



**Program: MSc Information System
Processing in Computing**

Module: Networks and Systems
Administration

Assignment:
CA 1

Submitted to:
Prof. Obinna Izima

Submitted by:
Nelson Morris (10555450)

TABLE OF CONTENTS

Acronyms.....	
1.Introduction.....	5
1.1 Aim of the project.....	6
1.2 Scope of the project.....	6
1.3 Approach used in carrying out the project.....	6
2. Background.....	7
3. Technologies used in the project.....	7
3.1 Similar Technologies/System.....	8
4. Technical Description.....	8
4.1 PC, Laptop & Tablet.....	9
4.2 Switches, Routers, and Modems.....	9
4.3 Server.....	11
4.4 Access Point.....	11
4.5 Cloud Network.....	12
4.6 IOT.....	12
4.7 DHCP	12
4.8 HTTP.....	13
4.9 DNS.....	14
4.10 FTP.....	15
4.11 ACL.....	16
4.12 Peer to Peer Connections.....	17

4.13 IP address List.....	18
5. Project Testing and Evaluation.....	19
6. Demonstration of the Company Network system.....	20
6.1 DHCP.....	20
6.2 DNS.....	23
6.3 HTTP.....	25
6.4 FTP.....	28
6.5 ACL.....	32
6.6 IOT.....	34
7. References.....	41

TABLE OF FIGURES

Figure No 1. Network Architecture.....	9
Figure No 2. Switch Example.....	10
Figure No 3. Switch Connected to Wireless Access Point.....	10
Figure no 4. Routers.....	10
Figure No 5. Office Server.....	11.
Figure No 6. IoT Server	11
Figure No 7. Access Point Connected to PC.....	11
Figure No 8. Cloud Connection.....	12
Figure No 9. IOT connection.....	12

Figure No 10. DHCP Server Office.....	13
Figure No 11. HTTP Details.....	14
Figure No 12.DNS	15
Figure No 13. FTP Office Server.....	16
Figure No 14. Blocking Connection From HR to Management.....	17
Figure No 15. Ping From Logistics3 to CustomerSupport Main and Finance Main.....	17
Figure No 16. Ping from Logistics3 to HR Main.....	18
Figure No 17. Peer to Peer Connection Successful.....	18.

Figure No 18. IP Address List.....	19
Figure No 19. DHCP Server connection to the PC in IT Department.....	20
Figure No 20. Setting the DHCP Server.....	21
Figure No 21. DHCP IP Configuration for IT1	22
Figure No 22.DHCP IP Configuration for IT2 and IT3.....	22
Figure No 23.DHCP IP Configuration for IT4 and IT5.....	23
Figure No 24.IoT DNS.....	24
Figure No 25.Office DNS.....	25
Figure No 26.HTTP configured page.....	26
Figure No 27. Index page configured through HTTP.....	27
Figure No 28. Running index.html	28
Figure No 29. Running FTP for username Nelly in IT4.....	29
Figure No 30. Making a file in IT4 for FTP.....	30
Figure No 31. Adding the file in the directory.....	31
Figure No 32.File addition in the Server.....	32

Figure No 33.Access Control Code in Router.....	33
Figure No 34. Ping Blocked by ACL	34
Figure No 35. IoT Server	35
Figure No 36.IoT Router.....	37
Figure No 37.IoT Registration.....	38
Figure No 38.Light IOT.....	39
Figure No 39.Smoke Detector IOT.....	40
Figure No 40.IoT Tablet.....	41

Acronyms

IoT: Internet Of Things
DHCP: Dynamic Host Configuration Protocol
HTTP: Hypertext Transfer Protocol
DNS: Domain Name System
FTP: File Transfer Protocol
IP: Internet Protocol
LAN: Local Area Network
ACL: Access Control List
PC: Personal Computer
MAC: Media Access Control

1. INTRODUCTION

Network has become very crucial and important in this day and age. This is not restrained just to personal communication, but communication in general which virtually connects everything right from business communication to media communication along with connecting the Internet to the world. Network plays a huge role and has long been understood by business professionals. When focusing on enterprise networking we see the in-depth role of networking with regards to actively being a mode of connectivity that actively connects all the departments or the sections of a company or an establishment. Networking has also played a huge role in connecting different branches of an establishment through secured channels.

1.1 Aim of the Project

This paper represents the design and implementation of the Network and System Project: **Building and deploying a Company Network with the implementation of System Administration Technologies focused on security and active communication between departments along with deployment of IoT technology through Cloud.**

The aim of this project is to demonstrate an entire company system with different departments and how security and active communication is achieved between the departments. The project also focuses on different networking scenarios between departments that ultimately lead to a streamlined and structured premise.

1.2 Scope of the project

The project describes the creation and deployment of a Company Network that is capable to support complex tasks and implementation of system administration and other technologies such as Hypertext Transfer Protocol (HTTP), Domain Name System(DNS), Dynamic Host Configuration Protocol(DHCP), File Transfer Protocol(FTP), Access Control List along with Internet of Things (IoT) to manage the entire company structure through the cloud.

1.3 Approach used in carrying out the project

The project is based on understanding the current deployment of the network in today's companies. A disciplined approach was instrumental to understanding

the different Administration and Routing technologies along with the Internet of Things that can streamline and help the companies work more efficiently.

2. Background

As discussed in the aim of the project, the focus of this project is building a Company Network. This network is deployed and shown through Cisco Packet Tracer. The Cisco Packet Tracer Version No.8 is used for this Project. Deploying a computer network and exploring the different technologies was made possible through Cisco Packet Tracer. Building a Company Network will help the management, as well as the other departments, work in an efficient way based on the networking and system administration technology required for the department to function.

3. Technologies used in the project

1. DHCP: DHCP is also known as dynamic host configuration protocol. DHCP is a network protocol used on IP networks wherein automatic assigning of IP address and other information to every host is made through the DHCP server so that it can communicate effortlessly without any further endpoints.

2. DNS: DNS stands for Domain name system and is a grouped and circulated naming system represented for Personal Computer services. DNS naming system is also used for resources that have a connection to a private network or the Internet

3.HTTP: HTTP stands for Hypertext Transfer Protocol. It is the basic fundamental base of the World Wide Web. Using hypertext links, Hypertext Transfer Protocol is operated to load web pages. HTTP is an application layer convention used to move any data between arranged gadgets.HTTP runs on top of different layers of the organization convention stack.

4.FTP: FTP stands for File Transfer Protocol. It's additionally probably the most seasoned convention being used today and is a helpful method to move documents around. FTP is the least difficult and most regular approach to transfer files over the Web.

5.ACL: ACL stands for Access control list. ACL consists of rules set out for managing and handling traffic in a network and decreasing network breaches. A set of rules are defined for outgoing and incoming networks by the ACL. After

defining the rules the ACL filters the traffic in the network.

6. IoT: IoT stands for Internet of Things, or IoT. IoT also helps connect billions of physical devices over the internet for network sharing and communication. IoT is helping to make our world more smarter and responsive merging the physical and virtual worlds.

7. Cloud: Cloud which is also known as Cloud networking, gives users access to networking resources. IoT connects the physical machines to the virtual resource through a third-party centralized system. A cloud network makes an institution deliver more rapidly and securely bearing minimum cost.

8. Peer to Peer Connection: Peer to Peer Connection also known as P2P connection is a networking system that lets a host communicate with another host inside the same network.

3.1 Similar Technologies/System

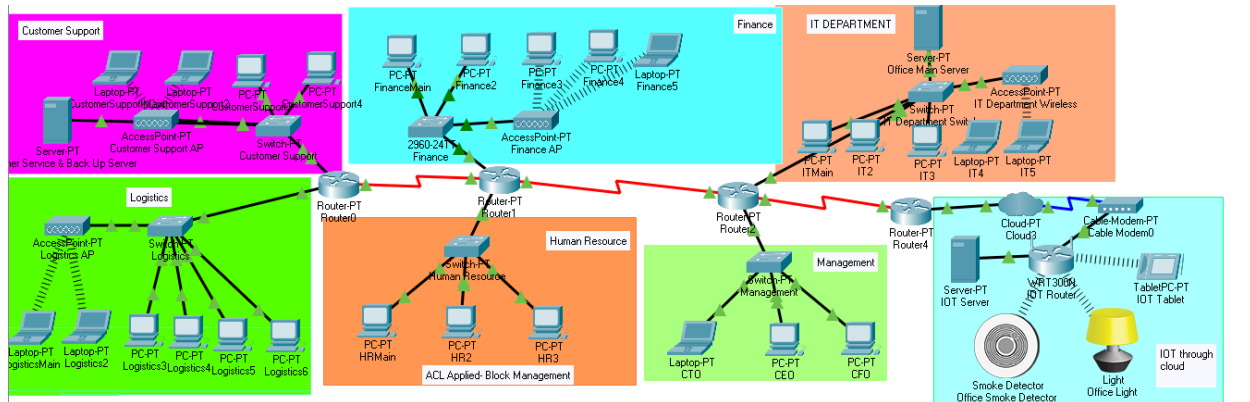
These are some of the Technologies that perform the same task as that of Cisco Packet Tracer as well as the Technologies mentioned above in 3.

1. GNS3: GNS3 which is also known as Graphical Network Simulator-3. This is a network simulator tool that was released in 2008. Gns3 is a network simulation tool that allows us to get software images from various vendors and we can import the software images into Gns3. It can run on multiple OS and also PC and different OS are supported with the software these include Windows, Linux, and macOS X

2. Google Cloud Platform: GCP stands for Google Cloud Platform. GCP has a variety of systems to offer which include compute, storage, networking, Stackdriver for everything DevOps, tools, big data, and artificial intelligence.

4. Technical Description

We have taken into consideration Cisco Packet Tracer as our software to build and deploy the network architecture along with deploying various systems technologies associated with it.



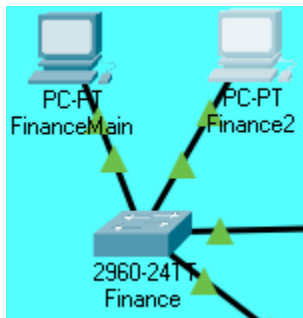
(Figure No 1. Network Architecture)

Figure No 1 represents the entire Network Architecture for our Company Network. Here we see that there are five departments which are Customer Support Department, Finance Department, IT Department, Logistics Department, HR Department and Management and a separate IOT base. We also see that there are 4 Routers that are connected through LAN cables. These Router cables have separate Switches which connects and joins with their respective department. We also see cloud networks connected to these routers which then connect to a wireless router connecting it remotely through the IOT section. Each component will be described individually in the next sections. We also have two servers which are Office Main Server(which handles the connection of the entire network) and the other one is the IOT server.

4.1 PC, Laptop & Tablet

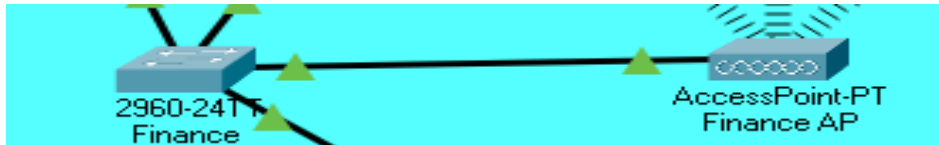
For our Machines we have visually shown connections through a PC, a laptop that can be connected in a wired or wireless manner and a Tablet that can be connected in a wireless manner. Individual IP address is assigned to this PC in a Static and DHCP manner based on the

4.2 Switches, Routers, and Modem



(Figure No 2. Switch Example)

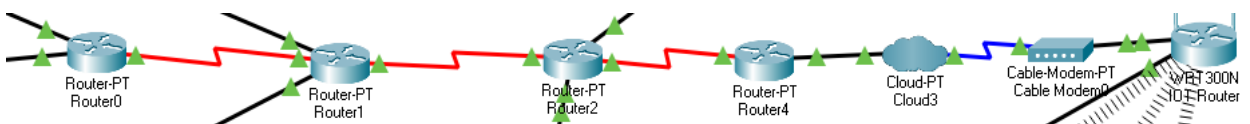
Figure No 2 Represents a switch from our Finance department. A switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. This switch is internally connected with the router which allows the travel of packets from a source to a destination.



(Figure No 3. Switch Connected to Wireless Access Point)

Switches can't connect to devices in a wireless manner, for this purpose we have attached Access Point which is a Wireless Switch.

In Figure No 3 we see a Router being connected to a Wireless Access point.



(Figure No 4. Routers)

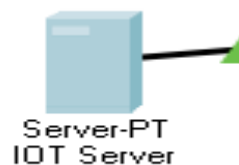
Figure No 4 talks about the Router configuration wherein we see the routers connected to each other through serial port. We have used a RIP configuration which eases and makes it easier for the packet travelling between these routers.

4.3 Server



(Figure No 5. Office Server)

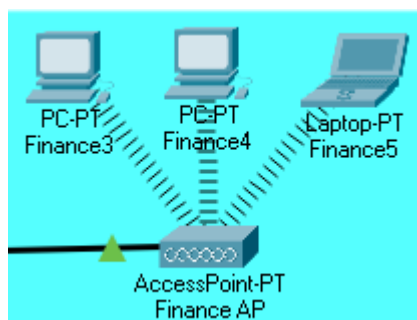
Figure No 5. Represents the first server in our office which handles all the networking responsibility of the main office along with all its departments. All the system administration tasks are handled through this server.



(Figure No 6. IoT Server)

Figure No 6. Represents the second server which is our IOT server which is connected to this network through the cloud .

4.4 Access Point

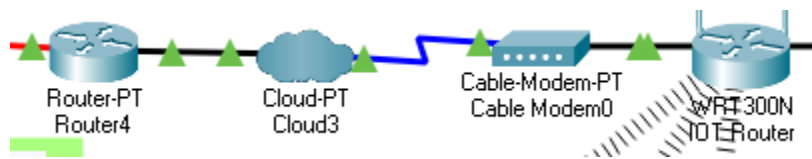


(Figure No 7. Access Point Connected to PC)

A wireless access point (WAP) is a networking device that allows wireless-capable devices to connect to a wired network.

In Figure 7. We see the Access Point in the Finance Department which connects the PC and Laptop Wirelessly, helping the packets to travel wirelessly.

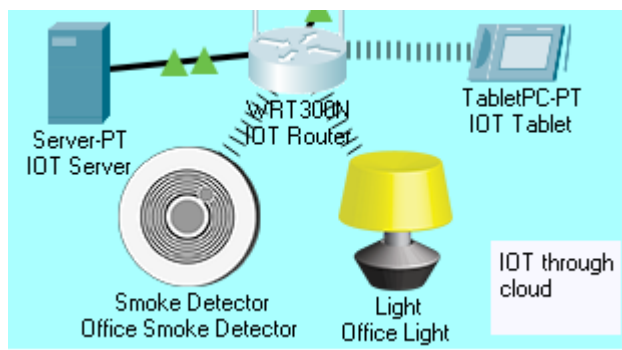
4.5 Cloud Network



(Figure No 8. Cloud Connection)

Figure No 8. represents the Cloud connection. Here we see that the Router 4 is connected through the Cloud and then through a cable modem this cloud is connected to a Wireless Router.

4.6 IOT



(Figure No 9. IOT connection)

4.7 DHCP

Office Main Server

Physical Config **Services** Desktop Programming Attributes

SERVICES

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

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 191.168.1.1

DNS Server: 191.168.1.4

Start IP Address: 191 168 1 1

Subnet Mask: 255 255 0 0

Maximum Number of Users: 512

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

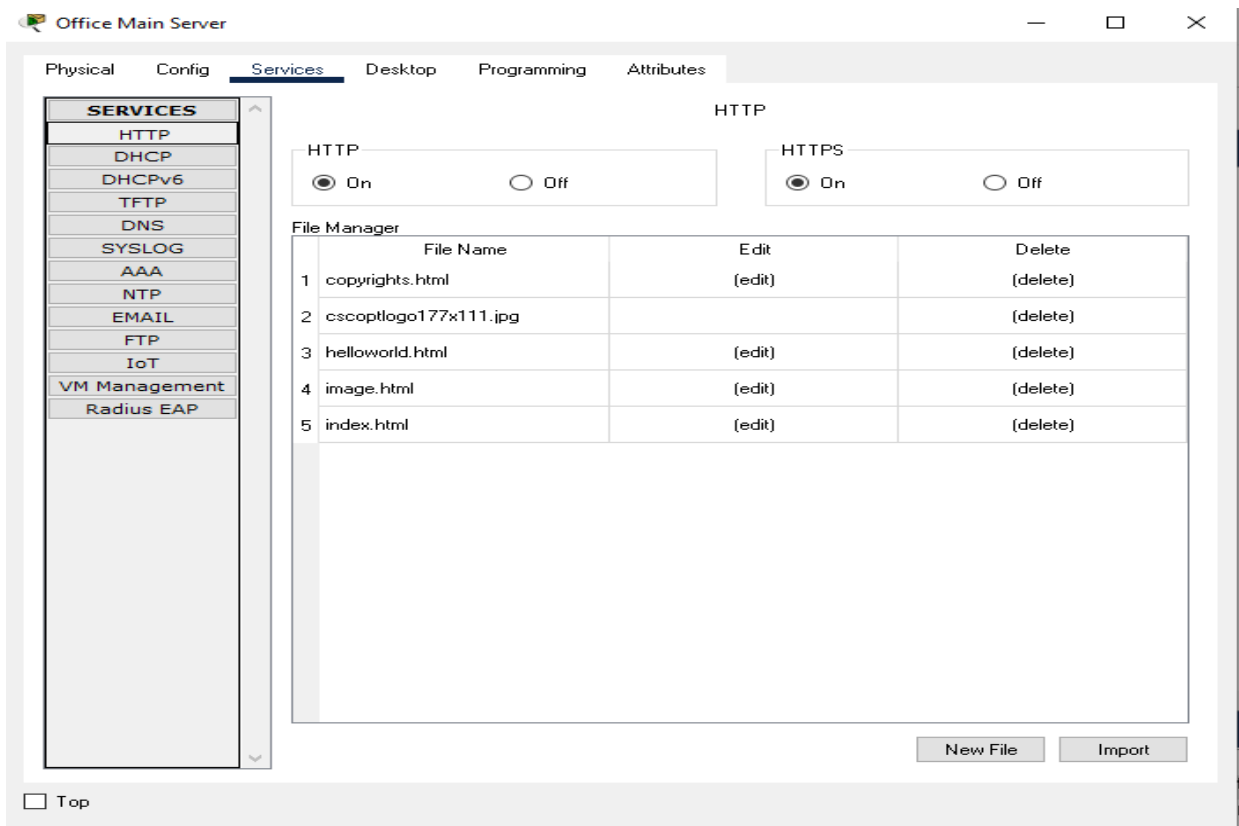
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	191.168.1.1	191.168.1.4	191.168.1.1	255.255.0.0	512	0.0.0.0	0.0.0.0

☐ Top

(Figure No 10. DHCP Server Office)

In figure 10. We have configured DHCP to the Office Main Server. We have configured the Start IP address to 191.168.1.1.

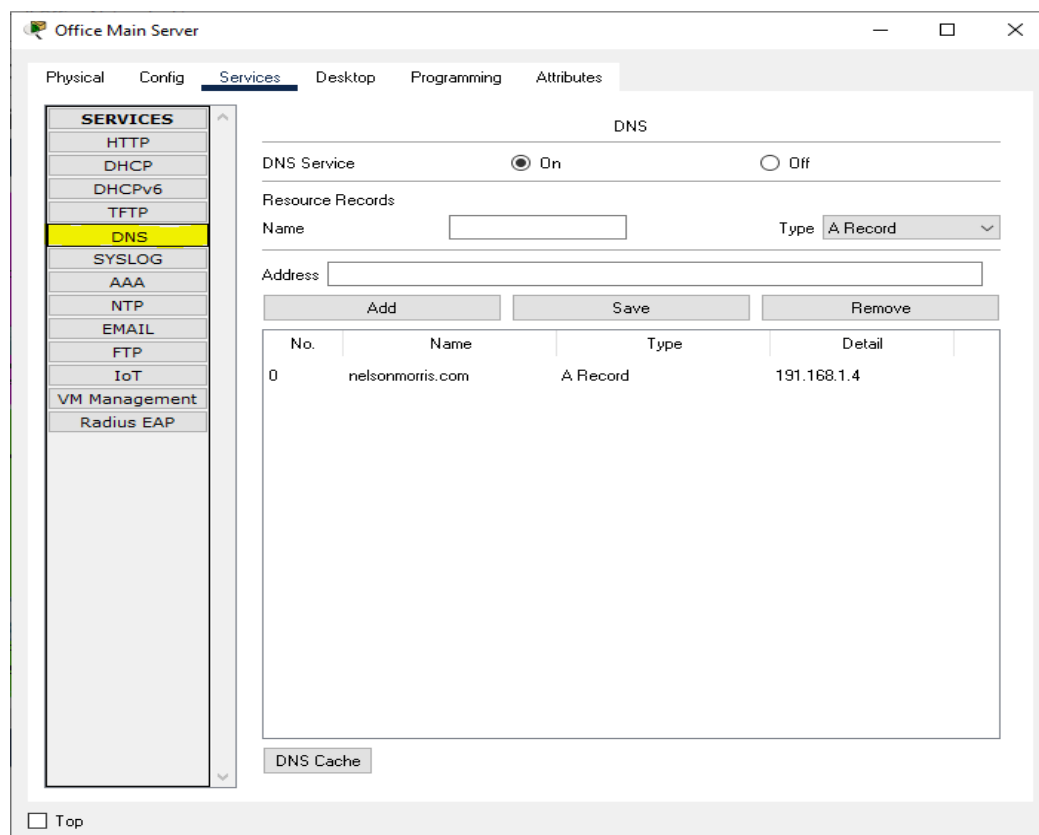
4.8 HTTP



(Figure No 11. HTTP Details)

In this figure we see HTTP service has been turned on and is configured to the Office Main Server. We will get in detail in the File Manager section in the Testing Part.

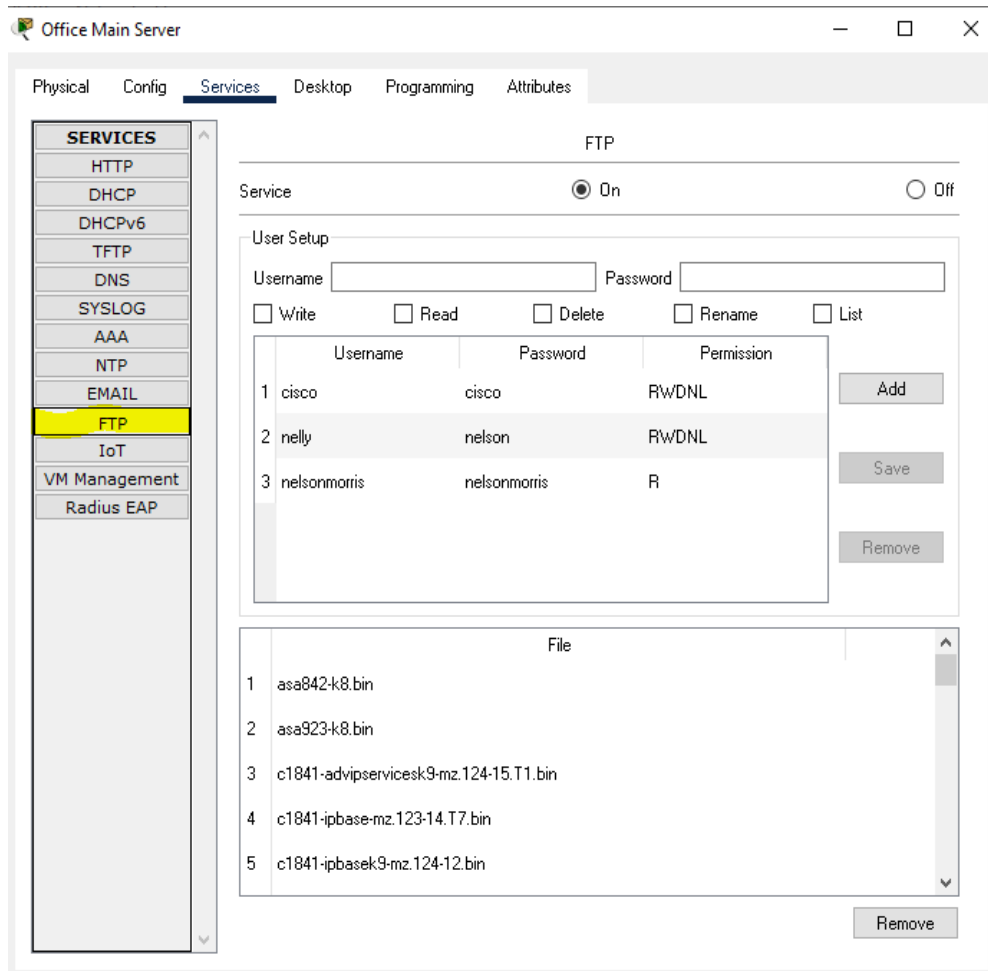
4.9 DNS



(Figure No 12.DNS)

Figure No 12. Depicts the DNS getting configured with name as nelsonmorris.com and a gateway for other machine configured with IP address 191.168.1.4

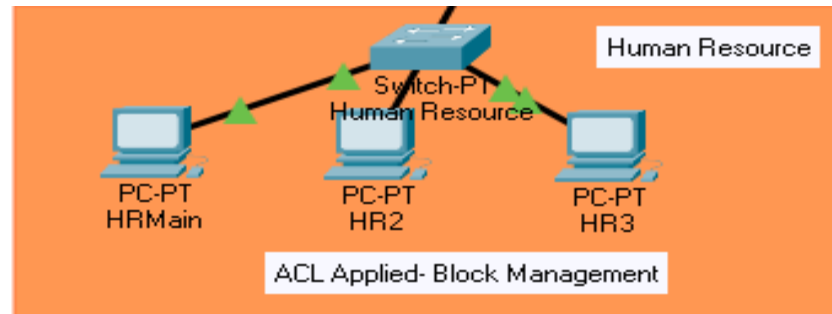
4.10 FTP



(Figure No 13. FTP Office Server)

FTP has also been configured in the Office Server and for this project we have made two users with different permissions. We will get in detail on this aspect in the Testing and Evaluation section.

4.11 ACL



(Figure No 14. Blocking Connection From HR to Management)

For this project we have applied for an ACL in the HR department which blocks transfer of any files to the Management department. We will get in detail on this aspect in the Testing and Evaluation section.

4.12 Peer to Peer Connections

```

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.0.2: bytes=32 time=419ms TTL=126
Reply from 192.168.0.2: bytes=32 time=2ms TTL=126
Reply from 192.168.0.2: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 419ms, Average = 143ms

C:\>ping 1.168.0.3

Pinging 1.168.0.3 with 32 bytes of data:

Request timed out.
Reply from 1.168.0.3: bytes=32 time=1ms TTL=127
Reply from 1.168.0.3: bytes=32 time<1ms TTL=127
Reply from 1.168.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 1.168.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

(Figure No 15. Ping From Logistics3 to CustomerSupport Main and Finance Main)

Peer to Peer connection depicts the transfer of files from one host to another anywhere in the department. Figure 15 depicts Logistics 3 PC pinging CustomerSupport Main and we see the connection and sending of packets was a success. We then see Logistics 3 PC pinging Finance Main and we see the connection and sending of packets was a success.

```

C:\>ping 126.168.3.2

Pinging 126.168.3.2 with 32 bytes of data:

Request timed out.
Reply from 126.168.3.2: bytes=32 time=1ms TTL=126
Reply from 126.168.3.2: bytes=32 time=31ms TTL=126
Reply from 126.168.3.2: bytes=32 time=2ms TTL=126

Ping statistics for 126.168.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 31ms, Average = 11ms

```

(Figure No 16. Ping from Logistics3 to HR Main)

Figure 16 depicts Logistics 3 PC pinging HRMain and we see the connection and sending of packets was a success.







Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	Logistics3	CustomerSu	ICMP		0.000	N	0
	Successful	Logistics3	FinanceMain	ICMP		0.000	N	1
	Successful	Logistics3	HRMain	ICMP		0.000	N	2

Figure No 17. Peer to Peer Connection Successful)

We see a report of the packets sent here giving a graphical view of the status of the packets.

4.13 IP address List

```

Customer Support Main:1.168.0.7
Customer Support 2:1.168.0.5
Customer Support3: 1.168.0.2
Customer Support 4:1.168.0.3
Logistics Main:128.168.1.2
Logistics 2:128.168.1.3
Logistics 3:128.168.1.4
Logistics 4:128.168.1.5
Logistics 5:128.168.1.6
Logistics 6:128.168.1.7
Finance Main:192.168.0.2
Finance 2:192.168.0.3
Finance 3:192.168.0.4
Finance 4:192.168.0.5
Finance 5:192.168.0.6
HR Main:126.168.3.2
HR 2:126.168.3.3
HR 3:126.168.3.4
IT Main:191.168.1.2
IT 2:191.168.1.3
IT 3:191.168.1.5
IT 4:191.168.1.7
IT 5:191.168.1.6
Tablet Pc:192.168.0.102
CTO:193.168.0.3
CEO:193.168.0.2
CFO:193.168.0.4
Office Main Server:191.168.1.4
IOT Server:192.168.0.103

```

(Figure No 18. IP Address List)

Figure 18. Shows all the IP addresses for this network.

5. Project Testing and Evaluation

Building a Company Network in Cisco Packet tracer depicts the entire architecture of the system in a systematic and graphical manner. This project focused on efficient communication and handling of resources between the departments. Focusing on the real world scenario of the companies this project tried to highlight the shortcomings in companies which includes communication and security, these areas were concentrated on in this project.

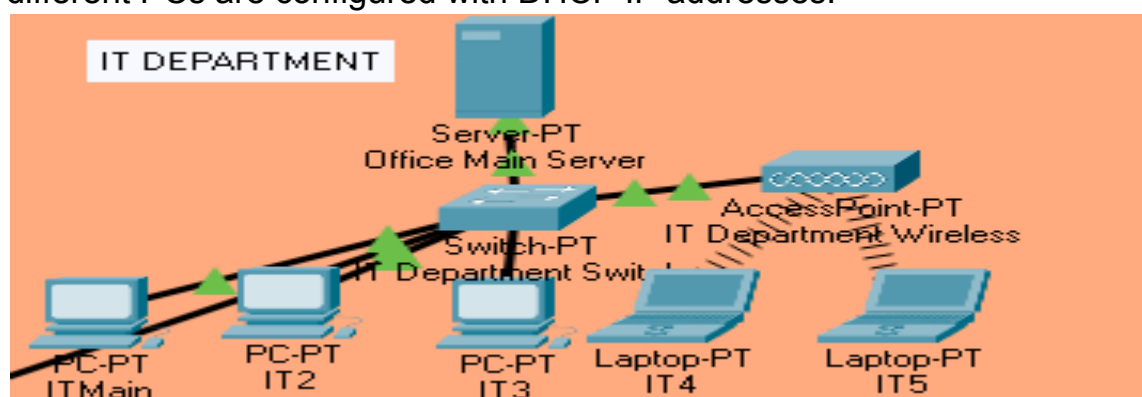
On critically evaluating the project we see the interaction between various departments through different routers, the project lacks in security between these routers which will choke the possibility of a breach or error while messages or any communication is transferred between the hosts from any department. However implementation of different technologies just through two servers limit the cost spared by the company for infrastructure. The use of cloud Networking in this project also extends the company to various technologies including IOT that makes the infrastructure of the company intelligent and reliable along with being cost-efficient.

6. Demonstration of the Company Network system

In this section various technologies of our company will be accessed with different situations and we will evaluate how the system accessed those tasks and provided a result.

6.1 DHCP

In this section we will show how DHCP is deployed in the IT Department and how different PCs are configured with DHCP IP addresses.



(Figure No 19. DHCP Server connection to the PC in IT Department)

Figure No 19 represents the office server connection to all the PCs.

Office Main Server

Physical Config **Services** Desktop Programming Attributes

SERVICES

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

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 191.168.1.1

DNS Server: 191.168.1.4

Start IP Address: 191 168 1 1

Subnet Mask: 255 255 0 0

Maximum Number of Users: 512

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

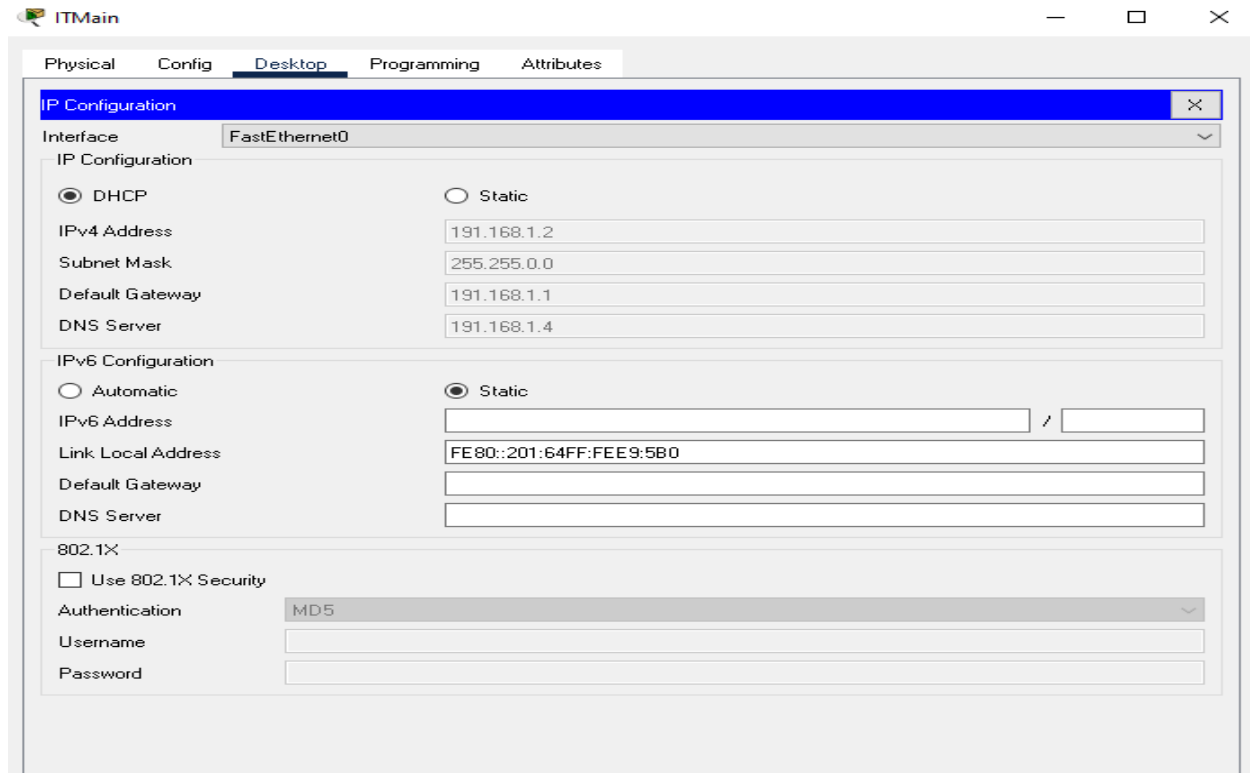
Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	191.168.1.1	191.168.1.4	191.168.1.1	255.255.0.0	512	0.0.0.0	0.0.0.0

☐ Top

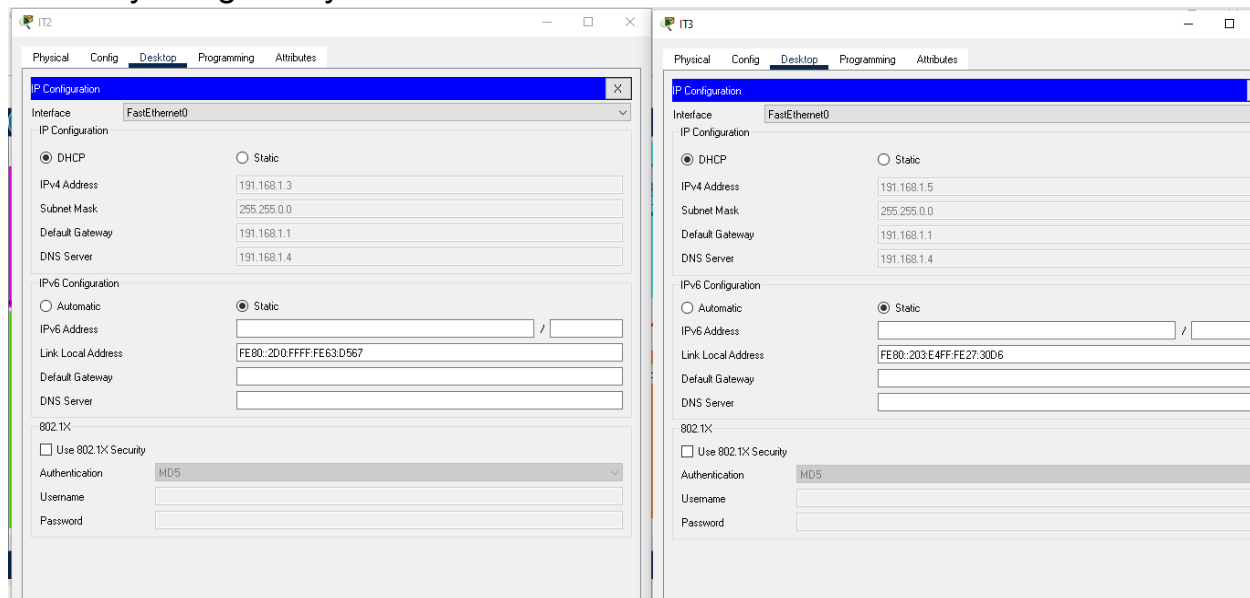
(Figure No 20. Setting the DHCP Server)

Figure 20. represents the IP address configured which will represent the start point of IP addresses for all the PCS which will be configured with this start IP address.



(Figure No 21. DHCP IP Configuration for IT1)

Figure No 21 represents the DHCP IP address configuration of IT1 which is randomly assigned by the Server.



(Figure No 22.DHCP IP Configuration for IT2 and IT3)

Figure No 22. represents the DHCP IP address configuration of IT2 and IT3 which is randomly assigned by the Server.

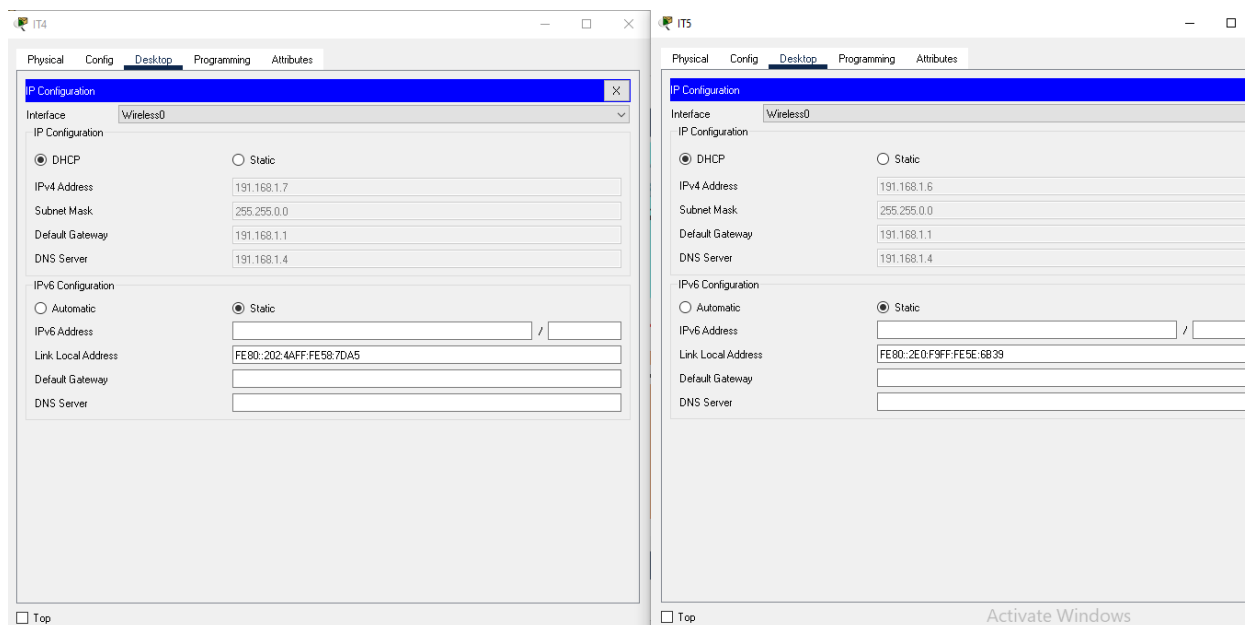
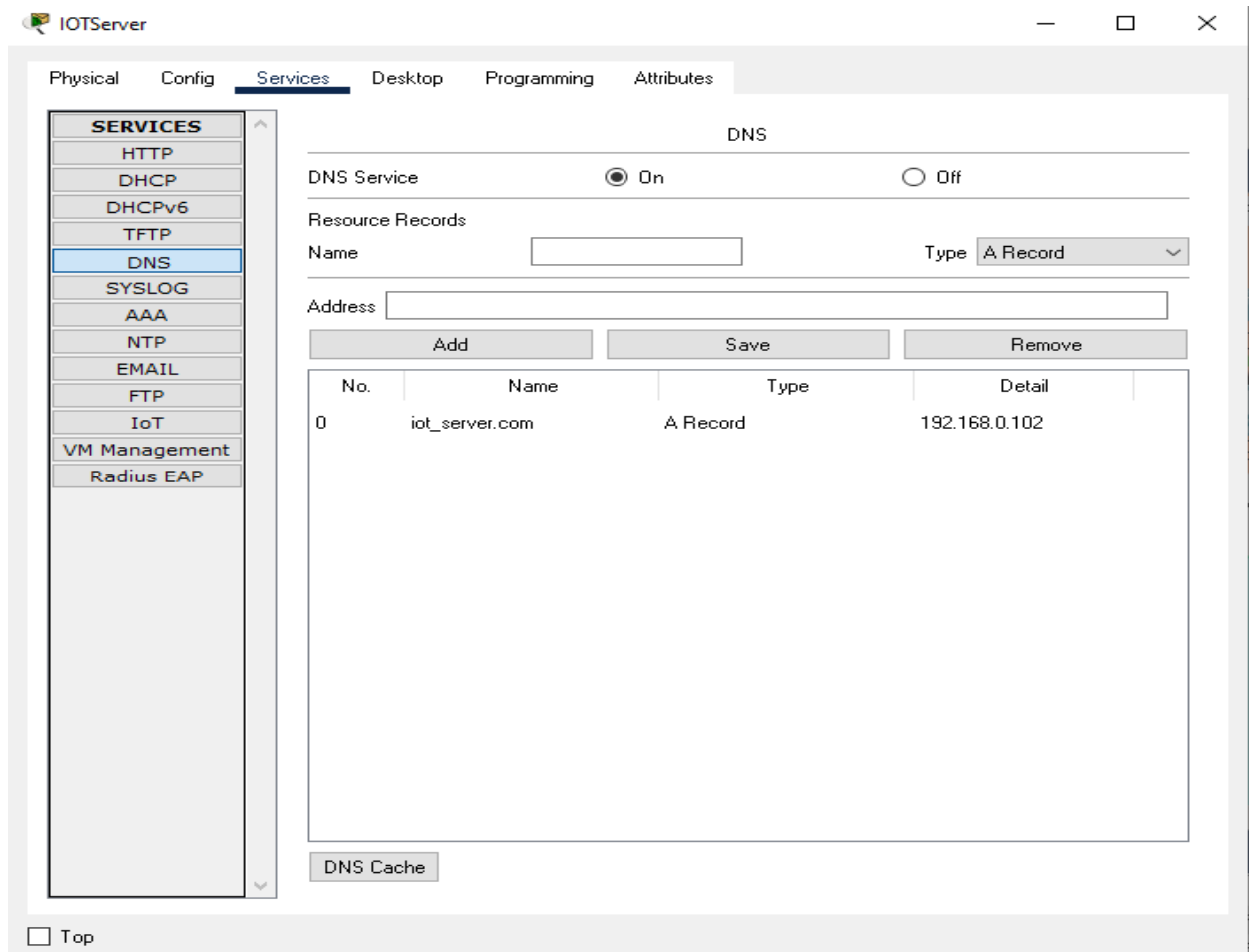


Figure No 23.DHCP IP Configuration for IT4 and IT5

Figure No 23. represents the DHCP IP address configuration of IT2 and IT3 which is randomly assigned by the Server.

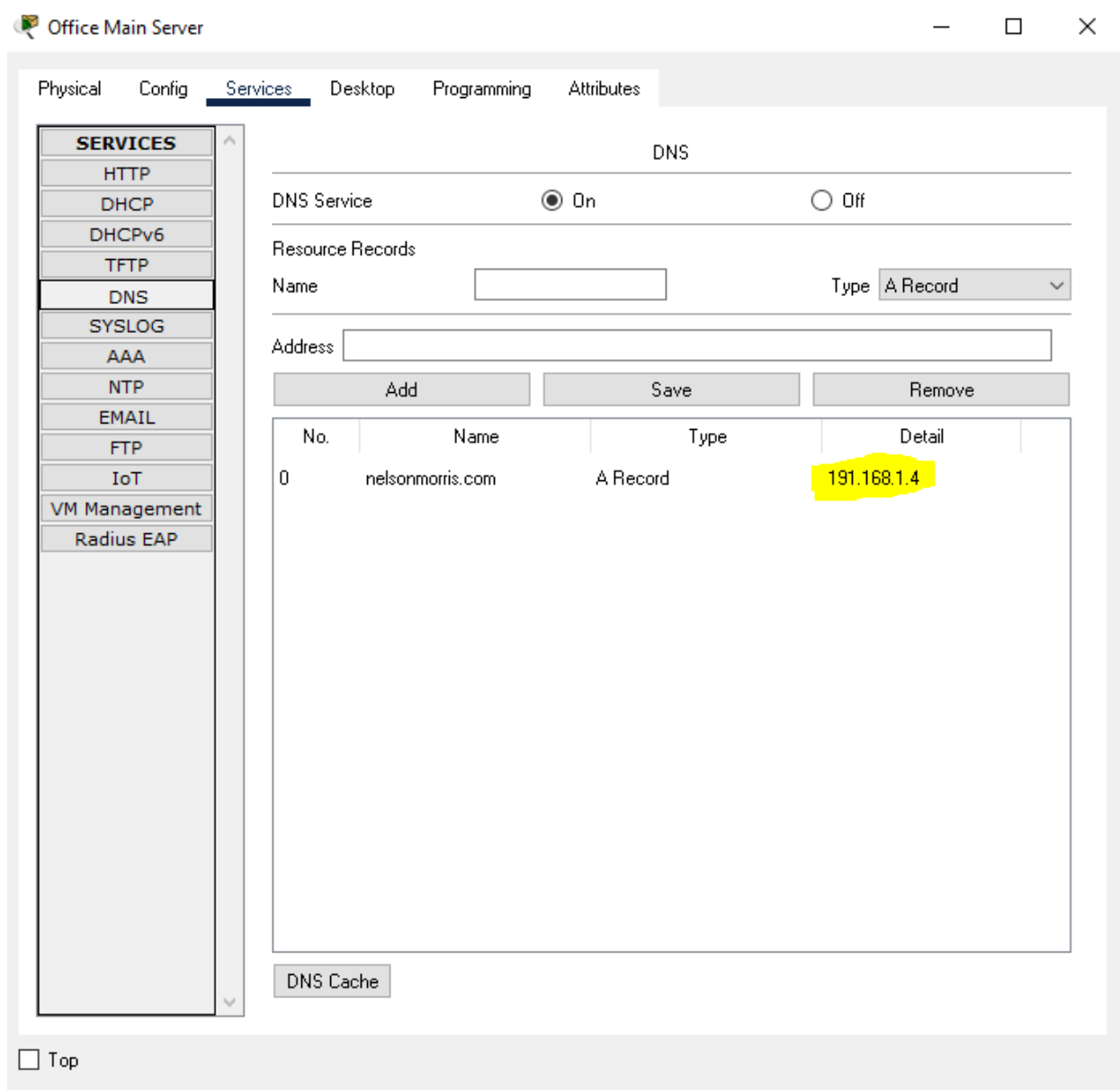
6.2 DNS

In this section we will see the configuration of the DNS server in both IOT server and Office Main Server. This DNS will act as a crucial part in assigning the gateway for HTTP and even FTP later in our demonstrations.



(Figure No 24.IoT DNS)

In Figure No 24. We have added a DNS name of `iot_server.com` for a gateway `192.168.0.102` that will be configured to the Machines automatically which will help the machines to use HTTP and even FTP technologies.

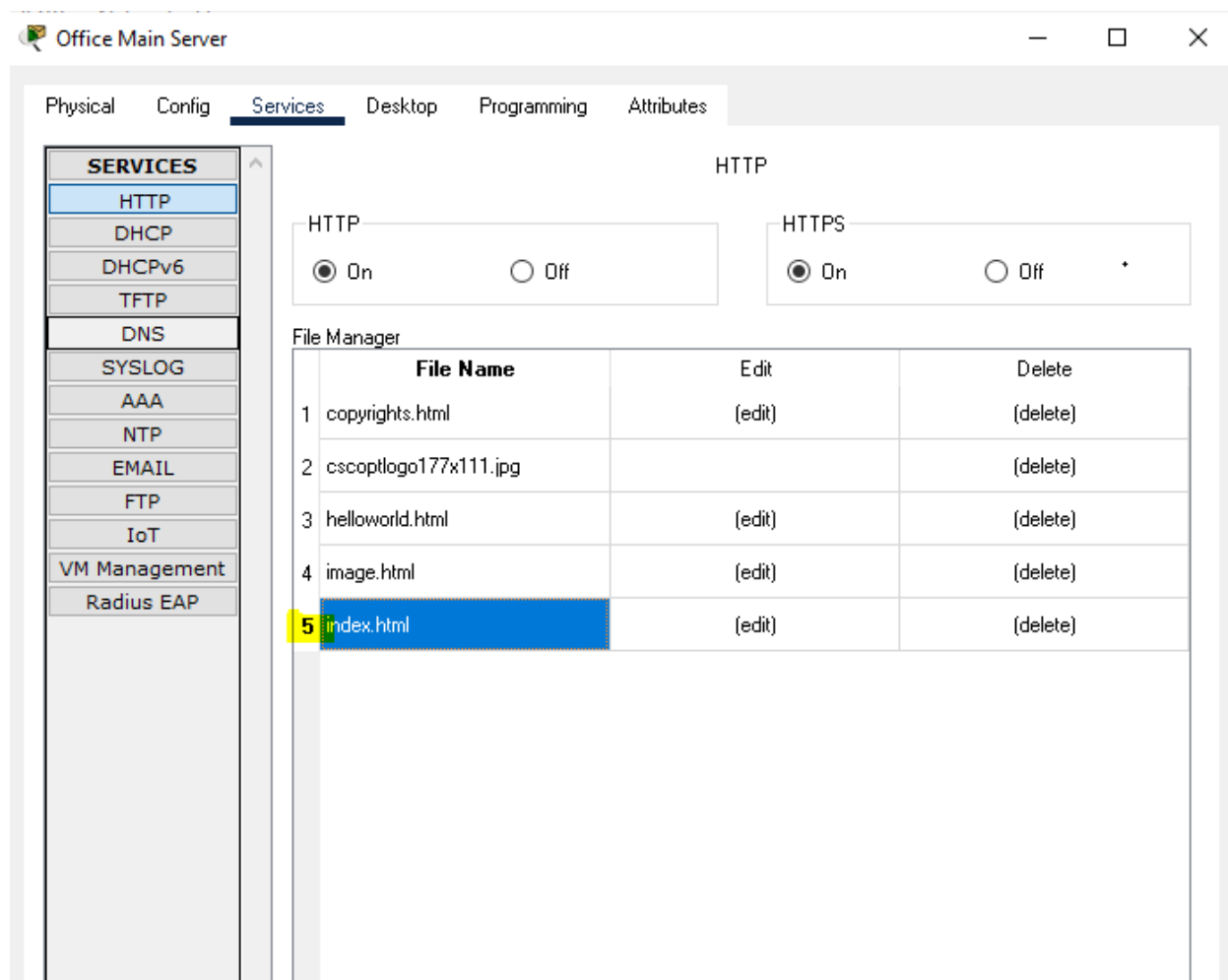


(Figure No 25.Office DNS)

In Figure No 25. We have added a DNS name of nelsonmorris.com for a gateway 191.168.1.4 that will be configured to the Machines automatically which will help the machines to use HTTP and even FTP technologies.

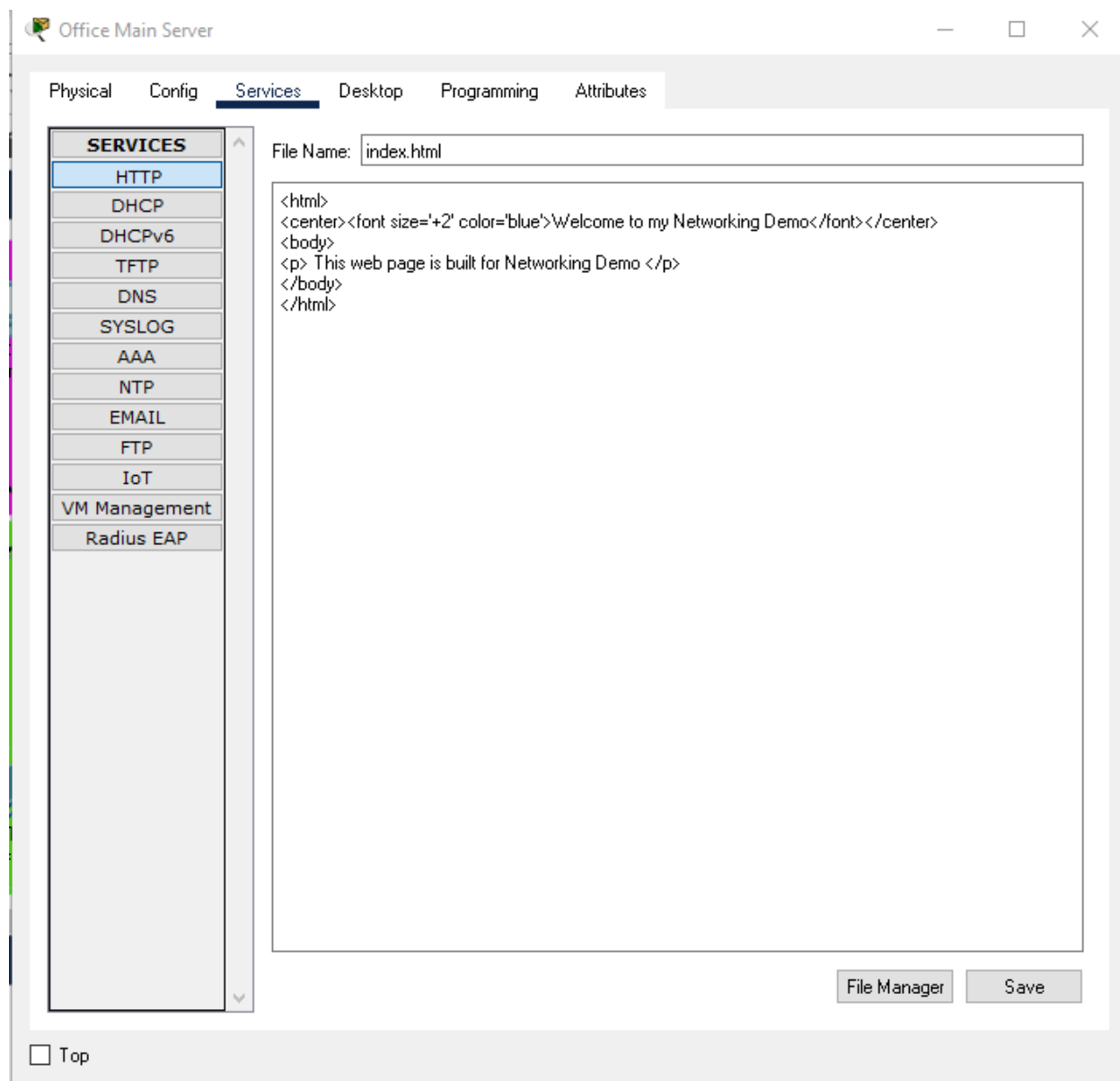
6.3 HTTP

In this section we will show how HTTP is configured and how different machines can access the Web. We have already configured DNS and DHCP in our network and all the PCS are configured with the same. We will now try to access the web through HTTP.



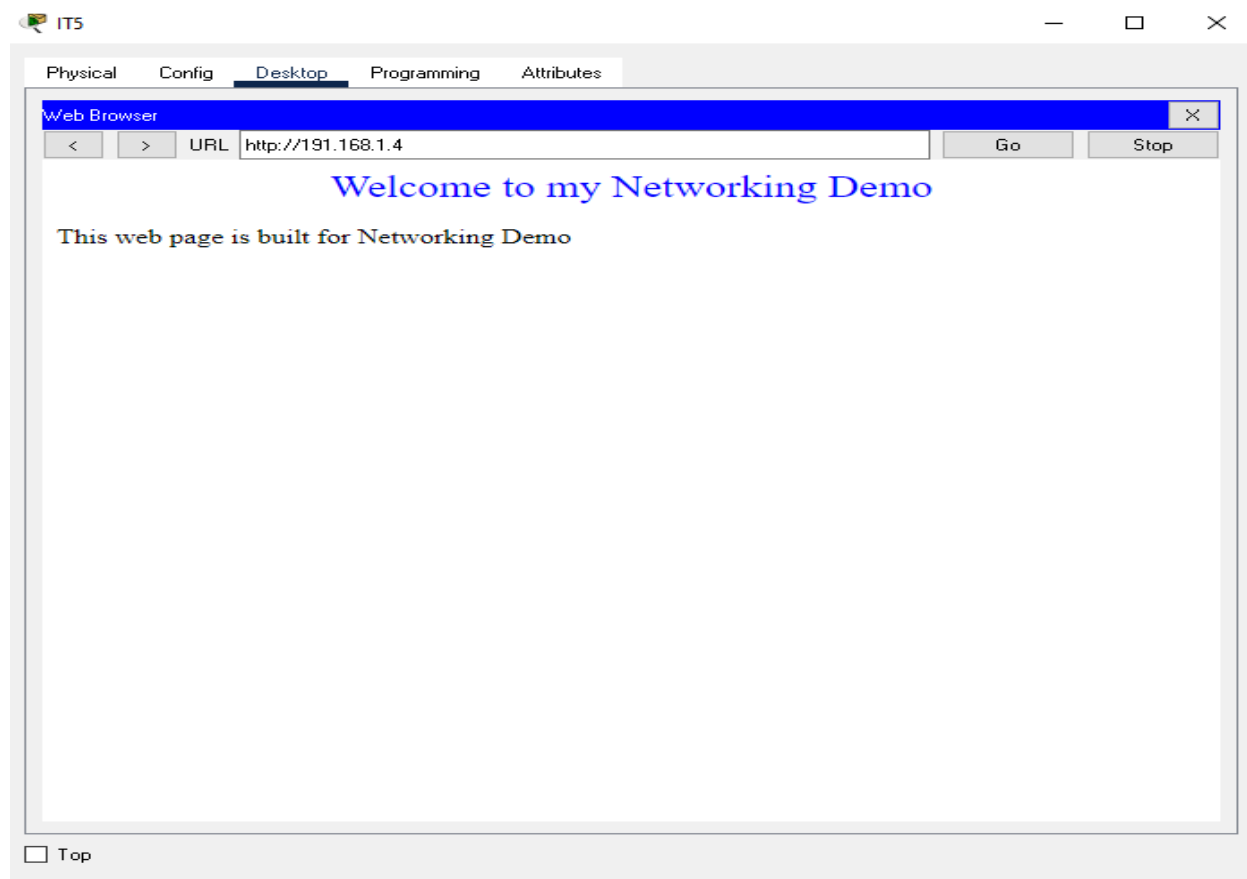
(Figure No 26.HTTP configured page)

Figure No 26. Depicts the file index.html which has been made for demonstration purposes.



(Figure No 27. Index page configured through HTTP)

Figure No 27. Depicts a web page created for demonstration purposes. This file will now be saved.



(Figure No 28. Running index.html)

Figure No 28. Represents the index page which is opened through our DNS server gateway which is 191.168.1.4 . We see that the file is running successfully in this domain hence providing web configuration through any machines.

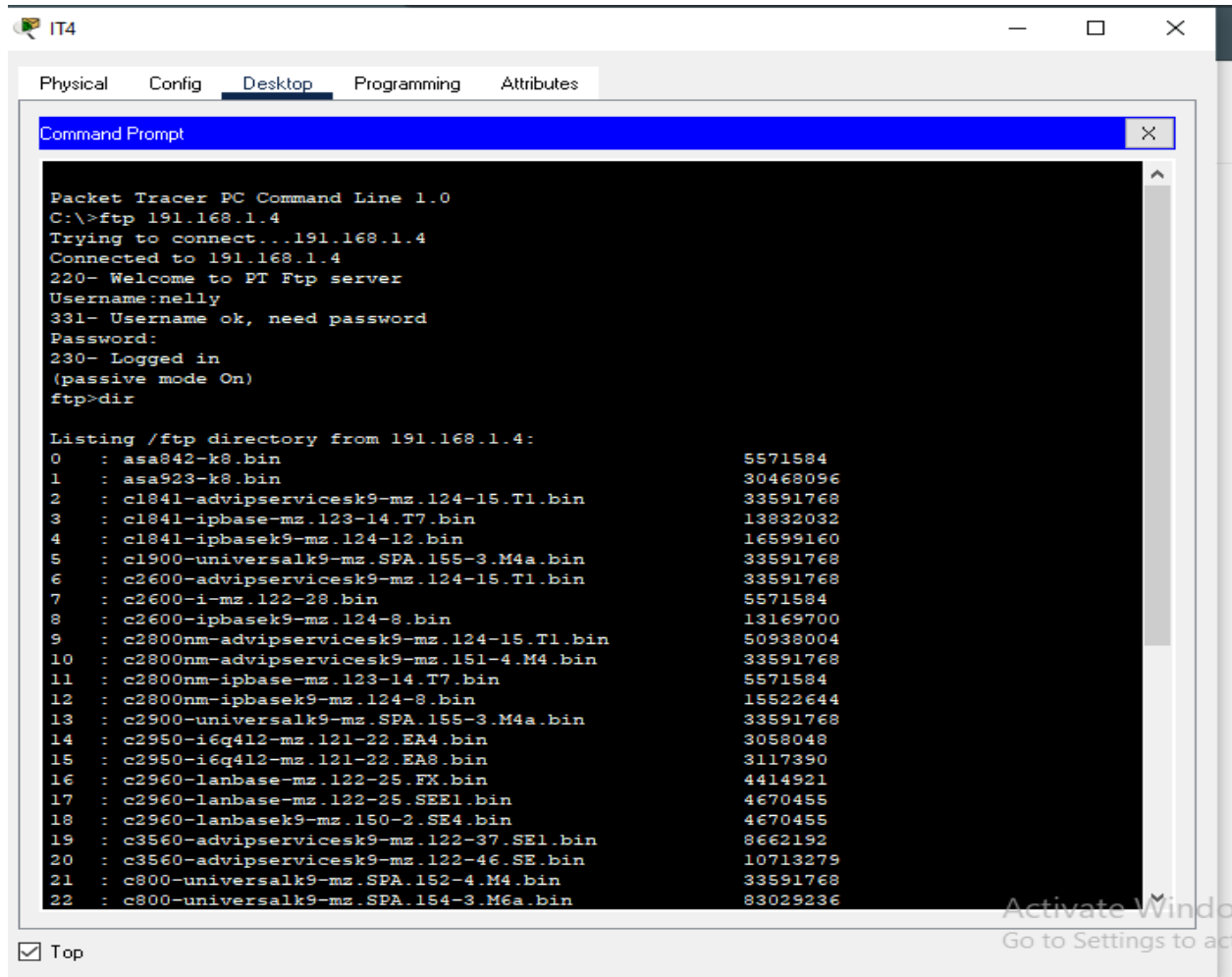
6.4 FTP

In this section we will add files into our server through our machine. This will be done through FTP. We have already set up two usernames which are depicted in Figure 13.

The first Username is nelly with permissions to RWDNL files directly in the directory of the server.

The second username is nelson morris with permission to (R) read the file from the server.

We will be demonstrating the FTP process with the username nelly for this project.



The screenshot shows a Packet Tracer PC Command Line window titled "IT4". The window has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, and a "Command Prompt" window is open. The command prompt shows the following text:

```

Packet Tracer PC Command Line 1.0
C:\>ftp 191.168.1.4
Trying to connect...191.168.1.4
Connected to 191.168.1.4
220- Welcome to PT Ftp server
Username:nelly
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

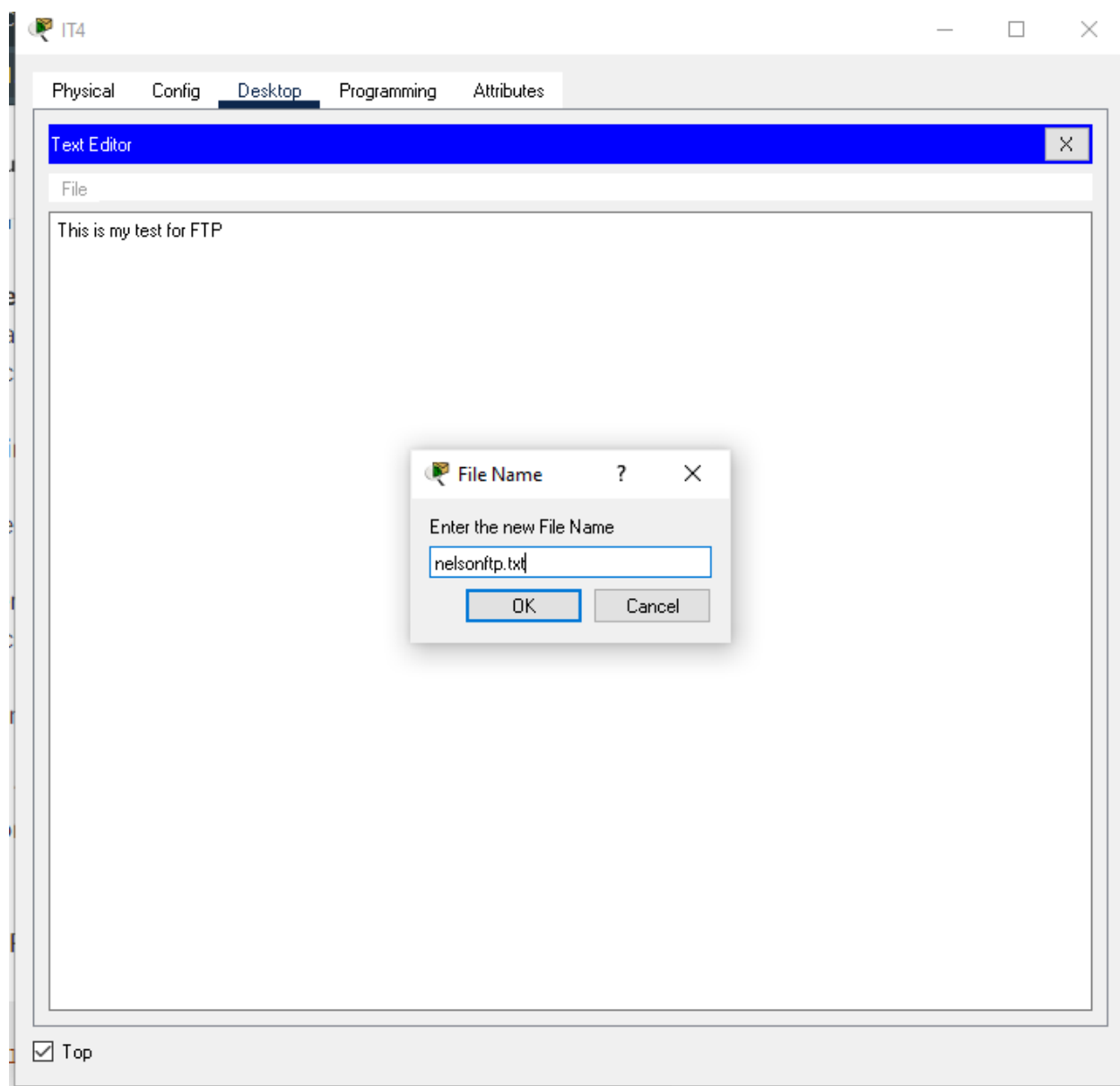
Listing /ftp directory from 191.168.1.4:
 0  : asa842-k8.bin                    5571584
 1  : asa923-k8.bin                    30468096
 2  : cl841-advipservicesk9-mz.124-15.T1.bin  33591768
 3  : cl841-ipbase-mz.123-14.T7.bin    13832032
 4  : cl841-ipbasek9-mz.124-12.bin     16599160
 5  : cl900-universalk9-mz.SPA.155-3.M4a.bin  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.M4a.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
15  : c2950-i6q412-mz.121-22.EA8.bin    3117390
16  : c2960-lanbase-mz.122-25.FX.bin    4414921
17  : c2960-lanbase-mz.122-25.SEE1.bin   4670455
18  : c2960-lanbasek9-mz.150-2.SE4.bin   4670455
19  : c3560-advipservicesk9-mz.122-37.SE1.bin  8662192
20  : c3560-advipservicesk9-mz.122-46.SE.bin  10713279
21  : c800-universalk9-mz.SPA.152-4.M4a.bin  33591768
22  : c800-universalk9-mz.SPA.154-3.M6a.bin  83029236

```

At the bottom of the window, there is a checkbox labeled "Top" which is checked.

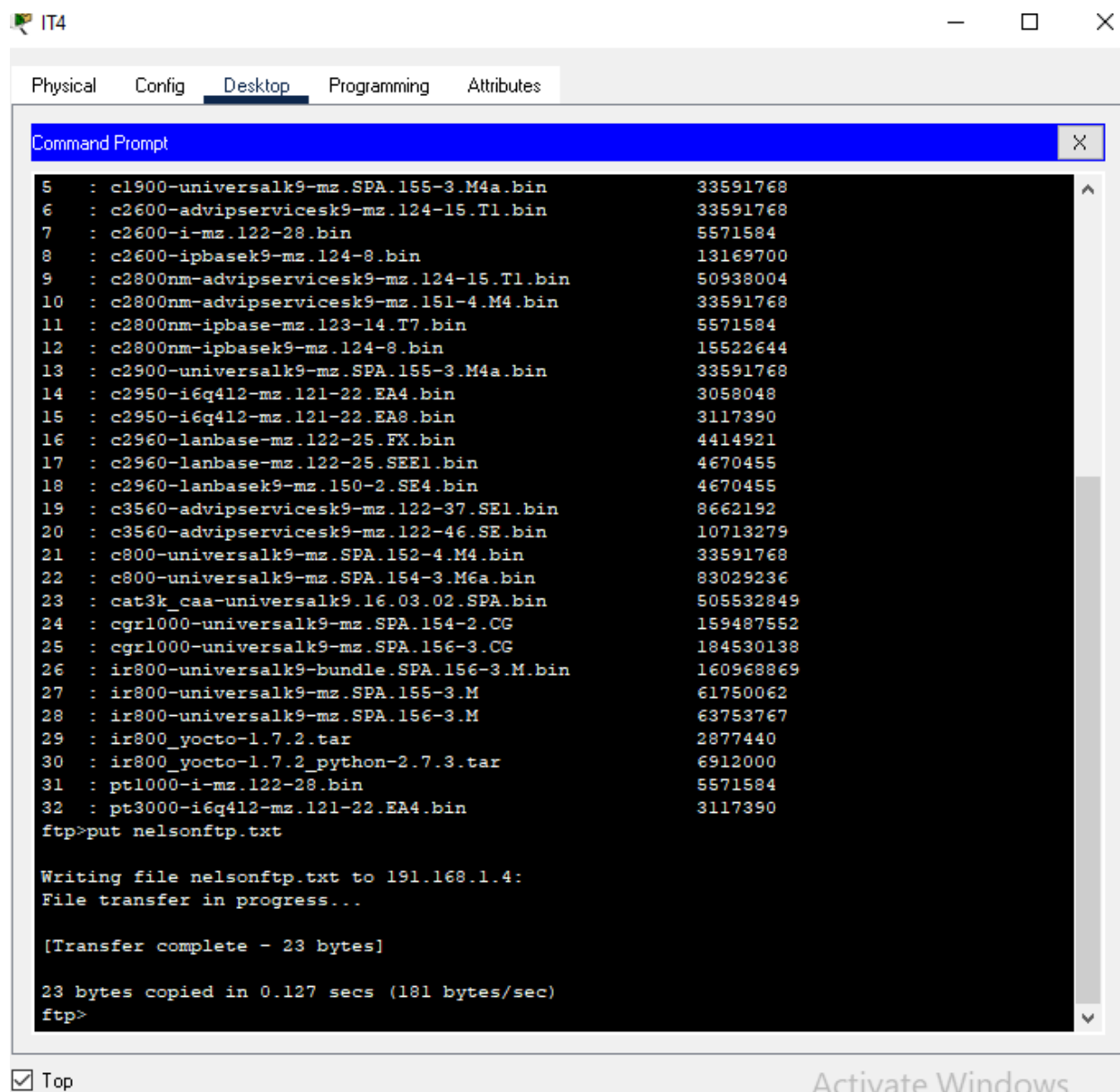
(Figure No 29. Running FTP for username Nelly in IT4)

Figure No 29. depicts the username nelly accessing the FTP server through IT4 PC. After logging in the user nelly can see the files in the directory. A new file will now be made which will be pushed into the server.



(Figure No 30. Making a file in IT4 for FTP)

A new file is created in the text editor section of IT4 which is depicted in Figure 30.



The screenshot shows a Windows Command Prompt window with a blue title bar. The window displays a list of files and their sizes, followed by a file transfer command and its output.

```

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
15 : c2950-i6q412-mz.121-22.EA8.bin 3117390
16 : c2960-lanbase-mz.122-25.FX.bin 4414921
17 : c2960-lanbase-mz.122-25.SEE1.bin 4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
19 : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
20 : c3560-advipservicesk9-mz.122-46.SE.bin 10713279
21 : c800-universalk9-mz.SPA.152-4.M4.bin 33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin 83029236
23 : cat3k_caa-universalk9.16.03.02.SPA.bin 505532849
24 : cgr1000-universalk9-mz.SPA.154-2.CG 159487552
25 : cgr1000-universalk9-mz.SPA.156-3.CG 184530138
26 : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
27 : ir800-universalk9-mz.SPA.155-3.M 61750062
28 : ir800-universalk9-mz.SPA.156-3.M 63753767
29 : ir800_yocto-1.7.2.tar 2877440
30 : ir800_yocto-1.7.2_python-2.7.3.tar 6912000
31 : pt1000-i-mz.122-28.bin 5571584
32 : pt3000-i6q412-mz.121-22.EA4.bin 3117390
ftp>put nelsonftp.txt

Writing file nelsonftp.txt to 191.168.1.4:
File transfer in progress...

[Transfer complete - 23 bytes]

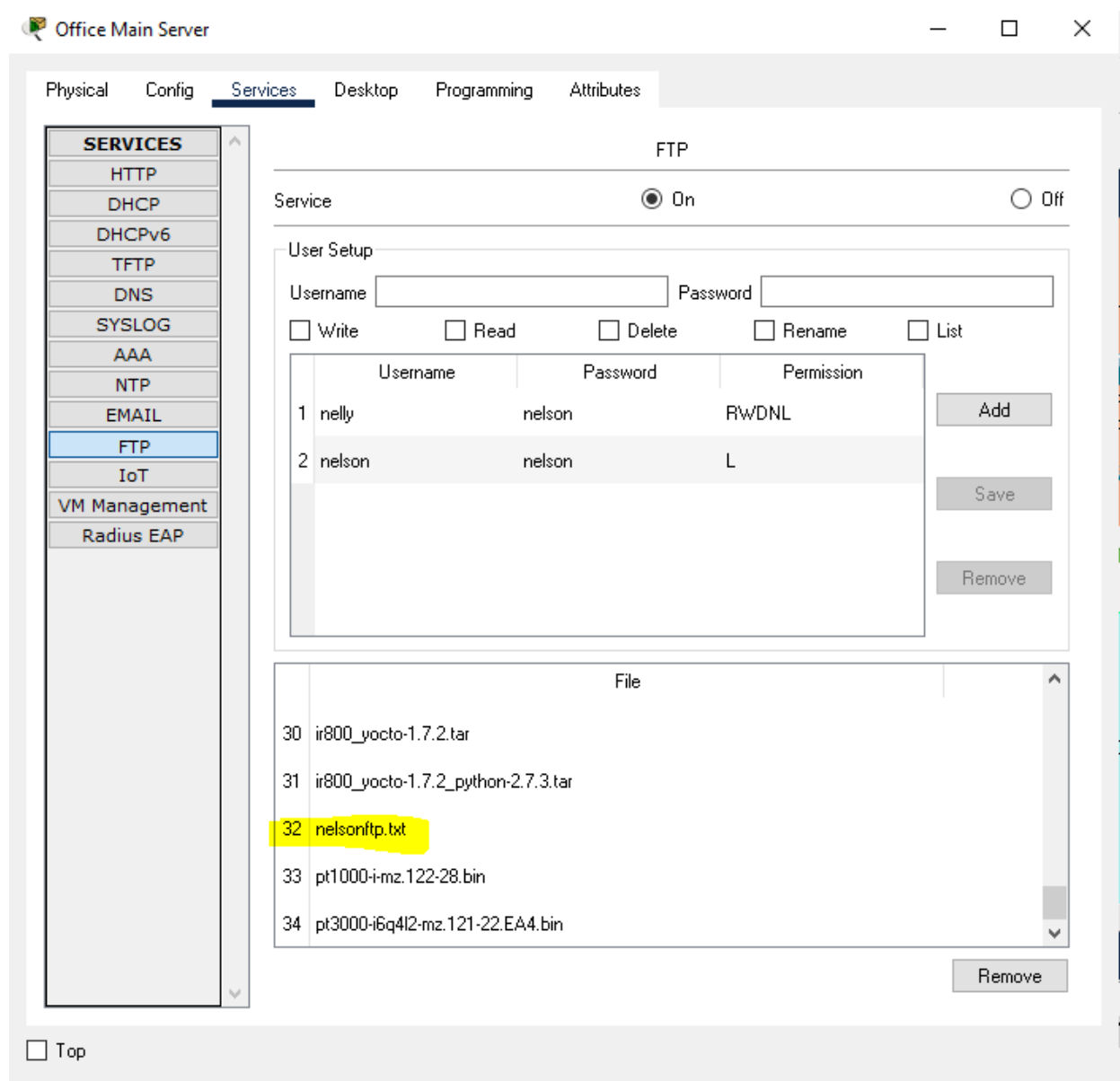
23 bytes copied in 0.127 secs (181 bytes/sec)
ftp>

```

At the bottom of the window, there is a checkbox labeled "Top" and a watermark that says "Activate Windows".

(Figure No 31. Adding the file in the directory)

After the creation of the file, the file is added to the server by the command `put nelsonftp.txt` which is depicted in Figure No 31.

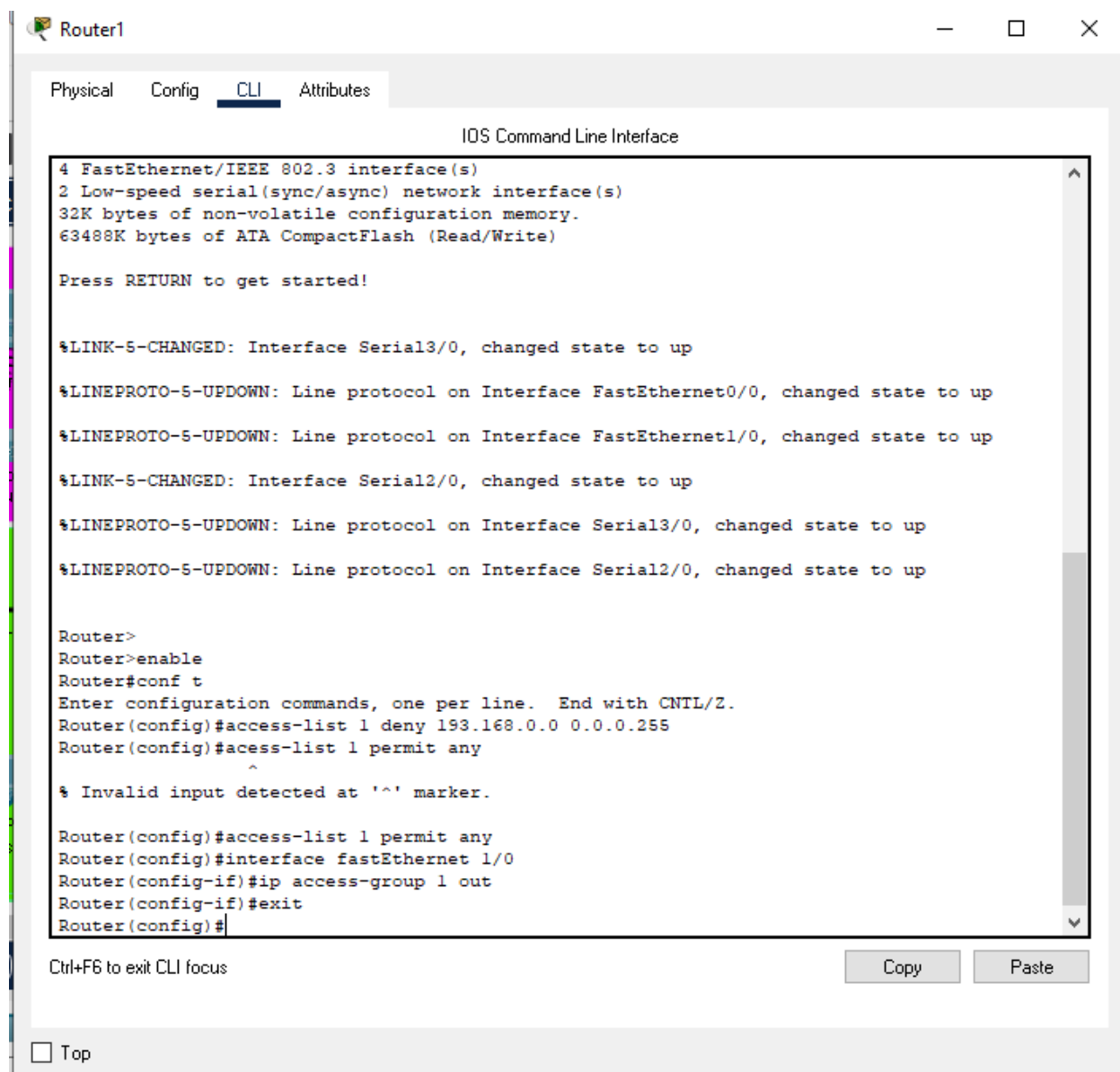


(Figure No 32.File addition in the Server)

In Figure 32. We see that the file nelsonftp.txt is added to the server. Thus depicting the completion of File Transfer Protocol.

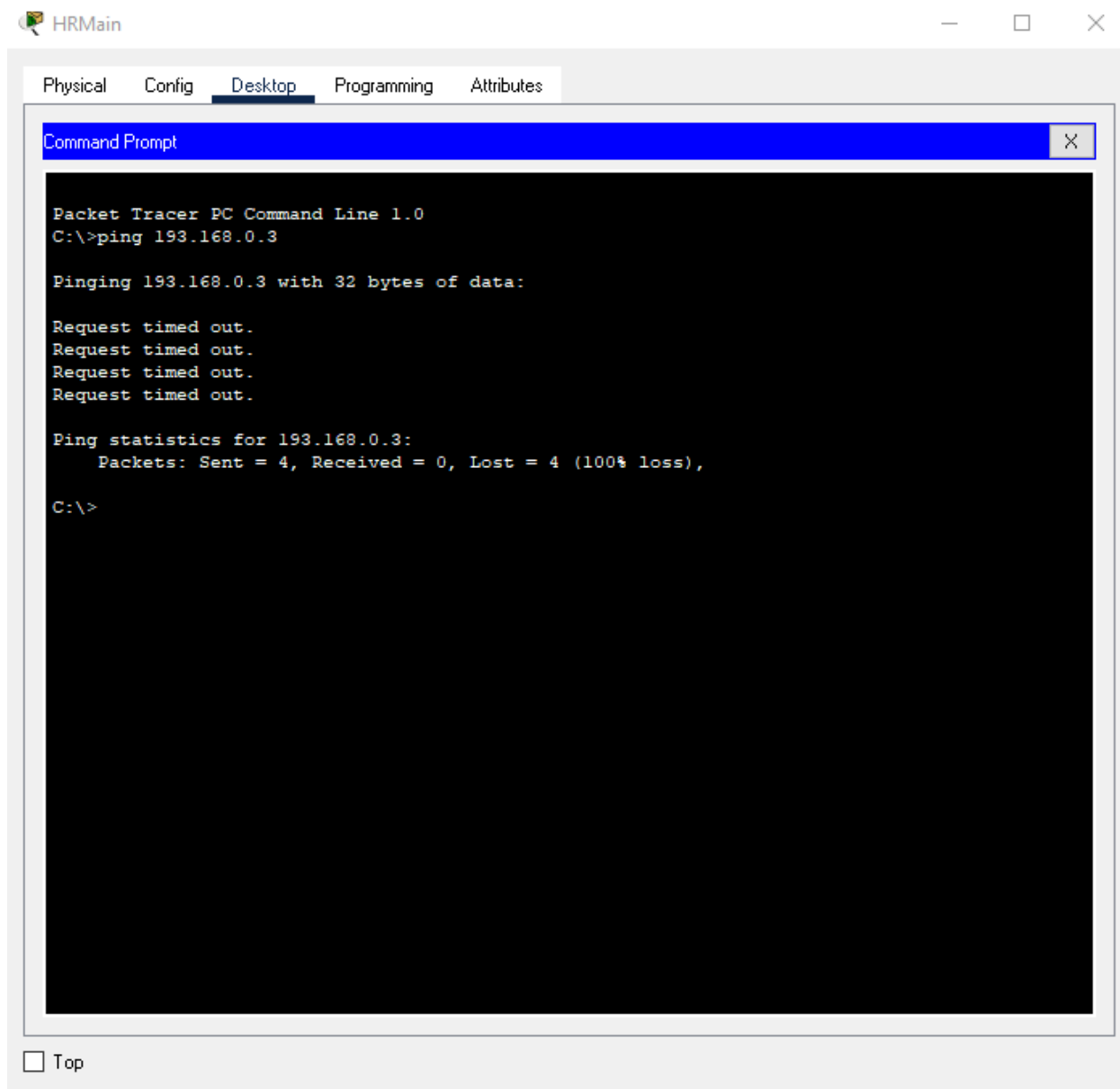
6.5 ACL

In this section will deploy ACL for our HR department which is depicted in figure No.14 . We will configure Router 1 of our network and block the connection between HR and Management.



(Figure No 33.Access Control Code in Router)

In figure No 33. We see that the Router is configured through CLI and that we block the management section through our Access list.

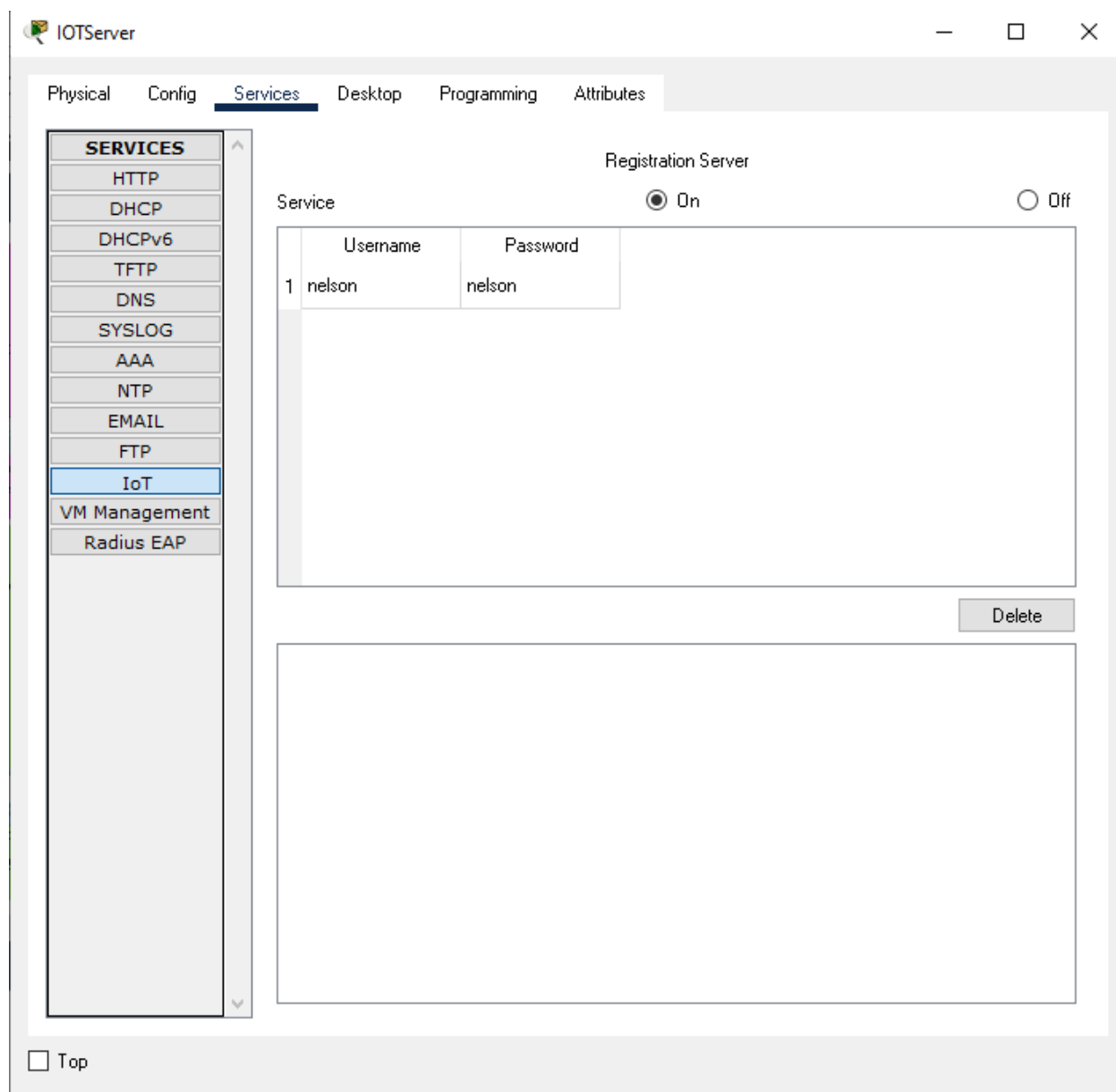


(Figure No 34. Ping Blocked by ACL)

In figure no 34. We are pinging CTO(192.168.0.3) in the Management department through HrMain. We see that the Packet sending is failed since the connection is blocked between HR and Management

6.6 IOT

IoT for this network is connected through cloud, and the below sections represent the configuration of the IOT server along with its connection to the Wireless Router and then connecting the smart devices with the server.



(Figure No 35. IoT Server)

We are turning on the IOT Registration on our server which is depicted in Figure No 35.

IoT Router

Physical Config **GUI** Attributes

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers):

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP: IP Address: 192 . 168 . 0 . 1 Subnet Mask: 255.255.255.0

DHCP Server Settings:

DHCP Server: ☒ Enabled ☐ Disabled **DHCP Reservation**

Start IP Address: 192.168.0. 100

Maximum number of Users: 50

IP Address Range: 192.168.0. 100 - 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 192 . 168 . 0 . 102

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

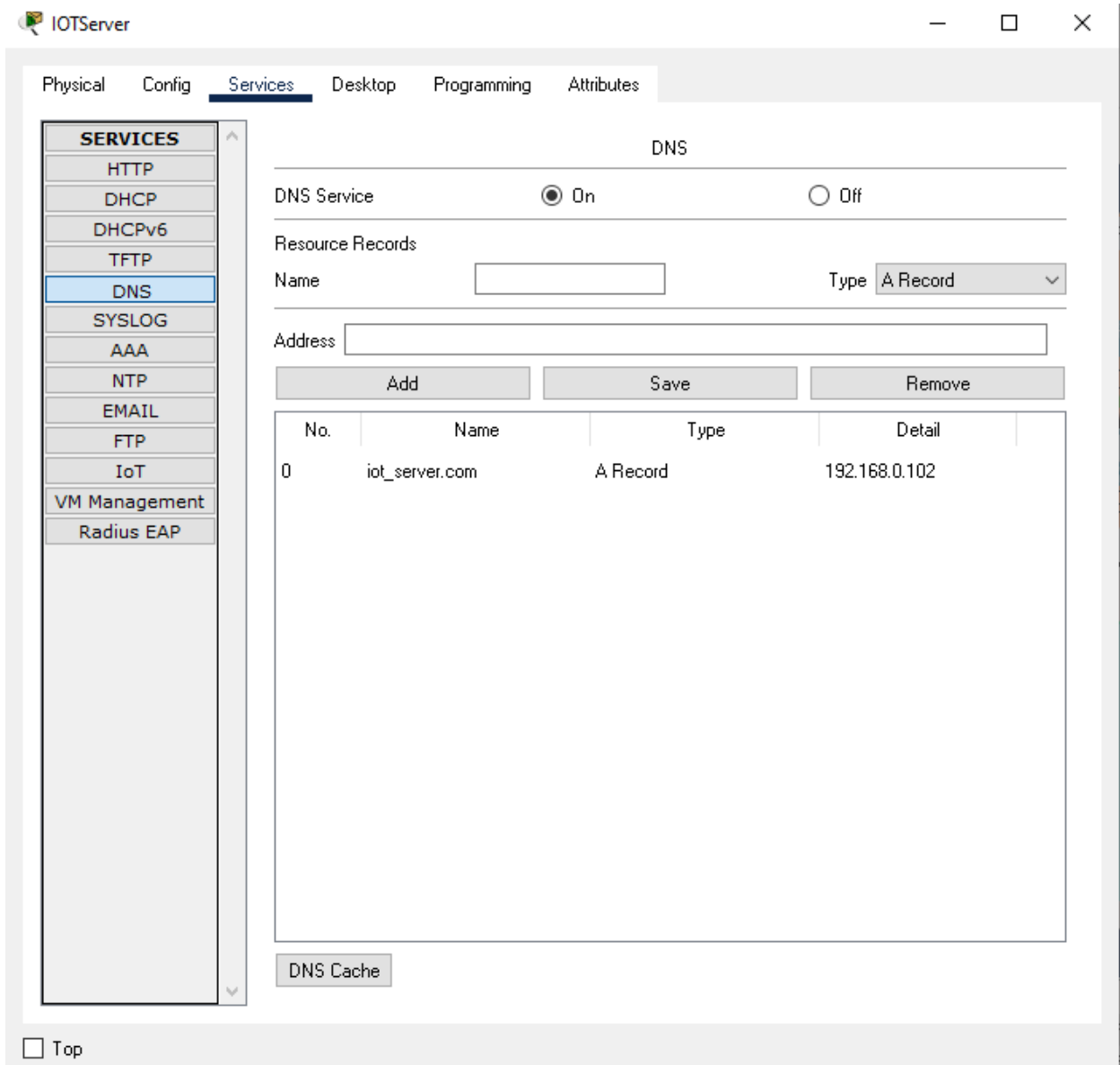
WINS: 0 . 0 . 0 . 0

[Help...](#)

☐ Top

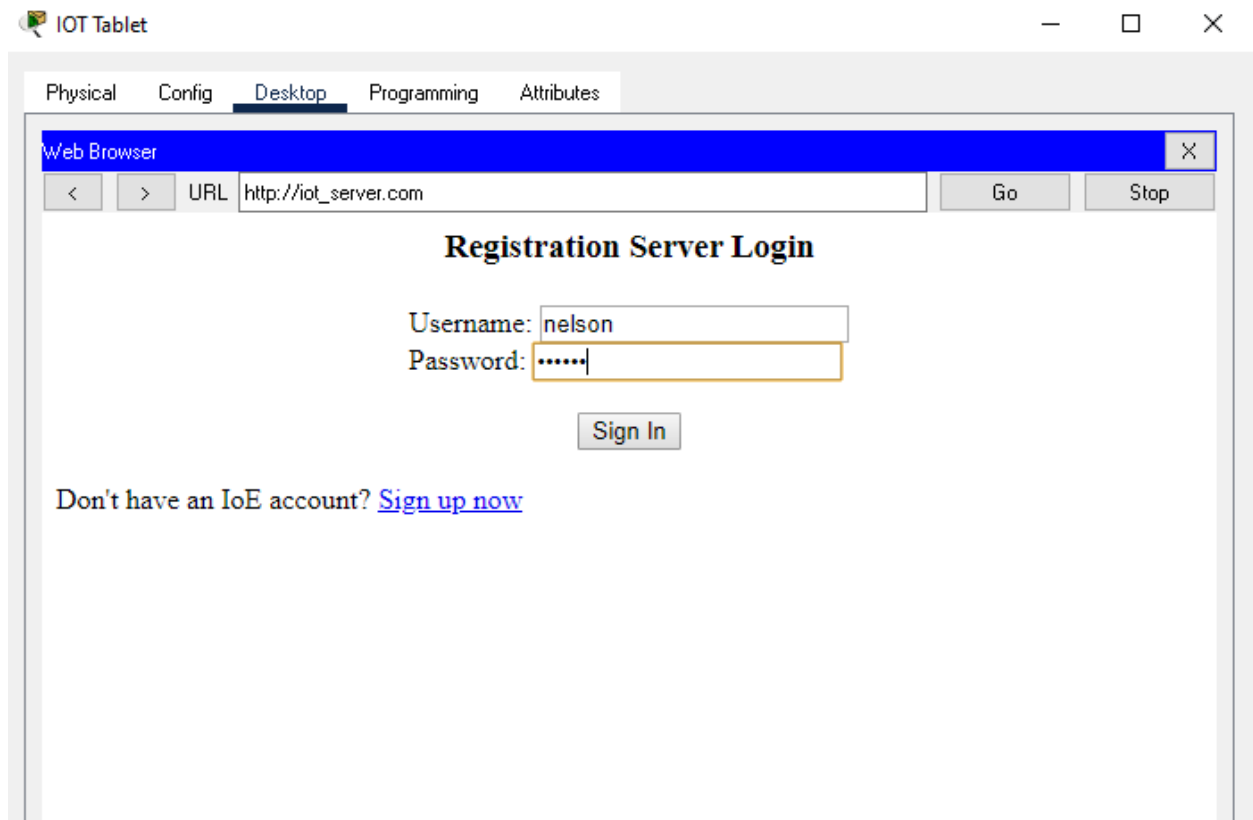
(Figure No 36.IoT Router DNS Configuration)

Figure NO 36. Show that through the GUI of the router we will set our DNS server which will be the same DNS as that of our IoT server.



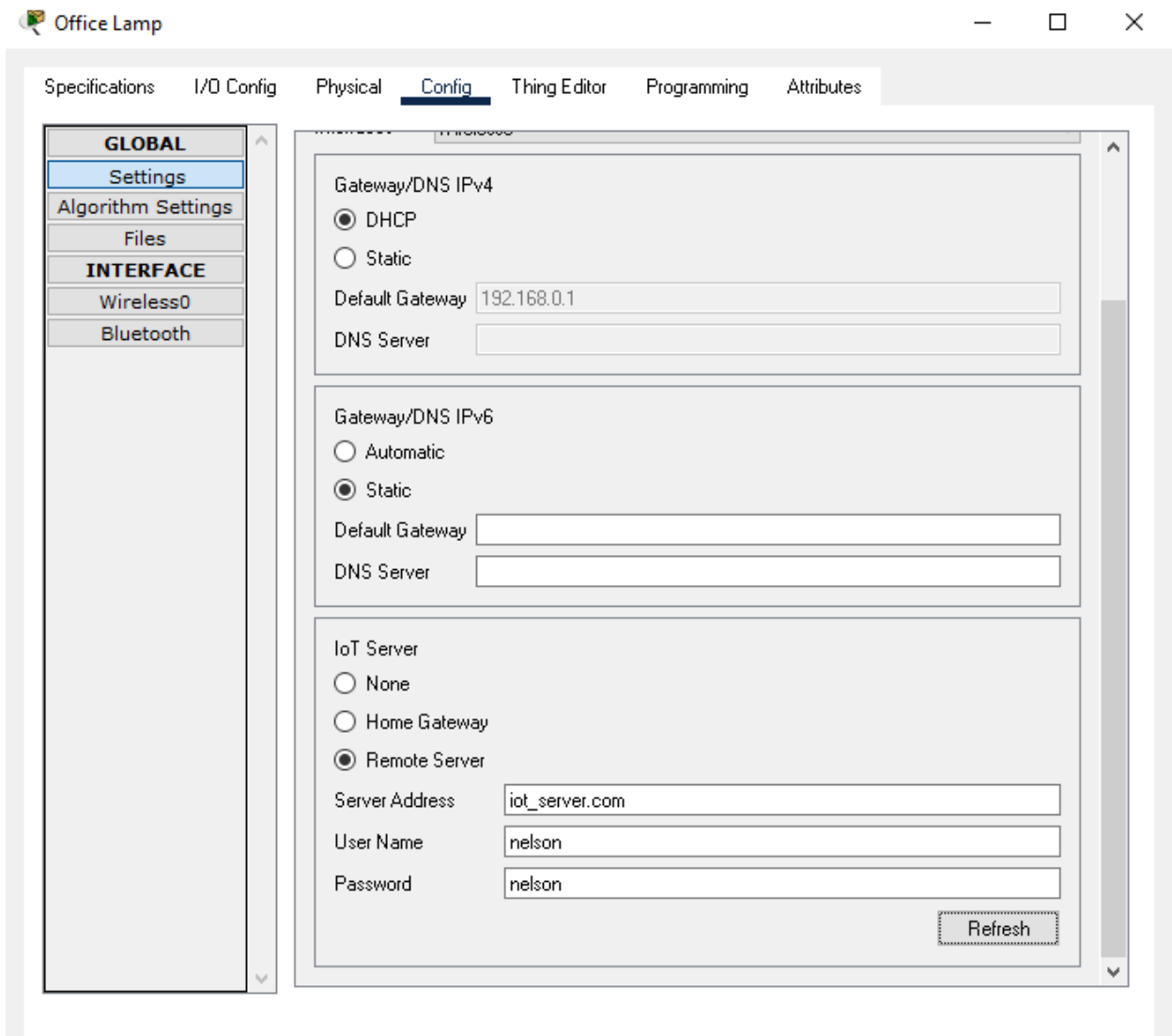
(Figure No 24.IoT DNS)

Figure No 24 Depicts the Name and Detail of our server. Here the DNS is 192.168.0.102



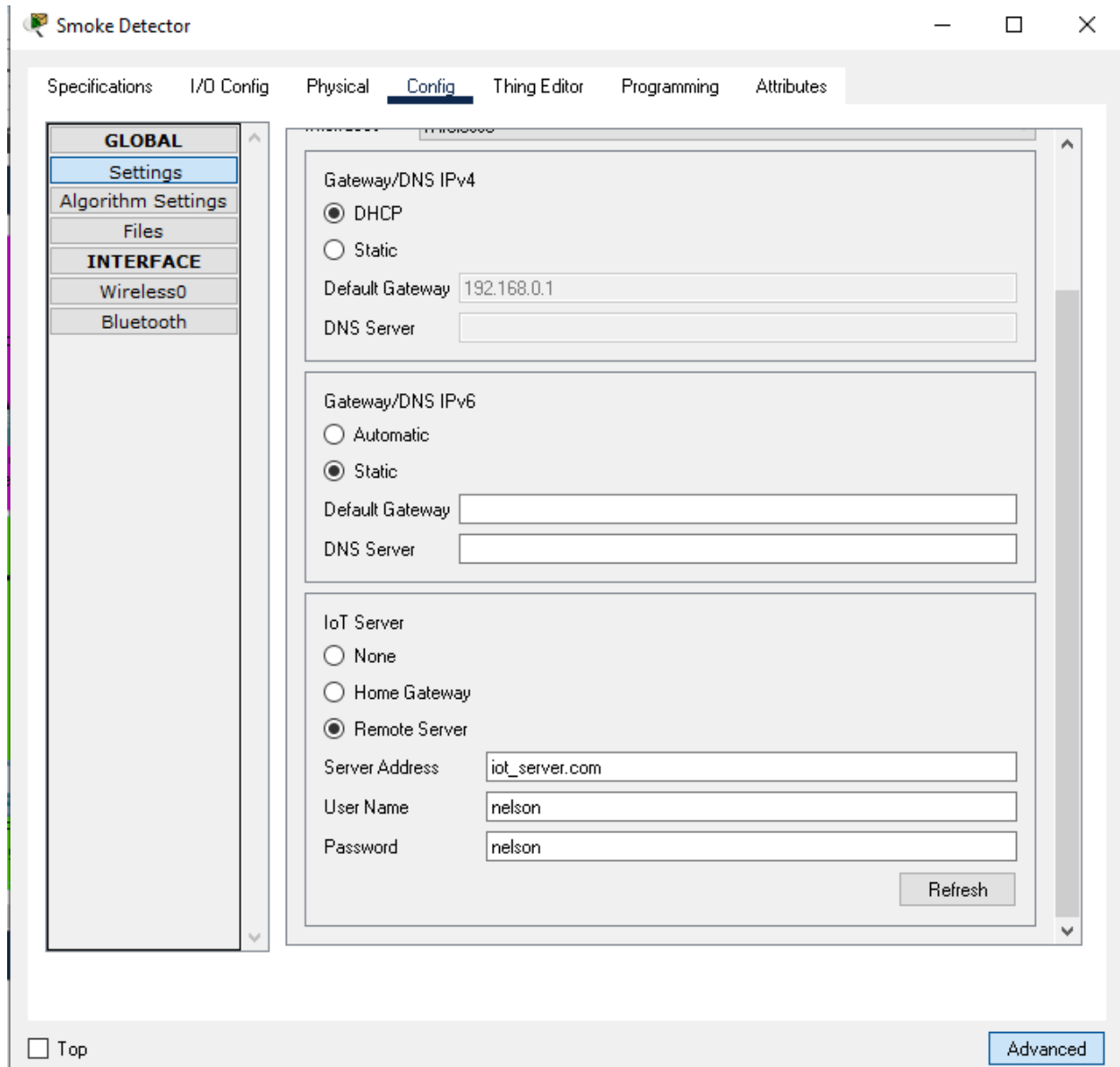
(Figure No 37.IoT Registration)

After the DNS and DHCP is set in all devices we will access the IoT Server through our tablet. After registering in the Server we will sign In which is depicted in Figure No 37.



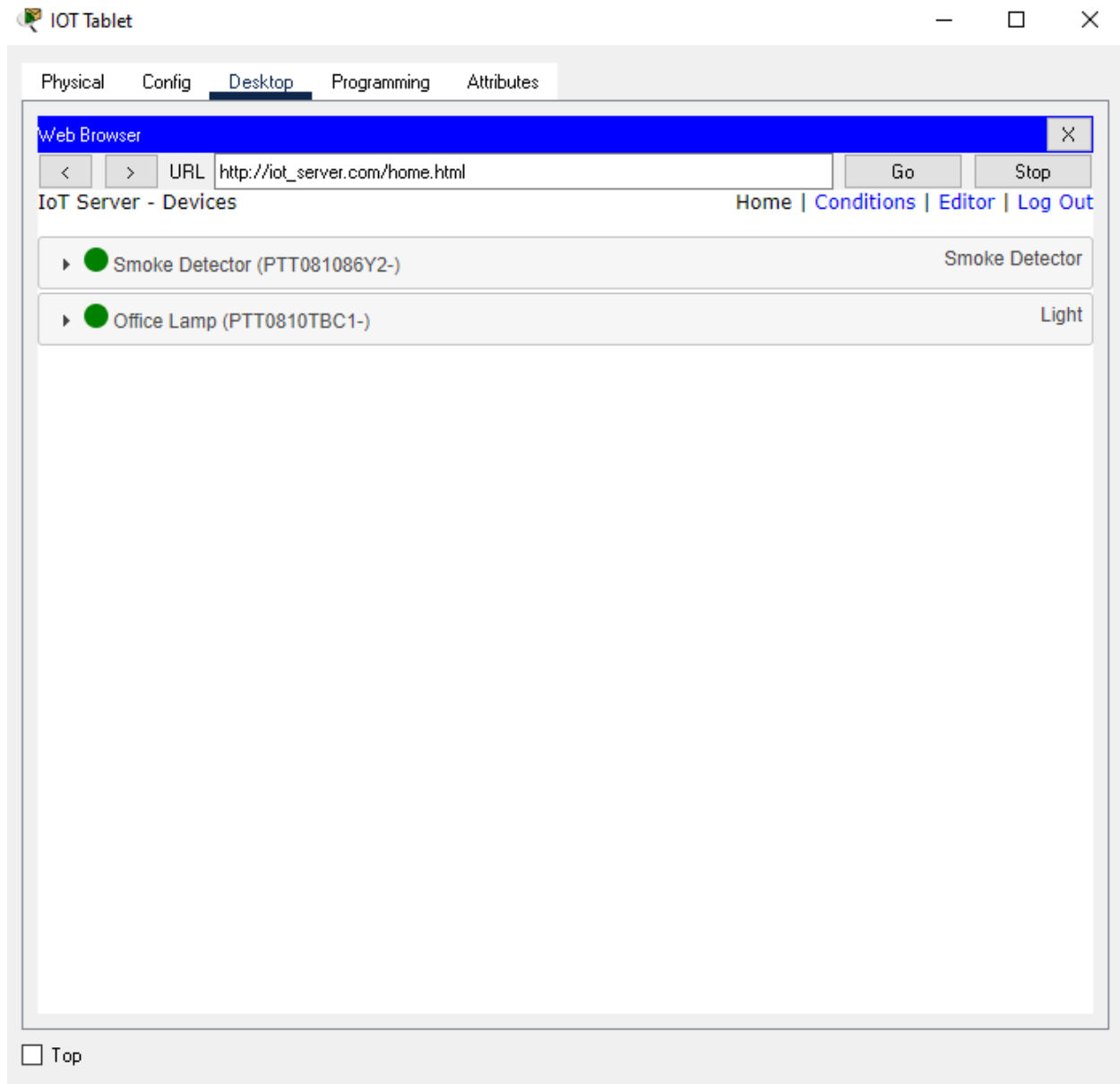
(Figure No 38.Light IOT)

In the Light IoT we will configure the IoT server where-in we will input the server address along with username and password which will connect this smart device depicted in Figure No 38.



(Figure No 39.Smoke Detector IOT)

In the Smoke Detector IoT we will configure the IoT server where-in we will input the server address along with username and password which will connect this smart device depicted in Figure No 39.



(Figure No 40.IoT Tablet)

In Figure No 40. We see the successful deployment of Smart devices in the IOT server and now the tablet can be used to control the devices.

7. References

James F. Kurose and Keith W. Ross (2017) Computer networking : a top-down approach. 7th edn. New York: McGraw-Hill.

William Stallings (2017) Network security essentials : applications and standards 7th edn. Harlow Pearson Education 2017.

Wikipedia. Network Switch (2021). Available at https://en.wikipedia.org/wiki/Network_switch (Accessed: 12 Mar 2021).

Albar Traders. Private Cloud Network Services(2021) Available at <https://albarrtraders.com/private-cloud-networks-services/> (Accessed: 15 Mar 2021)

Course Hero. Internet of Things(2021) Available at <https://www.coursehero.com/file/74514880/Internet-of-Things-Presentationpptx/> (Accessed :20 Mar 2021)