

Ex No: 6

Date:

PERFORMANCE ANALYSIS OF TCP & UDP PROTOCOL USING SIMULATION TOOL.

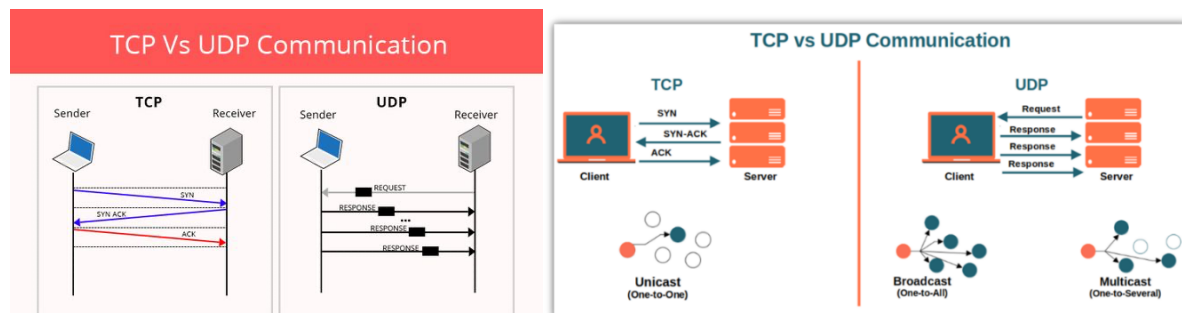
Aim:

To create a simple LAN connection with Switch-PT switch, Server-PT server (configured as a multi server), PC-PT PC's and Laptop-PT Laptops and analyze the performance of TCP and UDP protocols using CISCO packet tracer.

Theory:

Ideal settings for TCP (transmission control protocol) and UDP (user datagram protocol) performance vary depending on network settings and requirements. TCP and UDP were designed to do the same thing in two different ways, the former being designed for stability (never lose a packet), and the latter for speed. With TCP, your application will effectively stop all transfers in order to recover the lost segment, whereas UDP expects the application to either ignore the loss, or just queue up the lost segment while all the other segments continue. In a Multi-server, all the server methods/protocols (DNS, EMAIL, FTP, SMTP etc.) are run together. Basically, it's a one server replacement for all the different servers.

Simulation mode provides the ability to view the functionality of the different protocols. As data moves through the network, it is broken down into smaller pieces and identified in some fashion so that the pieces can be put back together. Each of these pieces is assigned a specific name (protocol data unit [PDU]) and associated with a specific layer. Packet Tracer Simulation mode enables the user to view each of the protocols and the associated PDU. The steps outlined below lead the user through the process of requesting services using various applications available on a client PC.



Procedure:

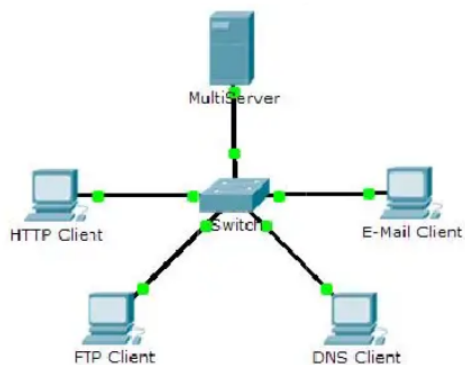
1. At first, the network is made by installing the required media (Laptop-PT, Laptop, PC-PT PCs, Switch-PT switch and Server-PT server).
2. The Multiserver (Server-PT) is configured to host Email, FTP and HTTP service. The DNS is configured accordingly.

3.All the PC's and Laptops are added to the Email and FTP configuration with unique Id and passwords.

4.To check TCP and UDP performance, we use nslookup (for DNS config), login to ftp and download a file (for FTP config), open the website (for HTTP config) and send and receive an email (for Email config) in the simulation mode. Also, in the multiserver command prompt...we ping the address 192.168.11.1 to check TCP and UDP performance.

5.Finally, the PDU in real time mode is matched with the packet transfer history in simulation mode for network verification.

SIMPLE LAN NETWORK



Part 1:Generate Network Traffic in Simulation Mode

Step 1: Generate traffic to populate Address Resolution Protocol (ARP) tables.

Perform the following tasks task to reduce the amount of network traffic viewed in the simulation.

- a. Click MultiServer and click the Desktop tab > Command Prompt.
- b. Enter the ping 192.168.1.255 command. This will take a few seconds as every device on the network responds to MultiServer.
- c. Close the MultiServer window.

Step 2: Generate web (HTTP) traffic.

- a. Switch to Simulation mode.
- b. Click HTTP Client and click the Desktop tab > Web Browser.
- c. In the URL field, enter 192.168.1.254 and click Go. Envelopes (PDUs) will appear in the simulation window.
- d. Minimize, but do not close, the HTTP Client configuration window.

Step 3: Generate FTP traffic.

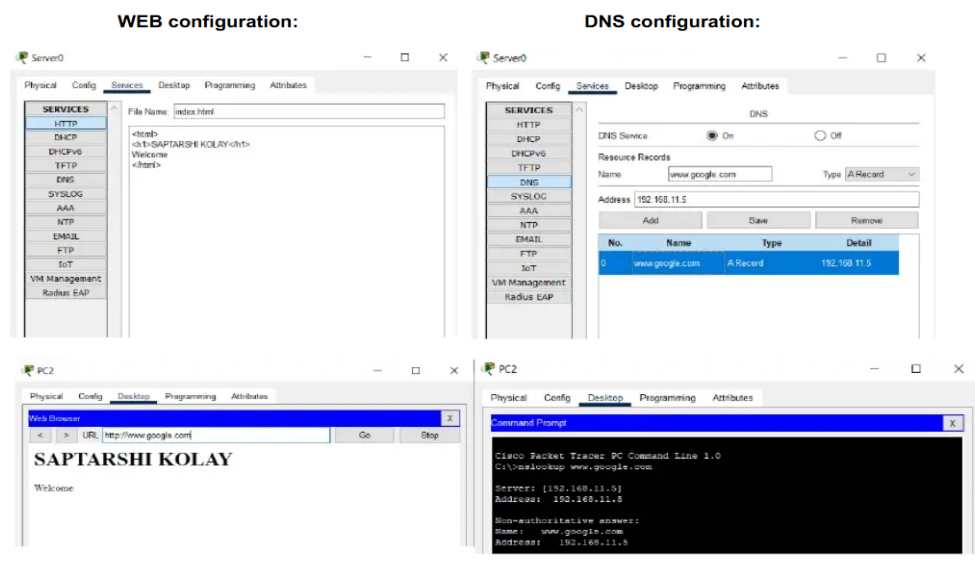
- Click FTP Client and click the Desktop tab > Command Prompt.
- Enter the ftp 192.168.1.254 command. PDUs will appear in the simulation window.
- Minimize, but do not close, the FTP Client configuration window.

Step 4: Generate DNS traffic.

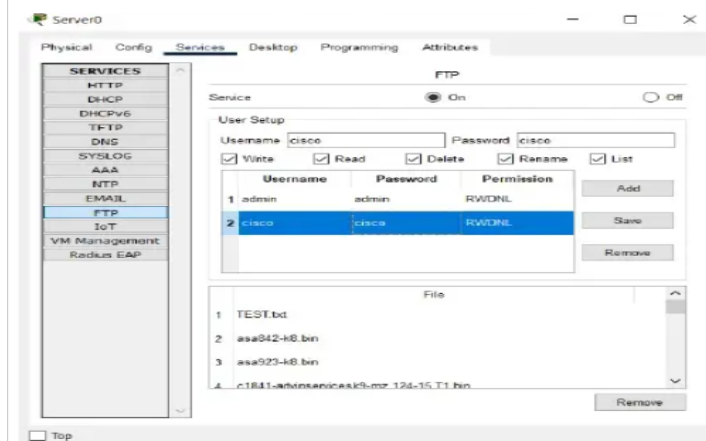
- Click DNS Client and click the Desktop tab > Command Prompt.
- Enter the nslookup multiserver.pt.ptu command. A PDU will appear in the simulation window.
- Minimize, but do not close, the DNS Client configuration window.

Step 5: Verify that the traffic is generated and ready for simulation.

Every client computer should have PDUs listed in the Simulation Panel.



FTP configuration:



Part 2: Examine Functionality of the TCP and UDP Protocols

Step 1: Examine multiplexing as all of the traffic crosses the network.

You will now use the Capture/Forward button and the Back button in the Simulation Panel. Click Capture/Forward once. All of the PDUs are transferred to the switch.

- a. Click Capture/Forward again. Some of the PDUs disappears. Click Capture/Forward six times. All clients should have received a reply.
- b. A variety of PDUs appears in the event list in the upper right pane of the simulation window.
- c. Click Back eight times. This should reset the simulation.

Note: Do not click Reset Simulation any time during this activity; if you do, you will need to repeat the steps in Part 1.

Step 2: Examine HTTP traffic as the clients communicate with the server.

Filter the traffic that is currently displayed to display only HTTP and TCP PDUs filter the traffic that is currently displayed:

- a. Click Edit Filters and toggle the Show All/None check box.
- b. Select HTTP and TCP. Click anywhere outside of the Edit Filters box to hide it. The Visible Events should now display only HTTP and TCP PDUs.
- c. Click Capture/Forward. Hold your mouse above each PDU until you find one that originates from HTTP Client. Click the PDU envelope to open it.
- d. Click the Inbound PDU Details tab and scroll down to the last section.
- e. Record the SRC PORT, DEST PORT, SEQUENCE NUM, and ACK NUM values.
- f. Close the PDU and click Capture/Forward until a PDU returns to the HTTP Client with a checkmark.
- g. Click the PDU envelope and select Inbound PDU Details.
- h. There is a second PDU of a different color, which HTTP Client has prepared to send to MultiServer. This is the beginning of the HTTP communication. Click this second PDU envelope and select Outbound PDU Details.
- i. Click Back until the simulation is reset.

Step 3: Examine FTP traffic as the clients communicate with the server.

- a. In the Simulation Panel, change Edit Filters to display only FTP and TCP.
- b. Click Capture/Forward. Hold your cursor above each PDU until you find one that originates from FTP Client. Click that PDU envelope to open it.
- c. Click the Inbound PDU Details tab and scroll down to the last section.
- d. Record the SRC PORT, DEST PORT, SEQUENCE NUM, and ACK NUM values.
- e. Close the PDU and click Capture/Forward until a PDU returns to the FTP Client with a checkmark.
- f. Click the PDU envelope and select Inbound PDU Details.
- g. Click the Outbound PDU Details tab
- h. Close the PDU and click Capture/Forward until a second PDU returns to the FTP Client. The PDU is a different color.
- i. Open the PDU and select Inbound PDU Details. Scroll down past the TCP section.
- j. Click Back until the simulation is reset.

Step 4: Examine DNS traffic as the clients communicate with the server.

In the Simulation Panel, change Edit Filters to display only DNS and UDP.

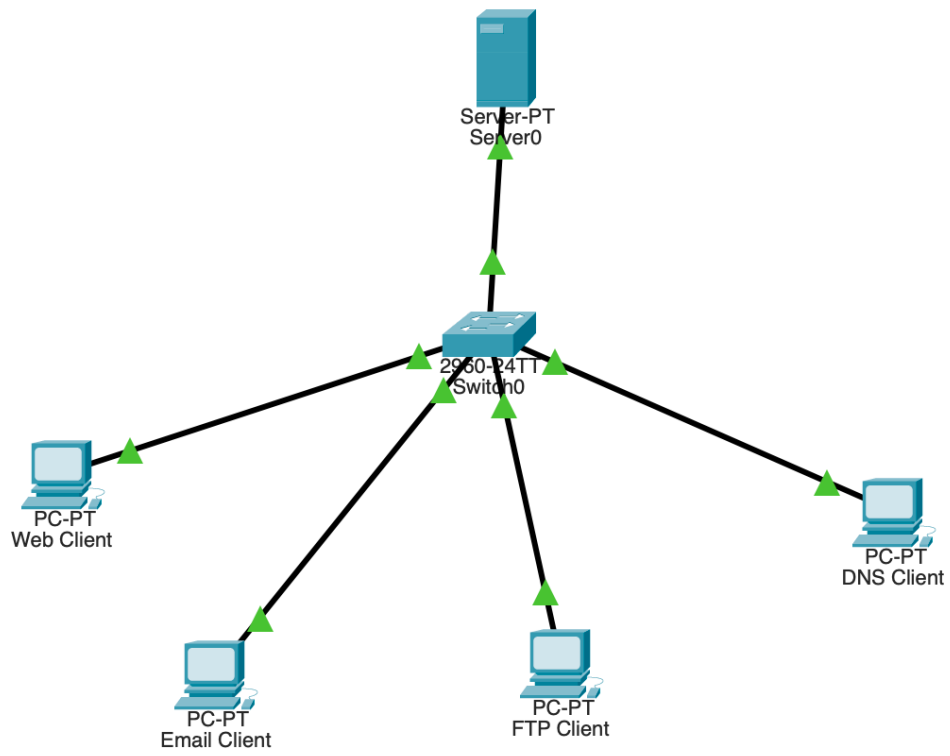
- a. Click the PDU envelope to open it.
- b. Click the Inbound PDU Details tab and scroll down to the last section.
- c. Record the SRC PORT and DEST PORT values.
- d. Close the PDU and click Capture/Forward until a PDU returns to the DNS Client with a checkmark.
- e. Click the PDU envelope and select Inbound PDU Details.
- f. Click Back until the simulation is reset.

Step 5: Examine the use of port numbers from the server.

To see TCP active sessions, perform the following steps in quick succession:

- a. Switch back to Realtime mode.
- b. Click MultiServer and click the Desktop tab > Command Prompt.
- c. Enter the netstat command.
- d. Repeat the netstat command several times until you see only one session still ESTABLISHED.

DNS SERVICES:



Server0

PhysicalConfigServicesDesktopProgrammingAttributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DNS

DNS Service

On

Off

Resource Records

Name

Type

A Record

Address

Add

Save

Remove

No.	Name	Type	Detail
0	suryakiran	A Record	192.168.1.4

DNS Cache

Top

Server0

PhysicalConfigServicesDesktopProgrammingAttributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

File Name: index.html

<html>

SURYAKIRAN SANTHOSH

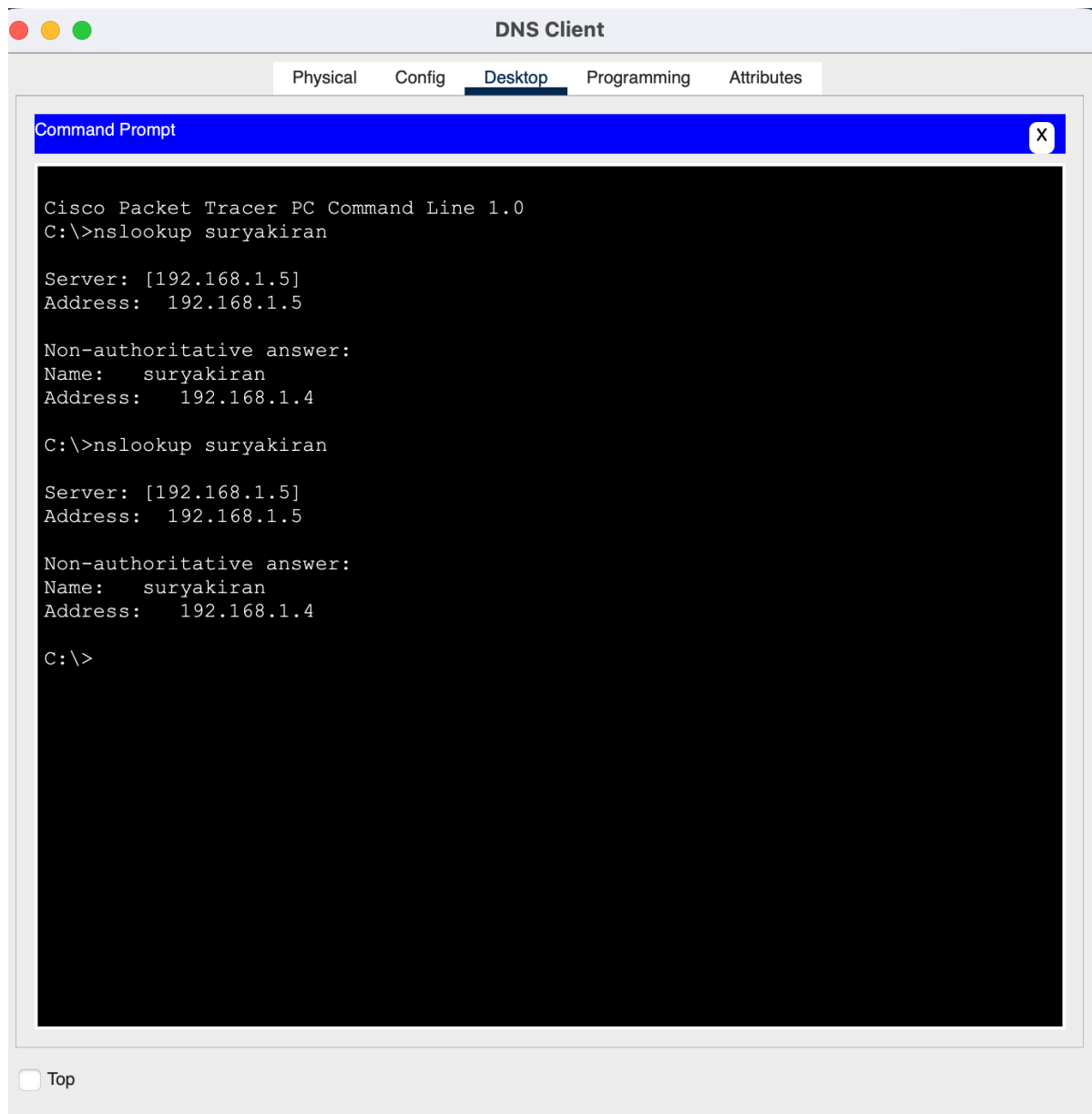
2403727710421277

II CSE D

</html>

File ManagerSave

☐ Top



FTP SERVICES:

Server0

PhysicalConfig[Services]DesktopProgrammingAttributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

FTP

Service

On

Off

User Setup

Username

Password

Write

Read

Delete

Rename

List

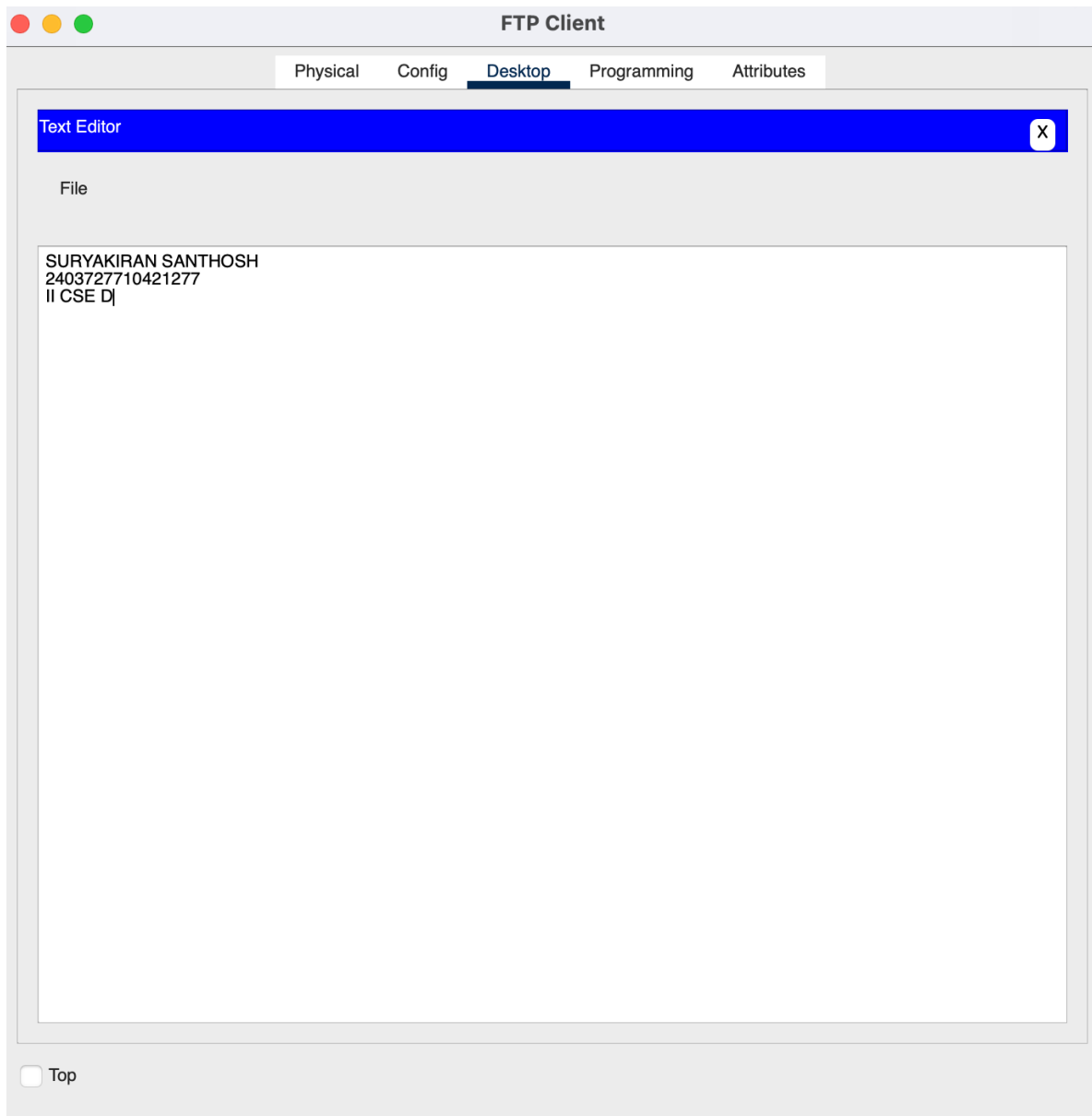
	Username	Password	Permission
1	cisco	cisco	RWDNL
2	suryakiran	2011	RWDNL

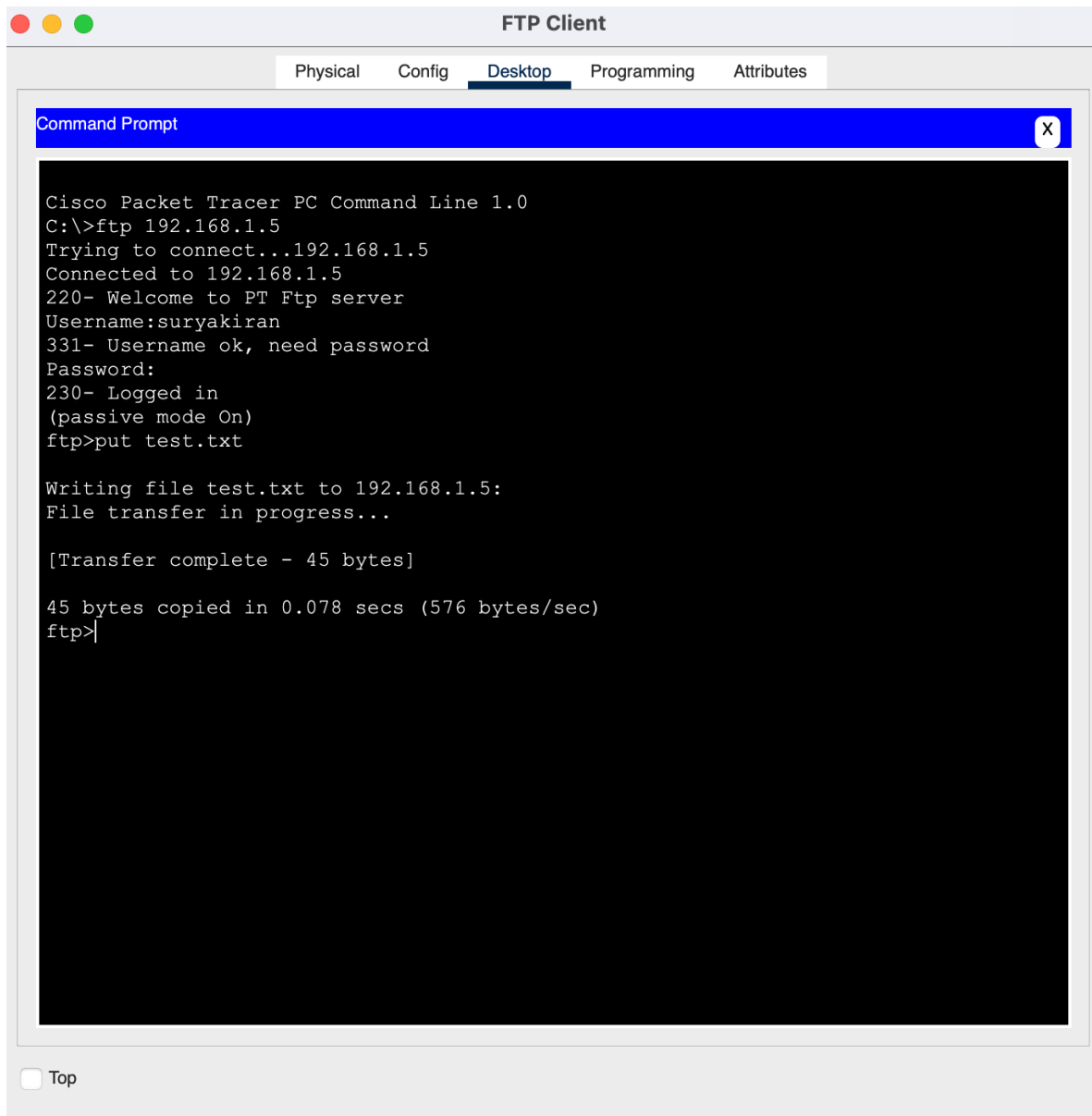
Add

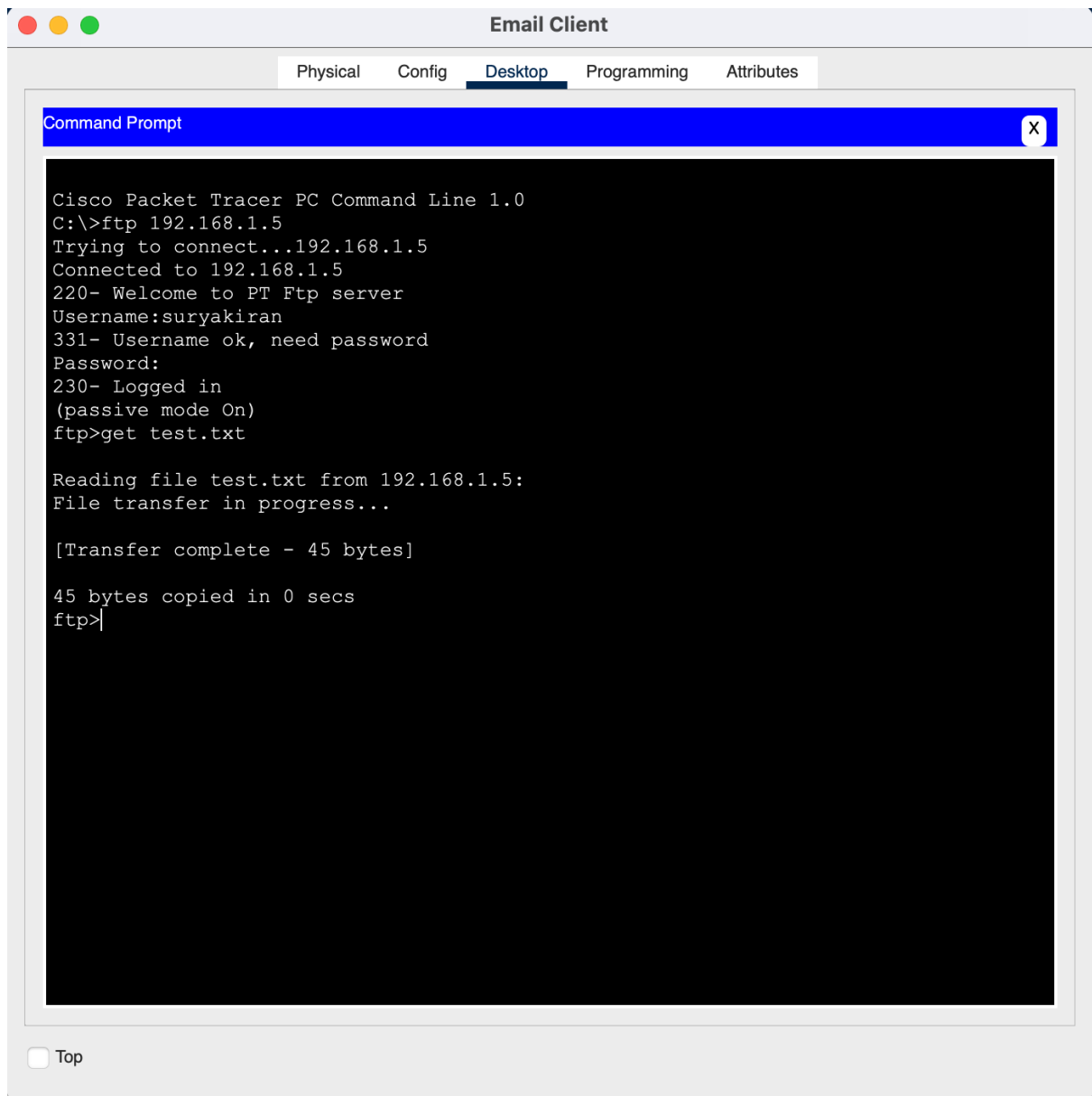
Save

Remove

	File
1	asa842-k8.bin
2	asa923-k8.bin
3	c1841-advipservicesk9-mz.124-15.T1.bin
4	c1841-ipbase-mz.123-14.T7.bin
5	c1841-ipbasek9-mz.124-12.bin
6	c1900-universalk9-mz.SPA.155-3.M4a.bin







HTTP SERVICES:

Server0

PhysicalConfig**Services**DesktopProgrammingAttributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

File Name: index.html

```
<html>
SURYAKIRAN SANTHOSH
2403727710421277
II CSE D
</html>
```

File ManagerSave

☐ Top

Server0

PhysicalConfigServicesDesktopProgrammingAttributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DNS

DNS Service

On

Off

Resource Records

Name

Type

A Record

Address

Add

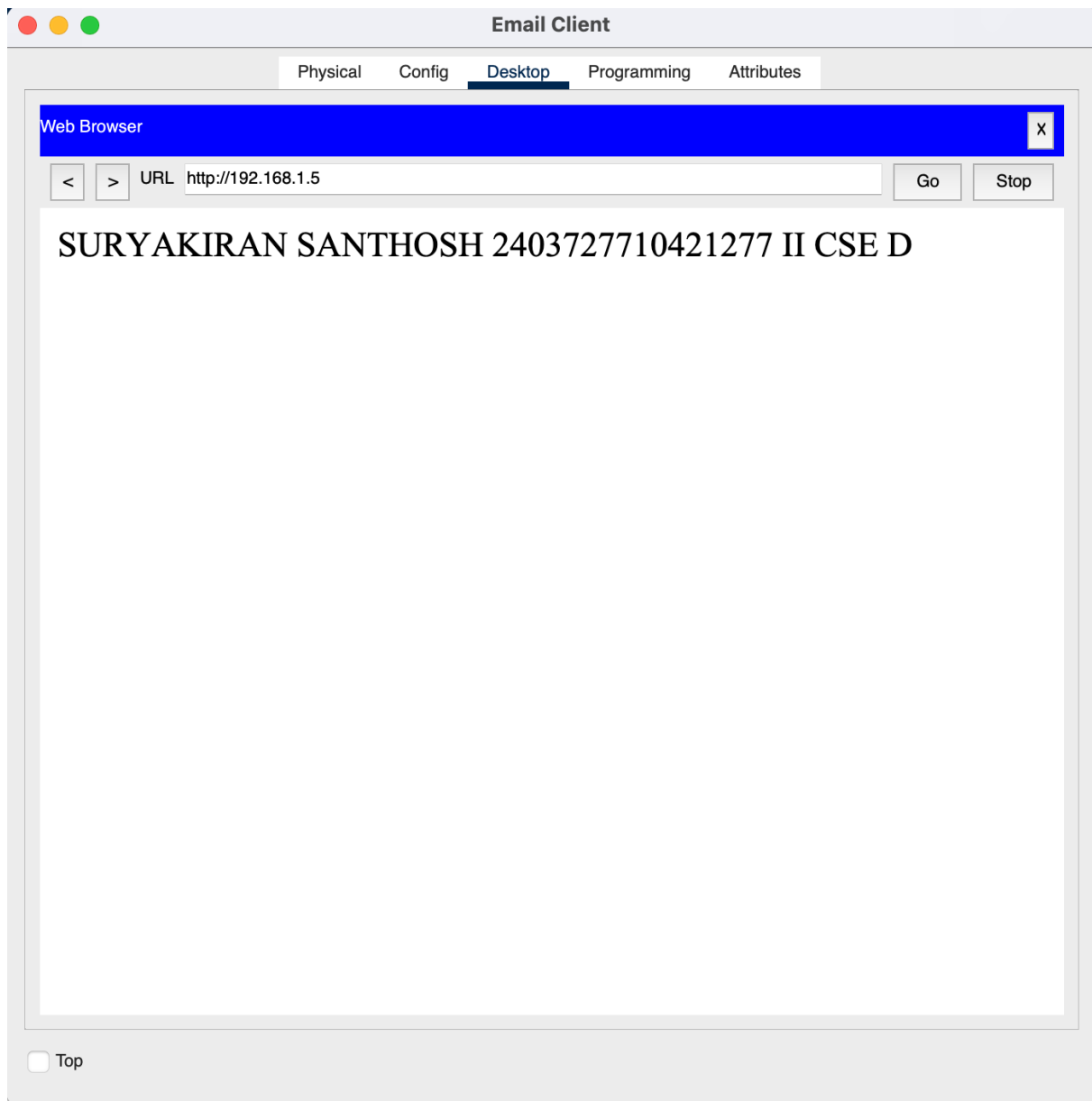
Save

Remove

No.	Name	Type	Detail
0	sandhranayana	A Record	192.168.1.5
1	suryakiran	A Record	192.168.1.4

DNS Cache

Top



RESULT

A multiserver (DNS,WEB,FTP) was created successfully and was used to analyse the TCP and UDP performance using packet tracer.