Project Report

Project Name: **Development of Virtual Area Network (VLAN) For Commercial Bank.**

Course Name: Foundations of TCP/IP

Course Code: ICE460

Section: 01

Submitted to:

Md. Mahir Ashhab

Lecturer

Department of Computer Science & Engineering.

Submitted by:

Name	**ID**
Sanjida Simla	2019-2-50-007
Jerin Tabassum Irina	2019-1-50-034

Submission Date:

22/12/2023

Introduction

In the ever-evolving landscape of banking and finance, the imperative to innovate and optimize technological infrastructure has never been more crucial. The project "Development of a Virtual Local Area Network (VLAN) for Commercial Bank" represents a strategic initiative aimed at revolutionizing the way our bank manages its digital ecosystem. This project revolves around the strategic implementation of VLAN technology to create a segmented network structure tailored to our bank's unique operational intricacies. By organizing network traffic, we intend to optimize communication channels between departments and branches, fostering a more responsive and secure banking environment. The VLAN setup not only segregates the network traffic logically but also optimizes bandwidth utilization, fostering a secure and efficient environment for our banking professionals. Each floor operates as an independent VLAN, offering a dedicated space for department-specific activities while maintaining the flexibility to communicate across the organization. The "Development of VLAN for Commercial Bank" project demonstrates our commitment to staying ahead in the digital financial world, ensuring that our bank remains competitive and adaptable to the industry's changing needs.

<u>Virtual Local Area Network (VLAN)</u>

Local Area Network (LAN) is known as a branch of computer network which covers a small area or location such as hospitals, homes or offices. It transmits higher data rate due to its area of coverage and also requires less telecommunication facilities. On the other hand, Virtual Local Area Network (VLAN) is the logical grouping of resources and Network connected to a network in order to adequately define the operations of active ports on a particular network.
Virtual Local Area Networks, or VLANs, are a type of network segmentation that works on the OSI model's Layer 2 (Data Link Layer). It makes it possible to logically split up a single physical network into several separate virtual networks, or VLANs. Devices connected to the same network switch or located in the same physical area share the same broadcast domain in a classical network, enabling unrestricted communication between them. On the other hand, VLANs introduce the idea of logical segmentation, which has several advantages for scalability, security, and network management. VLANs are established by assigning a unique VLAN identifier, often referred to as a VLAN tag, to network frames. This tag is embedded in the Ethernet frame header and is used to identify the VLAN to which a specific frame belongs. Devices within the same VLAN can communicate with each other as if they are on the same network, even if they are physically dispersed or connected to different switches. On the other hand, communication between devices in different VLANs requires a routing device, such as a router or layer 3 switch.

Protocols Used in VLAN:

- ***IEEE 802.1Q:*** This serves as the standardized protocol for the tagging of VLANs, establishing the framework for the VLAN tag's format within the Ethernet frame header. IEEE 802.1Q enables the identification of VLAN membership and the effective segmentation of networks. It permits an expansion in the Ethernet frame size by four bytes, ranging from 68 to 1522 bytes, as a result of inserting a four-byte VLAN tag into the frame. These tags, incorporating a VLAN identifier (VID), are affixed to each Ethernet frame based on the MAC address.

This is how it works: IEEE 802.1Q, often referred to as Dot1q, is the networking standard that supports virtual local area networking (VLANs) on an IEEE 802.3 Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames.

- ***VLAN Trunking Protocol (VTP):*** VTP is a Cisco proprietary protocol used to manage VLAN configurations across a network. It helps ensure consistency of VLAN information between switches, reducing the need for manual VLAN configuration. A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device, such as a router or switch. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network.

This is how it works: A trunk port can transmit data from multiple VLANs. If you have a dozen VLANs on a particular switch, you don't need additional cables or switches for each VLAN—just that single link. A trunk port allows you to send all those signals for each switch or router across a single trunk link. Just like a tree trunk. That is why it is called a trunk.

- ***Inter-VLAN Routing Protocols*****:** For communication between devices in different VLANs, a routing protocol is required. Common inter-VLAN routing protocols include Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP).

  This is how it works: Inter-VLAN routing is the ability to route, or send, traffic between VLANs that are normally blocked by default. Switches and VLANs work at the MAC address layer (Layer 2). Traffic can't be routed between VLANs at Layer 2 based on MAC addresses.

Virtual Area Network (VLAN) For Commercial Bank

Our VLAN (Virtual Local Area Network) project is designed to meet the distinctive needs of a modern banking environment, employing a segmented network architecture that aligns with the organizational structure.

This project encompasses three distinct floors within our banking facility, each dedicated to a specialized department.

1. The first floor caters for the Accountant Department
2. The second floor for Business Banking Department
3. The third floor for the Loan Department.

By strategically dividing the physical space and network infrastructure, we aim to streamline communication, enhance data security, and provide tailored services for each banking function.

Key elements of this VLAN project include a comprehensive DHCP (Dynamic Host Configuration Protocol) server, a multilayer switch, and a main router to facilitate seamless communication between departments and ensure robust connectivity. Additionally, the deployment of two crucial servers—an email server and a DNS (Domain Name System) server—further fortifies our network infrastructure.

Distributions

Distribution of First floors (Accountant Department):

1. ***Occupants on the Floor:***
   - Branch Manager
   - Second Officer
   - General Manager
2. ***Workstations for Each Official:***
   - Each official (Branch Manager, Second Officer, and General Manager) has three separate PCs.

1. ***Networking Equipment:***
    - One Router (2911) is also in the first floor as it is the main router of this banking management.
    - One Multilayer Switch (3650-24PS).
    - Switch (2960-24TT).
    - This Switch is also connected to each PC.
2. ***Additional Features on the Accountant Department Switch:***
    - The Accountant Department Switch features an AccessPoint-PT (Access Point 1).
    - A DNS server and an Email server is also in this floor. The DNS server is linked to the switch on this floor.
3. ***Access Point Connectivity:***
    - The Access Point 1 is linked to the printers in each of the departments on this floor.
4. ***Communication Devices:***
    - To facilitate more accurate communication with department officials, a SMARTPHONE (Smart Phone 1) and a TabletPC-PT (Tablet PC-Pt1) are connected to the Access Point.

<u>Distribution of Second floors (Business Banking Department):</u>

1. ***Occupants on the Floor: (Second Floor)***
    - Business Depository
    - Trade Finance
    - Corporate Card Service
2. ***Workstations for Each Department Official:***
    - Each official in the Business Depository, Trade Finance, and Corporate Card Service has three separate PCs.
3. ***Networking Equipment:***
    - One Multilayer Switch (3650-24PS) is connected to the Business Department Switch (Switch1 2960-24TT).
    - The Business Department Switch is also connected to each PC.
4. ***Additional Features on the Business Department Switch:***
    - The Business Department Switch features an AccessPoint-PT (Access Point2).
    - It also features an Email server.
5. ***Access Point Connectivity:***
    - The Access Point is linked to the printers of the departments floor.
6. ***Communication Devices:***
    - To facilitate more accurate communication with department officials, a (SMARTPHONE-PT) smartphone2 and a Laptop-PT (Business-Dpt Laptop1) are also connected to the Access Point along with the printers.

Distribution of Third floors (Loan Department):

1. ***Occupants on the Floor:***
    - Loan Servicing
    - Collection & Recovery
    - Credit Analysis
2. ***Workstations for Each Department Official:***
    - Each official in Loan Servicing, Collection & Recovery, and Credit Analysis has three separate PCs.
3. ***Networking Equipment:***
    - One Multilayer Switch (3650-24PS) is connected to the Business Department Switch (Switch1 2960-24TT).
    - The Business Department Switch is also connected to each PC.
    - An additional Multilayer Switch0 is located on the third floor.
4. ***Additional Features on the Business Department Switch:***
    - The Business Department Switch features an AccessPoint-PT (Access Point0).
    - The Access Point is linked to the loan department's printers on this floor.
5. ***Communication Devices:***
    - To facilitate more accurate communication with department officials, a TabletPC-PT (Tablet PC), a smartphone, and two Laptop-Pt (Loan-Dpt Laptop1 and Loan-Dpt Laptop2) are also connected to the Access Point.

Analysis and Design

i. Implement a hierarchical model with redundancy at each layer, utilizing one router and one multilayer switch for redundancy purposes.
ii. Establish connectivity to at least two Internet Service Providers (ISPs) for enhanced redundancy, ensuring each router connects to both ISPs.
iii. Deploy a wireless network in each department to accommodate user connectivity.
iv. Assign distinct VLANs and subnetworks to each department to ensure network segmentation. For instance, VLAN 10 (192.168.1.0/24) for the first floor, VLAN 20 (192.168.2.0/24) for the second floor, and VLAN 30 (192.168.3.0/24) for the third floor.
v. Configure essential device settings, including hostname, console password, enable password, implement banner messages, and disable IP domain lookup.
vi. Enable communication between devices in different departments by configuring inter-VLAN routing on the respective multilayer switches.
vii. Assign IP addresses to the multilayer switches to enable them to perform both routing and switching functions.
viii. Implement dynamic IP address assignment for all network devices through dedicated DHCP servers, while devices in the server room receive static IP addresses.

ix. Utilize OSPF as the routing protocol to propagate routes across both routers and multilayer switches.
x. Implement NAT using the outbound router interface's IPv4 address, incorporating the necessary Access Control List (ACL) rules.
xi. Conduct thorough testing to verify the functionality of all configured elements, ensuring seamless communication and adherence to the specified requirements.

We must understand DHCP, RIP, DNS Server in order to implement this design. Thus, the following will serve as an introduction to these functions:

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network protocol designed to streamline the automatic assignment and management of IP addresses and other configuration details for devices within a TCP/IP-based network. Its primary aim is to simplify the often-intricate process of IP address assignment and configuration for devices like computers, printers, and smartphones on a network.

Key Aspects of DHCP:

- **Automated IP Address Assignment:**

DHCP enables network administrators to automate the assignment of IP addresses to devices on the network. Instead of manually configuring each device with a static IP address, DHCP dynamically allocates addresses from an available pool.

- **Dynamic Configuration:**

Beyond IP addresses, DHCP can furnish additional configuration information to devices, including subnet masks, default gateways, DNS servers, and other network parameters. This dynamic configuration reduces the complexity of network management and minimizes configuration errors.

- **Lease Duration:**

IP addresses assigned by DHCP are not permanent; devices receive leases for specific periods. Upon expiration, devices must renew their lease or request a new IP address, ensuring efficient utilization of available IP addresses.

- **Centralized Management:**

Typically implemented using dedicated servers, DHCP centrally manages IP address assignments and configurations for network devices. Clients communicate with the DHCP server to obtain or renew their IP addresses.

- **Reduced Manual Configuration:**

DHCP diminishes the need for manually configuring IP addresses on individual devices, a valuable feature in large networks where manual management could be time-consuming and error-prone.

- **Protocol Operation:**

The DHCP process involves a sequence of messages between the DHCP client and server, encompassing DHCP Discover, DHCP Offer, DHCP Request, and DHCP Acknowledge messages.

These messages facilitate the negotiation and assignment of IP addresses and configuration parameters.
In summary, DHCP streamlines network configuration by automating the assignment of IP addresses and related parameters, serving as a fundamental protocol for the efficient operation of IP-based networks.

RIP (Routing Information Protocol)

Routing Information Protocol (RIP) is a distance-vector routing protocol used in computer networks to facilitate the exchange of routing information among routers. It is designed for simplicity and ease of implementation, making it suitable for smaller networks.

Here are the key elements and features of RIP:

- **Distance-Vector Protocol:**

RIP is a distance-vector protocol, meaning routers share information about the distance (metric) and direction to reach a destination. Each router maintains a routing table based on this information.

- **Hop Count as Metric:**

RIP uses the number of hops (router traversals) as its metric to determine the best path to a destination. The route with the fewest hops is considered the most efficient.

- **Periodic Updates:**

RIP routers exchange routing information at regular intervals, known as update intervals. These updates inform routers about changes in the network topology.

- **Split Horizon:**

RIP incorporates the split horizon technique to prevent routing loops. It avoids sending routing information back through the same interface from which it was received.

- **Hold-Down Timers:**

To stabilize the routing tables and prevent rapid, frequent changes, RIP uses hold-down timers. During this period, a router ignores updates about a route to allow time for convergence.

- **Route Poisoning:**

RIP uses route poisoning to advertise unreachable routes with infinite metric values. This informs other routers that a particular route is no longer valid.

- **Compatibility:**

RIP is a widely supported protocol and is often compatible across various networking devices and vendors.
In summary, RIP operates well in small to medium-sized networks, but its scalability may be limited in larger or more complex environments. Despite its relative simplicity, RIP remains a widely supported protocol, making it suitable for straightforward routing requirements.

DNS Server (Domain Name System)

A DNS server, or Domain Name System server, plays a pivotal role in the functionality of the internet by translating human-readable domain names into IP addresses that computers use to identify each other on the network. Here are key aspects of DNS servers:

- **Name Resolution:**

DNS servers resolve domain names, such as www.example.com, into corresponding IP addresses, allowing users and devices to access resources over the internet.

- **Hierarchical Structure:**

DNS operates in a hierarchical structure, with a distributed system of servers organized into zones. This structure helps in efficient and scalable name resolution.

- **DNS Zones:**

DNS divides the domain name space into zones, each managed by a specific authoritative DNS server. These zones help distribute the responsibility for maintaining DNS records.

- **Authoritative DNS Server:**

An authoritative DNS server holds the definitive records for a specific domain or zone. When queried, it provides accurate and up-to-date information for the requested domain.

- **Recursive DNS Server:**

Recursive DNS servers assist in the name resolution process by querying authoritative DNS servers on behalf of clients. They cache responses to speed up subsequent requests.

- **DNS Records:**

DNS maintains various types of records, including A records (mapping a domain to an IPv4 address), AAAA records (mapping to IPv6 addresses), MX records (identifying mail servers), and more.

- **DNS Query Process:**

When a user enters a domain name, their device sends a DNS query to a recursive DNS server. The recursive server, in turn, queries authoritative DNS servers to obtain the IP address associated with the domain.

- **Caching:**

DNS servers use caching to store previously resolved domain names and their corresponding IP addresses. This reduces the need to query authoritative servers for frequently accessed domains.

In essence, DNS servers form the backbone of internet navigation, enabling users to access websites, services, and resources using human-readable domain names while ensuring the efficient mapping of these names to corresponding IP addresses.

Implementations

Device Specification:

- Router-2911 (Main Router0)
- Multi-Layer Switch-3650-24PS
- Switch-2960-24TT (3)
- PC (9)
- Printer-PT (7)
- Access Point-PT (3)
- Laptop-PT (3)
- TabletPC-PT (2)
- SmartPhone(3)

PORT:

- **Switches:** In VLAN10, VLAN20 and VLAN30 we assign them 2 ports each, here fa0/1 is trunk means fa0/2-24 is the access port for VLAN10 and rest of the switches and VLANs individually.

```
Switch>enable
Switch#conf t
Switch(config)#vlan 10
Switch(config-valn)#name Accountant
Switch(config-valn)#exit
Switch(config)#int range fa0/2-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-valn)#exit
Switch(config)#int fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
Switch(config-if)#exit
Switch(config)#do wr
```

Same things are done for the rest of the switches. This is how we configure VLANs, name them, assign ports and configure trunks between switches to the router.

- **Multilayer Switch0:**

_All the VLANs are created in the switches should also create in the multilayer also. So,

```
Switch>enable
Switch#conf t
Switch(config)#vlan 10
Switch(config-valn)#name Accountant
```

```
Switch(config-vlan)#vlan 20
Switch(config-valn)#name Business
Switch(config-vlan)#vlan 30
Switch(config-valn)#name Loan
Switch(config-vlan)#exit
Switch(config)#int range gif1/0/1-4
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#exit
Switch(config)#do wr
```

Here we done the configuration from the multilayer switch to the access layer. Now we configure the router for inter VLAN routing purposes.

- **Main Router0:**

```
Router>enable
Router#conf t
Router(config)#int gig0/0
Router(config-if) no shut
Router(config-if )#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#int gig0/0.10
Router(config-subif)#
%LINK-5-CHANGED:   Interface GigabitEthernet0/0.10, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.10, changed state to up
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#exit
```

We are done the VLAN 10. Now for VLAN 20 and VLAN30:

```
Router(config)#int gig0/0.20
Router(config-subif)#
%LINK-5-CHANGED:   Interface GigabitEthernet0/0.20, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.20, changed state to up
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#exit

Router(config)#int gig0/0.30
Router(config-subif)#
%LINK-5-CHANGED:   Interface GigabitEthernet0/0.30, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.30, changed state to up
```

```
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#exit
```

DHCP Server configuration:

```
Router(config)#service dhcp
Router(config)#ip dhcp pool Accoutant-Pool
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.1
Router(dhcp-config)#exit
Router(config)#
Router(config)#ip dhcp pool Business-Pool
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns-server 192.168.1.1
Router(dhcp-config)#exit
Router(config)#
Router(config)#ip dhcp pool Loan-Pool
Router(dhcp-config)#network 192.168.3.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.3.1
Router(dhcp-config)#dns-server 192.168.3.1
Router(dhcp-config)#exit
Router(config)#do wr
Building configuration. . .
[OK]
Router(config)#
```

IP Addresses:

First floor (Accountant Department):

IP: 192.168.1.1 to 192.168.1.10, Subnet: 255.255.255.0, Default Gateway: 192.168.1.1, DNS server:192.168.1.1

Second floor (Business Department):

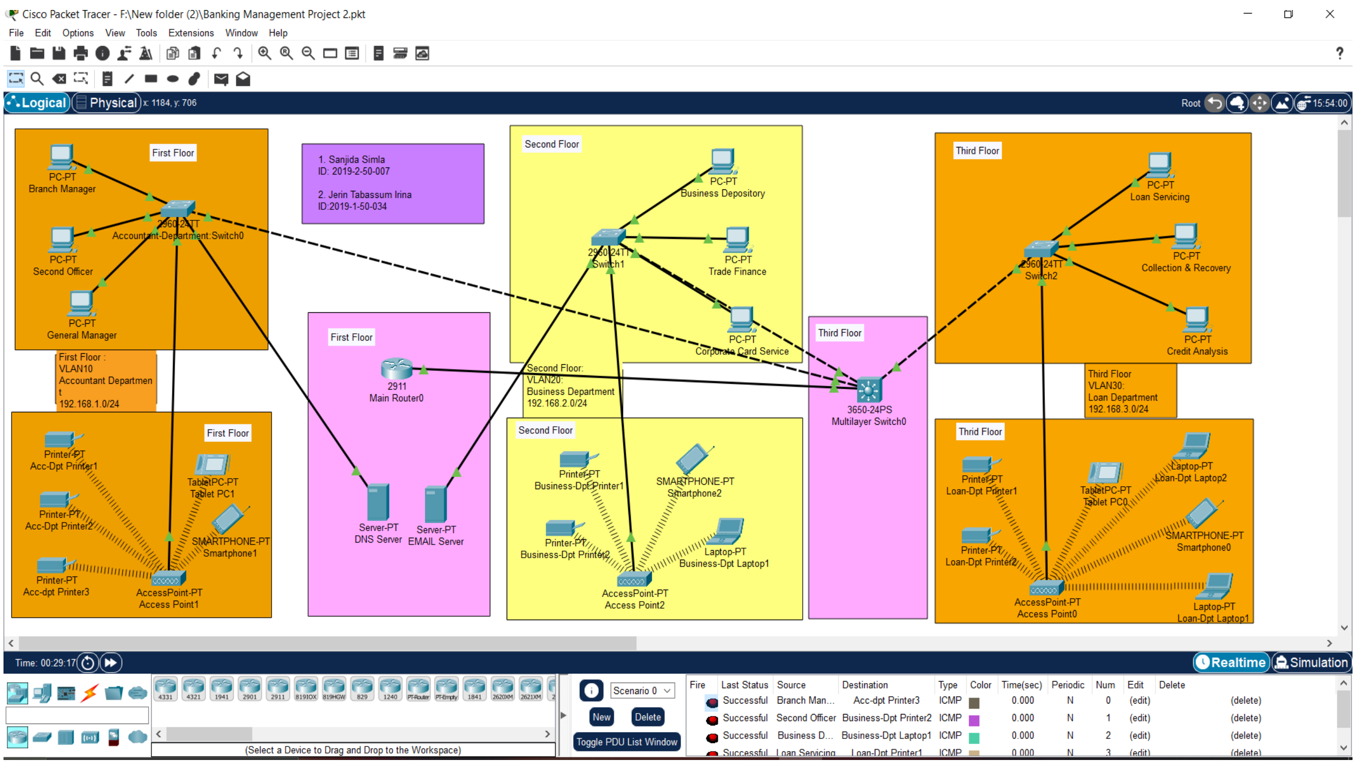
IP: 192.168.2.1 to 192.168.2.10, Subnet: 255.255.255.0, Default Gateway: 192.168.2.1, DNS server:192.168.2.1

Third floor (Loan Department):

IP: 192.168.3.1 to 192.168.3.10, Subnet: 255.255.255.0, Default Gateway: 192.168.3.1, DNS server:192.168.3.1

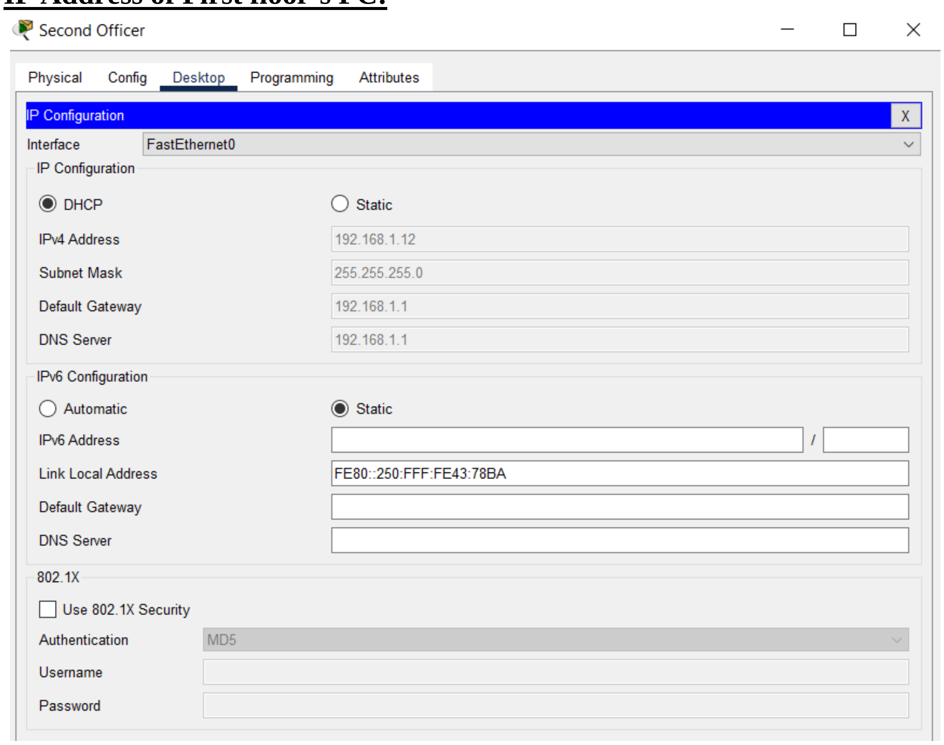
here we keep the IP Address in a range so that if any new PC needs to be added to the office, then it will get that IP corresponding to its VLANs.

Topology

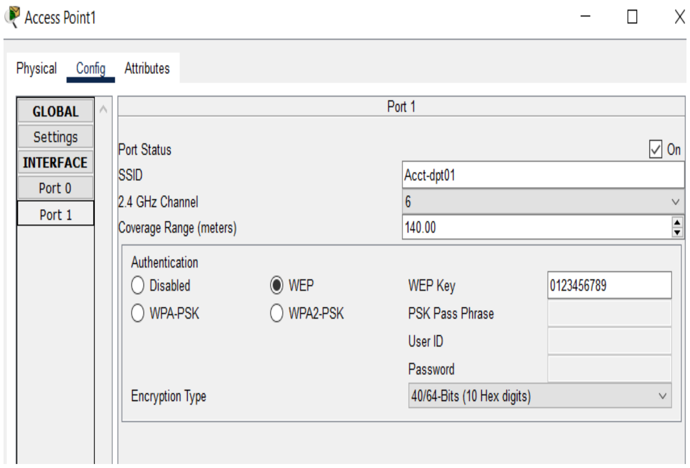


First Floor

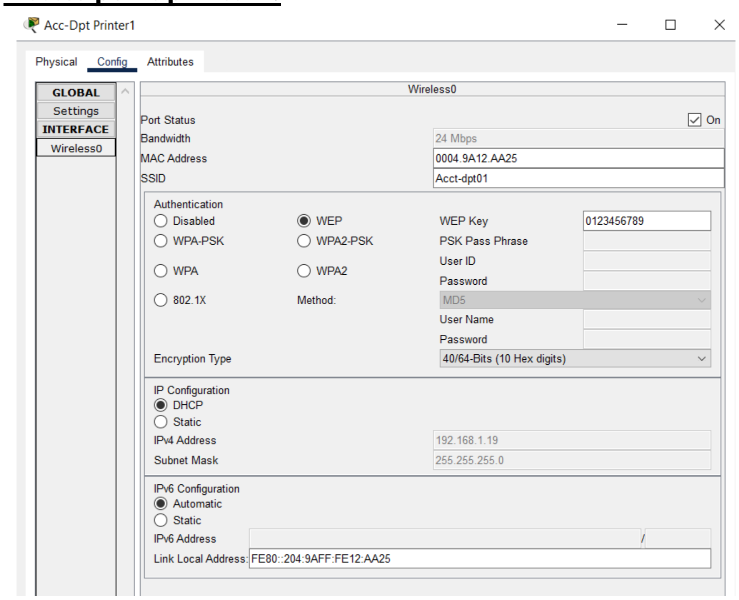
IP Address of First floor's PC:



Access point1:

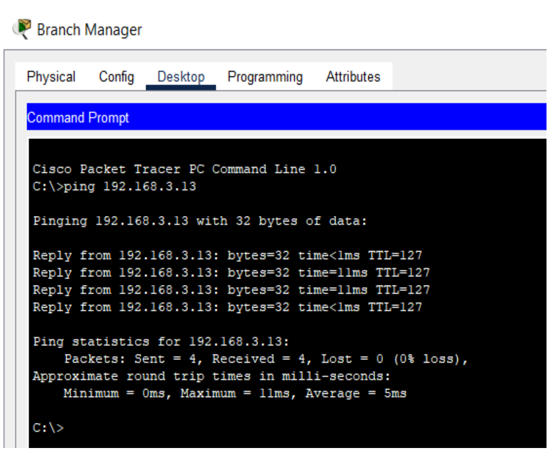


Access point printer1:

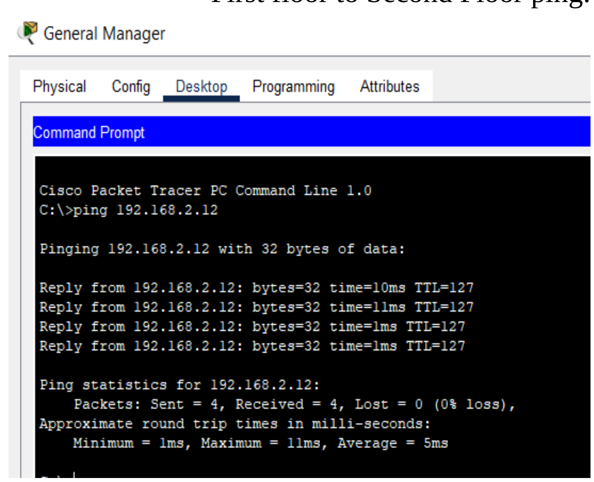


All Ping results:

First Floor to Third Floor ping:

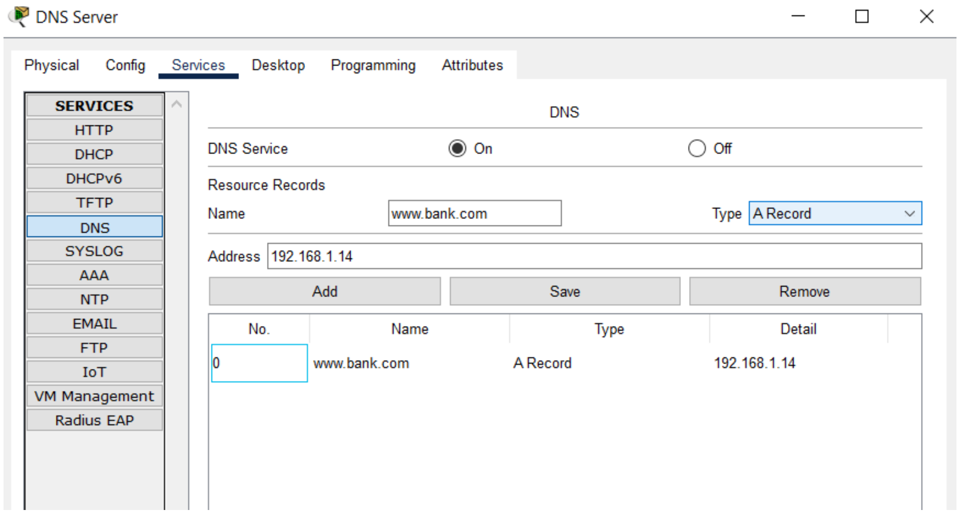


First floor to Second Floor ping:



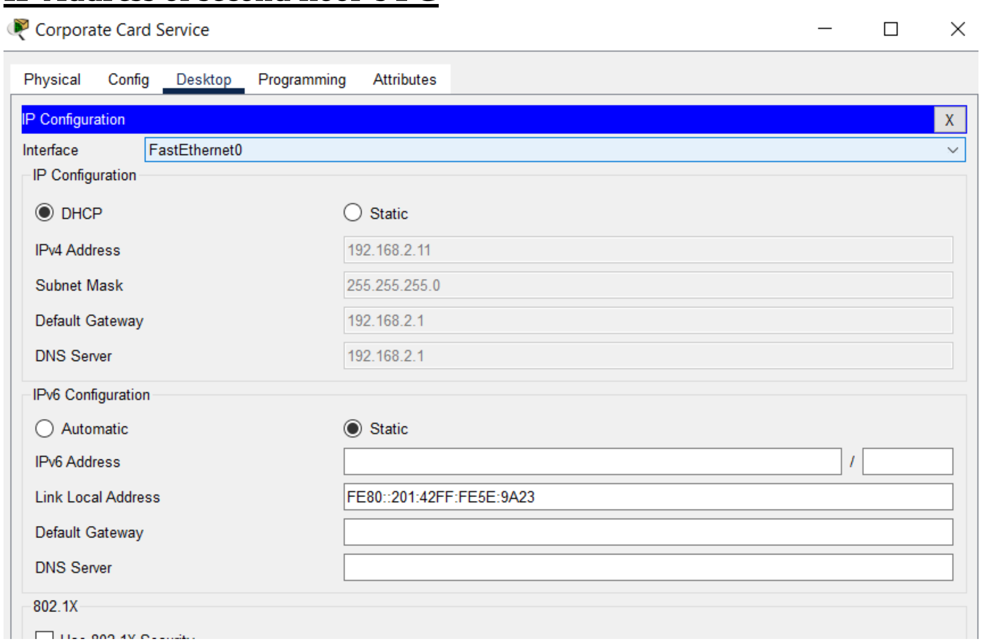
Fire	Last Status	Source	Destination	Type	Color	Time(s	Perioc	Num	Edit	Delete
	Successful	Branch Manager	Tablet PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	General Manager	Acc-Dpt Printer1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Second Officer	Smartphone1	ICMP		0.000	N	2	(edit)	(delete)

DNS Server:

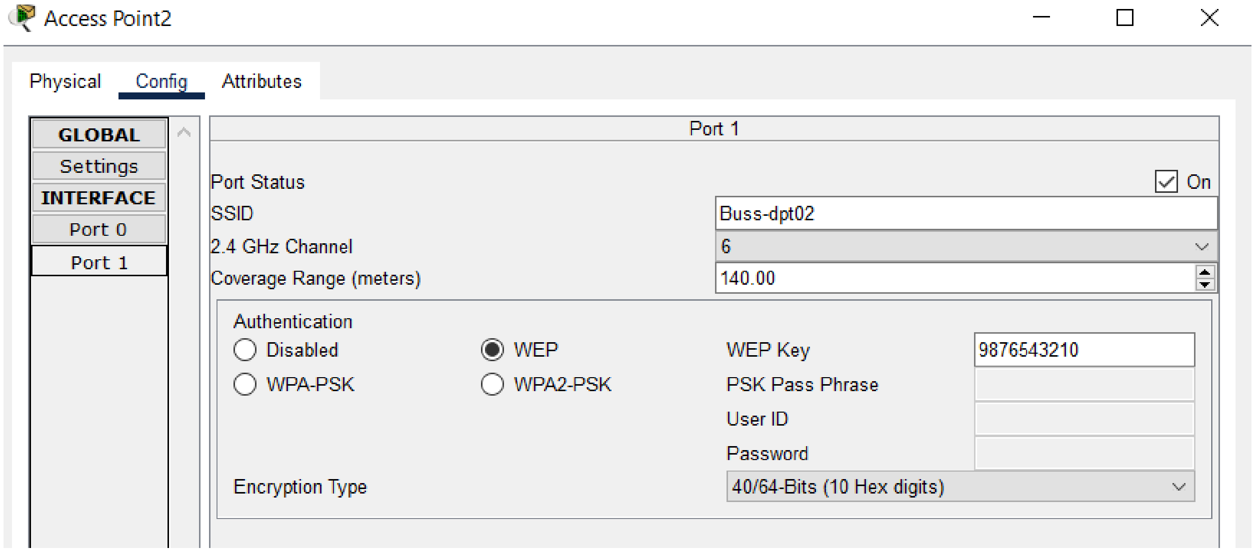


Second Floor

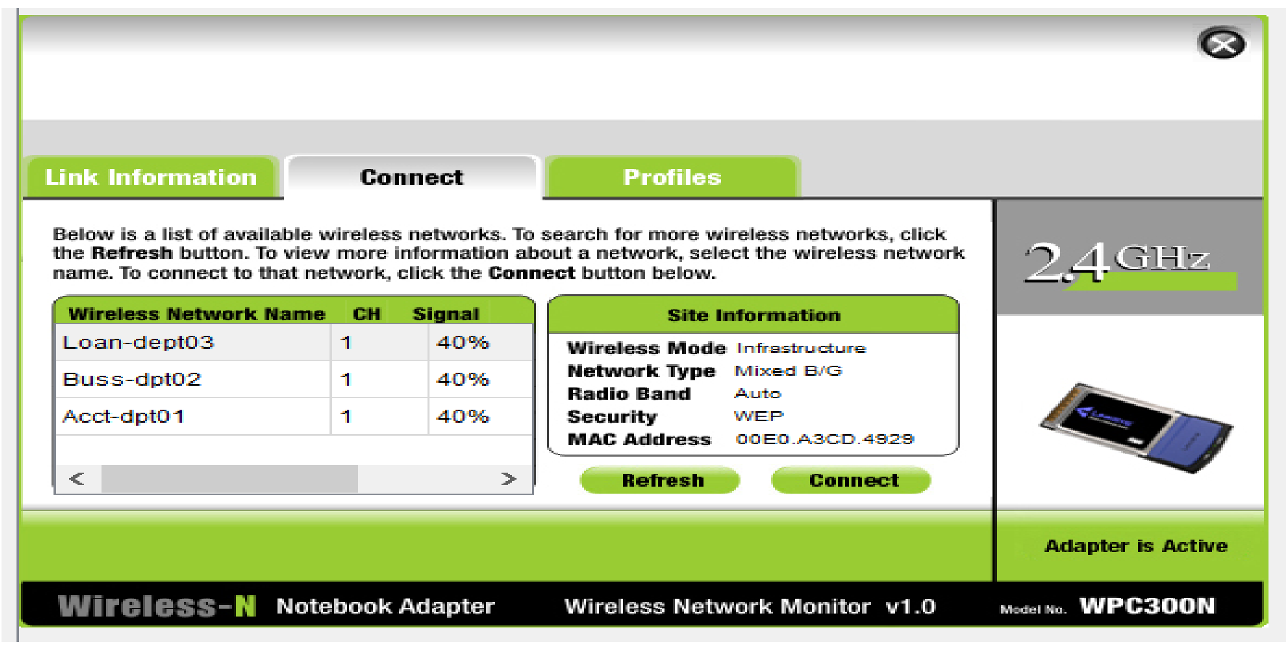
IP Address of second floor's PC



Access point2

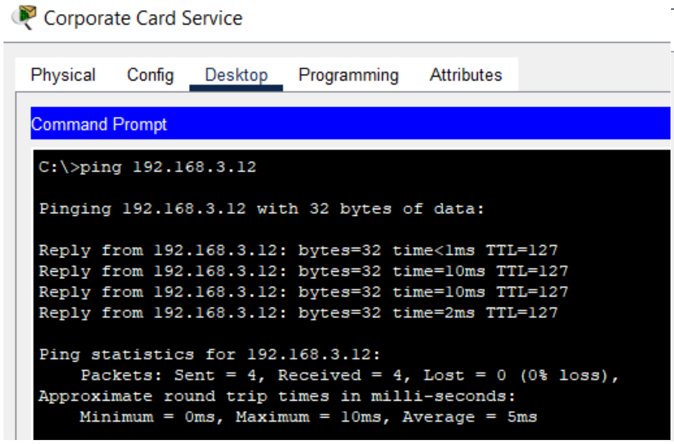


Laptop Connected to the accesspoint2:

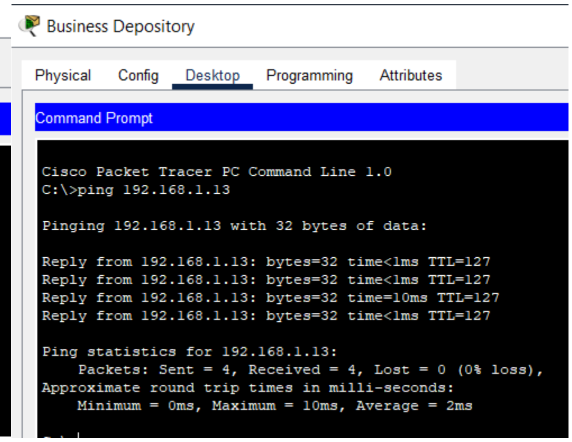


All the ping results in the Second Floor:

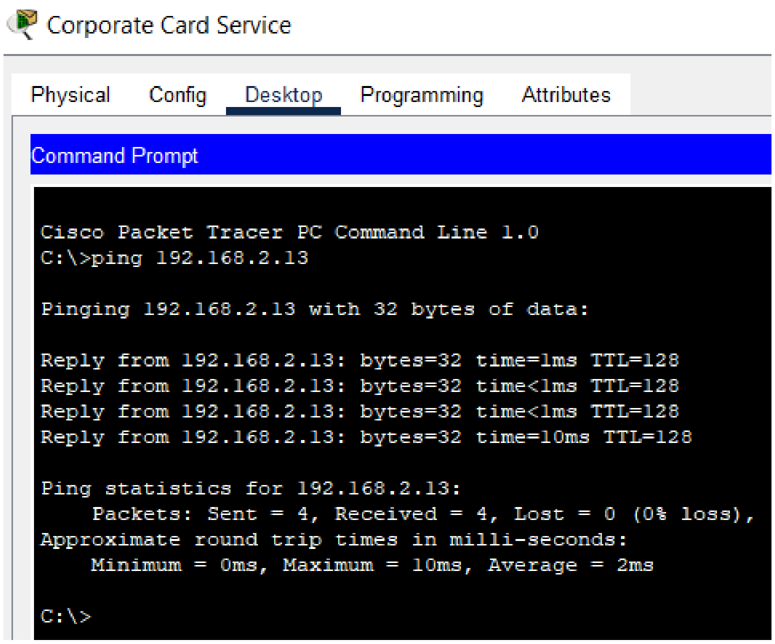
Second Floor to Third floor:

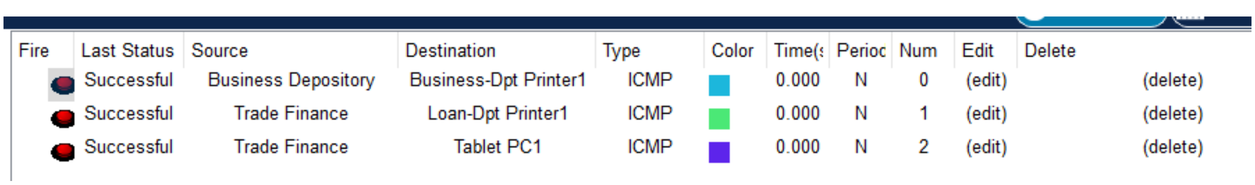


Second Floor to First floor:



Second Floor to Second floor:

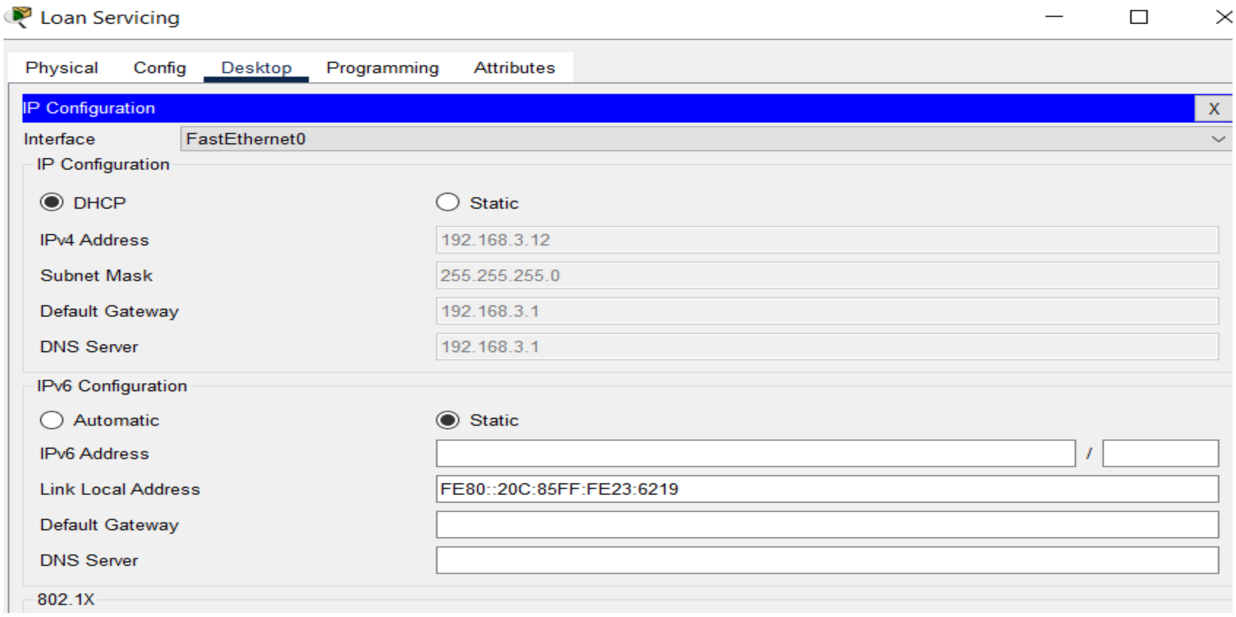




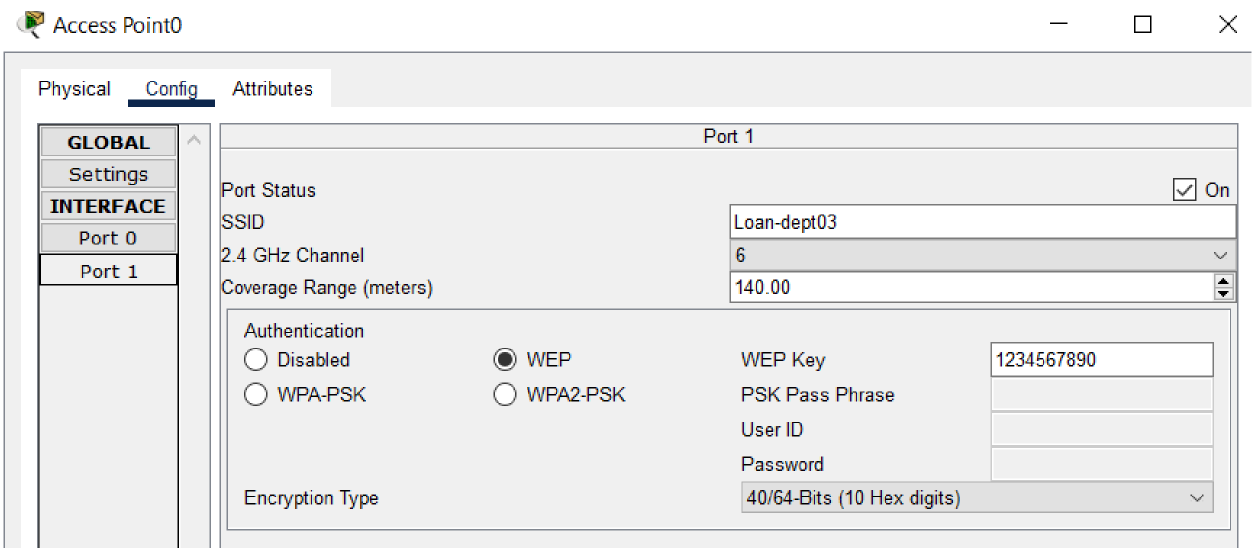
Fire	Last Status	Source	Destination	Type	Color	Time(s	Perioc	Num	Edit	Delete
	Successful	Business Depository	Business-Dpt Printer1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Trade Finance	Loan-Dpt Printer1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Trade Finance	Tablet PC1	ICMP		0.000	N	2	(edit)	(delete)

Third Floor

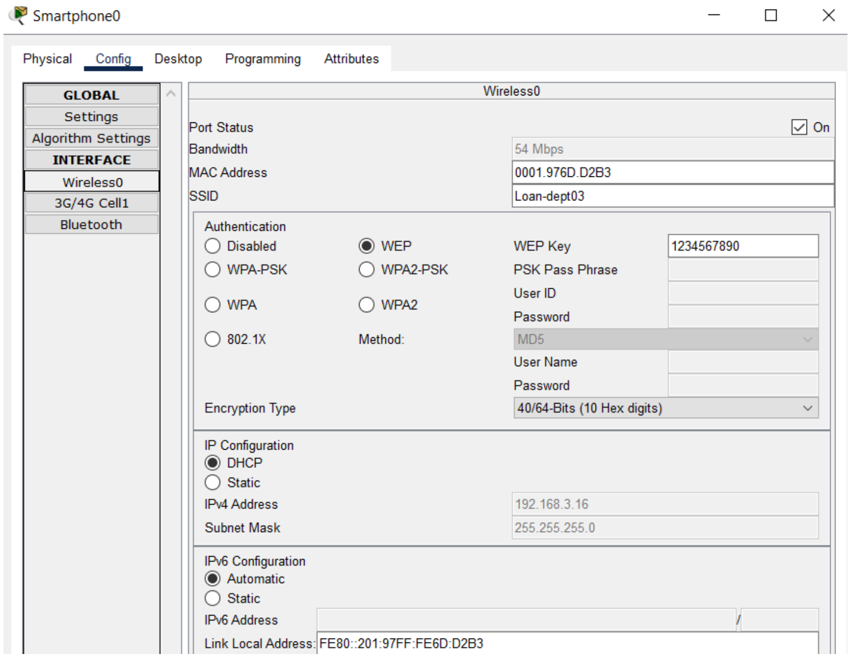
IP Address of Third floor’s PC



Access point3:

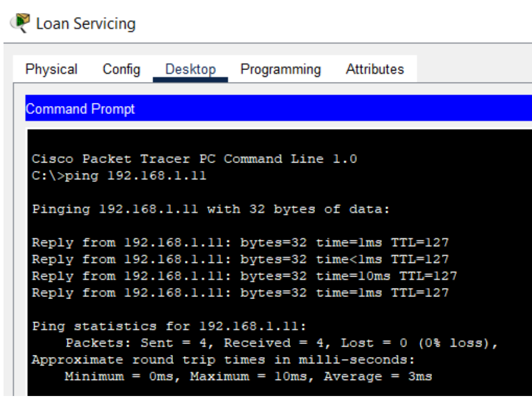


Smart phone connected to the third floor:

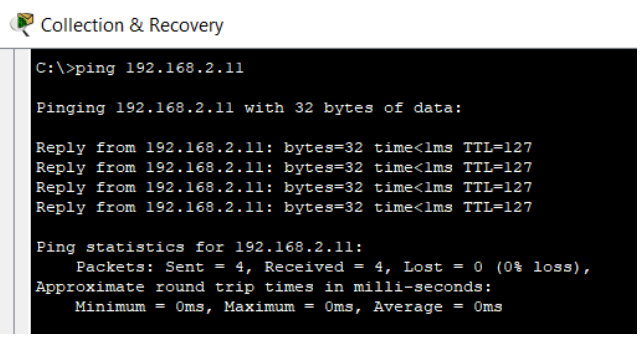


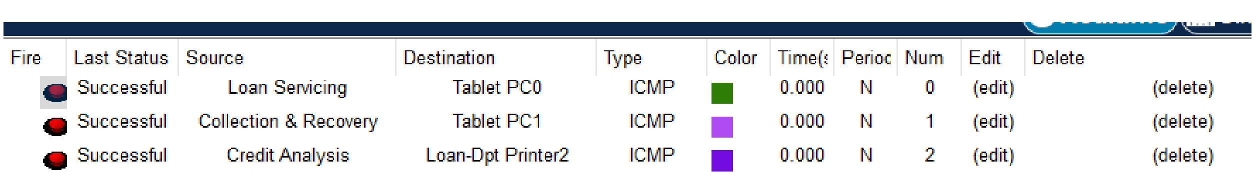
All the ping Result:

Third floor to First Floor:



Third floor to Second floor:





Fire	Last Status	Source	Destination	Type	Color	Time(s	Perioc	Num	Edit	Delete
	Successful	Loan Servicing	Tablet PC0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Collection & Recovery	Tablet PC1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Credit Analysis	Loan-Dpt Printer2	ICMP		0.000	N	2	(edit)	(delete)

Discussion

Our network management project focused on VLAN implementation and DHCP services, brings forth a structured and efficient solution tailored to our banking environment. The Virtual Local Area Network (VLAN) architecture divides our banking facility into three distinct floors, each dedicated to a specific department: Accountant, Business Banking, and Loan Department. This segmentation improves network performance and streamlines communication between departments.

The DHCP (Dynamic Host Configuration Protocol) services are crucial for our dynamic network environment. By automatically assigning IP addresses and configuration parameters to devices, DHCP eliminates the manual effort of IP address management. The inclusion of dedicated DHCP servers ensures that each department's devices receive accurate and timely configurations, contributing to a seamless and well-organized networking experience.

Within each department, we've strategically placed servers such as email and DNS servers to support essential services. The deployment of multilayer switches and a main router facilitates inter-departmental communication while maintaining logical separation through VLANs. This architecture not only enhances network security but also provides a scalable framework for future expansion and technology integration.

The decision to use dedicated servers for DHCP, email, and DNS services ensures reliability and centralized management. Each department has its own unique VLAN, reflecting our commitment to departmental isolation and efficient resource utilization. The implementation of AccessPoints further extends our network's capabilities, facilitating wireless connectivity for devices within each department.

The use of VLANs, coupled with DHCP services, creates a dynamic and adaptable network infrastructure suitable for the diverse needs of our banking environment. It promotes efficient resource allocation, improves network manageability, and sets the foundation for future technological enhancements.

In conclusion, our VLAN and DHCP-based network management project stands as a testament to our commitment to modernizing banking operations. The meticulous design and implementation of this network architecture not only address our current requirements but also lay the groundwork for a scalable, secure, and technologically advanced banking environment. As we move forward, we anticipate increased operational efficiency, enhanced collaboration, and a robust foundation for adapting to the evolving landscape of banking services.