



University of New Haven

CSCI-6649-03 Enterprise Network Project

Spring 2023

Project Final Report

Under

Prof. Luis Rivera

Fresh Connections (Grocery chain network)

By:

Neha Singam (00770807)

Nishchal Sreevathsa (00803363)

Pavan Kumar Davar (00770542)

Nitesh Yalamanchili (00794536)

Chandralekha Podili (00770060)

Table of Contents

1	Abstract	4
2	Introduction.....	4
3	Customer Needs and Goals	5
3.1.1	Needs	5
3.1.2	Goals	5
4	Analyzing Technical Goals and Tradeoffs	6
4.1	Technical Goals	6
4.2	Trade-offs	6
5	Analyzing Business Goals and Constraints.....	7
5.1	Business Goals	7
5.2	Business Constraints	7
6	Applications Requirements.....	7
7	Locations and Number of Users	8
7.1	Outline of the Network.....	8
7.2	Locations and Number of Users.....	9
7.3	Network Applications	10
7.4	Branch Networks	10
8	Data Storage Requirements.....	11
8.1	Data Stores	11
9	Network Architecture	12
9.1	Network Requirements	13
9.2	Network Topology	14
9.2.1	Cisco packet tracer for Network Design	15
9.2.2	VLAN	15
9.2.3	Physical Network Devices	16
10	Existing Network Design	17
10.1	Present Solution	17
10.2	Network Map:.....	18
11	Network Design	18
11.1	Proposed solution.....	18
11.2	Logical Network Design	20
11.3	Physical Network Design.....	21
11.3.1	Physical Design of Server Environment	21

11.3.2	Physical Design of Main Office.....	22
11.3.3	Physical Design of Branch offices.....	23
11.3.4	Physical Design of Cloud connectivity and Firewall	23
11.4	IP Addressing Scheme:.....	24
11.5	Routing Protocols:	24
11.6	Security and Network Management Strategies.....	26
12	Network Testing	27
12.1	DNS Server	27
12.2	Email Server	28
12.3	Web Server	29
12.4	DHCP Pool.....	29
12.5	Router Configuration	31
12.6	Firewall Configuration	32
12.7	FTP Server	33
12.8	Ping Screenshots.....	34

1 Abstract

This enterprise network project aims to design a secure and scalable network infrastructure for Fresh Connections, a grocery network with multiple locations. The project will focus on improving the company's operational efficiency, enhancing security, and providing better connectivity and communication between stores, suppliers, and customers.

To achieve this, a comprehensive analysis of the current network infrastructure, business requirements, and future growth plans of Fresh Connections will be conducted. Based on the analysis, a network design will be proposed that will include the implementation of a secure and reliable Wide Area Network (WAN) to interconnect all store locations, a robust Local Area Network (LAN) to support daily operations, and a centralized data center to manage and store critical business data.

To ensure data security, advanced security measures such as firewalls, intrusion detection and prevention systems, and virtual private networks (VPNs) will be integrated. Cloud-based services and virtualization technologies will also be adapted to provide scalable and cost-effective network solutions.

The successful implementation of this enterprise network project will enable Fresh Connections to streamline its operations, improve communication and collaboration, and enhance its overall customer experience. By achieving these goals, Fresh Connections will be better equipped to meet the demands of its customers and achieve its growth objectives.

Bottom of Form

2 Introduction

Fresh Connections, a grocery network that operates multiple stores across various regions, requires a reliable enterprise network to optimize its operations and increase efficiency. This report provides a detailed overview of a proposed enterprise network project designed to meet the specific requirements and objectives of Fresh Connections.

The report begins by analyzing the existing network infrastructure of Fresh Connections and the challenges and limitations it poses. This is followed by a thorough discussion of the objectives and requirements of the proposed network project, which include improving performance, enhancing security, and simplifying network management.

The proposed network topology and architecture are then presented, outlining the hardware and software components that will be used to build the network. The network design includes multiple layers of security, such as firewalls, intrusion prevention systems, and VPNs, to ensure maximum protection against external threats.

Furthermore, the report details the selection of network protocols and technologies, including the use of VLANs, QoS, and MPLS to optimize network performance and minimize latency. The network management and monitoring tools to be used for maintenance and troubleshooting are also outlined.

The report concludes with a cost-benefit analysis of the proposed project, highlighting the expected benefits and the estimated costs associated with implementing the new network infrastructure. Overall, the report provides a comprehensive plan for the design and implementation of an enterprise network project tailored to the specific needs of Fresh Connections.

3 Customer Needs and Goals

3.1.1 Needs

1. Reliability: The network needs to be reliable and ensure minimal downtime. Customers need to be able to access the services without any interruptions.
2. Security: The network should be designed with strong security measures to protect customer and company data from unauthorized access, hacking, and malware attacks.
3. Scalability: The network should be scalable to accommodate future growth and expansion. This is especially important for a growing grocery network like Fresh Connections.
4. Cost-effective: The network design should be cost-effective while meeting all the requirements and needs of the customers.
5. Speed: Customers expect fast and efficient service, and the network design should support high-speed data transfer.

3.1.2 Goals

1. Efficient and seamless communication: Customers need to be able to communicate with each other and with the company easily and without any delay.
2. Improved productivity: The network should be designed to improve employee productivity by providing faster access to data, applications, and services.
3. Enhanced customer experience: The network should enable Fresh Connections to provide a superior customer experience through faster checkout times, real-time inventory updates, and personalized promotions.
4. Centralized management: The network design should enable Fresh Connections to manage its operations centrally, with real-time visibility into all aspects of the network.
5. Business agility: The network design should enable Fresh Connections to quickly respond to changing market conditions and customer needs, and to launch new services and products more efficiently.

4 Analyzing Technical Goals and Tradeoffs

4.1 Technical Goals

The following are the technical goals that should be met when designing the enterprise network for Fresh Connections:

Scalability: The network design should be scalable to accommodate the growth of the grocery network. This includes adding new locations and users as well as increasing the bandwidth requirements.

High Availability: The network should be highly available to ensure that the grocery network operations are not disrupted. This includes implementing redundancy and failover mechanisms for critical network components.

Security: The network should be designed with security in mind to protect against unauthorized access, data breaches, and other cyber threats. This includes implementing firewalls, intrusion detection and prevention systems, and access control policies.

Performance: The network should provide high performance to support the grocery network operations. This includes optimizing the network architecture, implementing Quality of Service (QoS) mechanisms, and ensuring low latency.

Manageability: The network should be easy to manage and maintain. This includes implementing network management tools, monitoring and reporting mechanisms, and ensuring compliance with industry standards and regulations.

4.2 Trade-offs

When designing the enterprise network for Fresh Connections, the following trade-offs must be considered:

Cost vs. Performance: The cost of the network design should be balanced against the performance requirements. High-performance network components can be expensive, and it may not be feasible to implement them across the entire network.

Security vs. Usability: The network security measures may impact the usability of the network. For example, implementing strong authentication mechanisms may make it more difficult for users to access the network.

Scalability vs. Complexity: As the network grows, it may become more complex to manage and maintain. This can impact the scalability of the network, and the trade-off between scalability and complexity should be carefully considered.

Availability vs. Redundancy: Implementing redundancy mechanisms can increase network availability, but it can also increase the complexity of the network and impact performance.

Compatibility vs. Innovation: It is important to balance compatibility with existing systems and technologies with the desire for innovation. Upgrading the network to the latest technologies can improve performance and security, but it may also require replacing existing systems and disrupting network operations.

5 Analyzing Business Goals and Constraints

5.1 Business Goals

1. Improve network security: The enterprise network should be designed to ensure the highest levels of security to protect the sensitive data and information of the grocery network's customers, employees, and business operations.
2. Enhance network performance: The enterprise network should be designed to deliver high-speed connectivity and high bandwidth to enable smooth and efficient communication between different departments, employees, and customers.
3. Scalability and flexibility: The enterprise network should be scalable and flexible enough to accommodate future growth, new applications, and technologies without any significant disruptions to the current network.
4. Cost-effectiveness: The enterprise network should be designed to optimize the cost of implementation, maintenance, and support, while still meeting the performance, security, and scalability requirements of the grocery network.
5. Improve customer experience: The enterprise network should be designed to enable seamless online and offline transactions, fast checkout, and provide customers with superior shopping experience.

5.2 Business Constraints

1. Regulatory compliance: The enterprise network must comply with all relevant regulations, such as data privacy laws, financial regulations, and cybersecurity regulations.
2. Budget: The enterprise network design must be cost-effective and must fit within the budget constraints of the grocery network.
3. Timeframe: The enterprise network project must be completed within a specific timeframe to avoid any disruptions to the grocery network's operations.
4. Technical expertise: The enterprise network design and implementation must be done by qualified and experienced technical personnel to ensure its effectiveness and reliability.
5. Compatibility: The enterprise network design must be compatible with existing hardware, software, and applications already in use by the grocery network.

6 Applications Requirements

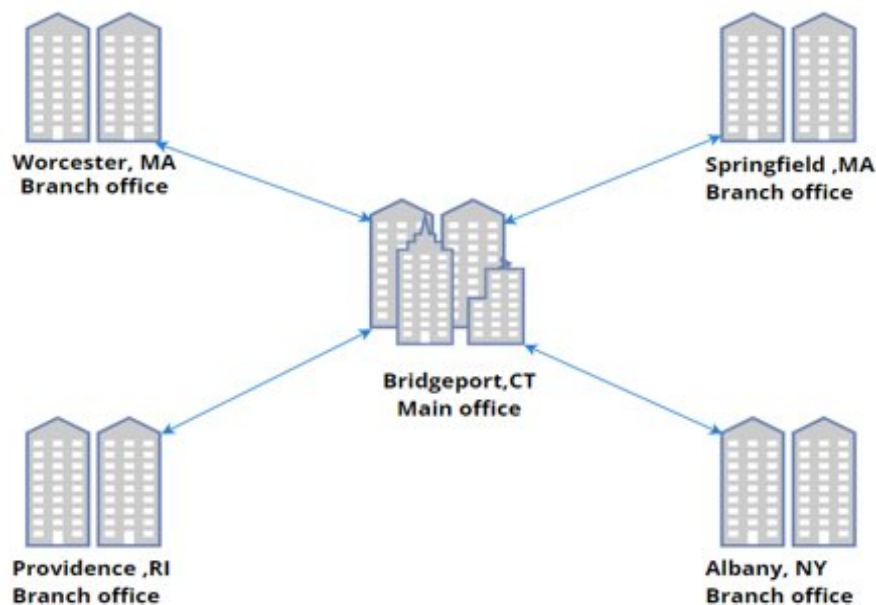
To design an enterprise network for Fresh Connections grocery network, the following applications are necessary:

1. Point of Sale (POS) System for sales transactions and inventory management.

2. Inventory Management System to keep track of stock levels and manage orders.
3. Customer Relationship Management (CRM) System to manage customer interactions and preferences.
4. Employee Management System to manage employee data, track attendance, and handle payroll processing.
5. Enterprise Resource Planning (ERP) System to provide an integrated view of business processes and data.
6. E-commerce Platform to sell products online and reach a wider customer base.
7. Business Intelligence (BI) System for data analytics and informed business decisions.
8. Network Security system with firewalls, intrusion detection systems, and antivirus software.

7 Locations and Number of Users

7.1 Outline of the Network



7.2 Locations and Number of Users

Fresh Connections is a grocery chain network with one main location in Bridgeport and four other locations in Albany, Worcester, Springfield, and Providence.

Bridgeport-Main Branch:

The Bridgeport main branch of Fresh Connections is a bustling center of grocery retail activity, located in the heart of the city. It is supported by a robust networking infrastructure and features a range of cutting-edge technologies and amenities.

Albany Branch:

The Albany branch is a hive of grocery shopping activity. It has a strong networking infrastructure to support it and communicates with partners and suppliers well.

Worcester Branch:

The Worcester branch is a key part of the company's grocery chain network. It is supported by an advanced networking infrastructure that enables efficient inventory management and exceptional customer service.

Springfield Branch:

The Springfield branch is a vibrant hub of grocery retail activity. It is supported by a sophisticated networking infrastructure that aids in making sure that products are always in stock and that customers can access the most recent news and special offers.

Providence Branch:

The Providence branch is a key part of the company's grocery chain network. It is backed by slashing networking infrastructure, which makes it possible to manage inventory effectively and provide excellent customer service.

Overall, the networking infrastructure of Fresh Connections is a key factor in the company's success as a leading grocery chain network, allowing it to manage operations effectively, optimize its supply chain, and deliver world-class customer support across all of its branches.

LOCATI ON	NUMBER OF EMPLOY EES	NUMBER OF DEVICE S	ESTIMATED NUMB ER OF CUSTOMERS	WEBSITE TRAFFIC (DAILY)	AVERAGE N ETWORK TR AFFIC (MBPS)
Store 1	25	15	500-700	1500-2000	100
Store 2	30	20	700-900	2000-2500	150
Store 3	20	15	400-600	1000-1500	80
Store 4	35	25	800-1000	2500-3000	200
Store 5	25	15	500-700	1500-2000	100

7.3 Network Applications

Network Applications	User Community Name	Number of Users	Applications	Total Bandwidth
Email	All Branches	70	Microsoft Exchange	2 Mbps
Web Browsing	All Branches	70	Google Chrome, Mozilla Firefox	3 Mbps
FTP File Transfer	All Branches	70	FileZilla	1 Mbps
Printers	All Branches	70	HP LaserJet	N/A

7.4 Branch Networks

Branch Networks	User Community Name	Number of Users	Applications	Total Bandwidth
Bridgeport	Employees	20	Email, Web Browsing, File Transfer	3 Mbps
	Payment Systems	20	FTP File Transfer	1 Mbps
Springfield	Employees	10	Email, Web Browsing, File Transfer	1.5 Mbps
	Payment Systems	15	FTP File Transfer	1 Mbps
Albany	Employees	20	Email, Web Browsing, File Transfer	3 Mbps
	Payment Systems	15	FTP File Transfer	1 Mbps
Providence	Employees	10	Email, Web Browsing, File Transfer	1 Mbps
	Payment Systems	10	FTP File Transfer	1 Mbps

Worcester	Employees	10	Email, Web Browsing, File Transfer	1.5 Mbps
	Payment Systems	15	FTP File Transfer	1 Mbps

8 Data Storage Requirements

8.1 Data Stores

Data Stores	Server Name	Location	Type	Storage Capacity
File Server	Bridgeport Server	Bridgeport	Network Attached Storage	2 TB
Database	Albany Server	Albany	Relational Database	1 TB
Backup	Springfield Server	Springfield	Tape Backup	100 GB

Server Traffic Flows

Servers Traffic Flows	Source	Destination	Protocol	Traffic Rate
Email Traffic	All Branches	Email Server	SMTP	1 Mbps
Web Traffic	All Branches	Web Server	HTTP	1.5 Mbps
File Transfer Traffic	All Branches	FTP Server	FTP	1 Mbps
DNS Traffic	All Branches	DNS Server	DNS	100 ps

9 Network Architecture

Designing a network for Fresh Connections, a grocery network, requires careful consideration of the network's requirements and goals. The following is the network architecture for this project:

- **Network Topology:** A hierarchical network topology is recommended for the Fresh Connections network. This topology divides the network into multiple layers, each with specific functions and responsibilities.
- **Core Layer:** At the core layer, a high-speed, reliable, and redundant backbone should be deployed to provide connectivity between all the other layers of the network. A pair of core switches are recommended for redundancy and reliability.
- **Distribution Layer:** The distribution layer provides aggregation points for access layer switches and implements policies that control the flow of traffic. For Fresh Connections, the distribution layer should be designed with redundancy in mind and should have switched with a high throughput capacity.
- **Access Layer:** The access layer provides network access to end devices such as cash registers, computers, printers, and security cameras. The access layer switches should be low-cost and easy to manage. These switches should be connected to the distribution layer for connectivity to the rest of the network.
- **VLANs:** A VLAN (Virtual Local Area Network) is a logical grouping of devices on a network. VLANs are used to segment traffic and to enhance security. For Fresh Connections, VLANs can be used to separate traffic between different departments, such as sales, marketing, and accounting.
- **Wireless Network:** Wireless access points should be deployed throughout the network to provide wireless connectivity to employees and customers. Wireless access points should be placed in strategic locations to provide coverage throughout the store and its parking lot.
- **Security:** Security is an important consideration in any network. For Fresh Connections, a firewall should be deployed at the perimeter to protect against external threats. Access control lists should be implemented to control traffic flow between different VLANs. Additionally, intrusion detection and prevention systems should be deployed to detect and prevent attacks.
- **Network Management:** A network management system should be deployed to monitor and manage the network. The management system should be able to identify and troubleshoot network problems quickly.
- **Redundancy and Resilience:** Redundancy and resilience are critical components of any enterprise network. For Fresh Connections, redundant switches, power supplies, and network connections should be deployed to ensure continuous network availability.

In conclusion, the suggested network architecture for the Fresh Connections grocery network is a hierarchical topology with a core, distribution, and access layer. VLANs should be used to segment traffic, and wireless access points should be deployed for wireless connectivity. Security measures should be implemented to protect against external threats, and a network management system should be deployed for monitoring and management. Redundancy and resilience should be incorporated into the design for continuous network availability.

9.1 Network Requirements

1. **Bandwidth Requirements:** The network should be designed to support high bandwidth requirements for the transfer of large amounts of data such as product information, inventory details, customer information, and financial transactions. The bandwidth should be scalable to accommodate future growth.
2. **Security:** The network should be designed with robust security features to protect against external threats such as hacking, viruses, and malware. The network should have firewalls, intrusion detection, and prevention systems, and encryption protocols.
3. **Redundancy:** The network should be designed to provide high availability and redundancy. This includes multiple Internet Service Providers (ISPs), redundant switches, and power backup systems to ensure that the network is always available.
4. **Scalability:** The network should be designed to support the growth of the grocery network. The network should be modular and scalable so that it can be easily expanded to meet the needs of the growing business.
5. **Quality of Service:** The network should be designed to support the Quality of Service (QoS) requirements of the business. This includes prioritization of data traffic to ensure that mission-critical applications such as inventory management and financial transactions are given priority over less critical traffic such as email.
6. **Mobile Access:** The network should be designed to support mobile devices such as smartphones and tablets. This includes providing secure access to business applications from mobile devices and ensuring that the network can handle the increased traffic from these devices.
7. **VoIP:** The network should be designed to support Voice over Internet Protocol (VoIP) communications. This includes ensuring that the network can handle the increased traffic from VoIP calls and providing the necessary Quality of Service (QoS) to ensure that call quality is not affected by other network traffic.
8. **Network Management:** The network should be designed with a robust network management system that allows for easy monitoring, management, and troubleshooting of

network issues. The system should provide real-time monitoring and alerts to ensure that issues are quickly identified and resolved.

9. Remote Access: The network should be designed to allow for remote access to business applications and data. This includes providing secure access to the network from remote locations such as home offices or remote branches.

10. Compliance: The network should be designed to comply with relevant regulations and standards such as PCI DSS (Payment Card Industry Data Security Standard) and GDPR (General Data Protection Regulation).

These are some of the key network requirements that are considered when designing an enterprise network project for Fresh Connections, a grocery network.

9.2 Network Topology

The network topology describes the layout of the network, including the devices, connections, and protocols used to facilitate communication. For Fresh Connections grocery chain, the network topology includes:

- **Centralized Main Cloud:** The main hub of the network that will host network services and provide a centralized point for network management and monitoring. Each branch will be connected to the main cloud via a router.
- **Branches:** There will be four sub-branches and one main branch, each of which will have a switch and DSL modem for internet connectivity. PCs and printers at each branch will be connected to the switch.
- **Routers:** Each branch will be connected to the main cloud via a router, which will facilitate communication between the branches and servers located in the main cloud.
- **Switches:** Each branch and the main cloud will have its own switch, which will connect the PCs and printers to the network and facilitate communication between devices within each branch.
- **Servers:** The main cloud will host several servers including an email server, FTP server, DNS server, web server, and DHCP server.
- **DSL Modems:** Each sub-branch and the main branch will have its own DSL modem for internet connectivity.

The network topology is designed to provide reliable and efficient communication between all branches and the main cloud. The centralized main cloud provides a point for network management and monitoring, while the routers, switches, and servers ensure efficient and secure network traffic. The use of DSL modems allows for internet connectivity in each branch. The network topology is also scalable and flexible to accommodate future growth and changes in technology.

The average load for this design is about 100 MBPS, and it supports up to 1.0 GBPS.

The average load for this design depends on the specific usage and traffic patterns of each branch. Assuming moderate usage, the network design should be able to support per branch without significant performance degradation. This means that the network should be capable of supporting multiple users simultaneously accessing the internet, email, and other basic business applications without experiencing major slowdowns or delays.

9.2.1 Cisco packet tracer for Network Design

1. Packet Tracer is a visual simulation tool designed by Cisco System. It allows users to create network topologies and imitate modern computer networks.
2. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.
3. Cisco Packet Tracer has two work- spaces—logical and physical. The logical workspace allows users to build logical network topologies by placing, connecting, and clustering virtual network devices by using a drag and drop user interface.
4. The physical workspace provides a graphical view of the logical network.
5. Using this on our network.

9.2.2 VLAN

A VLAN is a logical segment of a network that groups devices together based on their functionality or location. VLANs are created by network administrators to improve network performance, security, and management. Each VLAN operates as if it is a separate network, although devices in different VLANs can be physically located on the same network switch. VLANs allow network administrators to group devices that have similar network requirements and provide a way to manage traffic within a network more efficiently.

Benefits of VLANs:

The use of VLANs in a network offers several benefits, including:

Improved Network Performance: VLANs can be used to separate network traffic into smaller, more manageable segments, which can improve network performance by reducing congestion and improving bandwidth utilization.

Better Network Security: VLANs allow network administrators to create separate security domains, which can improve network security by preventing unauthorized access to sensitive resources.

Simplified Network Management: VLANs simplify network management by allowing administrators to group devices based on their location, function, or department, and manage them as a single entity.

Cost-Effective: VLANs can be implemented without the need for additional physical network equipment, which can make them a cost-effective solution for network segmentation.

9.2.3 Physical Network Devices

The physical network devices used for designing the project are as follows:

Cisco Catalyst 2960 Switches:

Cisco Catalyst 2960 switches are layer 2 switches that provide fast Ethernet and gigabit Ethernet connectivity for enterprise networks. They support advanced features like VLANs, Quality of Service (QoS), and security features like Access Control Lists (ACLs). They can also be managed using Cisco's Network Assistant software, making it easy to configure and manage a large number of switches. These switches can be used to connect different devices in the grocery network like servers, PCs, printers, and DSL modems.

Cisco 1841 Series Routers:

Cisco 1841 series routers are enterprise-class routers that provide high-performance connectivity between different networks. They are equipped with advanced security features, including VPN and firewall capabilities. They also support a variety of WAN technologies such as DSL, T1, and Frame Relay. These routers can be used to connect the grocery network to the Internet or to other external networks.

Network Cables:

Different types of network cables are used to connect devices within the grocery network. Copper straight through cables is used to connect end devices like PCs and printers to switches. Copper crossover cables are used to connect switches to each other. Serial DCE and DTE cables are used to connect routers to other devices such as modems.

Network Interface Cards:

Network Interface Cards (NICs) are used to connect end devices like PCs and printers to the network. They are available in different speeds such as 10/100/1000 Mbps and can be either wired or wireless.

Cisco 5505 ASA Firewall:

The Cisco 5505 ASA Firewall is a security appliance that provides enterprise-class firewall and VPN services. It is designed to protect the grocery network from unauthorized access and provide secure remote access for employees. It can also be used to inspect and filter network traffic to prevent malware and other malicious activity.

VLAN:

VLANs are logical networks that allow different devices on the same physical network to be separated into different groups. This can improve security and network performance by controlling the flow of network traffic. VLANs can be used to segregate different

departments within the grocery network, such as the accounting department and the marketing department.

DSL Modems:

DSL modems are used to connect the grocery network to the Internet over a digital subscriber line (DSL). They convert the digital signal from the network into an analog signal that can be transmitted over telephone lines.

Cisco Servers:

Cisco servers are enterprise-class servers that provide high-performance computing and storage for enterprise networks. They are designed to run mission-critical applications such as email, databases, and web servers.

Printers:

Printers are devices that allow documents and images to be printed on paper. They can be connected to the network using a wired or wireless connection and can be shared by multiple users.

PCs:

PCs, or personal computers, are end devices that are used by employees to perform different tasks such as email, word processing, and data entry. They can be connected to the network using a wired or wireless connection.

Cloud:

Cloud computing allows enterprises to access computing resources over the Internet. Cloud services can include storage, computing power, and software applications. Cloud computing can provide cost savings and increased flexibility for enterprises, as resources can be scaled up or down as needed. It can be used to host enterprise applications and data for the grocery network.

10 Existing Network Design

10.1 Present Solution

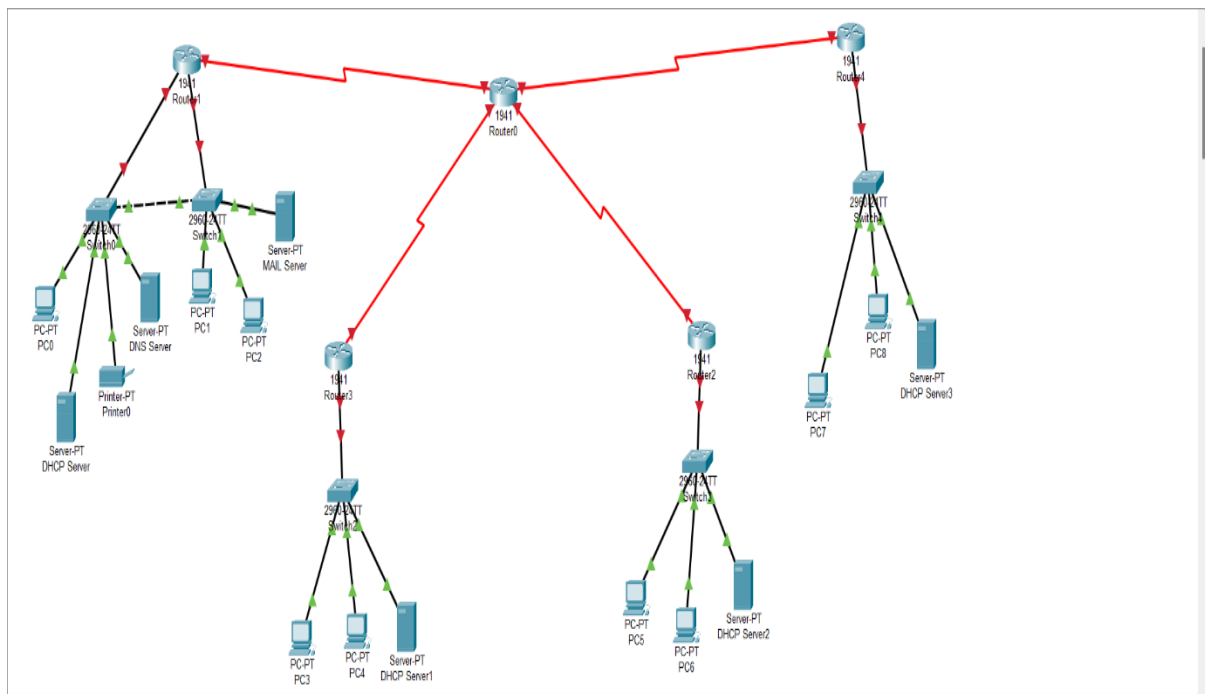
FreshConnections' current approach involves a centralized inventory management system connected to all branches via a wide area network (WAN), where the inventory management system acts as the hub, and the branches serve as spokes, using a hub-and-spoke network topology.

Each branch has a router that connects it to the WAN and provides access to the inventory management system and other network resources. These routers use dynamic routing protocols, such as OSPF or EIGRP, to facilitate efficient communication between the central hub and the branches.

The inventory management system stores information about products, including their current stock levels, pricing, and promotional information. When a customer purchases a product at a branch, the inventory management system is updated in real-time to track inventory levels, ensuring that products are always in stock.

Overall, FreshConnections' current solution is a dependable and efficient way to manage inventory across all its branches. The combination of the centralized inventory management system, WAN, and hub-and-spoke network topology ensures that products are always in stock, pricing and promotional information is up-to-date, and customers receive consistent quality across all branches.

10.2 Network Map:



11 Network Design

11.1 Proposed solution

To meet the requirements and goals of FreshConnections, we propose the following network design solution:

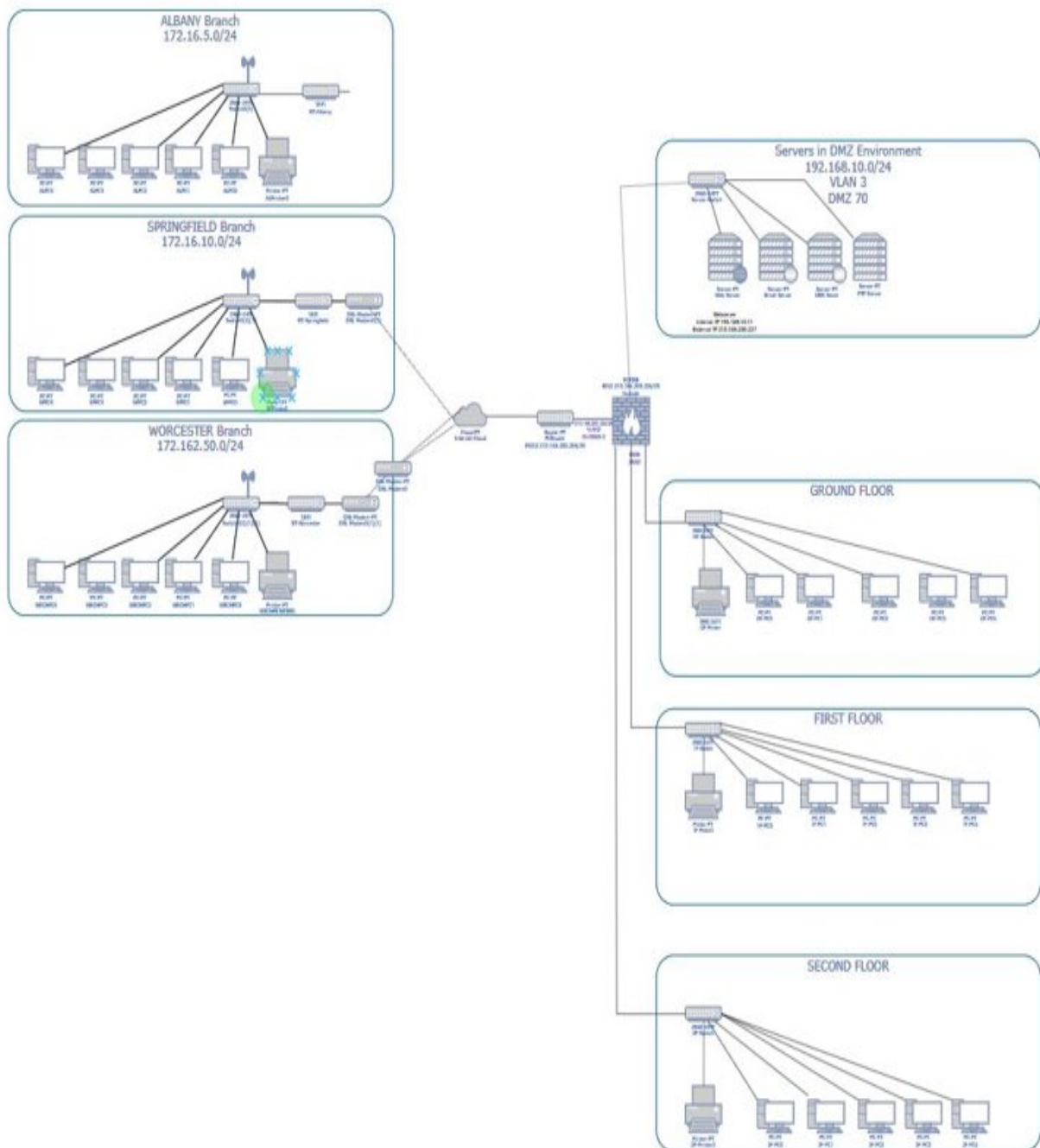
- **Network Topology:** We propose a hub-and-spoke network topology, with the centralized inventory management system serving as the hub and each branch serving as a spoke. This topology is efficient, scalable, and easy to manage.

- **Network Devices:** We propose using high-performance routers and switches from reputable vendors such as Cisco, to ensure fast and reliable communication between all branches and the central inventory management system.
- **IP Addressing:** We will use Class A, Class B and Class C addresses for IP addressing.
- **Network Security:** We propose implementing robust security measures to protect the network and its data, configuring firewall to the router and server, intrusion detection and prevention systems, and access controls.
- **Redundancy:** We propose implementing redundant links and devices to ensure the availability and reliability of the network. For example, each branch will have at least two routers, with one acting as a backup in case of a failure. We will also implement load balancing to distribute network traffic across multiple links.
- **Remote Access:** We propose implementing a secure remote access solution, such as a virtual private network (VPN), to enable authorized personnel to access the network from remote locations.
- **Network Management:** We propose implementing a network management system, such as Cisco Prime Infrastructure, to monitor and manage the network, ensuring efficient operation and timely troubleshooting.

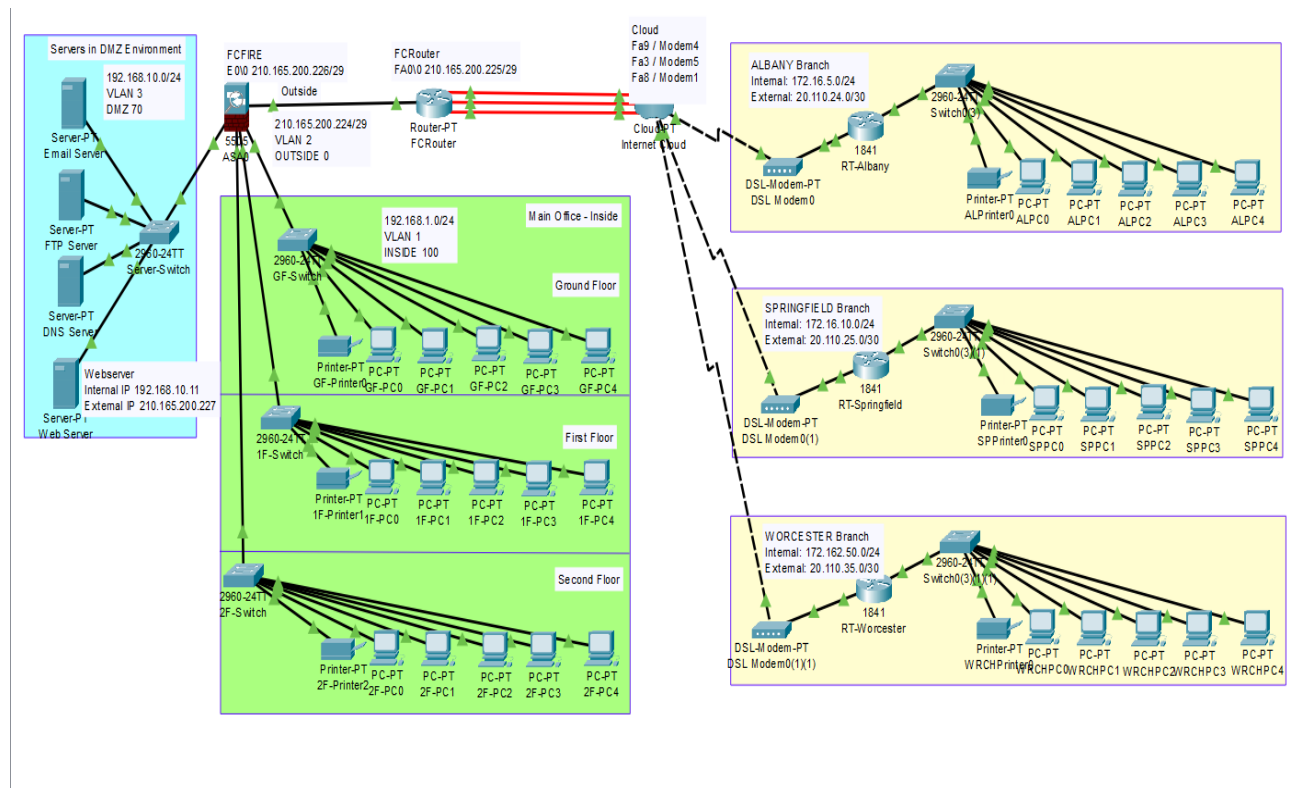
As part of the proposed network design for FreshConnections, we are upgrading the internet/link speeds to ensure fast and reliable communication between all branches and the central inventory management system. We propose using high-speed fiber-optic connections with a minimum speed of 1 Gbps to ensure optimal performance and minimize downtime or disruptions.

To provide maximum security and reliability, we propose using industry-standard firewalls, such as Cisco ASA or Fortinet. We also intend to implement other security measures, such as access controls, strong passwords, and regular security audits, to ensure the network remains secure and protected from potential threats. Overall, the proposed network design for FreshConnections includes high-speed internet/link speeds and robust security measures to provide fast and reliable communication while ensuring the safety and security of the network and its data.

11.2 Logical Network Design

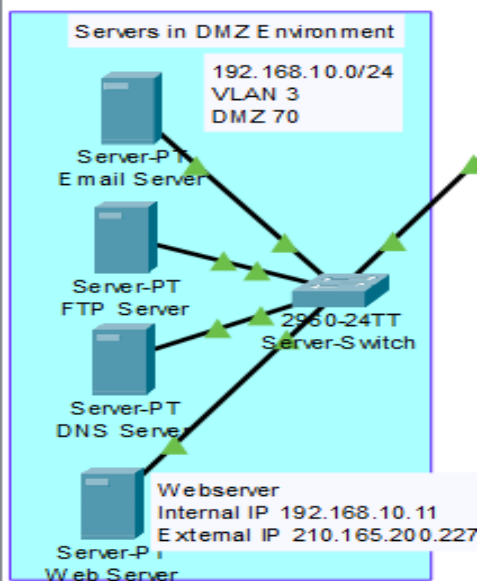


11.3 Physical Network Design

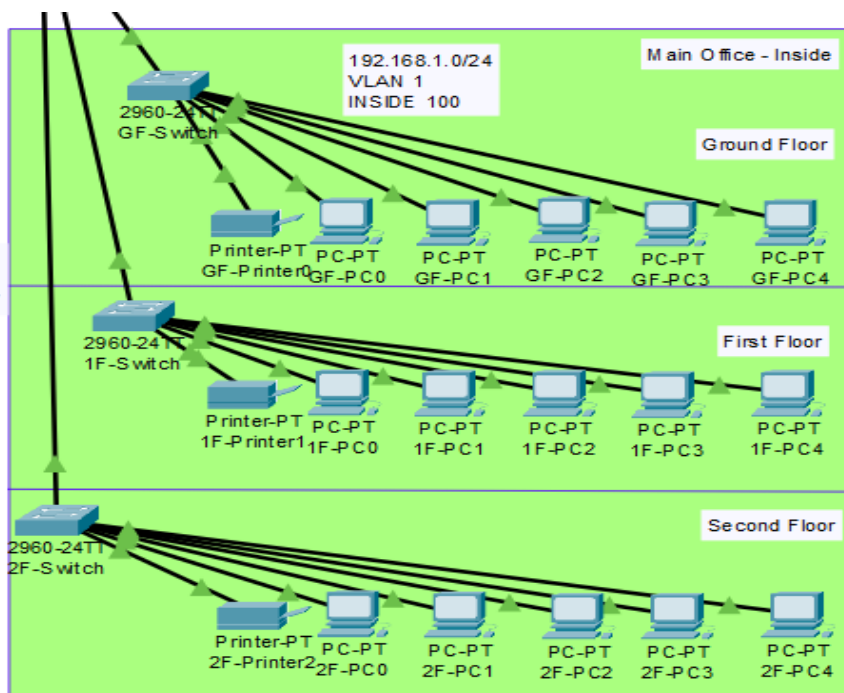


11.3.1 Physical Design of Server Environment

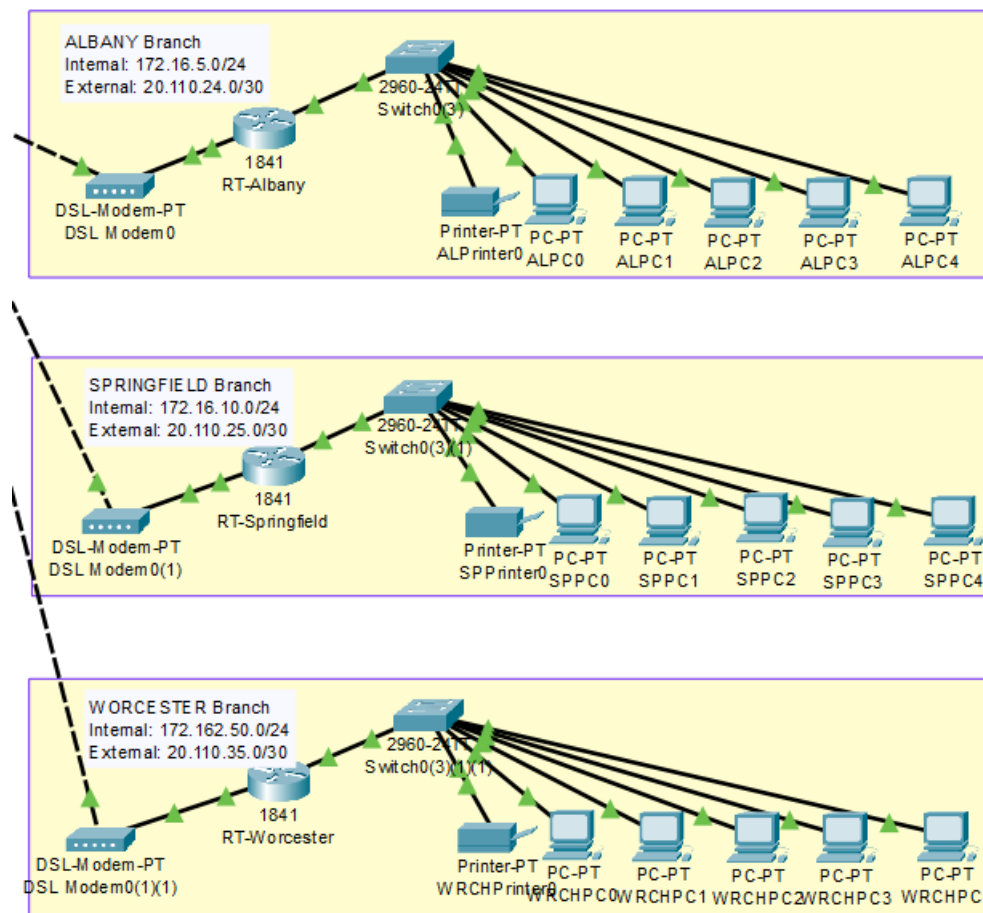
All the servers are placed inside the DMZ (Demilitarized zone) Environment in the Main Branch. A Demilitarized zone environment is a network architecture that provides an additional layer of security to an organization's network infrastructure. It also known as a perimeter network. It acts as a neutral zone between the internal network and the external network. It is designed to host services that need to be accessed for the the internet such as web servers, email servers, and FTP servers. By placing these services in the DMZ, the organization can provide access to the public without exposing the internal network to potential security threats.



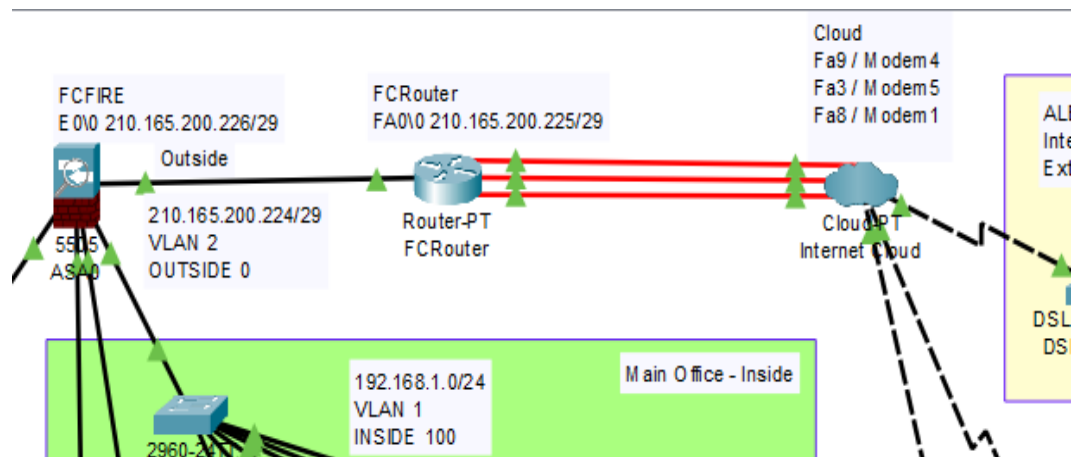
11.3.2 Physical Design of Main Office



11.3.3 Physical Design of Branch offices



11.3.4 Physical Design of Cloud connectivity and Firewall



11.4 IP Addressing Scheme:

Location	Number of Devices	IP-Addressing	Subnet	External IP-addressing
Bridgeport (Main Branch)	20	192.168.1.1/24 - 192.168.1.64/24	255.255.255.0	-
Albany	15	172.16.5.0/24 - 172.16.5.64/24	255.255.255.0	20.110.24.0/30
Springfield	15	172.16.10.0/24 - 172.16.10.64/24	255.255.255.0	20.110.25.0/30
Worcester	15	172.162.50.0/24 - 172.162.50.64/24	255.255.255.0	20.110.35.0/30
Providence	15	172.16.15.0/24 - 172.16.15.64/24	255.255.255.0	20.110.36.0/30

11.5 Routing Protocols:

There are a number of routing protocols available to configure and enable communication between devices. The major category of the routing protocols is

- Static Routing
- Dynamic Routing

1. Static Host Configuration Protocol:

Manually addressing unique address to each and every device.

Static Addressing is for a smaller number of devices.

new device → select "manual" configuration option to enter in the IP address, → subnet mask → default gateway → and the DNS server(s).

Servers are configured with Static IP Addresses.

- DNS Server IP Address: 192.168.10.12
- FTP Server IP Address: 192.168.10.13

- Web Server IP Address: 192.168.10.11
- Email Server IP Address: 192.168.10.14

2. Dynamic Host Configuration Protocol (DHCP):

- The server assigns an unused location to the new devices whenever they are connected to the network.
- Dynamic Addressing is for more devices.
- The server tracks the used and unused addresses for the devices.
- IP address may not be the same when the device goes offline and reconnects to the server.
- In this Network DHCP is used to assign IP address to end devices in the network.

In the network design, we used **OSPF dynamic routing** between all sites.

- OSPF routing protocol used to exchange routing information between routers within a network. It is commonly used in large enterprise networks because it provides efficient and scalable routing, supports load balancing, and can adapt to changes in network topology quickly.

Other Protocol which are used in the Implementation of FreshConnections Enterprise Network are:

1. **File Transfer Protocol (FTP):** FTP protocol used for transferring files between a client and server over a network. It is commonly used for uploading and downloading files to and from a web server.
2. **Simple Mail Transfer Protocol (SMTP):** SMTP protocol is used for sending email messages between mail servers. It is used by email clients to send messages to a server for delivery to the intended recipient.
3. **Post Office Protocol version 3 (POP3):** POP3 protocol is used for retrieving email messages from a mail server. It is used by email clients to download messages from a server and store them locally on the client's device.
4. **Simple Network Management Protocol (SNMP):** SNMP protocol is used for managing and monitoring network devices such as routers, switches, and servers. It allows administrators to monitor network performance and configure network devices remotely.
5. **Transmission Control Protocol/Internet Protocol (TCP/IP):** A suite of protocols used for communication over the internet and other networks. It provides reliable, connection-oriented communication between devices.
6. **Internet Control Message Protocol (ICMP):** ICMP (Internet Control Message Protocol) is a network protocol used to send error messages and operational information about network conditions. It is used by network devices such as routers and firewalls to communicate with one another, as well as by diagnostic tools such

as ping and traceroute. In firewalls, ICMP traffic is often turned off because it can be used by attackers to perform reconnaissance on the network, such as determining which IP addresses are active or identifying the type of firewall in use. ICMP traffic can also be used in denial-of-service (DoS) attacks, where a large number of ICMP packets are sent to a target system to overload it with traffic and make it unavailable to legitimate users. However, some types of ICMP traffic are necessary for proper network operation, such as ICMP echo request and reply packets used by the ping command to test network connectivity. In these cases, firewall rules can be configured to allow specific types of ICMP traffic while blocking others.

11.6 Security and Network Management Strategies

Firewall: FreshConnections uses a firewall to protect its network from unauthorized access and attacks. The firewall can filter incoming and outgoing network traffic and block any suspicious activity.

DMZ: FreshConnections uses a Demilitarized Zone (DMZ) to isolate its public-facing servers and services from the rest of the network. This helps protect against external attacks and ensures that any security breaches are contained.

Cloud Services: FreshConnections uses cloud services to store data and run applications in a virtual environment. This can help reduce the need for on-premises hardware and provide scalability and flexibility.

12 Network Testing

12.1 DNS Server

- In our network:
- Ip address – 192.168.10.12
- Website – www.freshconnections.com

DNS Server

Physical Config **Services** Desktop Programming Attributes

SERVICES

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

DNS

DNS Service ☒ On ☐ Off

Resource Records

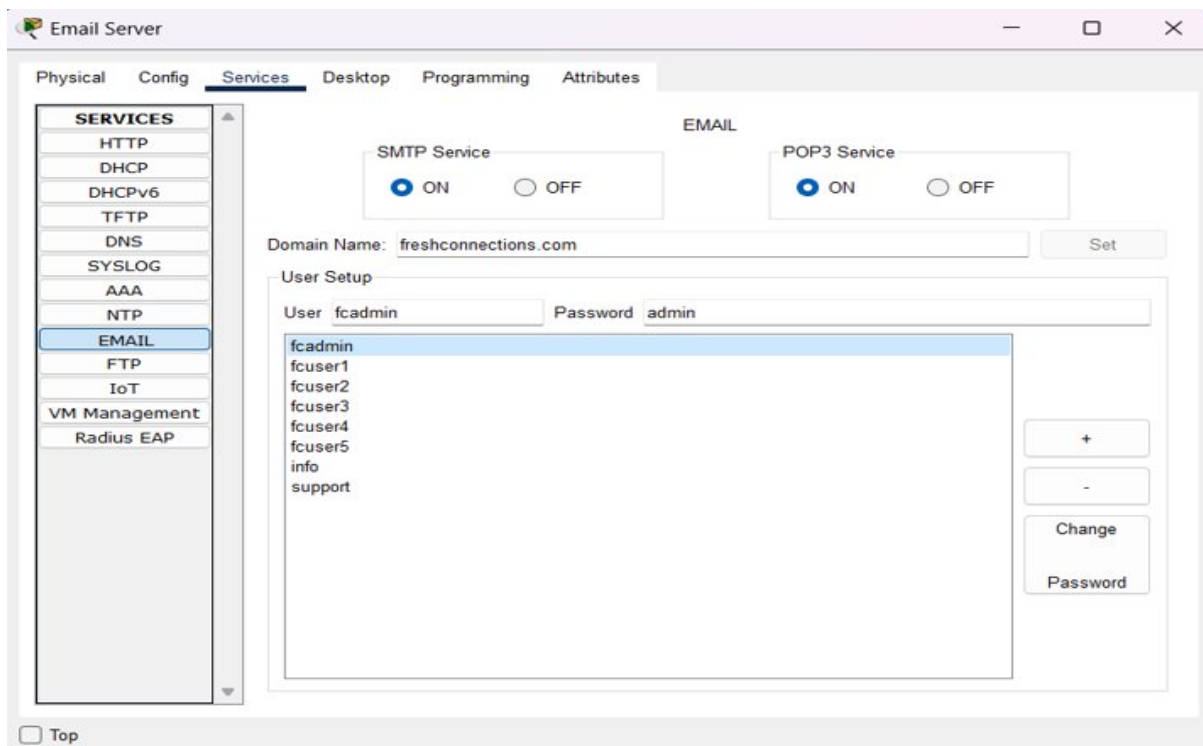
Name Type **A Record** ▼

Address

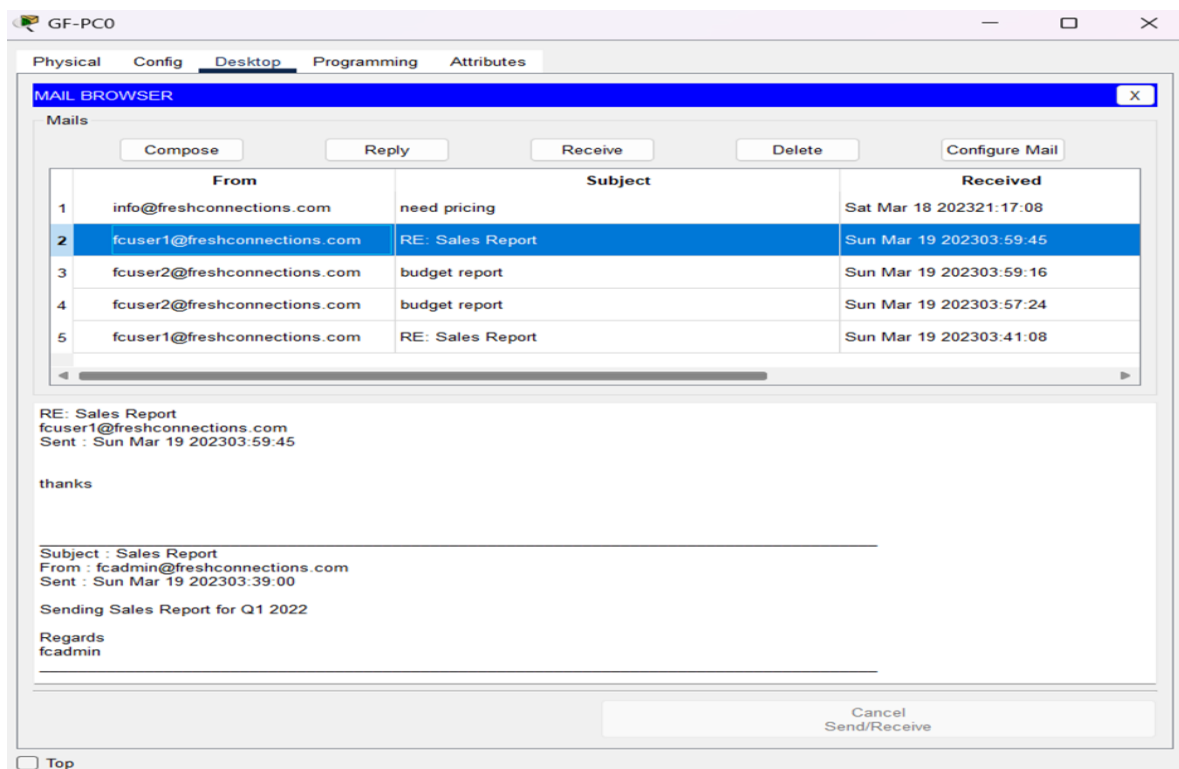
No.	Name	Type	Detail
0	FC_ftp_server	ARecord	192.168.10.13
1	freshconnections	ARecord	210.165.200.227
2	freshconnections.com	ARecord	192.168.10.11

☐ Top

12.2 Email Server

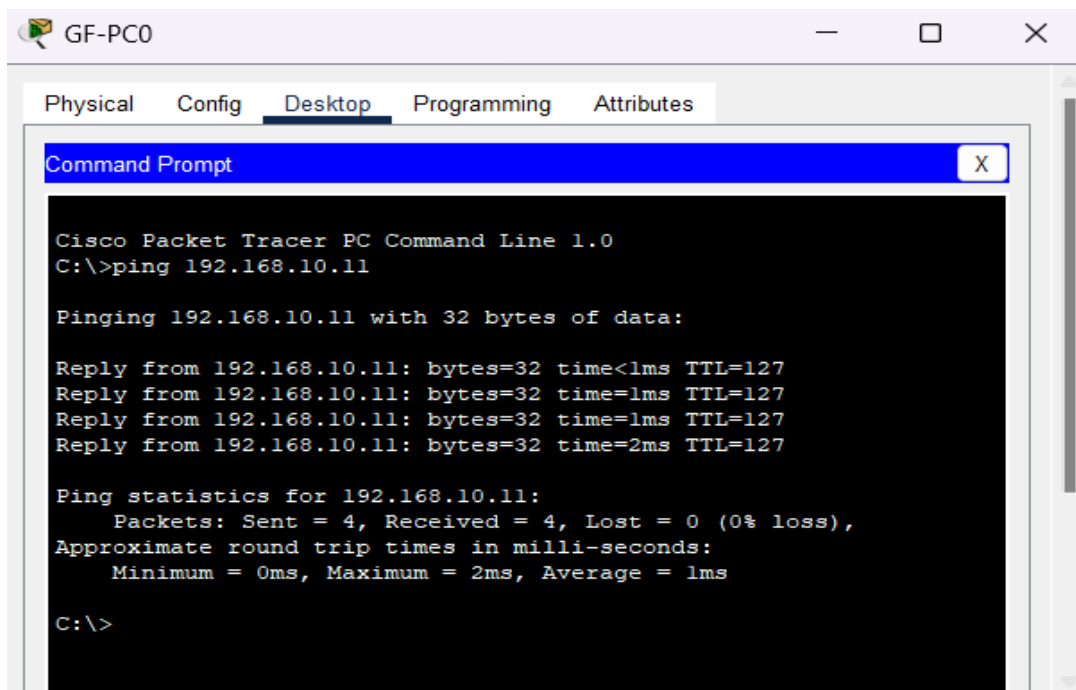


User-Id created in Email Server



Email's being sent from one user to another

12.3 Web Server



Pinging the Web Server



URL of the Web Server.

12.4 DHCP Pool

RT-Worcester

Physical

Config

CLI

Attributes

IOS Command Line Interface

```

Worcester-branch>en
Worcester-branch#show ip interface brief
Interface                IP-Address      OK? Method Status              Protocol
FastEthernet0/0          20.110.35.2     YES manual up                  up
FastEthernet0/1          172.162.50.1    YES manual up                  up
Vlan1                    unassigned      YES unset  administratively down down
Worcester-branch#
Worcester-branch#show ip dhcp pool

Pool worcesterpool :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 0 / 0
  Total addresses                   : 254
  Leased addresses                  : 6
  Excluded addresses                : 4
  Pending event                     : none

  1 subnet is currently in the pool
  Current index    IP address range      Leased/Excluded/Total
  172.162.50.1     172.162.50.1 - 172.162.50.254    6 / 4 / 254
Worcester-branch#
Worcester-branch#show ip dhcp binding
IP address          Client-ID/      Lease expiration      Type
                   Hardware address
172.162.50.18       0050.0F76.9672   --                     Automatic
172.162.50.17       00D0.BAEE.9E20   --                     Automatic
172.162.50.16       0090.0CBA.5B0C   --                     Automatic
172.162.50.19       000C.8520.D8A0   --                     Automatic
172.162.50.21       0007.EC30.6CA8   --                     Automatic
172.162.50.20       0009.7CC5.960E   --                     Automatic
Worcester-branch#
Worcester-branch#show ip dhcp conflict
IP address          Detection method  Detection time         VRF
Worcester-branch#
Worcester-branch#
Worcester-branch#
Worcester-branch#
Worcester-branch#
Worcester-branch#
Worcester-branch#
Worcester-branch#

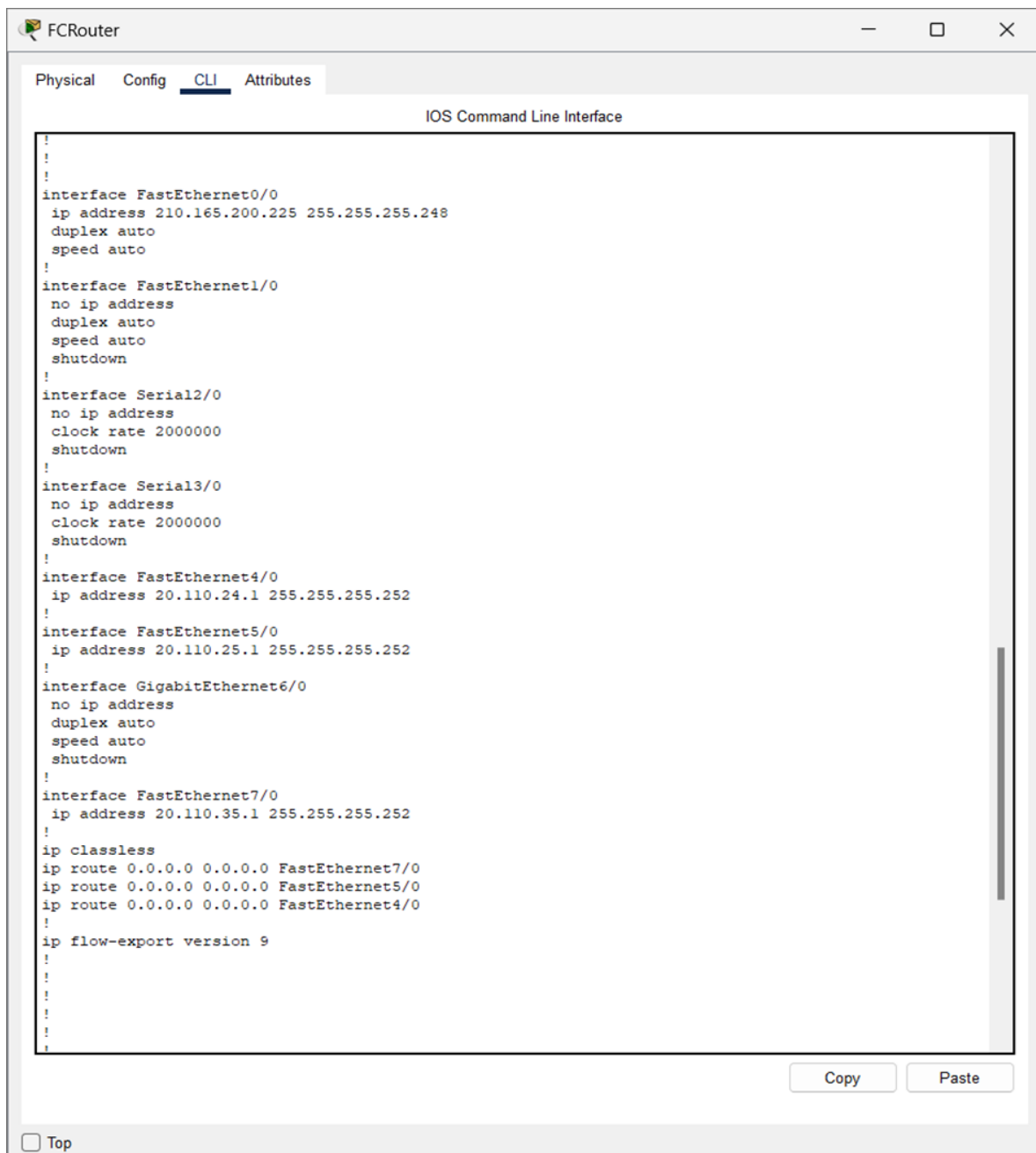
```

Copy

Paste

☐ Top

12.5 Router Configuration



The screenshot shows a web-based configuration interface for a router named "FCRouter". The interface has a top bar with the router name and standard window controls. Below this is a tabbed menu with "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is selected, displaying the "IOS Command Line Interface". The main area contains a text editor with a network configuration script. The script defines several interfaces: FastEthernet0/0 (with IP 210.165.200.225), FastEthernet1/0 (shut down), Serial2/0 (shut down), Serial3/0 (shut down), FastEthernet4/0 (with IP 20.110.24.1), FastEthernet5/0 (with IP 20.110.25.1), GigabitEthernet6/0 (shut down), and FastEthernet7/0 (with IP 20.110.35.1). It also includes static routes for 0.0.0.0/0 pointing to these interfaces and sets the flow-export version to 9. At the bottom right of the CLI window are "Copy" and "Paste" buttons. Below the CLI window is a "Top" link.

```
!
!
!
interface FastEthernet0/0
ip address 210.165.200.225 255.255.255.248
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
!
interface Serial2/0
no ip address
clock rate 2000000
shutdown
!
interface Serial3/0
no ip address
clock rate 2000000
shutdown
!
interface FastEthernet4/0
ip address 20.110.24.1 255.255.255.252
!
interface FastEthernet5/0
ip address 20.110.25.1 255.255.255.252
!
interface GigabitEthernet6/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet7/0
ip address 20.110.35.1 255.255.255.252
!
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet7/0
ip route 0.0.0.0 0.0.0.0 FastEthernet5/0
ip route 0.0.0.0 0.0.0.0 FastEthernet4/0
!
ip flow-export version 9
!
!
!
!
!
```

☐ Top

12.6 Firewall Configuration

ASA0

Physical Config CLI Attributes

IOS Command Line Interface

```
fcfire>en
Password:
fcfire#show run
: Saved
:
ASA Version 8.4(2)
!
hostname fcfire
domain-name freshconnections.com
enable password 7t/8VgClEuZul9lF encrypted
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
 switchport access vlan 3
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 210.165.200.226 255.255.255.248
!
<--- More --->
```

☐ Top

Copy Paste

ASA0

Physical Config CLI Attributes

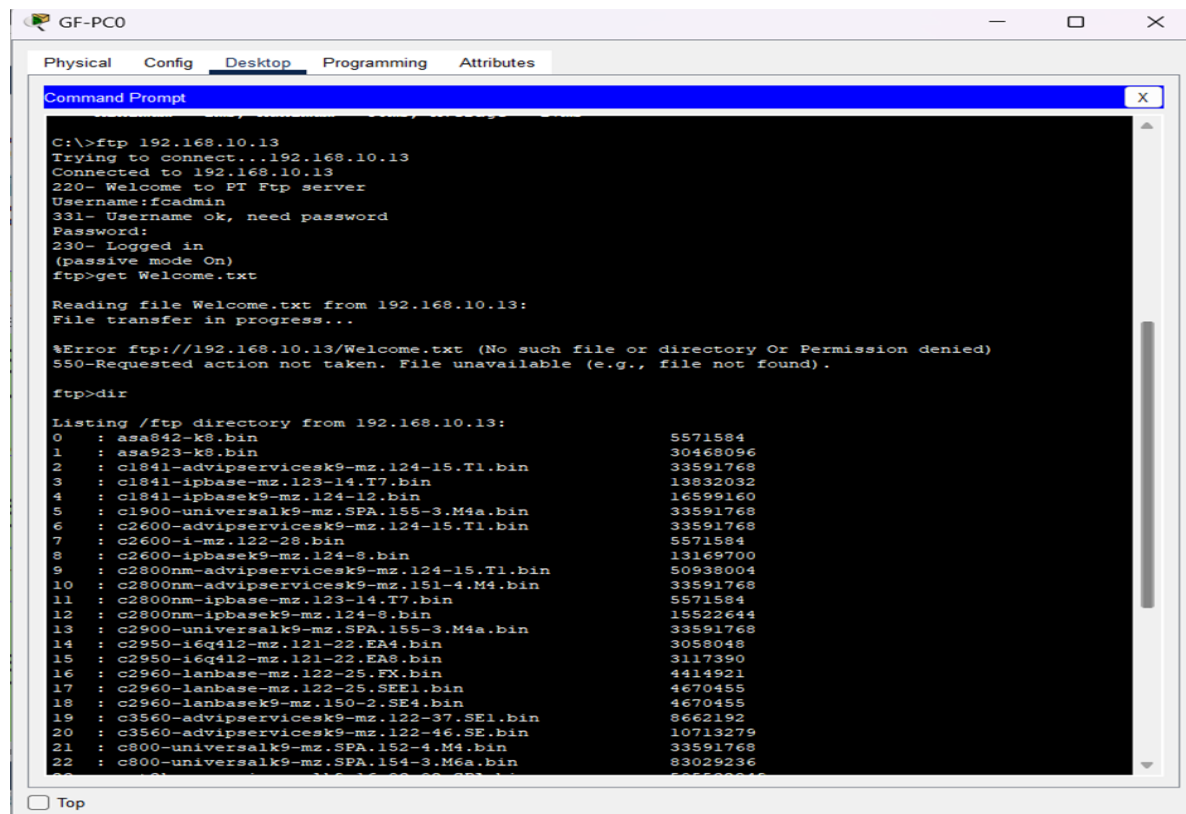
IOS Command Line Interface

```
interface vians
 no forward interface Vlan1
 nameif dmz
 security-level 70
 ip address 192.168.10.1 255.255.255.0
!
object network dmz-net
 subnet 192.168.10.0 255.255.255.0
 nat (dmz,outside) dynamic interface
object network dns-server
 host 192.168.10.12
object network email-server
 host 192.168.10.14
 nat (dmz,outside) static 210.165.200.229
object network ftp-server
 host 192.168.10.13
 nat (dmz,outside) static 210.165.200.228
object network inside-net
 subnet 192.168.1.0 255.255.255.0
 nat (inside,outside) dynamic interface
object network web-server
 host 192.168.10.11
 nat (dmz,outside) static 210.165.200.227
!
route outside 0.0.0.0 0.0.0.0 210.165.200.225 1
!
access-list dmz_acl extended deny ip any object inside-net
access-list dmz_acl extended permit ip any any
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list OUTSIDE-DMZ extended permit icmp any object web-server
access-list OUTSIDE-DMZ extended permit tcp any object web-server eq www
access-list OUTSIDE-DMZ extended permit icmp any object dns-server
access-list OUTSIDE-DMZ extended permit tcp any object dns-server
access-list OUTSIDE-DMZ extended permit tcp any host 192.168.10.11 eq www
access-list OUTSIDE-DMZ extended permit tcp any host 192.168.10.13 eq ftp
access-list OUTSIDE-DMZ extended permit tcp any host 192.168.10.14 eq pop3
access-list OUTSIDE-DMZ extended permit tcp any host 192.168.10.14 eq smtp
access-list OUTSIDE-DMZ extended permit tcp any host 192.168.10.12 eq domain
!
!
access-group dmz_acl in interface dmz
access-group OUTSIDE-DMZ in interface outside
aaa authentication ssh console LOCAL
!
username fccadmin password PNF1LNSBlnIyMLra encrypted
username fccalbany password /H8cA38wR26wFb24 encrypted
username fccspringfield password gzt7Lz1TsD4vaFcU encrypted
username fccworchester password iqqXThqqWbRy9SHR encrypted
!
class-map inspection_default
 match default-inspection-traffic
```

☐ Top

Copy Paste

12.7 FTP Server



```
C:\>ftp 192.168.10.13
Trying to connect...192.168.10.13
Connected to 192.168.10.13
220- Welcome to FT Ftp server
Username:fcadmin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>get Welcome.txt

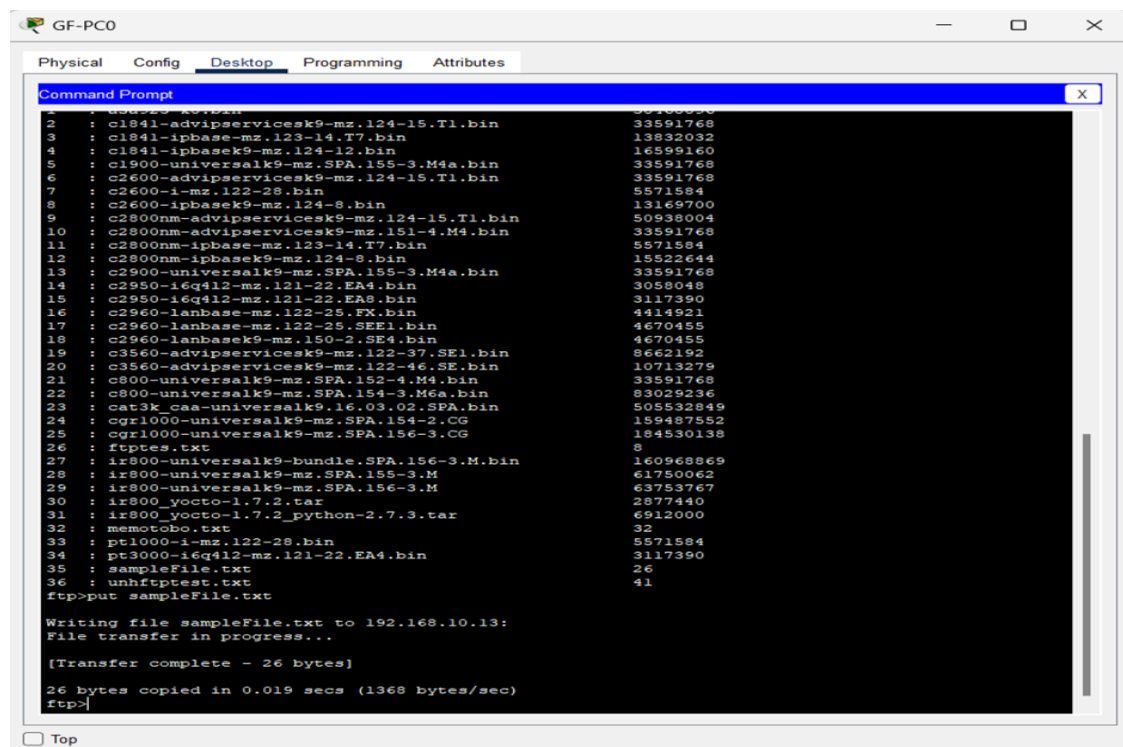
Reading file Welcome.txt from 192.168.10.13:
File transfer in progress...

%Error ftp://192.168.10.13/Welcome.txt (No such file or directory Or Permission denied)
550- Requested action not taken. File unavailable (e.g., file not found).

ftp>dir

Listing /ftp directory from 192.168.10.13:
 0 : asa842-k8.bin                5571584
 1 : asa923-k8.bin                30468096
 2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
 3 : c1841-ipbase-mz.123-14.T7.bin 13832032
 4 : c1841-ipbasek9-mz.124-12.bin 16599160
 5 : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
 6 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
 7 : c2600-i-mz.122-28.bin        5571584
 8 : c2600-ipbasek9-mz.124-8.bin  13169700
 9 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
12 : c2800nm-ipbasek9-mz.124-8.bin 15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin 3058048
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
```

Reading the file into FTP



```
 0 : asa842-k8.bin                5571584
 1 : asa923-k8.bin                30468096
 2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
 3 : c1841-ipbase-mz.123-14.T7.bin 13832032
 4 : c1841-ipbasek9-mz.124-12.bin 16599160
 5 : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
 6 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
 7 : c2600-i-mz.122-28.bin        5571584
 8 : c2600-ipbasek9-mz.124-8.bin  13169700
 9 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
12 : c2800nm-ipbasek9-mz.124-8.bin 15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin 3058048
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 : cat9k_caa-universalk9.16.03-02.SPA.bin 505582849
24 : cgr1000-universalk9-mz.SPA.154-2.CG 159487552
25 : cgr1000-universalk9-mz.SPA.156-3.CG 184530138
26 : fptes.txt                    8
27 : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
28 : ir800-universalk9-mz.SPA.155-3.M 61750062
29 : ir800-universalk9-mz.SPA.156-3.M 63753767
30 : ir800_yocto-1.7.2.tar        2877440
31 : ir800_yocto-1.7.2_python-2.7.3.tar 6912000
32 : memotobo.txt                 32
33 : pt1000-i-mz.122-28.bin        5571584
34 : pt3000-i6q412-mz.121-22.EA4.bin 3117390
35 : sampleFile.txt               26
36 : unhftptest.txt               41

ftp>put sampleFile.txt

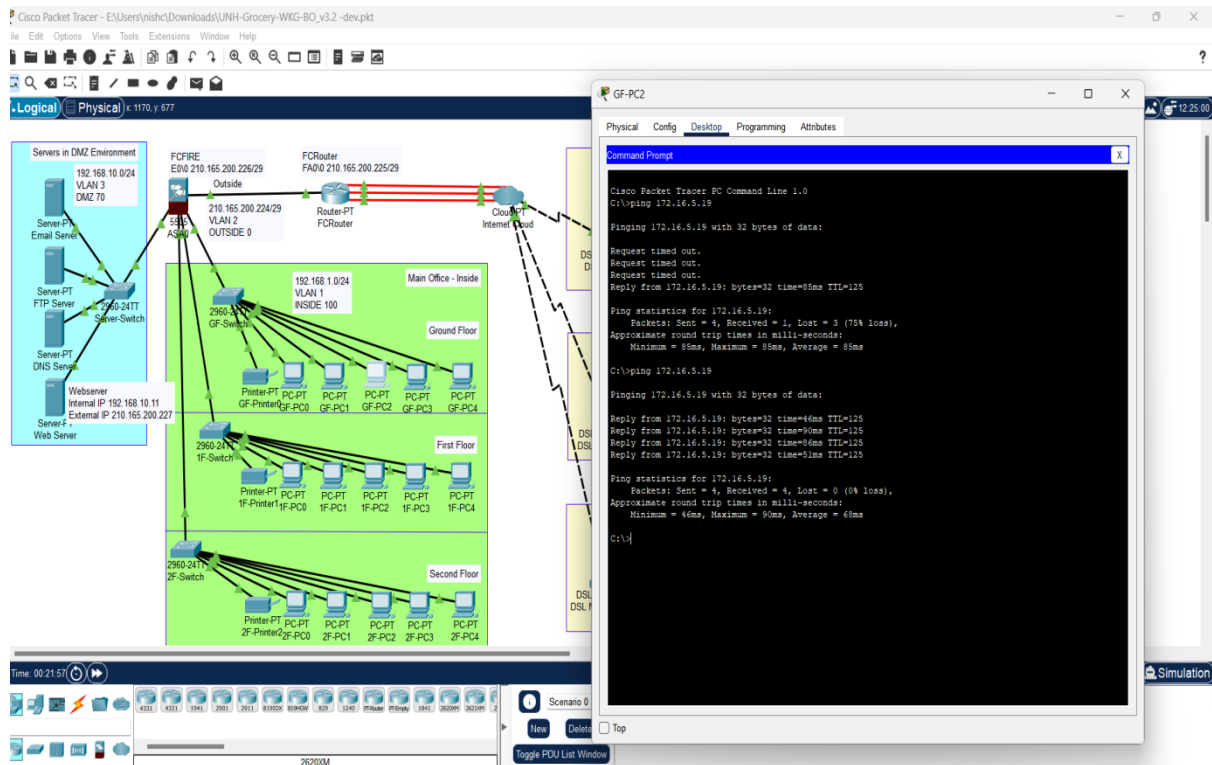
Writing file sampleFile.txt to 192.168.10.13:
File transfer in progress...

[Transfer complete - 26 bytes]

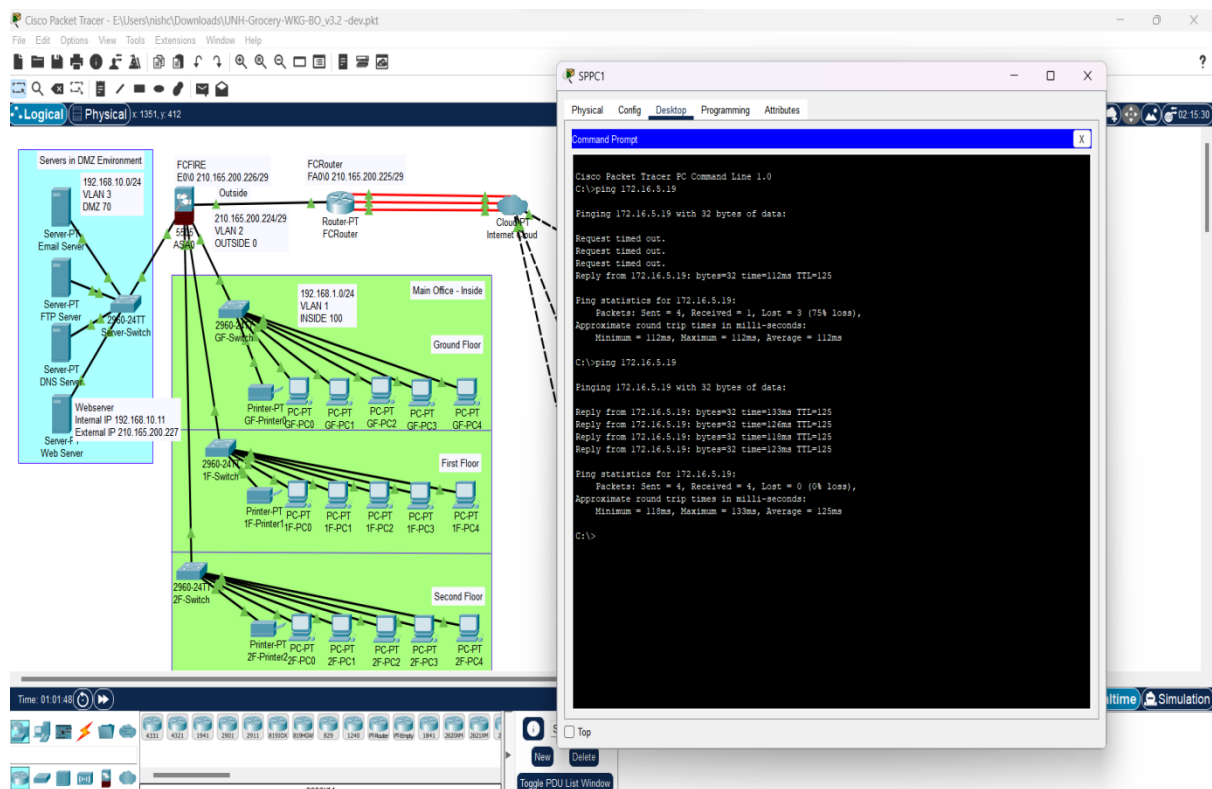
26 bytes copied in 0.019 secs (1368 bytes/sec)
ftp>
```

Writing the file into FTP

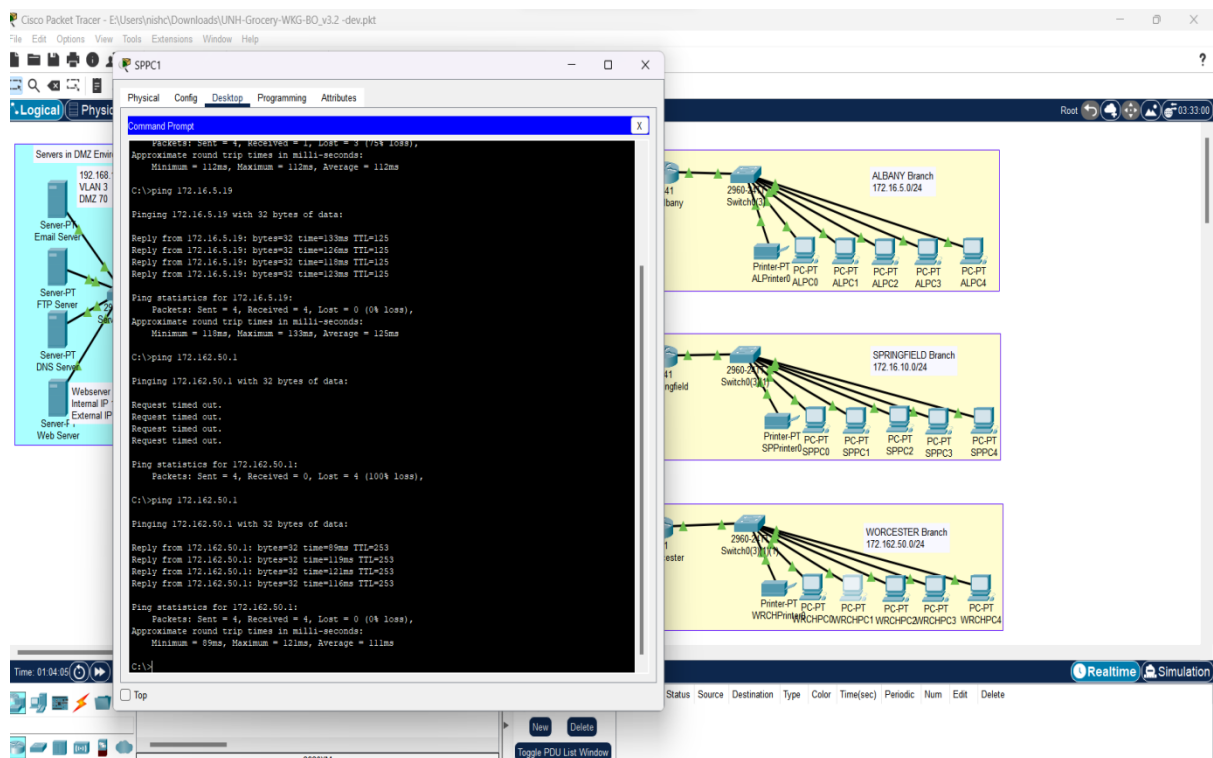
12.8 Ping Screenshots



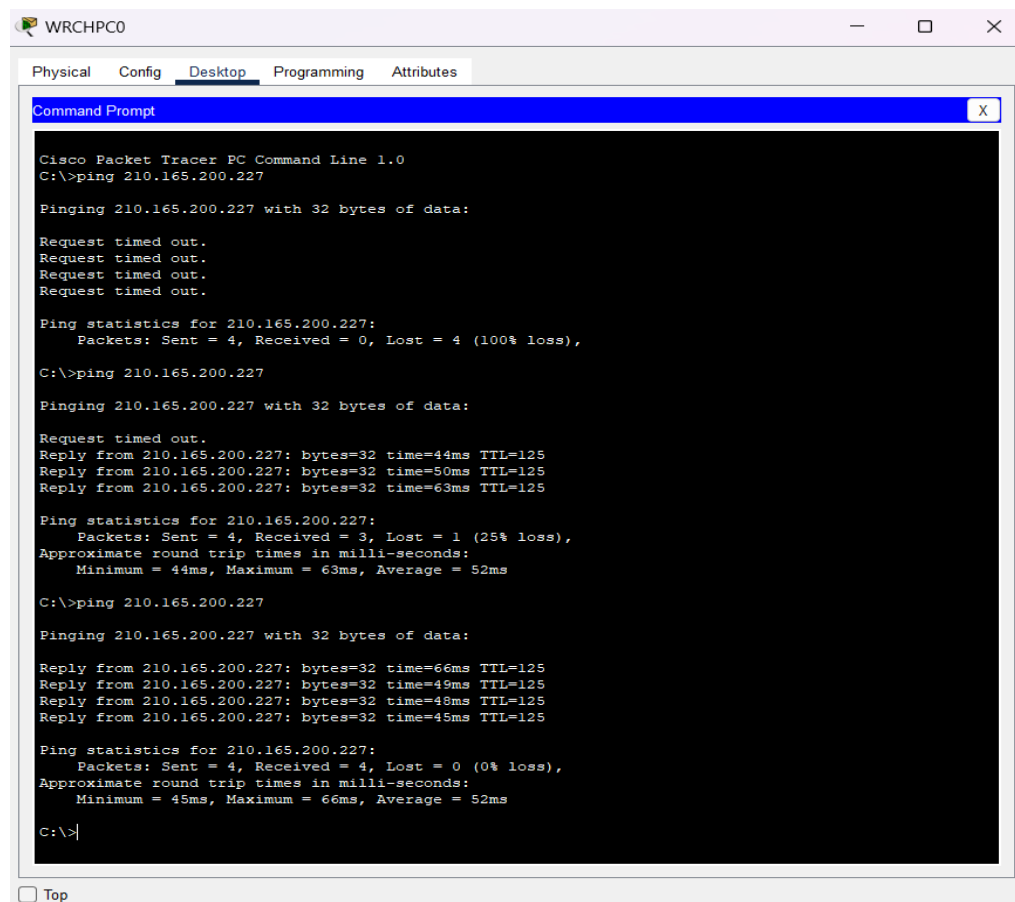
Pinging the PC in the Albany branch from Main Branch.



Ping SP PC1 from Springfield branch to Albany branch AL PC 1.



Pinging SP PC 1 from Springfield to Worcester Branch WRCH PC1.



Pinging the Web Sever from Worcester Branch



Accessing the Web Server from Worcester Branch.