கற்றது கை மண் அளவு கல்லாதது உலகளவு

INDEX

A1 Best Note Book

NAME: Arun Mohan STD: CSE SEC: A ROLL NO 220701[illegible]UB

S.No.	Date	Title	Page No.	Teacher's Sign / Remarks
1.	16/7/24	Study of various Network		
2.	30/7/24	Study of Network cables		
3.	06/8/24	Experiments on CISCO Packet tracer		
4.	09/8/24	setup and configure a LAN using Ethernet		
5	16/08/24	Experiments on Product capture using wireshark		
6.	20/8/24	Hamming code		
7	24/9/24	Sliding window		
8	4/10/24	virtual LAN config		
9	8/10/24	subnetting in CISCO		
10	15/10/24	Internetworking with routers in CISCO		
11.	18/10/24	Routing at network layer		
12	22/10/24	End-End Communication at Transport layer		
13.	25/10/24	Implement your own Ping		
14	29/10/24	write a code using RAW socket to implement		
15	5/10/24	Analyze various Type of sniffing		

கனவு காணுங்கள் கனவு என்பது நீ தூக்கத்தில் காண்பது அல்ல உன்னை தூங்கவிடாமல் பண்ணுவது எதுவோ அதுவே (இலட்சியம்) கனவு Dr. அப்துல் கலாம்

S.No	Date	Title	Sign
8a)	13/10/24	Virtual LAN configuration using cisco packet server	
b)	13/10/24	Configure of wireless LAN using cisco packet tracer	
9		Implementation of subnetting in cisco tracer	
10a)	10/10/24	Internetwork using a Router	
b)	28/10/24	Internetwork using wirless Router DHCP server and internet cloud	
11.a)	4/11/24	Static Routing	
b)	4/11/24	RIP using cisco packet tracer	
12.a)	6/11/24	Echo client server using TCP/UDP sockets	
b)	6/11/24	chat program using socket programming	
13.	8/11/24	Ping Program	
14.	9/11/24	Packet sniffing	
15.	11/11/24	Webalizer	

completed

21/11

Date :- 13-07-2024

Ex No:- 01

Study of Various Network

AIM :-

Study of various network commands used in Linux and Windows

Basic Network Commands:-

1) arp -a : Interface : 172.16.75.54 .... 0x12

Internet address	physical address	Type
172.16.72.1	7c-5a-1c-cf-bc-41	dynamic
172.16.72.133	4c-ac-a3-65-97-E3	dynamic

2) Hostname :-

DESTOP-- COIBHTO

3) nbtstat -a :

NBTSTAT [[-a RimoteName] [-A IP address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [interval] -a [adopter status] lists the network matches name table given its name.

4) netstat :

Active connections

Proto	Local Address	Foreign address	status
TCP	127.0.0.1:49678	Desktop COIBHTD:49679	Established

5) nslookup :

Default server : unknown

Address : 172.16.72.1

pathping usage :- pathping [-g host list]
[-h maximum hops] [-i address] [-n] [-p period]
[-q num queries] [-w timeout] [-u] [-b]
target_name options -4 Force using IPv4

Route :- Route [-F] [-p] [-4|6] command
[destination] [Mask network] [gateway]
[METRIC metric] [if interface]
-6 force using IPv6

Some important Linux Networking commands

1) ip : ip < options> <object> < command>

2) [root@server ~] # ip address show

1:lo < LOOPBACK, UP, LOWER_UP> mtu 65536
sequence state UNKNOWN group default
qlen 1000

link / loopback, 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo.

3) [root@server ~] # ip link set up

To alter the status of the interface by bringing interface enp250 online.

4) [root@server ~] # ip link set to down

To alter the status of the interface by bringing the interface enp250.

5) [root@server ~] # ip link set to promise on

To alter the states of the interface by enabling promiscuous

6) [root@server ~] # ip route add default via 192.168.1.254/21 dev lo

To add a default route for all address v/a the local gateway 192.168.1.254 that can be reached on device enp250.

7) [root@server ~] # ip route add 192.168.1.2.124 via 192.168.1.254

To add a route to 192.168.10/24 via gateway at 192.168.1.254.

8) [root@server ~] # ip route add 192.168.1.0/24 dev lo

To add a route to 192.168.1.0.124 that can be searched on device enp250

9) [root@server ~] # ip route delete 192.168.1.0/24 via 192.168.1.254

To delete the route for 192.168.1.0/24 via the gateway at 192.168.1.254

10) Display -> [root@server ~] # ip route get 10.10.1.4

uid 1000
cache.

2. ifconfig:

~~lo flags = 19~~

Output

enp2s0 > flags = 4163 <UP, Broadcast, Running>
> mtu 1500
inet 172.16.8.90 netmask 255.255.252.0
broadcast - 172.16.11.255
Rx packets 170123 bytes 2765293 1 (26.3 MiB)
Tx packets 4334 bytes 1136044 (1.0 MiB)
Rx errors 0 dropped 0 overruns 0
carrier collisions.

wlp3s0 > flags = 4099 <UP, broadcast,
multicast> mtu 1500
ether ec:fb:34:8f:9d:84
Rx packets 0 bytes 0
Rx errors 0 dropped
Tx packets 0 packets 0 byte
Tx errors.

3) mtr

mtr google.com

Op

Host	loss%	snt	Avg	best	worst
1. 172.16.8.1	0.0%	41	0.2	0.2	0.5
2. 142.250.171.262	0.0%	62	0.7	3.3	2.5
3. 142.251.227.217	0.0%	74	3.1	3.2	9.6

Op

mtr google.com

Host	loss%	snt	Avg	best	worst
1. 172.16.8.4	0.0%	30	0.2	0.2	0.4
2. 142.250.171.162	0.0%	42	2.6	2.5	3.9
3. 142.251.52.207	0.0%	57	3.1	2.2	7.2

d)

4) tcpdump:

[root@server ~] # dnf install - y tcpdump
to install - y tcpdump

[root@server ~] # tcpdump - D

1) lo [up, Running, connected]

2) any [pseudo - device that captures on all interfaces] up running)

[root@server ~] # tcpdump -qt

dropped privs to tcpdump tcpdump
verbose output suppressed use -v[v] for full protocol decode

[root@server ~] # tcpdump - qlo - c10

10 packets captured
20 packets received by filter
0 packets dropped by kernel

[root@server ~] # tcpdump - i lo - c10 host 8.8.8.8

dropped privs to tcpdump

for full protocol decode listening on to
lst type EN10MB (ethernet) snapshot
length 262144 bytes.

[root@ server N] # tcpdump -i eth0 sec host
8.8.8.8

dropped privs to tcpdump
tcpdump restore output.

3. lo [up, running]
4. wlp 3s0 [up
5. bluetooth [adapter number 0]
6. usbmon0 (All USB buses)

tcp dump -i lnto

O/P No such device lnit

5) ping # ping google.com

O/P
PING google.com (142.250.77.142) 56(84)
64 bytes from maa05s16-in-f14.1100.net
(142.250.77.142)
; icmp_seq=1 ttl=120 time=2.37 ms
04 bytes from maa05s16-in-f14.1100.net.142
.850.77.142)
; icmp_seq=3 : ttl=120 time=2.6 ms

64 bytes from maa05s16-in-f14.1100.net (142.250
77.142
: icmp_seq=3 : ttl=120 time=2.6 ms

<stopped ping.google.com

configuring an ethernet connection by using nmcli

If you connect a host to the network over ethernet, you can manage the connections setting on the command line by using nmcli

Procedure

1) List the network manager connection profiles
nmcli connection show

O/P

name	uuid	type	device
wired connection	a5a94080-2bbc-3995-1ec4	ethernet	
lo	exa-debi-2gfa-4761-9932-61294c2cc58		

2) # nmcli connection add con-name connection name <device-name> type ethernet.

3) optional Rename the connection profile
nmcli connection modify "wired connection"
"wired connection" is the name of connection

Display the current setting of connection profile # nmcli connection show.

connection interface-name: Apso
connection outbound: yes
ipv4.method: auto
ipv6.method: auto

configure the ipv4 settings
To use DHCP, enter
nmcli connection modify "wired connection"
method auto
to set a static ipv4 address, network mask default gateway, DNS servers & search
nmcli connection modify "wired connection
ipv4 address 192.02.254 ipv4.dns. 192.0.2.20
ipv4 example.

config the ipv6 settings
to use statelss address autoconfig [SLAAC]
enter
nmcli connection modifies "wired connection
method auto.

Activate the profile
nmcli connection modifies "wired connection
method auto.

Verification:
1) Display the IP setting of NIC:
ip address show enps120
enpiso 1 < broadcast - multicast, up, lowerup
mtu 1500 qdisc - iq- code - state up group default
len 1000

2) Display the ipv4 default gateway
ip route show default
default via 192.0.2.234 dev. episo pro net
102.

3) Display the ipv6 default gateway
ip.6 route show default
default via 2001: db8 :1 : ffe dev enp
static metric 102 pref

4) Display the DNS settings
cat /etc (resolve_conf)
search example.com
name server 192.0.2.200
name server 2001: db8 : : : ff66

5) Use the ping utility to verify the host can send packets
ping <host_name :or_ ip- addr

4) Display the current setting of connection profile # nmcli connection show.

connection interface-name: Apso

connection autoconnect yes

ipv4.method: auto

ipv6.method: auto

5) configure the ipv4 settings

To use DHCP, enter

nmcli connection modify "wired connection"

method auto

to set a static ipv4 address, network mask default gateway, DNS servers & search

nmcli connection modify "wired connection"

ipv4 address 192.02.254 ipv4.dns. 192.0.2.20

ipv4 example.

6) config the ipv6 settings

to use statelessaddress autoconfig [SLAAC]

enter

nmcli connection modifies "wired connection

method auto.

7) Activate the profile

nmcli connection modifies "wired connection

method auto.

Verification:

1) Display the IP setting of NIC:

ip address show enps 20

enp1s0 <broadcast - multicast, up, lowerups

mtu 1500 qdisc - iq - code. state up group default

len 1000

2) Display the ipv4 default gateway

ip route show default

default via 192.0.2.234 dev. enp1s0 pro metric

102.

3) Display the ipv6 default gateway

ip.6 route show default

default via 2001: db8:1.: ffff dev enp1s0 pro

static metric 102 pref

4) Display the DNS settings

cat /etc (resolve_conf)

search example.com

name server 192.0.2.200

name server 2001: db8 : 1 : ffff

5) Use the ping utility to verify that this host can send packets

ping <host_name : or - ip- address>

Trouble shooting :

- Verify that the network lable is plugged into the host of sub.
- check wheather the link failure exists ones on this host oral host connect to sum
- verify that network cable & network interface are working as expected perform hardware diagonies steps and replace defeat cables and network interface and
- If configuration on disc doesn't match then config. on the device, start & restart manager creates on it

student observation :

1) What command is used to find the reachability of a host machine from your device

(a) ping

2) Which command will give the details of taken by packet to reach its destination

(a) trace out c

3) Which commands displays the Tcp port status in your machine,

(a) net state - tae

4) Which command displays ip config your machine

(a) ip config

5) write & modify the ip-config in where machine give any answer it.

(a) Edit the network config file & the use ipdown & 'ipup' or 'ip' command to apply changes,

RESULT :

Thus study of various network command is executed & verified successfully.

Ex: No: 2
Date: 20.7.24

AIM:-

study of different types of Network cables

1a) understand different types of network cables

1. unshield twisted pair (UTP) cable
2. Shielded Twisted pair (STP) cable
3. Coaxial cable
4) Fibre optic cable.

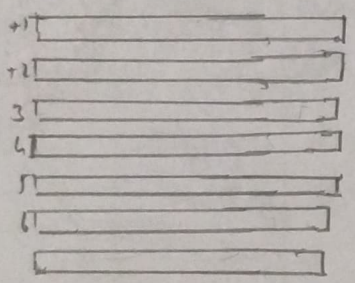
Cable Type	Category	Max data Transmission	Advantages Disadvantages	App use	Image
UTP	Category 3 and 5	10bps upto 100 Mbps	advantage * cheaper cost * Easy to install Disadvantage * More to Electro magnetic interference and noise	10-Base-Ethernet Fast Ethernet gigabit	
	category 5e	1Gbps			
STP	category 6, 6a	10Gbps	Advantages shielded Faster Than UTP less Noise	Higher Ethernet (10M) widely used in data centers	
Coaxial cable	RG-6 RG-59 RG-11	10-100 Mb/s	Advantage 1. High Bandwith 2. Immune to Interference Disadvantage * Limited distance 2. cost	speed of signal is 300 Million network high speed internet	
Fibre optic cable	single mode multi mode	100Gbps	Advantages * High speed * High Band width Disadvantages * Expensive * Require skilled	Maximum distance fibre optic cable is around 100 meters	

b) Make your Own Ethernet cross-over cable, straight Cable

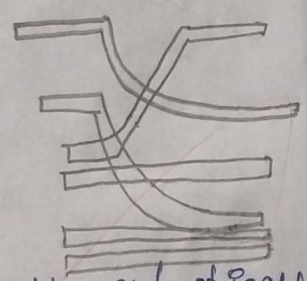
Tools and parts needed.

* Ethernet cabling CAT5e is certified for gigabit support, but CAT5 cabling works as well, just over shorter distances.
* A crimping tools. This is an all in one networking tool shaped to push down the pins in the plug and strip and cut the shielding off the cables.
    * Two RJ45 plugs
    * Optional two plug shields

straight their cable



X-over cable.



Difference b/w crossover cable and straight cable straight through network cable: Both sides should be A cross cable: one side A, one side B.

step 1:- To start construction of the cables, begin by threading sheilds onto the cables

step2:- Next strip approximately 1.5cm of cable shielding from bothe the ends. The crimping tool has a round area to complete this task.

step3:- After, you will need to untangle the wires; there should be four "twisted pairs". Referencing back to the shut, arrange then from top to bottom. One end should be in arrangement A and other in B.

step4:- One the order is correct, bunch them together in a wire, and if there are any that stick out farther than others, snip them back to create an even level. The difficult aspect is placing. These into the RJ45 plug without messing up the order. To do so, hold the plug and have the gold pins facing forward you, as shown.

step 5 :-

Next, push the cable right in. The notch at the end of the plug needs to be just over the cable shielding, and if it isn't, that means that you stripped off too much shielding. Simply strip the cables back a little more.

step 6 :- After the wires are securely sitting inside the plug, insert it into the crimping tool and push down.

step 7 :- Lastly, repeat for the other end using diagram (B) using diagram (A)

RESULT :-

Thus study of various type of cables is executed & verified successfully.

student observation.

1) What is the DIB cross cable & straight cable.

straight cable	cross cable.
The wiring of both ends of cable in identical	The transmit & receive wires are crossed & end of cable
It is used for connection types of devices	It is used for connection similar devices.

2) Which type of cable used to connect two PC) (straight / cross cable)

⊗ cross cable is used to connect two PC's directly.

3) Which type of cable is used to connect a router or switch to APC

⊗ A straight cable is used to connect a router or switch on PC

4) Find out the category of twisted pairs table in your lab to connect PC

⊗ cat 5e, cat 6, cat 6a

5) Write down your understanding, challenges faced, or received while making a twisted pair

⊗ creating a twisted pair cable required arranging wires according to specific std. challenges to specifics.

crimping :- Output a functional cable that provides proper connectivity b/w devices

STUDY OF PACKET TRACKER TOOL

EXP NO: 3

30-7-24

AIM:- To study the packet tracker tool installation & user interface overview.

INTRODUCTION:-

1. It allows you to make complex system without for dedicated equipment.

2. It helps you practice your network configuration & trouble shooting skills via computer

3. It is available for & windows desktop

4. Protocols in packets tracker coded to work & behave in real hardware.

INSTALLING PACKET TRACKER:

WINDOWS:- Installation in windows is pretty simple is straight the setup comes in single file name packettracer open ship file to begin the setup wizard choose location and start installation.

Linux:- It is ubuntu / urban distribution should download the file for ubuntu, and those using fedora redos must download the file for fedora

grant executable process channel

Tx packet tracer 601 - 1386 - Installer - rpm.bin

, packet tracker 601 - 1386 - Installer - rpm - bin

User Interface Overview:-

The layout of Packet Tracer is divided into several components. The components of the Packet Tracker Interface are follows

1. Menu Bar:- This is a common menu found in all software applications, it is used to open, save, point change preferences and soon.

2. Main Toolbar:- This bar provides shortcut icons to mean options to menu options that are commonly accessed such as open, save, zoom, undo.

3. Logical / Physical workspace at - These tab allows you to toggle between the logical and physical workspace

4. Workspace:- This is the area where topologies are created and simulations are displays.

5. common tool Bar :- This toolbar provides controls for manipulating topologies, such as select, move layout, place note, delite, inspect, resize shape.

6. Real time / simulation tabs :- These tabs are used to toggle between the real and simulation modes Buttons are also provided to control the time.

7. Network component box :- This compound contains all of the network and each devices available. The area contains 7.b: Device specific selection

8. User - Created packet box - Users can create highly customized packets to test their topology from this area, and the results are displayed.

d) Analyse the behaviour of network devices using (Cisco Packet Tracer simulator)

1. From the network K compound box, click and drag and drop the components

a) 4 Generic Pcs and one HUB

b) 4 Generic Pcs and one Switch

2. click on connections

a) click on copper straight - Through cable

b) select one of the Pc and connect it to HUB using cable.

c) similarly connect 4 Pcs to the switch using copper straight through cable.

3. click on the Pcs connected to hub, go the Desktop tab, click on IP configuration, and enter an IP address and subnet mask.

click on PDU (message icon) from common tool Bar, a) Drag and drop it one of Pc (sourse machine) and then drop it on another Pc connected to HUB.

4. Observe the flow of PDU from source Pc to destination Pc by selecting the Realtime mode of simulation.

5. Repeat step # 3 to 5 for Pcs connected to switch.

6. Observe how HUB and switch are forwarding the PDU and write your observation and conclusion about switch and HUB

RESULT

The study of Packet tracer tool and user interface installation has been done successfully.

Ex:2 student observation

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

1) what is the difference between cross cable and straight cable?

Ans

straight cable	Cross cable
* The wiring of the ends of the cable is identical	* The Transmit and receives wires are crossed on one end of the cable
* It is used for connecting different types of devices	* It is used for connecting similar devices

2) Which type of cable is used to connect two PC? (straight / cross cable)

A cross cable is used to connect two PCs directly.

3) Which type of cable is used to connect a router / switch to your cable?

A cross cable is used to connect a router / switch a PC.

4) Find out the category of twisted pair cable used in your lab to connect PC to switch?

Cat 5e, Cat 6 or Cat 6a.

5) Write down your understanding, challenges faced and output. received while making a twisted pair boss/ straight cable.

Creating a twisted pair cable requires arranging wires according to specific standards (T568A / T568B).

Ex:3 Student observation

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

→ A Hub broadcast packets to all ports while a switch forwards packets only to the destination. Port based on the MAC address

b) Find out the network topology implemented in your college and draw and label topology in observation

A star topology is implemented where each PC is connected to a central switch or hub.

switch

PC PC PC PC

Ex No:- 04 Setup and Configuration of a
DATE :- 9/8/24 LAN using switch and Ethernet cable

AIM:- Setup and configure a LAN (local Area Network) using a switch and Ethernet cables in the lab.

What is a LAN?

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

How to set up a LAN?

1. Plan and design an appropriate network topology taking into account network requirements and equipment location.

2. you can take 4 computers, a switch with 8, 16 or 24 parts which is sufficient or for network of these sizes

3. Connect your computer to network switch ethernet cable. One to your computer other end to another.

4. Assign IP address to your PCs

* Login to client comp as Administrator or as owner
* click network and connection.
* Right click local area connection, ethernet. go to properties → select internet protocol (TCP/IPV4) → select the following ip address option and assign ip address.

Networking sharing

Internet Protocal version 4 (TCP/IPV4) Prop

General

You can get IP settings assigned automatically if your network supports this capability.

* obtain an IP address automatically
* Use the fall IP address

IP address 10.1.1.1

Subnet mask 255.00.0

Default gateway

* obtain DNS server address automatica
* Use the fall DNS server address

Preferred DNS server . . .

Alternate DNS server . . .

validate setting upon exit

Advanced

Similarly assign IP address to all the PCs connected to switch

PC_1 - IP address : 10.1.1.1 , subnet mask 255.0.0.0

PC_2 - IP address : 10.1.1.2, subnet mask 255.0.0.0

PC_3 - IP address : 10.1.1.3, subnet mask 255.0.0.0

PC_4 - IP address : 10.1.1.4, subnet mask 255.0.0.0

5. configure a network switch

6. check the connectivity b/w switch and other machine using ping command in the command prompt of the device

7. Try to access the shared folder from other computers to network.

RESULT:

LAN was successfully setup using switch and Ethernet cable.

Exercise : 5 Packet capturing tool : Wireshark

DATE :

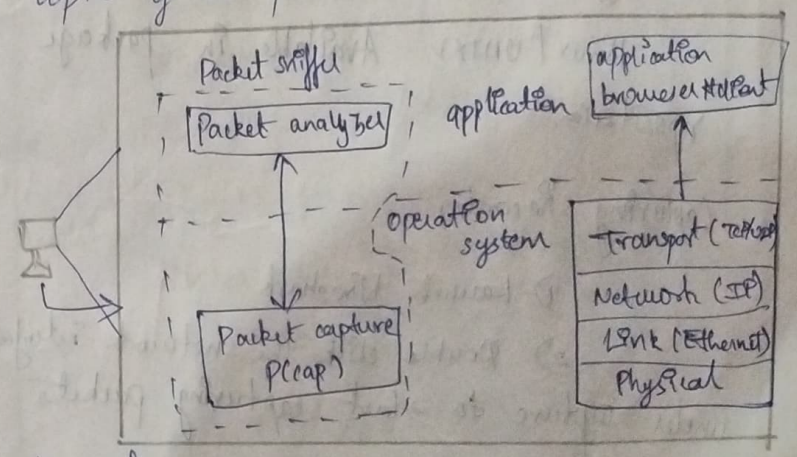
AIM :

Experiments on Packets capture tool : Wireshark

Packet sniffer captures messages in sent / received by your computer

Functions : stores and displays protocol fields in message.

* Passive : Does not send packets or receives packets addressed to it only receive copies of all packets



Wireshark :

Wireshark is a network analysis tool that captures and displays packets in real time. It features filters color coding and detailed discription capabilities.

Features :

* capture network traffic
* Decode packet protocols with dissectors.

* Analysis network problem
* Browse traffic interactively

Uses:

network administrators Troubleshoot network Issues.

network security engineers. Examine security problems.

Getting Wireshark:

Windows / mac Os : Download from the offical website

Linux / UNIX: Available in package repositories.

Capturing Records:

1) Launch Wireshark

2) Double click the network interface under capture to start capturing packets

The Wireshark Network Analyse

File Edit View Go capature Analyse

Welcome to Wireshark

Capture:

using this filter Enter a capture filter

VirtualBox Host - only network

wifi

VmWare Network Adapter VmNe

Ethernet - 2

Ethernet -

Sample:

Use sample files to practice in wireshark open file via -> open.

Altering Packets

Apply filter to focus on specific network traffic use other apps to isolate traffic for analysis Type a filter enter eg: dns

use analyse > display filter to pick or save filters see the docs for more

Create a file to display only DNS packets + provide flow graph.

Go to capture -> option
select stop capture after 100 packets
click start capture
save packets

Create a filter to display only http packets

Go to capture -> option
select stop after 100 packets
save the packets

Create a filter to display only IP/TCP packets and inspect the packet

select LAN, go to capture option
Select stop capture after 100 packets
search start capture
search ICMP/ IP packets in search bar
save the packets

capturing + analysing packets using wireshark tool To filter, view packets from the ethernet

select LAN, go to capture -> option
select stop capture automatically after
Then check start capture
save the packets

Capturing & analysing packets using wireshark tool to filter, view capture too packets from ethernet

Procedure:

Select LAN go to capture -> option
Select step captures automatically after 100 packets then check start capture
save the packets

Create a filter to display only TCP/UDP packets

Inspects the packets & provide flow graph select LAN, go to capture -> opti
Save the packets

RESULT:

Thus the experiment on packet capture tool wireshark is executed successfully

EX: 5 student observation

1) What is promiscous mode?

A network interface in promiscous mode captures all traffic on the network segment regardless of destination address.

2) Does ARP packets has transport layer header? Explain

Arp packets do not have transport layer header. They operate as datalink layer to map ip address to mac addr.

3) What transport layer protocal is used by DNS

DNS primarily uses DNS for queries & responses & TCP for zone transfer.

4) What is the port number used by HTTP protocal

The HTTP - protocol uses port 80 by default communication.

Exp:- 6
12/9/24

Hamming Code

AIM:-

Write a program to implement error detection and correction using hamming code concept. Make a test run to input data stream and verify error.

Receiver:-

Create sender programs with below features

1. Input to sender file should be a text of any length.
2. Program should convert text to binary
3. Apply hamming code concept.
4. Save this output in a file called channel
5. Apply hamming code on the binary data to check
6. Else remove the redundant & convert the binary data to ascii & display the output

Code:-

```
import numpy as np
# fn to convert text to binary.
def text_to_binary (text)
    return "join (format card (char) +08b') for
char into text)
def binary_to_text (binary)
chars [binary [i:i+8] for i in range (0, 8)]
return "join' (chr (int (char, 2)) for char in chars)

# fn to calculate redundant bits
def calc_red_bits (m)
    r=0
    while (2^r ≤ m+r+1)
        r+=1
    return r

def pos_red_bits (data, r)
    j=0
    k=0
    m = len (data)
    res

for i in range (1, m+r+1)
    if i=2+j
        j+=1
else:
    res = res + data [k]
    k=+1
return res
```

```
def cal. parity - bits (arr, r)
    n = len (arr)
    arr = list (arr)
    for i in range (r)
        p = 0
        pos = 2**r;
    for j in range (i, n+1)
        if j & pos:
parity = int (arr [j-1])
        arr [pos-1] = str(p)
        return join (arr)

def detect correct (data, r)
    in = len (data)
        res = 0
# calculate parity bits
    for i in range (r)
        parity = 0
        pos = 2*i
    for j in range (i, n+1)
    parity n = int (data [j-1])
if parity != 0
        res += position
if res != 0
print ("error at pos : (res)")
    data = list (data)
    if res <= n
data [res-1] = '0' if data [res-1] == '1' else
print ("Error corrected at pos (res)")
else
    print ("error pos out of range. No
correction")
    corrected data = join (data)
    return corrected data
else
    print ("No error detected")
        return data:

def remove bits (data, r)
    j = 0
    orignal data = ''
for i in range (i < len (data +1)):
    if i == 2 ** j:
    j += 1
else
    orginal data r = data [i-1]
    return orignal data
if position < 1 or position > len (data)
print ("Error pos is out of range)
return data.
```

```
data [position-1] = '0'
if data [position-1] == '1' else '1'
print ("Introduced error at pos: {position}
return join(data)

def sender (text):
    binary_data = text_binary (text)
        n = len (binary_data)
        r = calc_red_bits (n)
        arr = pos_redundant_bits (binary_r)
        arr = calc_parity_bits (arr,r)
print ('f' sender output (binary with
    redundant bits {arr}")
    return arr

# receiver program
def receiver (data):
    r = calc_red_bits (len (data))
    corrected data = detect_correct (data_r)
    ascii output binary to text (original data)
print (f" decoded text: {ascii_p}")

channel data = sender (input text)
receiver (corrupted_data)
```

Output:-

Enter the text to be encoded. ok

sender message in binary : 0110000101101011

no. of. parity bits : 5

parity bits redundent bits for sent message

P1 : 1

P2 : 0

P4 : 1

P8 : 1

P16 : 1

The hamming code for even parity : 1001110100010111101011

Enter pos to change the bit : 6

Recieved msg in binary : 0110000101101011

Decoded msg : ok

RESULT Thus the above code has been executed successfully

Exp No: 7 Sliding Window
7/10/24

AIM:
Write a program to implement flow control at data link layer using sliding window protocol from one node to other.

Create a sender program with followings:

1. Input window size
2. Input a text message from user
3. Consider 1 char per frame
4. Create a frame with following feilds
5. Send the frames
6. Wait for the acknowledgement from the receiver.
7. Read a file called receiver buffer
8. check ACK feild.
9. If the no is as expectable, send how set of frames accordingly. Else if NACK is received resend the frames.

create a receiver file:

1. Read a file named sender buffer
2. check the frame no
3. If the Frame no are as exempted write the approx Ack no in the receiver buffer file.

code:
```
import time
import random

class frame:
    def_init - (self, frame, no data):
        self.frame - no-frame-no
        self-data - data
        self-acklowledge-false
    def send frames (frames, window-size)
print ("sending frames")
for i in range (window, size)
    if i < len (frames [i] acknowledge
print (" sent frame { frame [i]. frame no};
    { frame [i] data)
def receiver frames | frames, window, size)
    for i in range (window size)
if random. random () < 0):
```

```
frames [i]. acknowledge . True
def sliding window protocol()
window_size = int (input ("Enter window
size"))
message = input ("Enter an message to send")
frames = [Frame [i, message[i]]
for i in range (len (message))]
base = 0
while base < len (frames)
send_frames (frames [base:], windowsize)
while base < len (frames) and frames [base]
ack base += 1
if base < len (frames):
    print ("Resending ask ack frames")
    time sleep (2)
if name == "main":
sliding - window_protocol()
```

Output :-

```
Enter window size = 3
Enter a message to send : hello
--- sending Frames ---
sent frame 0 = h
Frame sent 1 waiting for acknowledgement
sent frame 1 = e
Frame sent 2 waiting for acknowledgement
sent frame 2 : l
Frame sent, waiting for acknowledgement
sent frame 3 : l
Frame sent, waiting for acknowledgement
sent frame 4 : o
Frames sent, waiting for acknowledgment
--- Receiving Frames ---
Received frame 0 : h [OK]
Received frame 1 : e [OK]
Received frame 2 : l [OK]
Received frame 3 : l [OK]
Received frame 4 : o [OK]
```

21/11

RESULT :-

Thus the sliding window protocol has been executed successfully.

Exp: 8A
13/10/24

Virtual LAN

AIM - (a) simulate - virtual LAN configuration using Cisco packet tracer simulation.

Device	Interface	IP address	subnetmask	Default
S1	VLAN-1	192.168.1	255.255.255.0	N/A
S2	VLAN-1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1

part 1: Build the network and configure basic devices settings

step-1: Build the network

obj: connect the device as shown in the topology

Steps:

* Drag switch S1 & S2 to the rack
* Drag PC-A and PC-B to the table & power them on
* Connect the devices with copper

step2: Assign VLANs to switch interfaces

objective: Assign ports to VLANS

* Assign PC-A to VLAN 10
* Remove the management IP addr from VLAN & configuration.

steps:

* Assign PC-A to VLAN 10
* Remove the management IP addr
* verify with show VLAN brief and show IP interface.

Part-3 Maintain VLAN port assignment and the VLAN addr

step1: Assign multiple interfaces to a VLAN

step2: Remove VLAN assignment from an Interface

steps: Use the no switch port access VLAN command to remove VLAN assignments

Part-4: configure an 802.1Q Trunk between switches.

step 1 :- Use DTI to initiate tracking.

step2 :- configure basic switch settings

obj :- configure both switches

steps :-

* use the terminal in each pc to console the switch & enter privileged EXEC mode.

* set the device name for each switch
* set the privileged exec password
* set the console password and enable
* Encrypt plaintext password.

steps : configure pc rests

obj : Assign ip addr to PCA and PCB

steps :- In ip config input the ipd address for PCs 1st connectivity.

step 4 :- Test connectivity

obj : Test pings between devices close configuration window.

step :- Assign PCA to VLAN10 (operations) Remove the management ip address from VLANs

part 4 : configure an S2 / a truck between switches.

step 1 : Use DTP to initiate trucking

obj : configure dynamic tracking.

verify using show interfaces trunk & ensuring is enabled between S1 & S2

Questions :-

1. can S1 ping S2 ?

Yes if trucking is successfully configure

S1 can ping S2

2. can PC-A ping PC-B?

Yes, if VLANs are properly configured trunking is enabled PC-A can ping PC-B

Reflection questions :-

1. What is needed to allow host an VLAN to communicate to host on VLAN. 99?

We need a 3 layer devices such as a router or a 3 layer switch the VLAN routing configuration.

2. What are the primary benefits that an organisation can receive through effective?

* Improved network segmentation

Student observation:

a) Draw and label the VLAN for 10 faculty in robotics department, sitting in 2 different

b) show the ip configuration for each device

faculty-1 192.168.10.1/24 faculty-2 192.168.10.2/24
faulty-3 192.168.10.3/24 faculty-4 192.168.10.4/24
faulty-5: 192.168.10.5/24 faculty-6 192.168.10.6/24
faulty-7: 192.168.10.7/24 faculty 192.168.10.8/24

c) Write the commands

switch (config) # vlan 10
switch (config-vlan) # name Robotics-VLAN
switch (config-vlan) # exit
switch (config-if-range) # switch port access
switch (config-if) # exit.

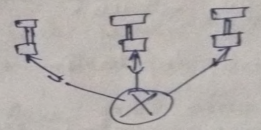
RESULT:- Thus the above exercise is executed successfully.

EX NO:- 8b

AIM:- To design a topology with three PCs connected from linksys wireless routers

Procedure:-

Configure static ip on PC and wireless router set SSID to mothu network set IP address of router to all PC's. connect your PC by WAP Key.



Step 1 click on wireless Router

stepup wireless security Access Administration

Management Router pass: admin
Router Access Router pass: admin

setup wireless security. Access restriction Administration

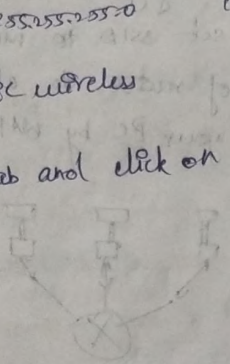
security mode Disabled
Disabled
wep.

Now configure the static ipon all three PCs and set the subnet mask

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

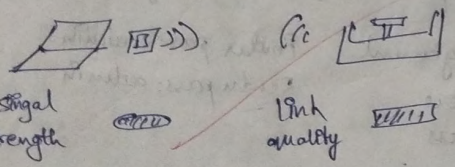
Click PC wireless

click on connect tab and click on refresh button.



WEP Key
security WEP
WEP: 0x0A
WEPKEY1: 0123456789

Cancel cannot



Repeat for all PC's

RESULT: Thus the above exercise is executed and verified successfull.

Student observation:

1). What is SSID a wireless router

The SSID service set identifier of wireless router. It allows devices to connect to it

2) What is a security key in wireless router

A security key in a wireless router is a password used to protect a wifi network.
WPA2 keys

3) Configure a simple wireless LAN in your LAB using a real point & write down the configur in your network.

Access point setup. connect the access point to power and network the access

eg:- 192.168.1.1

set SSID name and configure

set security mode WPA2-PSK.

Password: set a key.

Ex:9
8/10/24

Subnetting

AIM:

Implementation of subnetting in cisco packet tracer simulator

classless ip subnetting is a techique that allows for more efficied use of ip address by allowing for subnet mask that are just the default masks. when we leave limited no of ip addr but need to create multiple network

Creating a network topology:

Once we have created our network topology we can add devices to it. Here we will be adding routers, switches, PCs to add a devices select the devices topology.

The ip addressing for the network shown in the topology can be as followed

Router R_1:

Switch S1:

Fast

PC1 : 192.168.1.11

PC2 : 192.168.1.12

PC3 : 192.168.1.13

PC4 : 192.168.1.14

PC5 : 192.168.1.15

Fast ethernet 0/2
192.168.2.0/27

PC1 : 192.168.2.11

PC2 : 192.168.2.12

PC3 : 192.168.2.13

PC4 : 192.168.2.14

PC5 : 192.168.2.15

Router R_2
switch S2

Fast ethernet 0/1
192.168.30/27

PC1 : 192.168.3.11

PC2 : 192.168.3.12

PC3 : 192.168.3.13

PC4 : 192.168.3.14

PC5 : 192.168.3.15

Configure the devices:-

Router configuration

configuration interface

Fast ethernet 0/0:

Enter: Interface ethernet 0/0

Active: no shutdown

Exit: Interface configuration: exit

Fast ethernet 0/1:

* Repeat the above steps.

Configure gigabit ethernet:-

switch configuration:-

Enter enable and configure terminal

Enter interface fast ethernet 0/1 then switchport mode access, exit

Repeat for fast ethernet 0/2 for connecting to the second PC

PC configuration:-

* Must be in the same subnet as the router i.e fastethernet 0/1 interface

* set to the fastethernet 0/1 interface

* Enter DNS detail or reached.

Testing the network:

A successful ping indicates proper pc-to-p communication

RESULT:-

Thus the above connection in also packet tracer was executed successfu

Student observation

a) Write down your understanding of subnetting.

Subnetting is the process of dividing a large network into small manageable sub networks Each subnet operation.

b) What is the advantage of implementing subnetting with a network.

Ex:10 Internetwork using a routers
10/10/24

AIM:

Internetworking with routers in cisco

Packet Tracer Simulatator

Design and configure a simple Internetwork using a router

In this network, a router and 2 hs are used. Computers are connected with routers using a copper straight-through cable. After forming the network, to check network connectivity a simple ps transfer from PC0 to PC1

Procedure:

step1 (configuring router)

1) select the router and open CLI

2) Press Enter to start configuring router

3) Type enable to activate the privileged mode

step2: (configuring Pcs)

1) Assign IP address to every Pc in the network

2) Select the Pc, to the desktop and select IP configuration and assign an IP address, Default gateway, subnet Mask

step3 Connecting PCs with Router

1) Connect Fast Ethernet 0 port of PC0 with Fast Ethernet 0/0 port of Router 1 using a copper straight-through cable.

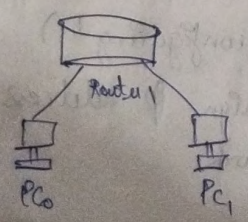
2) Connect Fast Ethernet 0 port of PC1 with Fast Ethernet 0/0 port of Router 1

Router configuration Table

Device name	IP addr Fast Ethernet	Subnet mask	IP addr Fast Ethernet	Subnet mask
Router	192.168.10.1	255.255.255.0	192.168.20.1	255.255.255.0

Pc configuration Table

Device name	IP addr	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



RESULT

Thus the Internetworking with routers in CISCO has be Implemented successfully.

Ex 10.b Internetwork using wireless router
28/10/24 DHCP server and Internet cloud

AIM:-
Design and configure an Internetwork using wireless router, DHCP, server and Internet cloud

Address table:-

Device	Interface	IP address	Subnet mask	Default gateway
PC	Ethernet0	DHCP		192.168.0.1
wireless Router	LAN	192.168.0.1	255.255.255.0	
wireless Router	Internet	DHCP		
cisco.com server	Ethernet0	208.67.220.220	255.255.255.1	
Laptop	wireless0	DHCP		

Objective:-
Part1:- Build a simple network in Logical Topology workspace.
Part2:- configure the network devices
Part3:- Test connectivity between Network devices.

Part-4 : Save the file and close packet tracker

Part 2:- configure the network devices

Step1:-
configure the wireless router
a) Create the wireless network on the wireless router. change all the nessary
b) save the settings

Step 2:-
configure the laptop
a) configure the laptop to access the wireless network

Step:- 3
a) configure the PC for the wired network

Step4:- configure the Internet cloud
a) Install network modules if nessary
b) Identify the From and to ports
c) Identify the type of provider

step 5:-

configure the cisco.com server.

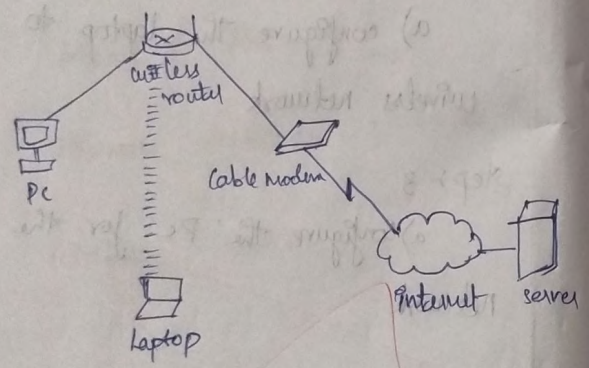
a) configure the cisco.com server

b) configure the cisco.com server global settings

Part-3 verify connectivity

step1:- Refresh the IPV6 settings on the PC

Test connectivity to the cisco.com server from the PC



student observation

1) Key feature of configuration wireless routers and DHCP servers

Ans * wireless router configuration set the SSID (network name), security type (WPA2 or WPA3) and method to secure network access.

* DHCP server configuration :- Enable the DHCP server to automatically assign IP address to devices on network.

2) What is the significance of DHCP server in internetworking.

* Automated IP assignment. DHCP simplifies IP address management by dynamically assign IP addr to devices. reducing the risk of IP conflicts and manage errors

RESULT

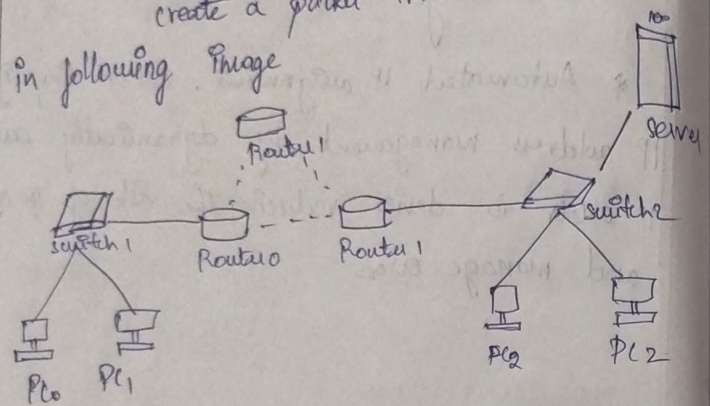
Thus the internetworking using wireless router, DHCP server and Internet-cloud is implemented successfully.

Ex: 11a
4/11/24

Static Routing

AIM:
simulate static routing configuration using cisco packet tracer

setting up a practice lab:
create a packet tracer lab as shown in following image



The following table lists the connected networks

Router	Available networks on local interfaces	network available on other router's
Router 0	10.0.0.0.18, 20.0.0.0.18, 40.0.0.018	30.0.0.0.18, 50.0.0.0.18
Router 1	20.0.0.0.18, 30.0.0.018, 50.0.0.0.18	10.0.0.018, 40.0.0.018
Router 2	40.0.0.0.18, 50.0.0.0.18	10.0.0.018, 20.0.0.0.18, 30.0.0.018.

Router 0 configuration

enable configure terminal.

ip route 30.0.0.0 255.0.0.0 20.0.0.2.10

ip route 30.0.0.0 255.0.0.0 40.0.0.2.20

ip route 30.0.0.100 255.255.255.255 40.0.0.2.10

ip route 30.0.0.100 255.255.255.255 20.0.0.2.20

ip route 50.0.00 255.0.00 20.0.02.20

exit

Router 1 configuration:

enable configure terminal

ip route 10.0.0.0 255.0.0.0 20.0.0.1 10

ip route 10.0.0.0 255.0.0.0 50.0.0.1 20

ip route 40.0.0.0 255.0.0.0 20.0.0.1 10

ip route 40.0.0.0 255.0.0.0 50.0.0.1 20

exit

Router 2 configuration

enable
configure terminal

ip route 10.0.0.0 255.0.0.0 40.0.0.1

ip route 30.0.0.0 255.0.0.0 50.0.0.2

exit

Verifying static routing

tracert command sends ping requests to destination host and traces the path they take to reach.

RESULT:

Thus the static routing configuration has been implemented successfully.

Ex:- 11b
4/11/24

RIP using cisco packet tracer

AIM:

Simulate RIP using cisco packet tracer

Initial IP configuration

Devices	Interface	IP configuration	connected with
PC0	Fast Ethernet	10.0.0.2/8	Router0's Fa0/
Router0	Fa0/1	10.0.0.1/8	PC0's fast Ethernet
Router0	S0/0/1	192.168.1.254/30	Router 2's S0/0/1
Router0	S0/0/0	192.168.1.249/30	Router 1's S0/0/0
Router1	S0/0/0	192.168.1.250/30	Router0's S0/0/0
Router1	S0/0/1	192.168.1.246/30	Router 2's S0/0/0
Router2	S0/0/0	192.168.1.245/30	Router 1's S0/0/
Router2	Fa/1	20.0.0.1/30	PC1's Fast Ethern
PC1	Fast Ethernet	20.0.0.2/30	Router 2's fa0

Assign IP address to interfaces of routers

* set the clock rate for DCE and not for the DTE end

* show controllers interface gives whether the interface is DCE or DTE

Configure RIP routing protocol

Router0

router rip
network rip
network 10.0.0.0
network 192.168.1.252
network 192.168.1.248

Router1

router rip
network 192.168.1.244
network 192.168.1.248

Router2

router rip
network 10.0.0.0
network 192.168.1.252
network 192.168.1.244

Access the command prompt of PC1 and use ping command to test the connectivity.

RESULT

Thus the simulation of RIP using Cisco packet tracer

Ex: 12a
6/11/24

Echo client server using TCP/UDP sockets

AIM: implement echo client server using TCP/UDP sockets

Algorithm (server):

1) Create a TCP socket
2) Build socket to local address port
3) Listen for incoming client connections
4) Accept a client connect
5) Loop
   * recive data from client
   * else break loop
6) close the connection.

Algorithm (client)

1) Create TCP socket
2) connect to server, using specified address & port
3) send a message to server
4) Receive the echoed message from the server.
5) Display received message
6) Close the socket.

Program:

server.py

```
import socket
def tcp_server()
    server_socket = socket (socket: AF_INET, socket.sock_STR)
    server_socket.bind ("localhost", 12345))
    server_socket.listen (1)
print ("TCP server is written for a connection)
connection, client_address = server_socket.accept()
    print ("connected to {client_address}"),
try
    while, True
        data, connection.recv(1024)
    if data
        print (f"Received : {data.decode()}")
else
    break
finally
    connection.close()
if_name = "main"
    tcp_server()
```

tcp_client.py

```
import socket
def tcp_client()
    client_socket = socket.socket (socket.AF_INET, socket.sock)
client.socket.connect (("localhost", 12345))
try.  message = input "Enter a message to send")
    client_socket.sendall (message.encode())
    data = client.socket.recv (1024)
    print (f" Received from server : {data.decode}
finally
    client socket.close()
    if_name = "__main__"
        tcp_client()
```

Output:

Terminal: 1

Tcp_server.py

```
PS. C:\Education\sems\CN\lab\python -u "C:\Education\sems\CN\lab\EX12\tcp_server.py"
Tcp server is waiting for a connection...
connected to ('127.0.0.1', 53356)
Received : hello this is tcp client
```

Terminal 2

TCP-client.py

Enter message to send hello this is tcp client Received from server: hello this is tcp client.

Result

Thus the program to echo client server using TCP/UDP sockets is executed successfully.

Ex) 12b 6/11/24 chat program using socket programming

Aim: To implement the chat client server using TCP/UDP server

Algorithm:

chat server

1) start the server by creating a socket, bind to a specific address and port, listen for incoming connections

2) When a new client connects and client a list of clients start a new process to talk too the clients

3) For each connected client keep checking new messages.

4) Keep running the process till the server stop

chat client

1) connect to server by creating a socket

2) start a process to listen to message from the server

3) Keep running till the user decides to quit

chat_server.py

```
import socket
import threading
def handle_client (client_socket)
  while True:
    try: message = client_socket.recv (1024)
encode
    if not message:
        break
    print (f" Received message from client {message}")
    client_socket.send (respone.encode ('utf8'))
client_socket.close()
def start_server()
    server = socket.socket (socket.AF_INET,
socket_sock_STREAM)
    server.bind (('127.0.0.1', 12345))
    server.listen(5)
    print ('chat server started on 127.0.0.1:12345')
while True
    client_socket, addr = server.accept()
    print(f" New connection from {addr}")
    client_handr.start()
```

chat_client.py

```
import socket
import threading
def recive_massag (client_socket)
while True:
    Try
        message = client_socket.recv (1024).dec
    if message
        print (f" server: {message}")
    except Exception as e:
    print (f" An error occured = {e}")
    break.
def start_client()
    client_socket = socket.socket (socket.AF_
INEY, socket.sock_stream)
    host = '127.0.0.1'
    port = 12345
    client_socket.connect ((host, port))
print (" Connected to the chat server.")
if __name__ = "__main__":
    start_client()
```

Output:

Terminal=1

chat_server.py

chat server started on 127.0.0.1:12345

New connection from ('127.0.0.1', 53686)

Received message from client: hello this is chat client

Type your message to client = hello this is chat server

Terminal:2

chat_client.py

connected to the chat server

You: hello this is chat client

You: server: hello this is chat server.

RESULT:

This the program to implement chat program using socket programming is executed successfully.

Ex No: 13
8/11/24

Ping Program

AIM:

Implement your own ping program

Algorithm:

ping_client.py

1) socket creation

2) Then set a timeout of 2 second to ensure if no respone is recieved it will stop waiting and print "Request point"

3) send a 'ping' msg to specified host post

Ping_server.py

1) Initialize UDP socket

2) Bind to IP address & port

4) Reverse data

5) send response

Program:

ping_server.py

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

```
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()
```

Ping_client.py

```
import socket
import time
def ping_server (host = '127.0.0.1', port=12345):
with socket.socket (socket.AF_INET, socket.sock_
try:
    s.settimeout (2)
    start = time.time()
    s.sendto (b'ping', (host, port))
    data, addr = s.recv from (1024)
    end = time.time()
    print (f "Received {data.decode ()} from
{addr} in {end-start: 2f} seconds")
except socket.timeout
    print ("Request timed out")
if __name__ == "__main__":
    ping_server()
```

Output:-

Terminal 1

```
ping_server.py
UDP server running on 127.0.0.1:12345
Received message from ('127.0.0.1', ) = Ping
```

Terminal 2

```
ping_client.py
Received pong from ('127.0.0.1', (12345) in 0.00
seconds
```

RESULT:

Thus the ping program has been executed successfully.

Ex: NO: 14
9/11/24

Packet Sniffing

AIM:-
write a code using RAW sockets to implement packet sniffing.

Algorithm

1) Install python and scapy
2) Create a program open text editor and create a file in notepad called.
3) setup packet tracer by check if packet has IP layer, identify the packets
4) Run the packet snippet by using command
5) Run the packet snippet by using command

Program:-

```
from scapy.all import sniff
from scapy.layer.inet import IP, TCP, UDP, ICMP
def packet_callback (packet)
    if IP in packet
        ip_layer = packet [IP]
        Protocol = IP_layer.proto
        src_ip = ip_layer.scr
        if protocol == 1
            protocolname = "KMP"
        elif protocol == 6
        protocol_name = 'TCP'
        protocol_name = 'UDP'
else:
        protocol_name = 'unknown protocol'
        print (f"protocol = {protocol_name})
        print (f" Destination IP = {dst_ip}")
        print ("_"*50)
if __name__ == "__main__"
    main()
```

output:

```
protocol = UDP
source IP = 172.16.33.84
Destination IP = 244.0.0.251
Protocol = UDP
source IP = 172.16.33.84
Destination IP = 244.0.0.251
Protocol : UDP
source IP = 172.16.32.182
Destination IP = 8.8.8.8
```

24/11

RESULT:-
Thus the packet sniffing program has been executed successfully

EX: 15 Webalizer

7/11/24

AIM:

To analyse the different types of weblogs using webalizer tool

Algorithm:

* At first you must have installed Xampp and hosted

* In the web alizer. config update the destination path to store the weblogs

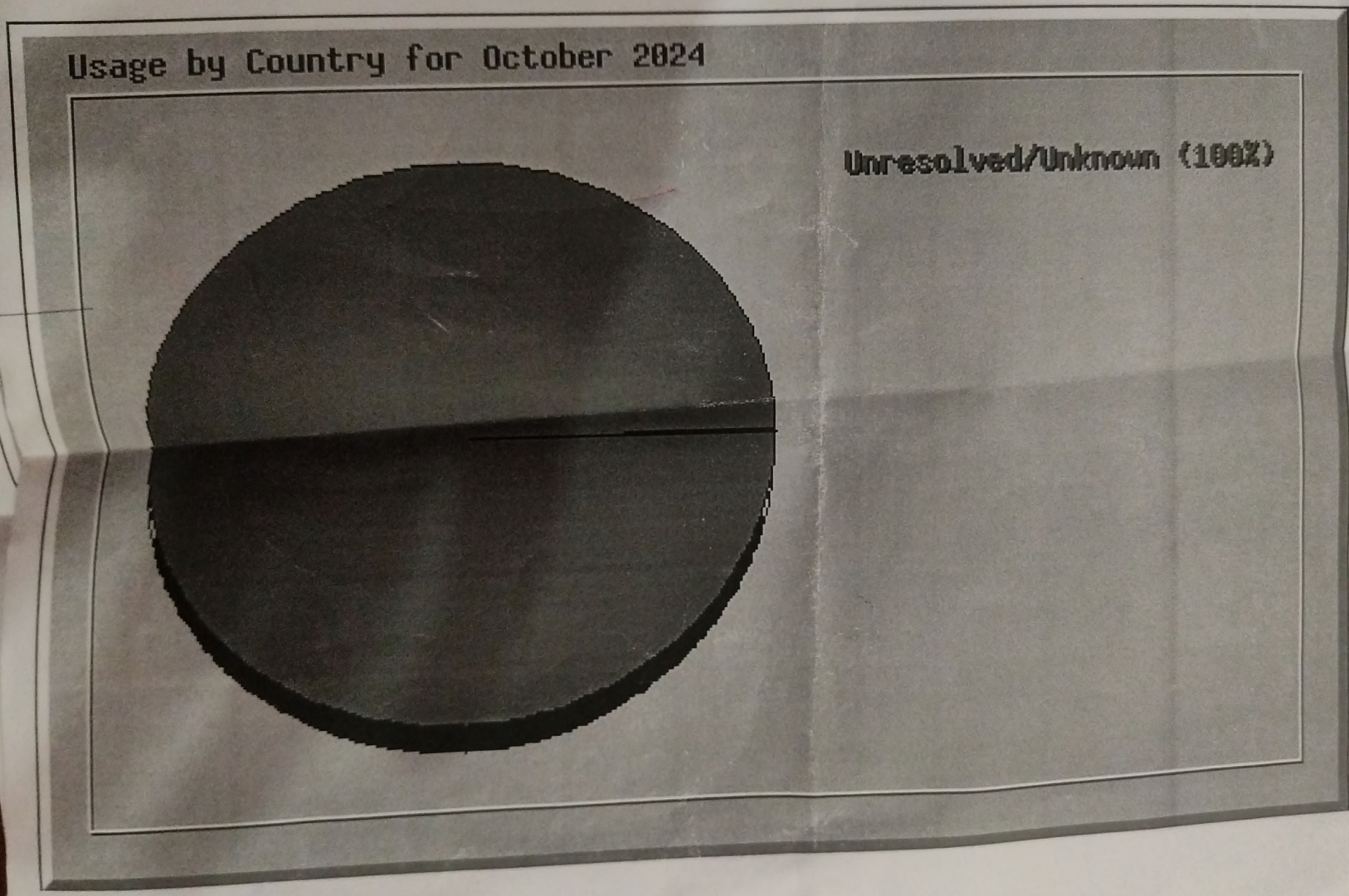
* After updating it open command prompt

* The result is stored in the updated destination path

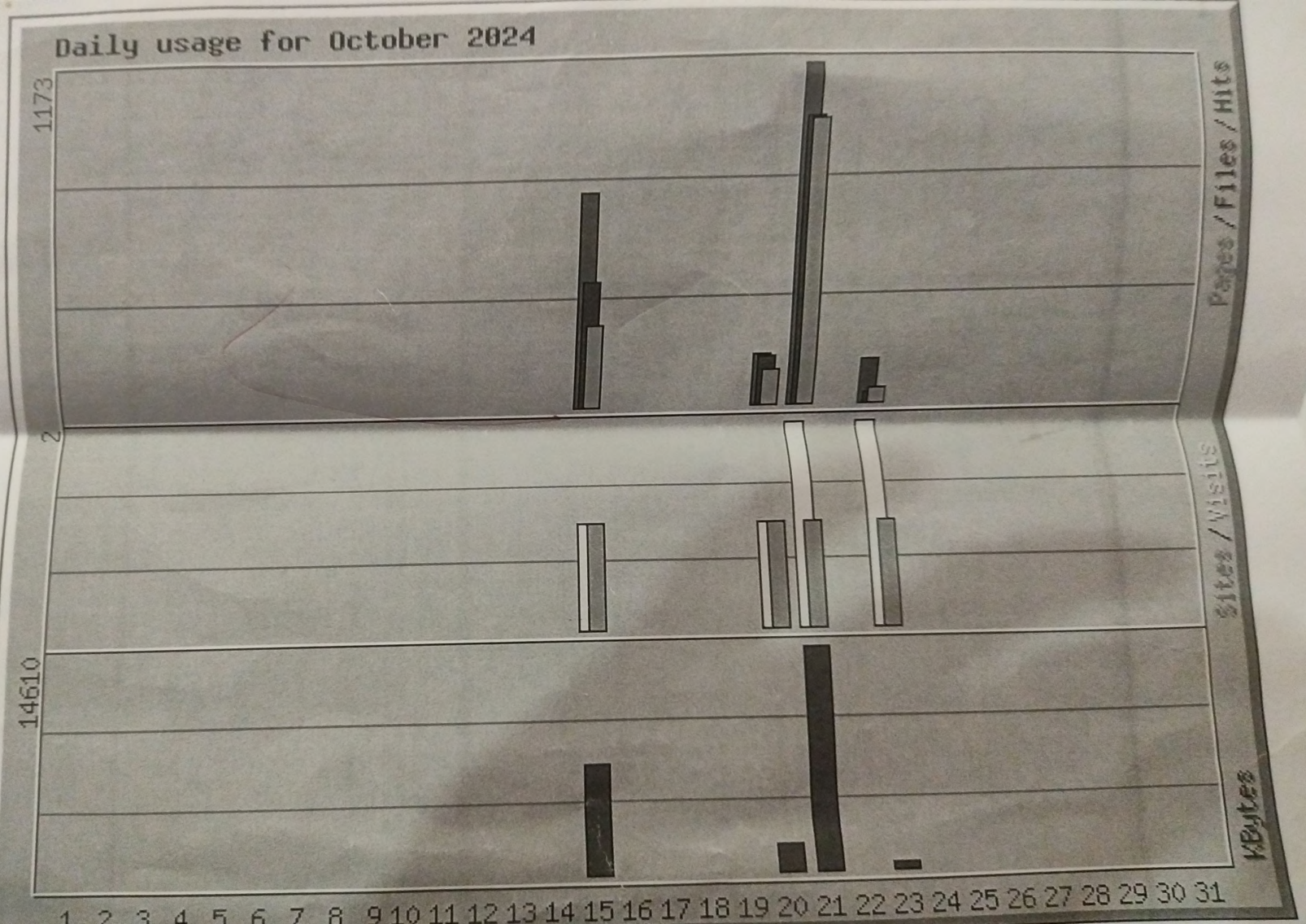
* check the various logs in the index.html file.

RESULT

Thus the different types of weblogs has been analysis using webalizer tool.


Usage by Country for October 2024
Unresolved/Unknown (100%)

Hourly usage for October 2024


Daily usage for October 2024
1173
2
14610
Pages / Files / Hits
Sites / Visits
KBytes
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31