INDEX

NAME: ASITHA-B STD: 9506701019 SEC: ROLL NO.:

S.No.	Date	Title	Page No.	Teacher's Sign/ Remarks
1.	16/07/24	Study of various network commands used in Linux & windows	9	
2.	30/07/24	Study of network cables	9	
3.	06/08/24	Experiments on cisco packet tracer (S/W simulation tool)	9	
4.	09/08/24	Setup and configure a LAN using ethernet	9	
5.	16/08/24	Experiments on product capture using wireshark.	9	
6.	20/9/24	Hamming code		
7.	24/9/24	Sliding window		
8.	4/10/24	Virtual LAN configuration		
9.	8/10/24	Subnetting in cisco using LAN		
10.	15/10/24	Internetworking with routers in cisco packet tracer simulation		
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 program		
14.	29/10/24	Write a code using RAW socket to implement packet sniffer		
15.	5/7/24	Analyse various type of server using cybaliez tool.		

Palaniappa

completed

13/09/24

Ex:no-1

Aim: Study of various network commands used in Linux and Windows.

Basic networking commands:

(1) arp -a:

Address resolution protocol will show IP address of computer.

Interface:- 172.16.75.84 --- 0x19

Internet address	PhysicalAdd	Type
172.16.72.1	7C-5a-1C-(f-be-41	Dynamic
172.16.72.133	4C-ae-a3-65-97-f3	Dynamic
172.16.79.255	ff-ff-ff-ff-ff-ff	static

(2) Hostname:

Displays the name of your computer

DESKTOP-C01BHTD

(3) IPconfig/all:

Information about TCP/IP connection

Windows IP configuration

Hostname . . . . . : DESKTOP-C01BHTD

Primary DNS suffix . . . . . :

Node type . . . . . : Mixed

IP Routing Enabled . . . . . : No

WINS Proxy Enabled . . . . . : No

(4) nbqstat-a:

Help solve problems with NetBIOS

Displays protocol statistics & current TCP/IP connects using NBT.

NBTSTAT [[-a RemoteName] [-A IP address]

[-n] [-r][-R] [-RR] [-s] [-S] [interval]]

-a (adapterstatus) : lists the remote machine's name table given its IP address.

(5) netstat -r :- monitoring network connections both incoming and outgoing as well as viewing routing table interfaces statistics.

Interface List.

24 ..... 20 80 10 86 C4 do ..... Intel(R) Ethernet connection I219-LM

15 ..... 40 82 99 T9 a3 ..... Microsoft Wi-fi Direct

19 ..... 40 82 a9 79 1f 94 ..... Bluetooth Device

(6) nslookup www.google.com

displays: IP address, Mx records or NS servers of a domain

Server: Unknown

Address: 172.16.72.1

Non-authoritative answer:

Name: www-google.com

Addresses: 2404:6800:4007:81e::2004

142.250.183.228

PathPing :- Combination of Ping and Tracert commands usage :-

pathping [-g host_list] [-h maximum_hops]

[-w timeout] [-4][-6] target_name.

options:-

-g host_list Loose source route along host-list

-h maximum_hops Maximum number of hops to search for target.

(8) Ping :- Test connectivity between two nodes

usage :- Ping [-t] [-a][-n count][-l size][-f]

[i TTL] [-v TOS] [-r count] [-s count]

[-j host_list] [-k host_list][-w timeout][-4]

[-S srcaddr] [-C compartment][-p] [-4][-6]

target-name.

Route :- The route command in windows is used to display & manipulate the IP routing table. It allows setting up static routes to specific hosts or network via a designated network interface.

output :-

manipulates network routing tables.

ROUTE [-f][-p][-4][-6] command [destination]

[mask netmask] [gateway] [METRIC metric]

[IF interface]

-f clears the routing tables of all gateway

If this is used in conjunction with one of t

the tables are cleared prior to running the com

-p When used with the ADD command, makes a route persistant across boots of the system.

-4 Force using IPV4

-6 Force using IPV6

Command one of these:

PRINT prints a route

ADD Adds a route

DELETE Deletes a route

CHANGE Modifies an existing route

Some important Linux commands:-

IP:- The IP command can show address information, manipulate routing, plus display network, various devices. Interfaces and tunnels.

ip <options> <object> <command>

(a) To show the IP addresses assigned to an Interface on your server.

ip address show:-

enp250: <Broadcast, multicast, UP lower up>

mtu: 1500 qdisc noqueue state

DOWN group default qlen 1000.

link/ether: 50:99:4C:35:11:44: ff:ff:ff

inet 172.16.8.107/22 brd 172.16.11.255

scope global enp250 valid lft.

(b) To assign an IP to an interface, for example

enp250 ip address add 192.168.1.254/24 dev epp250

(c) To delete an IP on Interface

ip address del 192.168.1.254/24 dev enp250

(d) Alter the states of the interface by bringing the interface online:-

ip link set enp250 up

(e) Alter the states of the interface by bringing the interface offline.

ip link set enp250 down

(f) After the states of the interface by enabling promiscous mode for the interface.

ip link set enp250 promise on

(g) Add a default route (for all addresses) via local gateway 192.168.1.254 that can be reached on device enp250:

ip route add default via (g) 168.1.254 de

(h) Add a route to 192.168.1.0.124 via the gateu at 192.168.1.254

ip route add 192.168.1.0/24 via 192.168.1.25

(i) Add a route to 192.168.1.0.124 that can be reached on device enp250:

ip route add 192.168.1.0/24 dev enp25

(j) Delete the route for 192.168.1.0/24 via the at 192.168.1.254

ip route delete 192.168.1.0/24 via 192.1

ip route get 10.10.1.4

o/p:- 10.10.1.4 via 192.168.1.254 dev ens160 src 192.168.1.1 uid 0 cache.

(2) ifconfig :- The ifconfig command a staple in many sysadmin's tool but for configuring and troubleshooting network has since been replaced by the ip command.

Output :-

ens160 : flags = 4163 <up, Broadcast, running, multicast> mtu 1500 inet 192.168.247.130 netmask 255.255.255.0 broadcast 192.168.247.255 inet6 fe80 ::661c:3ce:9550 prefixelen 64 scopeid 0x20 <link> ether 00:0c:29:06 txqueuelean 1000 (Ethernet)

RX packets 45 bytes 6072 (5.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 1123 (10.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0.

(3) mtr :- traceroute is a command line tool for network diagnostic, combining the functionality of ping and traceroute. It shows the route from a computer to a specified hosts and provides statistics like response time and packet loss at each hop. this helps identify the problematic

time/packet loss

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

mtr google.com

output :- my traceroute [v0.93]
fedora (192.168.247.130) → google.com (142.250.198.174)
keys: Help display mode restart statistics order of fields quit

Hostname :- Packet Pings
Loss% Snt Last Avg Best Wrst StDev
1. gateway 0.0% 128 1.4 0.2 6.2 1.0
2. (waiting for reply)
3. (waiting for reply)
4. (waiting for reply)
5. (waiting for reply)
6. (waiting for reply)
maa03541-in-f14.1e100.net 0.0% 1519.2 9.4 3.2

(b) Show numeric ip addresses (if you use -g 40
get ip addresses (numbers) instead of hostna

mtr -g google.com

mtr : invalid option -- 'g'

usage:
mtr [options] hostname.

-F Filename File read hostname(s) f
-4 use IPv4 only
-6 use IPv6 only
-u ... udp use UDP instead
-t ... tcp use TCP instead

2024-07-24123:23:05

Keys: Helps display mode restart statistics order of fields quit.

Host	Packets	Pings				
1. gateway (192.168.247.2)	105%.	snt	last	Avg	Best	cost - st dev.
	0.07.	11	0.3	1.0	0.2	2.2

(2) (waiting to reply)
(3) (waiting for reply)
(4) (waiting for reply)
(5) (waiting for reply)
(6) maaa3541 - in - f14 (100.net 0.0.0.10 4.4.9.4 14
12.0.22 (142.250.195.174)

(d) Set the no.of pings that you want to send:

nttr -c 10 google.com

o/p: my traceroute [v0.95]

fedora (192.168.247.130) → google.com (142.250.198.174)

2024.07.24123:23:25:20.05030

Keys: Help display mode restart statistics order of fields

quit pings.

Host	105%.	snt	Last	Avg	Best	cost	stdev
(1) gateway							
(2) waiting for reply	0.07	8	0.3	1.5	0.3	4.1	12
(3) waiting for reply							
(4) waiting for reply							
(5) maaa03541 - in - f14.100.net	0.07	9	8.5	14.9	4.6	38.3	10.8

29 Jul 2024 23:21:59:157

package tcpdump-14:4:99.4-66.el10.1.864 is already installed.

Dependencies resolved.

Nothing to do.

Complete!

Before starting capture, you need to know what interfaces tcpdump can use you will need sudo or have root access in this case.

output:

ens160 [up, running, connected]

any (pseudo device that captures on all interfaces) [up, running, loopback]

Bluetooth-monitor (Bluetooth Linux monitor)

usbmon0 (raw USB traffic, all USB buses)

If you want to capture traffic on ethO that with tcpdump -i ethO

tcpdump -i ethO

output:

dropped: privs to tcpdump

tcpdump: verbose output suppressed, use -v[v]... for full protocol decode listening on ethO, Ethernet, snapshot length 262144 by

tcpdump -i etho -c 10:

capture traffic to and from one host you can filter out traffic coming from a specific host. For ex to find traffic coming from and going to 8.8.8.8 we the command

tcp dump -i etho -c 10 host 8.8.8.8

dropped privs to tcpdump
tcpdump: verbose output suppressed use -v[v]... for full protocol decode listening on ens160 link type ENIOMB (Ethernet) snapshot length 262144 bytes

tcpdump -i etho src host 8.8.8.8

ed privs to tcpdump
mp: verbose output suppressed use -v[v] for full
ol decode listening on ens160 link-type
(Ethernet) snapshot length 262144 bytes.

tcpdump -i etho dst host 8.8.8.8

traffic to and from a network dropped privs to
tcpdump: verbose output suppressed use.
ll protocol, decode on ens160 link-type ENIOMB,

dump -i ethernet 10.1.0.0 mask 255.255.255.0

to tcpdump
bose output, suppressed, use -v[v]... for
decode listening on ens160 link-type
ernet) snapshot length 262144 bytes.
dump -i etho port not 53 and not 25.

dropped privs to tcpdump
tcpdump: verbose output suppressed use -v[v]
tcpdump full protocol decode listening on ens160,
link type ENIOMB (Ethernet) snapshot length 262144 bytes.

(5) Ping: Ping is a tool that verifies IP connectivity by sending ICMP echo request messages & displaying the receipt of echo reply messages with round-trip times. It is primarily used to troubleshoot connectivity reachability and name resolution.

Ping google.com:

PING google.com (142.250.195.174) 56(84) bytes of data
64 bytes from maa03041-in-f14.1e100.net (icmp_seq
ttl=128 time=4.53 ms.
64 bytes from maa3541-in-f14.1e100.net
icmp seq=2 ttl=128 time=9.67 ms
10 packets transmitted, 10 received, 0% packet loss,
9016.
alt min/avg/max/mdev = 4.087/6.280/11.96/2.45

Configuring an Ethernet connection by using nmc

If you connect a host to the network over ethernet, you can manage the connections s the command line by using the nmcli utility.

Procedure:

1) List the network manager connection profi

nmcli connection show

NAME UUID

wiredconnection1 5ed94722-ideb-35d1-5

TYPE DEVICE

ens160

(2) nmcli connection add con-name <connection-name
if name <device-name> type ethernet

(1) nmcli connection add con-name "My connection"
if name ens160 type ethernet

(3) connection 'My connection' (66199d1c-1c72-4dc1-bd0
7202172 b1501) successfully added.

Rename the connection profile (optional)

(iii) nmcli connection modify "wired connection":-

(iv) Display the current settings of the connection
profile nmcli connection show "wired connection"

connection.id: wired connection
connection.uuid: 5ed9474a2-1d8-35d1-5719-
6690c0bcacbb
connection.stable-id: --
connection.type: 802-3-ethernet
connection.interface-name: ens160

onfigure the IPV4 settings:-
se DHCP enter:
i connection modify "wired connection" IPV4
method auto
a static IPV4 address, network mask,
gateway, DNS servers and search domain enter.

onnection modify "wired connection," IPV4
anual ipv4 address 192.0.2.1/24
ay 192.0.2.254 ipv4 dns 192.0.2.200
earch example.com

Activate the profile
cli connection up Internal LAN
nection successfully activated.

Verification:-

(1) Display the IP settings of the VM:-

#ip address show ens160

2: ens160: <BROADCAST, MULTICAST, UP, LOWER_UP>
mtu 1500 qdisc fq_codel state UP group default
qlen 1000
link/ether 00:0c:29:05:84:ec brd ff:ff:ff:ff:ff:ff
altname enp3s0
inet: F12 0.21/24 brd 192.0.2.255 scope global non
refix route ens160.
valid_lft forever preferred_lft forever

(2) Display the IPV4 default gateway.

#ip route show default

default via 192.0.2.254 dev ens160 proto static
metric 20100

(3) Display the IPV6 default gateway:-

#ip-6 route show default

* Display the DNS settings:-

#cat/etc/resolv.conf

This is (run/systemd/resolve/stub-resolv
managed by man: systemd-resolved(5)

(5) use the ping utility to verify that th
send packets to other hosts: #ping <ho

ping 8.8.8.8

ping 8.8.8.8 (8.8.8.8) 56 (84

From 192.0.21 icmp.seq=1

Trouble shooting :

- Verify that the network able is plugged in to the host and a switch
- Check whether the link failure exists only on this host or also on other hosts connected to the same switch
- Verify that the network cable and the network interface are working as expected, perform hardware diagnosis steps and replace defect cables
- If the configuration on the disk does not match the configuration on the device starting or restarting network manager creates on in-memory section that reflects the configuration of the

Aim: Study of different types of network cables

(a) understand the different types of network cables

Different types of cables used in networking are:

(1) unshielded twisted pair (UTP) cable
(2) shielded twisted pair (STP) cable
(3) coaxial cable
(4) fibre optic cable

cable type	category	Maximum data transmission	Advantages/ Disadvantages	Applications/ uses	Images
UTP	category-3	10 bps	Advantages: • Cheap in cost • Easy to install as they have a smaller overall Dimensions	to connect Ethernet	
	category-5	upto 100 Mbps		Fast Ethernet Gigabit Ethernet	
	category-5e	1 Gbps	Disadvantage: more prone to EMI	• Fast Ethernet • Gigabit Ethernet	Twisted pair colour plast insu
STP	category 6, 6a	10 Gbps	Adv:- • shielded • Faster than UTP • less susceptible to noise & interferences Disadvantages • Expensive • Greater installation effort	Gigabit ethernet, LAN	ethernet 55 m) widely used data cent

Thus the study of various network

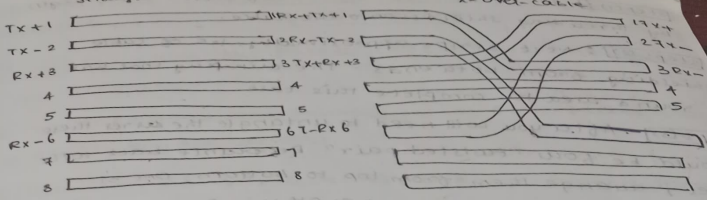
used in Linux & windowes is done and

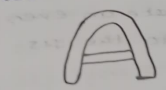
successfully

Coaxial cable	RG-6 RG-59 RG-11	10-100 Mbps	• High bandwidth • Immune to interference • Low loss Band width • Versatile Disadvantages: Limited distance cost	Speed of signal is 500m television network Highspeed internet connections	Braided shield, Protective, cover, conductor, outer jacket, Foil shield
Fibre optics cable	single mode multi mode	100Gbps	Advantages: High speed, High bandwidth, High security, Long distance. Disadvantages: Expensive	Maximum distance of fibreoptic cable is around 100 metres	

straight through network cable: both sides should be

A crossover cable: one side of one side B.





white/orange strip

orange solid

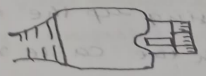
white/green stripe

Blue solid

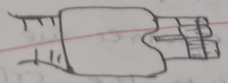
white/Blue strip

Green solid

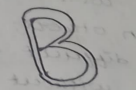
White/ brown strip



clip underneath pins facing you.



clip underneath pins facing you.



white/gree

green

white

white

b) Make your own Ethernet cross-over cable / straight cable:-

ls and parts needed:-

hernet cabling cable is certified for gigabet

ut but cat5 cabling works as well, just over

el distances.

mping tool. This is an all-in-one networking

ped to push down the pins in the plug and

d act the shielding off the cables.

plug.

o plug shields

by threading shields onto the cable.

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

Step:-(3) After you will need to untangle the wires these should be four "twisted pair" Reference back to the sheet, arrange them from top to bottom. One at a time should be in arrangement A as other in B.

Step:-(4) Once the order is correct bunch them together in a wire and if there are any that stick out further than others. Snip them back on to create an even level. The difficult aspect is placing these into the RJ45 plug without messing up the order.

Step:-(5) Next push the cable right in the notch at the end of plug needs to be just over the cable shielding if it isn't that means that you stripped off too much shielding simply snip the cables back a little more

(6) After the wires are securely sitting inside plug, insert it into the crimping tool & push down.

(7) Lastly repeat for the other end using B using diagram A. To test it plug it attempt to connect two devices directly.

Thus the study of different network are verified and executed successfully.

EXPERIMENT NO: 01 PACKET TRACER

Aim:- To study the packet tracer and use interface

(a) To understand and environment of cisco packet tracer to design simple network

Introduction As simulator as the name suggests simulates network devices and the environment. Packettracer is an existing network design, simulation and modelling

- It allows you to model complex systems without need of dedicated equipment.
- It helps you to practice your network configuration troubleshooting skills via computer or an android based mobile device.
- It is available for both the Linux & windo environment.
- Protocol in packet tracer are coded to work the same way as they would on real h

Installing Packet Tracer:-

To download packet tracer, go https://www.netacad.com & log in with networking academy credentials then packet tracer graphic and downl appropriate for your OS.

Installation

Pretty simple & straightforward. The setup comes in a single file named packet tracer - setup 6.0.1 Open this file to begin the setup wizard accept the agreement, choose a location & 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 to fedora. Grant executable permission to this file by using chmod and execute it to begin the installation.

ser- Interface overview: The layout of packet tracer divided into several components of the packet acer interface as follows.

o Menu Bar This is a common menu found in all ate application it is used to open, save, print ge preferences and soon

ain-toolbar This bar provides shortcut icons in options that are commonly accessed such save, zoom, undo on the right hand icon. sed for entering network information.

l/physical workspace tabs

These tabs allow you to toggle logical & physical work tabs.

created and simulations are performed

Network Component Box: This components contains all of the network and end devices available to the packet

User Created Packet Box: Users can create highly customized packets to test their topologies from this area and display as list.

(d) Analyse the behaviour of network devices using cisco packet tracer simulation:

(1) From the network component box, click and drag and drop the below components.

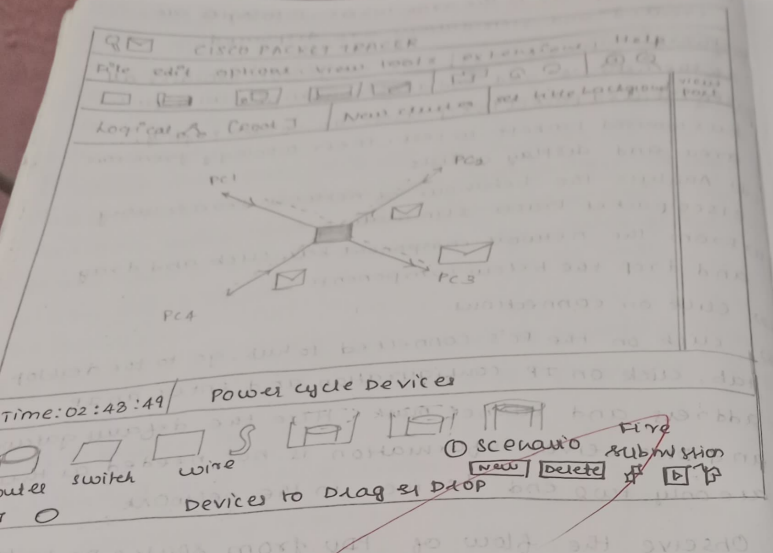
(2) Click on connections

(3) Click on the PC's connected to hub, go to the de tab, click on IP configuration and enter an IP address and subnet mask. Here the default and DNS server information is not needed are only two end devices in the network

(4) Observe the flow of PDU from source P destination PC by selecting the real time simulation.

(5) Repeat step 3 to 5 for the connected P

(6) Observe how HUB and switch are for PDU and write your observation and about the behaviours of switch and



Thus the experiments on cisco packet tracer is verified & executed successfully.

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

The ping command is a networking utility used to test the reachability of host on an IP network.

(2) Which command will be given the details of hops taken by a packet to reach its destination.

Traceroute shows the sequence of routers or nodes (hops) that data packets pass through to reach their destination.

(3) Which commands display the ip configuration of your machine on windows?

command prompt (cmd) : ipconfig

powershell : Get-NetIP address

(4) Which command displays the TCP port status in your machine on Window. MacOS and Linux.

netstat -an

(5) Write the command to modify the ip configu in a ~~Linux~~ machine. use the 'ipconfig' command by name of your network interface & the new to be changed on your computer. use ip-add command followed by the new ip address mask. Change the ip address in the file system.

Student observation - Expno: 4

1) What is the difference btw straight & cross cable

Straight cable: The wiring of both the ends of the cable is identical. used for connecting different types of devices.

Ex:- PC – switches/ Routers

Cross cable • The transmitter & reciver wires are crossed on one end of the wire

• used for connecting similar devices

Ex:- PC to PC

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

A:- Cross cable.

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

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

4) Find the category of twisted pair cable & your LAN to connect the PC to the network

We need to physically inspect the ethernet e connected to your PC. the cable typically its category printed along the length of

cable :- • **common category**

→ cat 5: support upto 100Mbps

→ cat 5e: support upto 1Gbps

→ cat 6: support upto 10Gbps for shorter distances

5) write down your understanding observation using and output received while making a twisted pair straight cable

Twisted pair cable involves arranging wires in a specific order & crimping connectors. the correct wiring sequence is essential for proper communication. output received: successfully made cables with allow proper network comm Indicated by functioning network connectio devices.

Student observations: Ex: 03

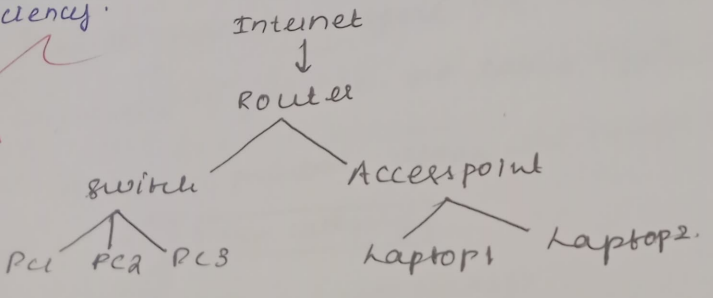
1) From your observation write down the behaviour of switch & hub in terms of forwarding the packet received by them:

HUB: Broadcasts: sends incoming packet to all connected devices, regardless of the destination.
Collision domain: All devices share the same collision domain, leading to potential data collision.

Switch: Unicasts: sends packets only to the intended destination by using MAC addresses.
Collision Domain: Each connected device has its own collision domain reducing collision & improving network efficiency.

2) Find out the network topology implemented in you college and draw label that:-

Star topology: All devices are connected to a central switch or hub. This is one of the most common & widely used topology in modern networks due to its simplicity & efficiency.



Aim: Setup and configure a LAN using a switch and ethernet cable in your lab.

What is LAN? A local area network connects devices within a limited area, like an office or school, allowing users to share resources such as data, printers, and internet access. A LAN switch acts as the central device managing and directing communication between connected devices for fast and secure data transfer.

- How to setup a LAN:

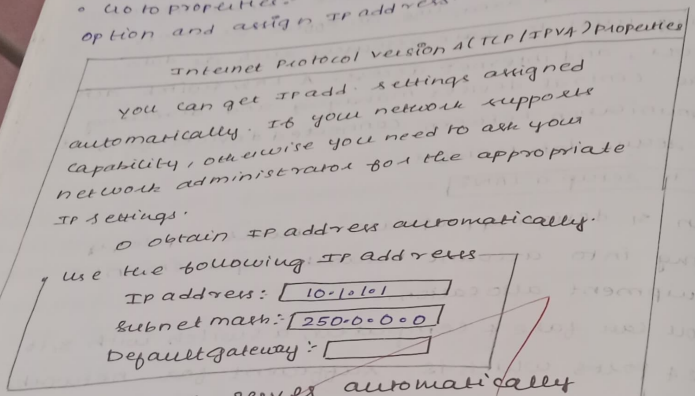
① Plan & design appropriate network topology taking into account network requirements & equipment allocation.

② You can take 4 computers, a switch with 8 or 24 ports which is sufficient for most of these sizes and 4 ethernet cables.

③ Connects your computers to network via an ethernet cable which is done by plugging one end of the ethernet to your computer and other end into switch.

Step:1- Assign IP address to your PC's:

- Log on the client computer as Administrator.
- Click network or internet connections
- Right click local area connection/ Ethernet
- Go to properties:- Select use the following address option and assign IP address.



Similarly assign IP address to all the PC's connected to switch.

- PC1 IP address : 10.1.1.1 Subnet mask 255.0.0.0
- PC2 IP address : 10.1.1.2 Subnet mask 255.0.0.0
- PC3 IP address 10.1.1.4 Subnet mask 255.0.0.0

Step:5- Configure a network switch:

(1) Connect your computer to the switch: To access the switch's web interface, web interface, you will need to connect your computer to the switch using an ethernet cable.

(2) Log in to the web interface: Open a web browser & enter the IP address of the switch in the address bar. This should be bring up the login page for the switch's web interface. Enter the username & password to login.

(3) Configure basic settings. Once you are logged in, you will be able to configure basic settings for the switch.

(4) Assign IP address as 101.1.5, subnet mask 255.0.0.0.

Step:-6- Check the connectivity between & other machine by using ping command in the command prompt of the device.

Step:-7- Select a Folder → goto Properties → sharing tab → share it with everyone in same LAN.

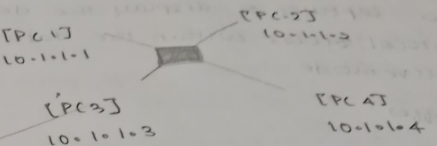
Step-8:- Try to access the shared folder from other computers of the network

Results

:- Thus the experiment of setup and gure LAN using ethernet TS executed verified successfully.

Ex:- 04 - Student Observation

Draw a neat diagram of the LAN in the configuration. Observation book that you have implemented in your lab. Write the IP configuration of each and every device. Write the outcome & challenges faced while configuring the LAN.



Outcome:- LAN was successfully setup and all devices could communicate with each other using their assigned IP addresses. Shared resources like folders were accessible from connected PCs.

Challenges faced:- • Ensuring each file has a IP address to avoid conflicts.

• Initial difficulty accessing the switch interface due to incorrect IP address

• Properly configuring folder sharing to ensure all devices could access resources.

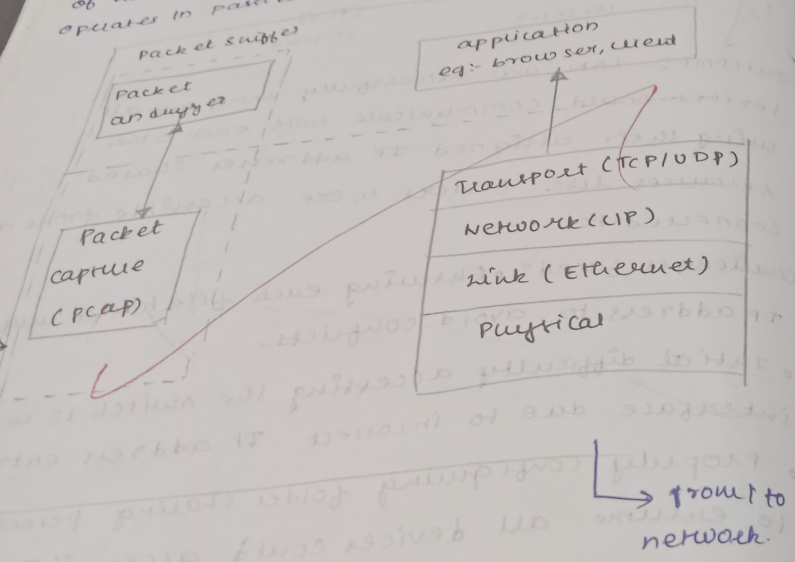
16/08/24 EXPERIMENTS ON PACKET CAPTURE TOOL WIRESHARK

EX:- NO-5

Aim:- Experiments on packet capture tool: wireshark

Packet Sniffer:-

Monitor network traffic sent to and from your computer. captures & display the details of various protocol fields within the data packets. operates in passive mode.



[diagnostic tool's]

tcpdump's: tcpdump -env host 10.0.2.15

execute

wireshark's: sudo wireshark -r exe -s out

[Descriptions]

(Wireshark) It is a nlw analysis tool that captures and displays network packets in real time. File provides features such as filters and color coding to help you analyse network traffic & troubleshoot issues effectively

[What can we do with wireshark:-]

- capture network traffic
- Decode various packet protocols
- Apply filters to capture & display specific data
- Monitor statistics & analyse problems.

Users:-

- Network administration
- Security Engineer
- Developers
- Learners

Getting wireshark:-

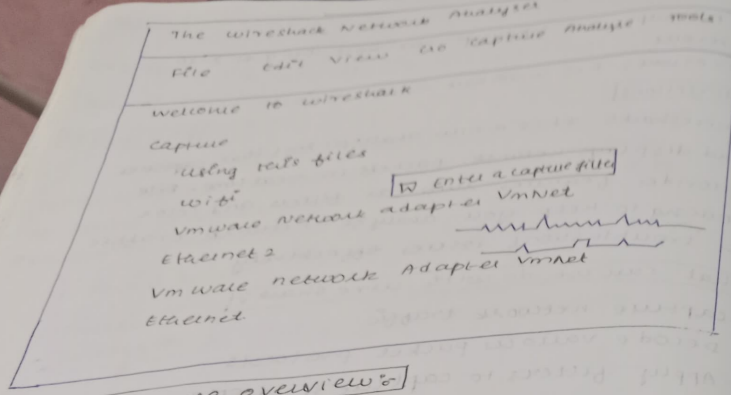
For windows :- Download from offical w

For Linux :- Available & package re

Capturing packets:-

- Launch wireshark
- Double click the network inte

capture to start capturing packets



Wireshark Interface overview:

- stop capturing traffic: click red 'stop' button
- ear left corner.
- acket list" pane:
- displays all packets in a current capture
- each title corresponds to one packet
- electing a line should show more details
- ket details' and 'packet bytes' panel.
- details" pane:
- detailed information of selected
- protocols & its field in a format

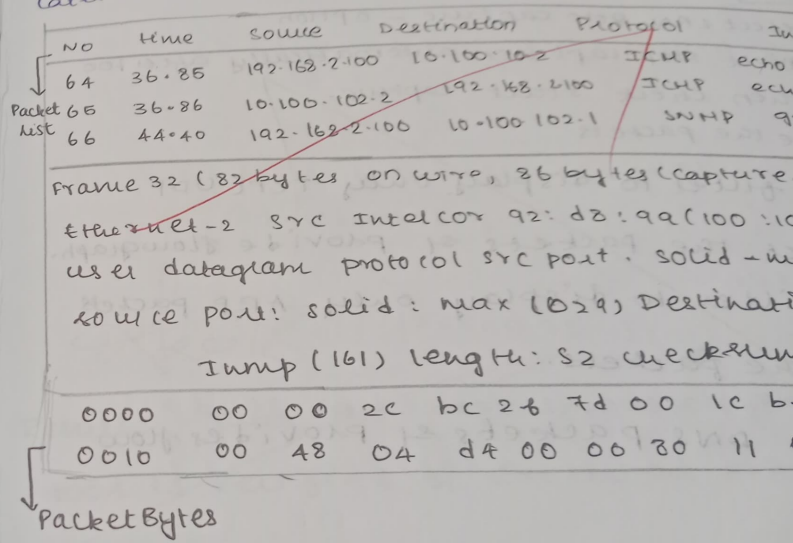
- packet bytes pane: shows the selected packet data in a hexdump style shows the data of the current packet

Color coding:

- Light purple - TCP traffic
- Light Blue - UDP traffic
- Black - packet with errors

Examples:

- use sample files to practice in wireshark
- open file via → open
- save your capture with file > save for later review.



Filtering Packets:

- Apply filters to focus on specific network traffic - use other apps to isolate traffic for analysis. Types a filter, press enter eg: dns
- > use analyse > display filter to pick or save filters, see the docs for more info.
- > choose packet, follow TCP stream to see the full conversation use follow for other protocol

Capturing and Analyzing Packets using Wireshark:

filter, view capture packets, capture 100 ckets from the ethernet.

edure:

1) select LAN, goto capture - option
2) select stop capture automatically after 100 ts then check start capture.
3) save the packets.
4) e a filter to display only TCP/UDP
5) inspect the packets & provide flowgraph.
6) a filter to display only ARP packets
7) pect the packets.
8) y only DNS packets & provide flow

9) filter to display only HTTP packets.
10) only IP/ICP packets & inspect
11) et.
12) ly DHCP packets & inspect packets.

Result: Thus the experimen
tool is verified & execut

Exp:- 5- Student observation

1) What is promiscuous mode?

A network interface is promiscuous mode captures all traffic on the nlw segment regardless of destination address, allowing for comprehensive monitoring.

2) Does ARP packets has transport layer headers? Explain?

- ARP packets doesn't have transport layer headers, they operate as datalink layer to map IP addresses to MAC addresses.

3) Which transport layer protocol is used by DNS?

DNS primarily uses UDP protocol for queries & responses, TCP for zone transfers & large responses.

4) What is port number used by HTTP protocol?

HTTP uses port 80 by default for communication.

5) What is Broadcast IP address?

Broadcast IP address is used to send data to all devices on a LAN segment for

Aim:- Write a code to implement error detection and correction using Hamming code concept. make a test run to input data stream & verify error correction feature.

Error correction at data link layer:- Hamming code is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is transmitted from the sender to the receiver. It is a technique de by R.W. Hamming for error correction.

Create sender program with below feature

1. Input to sender file should be a text of length. Program should convert the text

2. Apply Hamming code concept on the bi and add redundant bits to it.

3. Save the output in a file called c

Create Receiver program with belo

1. Receiver program should read t from channel file.

2. Apply Hamming code on the bina for errors.

3. If there is an error, display error.

4. Else remove the redundant binary data to Ascii and disp

Student Observation: [rate]

```
import numpy as np
def txt_to_bin(txt):
return ' '.join(format(ord(c), '08b') for c in txt)
def bin_to_txt(bin_str):
char = [bin_str[i:i+8] for i in range(0,
len(bin_str), 8)]
return ''.join([chr(int(c,2)) for c in chars])
def calc_r_bits(m):
r = 0
while (2**r < m+r+1):
r += 1
return r
def pos_r_bits(data, r):
k = 0,0
len(data)
= ''
s = []
i in range(1, m+r+1):
== 2**j:
+= '0'
append(i)
else:
res += data[k]
k += 1
print("Positions of redundant bits: ", r_pos)
return res, r_pos
def calc_p_bits(arr, r):
n = len(arr)
arr = list(arr)
for i in range(r):
p = 0
pos = 2**i
for j in range(1, n+1):
if j & pos:
p = int(arr[j-1])
arr[pos-1] = str(p)
print("parity bit in position {pos}: ", p
receiver code = list(hamming_code)
error_pos = int(input("Enter positions to
bit"))-1
receiver_code = toggleBit(receiver_c
print("The Recived code is after erro
receiver_code = parityBits(receiver_
error_index = ''
pos.reverse()
for i in pos_p:
error_index = error_i
```

```
error_index = int(serial_index, 2) - 1
receiver_code = toggle_bits (receiver_code,
                             error_index)

for i in pos_p:
    receiver_code = receiver_code.pop(i)
receiver_code = "".join(receiver_code)
decoded_list = []
for i in range(0, len(receiver_code), 8):
    decoded_list.append(receiver_code[i:i+8])
decoded_msg = ""
for i in decoded_list:
    decoded_msg = decoded_msg + chr(int(i,2))
print("Decoded message at receiver side:",
      decode_msg)
```

ut:-

the string: abc

y representation: 01100001 01100111
01101001 01101100 01100001

parity bits:-6

amming code: 010011000001101

arity): 000111011010010101010
11000110000101

position to change
the bit (1-based index)

Practical-7

Aim: Write a program to implement flow control at data link layer using SELECTIVE WINDOW PROTOCOL simulate the flow of frames from one node to another.

Program:

```
import time
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 ackn

def receive_frames(frames, win
    print("\n...Received Frames...

    for i in range(window_siz
        if (i < len(frames) an
            acknowledged:
```

```
if random.random() < 0.8:
    print(f"Received frame {frames[i]}")
    frames[i] = (frames[i][0], frames[i][1], True)
else:
    print(f"Frame {frames[i]} lost")
```

```
else
    print("Received frame", frames[i])
    frames[i] = (frames[i][0], frames[i][1], True)
```

```
def sliding_window_protocol():
    window_size = int(input("Enter window size: "))
    message = input("Enter the message to send: ")
    base = 0
    while base < len(frames):
        for frame in range(base, min(base + window_size, len(frames))):
            print("Sending frame", frames[frame])
        time.sleep(2)
        for frame in range(base, min(base + window_size, len(frames))):
            if frames[frame][2]:
                print("Frame", frames[frame], "acknowledged")
                base += 1
            else:
                print("Frame", frames[frame], "not acknowledged")
                frames[frame] = (frames[frame][0], frames[frame][1], False)
```

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

Output:

```
Enter window size: 3
Enter message to send: abcd
```

Sending Frame:

```
Sent Frame 0: a
Sent Frame 1: b
Sent frame 2: c
Frames sent, waiting for acknowledgement
```

Receiving Frame:

```
Received frame 0
Received frame
Received fram
Resending
```

Sending Frame:

```
Sent Frame 3: d
```

Receiving fra

```
Received f
```

All frames sent and

4/20/11

Result:

Thus the above sliding program is executed and ve

Ex:08 Practical:08

(b) Configuration of wireless LAN using cisco packet tracer.

Aim: To design a topology with three Pc's connected from linksys wireless routers

Procedure:

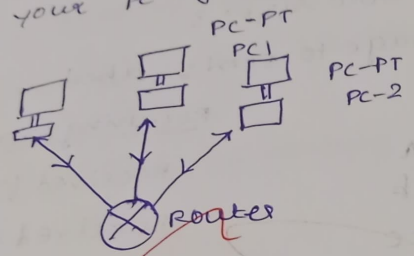
configure static IP on Pc and wireless router.

set SSID to mobilenetwork

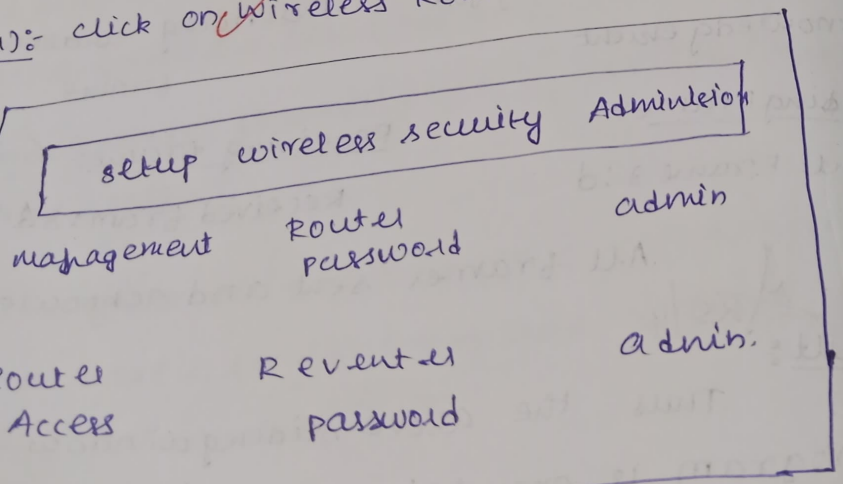
set IP address of router to all Pc's

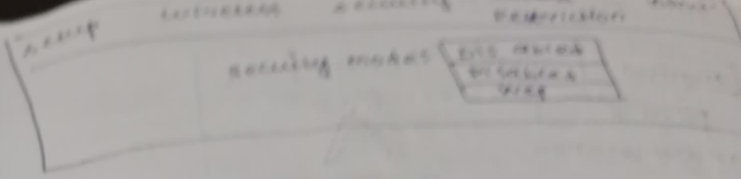
secure your network

connect your Pc by WAP key

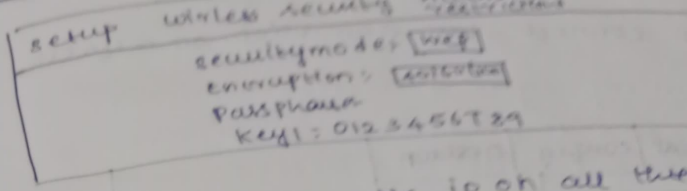


1):- click on wireless Router





Setup:



Now configue the static ip on all the and set the subnet mask.

	IP	subnet mask
PC	192.168.0.2	255.255.255.
PC0	192.168.0.3	255.255.25
PC1	192.168.0.4	255.255.
PC2		

Now its time to connect Pc's router. So click Pc select PC wireless.