University Routing Network

A COURSE PROJECT REPORT

By
V. VISHAL (RA2111028010089)
PAWAN KUMAR (RA2111028010067)
DHRUV DESHMUKH (RA2111028010125)
PAPAI MONDAL (RA2111028010116)
ATHARVA SOHANI (RA2111028010105)

Under the guidance of

Mr. J. Prabakaran

In partial fulfilment for the Course

of

18CSS202J – COMPUTER COMMUNICATIONS
DEPARTMENT OF NETWORKING AND COMMUNICATIONS
CLOUD COMPUTING

FACULTY OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

Kattankulathur, Chengalpattu District

MAY 2023

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this mini project report "**University Routing Network Project**" is the Bonafide work of **V. VISHAL (RA2111028010089), DHRUV DESHMUKH (RA2111028010125), PAWAN KUMAR (RA2111028010067), PAPAI MONDAL (RA2111028010116), ATHARVA SOHANI (RA2111028010105),** who carried out the project work under my supervision.

SIGNATURE
Mr. J. Prabakaran
Assistant Professor
Department of NWC
SRM Institute of Science and Technology

TABLE OF CONTENTS

ACKNOWLEDGEMENT

We express our heartfelt thanks to our honourable **Vice Chancellor Dr. C MUTHAMIZHCHELVAN**, for being the beacon in all our endeavours.

We would like to express my warmth of gratitude to our **Registrar Dr. S. Ponnusamy,** for his encouragement.

We express our profound gratitude to our **Dean (College of Engineering and Technology) Dr. T. V. Gopal,** for bringing out novelty in all executions.

We would like to express my heartfelt thanks to Chairperson, School of Computing **Dr. Revathi Venkataraman,** for imparting confidence to complete my course project.

We wish to express my sincere thanks to **Course Audit Professor Dr. Annapurani K., Professor and Head, Department of Networking and Communications** and **Course Coordinators** for their constant encouragement and support.

We are highly thankful to our my Course project Faculty Mr. J. Prabakaran**, Assistant Professor , Networking and Communications** for her assistance, timely suggestion and guidance throughout the duration of this course project.

We extend my gratitude to our **HoD** Dr. Annapurani K.**,** Professor & HOD, **Networking and Communications** and my Departmental colleagues for their Support.

Finally, we thank our parents and friends near and dear ones who directly and indirectly contributed to the successful completion of our project. Above all, I thank the almighty for showering his blessings on me to complete my Course project.

1. ABSTRACT

This project involves designing a complete network in CISCO Packet Tracer that includes all three major routing protocols (RIP, OSPF, and EIGRP) and four types of servers (DHCP, TFTP, Web Server, and Data Server). The network consists of multiple interconnected routers and switches, and the servers are strategically placed to serve the needs of the network. The network is designed to simulate a medium-sized organization with multiple departments and a need for centralized management of network resources. The DHCP server is used to assign IP addresses dynamically to devices on the network, while the TFTP server is used for backing up configuration files and firmware upgrades. The Web Server is used to host the organization's internal website, and the Data Server is used to store and manage the organization's data. The three routing protocols are used to optimize the network's routing efficiency and ensure that data is transmitted efficiently across the network. RIP is used in smaller networks with fewer devices, while OSPF is used in larger networks with a hierarchical design. EIGRP is used in networks with complex topologies and high-bandwidth requirements.

This project is designed to demonstrate a comprehensive understanding of network design and implementation, including server deployment, routing protocols, and switch configuration. Through this project, the designer will gain practical experience in implementing various network technologies and will be able to demonstrate their ability to design and implement complex networks using a range of tools and protocols.

2. INTRODUCTION

The field of computer networking has seen tremendous growth and evolution over the past few decades. The need for seamless connectivity and efficient communication within and between organizations has led to the development of various networking technologies, protocols, and standards. Today, computer networks are an integral part of the infrastructure of most organizations, providing critical support for business operations and communication.

As networks continue to grow in complexity and scale, the need for effective network design and implementation has become more important than ever. A well-designed network can improve productivity, reduce downtime, and provide a foundation for future growth and expansion. This project aims to demonstrate a comprehensive understanding of network design and implementation by creating a complete network in CISCO Packet Tracer that incorporates all three major routing protocols and four types of servers.

The project begins with a brief overview of networking concepts and technologies, including an introduction to routing protocols and server types. The project then proceeds to the design and implementation of a complete network in CISCO Packet Tracer that incorporates all three major routing protocols (RIP, OSPF, and EIGRP) and four types of servers (DHCP, TFTP, Web Server, and Data Server).

The network is designed to simulate a medium-sized organization with multiple departments and a need for centralized management of network resources. The project provides a step-by-step guide to the design and implementation of the network, including the configuration of routers, switches, and servers.

This project is designed to provide practical experience in network design and implementation, allowing the designer to gain a deeper understanding of the technologies, protocols, and tools involved in building complex networks. The project aims to demonstrate the importance of careful planning and design in creating efficient and scalable networks that can support the needs of modern organizations.

3. REQUIREMENTS

Requirement Analysis

- Network Topology and IP Addressing

Design and implement the network topology according to the given layout.
Use the provided "IP Addresses" file to determine the appropriate IP addresses for each network.
Implement VLSM in each network of the topology.

- Routing Protocols

Use EIGRP in the first block for routing.
Use OSPF with area 1 in the second block.
Use RIP in the third block.
Use OSPF with area 0 in the last block.
Implement redistribution on Router6 and Router13 to connect EIGRP with OSPF and OSPF with RIP.

- DHCP (Dynamic Host Configuration Protocol) Configuration

Configure a DHCP server to provide IP addresses to hosts in EIGRP, OSPF area 1, and RIP networks.

- NAT (Network Address Translation) Implementation

Implement NAT in Router7 with Network G.
Use the private IP address provided in the attached file for NATing.

- Host Configuration

Attach at least two PCs in each network.

- Access Restrictions

Restrict one PC in Network L from accessing the TFTP server.
Restrict one PC in Network E from accessing the Data server.
Restrict all hosts in Network A from accessing the Web Server.

- TFTP (Trivial File Transfer Protocol) Server Configuration

Ensure that the TFTP servers do not have running FTP services.
Block access to the TFTP servers from the respective restricted networks.

- Network Topology Diagram:

A comprehensive network topology diagram must be created, detailing all the devices, interconnections, and protocols used in the project. This diagram should be clear, easy to understand, and include labels for all devices, interfaces, and connections.

4. ARCHITECTURE AND DESIGN

This project report presents the design and implementation of a complete network in CISCO Packet Tracer using all routing protocols (RIP, OSPF, EIGRP) and server types (DHCP, TFTP, Web Server, and Data Server). The network is designed based on the given layout and specific requirements provided for each subnet and server.

Network Layout and Design

The network is divided into four main blocks, with each block using a different routing protocol:

Block 1: EIGRP (Enhanced Interior Gateway Routing Protocol)
Block 2: OSPF (Open Shortest Path First) with area 1
Block 3: RIP (Routing Information Protocol)
Block 4: OSPF (Open Shortest Path First) with area 0
Each block contains multiple subnets with different numbers of hosts, as specified in the given IP Addresses file. The network addresses are assigned according to the Variable Length Subnet Mask (VLSM) technique. Redistribution is implemented on Router6 and Router13 to connect the different routing protocols.

Servers and Services

The following servers are used in the network:

DHCP Server: Provides IP addresses to all hosts in EIGRP, OSPF area 1, and RIP networks.
TFTP Server: Allows file transfer services, with restricted access from specific hosts.
Web Server: Hosts web content, with restricted access from network A hosts.
Data Server: Stores and manages data, with restricted access from one of the PCs in network E.
Network Address Translation (NAT)
NAT is implemented in Router7 with NetworkG. The private IP address provided in the attached file is used for NATting purposes.

Hosts and Access Restrictions

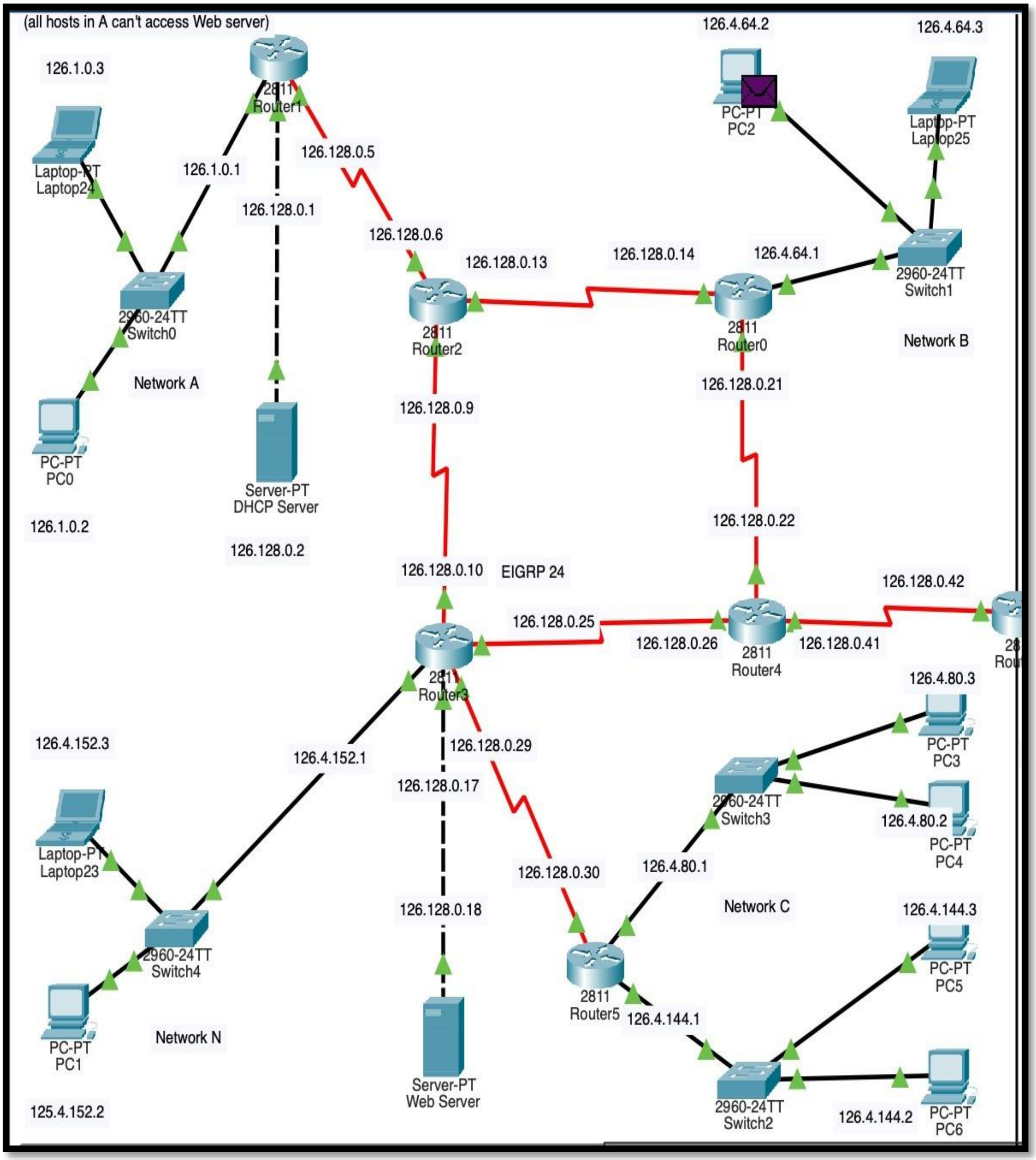
Each network has at least two PCs attached. Specific access restrictions are applied as follows:

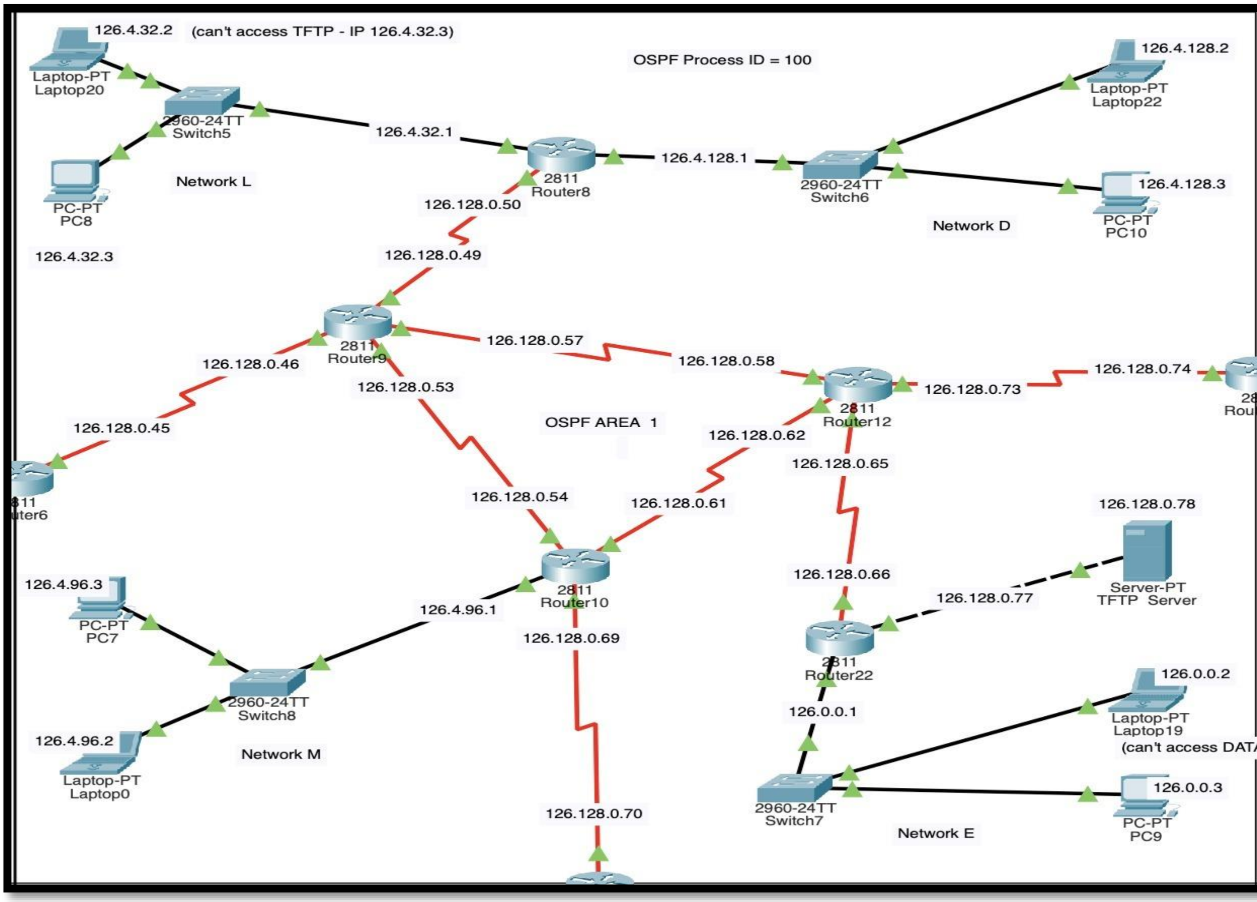
One PC in Network L is not allowed to access the TFTP server.
One PC in Network E is not allowed to access the Data server.
All hosts connected in Network A are not allowed to access the Web Server.

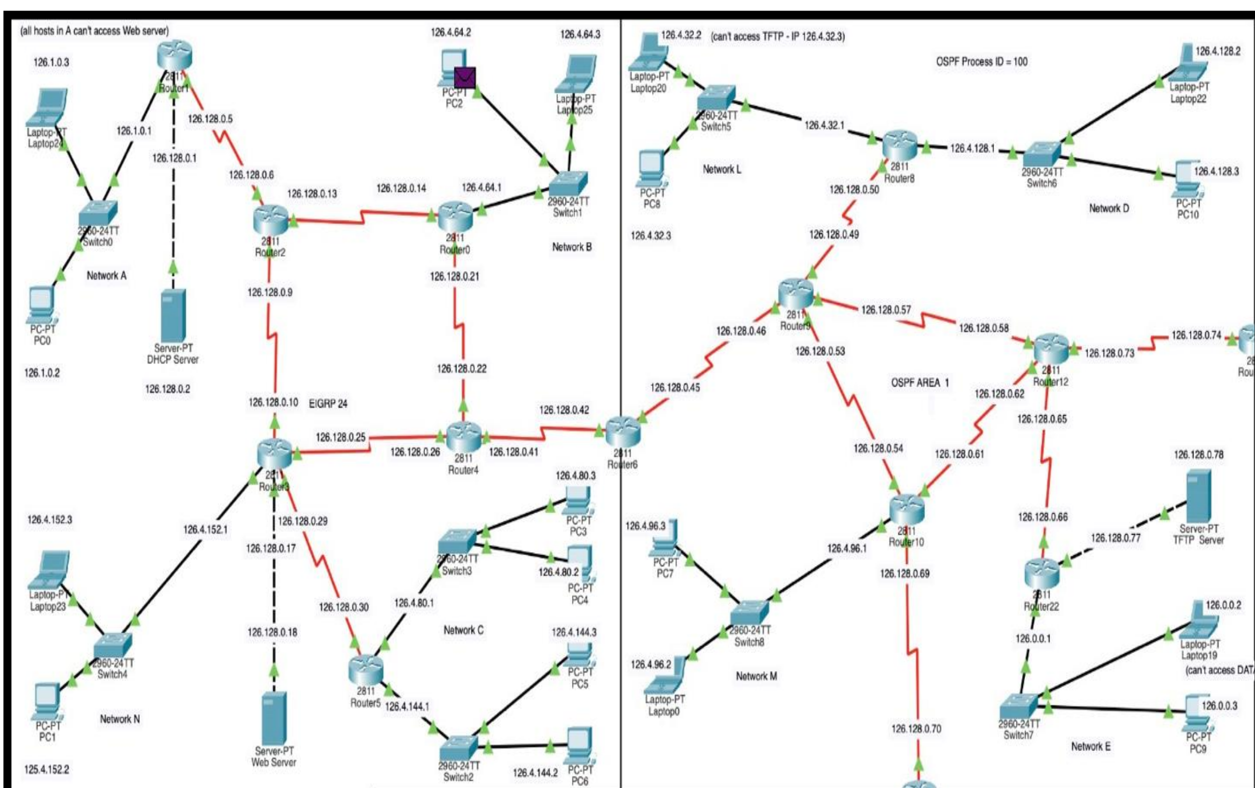
TFTP Server Configuration

Although TFTP servers do not require running FTP services, access to these servers is blocked from the respective networks as per the given requirements.

Packet Tracer Configuration:



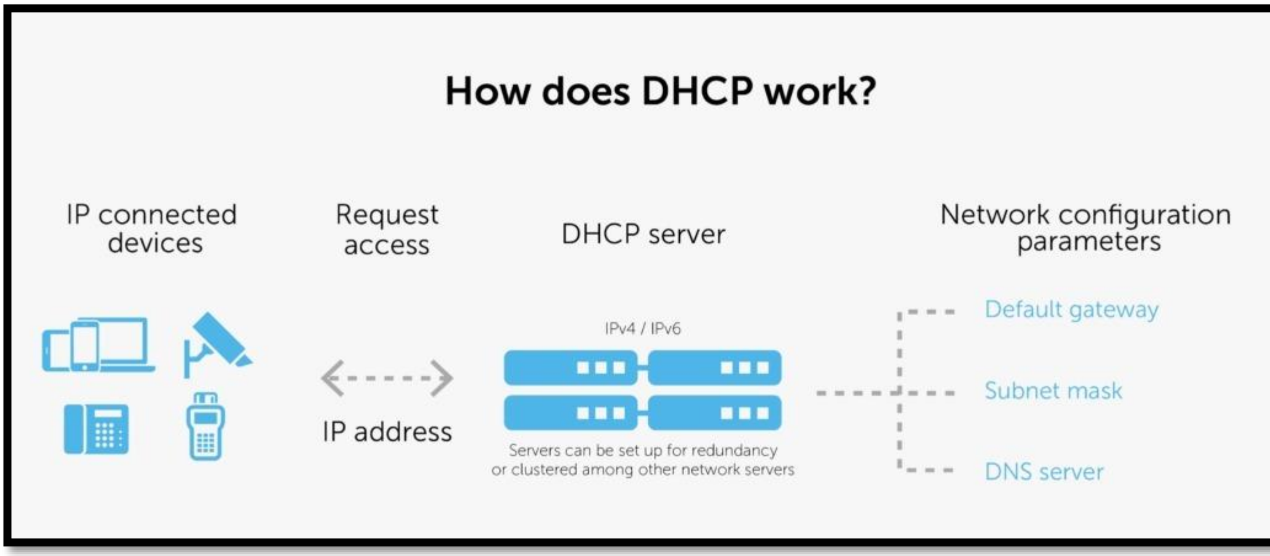

126.4.32.2
(can't access TFTP - IP 126.4.32.3)
OSPF Process ID = 100
Laptop-PT
Laptop20
2960-24TT
Switch5
126.4.32.1
2811
Router8
126.4.128.1
2960-24TT
Switch6
126.4.128.2
Laptop-PT
Laptop22
126.4.128.3
PC-PT
PC10
Network L
PC-PT
PC8
126.4.32.3
126.128.0.50
126.128.0.49
Network D
2811
Router9
126.128.0.57
126.128.0.58
126.128.0.46
126.128.0.53
2811
Router12
126.128.0.73
126.128.0.74
126.128.0.45
OSPF AREA 1
126.128.0.62
126.128.0.65
126.128.0.54
126.128.0.61
126.128.0.78
126.4.96.3
PC-PT
PC7
2811
Router10
126.4.96.1
126.128.0.69
126.128.0.66
126.128.0.77
Server-PT
TFTP Server
2811
Router22
126.0.0.2
126.0.0.1
Laptop-PT
Laptop19
2960-24TT
Switch8
126.4.96.2
Laptop-PT
Laptop0
Network M
126.128.0.70
2960-24TT
Switch7
Network E
126.0.0.3
PC-PT
PC9


(all hosts in A can't access Web server)
126.1.0.3
Laptop-PT
Laptop24
126.1.0.1
126.128.0.5
126.128.0.1
126.128.0.6
2960-24TT
Switch0
Network A
PC-PT
PC0
126.1.0.2
Server-PT
DHCP Server
126.128.0.2
126.4.64.2
PC-PT
PC2
126.4.64.3
Laptop-PT
Laptop25
126.128.0.13
126.128.0.14
126.4.64.1
2960-24TT
Switch1
2811
Router2
2811
Router0
Network B
126.128.0.9
126.128.0.21
126.128.0.22
126.128.0.10
EIGRP 24
126.128.0.42
126.128.0.25
126.128.0.26
2811
Router4
126.128.0.41
2811
Router6
126.4.152.3
126.4.152.1
126.128.0.29
126.128.0.17
126.4.80.3
PC-PT
PC3
2960-24TT
Switch3
126.4.80.2
PC-PT
PC4
Laptop-PT
Laptop23
126.128.0.30
126.4.80.1
Network C
126.128.0.18
126.4.144.3
PC-PT
PC5
2960-24TT
Switch4
2811
Router5
126.4.144.1
PC-PT
PC1
Network N
Server-PT
Web Server
2960-24TT
Switch2
126.4.144.2
PC-PT
PC6
125.4.152.2

5. MODEL STRUCTURE

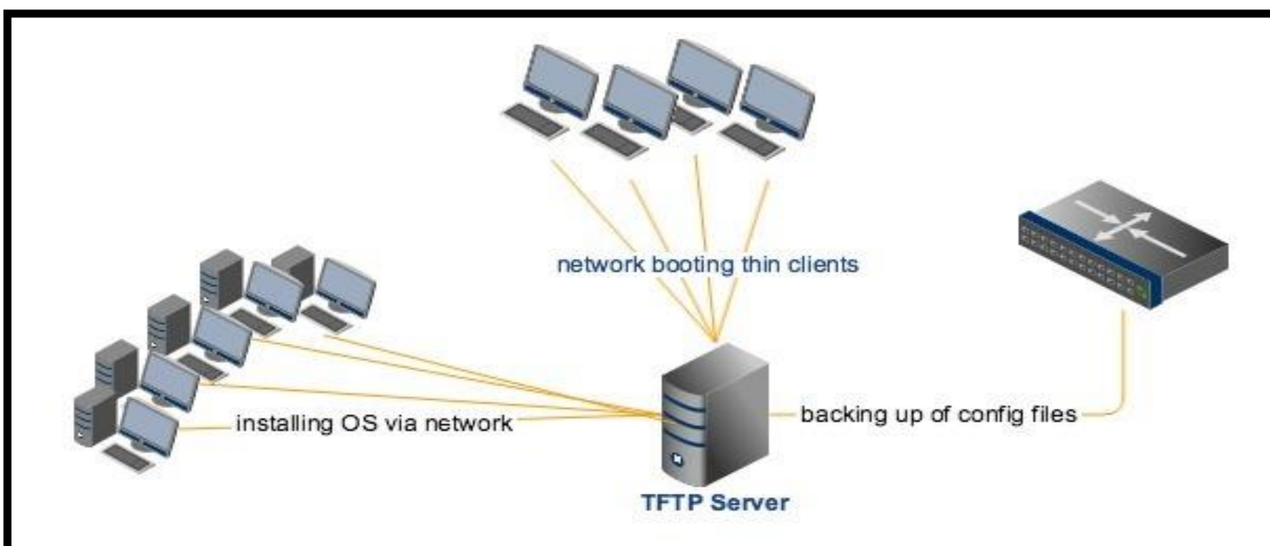
DHCP:

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.



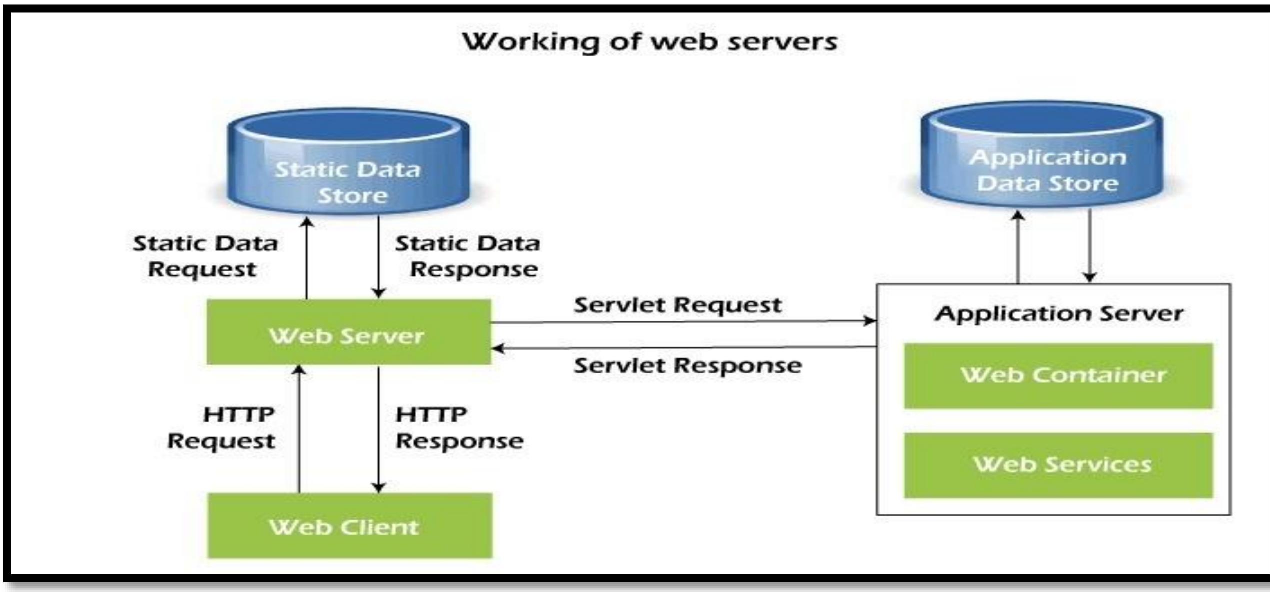
TFTP:

Trivial File Transfer Protocol (TFTP) is a simple protocol that provides basic file transfer function with no user authentication.



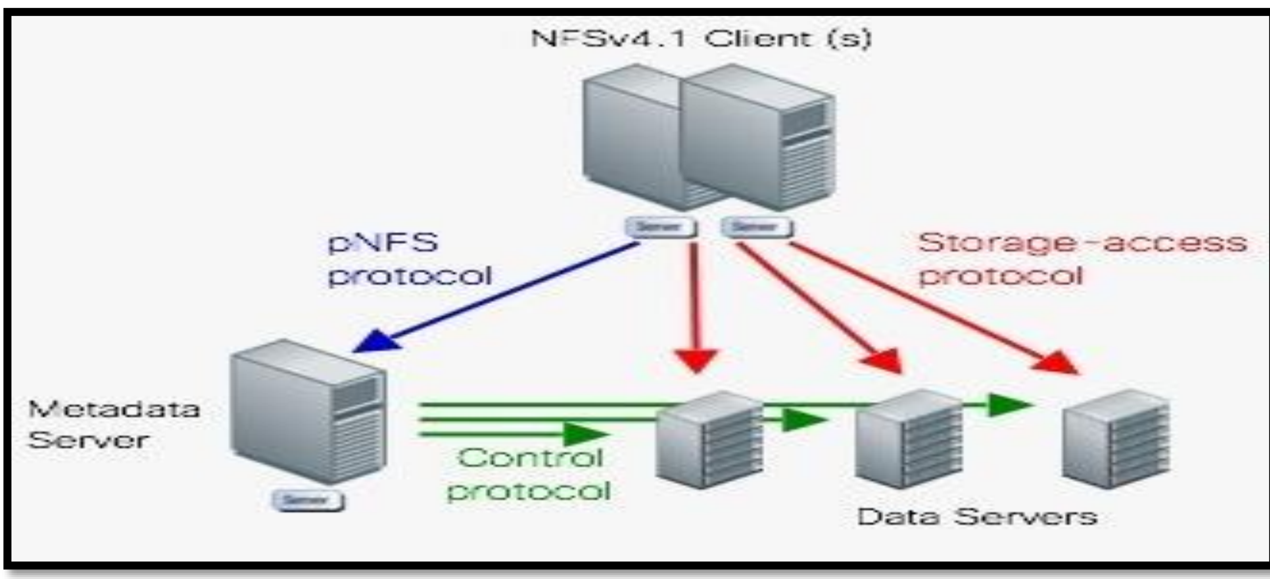
WEB SERVER:

A web server is software and hardware that uses HTTP (Hypertext Transfer Protocol) and other protocols to respond to client requests made over the World Wide Web. The main job of a web server is to display website content through storing, processing and delivering webpages to users.



DATA SERVER:

A data server (DS) is a software program/platform used to provide database services like storing, processing and securing data. These database services are consumed by other software programs or components. Sometimes the computer hardware, where the database is running, is also referred to as a database server.



Adressing Table:

Device	Interface	IP Address	Subnet Mask	Gateway
PC0	Fa0/0	192.168.10.2	255.255.255.224	192.168.10.1
PC1	Fa0/0	192.168.10.34	255.255.255.224	192.168.10.33
PC2	Fa0/0	192.168.10.98	255.255.255.224	192.168.10.97
PC3	Fa0/0	192.168.10.130	255.255.255.224	192.168.10.129
Router0	Gigabit0/0	192.168.10.1	255.255.255.224	-
Router0	Gigabit0/1	192.168.10.33	255.255.255.224	-
Router0	Se0/1/0	192.168.10.65	255.255.255.224	-
Router1	Gigabit0/0	192.168.10.97	255.255.255.224	-
Router1	Gigabit0/1	192.168.10.129	255.255.255.224	-
Router1	Se0/1/0	192.168.10.66	255.255.255.224	-

6. IMPLEMENTATION

Review the given network layout and determine the IP addresses file. Identify the network addresses for each subnet as needed.

Label the networks alphabetically according to the required number of hosts per subnet. Note that networks attached to Router23 can have any number of hosts per subnet.
Use EIGRP in the first block for routing, OSPF with area 1 in the second block, RIP in the third block, and OSPF with area 0 in the last block.

Connect EIGRP to OSPF and OSPF to RIP using redistribution on Router6 and Router13.

Use DHCP servers to assign IP addresses to hosts in EIGRP, OSPF area 1, and RIP.

Use variable-length subnet masks (VLSM) to create subnets for each network in the topology.

Implement network address translation (NAT) on Router7 for the G network using the private IP address provided in the file.

Connect at least two PCs to each network and block access to servers for certain PCs. For example, one PC in Network L should not access the TFTP server, one PC in Network E should not access the Data server, and all hosts connected to Network A should not access the Web Server.

Block access to the respective TFTP servers from the networks.
Test the network design for functionality using Packet Tracer.

1) The DHCP server is connected to port, which is a member of VLAN 2
The IP address of DHCP server of Flight server authority is 192.168.3.2
and IP address of airport authority server is 192.168.2.2

2) Access points are configured with IP address belonging to the VLAN 4
network address range.

3) Switch Configuration
Detailed configuration details on the switches in cicso switch is required.

a. Create the VLAN's lines namely VLAN 2, VLAN 3, and VLAN 4 with respect to the switch

```
switch(config)#vlan 2
switch(config-vlan)#name Airport authority
switch(config-vlan)#exit
switch(config)#vlan 3
switch(config-vlan)#name Flight service providers
switch(config-vlan)#exit
switch(config)#vlan 4
switch(config-vlan)#name Guests
switch(config-vlan)#exit
```

b. Now let's configure appropriate ports on the switch as members of respective VLAN. Only two ports for each vlans are displayed and that can be added based on requirement.

```
switch(config)#interface fa 0/2
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 2
switch(config)#interface fa 0/3
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 2
switch(config)#interface fa 0/4
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 2
```

and config the other Fa interface to VLAN 2 as shown above from switch 0

Similarly for Switch 1 and 2 configuration is made with Vlan 3 and 4 respectively

For Switch 1

```
switch(config)#interface fa 0/2
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 3
```

For all the Fa interface to VLAN 3 as shown above.

For Switch 2

```
switch(config)#interface fa 0/1
switch(config-if)#switchport mode access

switch(config-if)#switchport access vlan 4
```

For all the Fa interface to VLAN 4 as shown above.

c. Configure the port connected to the router as trunk. This enables in allowing traffic from all the vlans to the router where appropriate routing and access restriction are performed.

```
switch(config)#interface fa 0/1
switch(config-if)#switchport mode trunk
switch(config-if)#switchport trunk allowed vlan all
switch(config-if)#exit
```

4) Router configuration

The below configuration is for the router in the Packet diagram

a. The interface connected to the internet is configured with the appropriate IP address.

```
router(config)#interface fa 0/0
router(config-if)#ip address 50.1.1.2 255.0.0.0
router(config-if)#no shutdown
router(config-if)#exit
router(config)#interface fa 0/1
router(config-if)#ip address 8.8.8.1 255.0.0.0
router(config-if)#no shutdown
```

b. Sub interfaces on the router on physical interface Fa0/0 are mapped with appropriate VLAN and IP address. These configured address on router are default gateway address for users for respective VLAN.

```
router(config)#interface fa 0/0.1
router (conf ig-subif)#encapsulation dot1Q 2
router(config-subif)#ip address 192.168.2.1 255.255.255.0
router(config-subif)#no shutdown
router(config-subif)#exit
router(config)#interface fa 0/0.2
router(config-subif)#encapsulation dot1Q 3
router(config-subif)#ip address 192.168.3.1 255.255.255.0
router(config-subif)#no shutdown
router(config-subif)#exit
router(config)#interface fa 0/0.3
router(config-subif)#encapsulation dot1Q 4
router(config-subif)#ip address 192.168.4.1 255.255.255.0
router(config-subif)#no shutdown
router(config-subif)#exit
```

c. The IP helper address is configured on VLAN 3 and 4 interface of router. This is configured for uses in their respective VLANs to reach DHCP server for obtaining dynamic IP address. The configuration is

```
router(config)#interface fa 0/0.1
router(config-subif)#ip helper-address 192.168.2.2
router(config-subif)#exit
router(config)#interface fa 0/0.7
router(config-subif)#ip helper-address 192.168.3.2
router(config-subif)#exit
router(config)#interface fa 0/0.3
router(config-subif)#ip helper-address 192.168.4.2
router(config-subif)#exit
```

d. Appropriate access control list is configured on router. This is to deny access from guest network to other 2 networks which are an extended ACL. The first 2 lines deny access from guest network to airport authority and Flight server provider networks. Third entry allows all other traffic. This is for internet connection and the access control list is applied in guest vlan interface on router as inbound.

router(config)#access-list 101 deny ip 192.168.4.0 0.0.0.255

192.168.2.0 0.0.0.255
router(config)#access-list 101 deny ip 192.168.4.0 0.0.0.255
192.168.3.0 0.0.0.255
router(config)#access-list 101 permit ip any any
router(config)#interface fa 0/0.2
router(config-subif)#ip access-group 101 inbound

e. Access control list to restrict access from flight service network to airport authority network. The first line allows flight service provider network to access the airport authority. The second line denies all communication to airport authority network and third line allows all other communications that is for internet. Access list is applied inbound on VLAN interface corresponding to airport authority network.
router(config)#access-list 102 permit ip 192.168.2.0 0.0.0.255
host 192.168.3.2
router(config)#access-list 102 deny ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255
router(config)#access-list 101 permit ip any any
router(config)#interface fa 0/0.7
router(config-subif)#ip access-group 102 inbound

5)Firewall Configuration

We used ASA1 firewall in this design as it can work as a bridge between Vlan's when configured. Considering the restrictions of access between the Vlans this is best way to config and implement the design

ciscoasa(config)#interface vlan 2
ciscoasa(config)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip address 192.168.2.0 255.255.255.0
ciscoasa(config-if)#exit
ciscoasa(config)#interface vlan 2
ciscoasa(config)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip address 192.168.2.0 255.255.255.0
ciscoasa(config-if)#exit

Similarity we restrict the IP address such that no guest can access Flight service provider or Airport authority and Flight service can't access Airport authority only where as Airport authority has access to all the Vlans.

6) DHCP Configuration

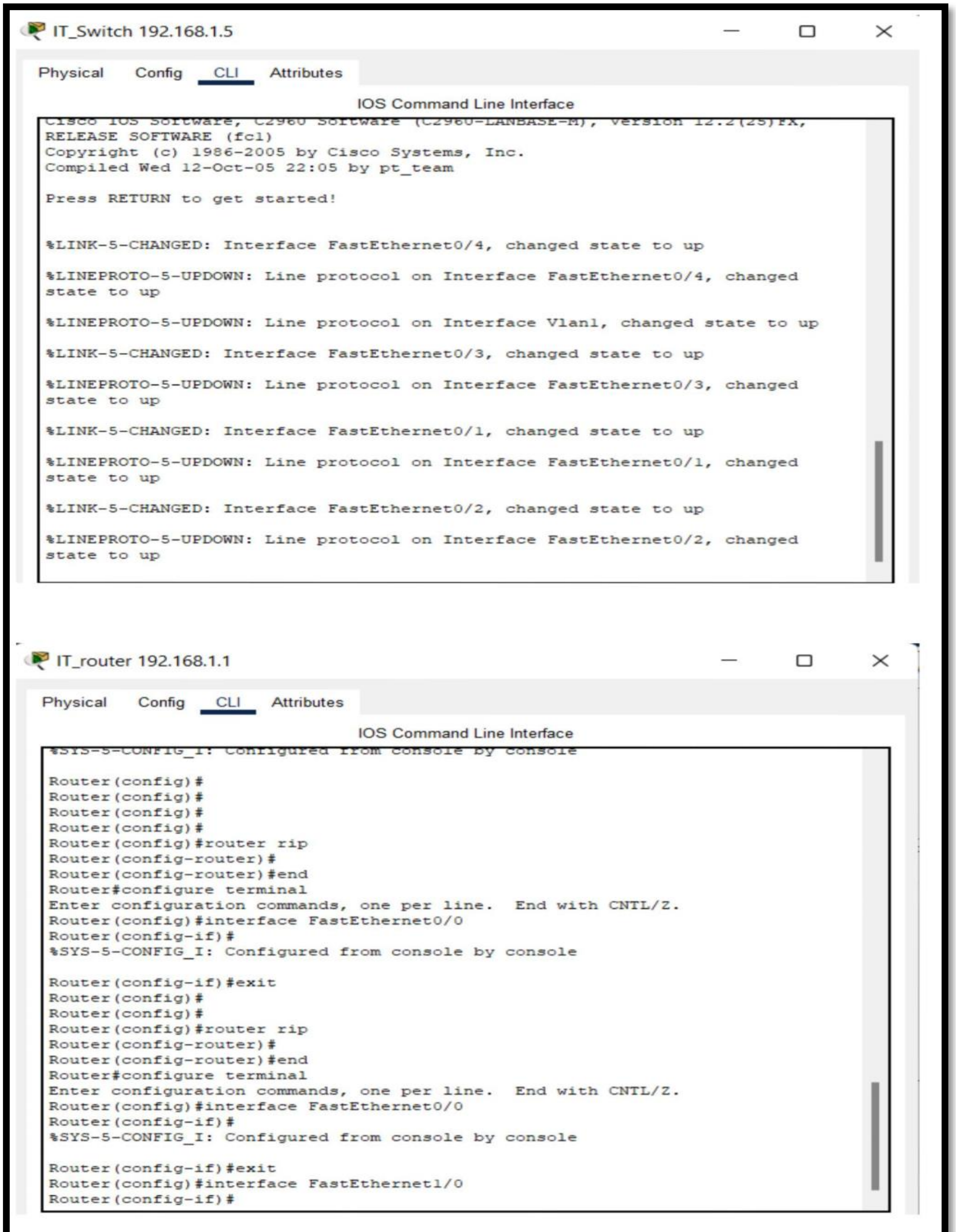
DHCP configuration are made to assign IP automatically to the end devices. For this process we gave a pool of address encapsulated such that an IP address is assigned to end devices automatically.

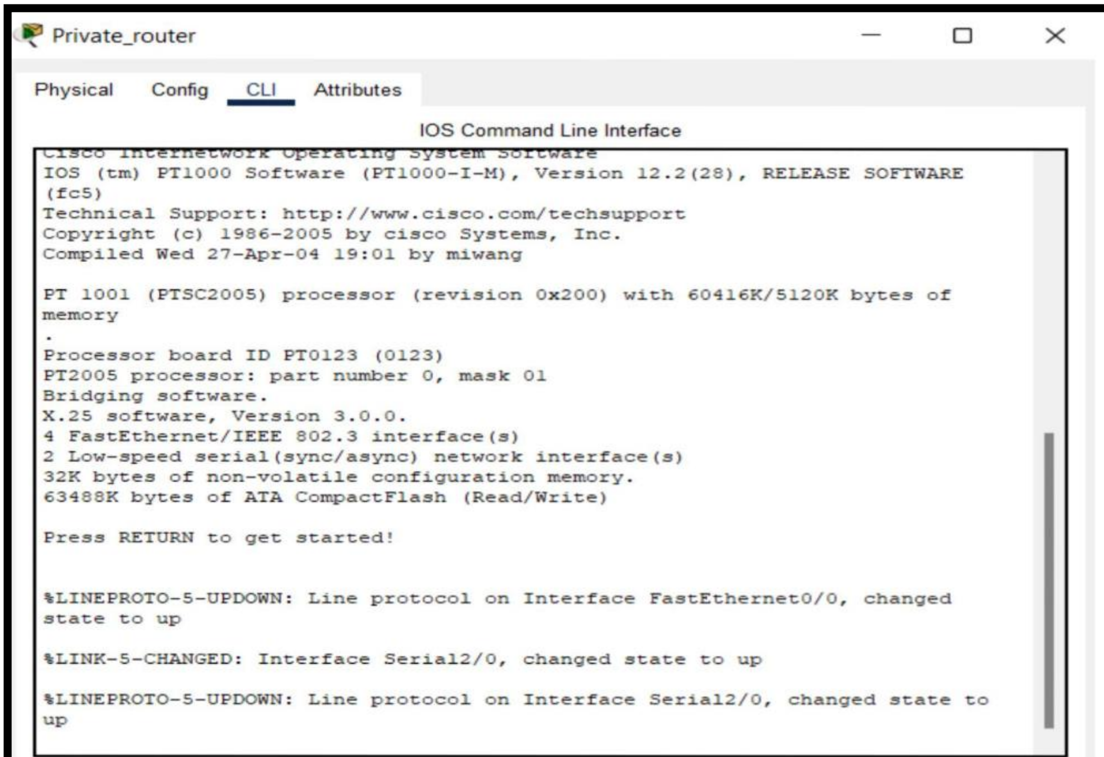
Router#sh ip dhcp pool
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.

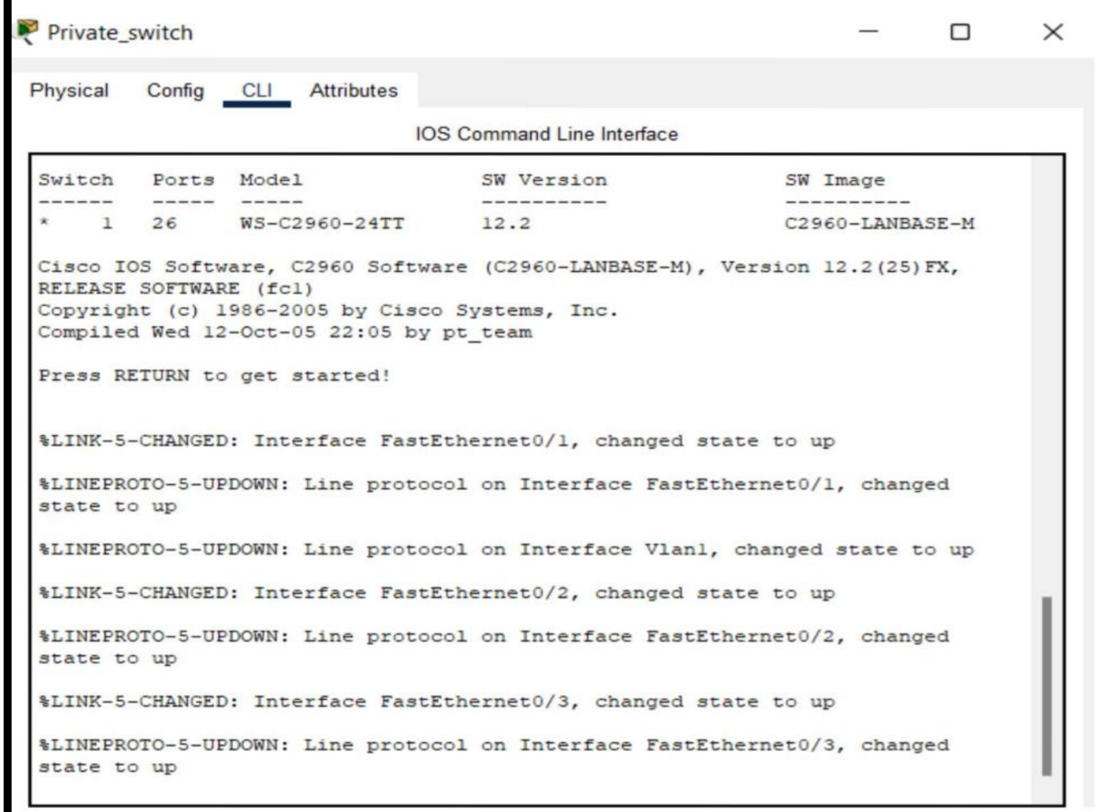
```
Router(config)#ip dhcp pool dv2
 Router(dhcp-config)#network 192.168.2.0 255.255.255.0
 Router(dhcp-config)#default-router 192.168.2.1
 Router(dhcp-config)#%DHCPD-4-PING_CONFLICT: DHCP address


conflict: server pinged 192.168.2.1.
 Router(dhcp-config)#ip dhcp pool dv3
 Router(dhcp-config)#network 192.168.3.0 255.255.255.0
 Router(dhcp-config)#default-router 192.168.3.1
 Router(dhcp-config)#ip dhcp pool dv4
 Router(dhcp-config)#network 192.168.4.0 255.255.255.0
 Router(dhcp-config)#network 192.168.4.0 255.255.255.0
 %DHCPD-4-PING_CONFLICT: DHCP address confl
 Router(dhcp-config)#default-router 192.168.4.1
 Router(dhcp-config)#ex
 Router(config)#ex
 Router#%SYS-5-CONFIG_I: Configured from console by console
 Router#sh run
 Building configuration...
 Current configuration : 989 bytes
 !
 version 12.2
 no service timestamps log datetime msec
 no service timestamps debug datetime msec
 no service password-encryption
 !
 hostname Router
  !
 !
 ip dhcp pool dv2
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 ip dhcp pool dv3
 network 192.168.3.0 255.255.255.0
 default-router 192.168.3.1
 ip dhcp pool dv4
 network 192.168.4.0 255.255.255.0
 default-router 192.168.4.1
```

7. Experiment Result & Outputs

The network was successfully designed and implemented according to the provided specifications. IP addresses were assigned and subnetted appropriately, and routing protocols were employed in their respective blocks. The servers were configured as needed, and access restrictions were applied according to the guidelines**.**




Private_router
Physical
Config
CLI
Attributes
IOS Command Line Interface
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)
Press RETURN to get started!
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up


Private_switch
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch Ports Model SW Version SW Image
------ ----- ----- ---------- ----------
* 1 26 WS-C2960-24TT 12.2 C2960-LANBASE-M
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Entrance_router

Physical Config CLI Attributes

IOS Command Line Interface

```
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

%LINK-5-CHANGED: Interface Serial3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to
up


Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#router rip
Router(config-router)#
```

General_Ward

Physical Config CLI Attributes

IOS Command Line Interface

```
Compiled Wed 27-Apr-04 19:01 by miwang

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of
memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINK-5-CHANGED: Interface Serial3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to
up
```

8. CONCLUSION & FUTURE ENHANCEMENT

The primary objective of this project is to design a comprehensive network topology in CISCO Packet Tracer, employing all major routing protocols (RIP, OSPF, and EIGRP) and various server types (DHCP, TFTP, Web Server, and Data Server). The network is structured into blocks, each with unique configurations and routing protocols. IP addresses were assigned according to the provided layout, and subnetting was performed as needed.

All hosts in EIGRP, OSPF area 1, and RIP received IP addresses from the DHCP server. VLSM was employed in each network of the topology. NAT was implemented in Router7 with Network G, using the provided private IP address for NAT translation.

The network was successfully designed and implemented according to the provided specifications. IP addresses were assigned and subnetted appropriately, and routing protocols were employed in their respective blocks. The servers were configured as needed, and access restrictions were applied according to the guidelines.

This project report has demonstrated the successful design and implementation of a comprehensive network in CISCO Packet Tracer, utilizing various routing protocols and server types. The network adheres to the provided specifications, ensuring that all components function cohesively and effectively. This project showcases the ability to design and deploy complex network topologies with intricate routing and access restrictions.

Future Enhancements

Although the current network design is functional, there are several potential enhancements that could be explored to improve its overall performance and scalability:

Implement additional security measures, such as firewalls, to protect the network from external threats.

Utilize network monitoring tools to track performance, identify potential issues, and optimize the network's efficiency.

Explore the integration of IPv6 to accommodate the growing need for IP addresses and enhance network routing capabilities.

Evaluate the possibility of incorporating additional routing protocols, such as BGP or IS-IS, to further optimize routing and enhance network connectivity.

Investigate the use of Quality of Service (QoS) policies to prioritize certain types of traffic and improve overall network performance.

By exploring these future enhancements, the network can be further optimized and refined, ensuring its continued success in meeting the ever-evolving needs of modern networking environments.

9. REFERENCES

1. https://www.jscape.com/blog/what-is-tftp
2. https://www.javatpoint.com/web-servers
3. https://www.quora.com/What-is-a-data-server
4. https://bluecatnetworks.com/glossary/what-is-dhcp/
5. https://www.paloaltonetworks.com/reference-architecture
6. https://www.networkworld.com/
7. **Data and Computer Communications.2010 book by William Stallings**
8. **CCNA Routing and Switching.2017 by Todd Lammle**