# VISVESVARAYA TECHNOLOGICAL UNIVERSITY

**"JnanaSangama", Belgaum -590014, Karnataka.**

**LAB REPORT**
**on**

# COMPUTER NETWORKS

***Submitted by***

**GAMANA YELURI R (1BM21CS065)**

***in partial fulfillment for the award of the degree of***
**BACHELOR OF ENGINEERING**
***in***
**COMPUTER SCIENCE AND ENGINEERING**

**B.M.S. COLLEGE OF ENGINEERING**
**(Autonomous Institution under VTU)**
**BENGALURU-560019**
**JUN-2023 to SEP-2023**

**B. M. S. College of Engineering,**
**Bull Temple Road, Bangalore 560019**
(Affiliated To Visvesvaraya Technological University, Belgaum)
**Department of Computer Science and Engineering**

## CERTIFICATE

This is to certify that the Lab work entitled "COMPUTER NETWORKS" carried out by **GAMANA YELURI R (1BM21CS065),** who is a bonafide student of **B. M. S. College of Engineering.** It is in partial fulfillment for the award of **Bachelor of Engineering in Computer Science and Engineering** of the Visvesvaraya Technological University, Belgaum during the year 2023. The Lab report has been approved as it satisfies the academic requirements in respect of a **Computer Networks - (22CS4PCCON)** work prescribed for the said degree.

**Dr. Latha N.R.**
Assistant Professor
Department of CSE
BMSCE, Bengaluru

**Dr. Jyothi S Nayak**
Professor and Head
Department of CSE
BMSCE, Bengaluru

`

# Index


| Sl. No. | Date | Experiment Title | Page No. |
|---|---|---|---|
| | | **CYCLE 1** | |
| 1 | 15/6/23 | Create a topology and simulate sending a simple PDU from source to destination using hub and switch as connecting devices and demonstrating ping messages. | 4 |
| 2 | 22/6/23 | Configure IP address to routers in packet tracer. Explore the following messages: ping responses, destination unreachable, request timed out, reply. | 9 |
| 3 | 13/7/23 | Configure default route, static route to the Router. | 18 |
| 4 | 13/7/23 | Configure DHCP within a LAN and outside LAN. | 23 |
| 5 | 20/7/23 | Configure Web Server, DNS within a LAN. | 32 |
| 6 | 20/7/23 | Configure RIP routing Protocol in Routers. | 35 |
| 7 | 27/7/23 | Configure OSPF routing protocol. | 40 |
| 8 | 3/8/23 | To construct simple LAN and understand the concept and operation of Address Resolution Protocol (ARP). | 45 |
| 9 | 10/8/23 | To construct a VLAN and make a pc communicate among VLAN. | 49 |
| 10 | 10/8/23 | Demonstrate the TTL/ Life of a Packet. | 53 |
| 11 | 10/8/23 | To construct a WLAN and make the nodes communicate wirelessly. | 58 |
| 12 | 10/8/23 | To understand the operation of TELNET by accessing the router in server room from a PC in IT office. | 62 |
| | | **CYCLE 2** | |
| 13 | 17/8/23 | Write a program for error detecting code using CRC CCITT (16-bits). | 66 |
| 14 | 17/8/23 | Write a program for congestion control using Leaky bucket algorithm. | 72 |
| 15 | 24/8/23 | Using TCP/IP sockets, write a client-server program to make client sending the file name and the server to send back the contents of the requested file if present. | 76 |
| 16 | 24/8/23 | Using UDP sockets, write a client-server program to make client sending the file name and the server to send back the contents of the requested file if present. | 80 |
| 17 | 24/8/23 | Tool Exploration -Wireshark | 84 |

# WEEK 1

Create a topology and simulate sending a simple PDU from source to destination using hub and switch as connecting devices and demonstrate ping messages.

OBSERVATION:

15/6/23

LAB-1

Aim -
Create a topology and stimulate sending a simple PDU from source to destination using a simple hub & switch as connecting domains

Diagram / Topology -

Procedure -

- Select a Generic hub from Hubs and place it.
- Select 3 PC's from End-devices.
- Connect hub and 3 PC's using copper straight through
- Select a switch and place it next to hub.
- Select 3 PCs from End-devices & place it.
- Connect switches & PC's using copper straight through.
- Connect switch & hub using copper crossover.

Ping-output -

PC > Ping 192.160.1.5

Pinging 192.160.1.5 with 32 bytes of data :

Reply from 192.160.1.5 : Bytes = 32 time = 0ms TTL = 128

Reply from 192.160.1.5 : Bytes = 32 time = 0ms TTL = 128

Reply from 192.160.1.5 : Bytes = 32 time = 0ms TTL = 128

Reply from 192.160.1.5 : Bytes = 32 time = 0ms TTL = 128

Ping Statistics for 192.160.1.5 :

Packets sent : 4, received = 4, lost = 0,

Approximate round trips in ms :

minimum = 0ms, Maximum = 0ms, Average = 0ms.

PC> Ping 192.160.1.2
Pinging 192.160.1.2 with 32 bytes of data:
Reply from 192.160.1.2 : bytes = 32 time = 0ms TTL = 128
Reply from 192.160.1.2 : bytes = 32 time = 0ms TTL = 128
Reply from 192.160.1.2 : bytes = 32 time = 0ms TTL = 128
Reply from 192.160.1.2 : bytes = 32 time = 0ms TTL = 128
Ping statistics for 192.160.1.2:
Packets: sent = 4, received = 4, Lost = 0
Approximate round trip in ms:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC > Ping 192.160.1.5
Pinging 192.160.1.5 with 32 bytes of data:
Reply from 192.160.1.5 : bytes = 32 time = 0ms TTL = 128
Reply from 192.160.1.5 : bytes = 32 time = 0ms TTL = 128
Reply from 192.160.1.5 : bytes = 32 time = 0ms TTL = 128
Reply from 192.160.1.5 : bytes = 32 time = 0ms TTL = 128
Ping statistic for 192.160.1.2:
Packets: sent = 4, received = 4, Lost = 0
Approx roundtrip in ms:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Observation:
→ Switch broadcasts the packets to all the devices during first itatation & records the IP addresses of the intended destination device & send the packet to that specified destination next time.
→ Hub broadcasts the packets to all the end devices & the device which are not intended to receive the packet discards the packet & the intended devices receives the packet & sends packets acknowledgment.

TOPOLOGY:

OUTPUT:

PC3
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ping 192.160.1.5
Pinging 192.160.1.5 with 32 bytes of data:
Reply from 192.160.1.5: bytes=32 time=1ms TTL=128
Reply from 192.160.1.5: bytes=32 time=0ms TTL=128
Reply from 192.160.1.5: bytes=32 time=0ms TTL=128
Reply from 192.160.1.5: bytes=32 time=0ms TTL=128
Ping statistics for 192.160.1.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>

# WEEK 2

Configure IP address to routers (one and three) in packet tracer. Explore the following messages: ping responses, destination unreachable, request timed out, reply.

OBSERVATION:

22/6/23

## LAB - 2

### PROGRAM 2.1

AIM -

Configure IP address to a single router. Explore the following messages : ping message, destination unreachable, request timed out, reply.

TOPOLOGY -

PROCEDURE -

- Select one Generic router & 2 generic PC's. connect the PC's to router using copper cross-over cable.
- Set the IP address of both PC's by clicking on PC & config tab. Along with IP address set gateway in the settings option on config tab.
- To set the IP addresses of a router, click on it & go to CLI tab and type the following commands

step 1 : type No & press enter.
step 2 : type enable & press enter
step 3 : type config T & press enter
step 4 : type interface fastEthernet 0/0 & press enter
step 5 : type IP address 10.0.0.10 255.0.0.0 & press enter
step 6 : type No shut & press enter
step 7 : type Exit
step 8 : type interface fast Ethernet 1/0 & press enter
step 9 : type IP address 20.0.0.10 25.0.0.0 & press enter
step 10 : type No shut & press enter
step 11 : type Exit
step 12 : type Exit
step 13 : type show IP route [for seeing the connection status]

- Close the tab & click on PC to go to command prompt. Type ping 20.0.0.1 to send packets across.
- At last send packets in simulation mode to get a sucessful transmission

PING OUTPUT :

Packet tracer PC command line 1.0
PC > Ping 20.0.0.1
Pinging 20.0.0.1 with 32 bytes of data :

Request timed out.
Reply from 20.0.0.1 : bytes = 32 time = 0ms TTL = 127
Reply from 20.0.0.1 : bytes = 32 time = 0ms TTL = 127
Reply from 20.0.0.1 : bytes = 32 time = 10ms TTL = 127

Ping statistics for 20.0.0.1 :
Packets : Sent = 4, Recived = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds :
Minimum = 0ms, Maximum = 10ms, Average = 3ms

# PROGRAM 2.2

**AIM -**

Configure IP address to three routers in packet tracer. Explore the following messages: ping response, destination unreachable, request timed out, reply.

**TOPOLOGY -**

**PROCEDURE -**

- Connect 2 PC's & 3 routers using copper cross over cable for PC to router and serial DCE cable to connect the routers to routers.
- Set the IP address of both PC's and gateway numbers.
- Now for setting IP address & gateway number to routers select one router and perform the following commands
  - Step 1: type No & press enter
  - Step 2: type Enable & press enter
  - Step 3: type configT & press enter

step4: type Interface fastEthernet 0/0 & press Enter
step5: type IP address 10.0.0.10 255.0.0.0 & press enter
step6: type No shut & press enter
step7: type Exit
step8: type interface se 2/0 & press enter
step9: type IP address 20.0.0.10 255.0.0.0 & press enter
step 10: type No shut & press enter
step 11: type Exit
step 12: type Exit

- Repeat these commands for the other two routers with respective IP/gateway addresses.
- Now to introduce the other two IP address to the first router we type the following commands
  step 1: type config T & press enter
  step 2: type IP route 30.0.0.0 255.0.0.0 20.0.0.20
  step 3: type IP route 40.0.0.0 255.0.0.0 20.0.0.20
  step 4: Exit
  step 5: Exit
  step 6: type show IP route
- Repeat these steps for the other two routers with appropriate addresses.
- Go to command prompt by clicking on PC & config tab. Type Ping message to send packets to the destination address.

PING OUTPUT:

output - 1:

Packet tracer PC command line 1.0
PC > Ping 40.0.0.1
pinging 40.0.0.1 with 32 bytes of data

Reply from 10.0.0.10 : Destination host unreachable
Reply from 10.0.0.10 : Destination host unreachable
Reply from 10.0.0.10 : Destination host unreachable
Request timed out.
Ping statistics for 40.0.0.1 :
Packets : sent = 4, Recived = 0, lost = 4 (100% loss).

Output 2 -
Packet Tracer PC command line 1.0
PC > ping 10.0.0.1
Pinging 10.0.0.1 with 32 bytes of data :
Reply from 10.0.0.1 : bytes = 32 time = 2ms TTL = 125
Reply from 10.0.0.1 : bytes = 32 time = 8ms TTL = 125
Reply from 10.0.0.1 : bytes = 32 time = 8ms TTL = 125
Reply from 10.0.0.1 : bytes = 32 time = 8ms TTL = 125
Ping statistics for 10.0.0.1 :
Packets : Sent = 4, Recived = 4, lost = 0 (0% loss),
Approximate round trip times in milli-seconds :
Minimum = 2ms, Maximum = 8ms, Average = 3ms

26/6/23

OBSERVATION -

- In program 2.1 when we ping the destination address we get allocated with 32 bytes. In this first 8 bytes are used to learn about the router and their addresses. Rest bytes are used for sending packets to destination address. Then, again if we ping all bytes are used for message sending and there will be no timed-out message.
- In program 2.2 when the routers doesn't know about the remaining addresses, and we ping a message we get host unreachable message. Once the routers have access / knowledge about other addresses, messages will be sent successfully.

# TOPOLOGY:

## PROGRAM 2.1

## PROGRAM 2.2

OUTPUT:

PROGRAM 2.1

PROGRAM 2.2

PC0
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 40.0.0.1
Pinging 40.0.0.1 with 32 bytes of data:
Reply from 10.0.0.10: Destination host unreachable.
Reply from 10.0.0.10: Destination host unreachable.
Reply from 10.0.0.10: Destination host unreachable.
Request timed out.
Ping statistics for 40.0.0.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100%
loss),
PC>

PC1
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 10.0.0.1
Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time=2ms TTL=125
Reply from 10.0.0.1: bytes=32 time=8ms TTL=125
Reply from 10.0.0.1: bytes=32 time=2ms TTL=125
Reply from 10.0.0.1: bytes=32 time=2ms TTL=125
Ping statistics for 10.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 8ms, Average = 3ms
PC>

Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Simulation Panel
Event List
Vis. Time(sec) Last De At Dev Type Info
28.315 -- Rout... CDP
28.316 Router5 PC0 CDP
28.316 Router5 Rout... CDP
45.862 -- Rout... CDP
45.862 -- Rout... CDP
Reset Simulation
Constant Delay
Captured to: 45.862 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters
Show All/None
Router1
Router5
Router2
PC-PC
20.0.0.20
30.0.0.10
30.0.0.20
40.0.0.10
20.0.0.10
Time: 01:54:00.015
Power Cycle Devices PLAY CONTROLS: Back
Auto Capture / Play
Capture / Forward
Event List
Simulation
Connections
Serial DCE
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Statu Sourc Destinatic Type Colo Time(s Period Num Edit Delete
Successful PC0 PC1 IC... 0.000 N 0 (ed... (delete)

# WEEK 3

Configure default route, static route to the Router.

OBSERVATION:

13/7/23

## LAB-3

AIM-

Configure default route, static route to the Router.

TOPOLOGY-

PROCEDURE:

- Connect 3 Routers and 2 PC's using copper cross-over cable for PC to router and a Serial DCE cable to connect router to router.
- Set the IP address of both PC's and respective gateway number.
- For All 3 Routers set the respective 2 IP address in CLI mode by using these commands
  Step 1: Enable

Step2: Config T
Step 3: Interface fastEthernet 0/0
Step 4: IP address 10.0.0.10 255.0.0.0
Step 5: No shut
Step6: Exit
Step7: Interface Se 2/0
Step 8: IP address 20.0.0.10 255.0.0.0
Step 9: No shut
Step 10: Exit
Step 11: Exit

- Repeat these commands for other two routers with their respective IP addresses.
- For Router 1, set the IP route of other IP addresses statically by using following steps
  Step 1: Config T
  Step 2: IP route 10.0.0.0 255.0.0.0 20.0.0.10
  Step 3: IP route 40.0.0.0 255.0.0.0 30.0.0.20
  Step 4: Exit
  Step 5: Exit
  Step 6: Show IP route.
- For Router 0 & Router 2 we set defaults IP routes which means it can access any IP address with any subnet mask.
- Set the default IP route by following these commands
  Step1: Config T
  Step2: IP route 0.0.0.0 0.0.0.0 20.0.0.20
  Step3: IP route 0.0.0.0 0.0.0.0 30.0.0.10
- Step 2 is given for Router 0 & Step 3 command for Router 1.
- Go to PC's command Prompt and type ping message to send packets across.

PING OUTPUT:

Packet Tracer PC command line 1.0
PC> Ping 40.0.0.1
Pinging 40.0.0.1 with 32 bytes of data:

Request timed out.
Reply from 40.0.0.1 : bytes = 32 time = 2ms TTL = 125
Reply from 40.0.0.1 : bytes = 32 time = 16ms TTL = 125
Reply from 40.0.0.1 : bytes = 32 time = 2 ms TTL = 125

Ping statistics for 40.0.0.1 :
Packets : Sent = 4, Recived = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 16ms, Average = 6ms

OBSERVATION:

- A default route is the route which takes effect when no other route is available for an IP address destination.
- If a packet is recived, the device first checks the IP destination address, if the IP destination address is not local the device checks its routing table.
- If the remote destination subnet is not listed then the packet is forwarded to the next hop toward the destination using the default route.
- The process repeats until the packet is delivered.

TOPOLOGY:

OUTPUT:

PC0

Physical | Config | Desktop | Custom Interface

## Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 40.0.0.1

Pinging 40.0.0.1 with 32 bytes of data:

Request timed out.
Reply from 40.0.0.1: bytes=32 time=2ms TTL=125
Reply from 40.0.0.1: bytes=32 time=16ms TTL=125
Reply from 40.0.0.1: bytes=32 time=2ms TTL=125

Ping statistics for 40.0.0.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 16ms, Average = 6ms

PC>ping 40.0.0.1

Pinging 40.0.0.1 with 32 bytes of data:

Reply from 40.0.0.1: bytes=32 time=21ms TTL=125
Reply from 40.0.0.1: bytes=32 time=9ms TTL=125
Reply from 40.0.0.1: bytes=32 time=2ms TTL=125
Reply from 40.0.0.1: bytes=32 time=4ms TTL=125

Ping statistics for 40.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 21ms, Average = 9ms

PC>
```

# WEEK 4

Configure DHCP within a LAN and outside LAN.

OBSERVATION:

13/7/23

## LAB-4

## PROGRAM 4.1

AIM -

Configure DHCP within a LAN and outside LAN

TOPOLOGY -

PROCEDURE -

- Connect 3 PC's and 1 Server to a switch using copper straight through cable.
- Click on server and go to services tab. Select DHCP and turn on the DHCP service.
- Set the IP address of the start IP address as 10.0.0.2 and click on Save button.
- Before this, set the IP address of server in Config Tab under fastethernet as 10.0.0.1
- Next click on PC0 and go to desktop tab, here click on IP configuration. Select DHCP here. It will request for an IP address and successfully get the DHCP request also sets the IP address.

- Repeat this steps for other 2 PC's.
- To send a packet across PC's, go to PC's command prompt and type ping destination IP address.

PING OUTPUT:

Packet tracer PC command line 1.0:

PC>Ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: bytes=32 time=0ms TTL=128
Reply from 10.0.0.3: bytes=32 time=0ms TTL=128
Reply from 10.0.0.3: bytes=32 time=1ms TTL=128
Reply from 10.0.0.3: bytes=32 time=0ms TTL=128

Ping statistics from 10.0.0.3:
Packets: Sent=4, Recived=4, Lost=0, (0% loss)
Approximate round trip times in milli-seconds:
Minimum=0ms, Maximum=1ms, Average=0ms.

OBSERVATION.

- DHCP is used to dynamically assign an IP address to any device or node.
- It is a client-server protocol in which servers manage a pool of unique IP addresses & also about client configuration parameters.
- DHCP-enabled clients sends a request to DHCP server when they want to connect to a network.
- The DHCP server responds to the client request by providing IP configuration information from address pools, previously specified by a network administrator.

13/7/23

# PROGRAM 4.2

AIM -

Configure DHCP within a LAN and outside lan:

TOPOLOGY -

PROCEDURE -

- Add a Router, a switch and 2 PC's to 4.1 program Network & connect the router to both switches.
- Set the server IP address of server and with the help of server set the first 3 PC's IP address through DHCP.
- Now set the Router IP address with the following commands statically.

Step 1 : No

Step 2 : Enable

Step 3 : Config T

Step 4 : Interface fastEthernet 4/0

Step 5 : ip address 10.0.0.20 255.0.0.0

Step 6 : No shut
Step 7 : Exit
Step 8 : interface fastEthernet 0/0
Step 9 : ip address 20.0.0.20 255.0.0.0
Step 10 : No shut
Step 11 : Exit
Step 12 : Exit
Step 13 : Show IP route

- Go to server and set the gateway as 10.0.0.20
- Again go to router CLI and follow these commands

Step 14 : Config T
Step 15 : interface fastEthernet 0/0
Step 16 : ip helper-address 10.0.0.1
Step 17 : No shut
Step 18 : Exit

- Now, go to server services and add one more Poolname as Server Pool 1, Start IP address as 20.0.0.2 and default gateway as 20.0.0.20. Then click add & save.
- Now set the other two PC's IP address by going to their Desktop → IP configuration and selecting DHCP which will automatically generate its IP address.
- Now the network is complete and can send packets from any PC to other by typing Ping destination IP address in their respective command prompts.

PING OUTPUT:

Packet tracer PC command line 1.0
PC > Ping 20.0.0.2
Pinging 20.0.0.2 with 32 bytes of data :

Request timed out.

Reply from 20.0.0.2 : bytes = 32 time = 0ms TTL = 127
Reply from 20.0.0.2 : bytes = 32 time = 0ms TTL = 127
Reply from 20.0.0.2 : bytes = 32 time = 0ms TTL = 127

Ping statistics for 20.0.0.2:
Packets sent = 4, Recived = 3, lost = 1 (25% loss).
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms.

OBSERVATION:
DHCP is used to assign IP addresses dynamically to different devices.
To assign continous IP address we create a server pool where we assign the starting IP address and a default gateway number. For PC's under different switches we create a different server pool again and start.
This takes care of delivering the packets to correct destination IP address and also sends back the ACK to the initial device.

Lee
18/7/23

TOPOLOGY:

PROGRAM 4.1:

PROGRAM 4.2:

OUTPUT:

PROGRAM 4.1:

PROGRAM 4.2:

PC0
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 20.0.0.2
Pinging 20.0.0.2 with 32 bytes of data:
Request timed out.
Reply from 20.0.0.2: bytes=32 time=0ms TTL=127
Reply from 20.0.0.2: bytes=32 time=0ms TTL=127
Reply from 20.0.0.2: bytes=32 time=0ms TTL=127
Ping statistics for 20.0.0.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>ping 20.0.0.3
Pinging 20.0.0.3 with 32 bytes of data:
Request timed out.
Reply from 20.0.0.3: bytes=32 time=0ms TTL=127
Reply from 20.0.0.3: bytes=32 time=0ms TTL=127
Reply from 20.0.0.3: bytes=32 time=0ms TTL=127
Ping statistics for 20.0.0.3:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>

Cisco Packet Tracer Student - C:\Users\ysrmo\OneDrive - Base PU College\Desktop\4thsem\CN\CN_LAB\lab4.2.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
10.0.0.20
20.0.0.20
Router-PT
Router0
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
Server-PT
Server0
10.0.0.1
PC-PT
PC3
PC-PT
PC4
Simulation Panel
Event List
Vis. Time(sec) Last De At Dev Type Info
2.992 Switch0 Serve... STP
2.992 Switch0 Rout... STP
2.992 Switch0 PC0 STP
2.992 Switch0 PC1 STP
2.992 Switch0 PC2 STP
Reset Simulation
Constant Delay
Capturing...
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters
Show All/None
Time: 00:32:11.943
Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward
Event List
Simulation
Connections
Scenario 0
New
Delete
Fire Last Stat Sourc Destinatic Type Colo Time(s Period Num Edit Delete
Successful PC0 PC3 IC... 0.000 N 0 (ed... (delete)

# WEEK 5

Configure Web Server, DNS within a LAN.

OBSERVATION:

20/7/23

## Lab-5

AIM -
Configure Web server, DNS within a LAN.

TOPOLOGY -

PROCEDURE -

- Connect a switch, PC and a server to form a LAN.
- Set PC's IP address by clicking on it and go to config tab there in fast Ethernet option set IP address as 10.0.0.1 and subnet mask.
- Set server's IP address as 10.0.0.2 and subnet mask respectively.
- Go to PC's Desktop and click on web browser, in the URL tab type 10.0.0.2. You will get a default display
- To make a cv here, we need to make changes in server services.
- Go to server → services → HTTP → index.html. Here create the cv and click on save
- Again go to PC → Desktop → webbrowser and type 10.0.0.2

you will the CV or content that is changed.

- Next, go to Server → Services → DNS and switch on the Services. Now add a Domain name and type the IP address as 10.0.0.2. Press add & save it.
- Again Go back to PC → Desktop → webbrowser and type the given domain name. Then we can see the CV which had been created earlier.

OUTPUT:

Web browser

| < | > | URL | http://gamana | Go | Stop |
|---|---|---|---|---|---|

CV

Gamana Yeluri R

USN: 1BM21CS065

Languages: C/C# / Java

Image:

OBSERVATION:

- If you wanted to go to a certain website you would open web browser and type domain name of that website. or else you can also type the IP address instead if you know that website's IP address.
- Since we can't remember IP addresses of all websites DNS server will search through its cache to find a matching IP address for that Domain name & when it finds it will resolve that domain name to IP address of website, once that is done then computer is able to communicate with a webserver & retrieve the webpage.

TOPOLOGY:

OUTPUT:

# WEEK 6

Configure RIP routing Protocol in Routers.

OBSERVATION:

20/7/23

LAB-6

AIM-
configure RIP routing Protocol in Routers

TOPOLOGY-



PROCEDURE -

- Create a Network using 3 routers and 2 PC's. connect routers using Serial DCE cable and PC to router using copper-cross over cable.
- Set the IP address and gateway no for both PC's as
  10.0.0.1 - IP 10.0.0.10 - gateway - PC 0
  40.0.0.1 - IP 40.0.0.10 - gateway - PC 1 respectively.
- Go to Router → CLI mode and execute the following commands:
  Step 1 - NO
  Step 2 - Enable
  Step 3 - Config T
  Step 4 - Interface FastEthernet 0/0

step5 - IP address 10.0.0.10 255.0.0.0
step6 - No shut
step7 - Exit
step8 - Interface se 2/0
step9 - IP address 20.0.0.10 255.0.0.0
step10 - Encapsulation ppp
step11 - Clock rate 64000
step12 - No shut

- Here for Router with FastEthernet execute only till step9 and type No shut
- Only for Router to Router connection execute all steps, also execute the step 11 only for the router connection which has a clock symbol at start. Repeat these steps for all routers.
- Again go to Router 0 → CLI mode and type these steps:
  step1: config T
  step2: router rip
  step3: Network 10.0.0.0
  step4: Network 20.0.0.0
  step5: Exit
- Repeat these steps for all routers.
- At last now go to each router and type show IP route. Here the IP addresses associated with that router will be labelled as C and other IP addresses are labelled as R.
- Lastly go to PC0 and ping a message to PC1 using ping destination IP address command.

PING OUTPUT:

Packet tracer PC command line 1.0

PC > Ping 40.0.0.1

Pinging 40.0.0.1 with 32 bytes of data:

Request timed out.

Reply from 40.0.0.1 : bytes = 32 times : 8ms TTL = 125

Reply from 40.0.0.1 : bytes = 32 times : 5ms TTL = 125

Reply from 40.0.0.1 : bytes = 32 times : 10ms TTL = 125

Ping statistics for 40.0.0.1:

Packets: Sent = 4, Recieved = 3, Lost = 1 (25% loss),

Approximate round trip times in milli seconds:

Minimum = 5ms, Maximum = 10ms, Average = 7ms

OBSERVATION:

- Routing Information protocol (rip) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between source and destination. It is a distance-vector routing protocol.
- Hop count is the no of routers coming in between source and destination. The path with least hop count is selected.
- updates of the Network are exchanged periodically.
- updates of routing information are always broadcast.
- Full routing tables are sent in updates.
- Routers always trust routing information recieved from neighbor routers.

24/7/23

TOPOLOGY:

OUTPUT:

Cisco Packet Tracer Student - C:\Users\ysrmo\OneDrive - Base PU College\Desktop\4thsem\CN\CN_LAB\lab6.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
20.0.0.20
Se2/0
30.0.0.10
Se3/0
Router-PT
Router1
10.0.0.10
Se2/0
20.0.0.10
Fa0/0
Router-PT
Router0
30.0.0.20
Se3/0
40.0.0.10
Fa0/0
Router-PT
Router2
Fa0
PC-PT
PC0
10.0.0.1
Fa0
PC-PT
PC1
40.0.0.1
Simulation Panel
Event List
Vis. Time(sec) Last De At De Type Info
0.006 Router2 Rout... ICMP
0.007 Router1 Rout... ICMP
0.008 Router0 PC0 ICMP
12.790 -- Rout... RIPv1
12.790 -- Rout... RIPv1
Reset Simulation
Constant Delay
Captured to: 12.790 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters
Show All/None
Time: 00:01:22.953
Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward
Event List
Simulation
Routers
Scenario 0
New
Delete
Fire Last Stat Sourc Destinatic Type Colo Time(s Period Num Edit Delete
Successful PC0 PC1 IC... 0.000 N 0 (ed... (delete)

# WEEK 7

Configure OSPF routing protocol.

OBSERVATION:

27/7/23

LAB-7

AIM-

Configure OSPF routing Protocol.

TOPOLOGY-



Procedure -

- Create the topology using 3 routers & 2 PC's
- Configure the PC's with IP address and gateway
- Configure each of the routers acc to IP address given
- During configuration, encapsulation ppp and clock rate should be set as done in RIP protocol.
- Then execute the following commands

Router → CLI → config mode

Step1 - router ospf 1 R1(config)# router ospf 1

Step2 - router-id 1.1.1.1

Step3 - Network 10.0.0.0 0.255.255.255 area 3

Step4 - Network 20.0.0.0 0.255.255.255 area 1

Step5 - exit

- repeat these commands for other routers.
- Then type show ip route.
- Next to set loopbacks go to interface s1/0/2 then do these

  step 1 : (in config-if mode) interface loopback 0

  step 2: ip address 172.16.1.252 255.255.0.0

  step 3: No shut down » 253, 254

- Repeat these steps for other 2 routers
- Create a virtual link between R1-R2, by this we create a virtual link to connect to area 0.

  In config mode of R1.

  step 1 : router ospf 1

  step 2 : area 1 virtual-link 2.2.2.2

  step 3 : # enter/exit

  In router 2 config-mode

  step 1 : # router ospf 1.

  step 2 : area 1 virtual link 1.1.1.1

  step 3 : exit

  step 4 : #

  on this step2 it should be in config router

- Check the routing table, show ip route.
- Lastly ping messages from PC to PC

PING OUTPUT-

Packet Tracer PC command-line 1.0

PC> Ping 40.0.0.10

Pinging 40.0.0.10 with 32 bytes of data:

Request timed out

Reply from 40.0.0.10 : bytes=32 times=11ms TTL=125

Reply from 40.0.0.10 : bytes=32 times=11ms TTL=125

Reply from 40.0.0.10 : bytes=32 times=8ms TTL=125

Ping statistics for 40.0.0.10 :
Packets Sent = 4 , Received = 3 , Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 8ms , Maximum = 11ms, Averge = 10ms

OBSERVATION:

- OSPF is a link-state routing protocol that is used to find the best path between source & destination router using its own SPF Algorithm.
- This network is divided into 4 areas. where area0 is the backbone.
- After we make the virtual-link between the area which is not connected to the backbone area, we can ping messages succefully.

27/7/23

TOPOLOGY:

OUTPUT:

Cisco Packet Tracer Student - C:\Users\Admin\Desktop\1BM21CS047\ospf.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
AREA 1
AREA 0
AREA 3
AREA 2
20.0.0.2
Se2/0
30.0.0.1
Se3/0
Router1
10.0.0.1
Fa0/0
Router0
20.0.0.1
30.0.0.2
40.0.0.1
PC-PT
PC0
10.0.0.10
PC1
40.0.0.10
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
20.002 -- Router1 OSPF
20.003 Router1 Router2 OSPF
22.376 -- Router0 OSPF
22.377 Router0 Router1 OSPF
22.378 -- Router0 OSPF
22.379 Router0 PC0 OSPF
22.380 -- Router2 OSPF
22.381 Router2 PC1 OSPF
22.383 -- Router1 OSPF
Reset Simulation
Constant Delay
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
Edit Filters
Show All/None
Time: 00:05:30.703
Power Cycle Devices PLAY CONTROLS:
Back
Auto Capture / Play
Capture / Forward
Event List
Simulation
Routers
(Select a Device to Drag and Drop to the Workspace)
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
Successful PC0 PC1 ICMP 0.000 N 0 (edit) (delete)
22°C
Mostly cloudy
Search
ENG
IN
11:03
27-07-2023

# WEEK 8

To construct a simple LAN and understand the concept and operation of Address Resolution Protocol (ARP).

OBSERVATION:

3/8/23

LAB - 8

AIM - To construct single LAN and understand the concept and operation of Address Resolution Protocol (ARP)

TOPOLOGY -



PROCEDURE -

- Create a topology of 3 PC's & a server
- Assign IP address to all PC's and server.
- Connect them through the switch
- Use the inspect tool to click on a PC to see ARP table
- Command in cmd for the same is arp -a.
- Initially ARP table is empty.
- Also in CLI of switch, the command - show mac address-table can be given on every transaction to see how the switch learns from transactions & build the address-table.
- Use the capture button in the simulation panel to go step by step so that the changes in ARP can be clearly noted.

PING OUTPUT:

PC > ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:

Reply from 10.0.0.4 : bytes = 32 time = 0ms TTL = 128

Reply from 10.0.0.4 : bytes = 32 time = 0ms TTL = 128

Reply from 10.0.0.4 : bytes = 32 time = 0ms TTL = 128

Reply from 10.0.0.4 : bytes = 32 time = 0ms TTL = 128

Ping statistics for 10.0.0.4:

Packets : Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC> arp -a

| Internet address | physical Address | Type |
|---|---|---|
| 10.0.0.4 | 0060.2f00.324d | dynamic. |

OBSERVATION:-

- when we ping 1 PC and server the address of server is known to PC & vice-versa
- when we ping between other two PC's simultaneously the addresses of each other are known.
- Every time a host requests a MAC address in order to send a packet to another host in the LAN, it checks its ARP cache to see if the IP to mac address translation address already exists. If the translation doesn't exits it performs ARP.

3/8/23

TOPOLOGY:

OUTPUT:

Logical
ARP Table for Server0
IP Address Hardware Address Interface
10.0.0.2 00D0.D35A.5B4A FastEthernet0
ARP Table for PC0
IP Address Hardware Address Interface
10.0.0.1 0001.C904.5457 FastEthernet0
ARP Table for PC2
IP Address Hardware Address Interface
10.0.0.3 0009.7C19.7260 FastEthernet0
ARP Table for PC1
IP Address Hardware Address Interface
10.0.0.4 0001.64A0.8ECB FastEthernet0
Switch1
Physical Config CLI
IOS Command Line Interface
Copy Paste
Simulation

# WEEK 9

To construct a VLAN and make a pc communicate among VLAN.

OBSERVATION:

10/8/23

LAB-9

AIM-
To construct a VLAN and make a PC communicate among VLAN

TOPOLOGY-

192.168.1.1
192.168.20.1
1841 Router
Fa0/0
Fa0/5
Fa0/4
Fa0/1
Fa0/2
Fa0/3
Switch 2960-24TT
Fa0
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
192.168.1.2
192.168.1.3
192.168.20.2
192.168.20.3

PROCEDURE -
- Create a topology as shown above. Chose 1841 router and 2960-24TT switch, hou.
- Set the ip address of the router and 4 PC's respectively we use class c type addresses also set gateways.
- In switch, go to config tab and select VLAN Database. Give any VLAN no. like 2 and name as vlan.
- Select the interface fastethernet 4/1 and make it trunk

- Next select the switches under 2nd interface which has interface 0/3 & 0/4. click on each of them and set VLAN number 2.
- Go to router → config tab and select VLAN Database and enter the name vlan & no. 2 created.
- Go to router → CLI and type the following commands.

  Step 1: configT
  Step 2: interface fa 0/0
  Step 3: IP address 192.168.1.1 255.255.255.0
  Step 4: NO shut
  Step 5: Exit.
  Step 6: configT
  Step 7: interface fa 0/0.1
  Step 8: encapsulation dot1q 2
  Step 9: ip address 192.168.20.1 255.255.255.0
  Step 10: No shut
  Step 11: Exit

- Ping message from PC to another VLAN PC.

PING OUTPUT:

Packet Tracer PC command line 1.0
PC> Ping 192.168.20.3
Pinging 192.168.20.3 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.3: bytes = 32 time = 0ms, TTL = 127
Reply from 192.168.20.3: bytes = 32 time = 5ms TTL = 127
Reply from 192.168.20.3: bytes = 32 time = 0ms TTL = 127
Ping statistics for 192.168.20.3:
  Packets: sent = 4, Received = 3, lost = 1 (25% loss),
  Approximate round trip times in milliseconds:
    Minimum = 0ms, Maximum = 5ms, Average = 1ms

OBSERVATION:

- We can have one device on one VLAN & another on another VLAN connected to the same switch. They will only hear other broadcast traffic from within their VLANS, as if they were connected to two switches
- Here VLANS doesn't use IP address instead deal with subnets / class C type addresses
- Inter-VLAN routing gives a flexible tool to logically subdivide their networks that has potential to enhance security & performance.

18/8/2023

TOPOLOGY:

OUTPUT:

PC0
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.20.3
Pinging 192.168.20.3 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.3: bytes=32 time=0ms TTL=127
Reply from 192.168.20.3: bytes=32 time=5ms TTL=127
Reply from 192.168.20.3: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.20.3:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 5ms, Average = 1ms
PC>

Cisco Packet Tracer Student - C:\Users\ysrmo\OneDrive - Base PU College\Desktop\4thsem\CN\CN_LAB\vlan.pkt
Logical
192.168.1.1
192.168.20.1
PC-PT PC0
192.168.1.2
PC-PT PC1
192.168.1.3
PC-PT PC2
192.168.20.2
PC-PT PC3
192.168.20.3
Simulation Panel
Event List
Play Controls
Back
Auto Capture / Play
Capture / Forward
Simulation

# WEEK 10

Demonstrate the TTL/ Life of a Packet.

OBSERVATION:

10/5/23

LAB - 10

AIM -

Demonstrate the TTL / Life of a Packet

TOPOLOGY -



PROCEDURE -

- Create a topology as shown above with two PC's and 3 Routers.
- Set the IP address and gateway for both PC's
- configure the routers either static / default routing way.
- In simulation mode send a simple PDU from one PC to another.
- use capture button to capture every transfer.
- click on the PDU during every transfer to see the Inbound & outbound PDU details.

OUTPUT:

IP

| 0 | 4 | 8 | 16 | 19 | 31 |
|---|---|---|---|---|---|
| 4 | IHL | DSCP | TL : 28 | | |
| ID : 0X6 | | | 0X | 0X0 | |
| TTL : 255 | PRO : 0x1 | | CHKSUM | | |
| SRC IP : 10.0.0.1 | | | | | |
| DST IP : 40.0.0.1 | | | | | |
| OPT : 0X0 | | | | 0X0 | |
| DATA (VARIABLE LENGTH) | | | | | |

OBSERVATION -

- The no. of hops the packet travel before being discarded as TTL
- Datagrams TTL field is set by the sender & reduced by each router along the path to its destination.
- The router reduces TTL value by one while forwarding the packets.
- when the TTL value is 0, the router discards it & sends an ICMP message.

18/8/2022

TOPOLOGY:

OUTPUT:

Cisco Packet Tracer Student - C:\Users\Admin\Desktop\1bm21cs065\ospf.pkt
Logical
AREA 1
20.0.0.2
Se2/0
10.0.0.1
Fa0/0
Router-PT
Router0
20.0.0.1
40.0.0.1
AREA 3
AREA 2
Fa0
PC-PT
PC0
10.0.0.10
PC-PT
PC1
40.0.0.10
PDU Information at Device: Router1
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
PPP
IP
ICMP
SRC IP: 10.0.0.10
DST IP: 40.0.0.10
DATA (VARIABLE LENGTH)
Simulation Panel
Event List
Play Controls
Time: 00:00:57.256
Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward
Event List
Simulation

Cisco Packet Tracer Student - C:\Users\Admin\Desktop\1bm21cs065\ospf.pkt
Logical
AREA 1
20.0.0.2
Se2/0
10.0.0.1
Fa0/0
Router-PT
Router0
20.0.0.1
40.0.0.1
AREA 3
AREA 2
Fa0
PC-PT
PC0
10.0.0.10
PC-PT
PC1
40.0.0.10
PDU Information at Device: Router2
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
PPP
IP
ICMP
SRC IP: 10.0.0.10
DST IP: 40.0.0.10
DATA (VARIABLE LENGTH)
Simulation Panel
Event List
Play Controls
Time: 00:00:57.257
Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward
Event List
Simulation

Logical
AREA 1
20.0.0.2
Se2/0
Se2/0
10.0.0.1
Fa0/0
Router-PT
Router0
20.0.0.1
AREA 3
Fa0
PC-PT
PC0
10.0.0.10
40.0.0.1
AREA 2
Fa0
PC-PT
PC1
40.0.0.10
PDU Information at Device: PC1
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
Ethernet II
PREAMBLE: 101010...1011
DEST MAC: 0060.4789.AB50
SRC MAC: 0009.7C28.C636
TYPE: 0x800
DATA (VARIABLE LENGTH)
FCS: 0x0
IP
DSCP: 0x0
TL: 28
ID: 0x3
TTL: 252
PRO: 0x1
CHKSUM
SRC IP: 10.0.0.10
DST IP: 40.0.0.10
OPT: 0x0
DATA (VARIABLE LENGTH)
ICMP
TYPE: 0x8
CODE: 0x0
CHECKSUM
ID: 0x4
SEQ NUMBER: 3
Simulation Panel
Event List
Play Controls
Event List Filters - Visible Events
Simulation

# WEEK 11

To construct a WLAN and make the nodes communicate wirelessly

OBSERVATION:

LAB-11

AIM -

To construct a WLAN and make the nodes communicate wirelessly

TOPOLOGY -



PROCEDURE -

- construct the above topology.
- Configure PC 0 & Router 0 as normally done
- Configure Access point 1 - Port 1 → SSID Name - WLAN.
- Select WEP & give any 10 digit hex key - 1234567890
- Configure PC1 & laptop with wireless standards
- Switch off the device. Drag the existing PT-HOST-NM-1AM to the component listed in LHS. Drag WMP300N wireless interface to the empty port. Switch on the device.

- In the config tab a new wireless interface would have been added. Now configure SSID, WEP, WEP Key, IP address and gateway to the device.
- Ping from every device to every other device.

PING OUTPUT:-

Packet Tracer PC command line 1.0

PC> Ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Request timed out

Reply from 10.0.0.3 : bytes = 32 time = 0ms TTL = 127

Reply from 10.0.0.3 : bytes = 32 time = 0ms TTL = 127

Reply from 10.0.0.3 : bytes = 32 time = 2ms TTL = 127

Ping statistics for 10.0.0.3

Packets : sent = 4, Received = 3, Lost = 1 (25% loss),

Approximate round trip times in milliseconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

OBSERVATION:-

- A WLAN is a group of colocated devices that form a network based on radio transmissions.
- Data sent in packets contain layers with labels & instructions, MAC address to endpoints for routing.
- The access point is the base station that serves as a hub to which other stations connect.
- With one access point we can connect to multiple devices wirelessly & transmit data.

18/8/2023

TOPOLOGY:

Cisco Packet Tracer Student
Logical
10.0.0.1
Fa0/0
Router-PT
Router0
Fa1/1
Fa2/1
Fa0/1
Switch0
Access Point-PT
Access Point0
Fa0
PC-PT
PC0
10.0.0.2
PC-PT
PC2
10.0.0.3
Laptop-PT
10.0.0.4
Realtime

PC1
Physical
Config
Desktop
Custom Interface
MODULES
WMP300N
PT-HOST-NM-1AM
PT-HOST-NM-1CE
PT-HOST-NM-1CFE
PT-HOST-NM-1CGE
PT-HOST-NM-1FFE
PT-HOST-NM-1FGE
PT-HOST-NM-1W
PT-HOST-NM-1W-A
PT-HOST-NM-3G/4G
PT-HEADPHONE
PT-MICROPHONE
PT-CAMERA
PT-USB-HARD-DRIVE
Physical Device View
Zoom In
Original Size
Zoom Out
Customize Icon in Physical View
Customize Icon in Logical View
The Linksys-WMP300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN access.

Laptop0
Physical
Config
Desktop
Custom Interface
MODULES
WPC300N
PT-LAPTOP-NM-1AM
PT-LAPTOP-NM-1CE
PT-LAPTOP-NM-1CFE
PT-LAPTOP-NM-1CGE
PT-LAPTOP-NM-1FFE
PT-LAPTOP-NM-1FGE
PT-LAPTOP-NM-1W
PT-LAPTOP-NM-1W-A
PT-LAPTOP-NM-3G/4G
PT-HEADPHONE
PT-MICROPHONE
PT-CAMERA
PT-USB-HARD-DRIVE
Physical Device View
Zoom In
Original Size
Zoom Out
Customize Icon in Physical View
Customize Icon in Logical View
The Linksys-WPC300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN access.

OUTPUT:

PC0
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 10.0.0.3
Pinging 10.0.0.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.0.0.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 10.0.0.3
Pinging 10.0.0.3 with 32 bytes of data:
Reply from 10.0.0.3: bytes=32 time=21ms TTL=128
Reply from 10.0.0.3: bytes=32 time=7ms TTL=128
Reply from 10.0.0.3: bytes=32 time=9ms TTL=128
Reply from 10.0.0.3: bytes=32 time=10ms TTL=128
Ping statistics for 10.0.0.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 7ms, Maximum = 21ms, Average = 11ms
PC>

# WEEK 12

To understand the operation of TELNET by accessing the router in server room from a PC in IT office.

OBSERVATION:

10/5/23

## LAB - 12

AIM -

To understand the operation of TELNET by accessing the router in server room from a PC in IT office.

TOPOLOGY -

PROCEDURE -

- Create a topology as shown above
- Configure the IP address & gateway for PC0.
- Configure the router by executing the following commands

step 1 : enable
step 2 : configT
step 3 : hostname r1
step 4 : enable secret p1
step 5 : interface fastethernet 0/0
step 6 : ip address 10.0.0.1 255.0.0.0
step 7 : No shut
step 8 : line vty 0 5
step 9 : login
step 10 : password p0
step 11 : Exit ; Exit
step 12 : wr

- Ping message to router
Password for User Acess Verification is p0.
password for enable is p1.
Accessing router CLI from PC.
show ip route

PING OUTPUT-

Packet Tracer PC command line 1.0
PC > Ping 10.0.0.1
Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes = 32 time = 0ms TTL = 255
Reply from 10.0.0.1: bytes = 32 time = 0ms TTL = 255
Reply from 10.0.0.1: bytes = 32 time = 0ms TTL = 255
Reply from 10.0.0.1: bytes = 32 time = 0ms TTL = 255

Ping statistics for 10.0.0.1:
Packets: sent = 4, Received = 4, lost = 0 (0% loss),
Approximate round trip times in millisecondes:
Minimum = 0ms, Maximum = 0ms, Average = 0ms,

PC > telnet 10.0.0.1
Typing 10.0.0.1 ... open
User Acess verification
Password: P0
R1 > enable
Password: P1:
r1 # show ip route

C 10.0.0.0/8 is directly connected, FastEthernet 0/0.

OBSERVATION -

- TELNET stands for Teletype Network. It is a type of protocol that enables one computer to connect to the local computer.
- It is used as a standard TCP/IP protocol for virtual terminal service provided by ISO.
- During TELNET operation, whatever is being performed on the remote computer will be displayed by the local computer. Telnet operates on a client/ server principle.

18/8/2023

TOPOLOGY:

OUTPUT:

PC0

Physical | Config | Desktop | Custom Interface

**Command Prompt**

```
Packet Tracer PC Command Line 1.0
PC>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=1ms TTL=255
Reply from 10.0.0.1: bytes=32 time=0ms TTL=255
Reply from 10.0.0.1: bytes=32 time=0ms TTL=255
Reply from 10.0.0.1: bytes=32 time=0ms TTL=255

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>telnet 10.0.0.1
Trying 10.0.0.1 ...Open


User Access Verification

Password:
% Password:  timeout expired!

[Connection to 10.0.0.1 closed by foreign host]
PC>telnet 10.0.0.1
Trying 10.0.0.1 ...Open


User Access Verification

Password:
Password:
Password:

[Connection to 10.0.0.1 closed by foreign host]
PC>telnet 10.0.0.1
Trying 10.0.0.1 ...Open


User Access Verification

Password:
r1>enable
Password:
r1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
r1#
```

# WEEK 13

Write a program for error detecting code using CRC- CCITT (16-bits).

CODE:

```
#include<stdio.h>
int arr[17];

void xor(int x[], int y[])
{
   int k=0;
   for(int i=1;i<16;i++)
   {
      if(x[i]==y[i])
         arr[k++]=0;
      else
         arr[i]=1;
   }
}

void main()
{
   int dd[17],div[33],ze[17],i,k;

   printf("Enter the dataword \n");
   for(i=0;i<17;i++)
      scanf("%d",&div[i]);

   for(i=i;i<33;i++)
      div[i]=0;

   for(i=0;i<17;i++)
      ze[i]=0;
   printf("Enter dividend \n");
```

```
for(i=0;i<17;i++)
    scanf("%d",&dd[i]);

i=0;
k=0;
    for(i=i;i<17;i++)
        arr[k++]=div[i];
while(i<33)
{
    if(arr[0]==0)
        xor(arr,ze);
    else
        xor(arr,dd);

    arr[16]=div[i++];

}
k=0;
for(i=17;i<33;i++)
    div[i]=arr[k++];
printf("Codeword: ");
    for(i=0;i<33;i++)
        printf("%d",div[i]);

for(i=0;i<17;i++)
    arr[i]=0;

printf("\nAt receiver end \n");

 k=0;
    for(i=i;i<17;i++)
        arr[k++]=div[i];
while(i<33)
{
```

```
        if(arr[0]==0)
            xor(arr,ze);
        else
            xor(arr,dd);

        arr[16]=div[i++];

    }
    k=0;
    for(i=17;i<33;i++)
        div[i]=arr[k++];

    printf("Codeword: ");
        for(i=0;i<33;i++)
            printf("%d",div[i]);
}
```

OUTPUT:

OBSERVATION:

17/8/23

# LAB - 13

AIM -
Write a program for error detecting code using CRC - CCITT (16 bits)

CODE -

```
#include <stdio.h>
int arr[17];
void xor [int x[], int y[])
{
    int k=0;
    for (int i=1; i<16; i++)
    {
        if (x[i]==y[i])
            arr[k++]=0;
        else
            arr[i]=1;
    }
}
void main()
{
  int dd [17], div [33], ze [17], i, k;
  printf(" Enter the dataword ");
   for (i=0; i<17; i++)
        scanf ("%d", &div[i]);
  for (i=i; i<33; i++)
      div[i]=0;
  for (i=0; i<17; i++)
      ze[i]=0;
```

```
printf(" Enter dividend ");
  for (i=0; i<17; i++)
      scanf ("%d", &dd[i]);
  l=0;
  K=0;
      for (i=l; i<17; i++)
          arr[K++] = dir[i];
  while (l<33)
  {
      if (arr[0] == 0)
          xor (arr, ze);
      else
          xor (arr, dd);
      arr[16] = dir[l+4];
  }
  K=0;
  for (l=17; l<33; l++)
      dir[l] = arr[K++];
    printf(" codeword");
      for (i=0; i<33; i++)
          printf("%d", dir[i]);
  for (i=0; i<17; i++)
      arr[i]=0;
  printf (" At receiver end");
   K=0;
      for (i=l, i<17; i++)
          arr[K++] = dir[i];
   while (l<33)
   {
      if (arr[0] == 0)
          xor (arr, ze);
```

```
else
    xor (arr, dd);
    arr [16] = dir [i++];
  }
K=0;
for (i=17; i<33; i++)
      dir [i] = arr [k++];
printf (" codeword");
    for (i=0; i<33; i++)
        printf ("%d", dir[i]);
}
```

OUTPUT:

Enter the dataword

10110011110010111

Enter the divisor

10001000000100011

codeword: 10110011110010111 00000000000 11011

At receiver end

codeword: 10110011110010111 00000000000 00000

30/8/2023

# WEEK 14

Write a program for congestion control using Leaky bucket algorithm.

CODE:

```
#include <stdio.h>
#include <stdlib.h> // Include this for the rand() function
int main()
{
   int buckets, outlets, k = 1, num, remaining;
   printf("Enter Bucket size and outstream size\n");
   scanf("%d %d", &buckets, &outlets);
   remaining = buckets;
   while (k)
   {
      num = rand() % 1000; // Generate a random number between 0 and 999
      if (num < remaining)
      {
         remaining = remaining - num;
         printf("Packet of %d bytes accepted\n", num); // Added missing variable
      }
      else
      {
         printf("Packet of %d bytes is discarded\n", num);
      }
      if (buckets - remaining > outlets)
      {
         remaining += outlets; // Fixed the calculation
      }
      else
         remaining = buckets;
      printf("Remaining bytes: %d \n", remaining);
      printf("If you want to stop input, press 0, otherwise, press 1\n");
      scanf("%d", &k);
```

```
    }
    while (remaining < buckets) // Fixed the condition
    {
        if (buckets - remaining > outlets)
        {
            remaining += outlets; // Fixed the calculation
        }
        else
            remaining = buckets;
        printf("Remaining bytes: %d \n", remaining);
    }
    return 0; // Added a return statement to indicate successful completion
}
```

OUTPUT:

```
PS D:\VS Code> cd "d:\VS Code\OS\" ; if ($?) { gcc bucket.c -o bucket } ; if ($?) { .\bucket }
Enter Bucket size and outstream size
2000
100
Packet of 41 bytes accepted
Remaining bytes: 2000
If you want to stop input, press 0, otherwise, press 1
1
Packet of 467 bytes accepted
Remaining bytes: 1633
If you want to stop input, press 0, otherwise, press 1
1
Packet of 334 bytes accepted
Remaining bytes: 1399
If you want to stop input, press 0, otherwise, press 1
1
Packet of 500 bytes accepted
Remaining bytes: 999
If you want to stop input, press 0, otherwise, press 1
1
Packet of 169 bytes accepted
Remaining bytes: 930
If you want to stop input, press 0, otherwise, press 1
1
Packet of 724 bytes accepted
Remaining bytes: 306
If you want to stop input, press 0, otherwise, press 1
1
Packet of 478 bytes is discarded
Remaining bytes: 406
If you want to stop input, press 0, otherwise, press 1
1
Packet of 358 bytes accepted
Remaining bytes: 148
If you want to stop input, press 0, otherwise, press 1
1
Packet of 962 bytes is discarded
Remaining bytes: 248
If you want to stop input, press 0, otherwise, press 1
0
Remaining bytes: 348
Remaining bytes: 448
Remaining bytes: 548
Remaining bytes: 648
Remaining bytes: 748
```

```
Remaining bytes: 348
Remaining bytes: 448
Remaining bytes: 548
Remaining bytes: 648
Remaining bytes: 748
Remaining bytes: 848
Remaining bytes: 948
Remaining bytes: 1048
Remaining bytes: 1148
Remaining bytes: 1248
Remaining bytes: 1348
Remaining bytes: 1448
Remaining bytes: 1548
Remaining bytes: 1648
Remaining bytes: 1748
Remaining bytes: 1848
Remaining bytes: 1948
Remaining bytes: 2000
PS D:\VS Code\OS>
```

OBSERVATION:

14/5/23

# LAB-14

AIM-
write a program for congestion control using leaky bucket algorithm.

CODE-

```
# include <stdio.h>
# include <stdlib.h>
int main()
{
  int buckets, outlets, K=1, num, remaining;
  printf("Enter Bucket size and the outstream size");
  scanf("%d %d", &buckets, &outlets);
  remaining = buckets;
while(K)
{
  num = rand() % 1000;
  if (num < remaining)
    {
      remaining = remaining - num;
      printf("Packets of %d bytes are accepted", num);
    }
  else
    {
      printf("Packet of %d bytes is discarded", num);
    }
  if (buckets - remaining > outlets)
    {
      remaining += outlets;
    }
```

```
else
    remaining = buckets;
printf(" Rimaining buckets : %d \n", remaining);
printf(" If you wan to stop input press 0, else press 1);
scand ("%d", &k);
}
while (remaining < buckets)
{
  if (buckets - remaining > outlets)
  {
    remaining += outlets;
  }
  else
    remaining = buckets;
  printf(" Rimaining byts : %d ", remaining);
}
return 0;
}
```

OUTPUT:

```
Enter Bucket size and outstream size
1000 200
Packet of 41 byts are accepted
Rimaining byts :1000
If you want to stop input press 0, otherwise press 1
1
Packet of 467 byts are accepted
Remaining byts 733
If you want to stop input press 0, otherwise press 1
1
Packets of 334 byts are aapted
Rimaining byts : 599
```

# WEEK 15

Using TCP/IP sockets, write a client-server program to make client sending the file name and the server to send back the contents of the requested file if present.

CODE:

ClientTCP.py

```
from socket import *
serverName = “127.0.0.1”
serverPort = 12000
clientSocket = socket(AF_INET, SOCK_STREAM)
clientSocket.connect((serverName,serverPort))
sentence = input(“\nEnter file name: “)
clientSocket.send(sentence.encode())
filecontents = clientSocket.recv(1024).decode()
print (“\nFrom Server:\n”)
print(filecontents)
clientSocket.close()
```

ServerTCP.py

```
from socket import *
serverName=”127.0.0.1”
serverPort = 12000
serverSocket = socket(AF_INET,SOCK_STREAM)
serverSocket.bind((serverName,serverPort))
serverSocket.listen(1)
while 1:
print (“The server is ready to receive”)
connectionSocket, addr = serverSocket.accept()
sentence = connectionSocket.recv(1024).decode()
file=open(sentence,”r”)
l=file.read(1024)
connectionSocket.send(l.encode())
```

print (“\nSent contents of “ + sentence)
file.close()
connectionSocket.close()

OUTPUT:

OBSERVATION:

classmate

Date

Page

24/8/23

# LAB-15

AIM - Using TCP/IP sockets, write a client-server program to make client sending the filename and the server to send back the contents of the requested file if present.

Client TCP.py

```
from socket import *
ServerName = '127.0.0.1'
ServerPort = 12000
clientSocket = Socket (AF_INET, SOCK-STREAM)
clientSocket.connect ((ServerName, ServerPort))
Sentence = input ("\n Enter file name:")

clientSocket.send (sentence.encode())
fileconteents = clientSocket.recv(1024).decode()
print("\n From server:\n")
print (fileconteents)
clientSocket.close()
```

ServerTCP.Py

```
from sockt import *
Server Name = "127.0.0.1"
ServerPort = 12000
Server Socket = socket (AF_INET, SOCK-STREAM)
serverSocket.bind ((serverName, serverPort))
serverSocket.listen (1)
while 1:
    print (" The server is ready to recive")
    connectionSocket, addr = serverSocket.accept()
    sentence = connectionSocket.recv (1024).decode()
    file = open (sentence, "r")
    l = file.read (1024)
```

```
connectionSocket.send(l.encode())
print('\n sent contents of ' + sentfile)
file.close()
connectionSocket.close()
```

# WEEK 16

Using UDP sockets, write a client-server program to make the client send the file name and the server to send back the contents of the requested file if present.

CODE:

ClientUDP.py

```
from socket import *
serverName = “127.0.0.1”
serverPort = 12000
clientSocket = socket(AF_INET, SOCK_DGRAM)
sentence = input(“\nEnter file name: “)
clientSocket.sendto(bytes(sentence,”utf-8”),(serverName, serverPort))
filecontents,serverAddress = clientSocket.recvfrom(2048)
print (“\nReply from Server:\n”)
print (filecontents.decode(“utf-8”))
# for i in filecontents:
# print(str(i), end = “ ”)
clientSocket.close()
clientSocket.close()
```

ServerUDP.py

```
from socket import *
serverPort = 12000
serverSocket = socket(AF_INET, SOCK_DGRAM)
serverSocket.bind((“127.0.0.1”, serverPort))
print (“The server is ready to receive”)
while 1:
sentence, clientAddress = serverSocket.recvfrom(2048)
sentence = sentence.decode(“utf-8”)
file=open(sentence,”r”)
```

```
con=file.read(2048)
serverSocket.sendto(bytes(con,”utf-8”),clientAddress)
print (“\nSent contents of “, end = “ “)
print (sentence)
# for i in sentence:
# print (str(i), end = “ “)
file.close()
```

OUTPUT:

OBSERVATION:

classmate

Date

Page

24/8/23

# LAB - 16

AIM -

Using UDP sockets, write a client-server program to make client sending the file name and the server to send back the contents of the requested file if present.

CODE -

Client UDP.py

```
from socket import *
serverName = "127.0.0.1"
serverPort = 12000
clientSocket = socket(AF_INET, SOCK_DGRAM)
sentence = input("\n Enter file name");
clientSocket.sendto(bytes(sentence, "utf-8"), (serverName,
  serverPort))
file contents, serverAddress = clientSocket.recvfrom(2048)
print("\n Reply from server: \n")
print(fileconteents.decode("utf-8"))
# for i in filecontents:
  # print(str(i), end="")
clientsocket.close()
client socket.close()
```

ServerUDP.py

```
from socket import *
serverPort = 12000
serverSocket = socket(AF_INET, SOCK_DGRAM)
serverSocket.bind(("127.0.0.1", serverPort))
print("The server is ready to receive")
while 1:
```

```
sentence, clientAddress = serverSocket.recvfrom(2048)
sentence = sentence.decode("utf-8")
file = open(sentence,"r")
con = file.read(2048)
serverSocket.sendto(bytes(con,"utf-8"), clientAddress)
print('\n Sent contents of', end = '')
print(sentence)
# for i in sentence:
    # print(str(i), end = '')
    file.close()
```

# WEEK 17

Tool Exploration -Wireshark

OBSERVATION:

24/8/23

LAB-17

AIM- Tool Exploration :- Wireshark

Wireshark is an open-source packet analyser, which is used for education, analysis, software development, communicat protocol development and network troubleshooting. It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems. Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a fre packet sniffer computer application. It puts the network card into an unselective mode, i.e, to accept all the packets which it receives

Uses of Wireshark -

Wireshark can be used in the following ways:

1. It is used by network security engineers to examine security problems
2. It allows the users to watch all the traffic being passed over the network
3. It is used by network engineers to troubleshoot network issue.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyse dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc, communicate in a local network or the rest of the world.

## Functionality of Wireshark

Wireshark is similar to tcpdump in networking. TCP dump is a common packet analyzer which allows the user to display other packets and TCP/IP Packets, being transmitted & received over a network attached to the computer. It has a graphic end and some sorting & filtering functions. Wireshark users can see all the traffic passing through the network. Wireshark can also monitor the unicast traffic which is not sent to the network's MAC address interface. But, the switch does not pass all the traffic to the port. Hence, the promiscuous mode is not sufficient to see all the traffic. The various network taps or port mirroring is used to extend capture at any point. Port mirroring is a method to monitor network traffic. When it is enabled, the switch sends the copies of all the network packets present at one port to another port.

Features of Wireshark

- It is multi-platform software, i.e. it can run on Linux, OSX, Windows, FreeBSD, etc.
- It is a standard three-pane packet browser.
- It performs deep inspection of the hundreds of protocols.
- It often involves live analysis i.e, from different types of the network like the Ethernet, loopback, etc. we can read live data.
- It has sort & filter options which makes ease to the user to view the data.
- It is also useful in VOIP analysis & can capture raw USB traffic.
- various settings, like timers & filters, can be used to filter output.
- It can only capture packet on the PCAP supported networks.