Mychoice

INDEX

NAME G. BALAJI ST IV SEC A ROLL NO 36 SUB CN-OBS

S.No.	Date	Title	Page No.	Teacher's Sign Remarks
1)	13/7/24	STUDY OF VARIOUS NETWORK COMMANDS IN WINDOWS & LINUX		
2)	27/7/24	STUDY OF DIFFERENT TYPES OF NETWORK CABLE		
3)	30/7/24	TO STUDY THE PACKET INTERFACE TOOL & USER INTERFACE OVERVIEW		
4)		LAN USING ETHERNET CABLE		
5)		PACKET CAPTURE USING WIRESHARK		
6)		HAMMING CODE		
7)		SLIDING WINDOW		
8)a)		CISCO PACKET TRACER Virtual LAN		
8)b)		WIRELESS LAN		
9)		SUBNETTING		
10)a)		ROUTERS Interconnecting with routers		
10)b)		INTERNET DHCP SERVER		
11)a)		STATIC ROUTING		
12)b)		RIP USING CISCO PACKET		
12)a		ECHO CLIENT		
12)b)		CHAT CLIENT SERVER		
13)		PING PROGRAM		
14)		RAW SOCKET		
15)		DIFFERENT TYPES OF WEBPAGES		

STUDY OF VARIOUS NETWORK COMMANDS IN WINDOWS

DATE: 13/7/24

EX NO: 1

AIM:

Study of various network commands used in Linux windows.

BASIC NETWORK COMMANDS:

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

Internet Address	Physical Address	Type
172.16.72.1	7C-5A-1C-41	dynamic
172.16.72.133	4C-ae-a3-45-97-f3	dynamic

hostname:

DESKTOP-L0IBH7U

nbstat -a:

NBTSTAT [[-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [interval]]

-a [adapter status] Lists the remote machine's name table given its name.

nslookup:

Default Server: Unknown

Address : 172.16.7.21

pathping:

pathping [-g host-list] [-h maximum hops] [-i address] [-n] [-p period] [-q num-queries] [-w timeout] [-4] [-6] target-name

SOME IMPORTANT LINUX COMMANDS:

ip <OPTIONS> <OBJECTS> <COMMAND>

a) [root@server] # ip address show

1: <LOOPBACK,UP, LOWER-UP> mtu 65536 qdisc sequence

b) [root@server~] # ip address add 192.168.1.254/24 dev enp503

To assign an IP to an interface

c) [root@server~] # ip address dl: 192.168.1.254/24 dev enp503

To delete an IP an interface

d) [root@server~] # ip link set eth0 up.

To alter the status of the interface by bringing the interface enp356mi

To alter the status of the interface

by bringing the interface enp250

[root@server]# ip link set etho promisc

To alter the status of the interface

by enabling promiscuous node for lo.

[root@server~] ip route add default via

192.168.1.254

To add a default route [for all address]

via the local gateway 192.168.254 that

can be reached on device enp350.

[root@server]# ip route add default

via 192.168.1.254 dev eth0

To add a route to 192.168.1.0/24 via the

gateway at 192.168.1.254

[root@server~]# ip route add 192.168.1.0/24

dev eth

To add a route to 192.168.1.0/24 that

can be reached on device enp250.

192.168.1.254

display: → [root @ server ~] # ip route get 10.10.1.4

10.10.1.4 dev ens src 192.168.1.254

rid 1000

cache

ip config

ens160: flags ⇒ 4163 <UP, BROADCAST, RUNNING, MULTICAST> with 1500 ..

inet 192.168.22.128 netmask 255.255.255.0 broadcast 192.168.22.255

mtr

mtr <options> hostname/ip

[root @ server ~] # mtr google.com

keys: help display mode restart statistics order of fields quit

HOST	LOSS %	SNT	LAST	AVG
1) -gateway	0.0%	163	1.2	1.0

BEST	WVRST	STDEV
0.3	6.1	0.6

5) [root @ server ~] # mtr -g google.com

-F, --Filename FILE readhostname[s] from a file

-4 use IPv4 only

-6 use IPv6 only

-u, --udp use UDP instead of ICMP echo

6) [root @ server ~] # mtr -b google.com

-F --Filename FILE read host

4) tcpdump

[root @ server ~] # dnf install. tcpdump

To install -y tcp dump

[root @ server ~] # tcpdump -D

1. ens250 [Up, Running, connected]
2. Any (Pseudo-device that captures on all interfaces) [Up, Running]

[root @ server ~] # tcpdump -i etho

dropped privs to tcp dump

tcpdump: verbose output suppressed

use -v [v] ... for full protocal

packets captured

packets received by filter

packets dropped by kernel

[root@server~]# tcpdump -i

eth0 -c 10 host 8.8.8.8

dropped privs to tcpdump

tcpdump: verbose output

suppressed, use -v[v]

for full protocol decode listening

[root@server~]# tcpdump -i

eth0 src host 8.8.8.8

dropped privs to tcpdump.

tcpdump: verbose output suppressed

use -v[v]. for full protocol

decode listening

[root@server~]# tcpdump -i

eth0 net 10.1.0.0 mask 255.255.

255.0

to capture traffic and to form

a specific network using the command

[root@server]# tcpdump -i eth0

to capture traffic and to form a

specific network using the command

[root@server~]# tcp dump -i eth0

port 53

To capture only DNS port 53 traffic

[root@server~]# tcp dump -i eth0

port not 53 and not 25

To capture all port except port

80 and 25

[root@server~]# ping google.com

PING google.com (216.58.200.142)

56(84) bytes of data 64 bytes

from maa10-in-f14.1e100.net

(216.58.200.142)

: icmp_seq=46tt

root@server ~# ping -c 10 google.com

PING google.com (142.250.193.100)

56(84) bytes of data -- google.com

ping statistics - 10 packets

transmitted, 0 received, +10 errors,

100% packet loss, time 9197 ms pipe 2

RESULT:

Thus the study of various Network communication commands used in Linux & windows is done and executed successfully

CONFIGURING AN ETHERNET CONNECTION BY USING NMCLI

If you connect a host to the network over ethernet, you can manage the connection's settings on the command line by using the nmcli utility

PROCEDURE:

List the Network Manager connection profile

nmcli connection show

nmcli connection add con-name <connection-name> ifname <device-name> type ethernet

nmcli connection modify "Wired connection 1"

nmcli connection show

nmcli connection modify "Wired connection 1" ipv4.method au

Activate the profile

nmcli connection up Internal ...

ip route show default

ip -6 route show default

cat /etc/resolv.conf

TROUBLE SHOOTING:

Verify that the network cable is plugged in to host & a switch.

Verify that the network cable & network interface are working as expected.

STUDENT OBSERVATION:

The command which is used to find the reachability of a host machine from your device?

ping command is used to find reachability of host machine from your devic

Which command will be give the details of hops taken by a packet to reach its destination.

traceroute

Which command displays the ip configuration of our machine

ifconfig

The command which displays the TCP port status?

netstat -tlnp

STUDY OF DIFFERENT KINDS OF NETWORK CABLE

EXP.NO: 2

DATE: 21/9/24

AIM:

Study of different types of network cables.

Understand different types of network cable.

Different type of cables used in networking are:

* Unshielded twisted Pair cable (UTP)
* Sheilded twisted Pair cable (STP)
* Coaxial Cable
* Fibre optic cable

LE PE	CATEG -ORY	MAXIMUM DATA TRANSMISSION	ADVANTAGE DISADVANT -AGE	APPLI -CATION	IMAGE
P	CATEGORY -3 CATEGORY 5	10bps UP TO 100Mbps	ADVANTAGE: CHEAPER EASY TO INSTALL	10 BASE-T ETHER -NET FAST ETHER -NET	
	CATEGORY 5	1 Gbps	DISADVANTAGE MORE PRONE TO EMI ELECTRO MAGNETIC INTERFERENCE	FAST ETHER -NET	

CABLE TYPE	CATEGORY	MAXIMUM DATA TRANSMISSION	ADVANTAGES/ DISADVANTAGES	APPLICATION	IMAGE
STP	CATEGORY 6, 6A	10 gbps	ADVANTAGE: SHELDED FASTER THAN UTP LESS SUCEPTIBLE	GIGABIT ETHERNET WIDELY USED IN DATA CENTRES	
SSTP	CATEGORY 7	1 gbps	DISADVANTAGES: EXPENSIVE GREATER INSTALLATION FORCE	GIGABIT ETHERNET	
COAXIAL CABLE	RG-6 RG-59 RG-11	10-100 Mbps	ADVANTAGES: HIGH BAND-WIDTH IMMUNE VERSATILE	SPEED OF SIGNAL IS GOOD	
			DISADVANTAGES: LIMITED DISTANCE COST		
FIBRE OPTICS CABLE	SINGLE MODE & MULTI MODE	100Gbps	ADVANTAGES: HIGH SPEED, BANDWIDTH DISADVANTAGE: EXPENSIVE SKILLED	MAXIMUM DISTANCE OF FIBRE OPTICS	

5) Make your own ethernet cross-over cable straight cable

Tools and parts needed

Ethernet cabling CAT5 is certified for gigabit support, but CAT5 cabling works as well over short distances

- crimping tool - all-in-one networking tool shaped to push down the pens in the plug and strip & cut the shielding off the cable

To start construct of the device, begin by threading shields onto the cable.

Next strip approximately 1-5cm of cable shielding from both the ends

After, you will need to cut wires. There should be four "twisted pairs".

Once the order is correct, bunch them together in a tube and that is perfect cable

farther from others slip them back to create an even look

Next, push the cable right in the notch as the end of the plug, insert it into crimping tool & push down.

Lastly, repeat for the other end using diagram(B) using diagram(A)

RESULT;

The study of different kind of cable networks have been done successfully.

STUDENT OBSERVATION

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

The difference is the wiring configuration at each end, with cross cables having some wires crossed over & straight cables having the same wiring configuration at both ends

2) Which type of cable is used to connect two PC?

cross cable

3) Which cable is used to connect a router/switch to your PC:

Straight cable is used to connect a router/switch to your PC

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

5e or c6 twisted pair cable is commo
used to connect a pc to a network sorce

6) Write down your understanding,
challenges faced & output received wh
making a twisted pair/straight cab
Making a twisted pair cable requires
careful wiring configuration, twisting
& crimping to ensure a secure &
reliable connection

EXP NO: 3

DATE: 30/7/24

AIM:

To study the packet tracer tool installation & user interface overview

2) To understand environment of CISCO PACKET TRACKER to design simple network

INTRODUCTION

A simulator as the name suggests, simulates network devices and its environment.

It allows you to model complex systems without the need for dedicated equipment

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

It is available for both the Linux & window desktop environment

INSTALLING PACKET

To download Packet tracer go to https://www.netacad.com & log in with your cisco networking academy credentials, then click on the packet installation in windows is pretty simple and straightforward. The setup comes in a single file named as setup [illegible].exe. Open this file to begin the setup wizard, accept the licence agreement, choose a location and start the installation.

LINUX:

Linux users with an Ubuntu/Debian distribution should download the file for Ubuntu, and those using Fedora/Redhat/ must download the file for [illegible]

chmod +x PacketTracer [illegible] Installer [illegible]
bin ./PacketTracer [illegible] Installer
[illegible]

USER INTERFACE OVERVIEW:

MEMBER: This is a common menu found in all software applications, it is used to open, save, print.

This bar provides shortcut to menu options that are commonly accessed, such as open, save, zoom undo & redo and on the right.

LOGICAL / PHYSICAL WORKSPACE TABS: These tabs allow you to toogle between the logical & Physical work areas.

WORKSPACE: This is the area where topologies are created and simultaneously displayed.

COMMON TOOL BAR: This toolbar provides controls for manipulating topologies.

REAL-TIME / SIMULATION TABS: These tabs are used to toggle between the real & simulation modes. Buttons are also provided to control the time.

NETWORK COMPUTER INTERFACE: This component contains all of the network and end devices available with Packet tracer and is further divided into two areas: Area 1: Device-Type selection box.

USER-RELATED PACKET BOX: Users can create highly-customised packets to test their topology from this area, and the results are displayed on a list.

4) ANALYSE THE BEHAVIOUR OF NETWORK DEVICES USING CISCO PACKET TRACER SIMULATION:

From the network component or click and drag-and-drop. The below components.

a. 2 Generic PCs & One HUB

b. 2 Generic PCs & one Switch

click on connections

click on copper straight-through cable.

Select one of the PC and connect it.

Similarly connect 4PCs to the switch using copper straight-through cable

Click on the PC connected to the... desktop tab, click on IP configura... the default gateway and DNS server information is not needed as there are only two end devices in the map

Click on the PDU from the command... tool bar.

Drag & drop it on one of PC & the... another PC connected to the hub

Observe the flow of PDU from... source PC to destination PC

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

Observe how hub & switch are forwarding the PDU & write ...

RESULT: The study of packet tracer ... interface installation has been done successfully

STUDENT OBSERVATION

a) From your observation write down the behaviour of switch & hub in terms of forwarding the packets received by them.

A switch forward packets only to the intended recipient, whereas a HUB broadcasts packets to all connected devices

b) Find out the network topology implemented in your college & draw & label that topology in your observation book.

Network topology implemented in my college is a hybrid topology

EXPT.NO DATE

AIM:
Setup & configure a LAN using a switch & Ethernet cables in your lab.

What is LAN:

A LAN 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.

HOW TO SET UP LAN

STEP1:
Plan & design an appropriate network topology taking into account network requirements.

STEP2.
You can take 4 computers, a switch with 8, 16 or 24 ports which is sufficient for networks of these sizes & Ps Ethernet cables.

STEP3:
Connect your computers to network switch via an ethernet cable, which is a as simple as plugging one end of ethernet cable into your computers.

STEP4:
Assign ip address to your PC's

1) Log on to the client computer as administrator or as owner.
2) Click network & internet connections.
3) Right click LAN
   Go to properties → select internet select use the following ip address option & assign ipaddress.

STEP 5:
Configure a network switch
Connect your computers to the switch.

To access the switch's web interface, you will need to connect your computer to switch using an Ethernet cable

Log in to web interface: Open a web browser & enter IP address. Enter the username & password to log in.

Configure basic settings: Once you're logged in you will be able to configure basic settings

Assign IP address as 10.1.1.5

STEP 6:

Check the connectivity between switch & other machine by using ping command in command prompt of the device.

STEP 7:

Select a folder → go to properties → click sharing tab → with same LAN

STEP 8:

Try to access the shared folders from other computers of the network

EXP NO: 5 DATE:

AIM: Experiments on Packet capture tool: Wireshark

Sniffs messages being sent/received from/by your computer

Passive Program

never sends packet itself

no packets addressed to it

receives a copy of all packets

Tcpdump: -Eg: tcpdump -enx host 10.129.41.2 -VV exe3.out

Wireshark

-wireshark -r exe3.out

DESCRIPTION:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. You can use Wireshark to inspect a suspicious program network traffic, analyze the traffic flow on your network or troubleshoot network problem

Capture network traffic

Watch smart statistics

Analyze problems.

Network administrators: Troubleshoot network problems.

Network security engineers: Examine security problems

People: Learn network protocol internals

Wireshark can be downloaded for windows or macOS from its official website

CAPTURING PACKETS:

After downloading & Installing Wireshark, launch it & double-click the name of a network interface under Capture do start capturing packets on that interface. Click the red "stop" button near the top left corner of window when you want to stop capturing traffic.

THE "PACKET LIST" PANE:

The packet list pane displays all the the packets in current capture file.

THE "PACKET DETAILS" PANE

The packet details pane shows the current packet in a more detailed form. The protocol & fields of the packet shown in a tree which can be expanded & collapsed

THE "PACKET BYTES" PANE

The packet bytes pane shows the data of the current packet in a hexadecimal style.

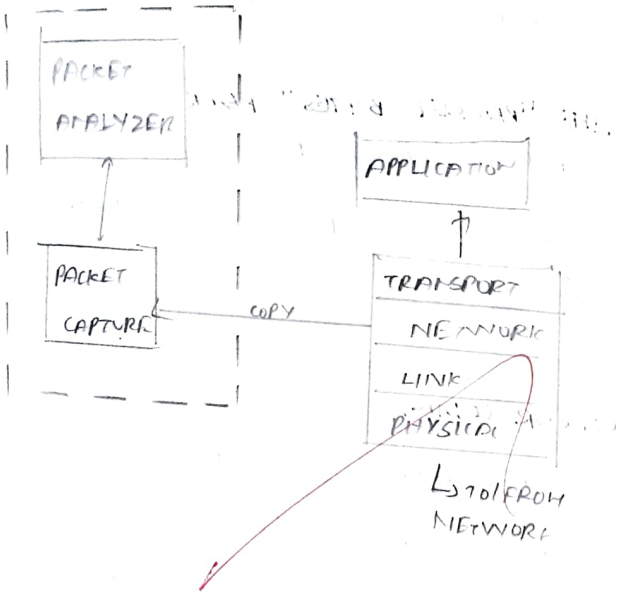
COLOUR CODING

You'll probably see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. To see exactly what the color codes mean, click View > Coloring Rules

SAMPLE:

Use sample files to practice in wireshark open via file yopen.

Save your captures with files saul for later review



FILTERING PACKETS:

Apply filters to focus on specific network traffic.

Close other apps to isolate traffic for analysis

Type a filter, press Enter eg 'dns' for DNS packets. Wireshark autocompletes

Use Analyzes display filters to pick or save filters. see the docs for more info. Right click a packet, choose follow TCP stream to see the full conversation use follow for other protocals too.

CAPTURING AND ANALYSIS PACKETS USING WIRESHARK TOOL:

To filters, view, capture, packets, capture 100 packets from the ethernet IEEE 802.3 can interface & save it.

PROCEDURE:

Select stop capture automatically after 100 packets

Save the packets

1) Create a filter to display only TCP/UDP packets, Inspect the packets and provide the flow graph.

PROCEDURE:

Select local area connection

Go to capture after 100 packets

Search TCP packets

To see flowgraph click Statistics

Save the packets

2) Create a filter to display any ARP packets & Inspect the packets

PROCEDURE:

Go to capture

Select stop capture after 100 packets

Then click start capture

Save the packets

3) Create filter to display only DNS packets and provide the flow graph.

PROCEDURE:

Go to capture

Select stop capture after 100 packets

click start capture

Save the packets

4) Create a filter to display only HTTP packets.

PROCEDURE: Go to capture after 100 packets

click start capture

3) display only IP/ICMP packets & inspect the packet

Select Local area connection
Go to capture → option
click start capture
Search ICMP/IP packets
Save the packets.

6) Create a filter to display only DHCP packets & inspect the packets.

Go to capture → option
Select stop after 100 packets
Search DHCP packets
Save the packets

STUDENT OBSERVATION

1) What is promiscuous mode?

This promiscuous mode is a configurati- for a network interface that allows it to capture all packets.

2) Does ARP packets have a transport layer header? Explain.

NO, ARP packets do not have a transport layer because it operates at the data link layer.

3) Which transport layer protocol is used by DNS?

DNS primarily uses UDP as its transport layer protocol.

4) What is the port no. used by HTTP protocol?

The default port number used by HTTP protocol is 80. For HTTPS, the secure version of HTTP, the default port is 443

5) What is broadcast IP address.

It is a special address used to send packets to all devices.

RESULT:

Thus experiment on packet capture tool is done successfully.

HAMMING CODE CONCEPT

EXPNO: 6

AIM:

Write a program to implement error detection & correcting using HAMMING code concept. Make a test run to input data stream & verify error correction featu.

SENDER PROGRAM

Convert text to Binary

Apply Hamming code & add redundant bits

Save output to "channel" file

RECEIVER PROGRAM:

Read input from channel file

Apply Hamming code to check for errors.

Display error positions if error exists

Else remove redundant bits & convert

```
import numpy as np

def text_to_binary(text):
    return ''.join(format(ord(char), '08b') for char in text)

def binary_to_text(binary):
    chars = [binary[i:i+8] for i in range(0, len(binary), 8)]
    return ''.join(chr(int(char, 2)) for char in chars)

def calc_redundant_bits(m):
    r = 0
    while (2**r < m + r + 1):
        r += 1
    print(f"No. of redundant bits: {r}")
    return r

def pos_redundant_bits(data, r):
    j = 0
    k = 0
    m = len(data)
    res = ''
    print("Placing redundant bits at positions: ", end="")
    for i in range(1, m + r + 1):
        if i == 2**j:
            res += '0'
            print(i, end=" ")
            j += 1
        else:
            res += data[k]
            k += 1
    print()
    return res

def calc_parity_bits(arr, r):
    n = len(arr)
    arr = list(arr)
    parity_output = "Parity Bits:\n"
    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)
        parity_output += f"P{position}: {parity}\n"
    return ''.join(arr)
```

```
def introduce_error(data, position):
    if position < 1 or position > len(data):
        print("Error position is
              out of range")
        return data
    data = list(data)
    return "".join(data)

def sender(text):
    binary_data = text_to_binary(text)
    m = len(binary_data)
    r = calc_redudant_bits(m)
    print(f"Binary: {arr}")
    return arr

def receiver(data):
    r = calc_redudant_bits(len(data))
    print(f"Binary with error: {
                data}")
    corrected_data = detect_and_
                correct(data, r)
    print(f"Decoded text: {ascii_output}")
```

```
if __name__ == "__main__":
    input_text = input("Enter text to be
                encoded: ")
    channel_data = sender(input_text)
    corrupted_data = introduce_error
                (channel_data, 2)
    receiver(corrupted_data)
```

8/11

RESULT:

Thus the above program have been executed successfully