waiting for acknowledgements...\n")
def receive_frames(frames, window_size):
    Print("\n--- Receiving frames ---")
    for i in range(window_size):
        if i < len(frames) and not frames[i].acknowledged:
            if random.random() < 0.2:
                print(f"Received frame {frames[i].frame_no}:
                      {frames[i].data} [ERROR]")
                frames[i].acknowledged = False
            else:
                Print(f"Received frame {frame[i].fram_no}:
                      {frame[i]data} [ok]")
                frames[i] acknowledges = True.
def Sliding_window_protocol():
    window_size = int(input("Enter window size:"))
    message = input("Enter a message to Send:")
    frames = [Frame(i, message[i] for, i in rang(len(
                                        message))]
    base = 0.
    while base < len(frames):
        send_frames(frames[base:], window.size)
        time.sleep(2).
        receive_frames(frames[base:], window_size)
        while base < len(frames) and frames[base].
                                        acknowledged.
            base += 1.
        if base < len frames):
            Print("\nResending unacknowledged fram...")
            time.sleep(2)
Print("\n All frames sent and acknowledged:
```

sliding - window - protocol ()

output:

Enter window Size: 3
Enter a message to Send: Protocol
..... Sending frames .....
Sent frame 0: P
Sent frame 1: r
Sent frame 2: O-
Frames Sent, waiting for acknowledgements. . .
.... Receiving frames ....
Received frame 0: P [OK]
Recieved frame 1: r [ERROR]
Recived frame2: o [ok]
Resending unacknowledged frames ....
---- Sending Frames. . . .
Sent frame 1: r
Sent frame 3: t.
Frames Sent, waiting for acknowledgements. . .
.... Receiving Frames. . . .
Received Frame 1: r [ERROR]
Recived Frame 3: t [ERROR]
Resending unacknowledged frames. . .
.... Sending frames. . . .
Sent frame1: r
Sent frame 3: t.
frames Sent, waiting for acknowledgements . . .

.... Receiving frames ...
Received frame 1: 2 [OK]
Received frame 3: t [OK]
Resending unacknowledged frames.

---. Sending frames...
Sent frame 4: 0
Sent frame 5: C
Sent frame 6: 0.
frames sent waiting for acknowledgements...
--- Reciving frames ----
Received frame 4: 0 [ERROR].
Received frame 5: c [OK]
Received frame6: o [OK]
Resending unaknowledged frames...

-.- Sending frames ----
Sent frame 4: 0
Frames sent, waiting for acknowledgements...
-+- Reciving Frames----
Recivid frame 4: 0 [OK]
Resending unacknowledged frames...
---- Sending frame ---
Sent Frame: !
frame sent, waiting for acknowledgement.

Result:
Thus, the program to implement Sliding windows protocal is executed sucessfully.

PRACTICAL-8

AIM:

a) Simulate Virtual LAN Configuration using CISCO Packet Tracer Simulation.

Objectives:

Part 1: Build the network and Configure Basic Device Setting
Part 2: Create VLANs and Assig Switch Ports
Part 3: Maintain VLAN Port Assignments and the VLAN Database.
Part 4: Configure an 802.1Q Trunk between Switches.

Instruction.

Part 1: Build the Network and Configure Basic Device Setting

Step 1: Build the network as shown in the topology
a. Click and drag both Switch S_1 and S_2 to the Rack.
b. Click and drag both PC-A and PC-B to the table and use the power button to turn them on
c. Provide network Connectivity
d. Connect Console Cable from device.

Step 2: Configure basic Settings for each Switch.
a. From the Desktop tab on each PC, use the Terminal to Console into each Switch.
b. Enter Configuration mode
c. Assign a device name to each Switch.
d. Assign class as the privileged EXEC encrypted Password.
e. Assign cisco as the Console.
f. Assign Cisco as the VTY
g. Encrypt the plaintext passwords.
h. Create a banner that warns anyone accessing

the device
i configure the IP address listed in the Addressing
Table for VLAN1 on the Switch
j Shut down all interfaces that will not be
used
k Set the clock on each Switch.
l close configuration window.

Step 3: Configure PC host
Step 4: Test connectivity
part 2: Creat VLANA and Assign Switch ports
Step 1: Create VLANA on the Switches
a. Create the VLANA on S1.
b. Create the same VLANA on S2
c. Issue the show VLAN A brief command to view
the list of VLAN's on S1.
Step 2: Assign VLANS to the Correct Switch interfaces.
a Assign VLANS to the interface on S1.
1) Assign PC-A to the operation VLAN.
2) From VLAN1 remove the management IP.
address and configure it on VLAN99.
b. Issue the show Vlan brief Command and
verify that the VLANA are assigned to the correct
interfaces.
c. Issue the show IP interface brief Command.
d. Assign PC-B to the operations VLAN on S2
e. From VLAN1, remove the mangement IP.
address and configure it on VLAN99.
f. use the show Vlan brief Command to
Verify that the VLANA assigned to the
Correct interfaces

Part 3: Maintain VLAN Port Assignments and the VLAN Database.

Step 1: Assign a VLAN to multiple interface from the Desktop tab on each PC, use Terminal to continue configuring both network switches.

Step 2: Remove a VLAN assignment from an interface

Step 3: Remove a VLAN ID from the VLAN database.

a. Add VLAN 30 to interface F0/24 without issuing the global VALAN command.

b. Verify that the new VLAN is displayed in the VLAN table.

c use the no VLAN 30 Command to remove VLA N 2 from the VLAN database.

Part 4: Configure an 802.1Q Trunk Between the Switch.

Step 1: use DTP to initiate trunking on F0/1.

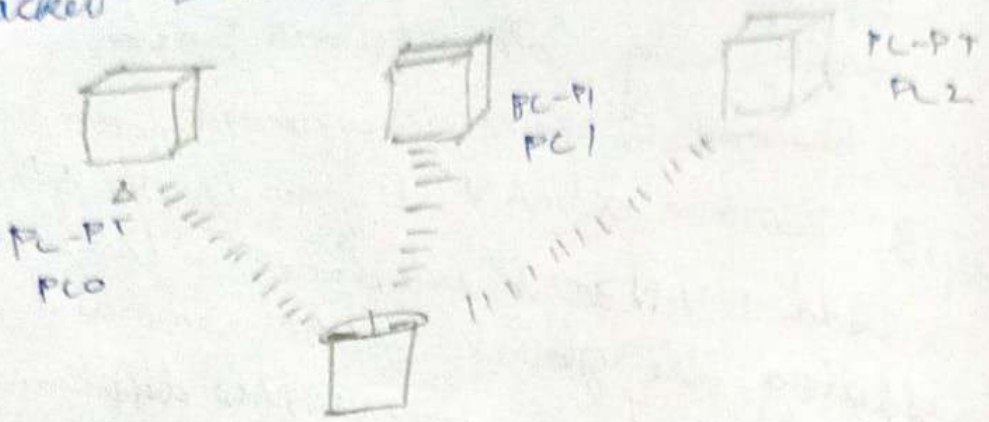
Step 2: Manually configure trunk interface F0/1

Result:

Thus Virtual LAN Configuration using CISCO PACKET TRACER is executed Successfully

AIM:

b) Configuration of wireless LAN using CISCO Packet Tracer.



To complete these tasks follow these step by step instructions:

Step 1: click on wireless router.

Select Administration tab from top menu. Set username and password to admin and click on Save Settings.

Next click on wireless tab and set default SSID to Mother Network.

Now select wireless Security and change Security mode to WEP.

Again go in the end of page and click on Save Settings.

Next click on wireless tab and set default SSID to Mother Network.

Now select wireless security and change Security mode to WEP.

Again go in the end of page and click on Save Settings.

PC	IP	Subnet Mask	Default Gateway
PC0	192.168.0.2	255.255.255.0	192.168.0.1
PC1	192.168.0.3	255.255.255.0	192.168.0.1
PC2	192.168.0.4	255.255.255.0	192.168.0.1

- Now its time to Connect mother Network
- click on connect button to Connect Mother network
- It will ask for WAP key. insert 0123456789. and click Connect.
- It will ask for WAP key insert 0123456789.
- Repeat same process on PC1 and PC2.

Student observation:

c) what is SSID of a wireless router?

- SSID (Service Set Identifier) is the name of a wireless network. It is used to identify and differentiate one network from another. when you Connect to a wifi network, you typically see a list of available SSIDs, which typically by nearby router or access points.

d) what is a Security key in a wireless router

- Security key is a password. that is used to Protect a wireless network. It ensures that only authorized access, securing data transmission and protecting the networks from potential attacks.

e) Configure a Simple wireless LAN in your lab using a real access point and write down the Configuration in your notebook.

1. Gather Equipment
   - wireless router or access point
   - Device for configuration
2. Connect to the access point
   - Plug in the router
   - Connect your laptop to the router
3. Access the Router Configuration Page.
4. Configure SSID and Security Settings.
5. Set up IP address and DHCP Setting
6. Save and Reboot
7. Verification.

These steps will help you set up and secure a simple wireless LAN in a lab environment.

Result:

Thus, Configuration of wireless LAN using CISCO Packet tracer is executed successfully

PRACTICAL-9.

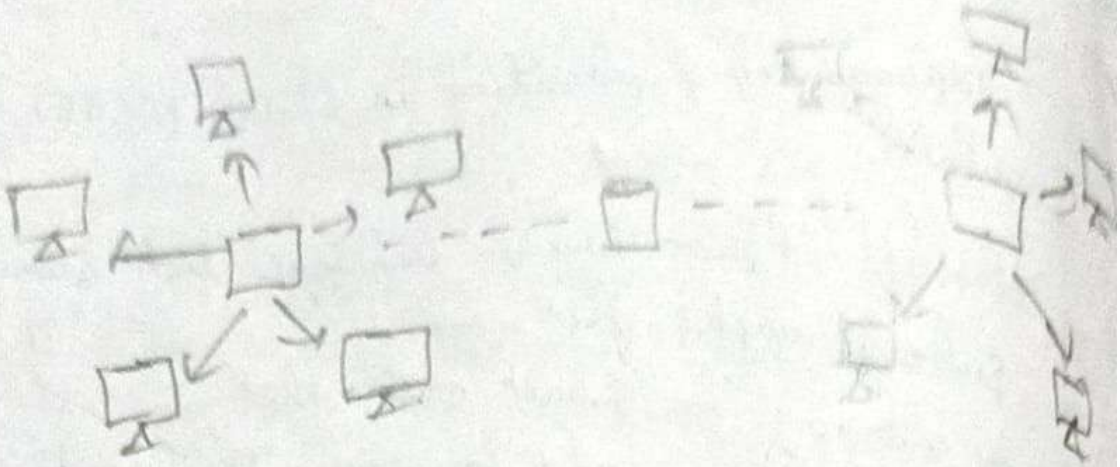
AIM:
Implementation of Subnetting in CISCO PACKET TRACER Simulator

classless IP Subnetting is a technique that allows for Subnet masks for more efficient use of IP address by allowing for Subnet mask that are not Just the default masks for each IP class. This means that we can divide our IP address space into smaller Subnets, which can be useful when we have a limited number of IP addresses but need to create multiple networks.

CREATING A NETWORK TOPOLOGY:
The first step in implementing classes IP Subnetting is to create a network topology in Packet Tracer.

ADDING THE DEVICES:
once we have created our network topology we can add device to it Here, we will be adding routers, wires and PCs

SUBNETTING:
To Subnet the network address of 192-168-2-0/24. to provide enough spaceat for at least 5 address for end devices, the switch, and the router we can use a /27 Subnet mask. This will give us 8 Subnets with 30 hosts address each.



configuration the devices:

Now that we have added our devices and connected them, we can start configuring them. This will open the command line interface (CLI) for the router. In the CCI, enter the following commands:

#enable
#Configure terminal
#interface terminal
#ip address {IP address} {Subnet-mask}
#no shutdown
#exit
ip address {IP address} {Subnet mask}
no shutdown.
exit

Replace "{IP address}" and "{Subnet mask}" with your desired IP address and Subnet mask.

Next, we will Configure the Switch. Right-click on the Switch and Select "CCI". In the CLI, enter the following Commands:

```
enable
Configure terminal
interface fast Ethernet 0/1
Switchport mode access
exit
interfacefast Ethernet 0/2
Switch port modeaccess
exit
```

To Configure the Gigabit Ethernet interface on the router you can follow these steps:

1. Right-click on the router and Select 'CLI'.
2. Enter the following Commands.

```
enable
configure terminal
interface Gigabit Ethernet 0/0
ip address {IP address} {Subnetmask}
no Shutdown
```

TESTING THE NETWORK:

open a Command prompt on each PC and try to ping the other PC. If the ping is Successfully then the network is functioning properly. We can also use the "ping" Command to test Connectivity between the router and the PCs.

Student observation:

a) write down your understanding of Subnetting

Subnetting is the process of dividing a large network into smaller, more manageable subnetworks (subnets). Each subnet can operate independently while still being part of the larger network. In subnetting, we modify the default subnet efficiency

b) Advantage of Implementing Subnetting

*) Improved Network Management.

Breaking down a large network into subnets makes it easier to manage and troubleshoot.

*) Enhanced Security.

Subnets can isolate sensitive areas, limiting access to certain parts of the network.

*) Efficient IP Address utilization.

Subnetting reduces IP wastage by allocating specific ranges to subnet based on need.

*) Reduced Network Traffic.

By confining broad cast traffic within each subnet, overall network performance improves

c) Subnetting Implementation in College.

*) Research and Mapping.

To determine if subnetting is in place at your college consult with the network administration IP addresses are segemented.

*) Subnets Diagram and IP Address list;

If subnetting is implemented, you can create a visual representation (a network diagram) and list the subjets with associated IP addresses for each department or section.

Practical - 10

Aim:

a) Internetworking with routers in CISCO PACKET TRACER Simulator

In this network, a router and 2 PCs are used computers are connected with router using a Copper Straight-through Cable. After forming the network, to check network connectivity a ping PDU is transferred from PDC to PC1.

Procedure.

Step-1 (Configuring Router).

1. Select the router and open CLI.
2. Press ENTER to Start Configuring Router.
3. Type enable to activate the privileged mode

Step-2 (Configuring PCs):

1. Assign IP Addresses to every PC in the network.
2. Select the PC-0 to the desktop and select IP Configuration and assign an IP address, Default gateway Subnet Mask
3. Assign the Default gateway of PC0 as 192.168.10.1.
4. Assign the Default gateway of PC1 as 192.168.20.1.

Step-3 (Connecting PCs with Router):

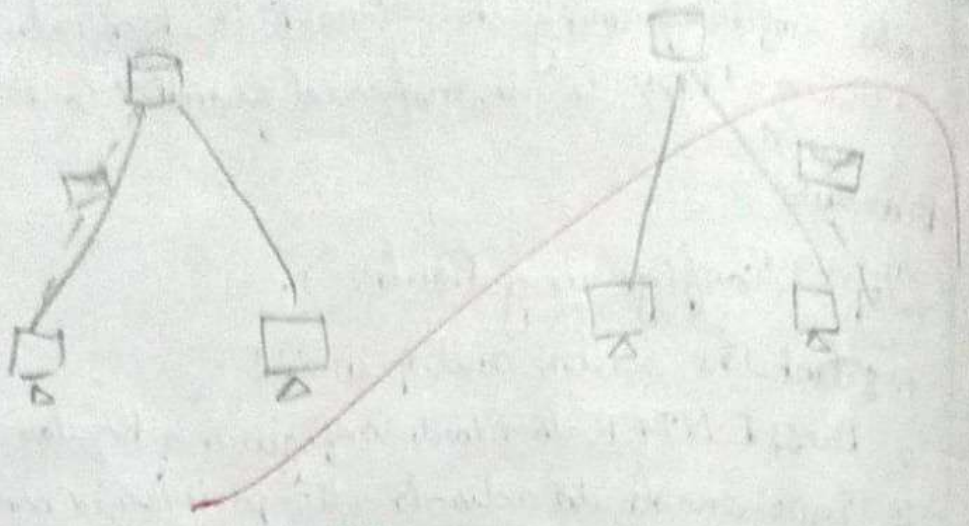
1. FastEthernet 0/0 Port of Router 1
2. FastEthernet 1/1 Port of Router 1.

Router Configuration Table:

Device Name	IP address FastEthernet 0/0	Subnet Mask	IP Address FastEthernet 1/0	Subnet Mask
Router 1	192.168.10.1	255.255.0	192.169.10.1	255.255.255.2

PC Configuration Table:

Device name	IP address	Subnet Mask	Gateway
PC0	192.168.10.2	255.255.255.0	192.168.10.1
PC1	192.168.20.2	255.255.255.0	192.168.20.1



Aim:

b) Design and Configure an internetwork using wireless router, DHCP server and internet cloud.

Address Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC	Ethernet	DHCP		192.168.0.1
wireless Router	Internet	DHCP		
Cisco.com Server	Ethernet	208.67.220.2		
Laptop	wireless	DHCP		

objectives:

Part 1: Build a Simple Network in the logical Topology workspace.

Step 1: Launch Packet Tracer

Step 2: Build the topology

a. Add network devices to the workspace.

To place a device onto the workspace first choose a device type from the Service Type Selection box

b change display names of the network devices to the workspace.

To change the display names of the network device i can on the Packet Tracer logical workspace then click on the Config tab in the device Configuration windows

c. Add the physical cabling between devices on the workspace using the device Selection box, add the physical cabling between devices on the workspace.

The pc will need a Copper Straight through Cable to Connect to the wireless router

Part 2: Configure the Network Devices.

Step-1 Configure the wireless router

a. Create the wireless network on the wireless router

b. click on the Save Setting tab

Step-2: Configure the laptop to access the wireless network

Step-3: Configure the PC.

a. Configure the PC for the wired network.

Step 4: Configure the Internet cloud.

a. Install network modules if necessary

b. Identify the power and To ports

c. Identify the type of provider.

Step-5: Configure the Cisco.Com Server.

a) Configure the Cisco Com Server as a DHCP Server

b) Configure the Cisco. Com Server as a DNS Server to provide domain name to IPV4 address resolution

c: Configure the Cisco Com Server Global Setting

d. Configure the Cisco. Com Server fast Ethernet

Interface settings:

Part-3: Verify Connectivity.

Step-1: Refresh the IPv4 setting on the PC.

a) Verify that the PC is receiving IPv4 configuration information from DHCP.

b) Test connectivity to the Cisco Com server from the PC.

Student observation.

1. write down the key feature of configuring wireless router and DHCP server.

wireless Router Configuration:

*) SSID Configuration: Set up a unique network name (SSID) for your wireless network to allow device to identify and connect.

*) Security Settings: Configure network security to protect against unauthorized access.

*) Password: Set a strong password for connecting to the network.

*) channel Selection: Choose a wireless channel that minimizes interfer for other networks or devices.

*) Frequency Band: Select the 2.4 or 5 GHz or 6 GHz band depending on device compatibility and Coverage requirements.

DHCP Server Configuration.

*) IP Address Range: Define the IP address range that the DHCP Server will assign to devices.

*) Subnet Mask: Specify the subnet mask to define network boundaries.

*) Lease Time: Set the duration for which an IP address is assigned to a device.

2) Significance of DHCP server in Internetworking:

* The Dynamic Host Configuration Protocol (DHCP) server is crucial in internetworking because it simplifies and automates the process of assigning.

* Automatic IP Assignment: DHCP dynamically assigns IP addresses, reducing manual configuration and preventing IP conflicts.

* Supports Scalability: DHCP servers make it easy to add and manage multiple devices across large networks, as essential feature in growing environements

3) Design and Configuration of an Inter-Network in a lab

Steps to Design and Configure an Inter-network:

1. Hardware Requirement.
   * one Switch
   * one router
   * Ethernet Cables.
2. Network layout:
   * Router
   * Switch
   * Devices.
3. Configuration Steps:
   i) Connect the router to Switch.
   ii) Configure the router's interface with an IP address
   iii) Configure the DHCP server on the router

PRACTICAL - 11

Aim:

a) Simulate Static Routing Configuration using CISCO Packet Tracer.

Static router are the router you manually add. to the router's routing table. The process of adding static router to the routing table is known as static routing.

Creating, adding, Verifying static router

Router automatically learn their Connected network. we only need to add router for the network that are not available on the router's interfaces

Router	Available networks on local interface.	Network available on other router's interface.
Router 0	10.0.0.0/8 20.0.0.0/8 40.0.0.0/8.	30.0.0.0/8, 50.0.0.0/8.
Router 1	20.0.0.0/8 30.0.0.0/8. 50.0.0.0/8	10.0.00/8, 40.0.0.0/8.
Router 2	40.0.0.0/8. 50.0.0.0/8	10.0.0/8, 20.0.0.0/8 30.0.0.0/8.

Router requirement

Obtain 2 route for network 30.0.0.0/8 and Configure the first route as the main route and the second route as a backup router.

Result :

PRACTICAL-12

Aim:
Implement echo client server using TCP/UDP ~~Sockets~~.

Sockets
TCP echo client - server algorithm.

Servers:
1. Create a TCP Socked.
2. Connect the Socked to a local address and port
3. Listen for incoming client Connections.
4. accept a client Connect
5. loop -
   *) Recive data from the client
6. close Connection

Client:
1. Create a TCP Socket
2. Connect to the Server using Specified address and port
3. send a message to Server
4. Display the received message
5. close Socket

TCP Server - Py

```
import Socket
def tcp-Server():
    Server.Socket: Socket: Socket.Socket(Socket.AETINET)

Server.Socket.Socket.Slobind(" local host " 12345))
Server.Socket.listen().
```

Print f

```
try:
    while true:
    data = Connection recv (1024).
    if data:
        Print(f"Recived : {data decode()}").
    else:
        break
finally:
    Connection.close().
```

TCP.client.Py:

```
import socket.
def tcp-client ().
    client-socket = Socket. Socket. AF_INET,
                    Socket - Socket. STREAM)
    client. Socket Connect (("local host" ) 12345))

try:
    message = input ("Enter a message to Send").
    clint. Socket. Sendall (message. encode())
    data = client. Socket recv (1024)
finally:
    client - Socket (closed)
if - name . - - = "main . . - ";
    tcp client ().
```

output:

```
) Python tcp. client. Py
Enter a message to Send Hi I am Abishek Srinath
Recived from Server: Hi, I am Abishek Vijay P.S
```

Result:

Thus the program to implement echo client server using TCP is executed Successfully

6) Aim:

To implement the chat client is server using TCP/UDP sockets.

Algorithum:

chat Server.

1. State the Server by creating a socket; bind. to a specific address and port, listen for incoming connections.

2. when a new client connects, add client to a list of a connected client start a new process to talk to the clients

3. For each connected client start a new checking for new message

4. keep running the process tell the server stops

chat-client.

1. Connect to the Server by creating a socket and connect it to Server address port.

2. Start a process by creating a to listen to message.

3. keep asking for the new message.

4. keep running till the user decides to quit.

chat-client.py

import socket

import threading

def receive_message (client_socket):

while True

try:

message : client. socket. recv(1024)

except Exception as e.

```
Print (f" an error occured {e}")
  break
def start_client():
  client_socket = socket.socket (socket.AF_INET, SOCK_STREAM)
  host = "127.0.0.1"
  port = 12345
  client.connect (host, port)
  print ("Connected to chat server")
  threading.Thread (target = receive: message args=
  client_socket.send (message.encode (utf-8))
  chat_server.py:
Import socket
Import threading
def handle_client (client_socket)
while true:
    try: message = client_socket.recv(
If not message:
    break
  while true:
  client_socket, addr = server.accept()
  print(f"New connection from {addr}")
  start() args = (client_socket)
if __name__ = "main"
```

output:

```
> Python chat_server.py
chat server started on [27.0.0.1:12345
New connection from ("127.0.0.1", 55220)
> Python chat_client.py
  you : Hi say hi
  you : server : Recied :
```

Result:

Thus the program to implement the client server using TCP is executed successfully

Aim:

Implement your own ping program

Algorithm

* Open a raw socket to send ICMP request.
* Create the ICMP echo request packet, including a header and data.
* Send packet: Send the ICMP request to target host.
* Calculate the time.
* Show response.

Server Script.py

```
import socket
def start_server(host = '127.0.0.1', port = 12345):
with socket.socket(socket.AF_INET, socket.SOCK_DGRAM) as s:
    s.bind(host, port)
    print(f'UDP Server (host='127.0.0.1', port=12345)
while True:
    data, addr = s.recv from(1024)
    print(f"Received message from {addr}: {data.decode()}")
    s.sendto(b'Pong', addr)
if __name__ == "__main__":
    start_server()
```

client.py

```
import socket
def start_server(host='127.0.0.1', port=12345):
try:
    s.bind(host='127.0.0.1', port=12345)
    print(f" UDP Server running on
        {host} : {port}")
```

while True:

data, address = sock.recvfrom(1024)

Print (f"UDP Server running at {host}")

s.sendto(b'Pong', address)

except socket.timeout:

Print("Request timed out")

output:

Python ping-server.py

UDP Server running on 127.0.0.1:12345

Received message from (127.0.0.1, 57734)

23/11

Result:

Thus the program to implement ping program is executed successfully.

Ex. No: 14

Aim:
write a Code using RAW Socket to implement Packet Sniffing

Algorithm:
*) Create a raw Socket
*) Continuously Capture incoming packets using recfrom
*) Parse and display information like the source and destinated IP address and protocal
*) close the Socket after the Capture Process

Code:

```
from scapy.all import sniff
from scapy.layers.inet import IP, TCP, UDP, ICMP

def packet_callback(packet):
    if IP in packet:
        proto = ip_layer.proto
        src_ip = ip_layer.src
        dest_ip = ip_layer.dst
        protocol_name =
        if protocol == 1:
            protocol_name = "ICMP"
        elif protocol == 6:
            protocol_name = "TCP"
        else:
            protocol_name = "Unknown protocol"

def main():
    sniff(prn=packet_callback, count=0)

if __name__ == "__main__":
    main()
```

output:

Protocol: TCP
Source IP: 192.168.1.7
Destination IP: 93.184.216.34.

. . . . . .

Protocol: TCP
Source IP: 192.168.1.2
Destination IP: 173.217.16.206.

23/11

Result:
Thus the code using RAW Socket to implement packet Sniffing.

Exno: 15

Aim:
To analyse the different types of web logs using webalizer tool.

Procedure:
S1. Run webalizer windows version.
S2. Input web log file.
S3. Press run webalizer.

Logfiles	Logbibe	Views	Settings	Additional HTML code	HTML

Input:
Logbibs

c:\Users\TCS\Downloads\accesslog:

X ? ..

Target Directory.

c:\User\TCS\.

clear existing directory.

Daily usage for November 2024.

Days	Hits	files	Pages	Visits	Sites	K.bytes
3	67.105%	651000%	160001	11000	1100000	1371000

A231.

Result:
Thus the procedure to analyse the different types of web logs using webalizer tool is executed successfully.