



Green University of Bangladesh

Department of Computer Science and Engineering (CSE)
Semester: (Fall, Year: 2022), B.Sc. in CSE (Day)

Controlling Network & Secure Access with Various Facilities in MAN

Course Title: Computer Networking Lab
Course Code: CSE 312
Section: D3

Name	ID
Md Badrul Nasim	201002189

Submission Date:
08-01-2023

Course Teacher's Name:
Mohammad Ehsan Shahmi Chowdhury

Contents

1	Introduction	2
1.1	Overview	2
1.2	Motivation	2
1.3	Problem Definition	2
1.3.1	Problem Statement	2
1.3.2	Complex Engineering Problem	2
1.4	Design Goals/Objectives	2
2	Design/Development/Implementation of the Project	3
2.1	Project Details	3
3	Performance Evaluation	21
3.1	Simulation Environment/ Simulation Procedure	21
3.2	Results Analysis/Testing	21
3.2.1	Complex Engineering Problem Discussion	24
4	Conclusion	25
4.1	Discussion	25
4.2	Limitations	25
4.3	Scope of Future Work	25

Chapter 1

1 Introduction

1.1 Overview

The purpose of the project was Controlling Network & Secure Access with Various Facilities in MAN. And we tried to do all necessary steps and implementation as per problem motivation. In this project we use some ideas and technologies that we have to learn first and then implement.

1.2 Motivation

We take the help of networks to facilitate our daily work and to communicate with each other. But data security, network access control, device control from remote locations are sometimes difficult. In addition, we are concerned about the possibility of limited services from connected within the same network. Also, since IPv4 is currently negligible. Therefore, we are also concerned about how we can form a large network using less IP within the same network so that IP is not wasted. And so on, network security & access control related issue.

1.3 Problem Definition

1.3.1 Problem Statement

Keeping these things in mind, we tried to make a big network system where these problems can be solved. We have tried some networks that cannot be accessed from the outside and not accessed from the inside. In addition, many security features like monitoring who is trying to access the network. We have maintained many more features and security.

We have ensured that how the external technician can come and fix the network problem. Tried to fix dynamic IP allocating, SMTP server, DNS server, Syslog server, NTP server, FTP server, HTTP server, Firewall, Router & Switch access list handle, Vlan setup, IP subnetting, Nat in networking and many more problems.

1.3.2 Complex Engineering Problem

Depth of analysis required	Here no obvious solution, and we did deep abstract thinking and analysis.
Familiarity of issues	Extend beyond our previous lab class experience by applying academic & other source based approaches.
Interdependence	Since we have high level problems including many component and sub network problem

1.4 Design Goals/Objectives

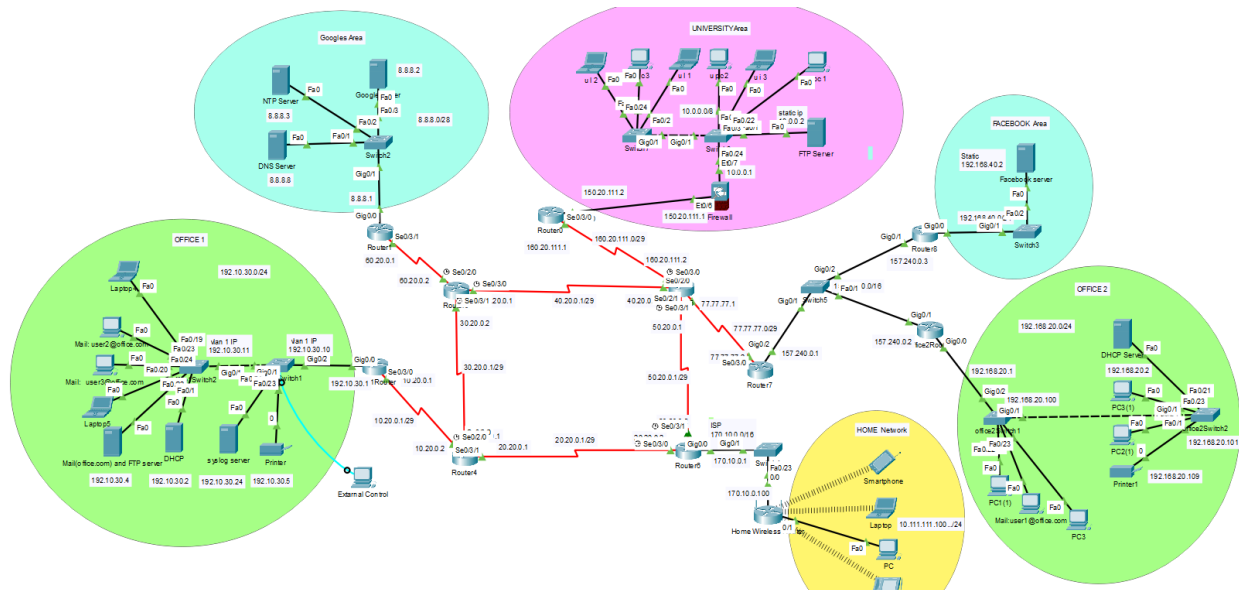
- To design and configure a large-scale MAN network
- To reduce IP waste subnetting
- To control devices from different locations
- How to setup DHCP, DNS, SMTP, FTP, Syslog, NTP, HTTP servers
- To configure other devices using ssh
- Vlan, Nat, Router & Switch access list handle setup

- We may use firewall for extra security
- Access limitation
- And many more

Chapter 2

2 Design/Development/Implementation of the Project

2.1 Project Details



IP assign: In this table, we've shown the useable IP addresses in our project.

Network	IP
Office 1	192.10.30.0/24
Office 2	192.10.20.0/24
Facebook Area	192.168.20.0/24
Google Area	8.8.8.0/28
Home Area	192.168.10.0/24
University Area	10.0.0.0/8
ISP1(Router 6)	170.10.0.0/16
ISP2(Router 7)	157.240.0/16

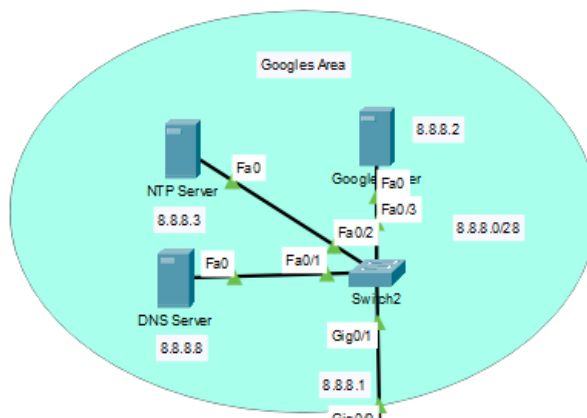
Sub netting: We have used IP sub netting in core network and the rest of the routers according to our needs

Device	Ip	Info
Router 3	30.20.0.0/29	<p>CIDR value /29 mean this IP block sized 16, valid usable IP 14 per block.</p> <p>This project we have used /29.</p> <p>We have assigned the first block of IP to each router.</p>
	40.20.0.0/29	
	60.20.0.0/29	
Router 4	10.20.0.0/29	
	30.20.0.0/29	
	20.20.0.0/29	
Router 5	40.20.0.0/29	
	50.20.0.0/29	
	160.20.11.0/29	
	77.77.77.0/29	
Router 6	50.20.0.0/29	
	20.20.0.0/29	

NTP Server Configuration:

Network Time Protocol (NTP) is a vital service for every network device. Any computer-based device needs to be accurately synchronised with a reliable time source such as an NTP server.

When it comes to Cisco routers, obtaining the correct time is extremely important because a variety of services depend on it. The logging service shows each log entry with the date and time - very critical if you're trying to track a specific incident or troubleshoot a problem.[\[1\]](#)



Step By Step Configuration

Step 1: At first we assign IP Address on the Server.

The screenshot shows the 'NTP Server' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is highlighted in blue. Below it, the 'IP Configuration' settings are displayed:

- ☐ DHCP
- ☒ Static
- IPv4 Address: 8.8.8.3
- Subnet Mask: 255.255.255.240
- Default Gateway: 8.8.8.1
- DNS Server: 8.8.8.8

Step 2: Here fast on service. Then set Date and Time.

The screenshot shows the 'NTP Server' configuration window with the 'Services' tab selected. The 'SERVICES' list on the left includes HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP. The 'NTP' service is selected and configured as follows:

- Service: ☒ On
- Authentication: ☐ Enable ☒ Disable
- Key: [Empty field] Password: [Empty field]

Below the authentication settings, there is a calendar for December 2022 and a time display showing 04:16:08PM.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

Step 3: Now configure CLI mode NTP server on Routers and Switches. Here we declare NTP server ip address. Then we Verify NTP to see current date and time. It is help to Syslog server. we will discuss later.

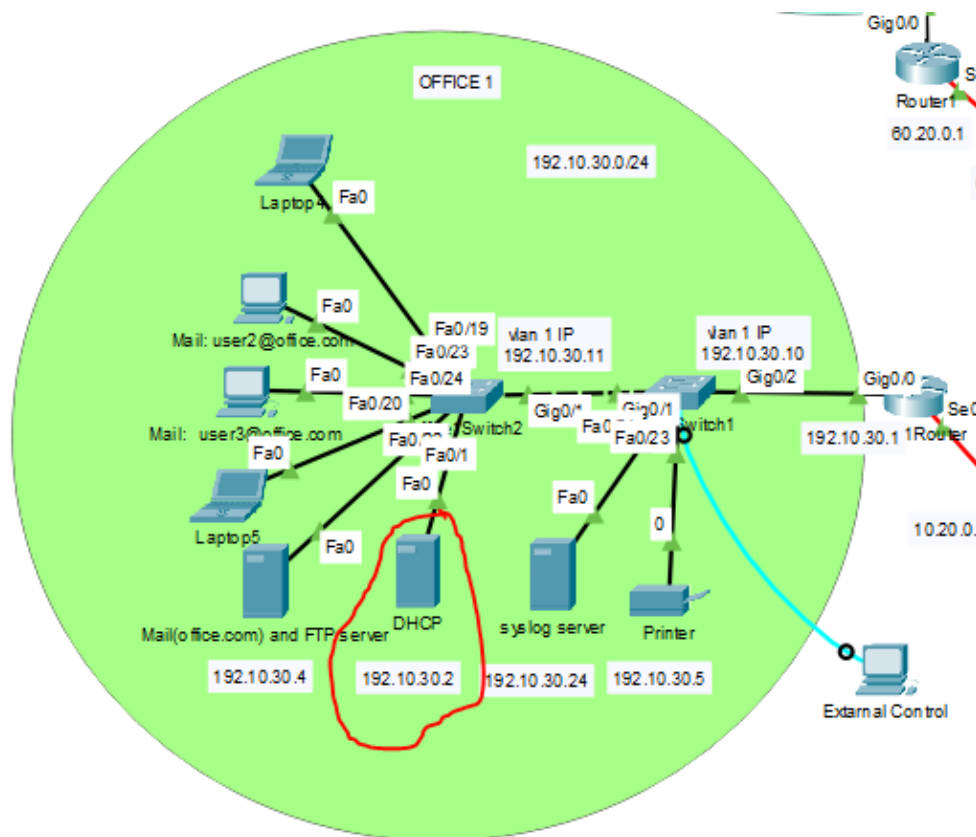
```

officelRouter(config)#
officelRouter(config)#
officelRouter(config)#
officelRouter(config)#ntp server 8.8.8.3
officelRouter(config)#^Z
officelRouter#
*Jan 02, 15:26:56.2626: %SYS-5-CONFIG_I: Configured from console by console
officelRouter#sh
officelRouter#show cl
officelRouter#show cld
officelRouter#show clock
15:27:08.36 UTC Mon Jan 2 2023
officelRouter#

```

DHCP Server Configuration: A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

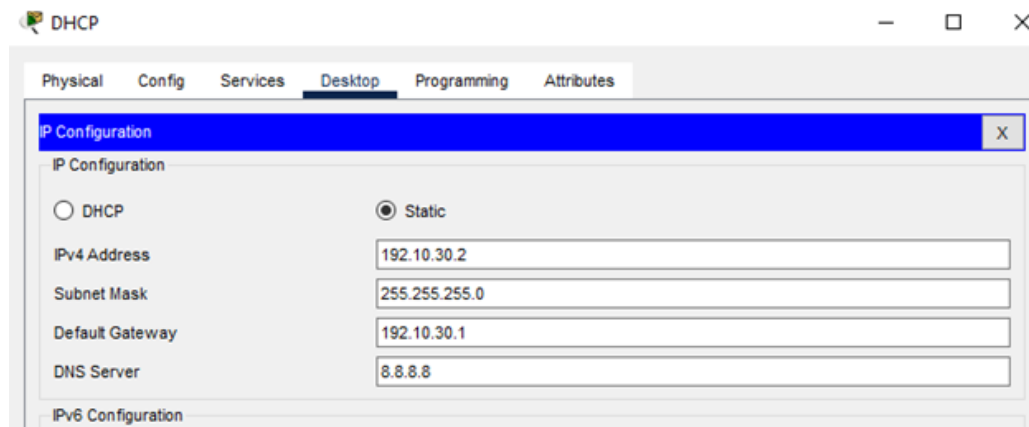
A DHCP server automatically sends the required network parameters for clients to properly communicate on the network. Without it, the network administrator has to manually set up every client that joins the network, which can be cumbersome, especially in large networks. DHCP servers usually assign each client with a unique dynamic IP address, which changes when the client's lease for that IP address has expired.[2]



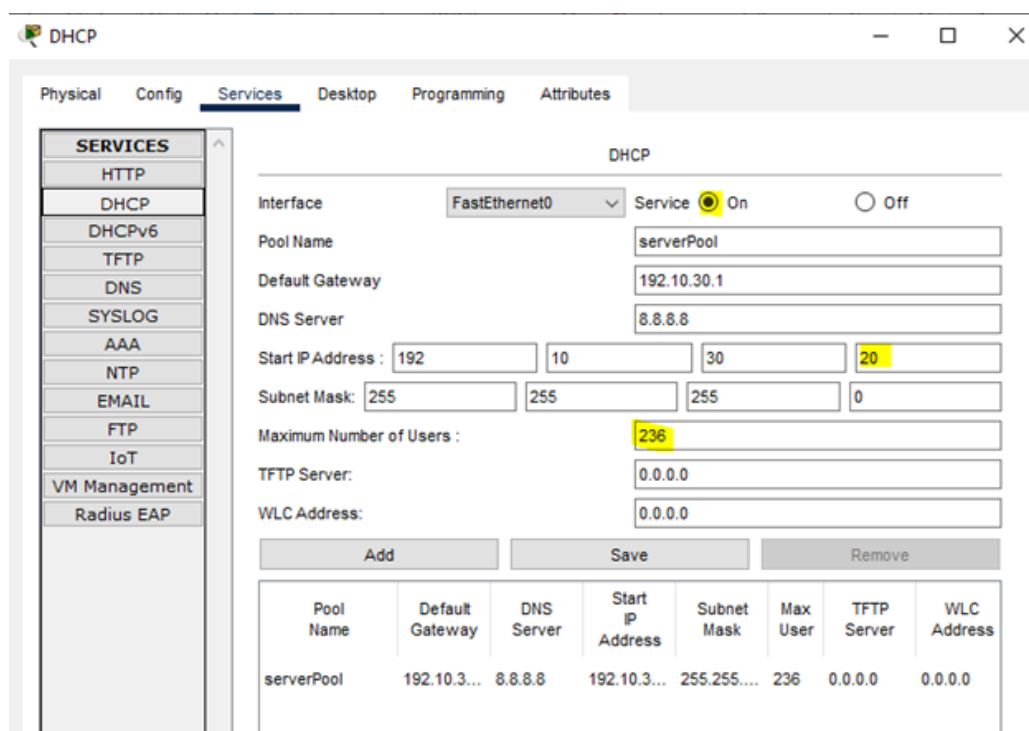
Step By Step Configuration

Here we show the configuration for the office 1 network but we also configured our project other specific networks. Such as Office 2, Home Network router, University area firewall.

Step 1: At first, we assign an IP Addresses on Server.



Step 2: Then on DHCP service. Then set IP range, Subnet Mask, Default Getaway, DNS server IP and also create DHCP pool for assign ip on specific network devices.

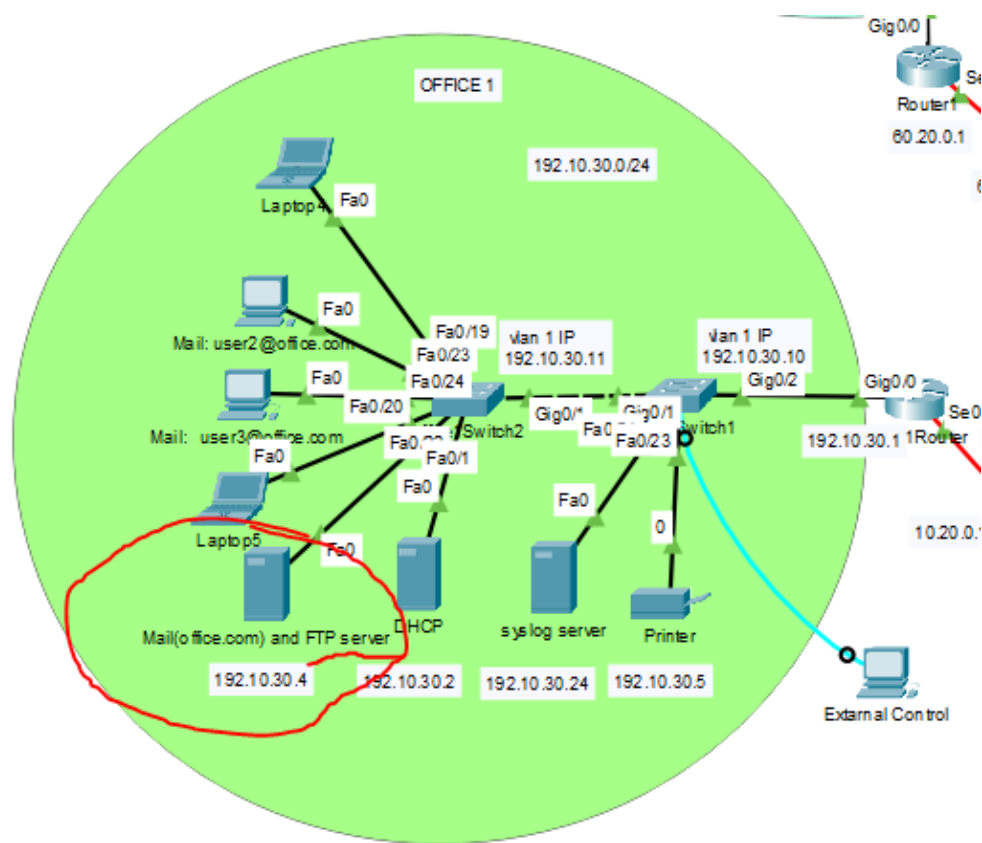


In this image, we see that starting ip 192.10.30.20 that mince this DHCP pool will serve 236 ip and other 2-19 range ip if we want to used statically specific device. Such as we used DHCP, FTP, Mail, Syslog server. This specific devices don,t used dynamicaly ip because we know dynamical ip change automatically for various reasons. Such as device shut down issue.

FTP server configuration:

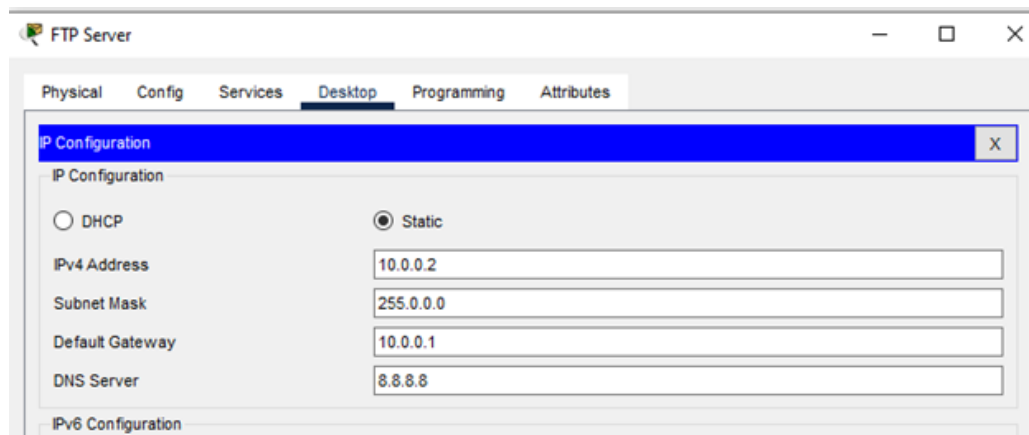
FTP is an acronym for File Transfer Protocol. FTP is used to transfer files between computers on a network. We can use FTP to exchange files between computer accounts, transfer files between an account and a desktop computer.

At fast, we are configuring an FTP server on University Area and Office Area Network. Here we show only University Area Network FTP server assign IP Addresses on Server.

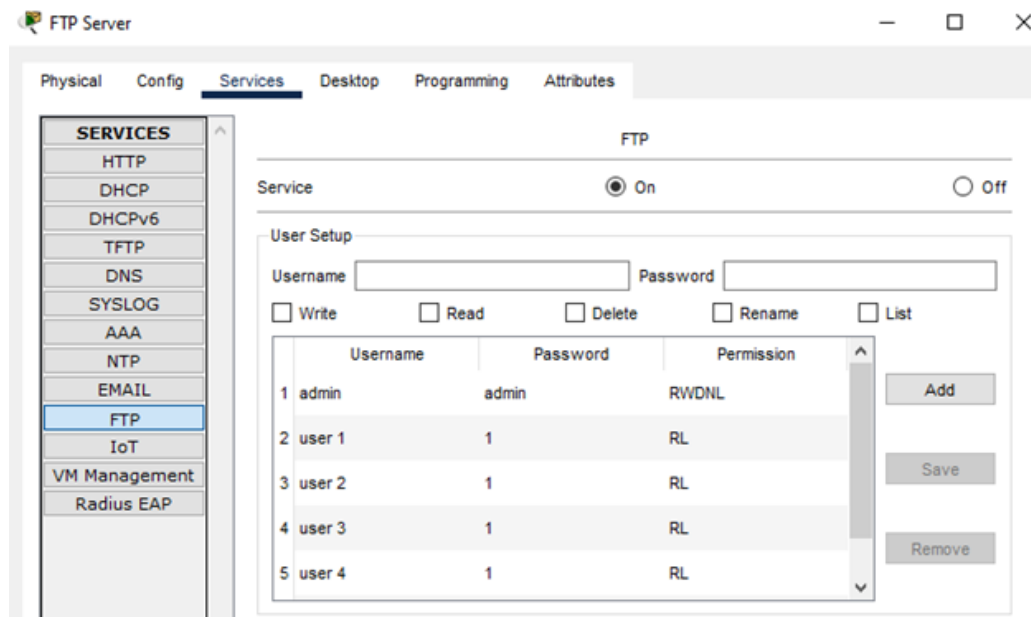


Step By Step Configuration

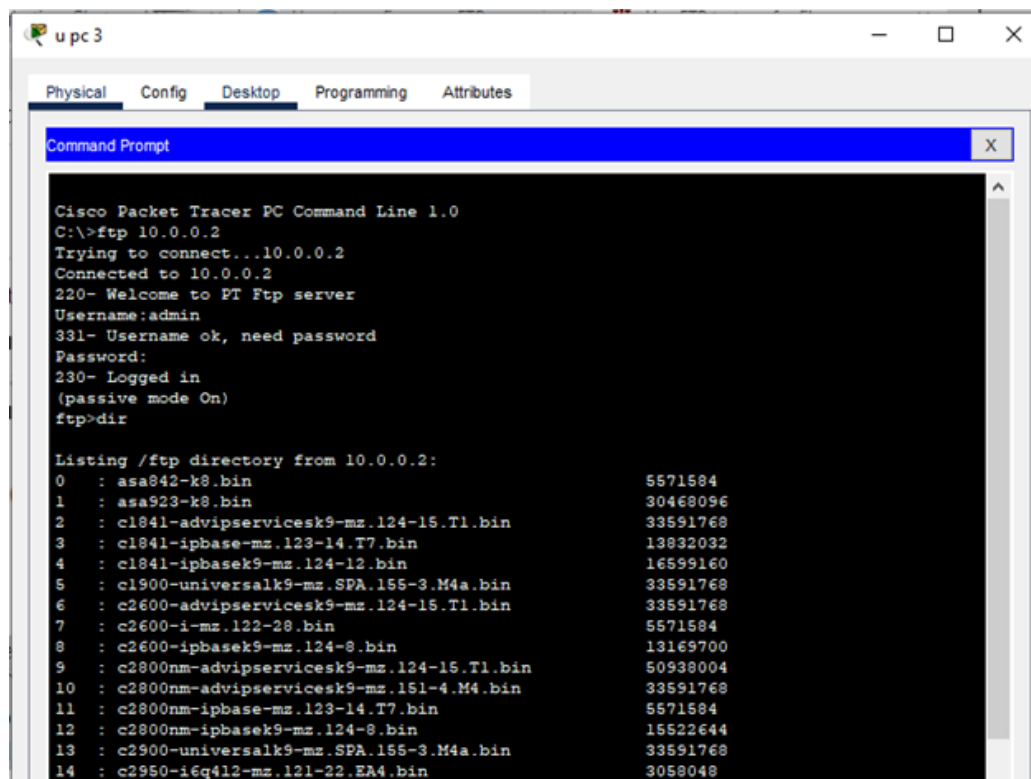
Step 1: At first, we assign an IP Addresses on Server.



Step 2: Then we on FTP service and also create admin, many users and set passwords and permissions



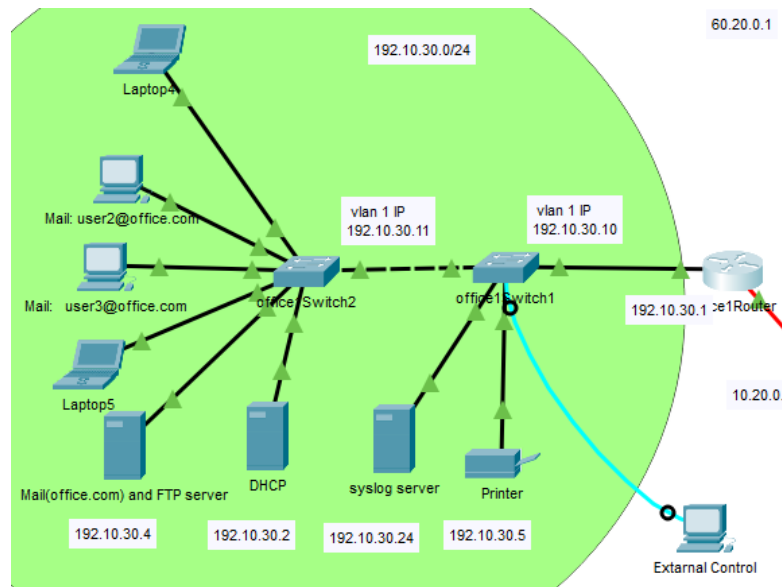
Step 3: Then verify FTP server on the University End device.



SMTP Server configuration:

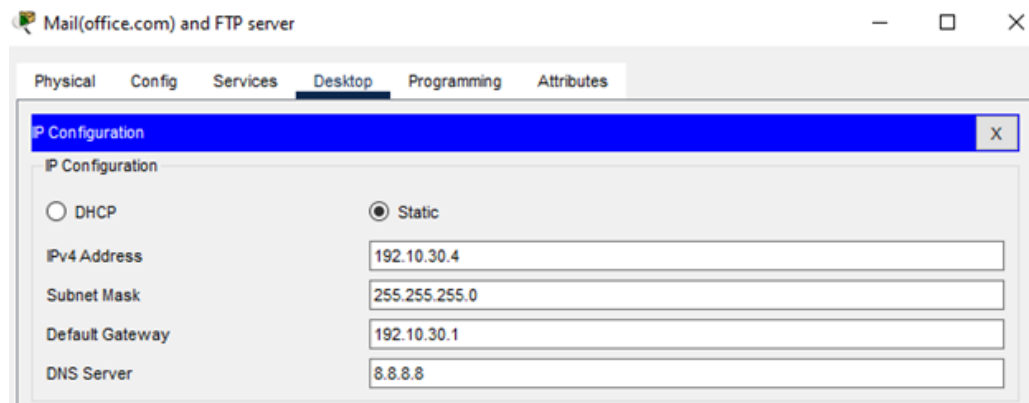
An SMTP server is a computer or an app that is responsible for sending emails. It functions following the Simple Mail Transfer Protocol (SMTP). An SMTP server receives emails from the email client. Then it passes them on to another SMTP email server and relays them to the incoming mail server.[5]

In this project, we have configured 1 SMTP server for 2 office networks. There we set up one center SMTP server, office1 and office 2 clients are used central SMTP server sending for emails.

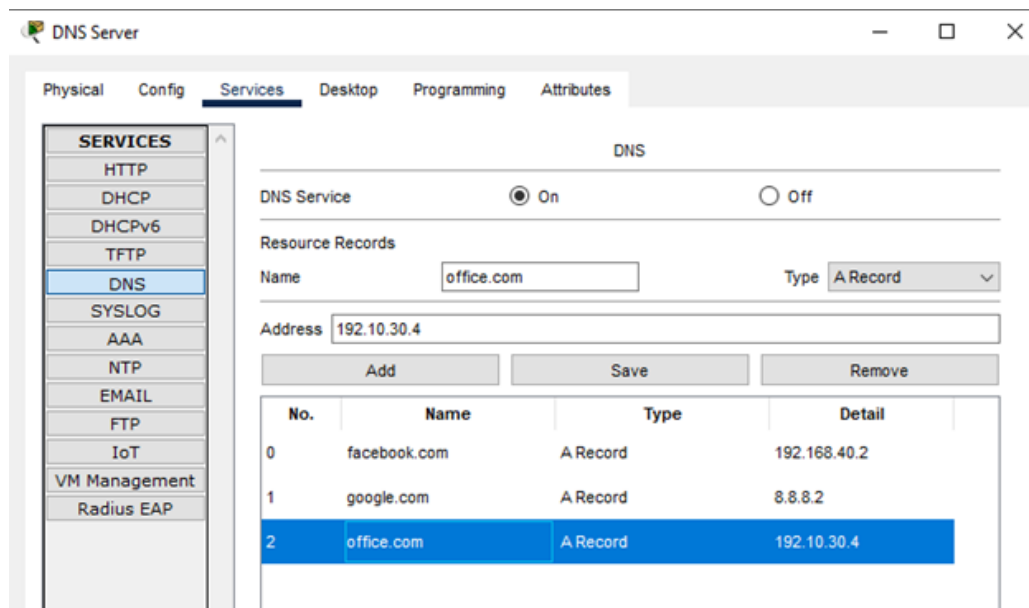


Now we see configuration process:

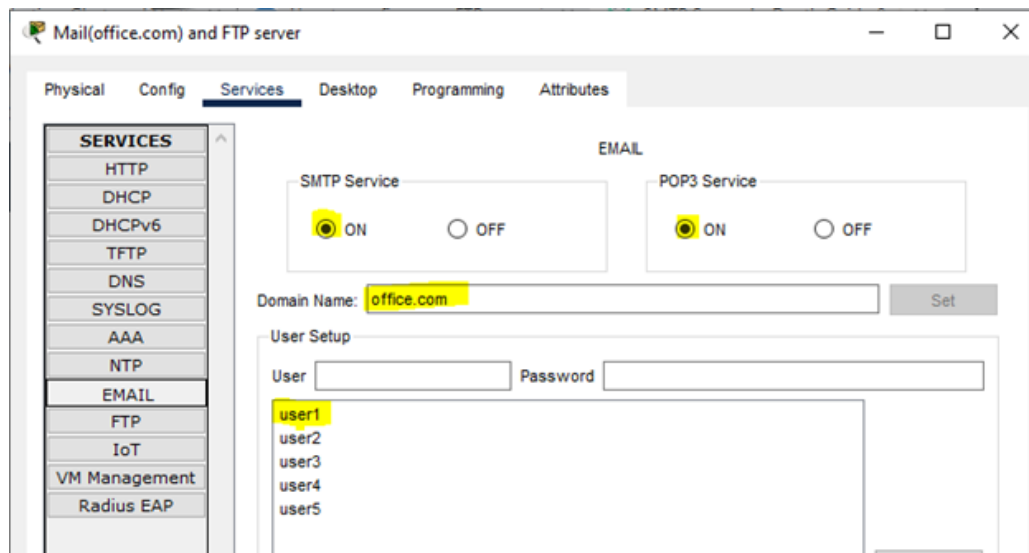
Step 1: At first set SMTP server on office 1 network. Then set the IP address.



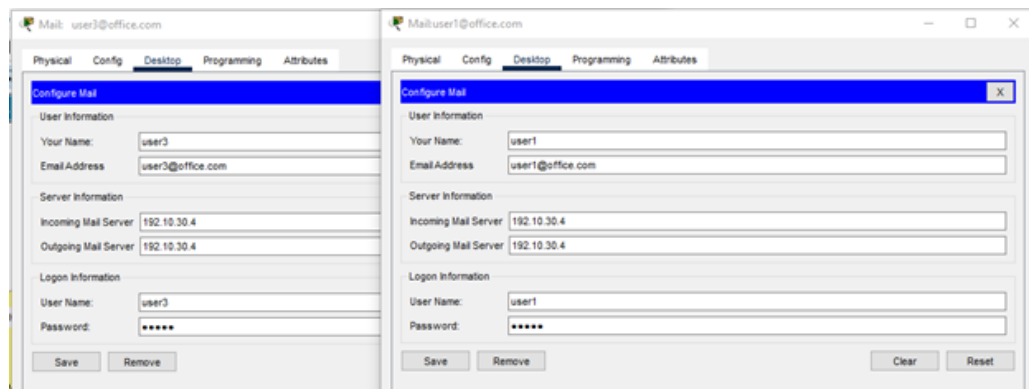
Step 2: Then we set the Domain name “office.com” against Mail server (192.10.30.4) ip.



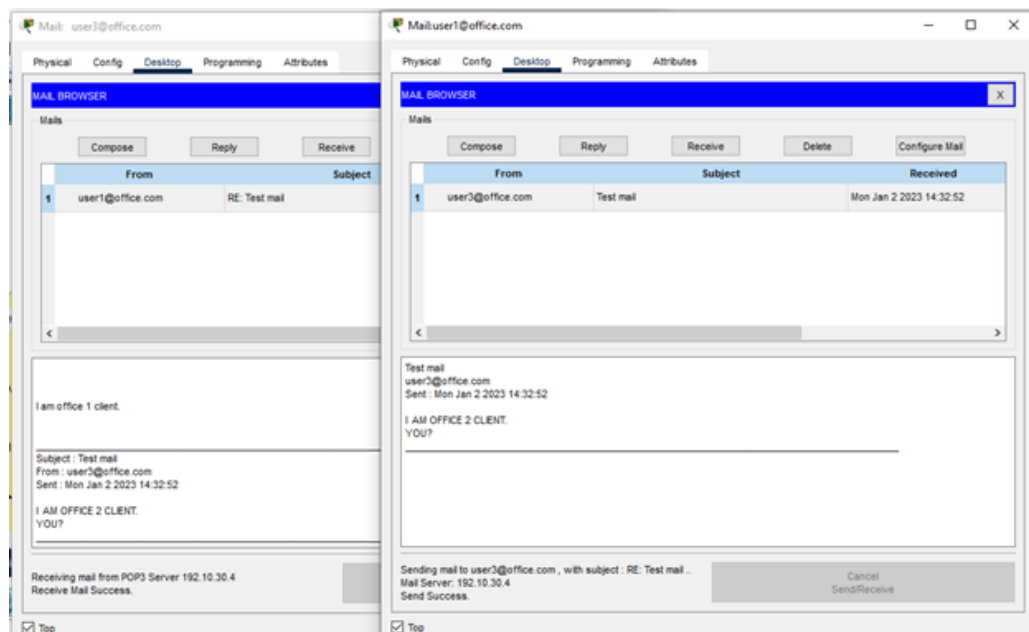
Step 3: Then on SMTP and POP3 service and set before creating the domain name. Also created few users for needs and set password both them.



Step 4: Then we configured user mail. Where user1 belongs to office network 2 and user3 belongs office network 1. Here we fill up many properties then save configuration.



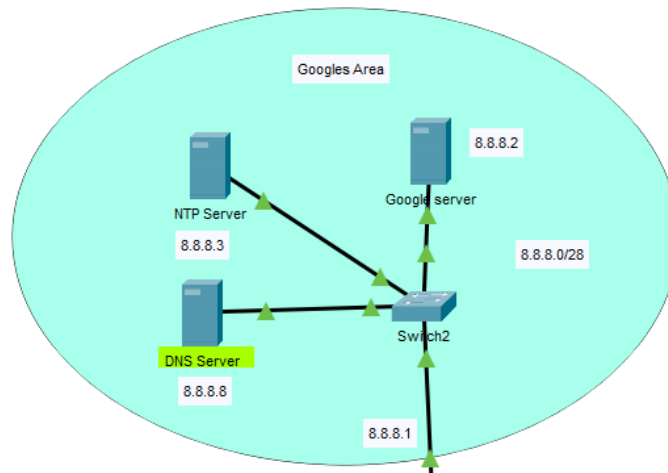
Step 5: Then verify the mail sending Office 1 to Office 2 and Office 2 to Office 1 .Then check it work properly.



DNS server configuration: The Domain Name System (DNS) is the phone book of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web

browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

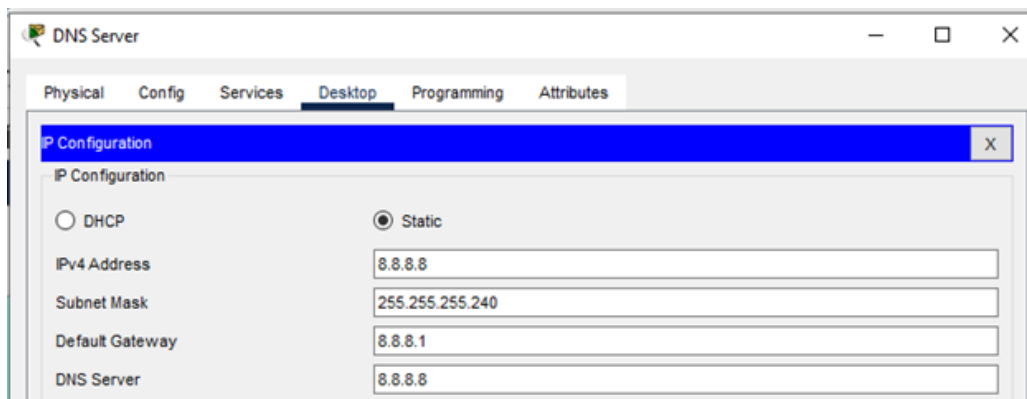
Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4).[4]



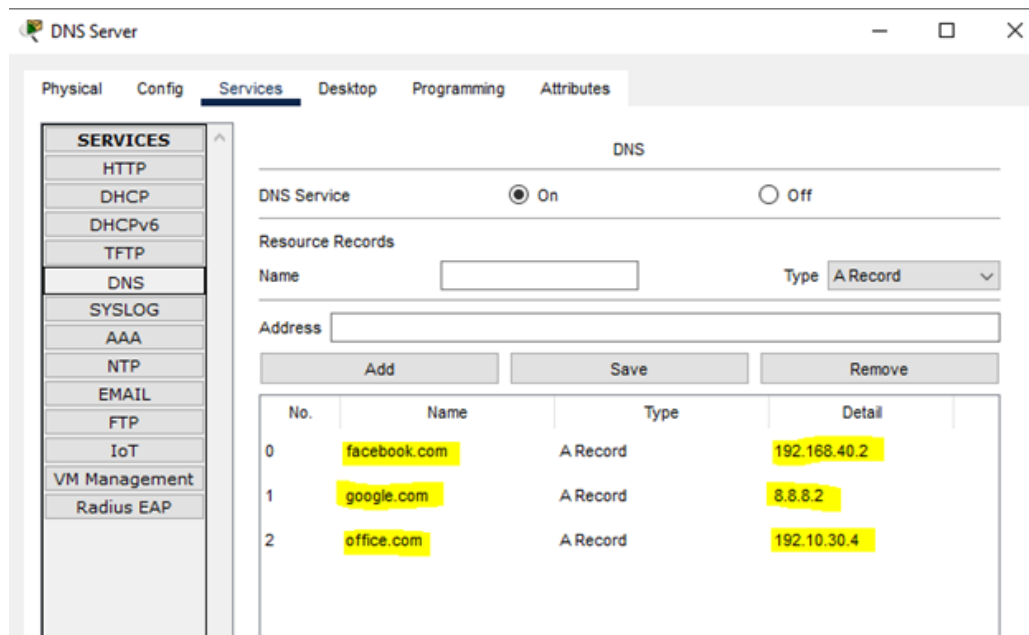
We are configured the DNS server globally. It is situated in our Google area network.

Step By Step Configuration

Step 1: At first, we assign an IP Address on Server.



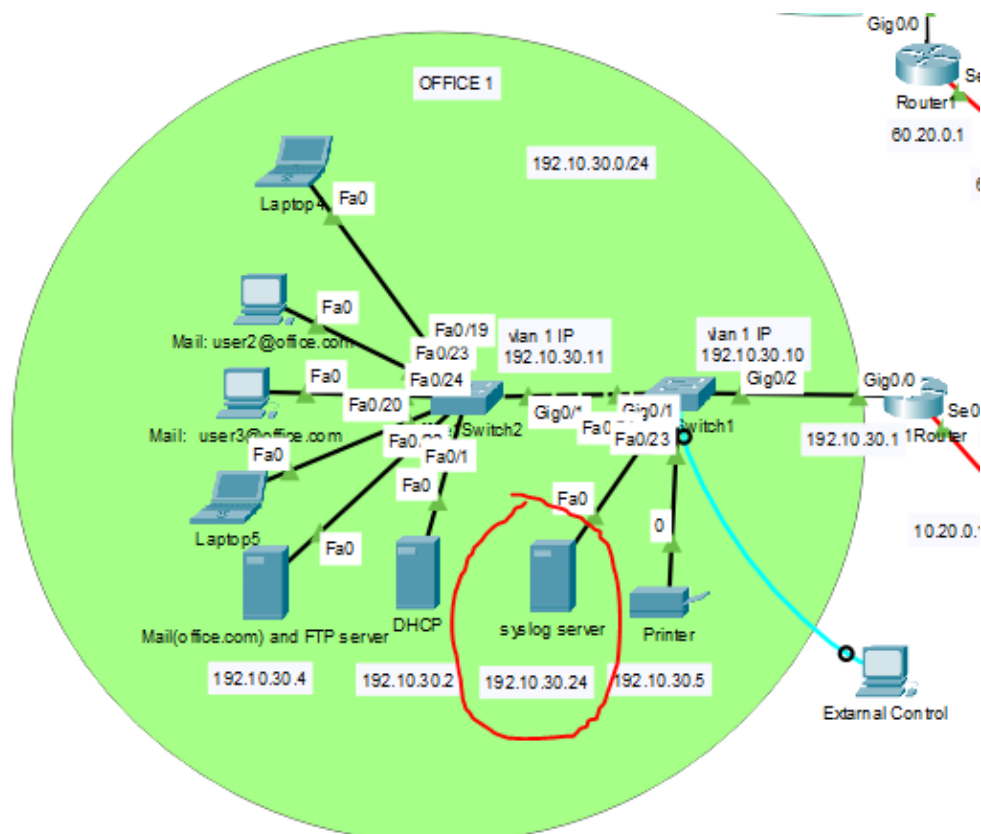
Step 2: At first on the DNS service. Then we add the domain name according to their IP address. This server we add 3 domain name Such as “facebook.com”, “google.com” and “office.com”.



Syslog Server:

System Logging Protocol (Syslog) is a way network device can use a standard message format to communicate with a logging server. It was designed specifically to make it easy to monitor network devices. Devices can use a Syslog agent to send out notification messages under a wide range of specific conditions.

These log messages include a timestamp, a severity rating, a device ID (including IP address), and information specific to the event. Though it does have shortcomings, the Syslog protocol is widely applied because it is simple to implement, and is fairly open-ended, allowing for a lot of different proprietary implementations, and thus the ability to monitor almost any connected device.[6]

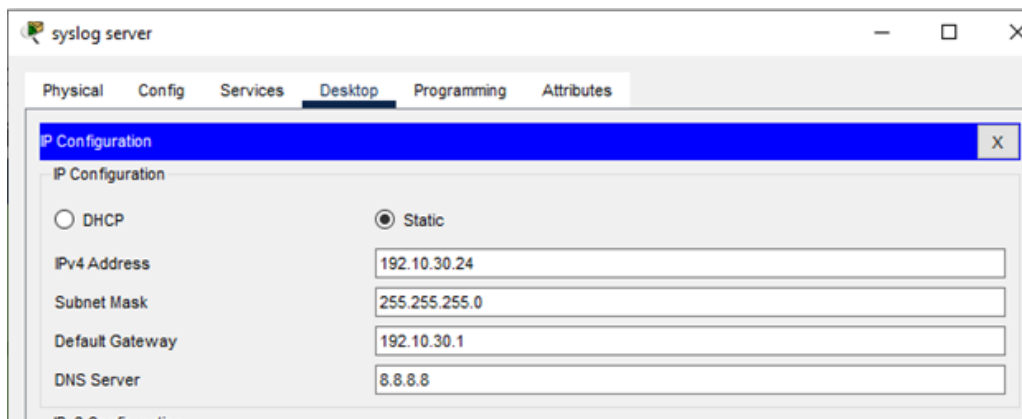


It helps save time, speed up the log review process, and implement preventive troubleshooting. The Syslog Severity level ranges between 0 to 7. Each number points to the relevance of the action reported.

Severity Level	Level Name	Description
0	Emergencies	System unusable
1	Alerts	Immediate action needed
2	Critical	Critical conditions
3	Errors	Error conditions
4	Warnings	Warning conditions
5	Notifications	Normal but significant conditions
6	Informational	Informational messages only
7	Debugging	Debugging messages

Step By Step Configuration

Step 1: At first we assign an IP Address on Server.

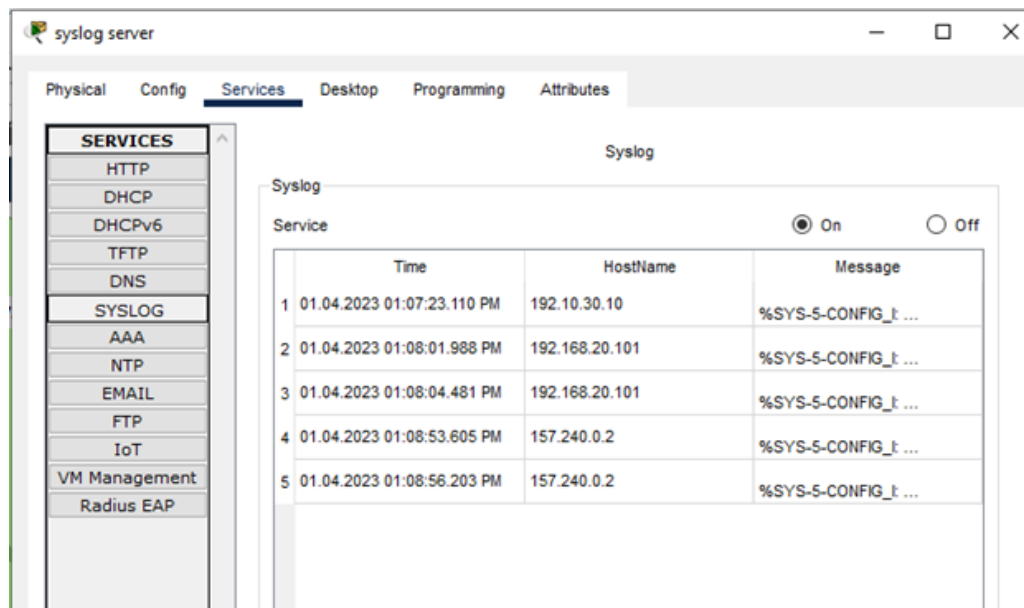


Step 2: Open the device CLI mode and run this command. In this command first, we declare the server address and then declare debugging (level 7). Cisco packet tracer could,t support 0 to 6 security levels. That is why the Syslog server only receives debugging messages. Since we are configuring the Syslog server only Office Area, this server covers this network router and switch.

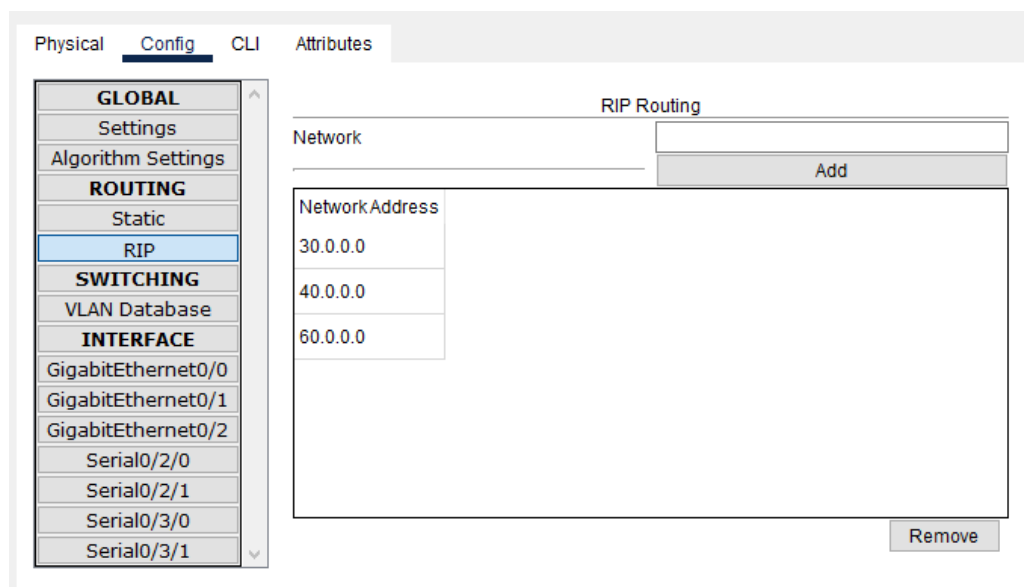
In this command, we also run “office1Switch1, offie1Switch2, office2Switch1, office2Switch2, office1Router, and office2Router.

```
office2Switch2(config)#logging host 192.10.30.24
office2Switch2(config)#logging trap debugging
```

Step 3: Then on the Syslog service and verify. In this image we see that log messages are generated.



Dynamic routing using RIP

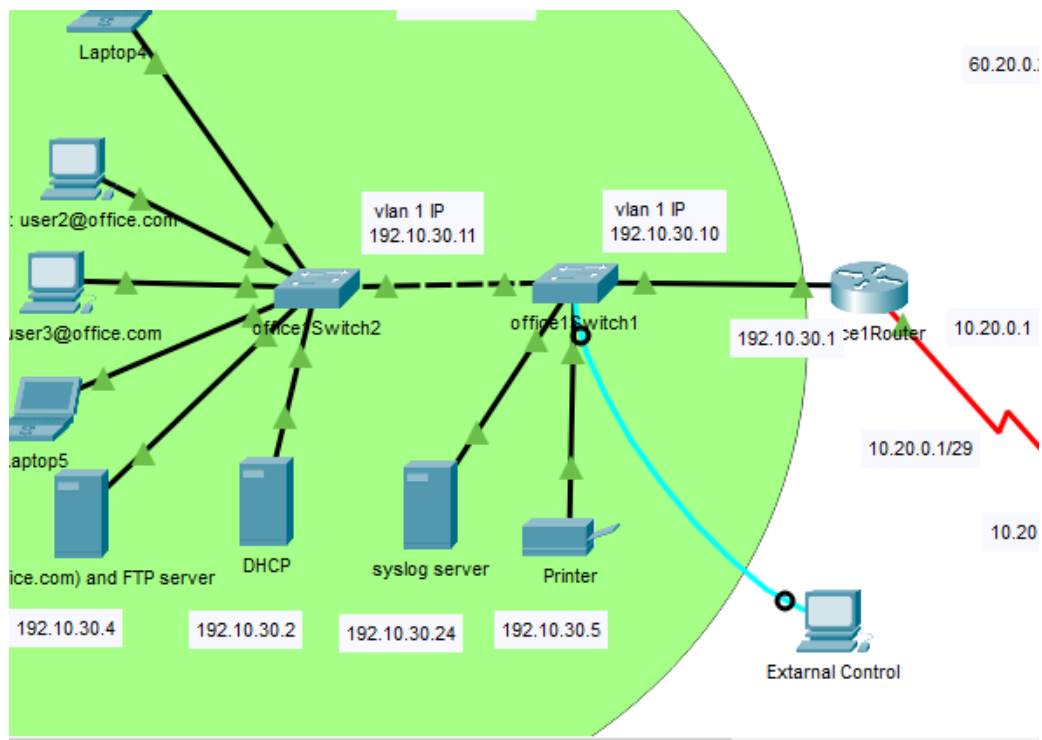


Dynamic routing is known as a technique of finding the best path for the data to travel over a network. And we have did RIP in all router like this one.

Security Section:

External Access security:

Console port password Configuration: Every Cisco router or switch has a single console port that is used to connect it to a computer directly for configuration and management. A console cable or a rollover cable is used to connect to the router or switch console port and is typically used during initial configuration as there is no network connection and remote access.^[7]



Step 1: Configure the security portion first. We need to configure the device's "hostname" and set the "enable password." Run these two commands in CLI mode.

```
Switch(config)# hostname office1Switch1
```

```
office1Switch1(config)# enable secret office
```

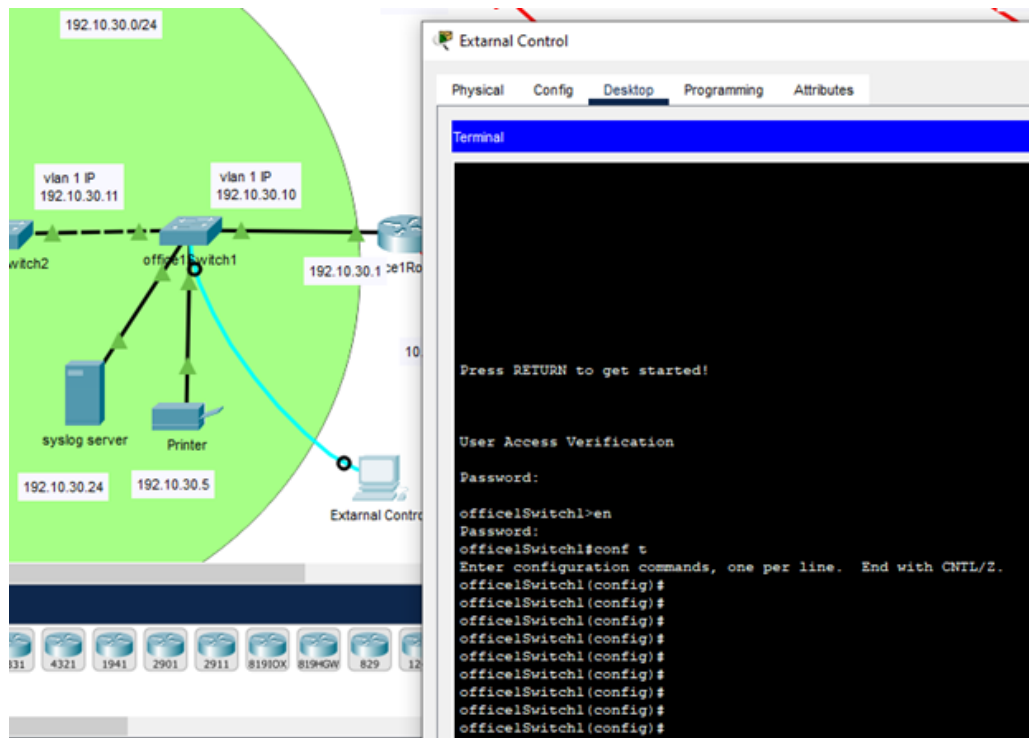
Step 2: Finally, run this command in CLI mode for console login.

```
office1Switch1(config)# line con 0
```

```
office1Switch1(config)# password office
```

```
office1Switch1(config)# login
```

Step 4: In this image, we see that an external PC remotely accessed a switch with a console cable.



SSH configuration: SSH or Secure Shell is a network communication protocol that enables two computers to communicate and share data. An inherent feature of ssh is that the communication between the two computers is encrypted meaning that it is suitable for use on insecure networks.

SSH is often used to "login" and perform operations on remote computers but it may also be used for transferring data.[8]

In this project, we are not using Telnet because Telnet sends the data in plain text, making it vulnerable to security attacks. In contrast, SSH encrypts transferred data, so a security breach doesn't likely occur.

Step 1: We already know that the layer 2 switch does not assign an IP address to the interface. So give "int VLAN 1" an IP address. This IP address will help during remote access. Then run this command in CLI mode.

```

office1Switch1(config)#int vlan 1
office1Switch1(config-if)#ip address 192.10.30.10 255.255.255.0
office1Switch1(config-if)#no shutdown
office1Switch1(config-if)#exit

```

Step 2: First, we have defined the domain name by using the ip domain-name Cisco command and have also run the RSA algorithm. Set the higher key value for encryption purposes.

```
office1Switch1(config)#ip domain-name cisco.com  
office1Switch1(config)#crypto key generate rsa  
The name for the keys will be: office1Switch1.cisco.com  
Choose the size of the key modulus in the range of 360 to 2048 for your  
General Purpose Keys. Choosing a key modulus greater than 512 may take  
a few minutes.  
  
How many bits in the modulus [512]: 1024  
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]  
office1Switch1(config)#user nasim secret nasim
```

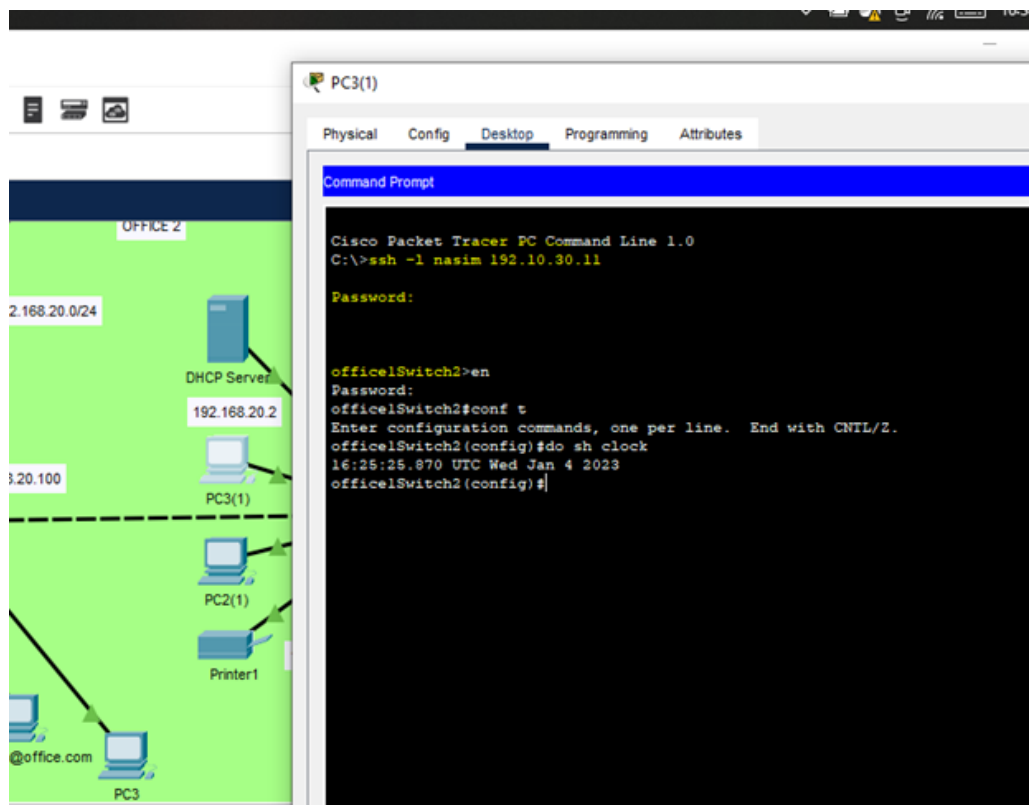
Step 3: Then, we need to enable only the SSH access to a device. This is done by using the transport input ssh command:

```
office1Switch1(config)#line vty 0 2  
office1Switch1(config-line)#login local  
office1Switch1(config-line)#transport input ssh  
office1Switch1(config-line)# exit
```

Step 4: After that, the local user is created by using the username nasim password nasim command.

```
office1Switch1(config)#user nasim secret nasim
```

Step 5: Using SSH, we attempt to remotely access the Office 2 PC from the Office 1 Switch 2.



Access List: An ACL is a list of permits or deny rules detailing what can or can't enter or leave the interface of a router. Every packet that attempts to enter or leave a router must be tested against each rule in the ACL until a match is found. If no match is found, then it will be denied.

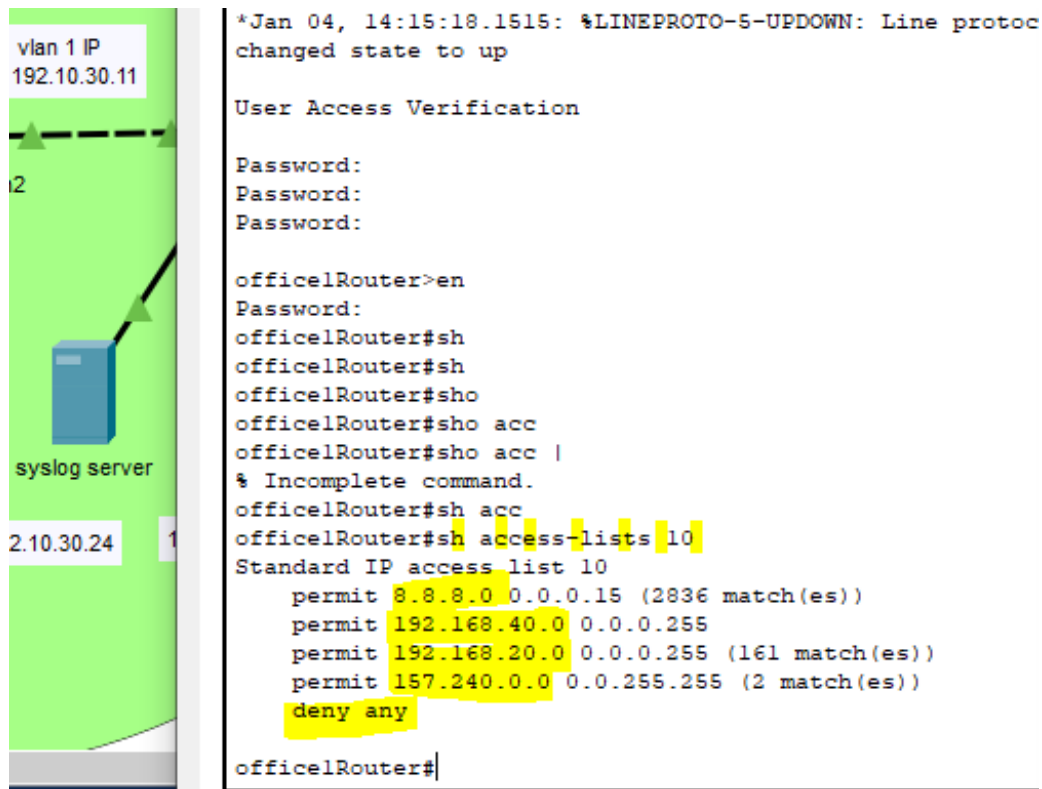
Step 1: Run this command in CLI mode. Create a list first, then set permit IP lists, and finally, deny all IP. Next, this list assigns interfaces.

```

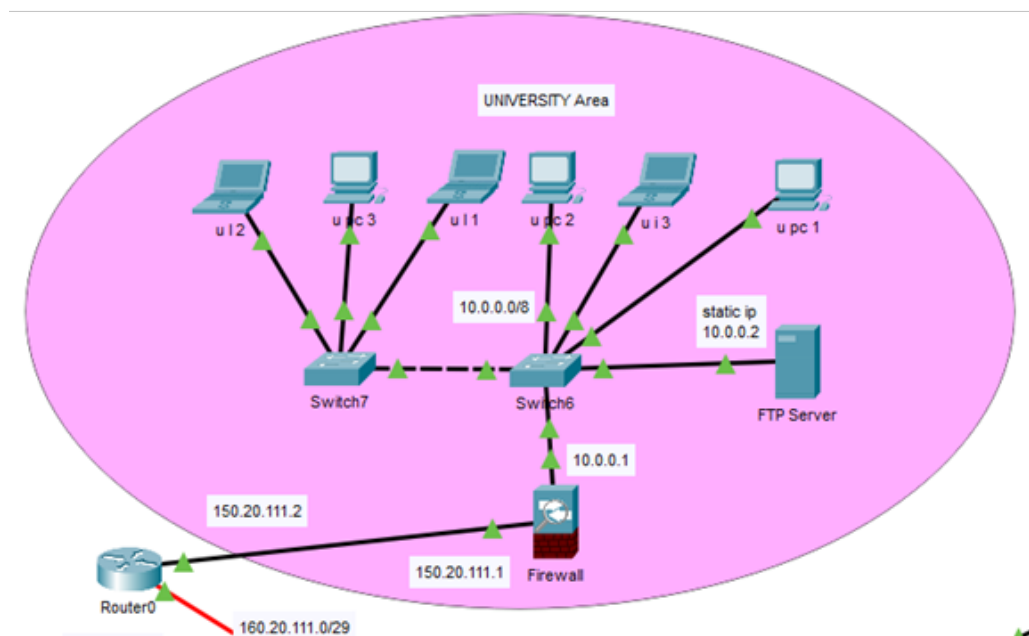
Office1Router(config)#access-list 10
Office1Router(config)#access-list 10 permit 192.168.20.0 0.0.0.255
Office1Router(config)#access-list 10 permit 192.168.40.0 0.0.0.255
Office1Router(config)#access-list 10 permit 157.240.0.0 0.0.255.255
Office1Router(config)#access-list 10 permit 8.8.8.0 0.0.0.15
Office1Router(config)#access-list 10 deny any
|
Office1Router(config)#interface gigabitEthernet 0/0
Office1Router(config)#ip access-group 10 out

```

We have created an access list for every router in our project. For example, the Office 2 router access list is shown. we see that those 4 networks (8.8.8.8/28, 192.168.10.0/24, 192.168.40.0/24, and 157.240.0.0/16) are permitted and the rest of the network is denied. The rest of the network can't ping this router. We have created an access list for the rest of the routers according to our needs.



Firewall configuration: A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.[3]



Configuration Firewall: We have configured firewall according to our needs.

Step 1: Assign IP interface vlan 1, security level 100, because it is a trusted network (local). This network IP used for university local devices. Then attach this vlan firewall interface 0/7. As it we have create another vlan 2 and assign IP. This network used for create connectivity Router.

```

ciscoasa(config)#int vlan 1
ciscoasa(config-if)#ip address 10.0.0.1 255.0.0.0
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)#exit

ciscoasa(config)#interface ethernet 0/7
ciscoasa(config-if)#switchport access vlan 1
ciscoasa(config-if)#exit

ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip address 150.20.111.1 255.255.0.0
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#exit
|
ciscoasa(config)#interface ethernet 0/6
ciscoasa(config-if)#switchport access vlan 2
ciscoasa(config-if)#exit
ciscoasa(config)#

```

Step 2: Then set the default route. Make an access list and place it outside. Declare the object group and define the subnet. Next, configure NAT and DHCP server using command also set DHCP pool and DNS IP.

```

ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 150.20.111.2

ciscoasa(config)#access-list uni extended permit tcp any any
ciscoasa(config)#access-list uni extended permit icmp any any
ciscoasa(config)#access-group uni in interface outside

ciscoasa(config)#object network local
ciscoasa(config-network-object)#subnet 10.0.0.0 255.0.0.0

ciscoasa(config-network-object)#nat (inside,Outside) dynamic interface

ciscoasa(config)#dhcpd address 10.0.0.10-10.0.0.41 inside
|ciscoasa(config)#dhcpd dns 8.8.8.8 interface inside

```

Chapter 3

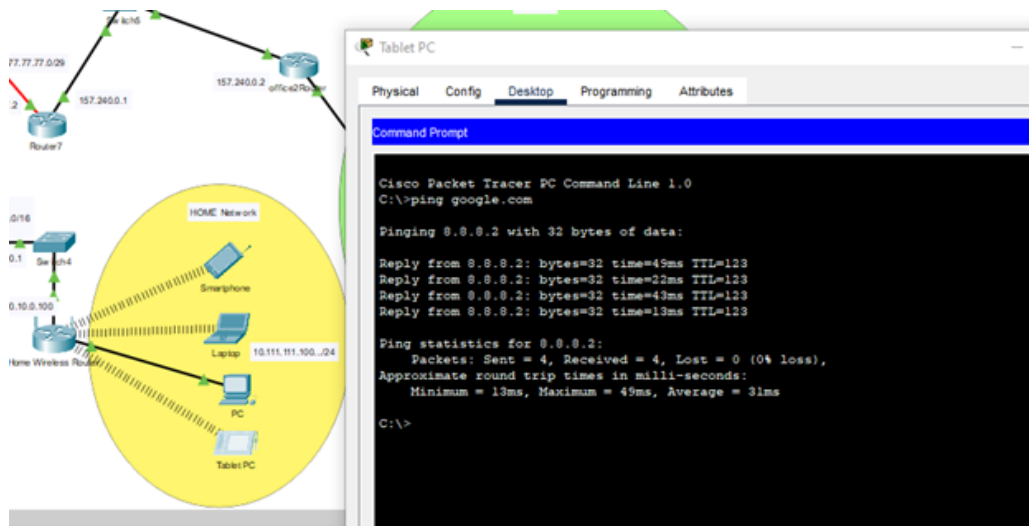
3 Performance Evaluation

3.1 Simulation Environment/ Simulation Procedure

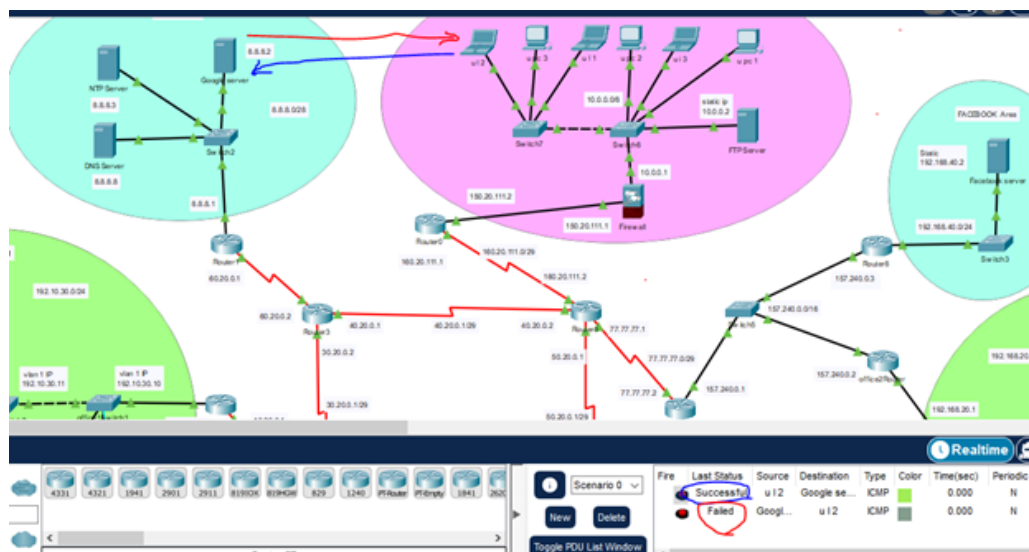
We used cisco packet teacher for this project

3.2 Results Analysis/Testing

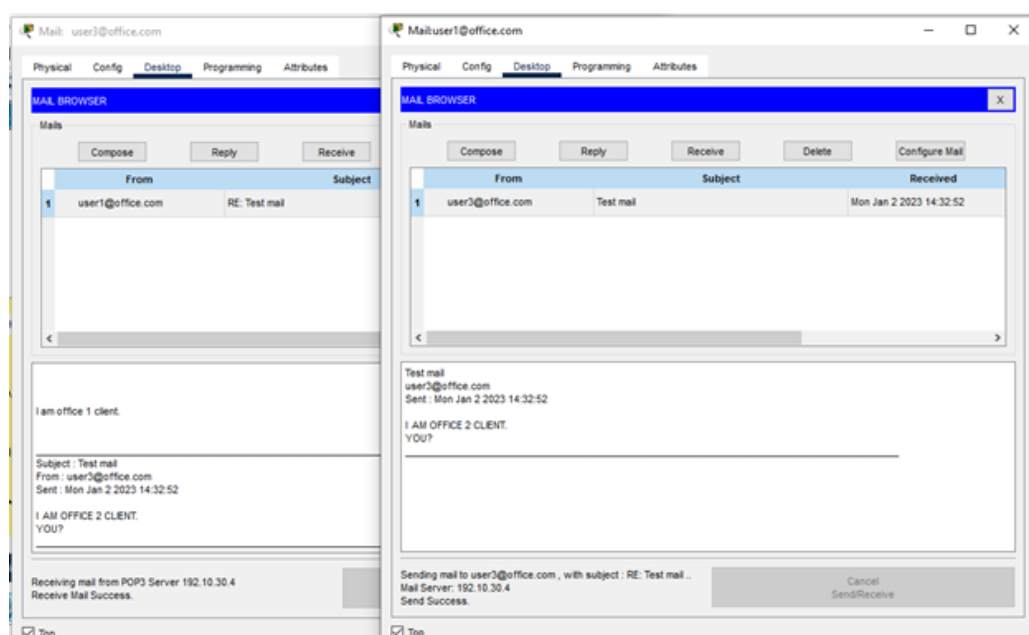
Ping Home Area to the Google server to check their connectivity.



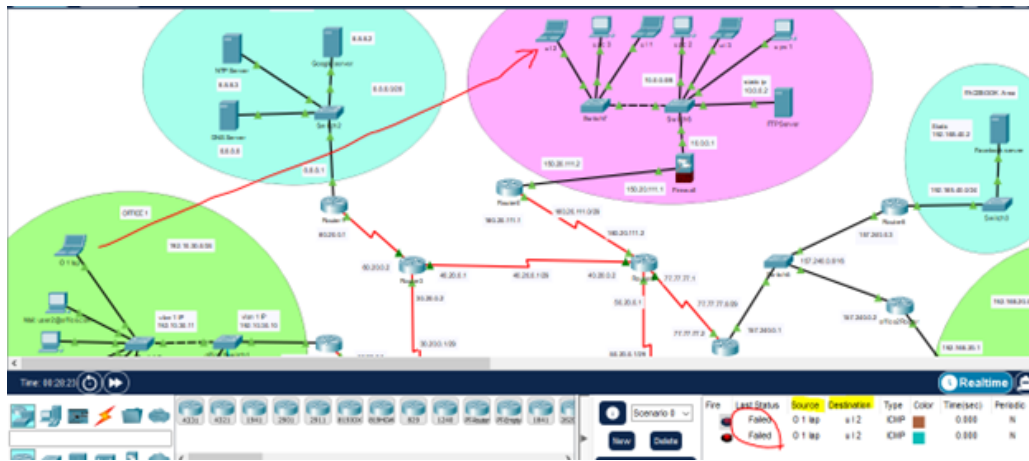
Ping the university to Google and Google to the university to check their connectivity.



Examine the mail sent from Office 1 to Office 2 as well as from Office 2 to Office 1. It works properly.



Send a packet from the office 1 PC to the university PC to test connectivity. The connection has failed because the firewall block the source address.



The Syslog server received activity messages from different routers and switches.

syslog server

Physical Config **Services** Desktop Programming Attributes

SERVICES

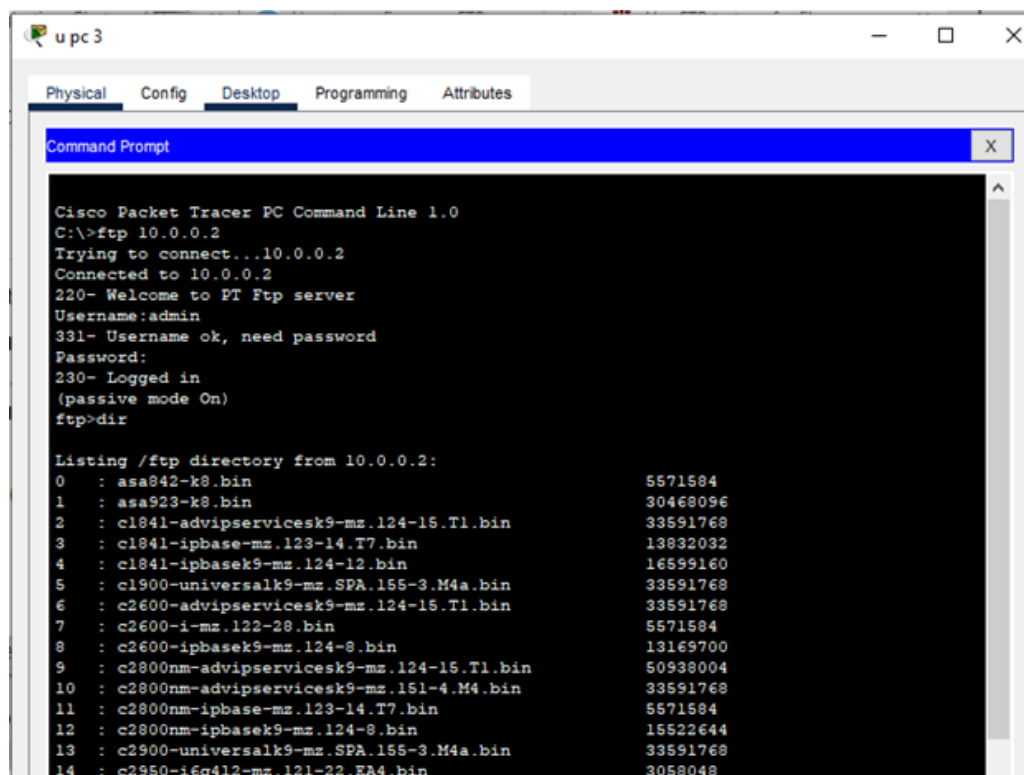
- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG**
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

Syslog

Service ☒ On ☐ Off

	Time	HostName	Message
1	01.04.2023 01:07:23.110 PM	192.10.30.10	%SYS-5-CONFIG_t ...
2	01.04.2023 01:08:01.988 PM	192.168.20.101	%SYS-5-CONFIG_t ...
3	01.04.2023 01:08:04.481 PM	192.168.20.101	%SYS-5-CONFIG_t ...
4	01.04.2023 01:08:53.605 PM	157.240.0.2	%SYS-5-CONFIG_t ...
5	01.04.2023 01:08:56.203 PM	157.240.0.2	%SYS-5-CONFIG_t ...

This network PC has access to the university's FTP server.



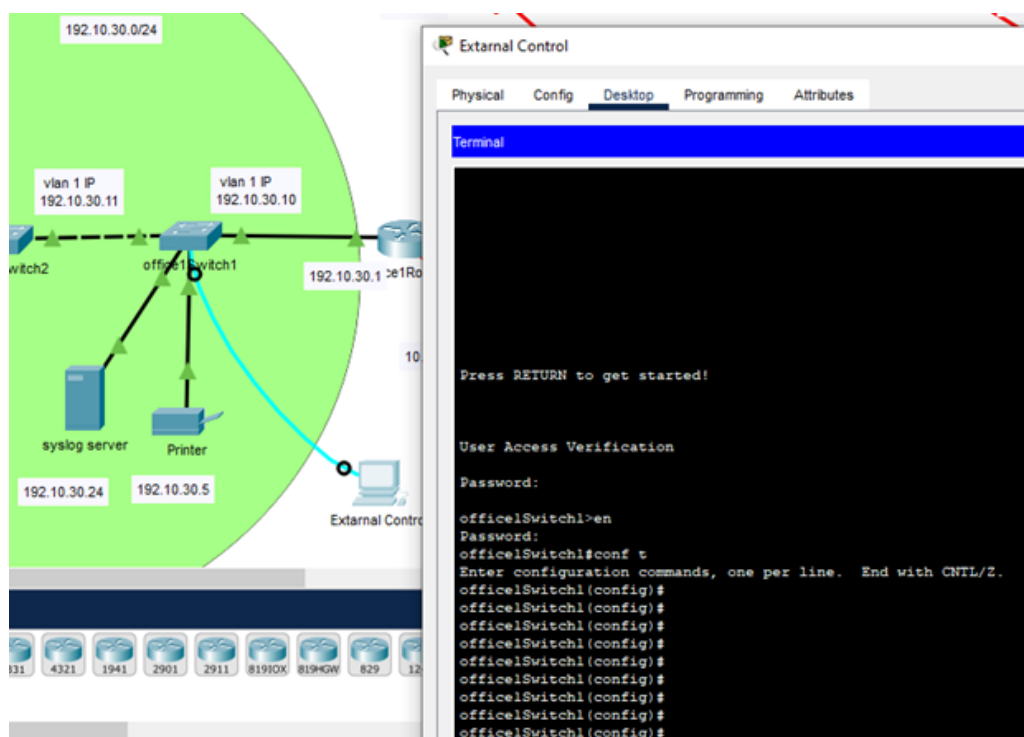
```

Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 10.0.0.2
Trying to connect...10.0.0.2
Connected to 10.0.0.2
220- Welcome to PT Ftp server
Username:admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 10.0.0.2:
 0 : asa842-k8.bin                    5571584
 1 : asa923-k8.bin                    30468096
 2 : c1841-advipservicesk9-mz.124-15.T1.bin  33591768
 3 : c1841-ipbase-mz.123-14.T7.bin    13832032
 4 : c1841-ipbasek9-mz.124-12.bin    16599160
 5 : c1900-universalk9-mz.SPA.155-3.M4a.bin  33591768
 6 : c2600-advipservicesk9-mz.124-15.T1.bin  33591768
 7 : c2600-i-mz.122-28.bin           5571584
 8 : c2600-ipbasek9-mz.124-8.bin     13169700
 9 : c2800nm-advipservicesk9-mz.124-15.T1.bin  50938004
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin  33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin  5571584
12 : c2800nm-ipbasek9-mz.124-8.bin   15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin  33591768
14 : c2950-i6q412-mz.121-22.EA4.bin  3058048

```

An external PC remotely accessed a Switch with a console cable.



3.2.1 Complex Engineering Problem Discussion

Already discussed in 1.3.2

Chapter 4

4 Conclusion

4.1 Discussion

We have tried to make the solution according to our original problem where no useless features are used. All the features we used made problem solving even more powerful. After each feature is added its proper working is tested. We have tried to implement maximum learning outcomes in lab classes. Also to add many new functionalities which we have learned from various sources. We faced many problems to solve this project. Since many new things we have learned and implemented.

4.2 Limitations

Since we have used RIP routing Protocol, we cannot use more than 15 routers in our project. This requires configuring OSPF routing. Our network connectivity does not have a backup ISP connection due to which the internet service will be down if the ISP is down.

4.3 Scope of Future Work

- In our project we are using NAT only in university network rest of the network we use static, dynamic and PAT as per our requirement.
- We are using RIP routing in our project, we want our project to be bigger where we will use OSPF and BGP routing protocol in addition to Rip Routing.
- Using access points on our network.
- Creating separate V LANs on the network and configuring trunk ports to establish connections between them.
- Creating EtherChannels with switch-to-switch backup lines.
- Handling double ISPs on a single network with no problems with internet connectivity if either ISP is down.

References

- [1] Configuring NTP on a Cisco Router.
- [2] What is a DHCP Server? | Learn What They Are & How They Work.
- [3] What is a Firewall? The Different Types of Firewalls.
- [4] What is DNS? – Introduction to DNS - AWS.
- [5] SMTP Server: In-Depth Guide & Answers to FAQs [2023], December 2022.
- [6] Alex Jablokow. What is a Syslog Server and How Does it Work? - WhatsUp Gold.
- [7] Libby. Cisco Console Port Security, November 2021.
- [8] UCL. What is SSH and how do I use it?, January 2018.