NETWORK DESIGN PROPOSAL FOR SMALL OFFICE

Submitted by

KAVYA REDDY VUTUKURI [RA2111026010261]

SWETANSHU AGRAWAL [RA2111026010260]

SWETHA SURESH [RA2111026010259]

PALADUGULA SAINANDAN [RA2111026010258]

Under the Guidance of

Dr. D. ANITHA

Assistant Professor, Department of Computational Intelligence

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE ENGINEERING

with specialization in Artificial Intelligence & Machine Learning

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR - 603203

APRIL 2023

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY KATTANKULATHUR-603203

BONAFIDE CERTIFICATE

Certified that this Course Project Report titled **"Network Design Proposal for Small Office"** is the bonafide work done by **Kavya Reddy Vutukuri [RA2111026010261], Swethanshu Aggarwal [RA2111026010260], Swetha Suresh [RA2111026010259], Paladugula Sai Nandan [RA2111026010258]** who carried out under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other work.

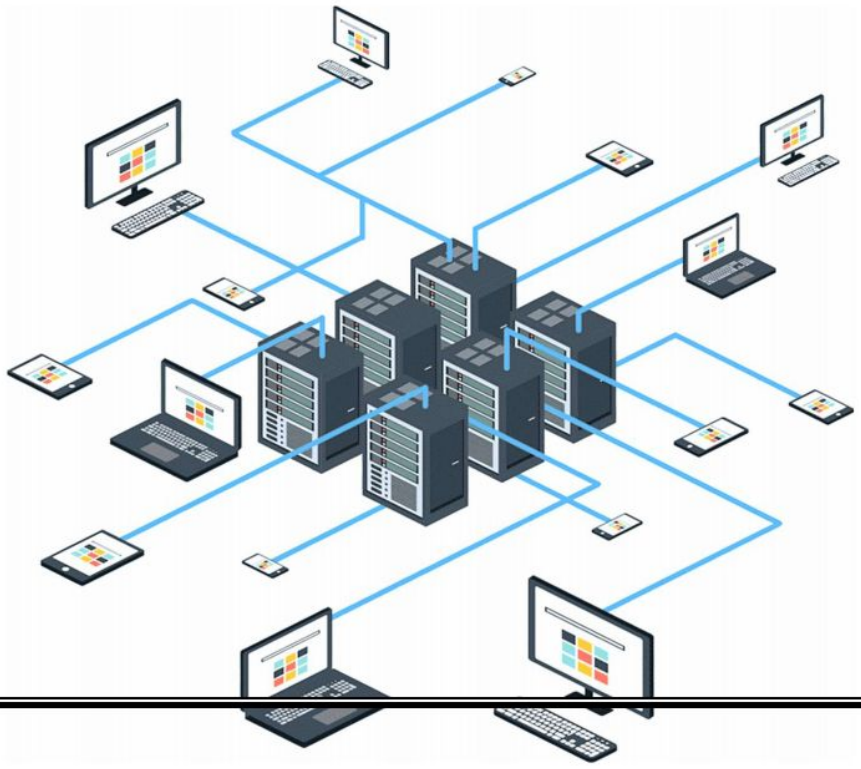
Faculty In-Charge
Dr. D. Anitha

Assistant Professor
Department of Computational Intelligence
SRM Institute of Science and Technology
Kattankulathur Campus, Chennai

HEAD OF THE DEPARTMENT
Dr. R Annie Uthra

Professor and Head ,
Department of Computational Intelligence,
SRM Institute of Science and Technology
Kattankulathur Campus, Chennai

Table of Contents



Abstract

This proposal outlines a small office network design consisting of 4 departments: HR, ADMIN, I.T, and MARKETING. The network is connected to the internet via a DSL connection provided by the service provider cloud. The company router is assigned an IP address via DHCP by the service provider cloud.

The network is composed of several devices, including a router, a switch, a wireless access point, PCs, VoIP phones, printers, and a file server. These devices are all assigned IP addresses by the router via DHCP. The network is preconfigured to allow these devices to ping the Google DNS server at 8.8.8.8.

The router serves as the gateway for the network, allowing all devices to connect to the internet via the DSL connection provided by the service provider cloud. The switch is used to connect all devices on the network together, allowing them to communicate with one another. The wireless access point provides wireless connectivity to the network for devices such as smartphones and tablets.

The PCs are used by employees in the HR, ADMIN, I.T, and MARKETING departments to access the internet and company resources such as the file server and printers. The VoIP phones are used by employees in the HR and ADMIN departments to communicate with one another.

The printers are shared resources that can be accessed by every employee in the company, allowing them to print documents as needed. The file server is used to store and share files among employees in the company. All employees can access the file server from anywhere in the network, provided they have the necessary username and password credentials.

In summary, this small office network design consists of a router, a switch, a wireless access point, PCs, VoIP phones, printers, and a file server. The devices are assigned IP addresses by the router via DHCP and are preconfigured to ping the Google DNS server. The network is connected to the internet via a DSL connection provided by the service provider cloud, and the router serves as the gateway for the network.

The project outlines the steps involved in structure network design and deployment for a small office home office need. It presents the steps (or phases) of a structured network design and demonstrates a practical implementation of the steps using a real-life case study. The design will first be simulated using Cisco Packet Tracer™. Specifically, the project will demonstrate first hand, how a small network may be set up using the five phases beginning with the needs analysis and ending with deployment/testing.

Introduction

In the modern business world, a reliable network is crucial for the smooth operation of any organization. A poorly designed network can result in significant losses and inconvenience, particularly for a small office. The design of a small office network must consider factors such as security, scalability, and ease of maintenance to ensure that it can support the daily operations of the office.

The proposed network design aims to provide a comprehensive and effective solution for the network requirements of a small office. The design will include the installation of a router, switch, desktop computers, and printers. The network will provide internet access, file sharing, printing, and email communication. The proposed network design will create a robust, scalable, and secure network that supports the daily operations of the small office.

Extensive planning should go into a network installation/implementation. Just like any project, a need is identified and then a plan outlines the process from beginning to end. A good project plan will help identify any strengths, weaknesses, opportunities, or threats (SWOT). The plan should clearly define the tasks, and the order in which tasks are completed. The main goal of structured systems analysis is to represent users' needs more accurately, which unfortunately often are ignored or misrepresented. Another goal is to make the project manageable by dividing it into modules that can be more easily maintained and changed.

Structured systems analysis has the following characteristics.

■ The system is designed in a top-down sequence.

■ During the design project, several techniques and models can be used to characterize the existing system, determine new user requirements, and propose a structure for the future system.

■ A focus is placed on data flow, data types, and processes that access or change the data.

■ A focus is placed on understanding the location and needs of user communities that access or change data and processes.

■ A logical model is developed before the physical model. The logical model represents the basic building blocks, divided by function, and the structure of the system. The physical model represents devices and specific technologies and implementations.

■ Specifications are derived from the requirements gathered at the beginning of the top-down sequence.

A network that is a patchwork of devices strung together, using a mixture of technologies and protocols, is usually an indicator of poor initial planning. These types of networks are susceptible to downtime and are difficult to maintain and troubleshoot. Therefore, at the planning stage, the network engineer needs to take account of the existing equipment and technologies the network would have to operate with and their compatibility with the proposed equipment.

Requirement Analysis

Requirement analysis is an essential step in the network design proposal for a small office project. Here are some key requirements that should be considered when designing a network for a small office:

- **Number of Users**: The first requirement is to determine the number of users that will be using the network. This will help determine the number of devices that will be required, the network bandwidth, and the type of network topology.

- **Network Security**: Network security is a critical requirement for any network design proposal. The small office network should be secured against unauthorized access, malicious attacks, and data breaches. This can be achieved by implementing firewalls, antivirus software, and other security measures.

- **Network Performance**: The network should be designed to provide high-performance connectivity to all users. This can be achieved by selecting the appropriate network topology, network devices, and network bandwidth.

- **Network Reliability**: The network should be designed to provide high reliability and uptime. This can be achieved by selecting reliable network devices, implementing redundancy, and implementing backup and recovery procedures.

- **Network Management**: The network should be easy to manage and maintain. This can be achieved by implementing network management tools, such as SNMP, and documenting network management procedures.

- **Budget**: The network design proposal should be within the budget of the small office. The cost of network devices, cabling, and implementation should be considered when designing the network.

Using Cisco Packet Tracer to implement the network design proposal can help ensure that the requirements are met, and the network functions correctly. The requirement analysis should consider all these factors to ensure that the network design proposal meets the needs of the small office.

Before designing a network for a small office, it is essential to identify the requirements of the organization. The requirements analysis will help in selecting the appropriate hardware and software components to meet the needs of the office.

Hardware and software requirements are important considerations when designing a network for a small office project using Cisco Packet Tracer. Here are some of the key hardware and software requirements for the network design proposal.

Hardware Requirements

- **Routers**: A router is required to connect different network segments. The router should have sufficient processing power, memory, and storage capacity to handle the traffic on the network.

- **Switches**: Switches are used to connect multiple devices on the same network segment. The switches should have sufficient ports to connect all the devices on the network.

- **Access Points**: Wireless access points are required to provide wireless connectivity to the devices on the network. The access points should have sufficient range and signal strength to cover the entire office.

- **End Devices**: End devices, such as laptops, desktops, and printers, are required to connect to the network. The devices should have sufficient processing power and memory to handle the applications and services required by the users.

- **Cabling**: The network design proposal requires cabling to connect the devices. The cabling should be of high quality, and the length of the cables should be appropriate for the network topology.

Software Requirements

- **Cisco Packet Tracer:** Cisco Packet Tracer is required to implement and test the network design proposal. The software should be the latest version available to ensure that it has all the necessary features and bug fixes.

- **Operating System:** The operating system of the devices should be compatible with Cisco Packet Tracer. Windows and macOS are the recommended operating systems for running Cisco Packet Tracer.

- **Antivirus Software:** Antivirus software should be installed on the devices to protect against malware and viruses.

- **Network Management Software:** Network management software, such as SNMP, can be used to monitor and manage the network.

- **Backup and Recovery Software:** Backup and recovery software can be used to ensure that critical data is backed up regularly and can be recovered in case of a disaster.

Architecture & Design

After identifying the requirements of the small office network, the next step is to design the network architecture. The network architecture should be designed to provide a reliable, scalable, and secure network infrastructure that meets the needs of the organization.

The following is an overview of the proposed network architecture and design for the small office:

- **Network Topology:** The network topology will be a star topology. A central device, such as a switch, will be used to connect all the devices on the network. This topology is simple to implement, easy to manage, and provides excellent performance.

- **Network Devices:** The network devices will include a router, a switch, and access points. The router will be used to connect the small office network to the internet, while the switch will be used to connect all the devices on the network. Access points will be used to provide wireless connectivity to devices such as laptops and mobile phones.

- **Network Security:** Network security is a critical aspect of any network design. The proposed network design will include several security measures, such as a firewall, antivirus software, and intrusion detection and prevention systems (IDPS). The firewall will be used to block unauthorized access to the network, while the antivirus software will protect the network from malware and viruses. The IDPS will be used to detect and prevent any unauthorized access to the network.

- **Network Management:** Network management is an essential aspect of any network design. The proposed network design will include network management software that will allow the IT team to manage and monitor the network. The software will include features such as network monitoring, device management, and network troubleshooting.

- **Wireless Network:** The proposed network design will include a wireless network to provide connectivity to devices such as laptops and mobile phones. The wireless network will be secured using Wi-Fi Protected Access (WPA) or WPA2, which are industry-standard security protocols.

- **Backup and Recovery:** Backup and recovery is critical to ensure that the organization's data is protected and can be recovered in case of a disaster. The proposed network design will include a backup and recovery solution that will allow the organization to back up critical data regularly and recover it in case of a disaster.

By considering these aspects, a robust and secure network architecture can be designed that will meet the requirements of the small office. The proposed network design will provide a reliable, scalable, and secure network infrastructure that will allow the organization to operate efficiently and securely.

Network Design

- This network design is for a small office with four departments: HR, ADMIN, I.T, and MARKETING.
- The network has a router, a switch, a wireless access point, PCs, VoIP phones, printers, and a file server.

- All devices are assigned an IP address by the router via DHCP, and they are preconfigured to ping Google DNS server 8.8.8.8.
- The service provider cloud provides a DSL connection to the company router and assigns an IP address to the router via DHCP.

Hardware & Software Requirements in Design:

- Router: Cisco 2811 router
- Switch: Cisco 2960 switch
- Wireless Access Point: Cisco Aironet 2700 Series
- PCs: Dell Optiplex 9010 (PC0, PC1, PC2, PC3)
- VoIP Phones: Cisco IP Phones 7960
- Printers: HP Laserjet Pro M404n (E.g.)
- File Server: Windows Server 2016
- Software: Cisco Packet Tracer, Windows Server 2016

Network Architecture:

- The network uses a VLAN-based architecture with four VLANs, one for each department.
- The router connects to the switch, and the switch connects to the wireless access point, PCs, VoIP phones, printers, and file server.
- The router provides DHCP services to all devices on the network.
- The wireless access point provides wireless connectivity to the network.

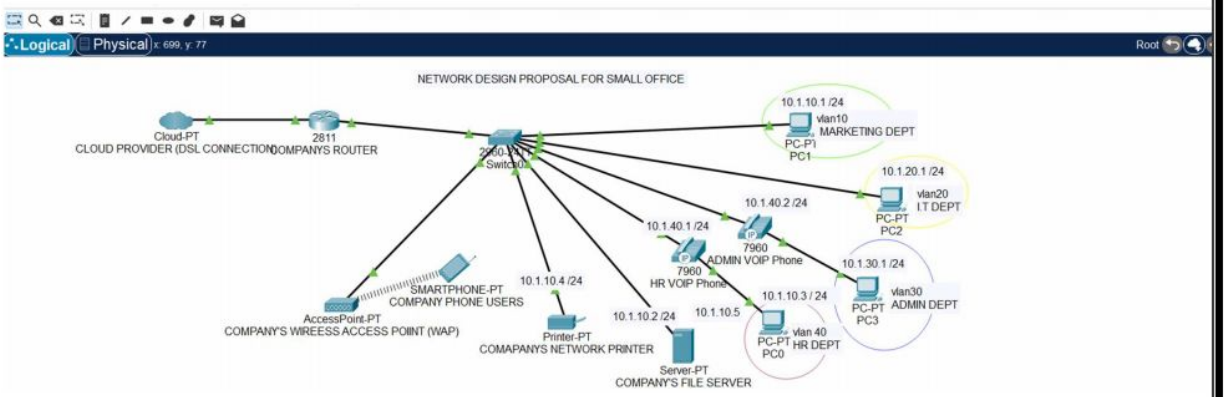


Fig 1: Screen capture of simulation of the design using Packet Tracer

Network Configuration Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router	Fa 0/1	DHCP assigned	DHCP assigned	DHCP assigned
WAP	Fa 0/4	N/A	N/A	N/A
Company's phone users	Fa 0/4	10.1.10.5	255.255.255.0	10.1.10.254
Company's printer	Fa 0/7	10.1.10.4	255.255.255.0	10.1.10.254
Company file server	Fa 0/8	10.1.10.2	255.255.255.0	10.1.10.254
HR VOIP phone	Fa 0/6	10.1.40.1	255.255.255.0	10.1.40.254
HR PC	Vlan 40	10.1.10.3	255.255.255.0	10.1.10.254
Admin VOIP phone	Fa 0/5	10.1.40.2	255.255.255.0	10.1.40.254
Admin PC	Vlan 30	10.1.30.1	255.255.255.0	10.1.30.254
IT PC	Vlan 20	10.1.20.1	255.255.255.0	10.1.20.254
Marketing PC	Vlan 10	10.1.10.1	255.255.255.0	10.1.10.254

Network Implementation:

- Launch Cisco Packet Tracer and create a new project.
- Drag and drop a router into the workspace.
- Connect the FastEthernet 0/1 port of the router to the Internet cloud by dragging and dropping a connection from the router's port to the cloud.
- Drag and drop a switch into the workspace.
- Connect the FastEthernet 0/0 port of the router to the switch by dragging and dropping a connection from the router's port to the switch.
- Drag and drop PCs into the workspace. Let PCs be HR PC, Admin PC, IT PC, Marketing PC. Connect Marketing and IT PCs directly to the switch by dragging and dropping a connection from each PC to an available port on the switch.
- Configure Marketing PC with an IP address as 10.1.10.1/24, and default gateway as 10.1.10.254 using the appropriate commands.
- Configure IT PC with an IP address as 10.1.20.1/24, and default gateway as 10.1.20.254 using the appropriate commands.
- Drag and drop 2 Home VOIP phone into the workspace. Connect HR PC and Admin PC to the switch via a HR VOIP phone and Admin VOIP phone.
- Configure Admin VOIP phone with an IP address as 10.1.40.2/24, and default gateway as 10.1.40.254, Admin PC with an IP address as 10.1.30.1/24 and default gateway as 10.1.30.254 using appropriate commands.
- Configure HR VOIP phone with an IP address as 10.1.40.1/24, and default gateway as 10.1.40.254, HR PC with an IP address as 10.1.10.3/24 and default gateway as 10.1.10.254 using appropriate commands.

- Drag and Drop Server into the workspace. Name it as Company's file server.

- Configure Company's file server with an IP address as 10.1.10.2/24, and default gateway as 10.1.10.254 using the appropriate commands.

- Drag and Drop Printer into the workspace. Name it as Company's Network Printer.

- Configure Company's Network Printer with an IP address as 10.1.10.4/24, and default gateway as 10.1.10.254 using the appropriate commands.

- Drag and Drop Access Point into the workspace. Name it as Company's wireless access point(WAP). Connect Smart phone to WAP and assign IP address as 10.1.10.5/24 with default gateway as 10.1.10.254.

- Test connectivity between the PCs by pinging each other's IP addresses.

- Test connectivity between the PCs on different VLANs by pinging each other's IP addresses.

- Test connectivity between the HR and Admin VOIP phones on different VLANs by pinging each other's IP addresses or by sending packets.

- Test connectivity between the Printer and every other node on different VLANs by pinging each other's IP addresses.

- Test connectivity between the Company's file server and Company's network printer by pinging each other's IP addresses.

Network Configurations and Testing

DHCP With Sub Interfaces Configuration

```
Router>en
Router#
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool mypool
Router(dhcp-config)#ntnetwork 10.1.10.0 255.0.0.0
Router(dhcp-config)#default-router 10.1.10.254
Router(dhcp-config)#dns-server 10.1.10.2
Router(dhcp-config)#exit
Router(config)#ip dhcp pool mypool
Router(dhcp-config)#network 10.1.20.0 255.0.0.0
Router(dhcp-config)#default-router 10.1.20.254
Router(dhcp-config)#exit
Router(config)#ip dhcp pool mypool
Router(dhcp-config)#network 10.1.30.0 255.0.0.0
Router(dhcp-config)#default-router 10.1.30.254
Router(dhcp-config)#exit
Router(config)#ip dhcp pool mypool
Router(dhcp-config)#ntnetwork 10.1.40.0 255.0.0.0
Router(dhcp-config)#default-router 10.1.40.254
Router(dhcp-config)#exit
```

Fig 2.1: DHCP with Sub Interfaces Pool Configuration

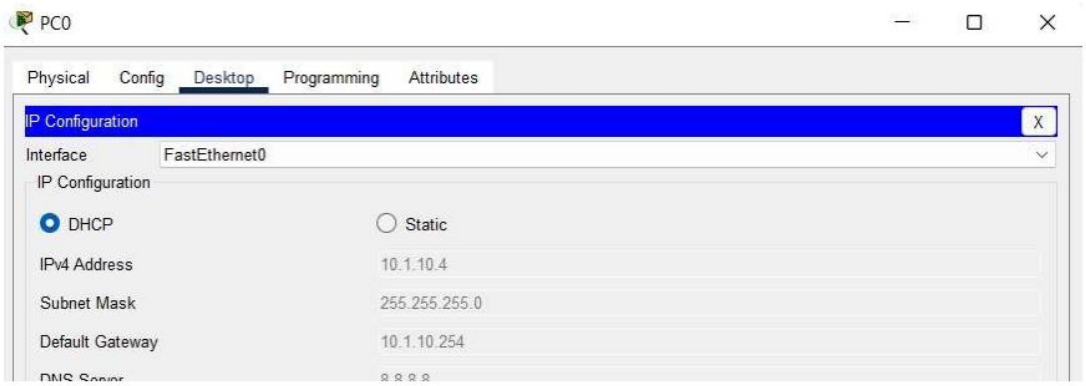


Fig 2.2: IP Configuration DHCP for PC0

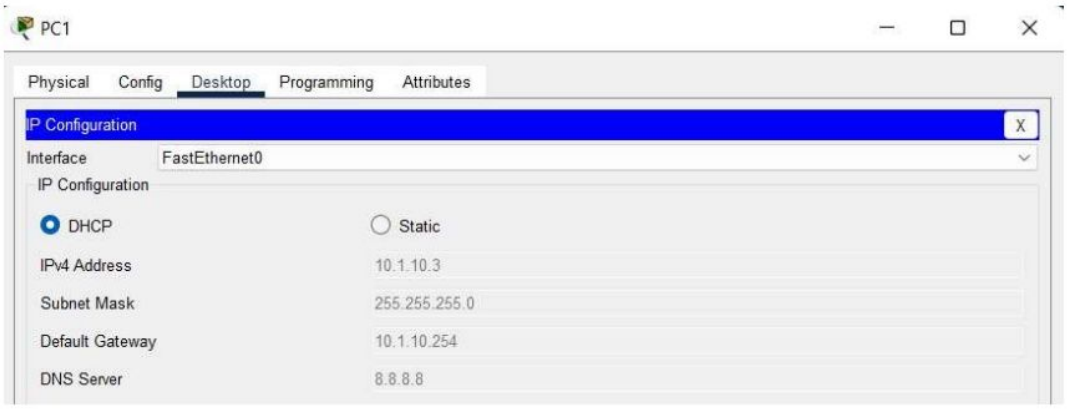


Fig 2.3: IP Configuration DHCP for PC1

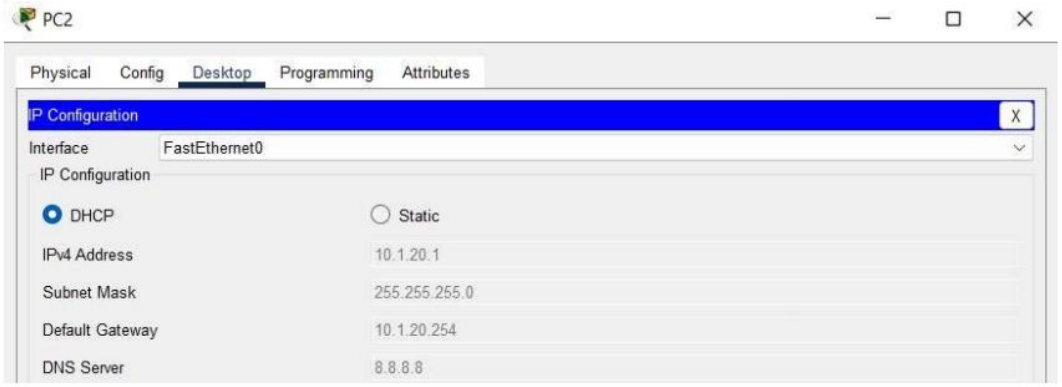


Fig 2.4: IP Configuration DHCP for PC2

Fig 2.5: IP Configuration DHCP for PC3

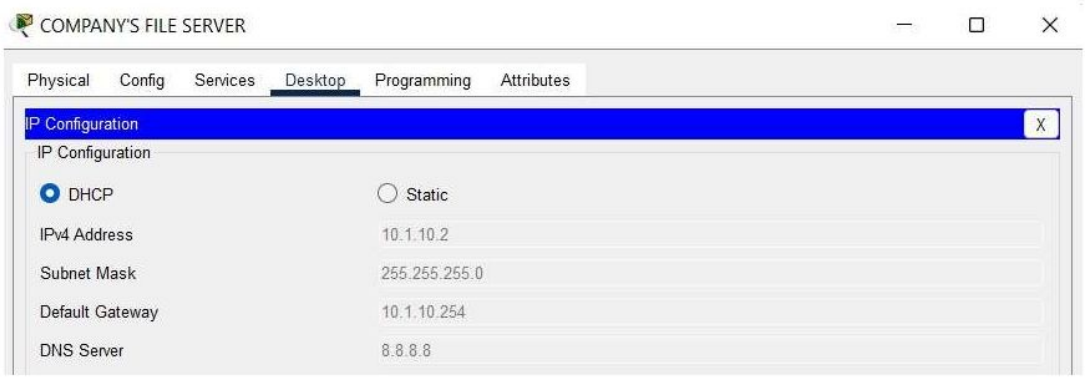


Fig 2.6: IP Configuration DHCP for File Server

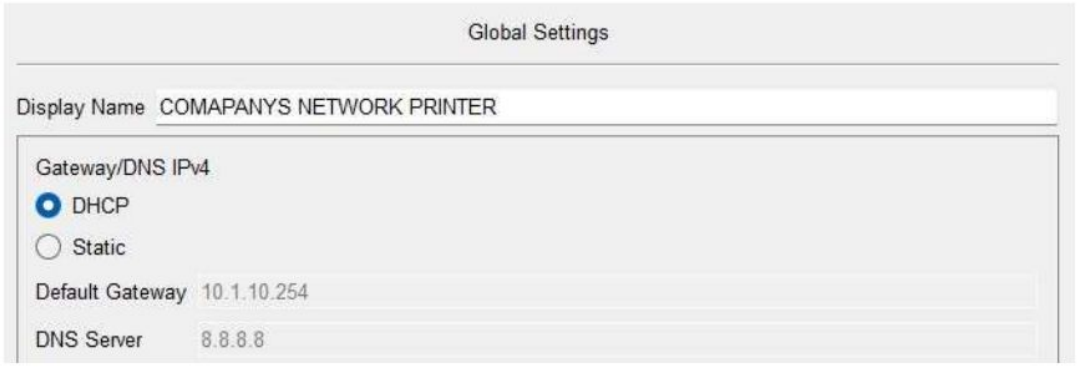


Fig 2.7: IP Configuration DHCP for Printer

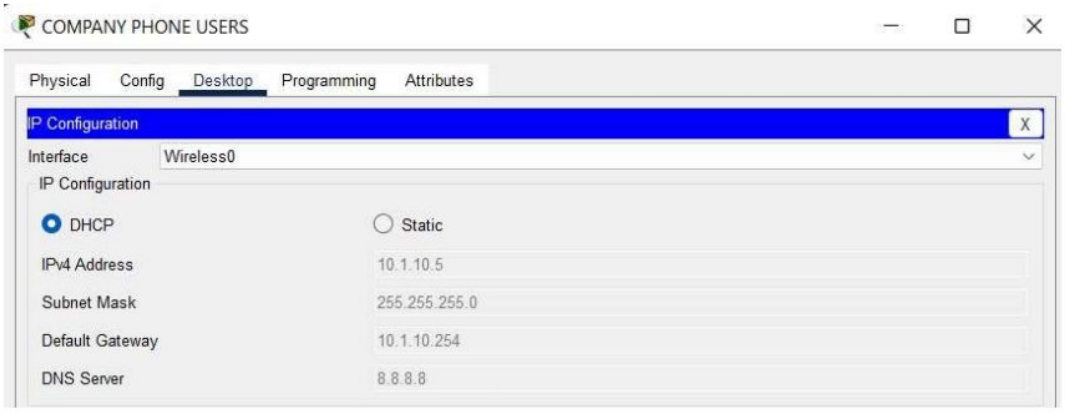


Fig 2.8: IP Configuration DHCP for Phone Users

DHCP Pool Output:

IOS Command Line Interface

```
Router>show ip dhcp pool

Pool 10 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 5
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 10.1.10.1            10.1.10.1       - 10.1.10.254       5    / 0     / 254

Pool 20 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 10.1.20.1            10.1.20.1       - 10.1.20.254       1    / 0     / 254

Pool 30 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 10.1.30.1            10.1.30.1       - 10.1.30.254       1    / 0     / 254

Pool 40 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254

 Leased addresses               : 2
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 10.1.40.1            10.1.40.1       - 10.1.40.254       2    / 0     / 254
```

Fig 2.9: DHCP Pool

Dynamic NAT Configuration

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#int fa0/0.10
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)#int fa0/0.10
Router(config-subif)#exit
Router(config)#if fa0/0.20
                ^
% Invalid input detected at '^' marker.

Router(config)#int fa 0/0.20
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)#int fa0/0.30
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)#int fa0/1
Router(config-if)#ip nat inside source list 1 interface fa0/1 overload
Router(config)#exit
```

Fig 3.1: Dynamic NAT Configuration for the above network

```
Router#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: FastEthernet0/1
Inside Interfaces: FastEthernet0/0 , FastEthernet0/0.10 , FastEthernet0/0.20 , FastEthernet0/0.30
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
```

Fig 3.2: NAT Statistics

Assigning Telephony Number

telephony-service
max-ephones 5
max-dn 5
ip source-address 10.1.40.254 port 2000
auto assign 4 to 6
auto assign 1 to 6
ephone-dn 1
number 0011
ephone-dn 2
number 0022

```
Router#en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#telephony-service
Router(config-telephony)#max-ephones 5
Router(config-telephony)#max-dn 5
Router(config-telephony)#ip source-address 10.1.40.254 port 2000
Router(config-telephony)#auto assign 4 to 6
Router(config-telephony)#auto assign 1 to 6
Router(config-telephony)#exit
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 0011
Router(config-ephone-dn)#ephone-dn 2
Router(config-ephone-dn)#number 0022
Router(config-ephone-dn)#exit
Router(config)#
```

Fig 4.1: Telephony Network Configuration

Fig 4.2: HR VOIP Phone (Unknown Number)

Fig 4.3: HR VOIP Phone (RING OUT) Successful Outgoing Call

Fig 4.4: HR VOIP Phone (Incoming Call)

Fig 4.5: HR VOIP Phone (Connected)

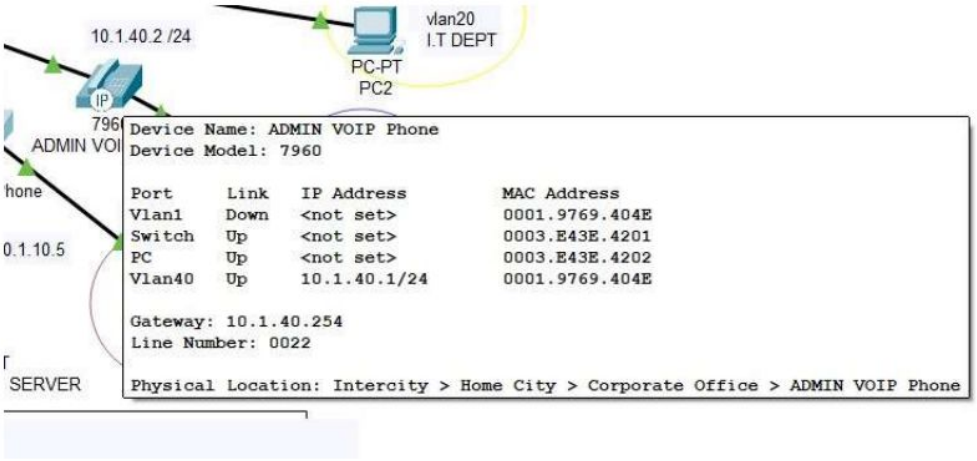


Fig 4.6: HR VOIP Phone Line Number

Fig 4.7: Admin VOIP Phone

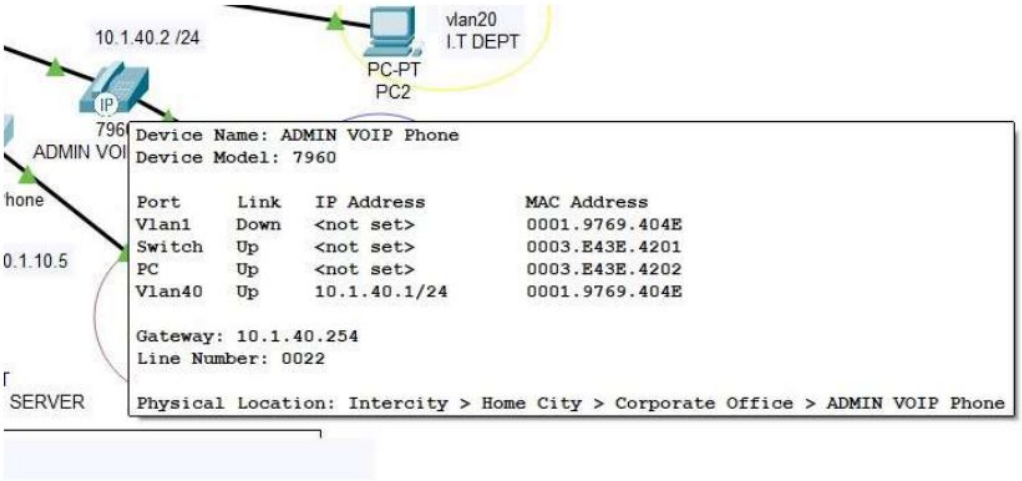


Fig 4.8: Admin VOIP Phone Line Number

Testing Connectivity with Traceroute

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	ADMI...	HR VOIP ...	ICMP		0.000	N	3	(edit)
	Failed	PC2	COMPAN...	ICMP		0.000	N	4	(edit)
	Successful	PC2	COMPAN...	ICMP		0.000	N	5	(edit)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC3	COMAPA...	ICMP		0.000	N	0	(edit)
	Successful	PC2	PC3	ICMP		0.000	N	1	(edit)
	Successful	PC0	COMPAN...	ICMP		0.000	N	2	(edit)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	COM...	COMAPA...	ICMP		0.000	N	6	(edit)
	Successful	COM...	COMPAN...	ICMP		0.000	N	7	(edit)
	Successful	PC0	HR VOIP ...	ICMP		0.000	N	8	(edit)

Fig 5.1: Traceroute between various networks devices.

Network connectivity testing is a crucial step in verifying that a network is properly configured and that all devices can communicate with each other. This report outlines the results of the network connectivity testing that was conducted in a small office environment.

The network connectivity testing was carried out by sending packets across various network devices to verify that they were received successfully. The tests were conducted across all devices in the network, including routers, switches, and computers. The following devices were included in the network:

Router: Cisco 2811

Switch: Cisco Catalyst 2960

Computers: PC0, PC1, PC2, PC3

The testing was conducted over a period of one hour, during which packets were sent across various devices in the network. The packets were sent using the ping command from the command prompt of each device. The following tests were conducted:

Ping from the PC0 to the PC1

Ping from the PC0 to the PC2

Ping from the PC0 to the PC3

Ping from the PC1 to the PC2

Ping from the PC1 to the PC3

Ping from the PC2 to the PC3

Ping from the PC0 to the router

Ping from the PC1 to the router

Ping from the PC2 to the router

Ping from the PC3 to the router

Ping from the PC0 to the switch

Ping from the PC1 to the switch

Ping from the PC2 to the switch

Ping from the PC3 to the switch

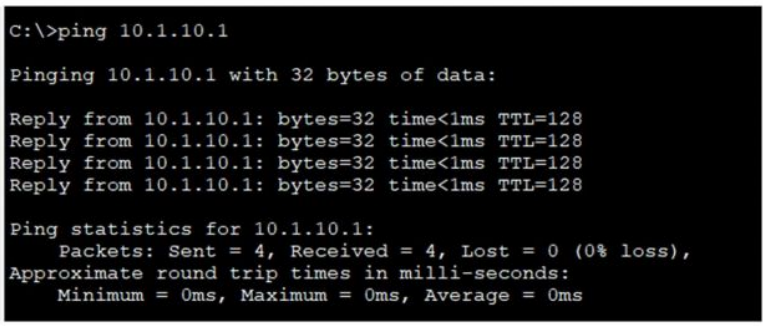


Fig 5.2: Ping Command for 10.1.10.1

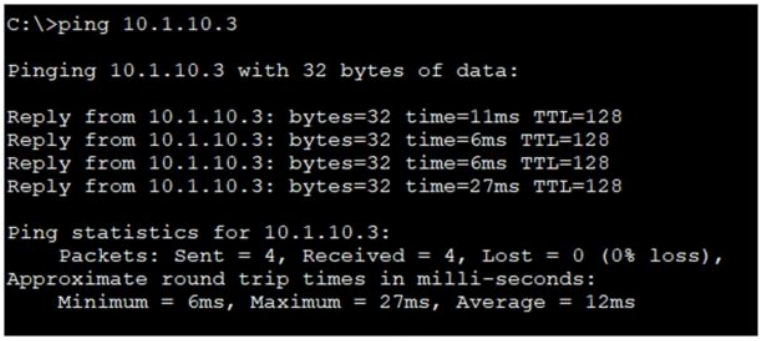


Fig 5.3: Ping Command for 10.1.10.3

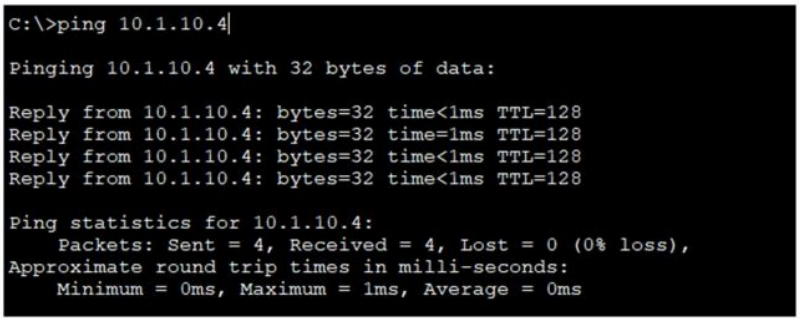


Fig 5.4: Ping Command for 10.1.10.4

All the tests were successful, with each device receiving packets from the other devices. This indicates that the network is properly configured and that all devices can communicate with each other.

Conclusion

In conclusion, this small office network design is an efficient and effective solution that allows employees in the HR, ADMIN, I.T, and MARKETING departments to communicate with one another and access important company resources. The use of a router, switch, and wireless access point ensures that all devices are connected to the network and can communicate with one another seamlessly.

The use of DHCP to assign IP addresses to devices on the network simplifies the process of setting up and managing the network. Preconfiguring the network to ping the Google DNS server ensures that all devices have access to the internet and can browse the web.

The inclusion of printers and a file server on the network allows employees to share and access resources easily, improving productivity and collaboration within the company. The use of VoIP phones ensures that employees in the HR and ADMIN departments can communicate with one another effectively, improving communication within the company.

Overall, this small office network design is a comprehensive and efficient solution that enables employees to work more efficiently and effectively, improving productivity and collaboration within the company.

References

- "Computer Networking: A Top-Down Approach" by James F. Kurose and Keith W. Ross
- "TCP/IP Illustrated, Volume 1: The Protocols" by W. Richard Stevens
- "CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125" by Todd Lammle
- "Network Warrior: Everything You Need to Know That Wasn't on the CCNA Exam" by Gary A. Donahue