

Network Design Of A Small Startup Firm

IT 491 Cisco Capstone Project

Professor Eljabiri

1 May 2022

Project Team Members

Jared Derro

Ron Nathaniel

Raj Gandhi

Khang Thai

Vraj Shah

Table of Contents

1. Introduction (Vraj)

- a. Project Background
- b. Problem Definition
- c. Glossary of Terms used

2. Project Management (Khang)

- a. Task Analysis
- b. WBS/Gantt
- c. Risk identification
- d. Management

3. Define (Ron)

- a. Stakeholders
- b. Requirements
- c. Project Scope

4. Design (Jared)

- a. Physical Design
- b. Logical Design
 - i. VLANs
 - ii. DHCP
 - iii. FTP, DNS
 - iv. Employee, Guest Wi-Fi
 - v. VOIP

5. Development (Jared)

- a. Scalability
- b. Redundancy
- c. Security

6. Evaluation (Raj)

- a. Solution Testing
- b. Team Conclusions

7. Works Cited (Jared)

Introduction (Vraj):

Project Background

In the current digital age, startup companies are looking to expand operations. However, to expand operations, they need a fully functional network. One of these startup companies is an accounting firm looking to create a network before the start of tax season. Since the startup's owner only has a budget of \$25,000, the owner wants a cheap but reliable, secure, redundant, and scalable network solution for their new building. Therefore, they hired our team to get the job done.

Problem Definition

Using Cisco Packet Tracer, our goal is to design a fully functional network that can support multiple users. Managers, employees, and guests will need access to the network's resources. The network's resources will consist of servers, IP phones, PC's, and printers. For our project, we have two main goals. First, the network needs to be secure, reliable, and redundant. Second, the network needs to be cost-efficient. More specifically, the number of resources cannot exceed the budget of \$25,000.

Glossary of terms used

1. Cisco Packet Tracer: Cisco's simulation software that allows users to create network topologies and imitate certain networks.
2. VLAN (Virtual LAN): Enables a group of devices available in multiple networks to be combined into one logical network.
3. FTP (File Transfer Protocol): Communication protocol that allows users to transfer files using a client-server model.

4. DHCP (Dynamic Host Configuration Protocol): Protocol that automatically assigns an IP address to a host.
5. DHCP Snooping: Prevents DHCP servers from offering IP addresses to untrusted DHCP clients.
6. DNS (Domain Name System): Converts IP addresses to human readable domain names.
7. VOIP (Voice over Internet Protocol): Allows users to make voice calls using an Internet connection.
8. Port Security: Preventing unknown devices from forwarding packets.
9. Extended Access Control List: Determines what traffic is allowed to flow within a network.

Project Management (Khang):

Task Analysis

There were four steps we followed for our task analysis. They consist of knowing the audiences, sticking to the schedule plan, breaking down the steps for project completion and considering any variables.

1. Knowing the audiences
 - a. The audiences that we present our projects to might not be as technologically adept as we are, so it is important that we use terms and explain the processes that goes on behind the making and the implementation of our project. Understandably, some of our team members are considered as the audience since some of us have not had the experience of ever using Cisco Packet Tracer in the first place. We had to first

understand our system of operation since we are basically starting from pretty much nothing.

2. Sticking to the schedule plan

- a. We created a schedule plan on Trello and wrote down what we needed to do every week. We made sure the goal for that week was reached and along with the goal, our understanding of the project grew as well. We also looked ahead into the next week to see what is it that the next goal of ours was to see if it can be implemented ahead of time or at the very least, begin ahead of schedule.

3. Breaking down the steps for project completion

- a. We broke the project down into multiple steps when we were making the schedule plan. We then assigned each person their task and made sure they focused on that one first. Jared looked over all of our work and tested the redundancy. Ron was in charge of implementing and working on research for the VOIP. Khang worked on setting up the physical design in Cisco Packet Tracer. Raj researched about the DNS and FTP server. Vraj worked on the DHCP server.

4. Considered any variables

- a. There were variables and risks that had to be considered. One of which was that we would most likely not meet in person outside of the classroom since most of us commute here from a decently far drive. We made sure to communicate clearly with each other using Discord as we are all active on it and it is linked onto our phone. We kept in mind that we should not go over the deadline that we gave ourselves and not to go over the budgets since this is a startup firm.

Roles

<u>Name</u>	<u>Role</u>	<u>Task</u>
Jared Derro	Project Manager	<ul style="list-style-type: none">❖ Document all progress❖ Conduct weekly meetings❖ Finalized Packet Tracer File for presentation.❖ Setup Guest, Employee Wi-Fi
Ron Nathaniel	Team Member	<ul style="list-style-type: none">❖ Setup VOIP❖ Look pricing of hardware within budget❖ Write Final Presentation
Raj Gandhi	Team Member	<ul style="list-style-type: none">❖ Setup DNS server.❖ Document scalability for future growth of the company.❖ Configured FTP server
Khang Thai	Team Member	<ul style="list-style-type: none">❖ Setup physical design in packet tracer.❖ Setup switch and backup router❖ Configured Port security and password encryption
Vraj Shah	Team Member	<ul style="list-style-type: none">❖ Create brochure for final presentation❖ Configured DHCP

Gantt Chart



Risk Identification and Management

<u>Risk</u>	<u>Reason</u>	<u>Level</u>	<u>Mitigation</u>
Difficulties in learning packet tracer	Our entire team does not have that much experience with using packet tracers.	Medium	Using outside resources to help if we encounter any problems. YouTube, Cisco Community, and other outside resources.
Packet Tracer file sharing	Since packet tracer can only be edited by 1 person at a time.	Low	Using Discord file transfer, once a new version is made, it will be uploaded and can be downloaded from there.
Hardware Limitation in Packet Tracer	Since packet tracer is an old program, there is a limited amount of hardware that is available to be used in the program.	Medium	Use the most cost-effective but efficient hardware that Cisco packet tracer provides.

Define (Ron):

Stakeholders:

Founding a startup is an incredibly difficult task, and usually not one that can be done alone. There are products to build, services to offer, and money to be made. For this reason, the Stakeholders of our Startup can be divided into three main groups: the Executives, the Clients, and the Employees.

The Executives are typically a small team of Co-Founders, who brought the Startup to life initially, and in its early stages are primarily in charge of running the company. They are primarily responsible for finding the initial employees, clients, investors (if needed), and developing relations with other businesses. Essentially, their task as the initially sole stakeholders is to find more candidates to become stakeholders, and to extend the “burden” of keeping the business alive on their shoulders as well. Taking two examples from the extremes, let’s say a team of three co-founders gather together and plan to start a company. At the very start, it is just the three of them as the only stakeholders. Now consider a large, post-IPO business, such as Cisco. Cisco does not fall on the shoulders of a small team of three, but rather is being carried by 80,000+ employees, and supported by the countless of their users worldwide. This is a great example of the initial Executives greatly extending the list of Stakeholders.

The Clients can vary from any type of consumer, be it Customer or Business, be it another Startup or post-IPO Enterprise, any client that is associated with the startup is a tremendous stakeholder and is helping the business stay alive in more ways than the client could ever imagine. The keyword here is Associated, as not every client has to be a paying one. In many cases, a non-

paying Design Partner could act as both a greater Stakeholder, and as a much more influential help than a paying customer would.

The Employees of the Startup, needless to say, help keep the business running in a Day-to-Day fashion. Employees, as opposed to Executives, generally focus more on short-term, tactical executions, and smaller operations. Of course, this does not diminish them as Stakeholders to the business, and they are an essential part of this Startup. Not that every company requires more employees than executives, but once a company has hired several employees, it becomes near impossible to reverse this, and return to no employees. At such a point, it can be argued that the Executives rely more on the Employees than the other way around. Once this point is reached, the collective employees are undoubtedly greater Stakeholders than the executives.

Requirements

There were multiple great requirements which were initially set, that the team had to keep in mind during development.

Firstly, the startup required a floor plan. During a small proof of concept early on in development, we had to ensure that our plan would be able to fit in a physical landscape, to ensure that this could really be built out. Of course, without the rest of the requirements, the floor plan remained in the back of our minds for the entirety of the project's development. It acted as a sense of Realism, that we had to always ensure this project remained viable.

Second, we needed devices, or any other host with a processor, and they all needed an IPv4 address to ensure they could all communicate, should access be granted to the communication line.

Meaning, it would be up to the Startup's IT department to decide who can communicate with who, and not the other way around.

Third, we needed a VOIP system. VOIP stands for Voice over IP, meaning that any multimedia communication device, such as a telephone, could have an IPv4 associated with it and allow for multimedia communication across local wireless networks. Before this, telephones were all linked with hard cables, called telephone lines. This would allow the team to develop fast and forgo worrying about hardware such as the telephone lines.

Next, we needed a way to store information internally. This is when we decided that servers dedicated to FTP, DHCP, and DNS would be required to ensure this. With dedicated servers, we would be able to store any value in our internal computers.

Now we can decide that all clients and employees should have access to their respective lines. We made the executive decision to ensure all lines of communication between hosts would be wired. We happened to settle on IPv4 for most of our communications.

Finally, we needed some sort of security for the network. We needed to ensure that only the exact requests we allowed were made. Should any outsider attempt to connect to an internal machine or originating internally to an unauthorized host outside the network, there had to be a way to block those connections automatically, without human intervention.

Project Scope:

While knowing the project requirements, we started implementing switches, routers, PC's, printers, and IP phones to our network design. In the early stages, we decided not to simulate the Internet because it was considered too complex for the project.

Setting out, we had set a Budget for ourselves of \$25,000 USD. Without a guarantee of whether this was possible, we tried to stick to it anyway. Of course, when a group of dedicated learners gather together, anything is possible. Fortunately, we were able to put the startup together only for \$22,397 USD, which is an incredible result. We were able to come in \$2,603 USD under budget, saving almost \$3,000 USD. This was accomplished by leveraging the following products:

Routers (2) - Cisco 2911 ISR = \$894 USD / router

= \$1,788 USD subtotal.

Switches (5) - Cisco 2950-24 switch = \$60 USD / switch

= \$2,088 USD subtotal.

Printers (5) - Xerox WorkCenter 3335 = \$349 USD / printer

= \$3,833 USD subtotal.

Phones (20) - Cisco 7960 = \$365.00 USD / phone

= \$7,300 USD subtotal.

PCs (20) - Acer Aspire 3.7 GHz 512 GB SSD 12 DB RAM = \$500 USD / pc

= \$16,733 USD subtotal.

FTP Server (1) - HPE ProLiant DL380 = \$2,438 USD / server

= \$19,171 USD subtotal.

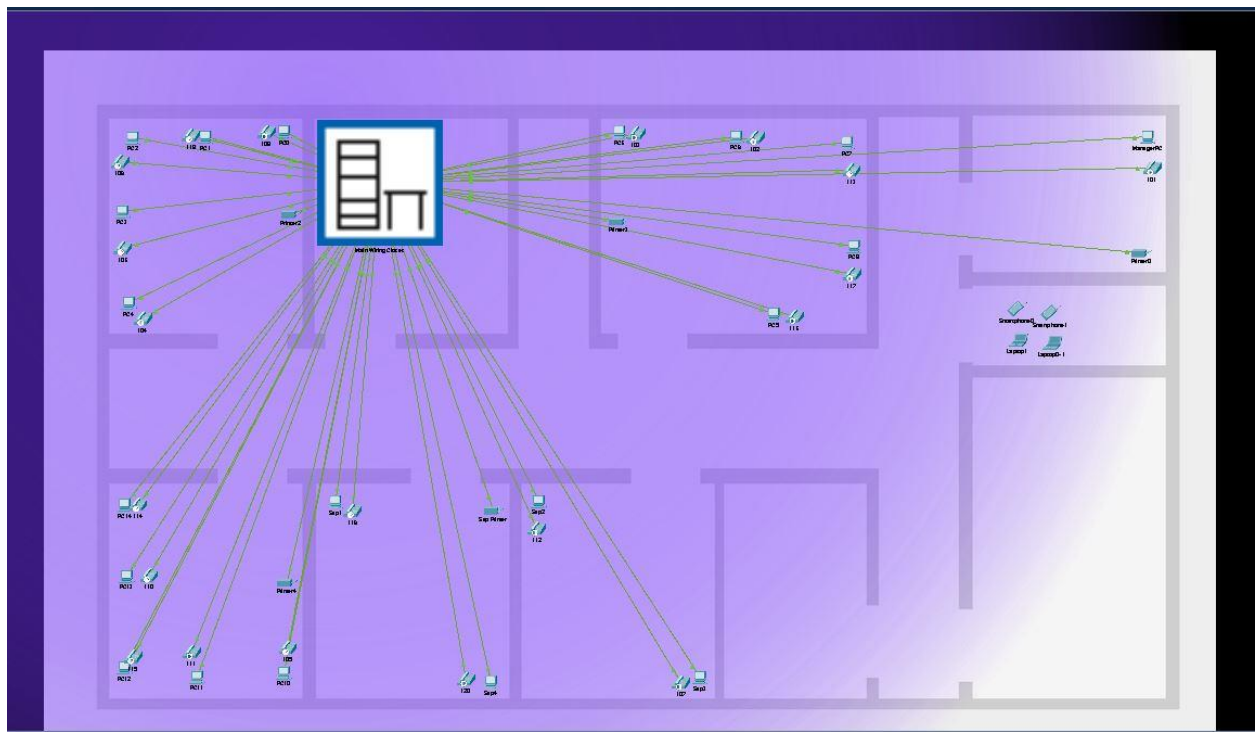
DNS/DHCP Servers (2) - PowerEdge T340 Tower Server = \$1,613 USD / server

= \$22,964 USD Total

Design (Jared):

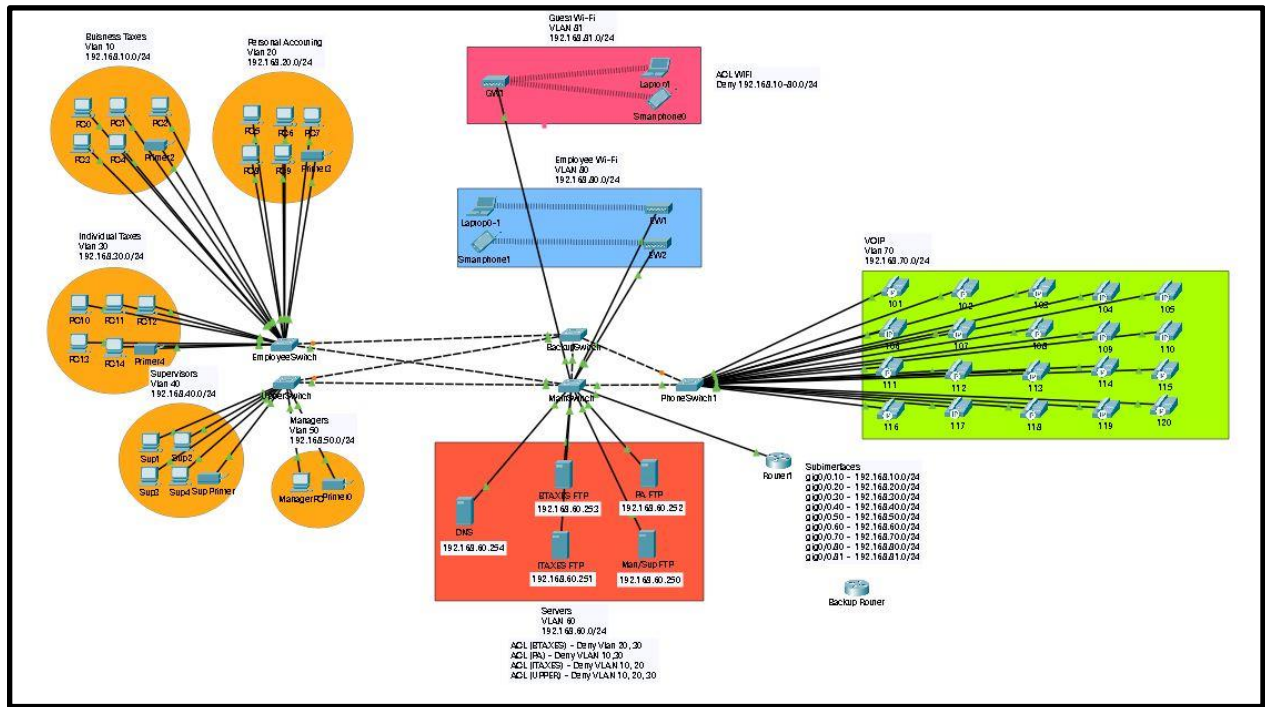
Physical Design

Our network design consists of three offices for each department, two offices for supervisors, and a manager's office. Each employee has their own Cisco IP phone. All connections lead to the main wiring closet. It was divided evenly so that there are only 5 employees in 1 room so as to not overcrowd the room. The manager's office will of course have his own office and the supervisor's office is shared as there are only 2 people. The printers for employee use are all in their own room to make more room for them but there is a personal printer for the manager himself.



Logical Design

Network Diagram



I. VLANs

The network is broken down into segments otherwise known as VLANs. VLANs provide QoS, scalability, security, and network segmentation. Each VLAN is assigned a subnet and it can contain 254 possible hosts. All VLANs are based on the 192.168.0.0 address. However, the third octet is based on their VLAN number. Both the main and backup switch use trunk ports that carry the traffic of more than one VLAN. Meanwhile, some ports on the “EmployeeSwitch,” “Phone switch,” and “UpperSwitch” use access ports to carry the traffic of one VLAN.

Table of VLANs:

<u>VLAN Number</u>	<u>Service</u>	<u>Subnet</u>
10	Business Taxes	192.168.10.0/24
20	Personal Accounting	192.168.20.0/24
30	Individual Taxes	192.168.30.0/24
40	Supervisors	192.168.40.0/24
50	Managers	192.168.50.0/24
60	Servers	192.168.60.0/24
70	VOIP	192.168.70.0/24
80	Employee Wi-Fi	192.168.80.0/24
81	Guest Wi-Fi	192.168.81.0/24

II. DHCP

All hosts except our servers are automatically assigned IPV4 addresses using DHCP. We do not use a dedicated DHCP server because DHCP are a relatively light load. Instead, the DHCP service is running on our router. In the router's configuration, each VLAN has its own DHCP pool except for VLAN 60. With DHCP pools, PC's, IP phones, and smartphones can quickly receive IPV4 addresses. For example, if an employee from the Personal Accounting department requests an IPV4 address, they will receive an IPV4 address within the range of 192.168.20.1 - 192.168.20.254. To prevent confusion, IPV4 addresses that contain a 0 in the fourth octet are excluded.

DHCP Pool Table

<u>DHCP Pool Name</u>	<u>Starting Index</u>	<u>Ending Index</u>
BTAXES	192.168.10.1	192.168.10.254
PA	192.168.20.1	192.168.20.254
ITAXES	192.168.30.1	192.168.30.254
SUP	192.168.40.1	192.168.40.254
MAN	192.168.50.1	192.168.50.254
VOIP	192.168.70.1	192.168.70.254
EW	192.168.80.1	192.168.80.254
GW	192.168.81.1	192.168.81.254

III. FTP, DNS

In our network design, the most important VLAN is VLAN 60 otherwise known as the Server VLAN. The Server VLAN contains the company's FTP servers and DNS server. Each server is statically assigned an IPV4 address with DHCP disabled. The DNS server's sole purpose is to provide human readable domain names to each FTP server. These human readable domain names are associated with a certain department. For example, the department, Business Taxes, is given the domain name, www.btaxes.com. Using the department's associated domain name, department members can login to the FTP server using a username and password. Once a user logs in, they have the ability to read, write, delete, rename, and list files. Supervisors and managers have their own FTP that no other department can access.

DNS Records

DNS

DNS Service

☒ On ☐ Off

Resource Records

Name

www.btaxes.com

Type

A Record

Address

192.168.60.253

Add

Save

Remove

No.	Name	Type	Detail
0	www.btaxes.com	A Record	192.168.60.2...
1	www.itaxes.com	A Record	192.168.60.2...
2	www.manftp.com	A Record	192.168.60.2...
3	www.pa.com	A Record	192.168.60.2...

FTP Usernames and Passwords

BTAXES FTP

Physical

Config

Services

Desktop

Programming

Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

FTP

Service

☒ On ☐ Off

User Setup

Username

Password

☐ Write ☐ Read ☐ Delete ☐ Rename ☐ List

	Username	Password	Permission
1	BTAXES	Password	RWDNL
2	MAN_1	Password	RWDNL
3	SUP_1	Password	RWDNL
4	cisco	cisco	RWDNL

Add

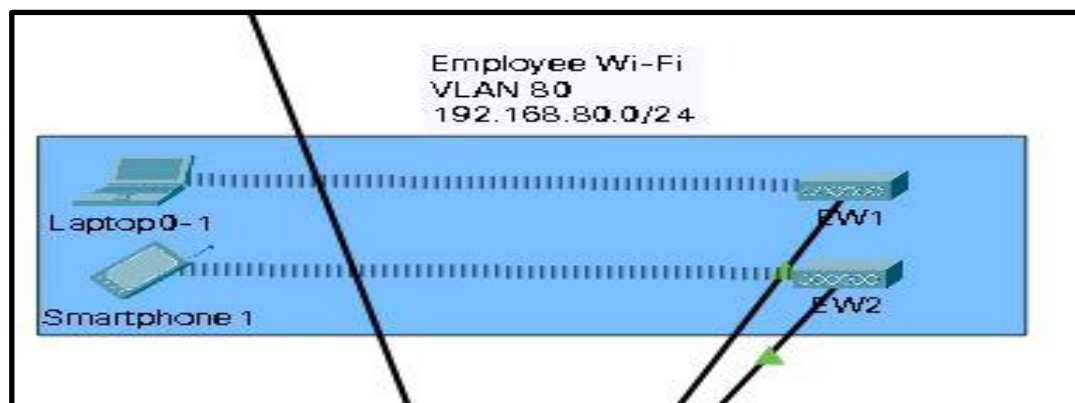
Save

Remove

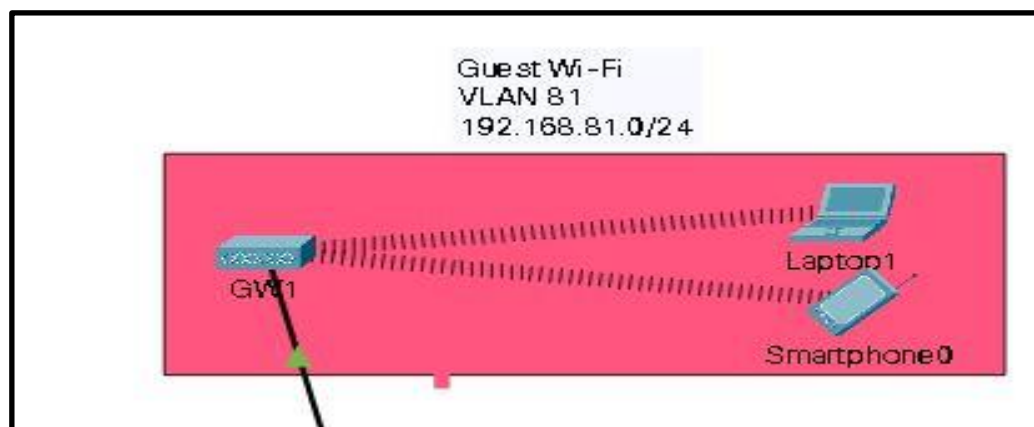
IV. Employee, Guest Wi-Fi

The network's employee Wi-Fi is hosted under VLAN 80 and subnet 192.168.80.0/24. The employee Wi-Fi has two access points with WPA-2 Encryption. Employees who connect to the employee Wi-Fi will automatically be assigned an IPV4 address and have access to the network. The network's guest Wi-Fi is hosted under VLAN 81 and uses subnet 192.168.81.0/24. The guest Wi-Fi contains only one access point with WPA-2 Encryption. Guests who connect to the guest Wi-Fi will automatically be assigned an IPV4 address. However, they cannot communicate with employees, servers, or the VOIP system.

Employee Wi-Fi Diagram



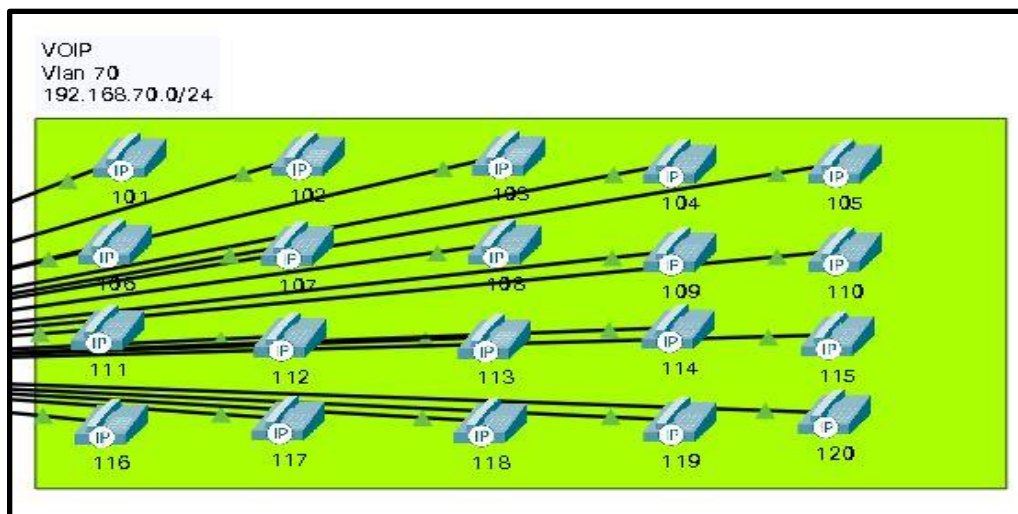
Guest Wi-Fi Diagram



V. VOIP

Every employee including department members, supervisors, and managers have access to a Cisco 7690 IP phone. Employees can easily call a department member, supervisor, or manager with no latency. The IP phones are hosted under VLAN 70 using subnet 192.168.70.0/24. Each IP phone is automatically assigned an IP address. In addition, IP phones have their own extension number. The extension number goes from 101 to 120.

VOIP Diagram



Development (Jared)

While developing our network design, we wanted to implement a scalable, redundant, and secure network for startup companies looking to expand. In this chapter, we'll be focusing on specific features that make our network design scalable, redundant, and secure.

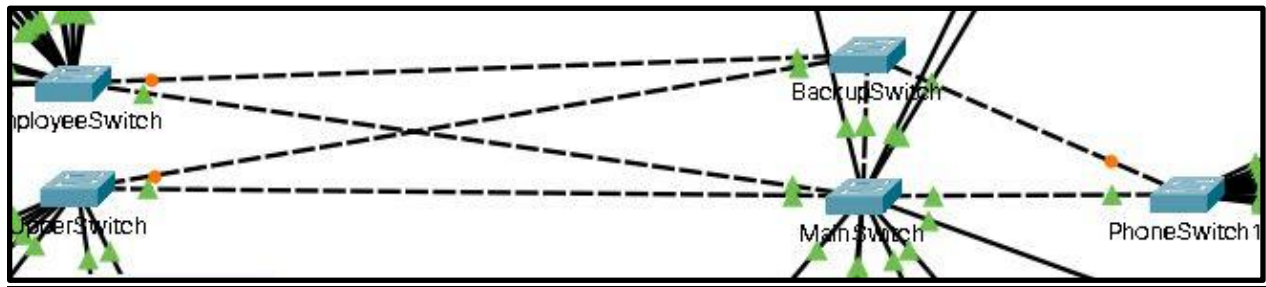
1. Scalability

Network scalability refers to the ability to increase or decrease hardware within a network. Network scalability is achievable with our network design because of VLANs. With our VLANs, the startup company could easily add more switches, servers, or hosts to the network. To add more switches, the startup company could simply attach new switches to either the main or backup switch. For hosts, the startup company could connect new hosts to the new switches. All they would have to do is put the new host in their assigned VLAN. For servers, the startup company could easily add more servers. There's a separate VLAN dedicated to segmenting the servers from the other hosts.

2. Redundancy

Our network design consists of two features to improve network redundancy. First, we have a primary root switch and a secondary root switch. The primary root switch otherwise known as the main switch is where all traffic is directed to. In case a connection between the host device and the main switch shuts down, the secondary root switch will automatically turn on. All traffic will be sent to the secondary root switch. Lastly, our network design contains a backup router. The backup router has the same configurations as the primary router. In case the primary router fails, the backup router can easily take its place.

Redundancy Diagram



3. Security

Our network design consists of four network security features. First, every switch and router use an encrypted password. By default, Cisco passwords are stored in clear text form. By using “service password-encryption,” clear text passwords are encrypted with MD5 protocol. With password encryption, rogue users will not be able to log into the router or view the running configuration.

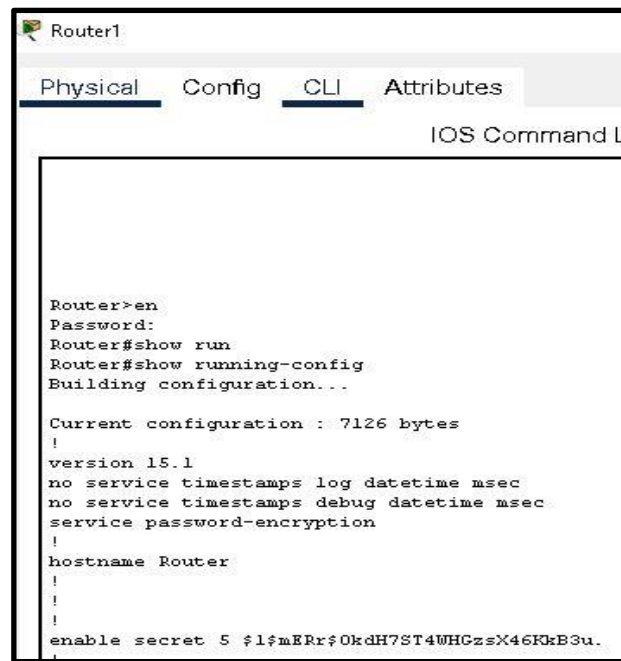
The second security feature our network design uses is DHCP Snooping. DHCP Snooping is a layer 2 security feature that prevents unauthorized devices from receiving or sending DHCP requests. DHCP Snooping prevents attacks such as DHCP Spoofing and DHCP Starvation. Certain employee devices are trusted to receive DHCP requests. For example, if a rogue PC tried to access VLAN 10, it would not receive an IPV4 address because it’s untrusted.

The third security feature our network design uses is port security. By default, interfaces on a Cisco switch are turned on. Any attacker could plug their PC, laptop, or smartphone into an open port causing a breach within the network. With port security, the MAC address of a trusted device is tied to a specific switch port. If a rogue computer, laptop, or smartphone tries to use a

port on any switch. The switch will automatically shut down the connection. Thus, the rogue user cannot access the network.

Lastly, our network design uses an Extended Access Control List (ACL). The router stores all extended ACLs. The extended ACLs determine what traffic can access certain parts of the network. We decided to implement extended ACLs for better network performance, improve segmentation, and prevent potential security breaches. For our network design, our ACLs are used for the FTP servers and the guest Wi-Fi. For the FTP servers, department members can only access their assigned FTP server. For example, an employee working in Individual Taxes, cannot access the Personal Accounting FTP server or the Business Taxes FTP server. If the employee wants to ping a different FTP server, the router will not send the packet. For the guest Wi-Fi, guests cannot communicate with the FTP servers, employees, or the VOIP system. If a guest attempts to ping an internal host, the router will not send the packet.

MD5 Encryption

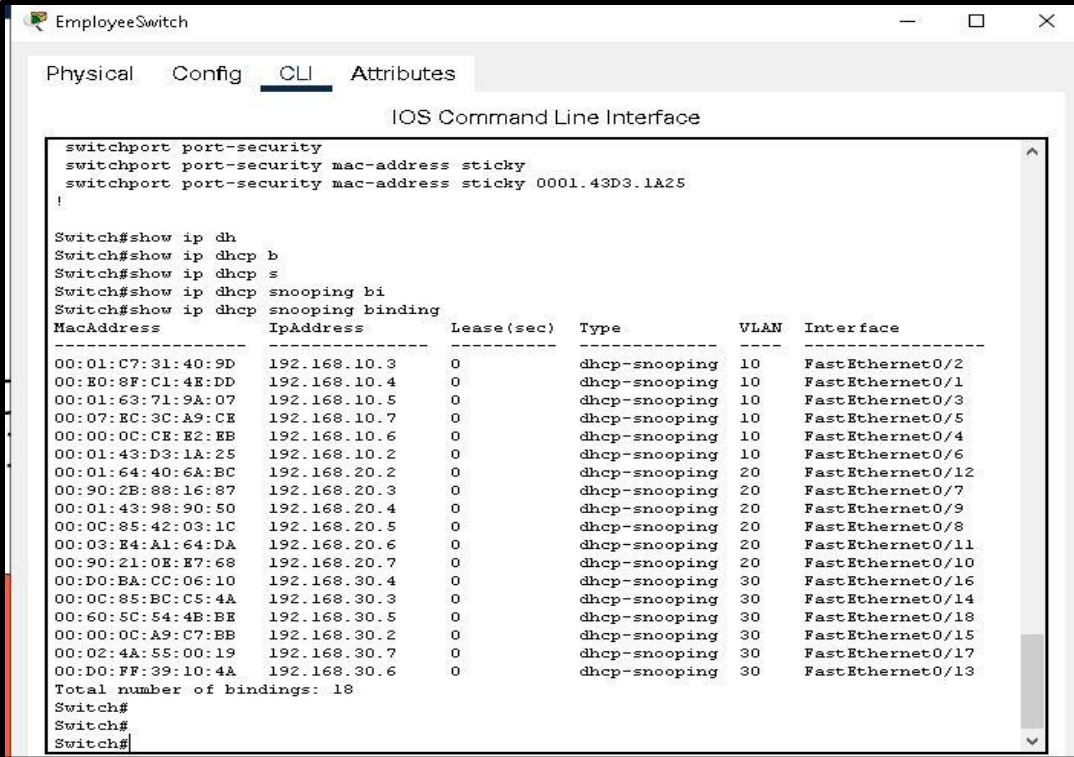


```
Router1
Physical Config CLI Attributes
IOS Command Line

Router>en
Password:
Router#show run
Router#show running-config
Building configuration...

Current configuration : 7126 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!
!
!
enable secret 5 $1$mERr$0kdH7ST4WHGzsX46FkB3u.
```

DHCP Snooping Example



```
EmployeeSwitch
Physical Config CLI Attributes
IOS Command Line Interface

switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0001.43D3.1A25
!

Switch#show ip dh
Switch#show ip dhcp b
Switch#show ip dhcp s
Switch#show ip dhcp snooping bi
Switch#show ip dhcp snooping binding
-----
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
00:01:C7:31:40:9D 192.168.10.3    0           dhcp-snooping  10    FastEthernet0/2
00:E0:8F:C1:4E:DD 192.168.10.4    0           dhcp-snooping  10    FastEthernet0/1
00:01:63:71:9A:07 192.168.10.5    0           dhcp-snooping  10    FastEthernet0/3
00:07:EC:3C:A9:CE 192.168.10.7    0           dhcp-snooping  10    FastEthernet0/5
00:00:0C:CE:E2:EB 192.168.10.6    0           dhcp-snooping  10    FastEthernet0/4
00:01:43:D3:1A:25 192.168.10.2    0           dhcp-snooping  10    FastEthernet0/6
00:01:64:40:6A:BC 192.168.20.2    0           dhcp-snooping  20    FastEthernet0/12
00:90:2B:88:16:87 192.168.20.3    0           dhcp-snooping  20    FastEthernet0/7
00:01:43:98:90:50 192.168.20.4    0           dhcp-snooping  20    FastEthernet0/9
00:0C:85:42:03:1C 192.168.20.5    0           dhcp-snooping  20    FastEthernet0/8
00:03:E4:A1:64:DA 192.168.20.6    0           dhcp-snooping  20    FastEthernet0/11
00:90:21:0E:E7:68 192.168.20.7    0           dhcp-snooping  20    FastEthernet0/10
00:D0:BA:CC:06:10 192.168.30.4    0           dhcp-snooping  30    FastEthernet0/16
00:0C:85:BC:C5:4A 192.168.30.3    0           dhcp-snooping  30    FastEthernet0/14
00:60:5C:54:4B:BE 192.168.30.5    0           dhcp-snooping  30    FastEthernet0/18
00:00:0C:A9:C7:EB 192.168.30.2    0           dhcp-snooping  30    FastEthernet0/15
00:02:4A:55:00:19 192.168.30.7    0           dhcp-snooping  30    FastEthernet0/17
00:D0:FF:39:10:4A 192.168.30.6    0           dhcp-snooping  30    FastEthernet0/13
Total number of bindings: 18
Switch#
Switch#
Switch#
```

Port Security Example

```
Switch#show po
Switch#show port-security a
Switch#show port-security address
```

Secure Mac Address Table				
Vlan	Mac Address	Type	Ports	Remaining Age (mins)
10	00E0.8FC1.4EDD	SecureSticky	FastEthernet0/1	-
10	0001.C731.409D	SecureSticky	FastEthernet0/2	-
10	0001.6371.9A07	SecureSticky	FastEthernet0/3	-
10	0000.0CCE.E2EB	SecureSticky	FastEthernet0/4	-
10	0007.EC3C.A9CE	SecureSticky	FastEthernet0/5	-
10	0001.43D3.1A25	SecureSticky	FastEthernet0/6	-
20	0090.2B88.1687	SecureSticky	FastEthernet0/7	-
20	000C.8542.031C	SecureSticky	FastEthernet0/8	-
20	0001.4398.9050	SecureSticky	FastEthernet0/9	-
20	0090.210E.E768	SecureSticky	FastEthernet0/10	-
20	0003.E4A1.64DA	SecureSticky	FastEthernet0/11	-
20	0001.6440.6ABC	SecureSticky	FastEthernet0/12	-
30	00D0.FF39.104A	SecureSticky	FastEthernet0/13	-
30	000C.85BC.C54A	SecureSticky	FastEthernet0/14	-
30	0000.0CA9.C7BE	SecureSticky	FastEthernet0/15	-
30	00D0.BACC.0610	SecureSticky	FastEthernet0/16	-
30	0002.4A55.0019	SecureSticky	FastEthernet0/17	-
30	0060.5C54.4BBE	SecureSticky	FastEthernet0/18	-

Extended ACL Table:





```
Router>en
Password:
Router#show ac
Router#show access-lists
Extended IP access list BTAXES
 10 deny ip 192.168.10.0 0.0.0.255 host 192.168.60.252
 20 deny ip 192.168.10.0 0.0.0.255 host 192.168.60.251
 30 deny ip 192.168.10.0 0.0.0.255 host 192.168.60.250
 40 deny ip 192.168.10.0 0.0.0.255 192.168.81.0 0.0.0.255
 50 permit ip any any (12 match(es))
Extended IP access list PA
 10 deny ip 192.168.20.0 0.0.0.255 host 192.168.60.253
 20 deny ip 192.168.20.0 0.0.0.255 host 192.168.60.251
 30 deny ip 192.168.20.0 0.0.0.255 host 192.168.60.250
 40 deny ip 192.168.20.0 0.0.0.255 192.168.81.0 0.0.0.255
 50 permit ip any any (12 match(es))
Extended IP access list ITAXES
 10 deny ip 192.168.30.0 0.0.0.255 host 192.168.60.253
 20 deny ip 192.168.30.0 0.0.0.255 host 192.168.60.252
 30 deny ip 192.168.30.0 0.0.0.255 host 192.168.60.250
 40 deny ip 192.168.30.0 0.0.0.255 192.168.81.0 0.0.0.255
 50 permit ip any any (12 match(es))
Extended IP access list UPPER
 10 deny ip 192.168.40.0 0.0.0.255 192.168.81.0 0.0.0.255
 20 deny ip 192.168.50.0 0.0.0.255 192.168.81.0 0.0.0.255
 30 permit ip any any (16 match(es))
Extended IP access list WIFI
 10 deny ip 192.168.81.0 0.0.0.255 192.168.10.0 0.0.0.255
 20 deny ip 192.168.81.0 0.0.0.255 192.168.20.0 0.0.0.255
 30 deny ip 192.168.81.0 0.0.0.255 192.168.30.0 0.0.0.255
 40 deny ip 192.168.81.0 0.0.0.255 192.168.40.0 0.0.0.255
 50 deny ip 192.168.81.0 0.0.0.255 192.168.50.0 0.0.0.255
 60 deny ip 192.168.81.0 0.0.0.255 192.168.70.0 0.0.0.255
 70 deny ip 192.168.81.0 0.0.0.255 192.168.80.0 0.0.0.255
 80 deny ip 192.168.81.0 0.0.0.255 host 192.168.60.253
 90 deny ip 192.168.81.0 0.0.0.255 host 192.168.60.252
100 deny ip 192.168.81.0 0.0.0.255 host 192.168.60.251
110 deny ip 192.168.81.0 0.0.0.255 host 192.168.60.250
```


Evaluation (Raj)

Solution Testing

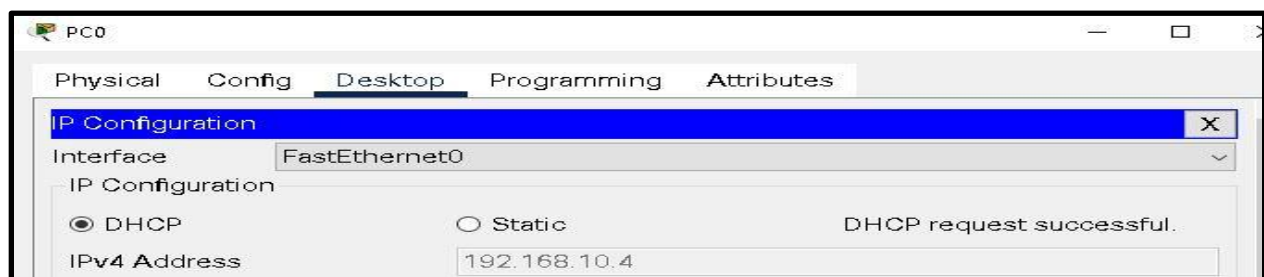
After setting up and organizing our network, to ensure that our programs were working properly, we conducted a few tests. First, we conducted multiple ping requests to ensure that the response time was appropriate. In doing so, we proved that different hosts were reachable across the IPV4 network. In the image below, an employee in Business Taxes attempts to ping an employee from Personal Accounting.

Ping Example

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Successful	PC0	PC1	ICMP		0.000
	Successful	PC0	PC5	ICMP		0.000

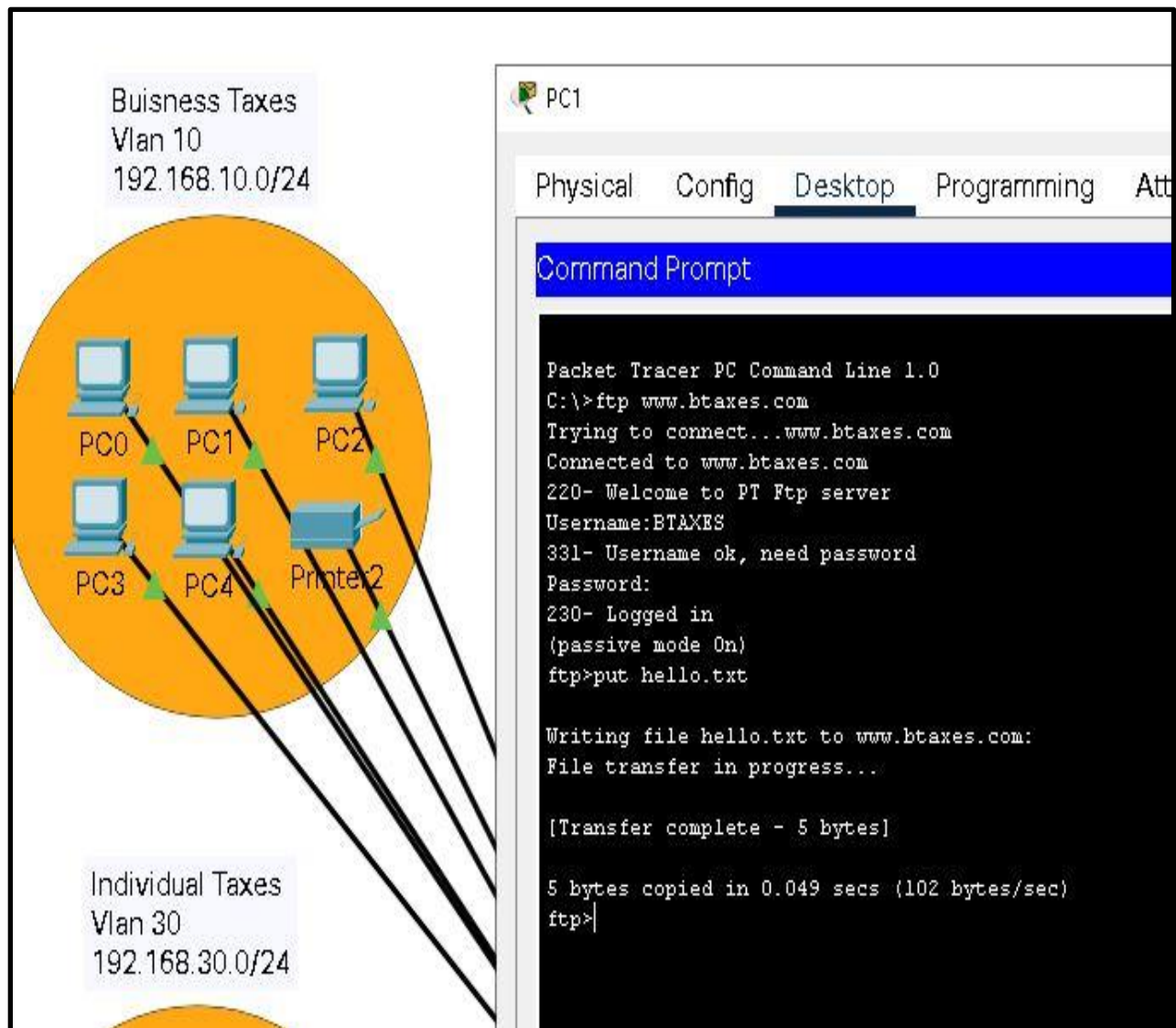
We went further into the testing process by even checking for DHCP requests. So first we sent out a Discover message to find out the DHCP server (Router). Then, the DHCP server (Router) received the message. It sent back a DHCP offer message. The offer message was received back from the DHCP server (Router) and a DHCP request message was sent back. The DHCP server (Router) acknowledged our request and gave us permission to use a dynamic IPV4 address.

Successful DHCP Request



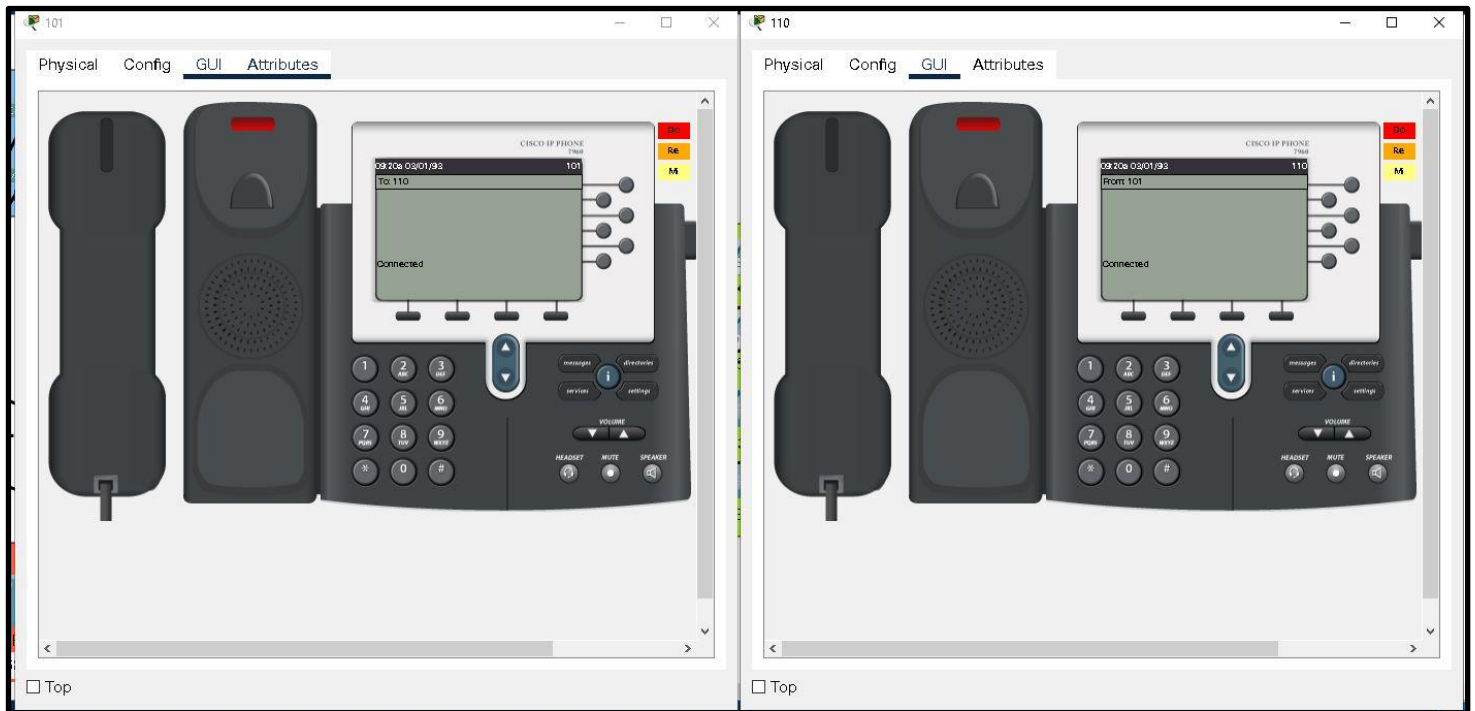
For FTP and DNS, we made sure designated employees could access their assigned FTP server using their username and password. In the example below, an employee from Business Taxes could successfully connect to the FTP server and send a file to it.

Successful FTP Connection



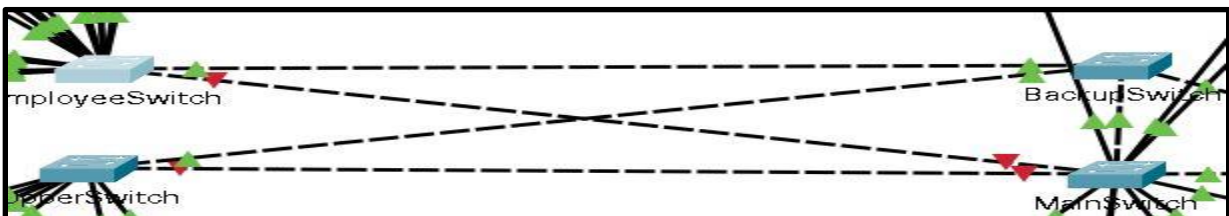
To fully test our VOIP system, we attempted to call from extension number 101 to 110. As you can see below, both phones were able to connect to each other.

Successful Phone Call



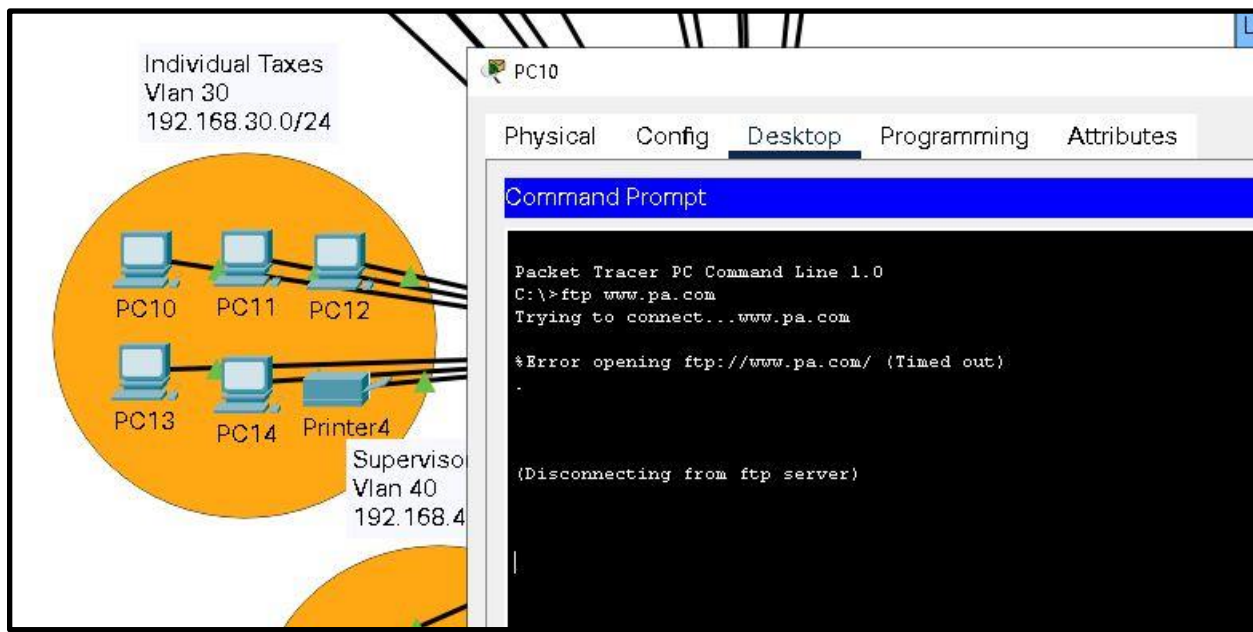
We also checked to make sure that there was network redundancy so that data properly flowed within the network. There are different channels that data can flow in the case of a failure. Even though the connection to the main switch was lost, it was still able to connect to the backup switch.

Redundancy Test



To make sure our extended ACL was fully working, an employee from Individual Taxes will try to connect to Personal Accounting's FTP server. As you can see below, the employee was unable to access the FTP server.

Blocked FTP Attempt



Lastly, to make sure guests cannot communicate with employees, managers, IP phones, or servers, we tried multiple ping attempts. As you can see, the guest could not communicate with any of the departments or services.

Blocked Guest Connection

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	Laptop1	PC5	ICMP		0.000	N	0	(edit)	
	Failed	Laptop1	PC0	ICMP		0.000	N	1	(edit)	
	Failed	Laptop1	PC10	ICMP		0.000	N	2	(edit)	
	Failed	Laptop1	Sup1	ICMP		0.000	N	3	(edit)	
	Failed	Laptop1	ManagerPC	ICMP		0.000	N	4	(edit)	
	Failed	Laptop1	BTAXES FTP	ICMP		0.000	N	5	(edit)	
	Failed	Laptop1	101	ICMP		0.000	N	6	(edit)	

Team Conclusions

We were able to achieve our two goals of creating a working network design on Packet Tracer and implementing realistic costs and equipment needs for the accounting firm. When designing the network, we made sure to take into consideration all the potential issues that could arise as well as any gaps. This way we were able to proactively handle all the problems before they arose. Fixing the problems after the fact would've been much harder to tackle so we wanted to take care of it in the developmental phase of the process. As is for any project in any field, a team must keep in mind the budget for the project so as not to run into financial stresses. Since we prepared the budget right at the get go, everyone knew the limits to keep in mind and spend as efficiently as possible. In fact, this way we were able to find the best products in the market to do the job and make sure the accounting firm's needs were well taken care of.

Works Cited

Dynamic Host Configuration Protocol (DHCP). Microsoft. 29 Apr. 2021.

<https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top#:~:text=DHCP%20allows%20hosts%20to%20obtain,other%20information%20to%20DHCP%20clients>. Accessed 1 May 2022.

Kerner, Sean. *FTP (File Transfer Protocol)*. (n.d).

<https://www.techtarget.com/searchnetworking/definition/File-Transfer-Protocol-FTP>. Accessed 1 May 2022.

Port Security in Computer Network. Geeksforgeeks. 15 Mar. 2022.

<https://www.geeksforgeeks.org/port-security-in-computer-network/>. Accessed 1 May 2022.

Access Control List (ACL). Imperva. (n.d).

<https://www.imperva.com/learn/data-security/access-control-list-acl/>. Accessed 1 May 2022.

service password-encryption command. Geekuniversity. (n.d).

<https://geek-university.com/service-password-encryption-command/>. Accessed 1 May 2022.

Voice Over Internet Protocol (VoIP). Federal Communications Commission. (n.d).

[https://www.fcc.gov/general/voice-over-internet-protocol-voip#:~:text=Voice%20over%20Internet%20Protocol%20\(VoIP\)%2C%20is%20a%20technology%20that,\(or%20analog\)%20phone%20line](https://www.fcc.gov/general/voice-over-internet-protocol-voip#:~:text=Voice%20over%20Internet%20Protocol%20(VoIP)%2C%20is%20a%20technology%20that,(or%20analog)%20phone%20line). Accessed 1 May 2022.