

EXPERIMENTS ON CISCO

PACKET TRACER

EXP:03
09/08/2021

Aim: To study the packet tracer tool installation, and use interface.

(a) To understand and environment of CISCO packet tracer, to design simple network.

Introduction As Stimulator as the name suggests Stimulates network devices and its environment. Packettracer is an existing network design, simulation and modeling tool.

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

Installing Packet Tracer:

To download packet tracer, go to <https://www.netacad.com> & log in with your cisco networking academy credentials then click on the packet tracer graphic and download the package appropriate for your OS.

Windows:

Pretty simple & straightforward; the setup comes in a single file named packet tracer - setup 6.0.) 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 & to begin the installation.

User-Interface overview:

The layout of packet tracer is divided into several components of the packet tracer interface as follows.

• Menu Bar

This is a common menu found in all software application it is used to open, save, print, change preferences and soon.

• Main Toolbar

This bar provides shortcut icons in menu options that are commonly accessed such as open, save, zoom, undo on the right hand icon. That is used for entering network information.

• Logical/Physical workspace tabs

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

Workspace:

This is the area where topologies are created and simulations are displayed.

Network component box:

The network and end devices available with packet.

User-created packet box:

Users can create highly, customised packets to test their topology from this area and display as lists.

(d) Analyse the behaviour of network devices using Cisco packet tracer simulator:

- (i) From the network component bar, click and drag and drop the below component.
- (ii) Click on connections.

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

- 4) Observe the flow of PDU from source PC to the destination PC by selecting the real time mode of stimulation.

- (5) Repeat step 3 to 5 for the connected PC to switch.

- (6) Observe how Hub and switch are forwarding the PDU and write your observation and conclusion about the behaviours of switch and HUB.

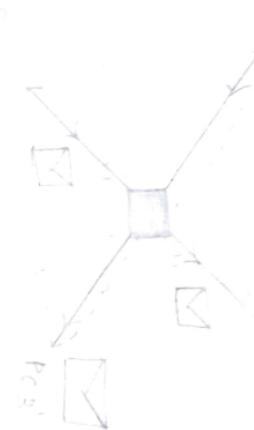
CISCO PACKET TRACER

File edit options view tools extensions help

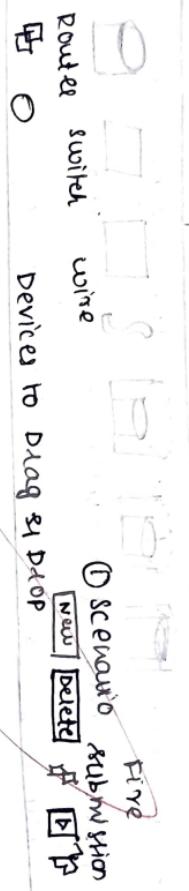


Logical & Physical New connection and heterogeneous link

PC1



Time: 02:48:49 Power cycle devices



Result:- Thus the experiments on CISCO packet
tracer is verified & executed successfully

Result:- Thus the experiments on CISCO packet
tracer is verified & executed successfully

Exp 1 - Student Observation

(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.

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

(3) Which command displays the IP configuration of your machine on windows?

Command prompt (cmd) : **ipconfig**

PowerShell : **Get-NetIPConfig**

(4) Which command displays the TCP port status in your machine on windows, Mac OS and Linux.

netstat -an

(5) Write the command to modify the IP configuration in a Linux machine. We use 'ipconfig' command follows by name of your network interface & the new IP address to be changed on your computer. We ip-address add command followed by the new IP address and subnet mask. Change the IP addresses in the file and restart the system.

System.

Student observation - exp no. 3

1) What is the difference b/w straight & cross cable.

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

e.g.: PC - switch/routers.

[Cross cable] • The transmitter & receiver wires are crossed on one end of the user.

• used for connecting similar devices.

e.g.: PC to DC

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.

) Find the category of twisted pair cables & in ~~your LAN~~ connect the PC to the network ~~socket~~.

We need to physically inspect the ethernet cable connected to your PC. The cable typically

as its category printed along the length of the cable :- **[common category]**

→ Cat 5: support upto 100Mbps

→ Cat 5e: support upto 1Gbps

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

Twisted pair cable involves arranging wires in a specific order of crimping connectors. The correct wiring sequence is essential for proper communication. Output received: successfully made cables will allow proper network communication indicated by functioning network connection blue devices.

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

HUB: Broadcasts: sends incoming packets to all connected devices, regardless of the destination.

Collision domain: All devices share the same collision domain, leading to potential data

collision.

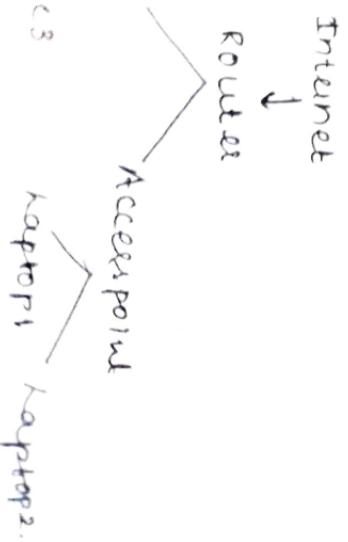
Switch: unicast: sends packets only to the intended destination by using MAC address.

Collision domain: Each connected device has its own collision domain reducing collision by improving network efficiency.

(3) Find out the network topology implemented in your college and draw labeled 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.



Setup and configure 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 devices 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 requirement & equipment allocation.
- ② You can take 4 computers, a switch with 8, 16 or 24 ports which is sufficient for networks of these sizes and 4 Ethernet cables.
- ③ Connect your computers to network switch via an Ethernet cable which is a simple as plugging one end of the Ethernet cable into your computer and other end into your network switch.

Step-1 Assign IP address to your PC :-

- 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.

Internet Protocol version 4(TCP/IPv4) properties

You can get IP address settings assigned automatically. If your network supports capability, otherwise you need to ask your network administrator for the appropriate IP settings.

- Obtain IP address automatically.
- * Use the following IP address

IP address:

Subnet mask:

Default gateway:

- obtain DNS server automatically
use the following DNS server address

Preferred DNS server:

Alternate DNS server:

- validate settings upon exit

similarly assign IP address to all the PCs 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 into the web interface: open a web browser & enter the IP address of the switch in the address bar. this should 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 10.1.1.5, subnet mask 255.0.0.0.

step:-6- check the connectivity between switch & other machine by using ping command in the command prompt of the device.

step:-7- select a folder → goto properties → click sharing tab → share it with everyone on the same LAN.

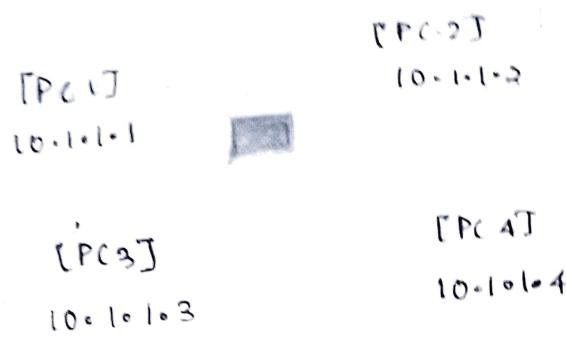
~~Step-8: Try to access the shared folder
from others computer of the network~~

~~Result~~

Result: Thus the experiment of setup and configure LAN using ethernet is executed and tested 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 of 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 all connected PCs.

Challenges faced: Ensuring each file has a unique

IP address to avoid conflicts.

- Initial difficulty accessing the switch via web interface due to incorrect IP address entry / log.
- Properly configuring folder sharing permissions to ensure all devices could access shared resources.

16/08/24

EXPERIMENTS ON PACKET

CAPTURE TOOL WIRESHARK

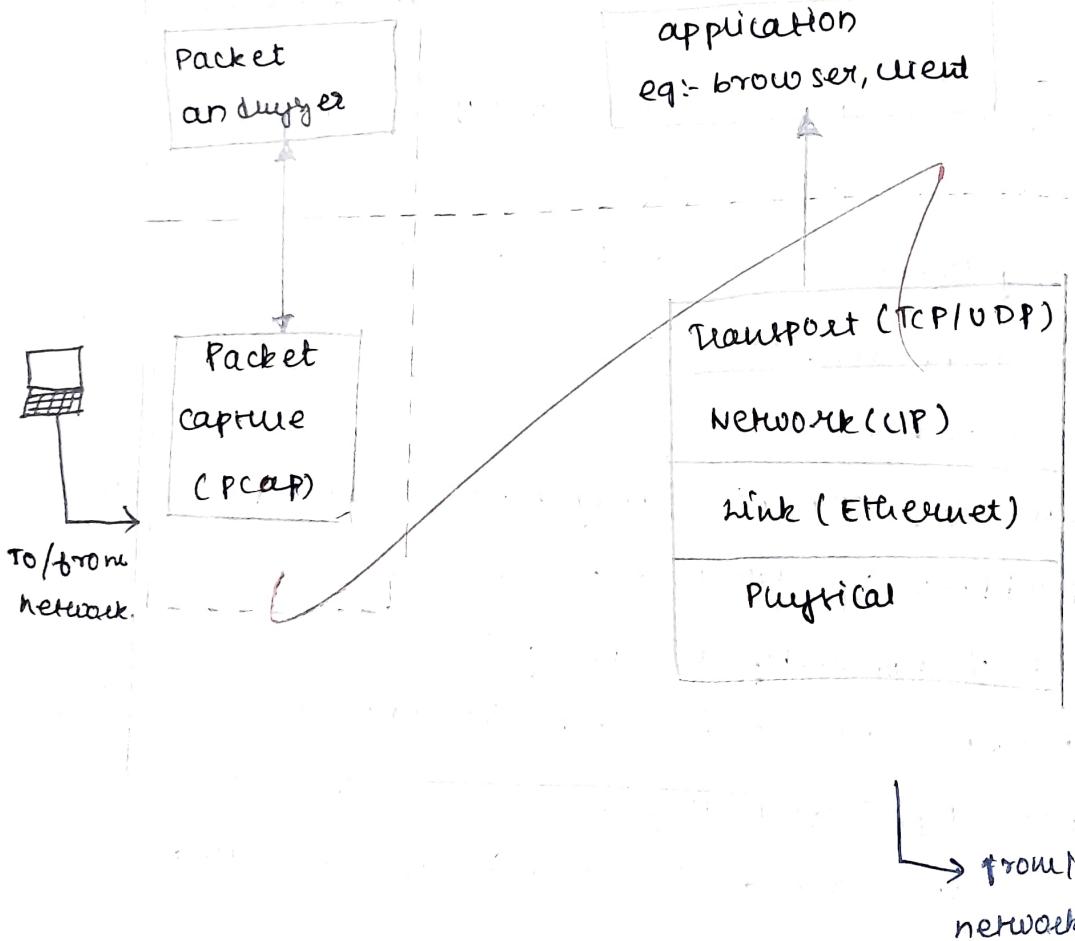
Ex: NO - 5

Aim: Experiments on packet capture tool: wireshark

Packet sniffer:

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

packet sniffer



Diagnostic tools:-

TCP dump :- ex:- `tcpdump -enx host 10.0.9.41:2:10`

exer out

wireshark :- ex:- `wireshark -z exp -3.out`

Description:-

(i) wireshark :- It is a new 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 wire shark:-

- capture network traffic
- decode various packet protocols
- apply filters to capture & display specific data.
- monitor statistics & analyse problems.

User:-

- Network administration
- Security Engineer
- Developers
- Researchers

Getting wire shark:-

For windows :- Download from official website.
For Linux :- Available in package repository.

Capturing packets:-

- Launch wireshark
- Double click the network interface under capture to start capturing packets.

The Wireshark Network Analyser

File Edit View Go Capture Analyse Tools

Welcome to Wireshark

Capture

Using Test files

wifi

Vmware Network Adapter VmNet

Ethernet 2

Enter a capture filter

Vmware Network Adapter VmNet

Ethernet

—+—+—+—+—

—+—+—+—+—

Wireshark Interface overview

- (1) Stop capturing traffic: click red 'stop' button
near left corner.
- (2) "Packet List" pane:
displays all packets in a current capture
each title corresponds to one packet
selecting a line should show more details
in 'packet details' and 'packet bytes' panel.
- (3) "Packet details" pane:
shows detailed information of selected
packet.
- display protocols & its field in a format
called tree.

[4] Packet Bytes pane

Shows the selected packet's data in hex dump style shows the bytes of the current packet.

[Color Coding]

Light purple - TCP traffic

Light blue - UDP traffic

Black - Packet continues

[Samples]

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

No	Time	Source	Destination	Protocol	Info
64	36.85	192.168.2.100	10.100.10.2	TCP	echo (ping)
65	36.86	10.100.10.2	192.168.2.100	TCP	echo (ping)
66	44.40	192.168.2.100	10.100.10.1	SNMP	get-request

Frame 32 (82 bytes on wire, 86 bytes captured)

Ethernet-2 Src IntelCor 92: d8: 99 (100: 10: b8: a2: d8: 09)

User datagram protocol Src port: solid-line (1024)

Source port: solid: max (1024) Destination port:

Jump (161) length: 82 checksum 0x0A1FB

0000	00	00	2C	BC	26	7D	00	1C	B8	A2	D8	AA	08..E
0010	00	48	04	D4	00	00	30	11	02	60	00	A8	02..d

Packet Bytes

Filtering Packets:-

- Apply filters to focus on specific network traffic. Use other apps to isolate traffic for analysis. Type a filter, press enter again.
- Use analysis > display filter to pick or save filters, see the doc for more info.
- Choose packet, follow TCP stream to see the full conversation use follow for other protocol.

Capturing and Analyzing Packets using Wireshark:

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

Procedure:-

(1) Select LAN, goto capture - OPTION

(2) Select stop capture automatically after 100 packets then check start capture.

(3) Save the packets.

- * Create a filter to display only TCP(UDP) packets inspect the packets to provide flowgraph.
- * Create a filter to display only ARP packets and inspect the packets.
- * Display only DNS packets to provide you graph.
- * Create a filter to display only HTTP packets.
- * Display only IP/ICMP packets to inspect the packet.
- * Display only DHCP packets to inspect packets.

~~Ques 18~~

~~Result: Thus the experiment on packet capture
tool is verified & executed successfully.~~

Exp: 5 - Student observation

1) What is promiscuous mode?

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

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

- ARP packets don't have transport layer headers, they operate at the data link layer to map IP addresses to MAC addresses.

3) Which transport layer protocol is used by DNS?

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

4) What is port number used by HTTP protocol?

A:- HTTP uses port 80 by default for communication.

5) What is Broadcast IP address?

Broadcast IP address is used to send data packets to all devices on a LAN segment for IPv4.

23/08/2024

Hamming code

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 developed by R.W. Hamming for error correction.

Create sender program with below features:-

1. Input to sender file should be a text of any length. Program should convert the text to binary.
2. Apply Hamming code concept on the binary data and add redundant bits to it.
3. Save the output in a file called channel.

Create Receiver program with below features:-

1. Receiver program should read the input from channel file.
2. Apply Hamming code on the binary data to check for errors.
3. If there is an error, display the position of the error.
4. Else remove the redundant bits and convert the binary data to Ascii and display the output.

Student Observation: [code]

```
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 char])

def calc_n_bits(m):
    n = 0
    while (2 ** n) < m + n + 1:
        n += 1
    return n

def pos_n_bits(data, n):
    j, k = 0, 0
    m = len(data)
    res = ''
    n_pos = []
    for i in range(1, m+n+1):
        if i == 2 ** j:
            res += '0'
            n_pos.append(i)
            j += 1
```

```
else:  
    res += data[K]  
    K += 1  
print("Positions of Redundant bits: ", pos)
```

```
return res, K-pos
```

```
def calc_P_bits(avr, x):
```

```
n = len(avr)
```

```
avr = list(avr)
```

```
for i in range(x):
```

```
P = 0
```

```
pos = 2 ** ;
```

```
for j in range(1, n+1):
```

```
if j > pos:
```

```
P = int(avr[j-i])
```

```
avr[pos-1] = str(P)
```

```
print("parity bit in position ", pos, " : ", P)
```

```
receiver_code = list(chamming_code)
```

```
error_pos = int(input("Enter positions to change the  
bit")) - 1
```

```
receiver_code = toggleBit(receiver_code, error_pos)
```

```
print("The Received code is after error: ", join(receiver  
code))
```

```
receiver_code = parityBits(receiver_code)
```

```
error_index = ""
```

```
pos_P = reverseP()
```

```
for i in pos_P:
```

```
error_index = error_index + receiver_code[i].J.
```

error_index = int(error_index, 2) - 1

receiver_code = toggleBits(receiver_code, error_index)

for i in pos_p:

 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)

Output:-

Enter the string: abc

Binary representation: 011000010110011

 01101001 01101100 01100001

No. of Parity bits:- 6

The Hamming code: 010011000001011

(even parity): 0001110101001010

 110001100001

Enter position to change

the bit (-base & index)

black birds a young bird or immature form
caught in date the tiger using different
methods probably because the prey are smaller
when one mode is adopted

caught like

leopard transient

class Transient

avg. weight (avg. ground, no. date)

avg. ground no. (ground, no.)

avg. date = 40.8

avg. abdominal weight = 10.8

adults ground (ground, no. date)

adults ground (ground, no. date)

adults ground (ground, no. date)

avg. for (ground) and no. of dates

avg. abdominal weight

adults ground (ground, no. date)

adults ground (ground, no. date)

avg. abdominal weight (ground, no. date)

adults ground (ground, no. date)

avg. abdominal weight (ground, no. date)

adults abdominal weight