Designing a VLAN-Based Network for a Small Branch Office: A Case Study on Network Segmentation, Wireless Integration, and Automatic IP Assignment

A CASE STUDY REPORT

Submitted by

SIDDA TEJASWI (RA2211003011107)

YASWANTH VEMPA (RA2211003011123)

for the course

21CSC302J – COMPUTER NETWORKS

in partial fulfilment of the requirements for the degree of

BACHELOR OF TECHNOLOGY

DEPARTMENT OF COMPUTING TECHNOLOGIES

SCHOOL OF COMPUTING

FACULTY OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR - 603203

NOVEMBER 2024

Abstract

This report presents a detailed case study on the design and implementation of a VLAN-based network for a small branch office of XYZ Company, leveraging Cisco networking equipment. The primary objective of the project is to establish a robust, secure, and scalable network infrastructure that supports efficient departmental segmentation through VLANs, wireless network integration for seamless user connectivity, and automatic IP address allocation using DHCP. The network design facilitates communication between three distinct departments— Admin/IT, Finance/HR, and Customer Service/Reception—while ensuring network isolation and enhanced security through VLAN configurations. A single router and switch were utilized to create an efficient, cost-effective solution in line with the company's requirements. The report also outlines the configuration of IPv4 addressing, wireless access points, and inter- VLAN routing to enable communication across departments. Emphasis is placed on the practical challenges and solutions encountered during the network design process, ensuring the system is future-proof and capable of supporting the company's growth and operational needs in the Bonalbo branch.

TABLE OF CONTENTS

1.Introduction

1.1 Background

In today's rapidly evolving digital landscape, the design and implementation of efficient network infrastructures are critical for businesses to maintain smooth operations and support expansion efforts. XYZ Company, a fast-growing enterprise in Eastern Australia with over 2 million customers globally, is planning to open a new branch in the village of Bonalbo. This branch will operate independently from the headquarters, requiring a dedicated network that supports the company's expanding customer base and operational needs.

1.2 Objectives

The key objectives of this project are to design and implement a network infrastructure for XYZ Company's Bonalbo branch that meets the following criteria:

- **VLAN Segmentation**: Create separate VLANs for the Admin/IT, Finance/HR, and Customer Service/Reception departments to ensure network segmentation, enhance security, and optimize network traffic management.
- **Wireless Network Integration**: Establish wireless networks for each department to support seamless connectivity for mobile devices and improve operational flexibility.
- **Automatic IP Assignment**: Implement a DHCP server to automatically assign IPv4 addresses to host devices, reducing manual configuration and ensuring efficient address management.
- **Inter-VLAN Communication**: Ensure devices across different VLANs can communicatesecurely through appropriate routing configurations.
- **Scalability and Future Growth**: Design a network that can scale as the company grows and adapts to future technological advancements.
- **Cost-Effectiveness**: Implement the network using a minimal number of devices, including one Cisco router and one Cisco switch, to meet the company's budget constraints while ensuring high performance and reliability.

By achieving these objectives, the network design will provide XYZ Company with a robust and scalable infrastructure that meets both its current operational needs and future growth aspirations.

2. Network Design

2.1 Topology

The network design for XYZ Company's Bonalbo branch follows a simplified yet effective topology aimed at supporting the company's operational needs. Given the small-scale nature of the branch and the company's requirements, a flat network structure with VLAN segmentation is employed. A single Cisco router is used to connect the internal network to the Internet Service Provider (ISP), while a single Cisco switch handles all internal communications, including VLAN separation for different departments.

efficient network segmentation and enhanced security. Wireless access points are deployed to provide wireless connectivity to users in each department, allowing for flexibility and ease of access.

The following key features are included in the design:

- VLAN configuration for departmental segmentation.
- DHCP for automatic IP assignment to host devices.
- Inter-VLAN routing using the router to allow communication between departments.
- Wireless network integration for each department's users.

This topology ensures cost-effectiveness while maintaining the necessary functionality to meet XYZ Company's requirements for its new branch in Bonalbo.

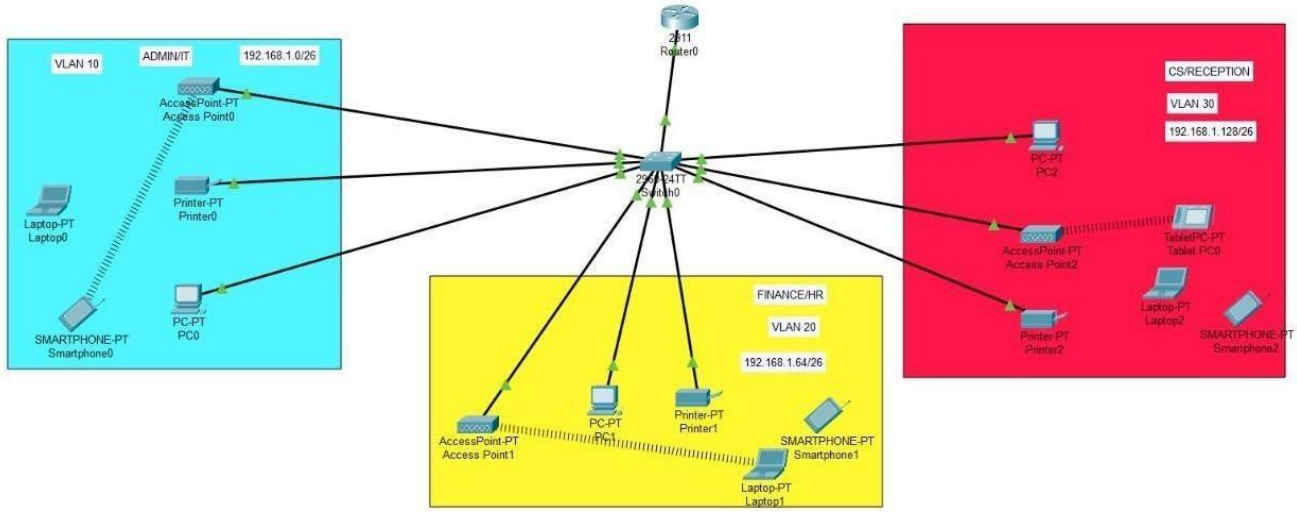


Figure : Topology of full network

2.2 Components

The network design for the project incorporates the following devices:

1. **Routers (Cisco 2911):**
   - Positioned at the core to provide inter-VLAN routing and connection to the ISP.
   - Configured with a base network of 192.168.1.0/24.
2. **Switch (Cisco 2960):**
   - Layer 2 switch managing the internal wired network.
   - Configured to handle VLANs for each department to isolate traffic.
3. **Wireless Access Points:**
   - Each department has its own access point for wireless users.
   - Integrated within respective VLANs for seamless wireless communication.
4. **Cisco Access Points (APs):**
   - Each department includes PCs, laptops, printers, and smartphones.
   - Devices automatically obtain IP addresses via DHCP.

2.3 IP Addressing Scheme

The network uses a subnetting strategy based on the 192.168.1.0/24 base address provided by the ISP. The following IP addressing scheme is applied to each VLAN:

Department	VLAN	Network Address	Subnet Mask	Host Address Range	Broadcast Address
Admin/IT	VLAN 10	192.168.1.0	255.255.255.192 /26	192.168.1.1 to 192.168.1.62	192.168.1.63
Finance/HR	VLAN 20	192.168.1.64	255.255.255.192 /26	192.168.1.65 to 192.168.1.126	192.168.1.127
Customer Service/Reception	VLAN 30	192.168.1.128	255.255.255.128 /25	192.168.1.129 to 192.168.1.254	192.168.1.255

- **DHCP Server:** Configured within the router to allocate dynamic IP addresses for all VLANs.
- **Default Gateway:** The router provides the gateway addresses for each VLAN.

Additional Data:

- **VLAN Configuration**:
  - VLAN 10: Admin/IT department
  - VLAN 20: Finance/HR department
  - VLAN 30: Customer Service/Reception
- **Wireless Network**:
  - Each department has its own wireless access point.
  - Devices such as laptops, smartphones, and tablets connect to the network wirelessly.

This VLAN-based design ensures efficient traffic segregation, security, and scalability for XYZ Company's branch in Bonalbo. The network is capable of supporting inter-VLAN communicationwhile providing wireless access for mobile devices across all departments.

3. Routing Configuration

3.1 Router Configuration

Basic Router Configuration

```
conf t
hostname XYZ-Router
line console 0
password cisco
login
exit
enable password cisco  # Sets the enable password to 'cisco'
no ip domain-lookup # Disables DNS lookup for incorrectly entered commands
banner motd # NO Unauthorized Access!!! #
service password-encryption
do wr
ip domain name xyz.local
username admin password cisco
crypto key generate rsa
key modulus 1024
line vty 0 15
login local
transport input ssh
ip ssh version 2
exit
```

3.2 Static and Dynamic Routing

The routing strategy in the XYZ network integrates both static and dynamic routing techniques to ensure optimal traffic flow and redundancy. Static routes are used for predictable internal communication between VLANs, while dynamic routing is employed using **OSPF** (Open Shortest Path First) for scalable, adaptive route discovery and selection.

- **Static Routing**: Configured to handle predefined paths for traffic, ensuring consistent routing of important internal communications (e.g., between departments).
- **Dynamic Routing (OSPF)**: This is used to handle external and changing routes, ensuringscalability and adaptability to network changes.

OSPF Configuration on Router:

```
router ospf 10
router-id 1.1.1.1
network 192.168.1.0 0.0.0.63 area 0  # Admin VLAN
network 192.168.1.64 0.0.0.63 area 0  # Finance/HR VLAN
network 192.168.1.128 0.0.0.127 area 0  # Customer Service VLAN
exit
do wr
```

3.3 Interface Configuration on Core Router

Below is the configuration for IP addressing on the core router interfaces to facilitatecommunication between departments and with external networks:

```
interface gig0/0
ip address 192.168.1.1 255.255.255.192  # Admin/IT
no shutdown
exit

interface gig0/1
ip address 192.168.1.65 255.255.255.192  # Finance/HR
no shutdown
exit

interface gig0/2
ip address 192.168.1.129 255.255.255.128  # Customer Service/Reception
no shutdown
exit

interface serial0/1/0
ip address 203.0.113.1 255.255.255.252  # Connection to ISP
clock rate 64000
no shutdown
exit
do wr
```

3.4 Interface Configuration on ISP Router

Below is the basic IP configuration on the ISP side to provide connectivity to the internet:

```
interface serial0/1/1
ip address 203.0.113.2 255.255.255.252  # ISP Link 1
no shutdown
exit

interface serial0/1/2
ip address 203.0.113.6 255.255.255.252  # ISP Link 2
no shutdown
exit
do wr
```

3.5 Default Route Configuration

To ensure external traffic can be routed outside the organization’s network, a default route isconfigured to point towards the ISP's network.

```
ip route 0.0.0.0 0.0.0.0 serial0/1/0  # Default route to ISP
ip route 0.0.0.0 0.0.0.0 serial0/1/1  # Backup route
exit
do wr
```

Summary:
This configuration provides a robust mix of static and dynamic routing for the XYZ Company's branch. With OSPF implemented for adaptive routing between internal VLANs and static routesensuring predictable paths, the network design is scalable and efficient. Secure SSH access and password encryption enhance security, while VLANs ensure proper segmentation of departmentnetworks.

4. Switching Configuration

4.1 Switch Configuration

Below is the basic configuration for the switches in the XYZ Company network. This configuration sets up basic security, SSH access, and fundamental settings for the VLANs on theswitches.

Switch Configuration for Finance Department Switch:

```
conf t
hostname Finance-SW
line console 0
password cisco
login
exit

enable password cisco
no ip domain-lookup # Disables DNS lookup for incorrectly entered commands
banner motd # No Unauthorized Access!!! #
service password-encryption
do wr

ip domain name xyz.local  # Domain name for SSH
username admin password cisco  # Local admin user configuration

crypto key generate rsa
modulus 1024  # Generates 1024-bit RSA keys for SSH
exit

line vty 0 15
login local
transport input ssh # Enables SSH for remote access
exit

ip ssh version 2  # Enables SSH version 2
do wr
```

4.2 VLAN Configuration

The VLANs on the switch are configured to segment the network according to department-specific needs.

```
vlan 10
name Admin
exit

vlan 20
name Finance_HR
exit

vlan 30
name Reception_CS
exit

interface vlan 10
ip address 192.168.1.1 255.255.255.192
no shutdown
exit

interface vlan 20
ip address 192.168.1.65 255.255.255.192
no shutdown
exit

interface vlan 30
ip address 192.168.1.129 255.255.255.128
no shutdown
exit

do wr
```

Summary:
This configuration sets up basic management access, security (SSH), and VLAN segmentationfor the Finance department's switch. The configurations for each VLAN enable secure and structured communication between different segments of the network.

5. Inter-VLAN Routing

5.1 Layer 3 Switching using SVIs (Switch Virtual Interfaces)

In the XYZ Company network, Inter-VLAN Routing is implemented by utilizing Layer 3 (L3)switches with SVIs. This allows the switch to route traffic between VLANs. Each VLAN is assigned a unique IP address, and the Layer 3 switch handles the routing between them. Belowis the configuration of the switch with SVIs for VLANs 10, 20, and 30 as seen in the topology diagram.

Inter-VLAN Configuration on the Layer 3 Switch:

```
# VLAN 10 (Admin)
interface vlan 10
ip address 192.168.1.1 255.255.255.192  # SVI for VLAN 10
no shutdown
ip helper-address 192.168.60.2  # DHCP relay to the server
exit

# VLAN 20 (Finance/HR)
interface vlan 20
ip address 192.168.1.65 255.255.255.192  # SVI for VLAN 20
no shutdown
ip helper-address 192.168.60.2  # DHCP relay to the server
exit

# VLAN 30 (Reception/CS)
interface vlan 30
ip address 192.168.1.129 255.255.255.128  # SVI for VLAN 30
no shutdown
ip helper-address 192.168.60.2  # DHCP relay to the server
exit

do wr  # Save configuration
```

In this configuration:

- Each VLAN has a corresponding Switch Virtual Interface (SVI) that acts as the gateway for the devices inthat VLAN.
- The ip helper-address command forwards DHCP requests to the DHCP server located in the server room(192.168.60.2).

5.2 Subnetting

Subnetting is crucial in allocating IP addresses efficiently and managing network resources. For this project, the base network address **192.168.1.0/24** is divided into subnets for each department using **/26** and **/25** subnet masks. This ensures each department (VLAN) has a distinct range of IP addresses.

Subnetting Details for Each VLAN:

VLAN	Network Address	Subnet Mask	Host Address Range	Broadcast Address
VLAN 10 (Admin)	192.168.1.0	255.255.255.192	192.168.1.1 - 192.168.1.62	192.168.1.63
VLAN 20 (Finance/HR)	192.168.1.64	255.255.255.192	192.168.1.65 - 192.168.1.126	192.168.1.127
VLAN 30 (Reception/CS)	192.168.1.128	255.255.255.128	192.168.1.129 - 192.168.1.254	192.168.1.255

By subnetting the network in this manner:

- Each VLAN has its own unique IP range, preventing IP conflicts.
- The network is scalable and can support the addition of more VLANs in the future.
- It ensures better management of network traffic and provides an organized and securestructure.

Advantages of Subnetting:

- Improved Security: Each department's traffic is separated, reducing the risk of broadcaststorms and isolating network issues.
- Efficient Address Allocation: Subnetting reduces the wastage of IP addresses and enableseffective usage of the IP address space.
- Enhanced Management: Subnets make it easier to troubleshoot, monitor, and managenetwork resources.

This configuration ensures smooth communication between different VLANs and an efficient allocation of network resources.

6. Security Measures

6.1 Access Control Lists (ACLs)

In the XYZ Company network, **Access Control Lists (ACLs)** are applied on routers to filter traffic based on defined criteria, such as source and destination IP addresses, ports, and protocols. This enhances security by restricting which devices can communicate with others.

ACL Configuration:

```
# ACL to permit traffic from VLAN 10 (Admin) to VLAN 20 (Finance/HR), and deny all other traffic
access-list 100 permit ip 192.168.1.0 0.0.0.63 192.168.1.64 0.0.0.63
access-list 100 deny ip any any  # Deny all other traffic

# Applying the ACL to VLAN 10 interface
interface vlan 10
ip access-group 100 in
exit
```

In this configuration:

- **ACL 100** allows traffic from devices in VLAN 10 (Admin) to VLAN 20 (Finance/HR), while blocking all othertraffic.
- The **ip access-group** command applies the ACL to the incoming traffic on the VLAN 10 interface.

6.2 NAT and PAT

Company network to conserve public IP addresses and provide a layer of security. NAT is used to map private internal IP addresses to a public IP address, while PAT allows multiple devices to share a single public IP address by mapping different ports.

NAT, PAT used for security and efficiency:

```
# Configuring NAT inside for the internal interfaces (LAN)
interface range gig0/0-1
ip nat inside
exit

# Configuring NAT outside for the external interfaces (WAN)
interface se0/2/0
ip nat outside
exit

interface se0/2/1
ip nat outside
exit

# Enabling PAT (overloading) with a pool of public IPs
ip nat inside source list 1 interface se0/2/0 overload

# Access list for the internal network that can use NAT
access-list 1 permit 192.168.1.0 0.0.0.255

do wr  # Save the configuration
```

In this configuration:

- **NAT inside** is applied to the internal interfaces (gig0/0-1), while **NAT outside** is applied to theexternal interfaces (se0/2/0 and se0/2/1).
- **PAT** (overloading) is enabled, allowing multiple internal IP addresses to share a single external IPaddress.

6.3 Port Security

Port Security is implemented on switches to restrict access to the network by limiting the number of MAC addresses allowed on a switch port. This helps prevent unauthorized devices from connecting to the network. Below is the configuration applied to the switch ports in the **Finance** department to enhance security.

```
# Apply port security on the FastEthernet ports of the Finance
VLANinterface range fastEthernet0/3-24
switchport port-
security switchport
port-security maximum 1
```

Port Security Configuration for the Finance Department:

In this configuration:

- **interface range fastEthernet0/3-24**: Specifies the range of switch ports used by the Financedepartment.
- **switchport port-security maximum 1**: Limits the number of MAC addresses to 1 per port,ensuring only one device is connected.
- **switchport port-security mac-address sticky**: Enables the switch to dynamically learn and store the MAC addresses of connected devices, making it easier to secure connections without manual configuration.
- **switchport port-security violation shutdown**: If a port violation occurs (e.g., more than one device is connected), the port is automatically shut down to prevent unauthorized access.

This configuration enhances security by ensuring that only one device can connect to each port. In case of a violation, the port is disabled, reducing the risk of unauthorized access to the Finance department's network.

7. Quality of Service (QoS)

7.1 QoS Configuration

In the XYZ Company network, **Quality of Service (QoS)** is not a requirement, but understanding its configuration can be useful for future scalability. QoS is typically implemented to prioritize certain types of network traffic (like voice, video, or critical business applications) to ensure they receive higher bandwidth and lower latency compared to less critical traffic.

QoS Configuration:

```
# Configuring QoS on a Cisco router interface
interface gig0/0
bandwidth 10000  # Set the interface bandwidth to 10,000 kbps (adjust as needed)

# Defining a QoS policy map
policy-map QOS-POLICY
  class VOICE
    priority percent 30  # Allocate 30% bandwidth for voice traffic
  class VIDEO
    bandwidth percent 20  # Allocate 20% bandwidth for video traffic
  class class-default
    fair-queue # Enable fair queuing for best-effort traffic
exit
```

In this configuration:

- **VOICE traffic** is given 30% of the available bandwidth to ensure smooth communication.
- **VIDEO traffic** is allocated 20% bandwidth for adequate video streaming.
- **Best-effort traffic** (anything not classified a14
- oice or video) uses fair-queue, meaning 14

it'shandled fairly, but without any specific priority.

8. Monitoring and Management

8.1 SNMP Configuration

Simple Network Management Protocol (SNMP) is a crucial tool for monitoring and managing devices in the network. SNMP allows for the collection of data regarding network performance and health, as well as sending notifications (traps) when specific events occur.

```
# Enable SNMP
snmp-server community <community-string> RO # Set the SNMP community string for read-only
access
snmp-server enable traps # Enable SNMP traps for event notification
```

In this configuration:

- **mycommunity** is the SNMP community string used for monitoring. It allows the SNMP manager to readdevice information but not change it.
- **traps** are SNMP notifications sent when specific events (like interface down, high CPU usage, etc.) occuron the device.Logging and Alerts

Logging and alerting are essential for maintaining network health by capturing and reporting important events. It allows the network administrator to troubleshoot issues efficiently by referring to the logs stored either locally or on an external syslog server.

```
# Enable logging on the device
logging buffered informational  # Set the logging severity level to informational

# Configure logging to an external syslog server
logging 192.168.1.100  # IP address of the external syslog server

# Configure SNMP traps for critical events
snmp-server enable traps syslog  # Enable SNMP traps to send syslog messages for
critical events
```

9. Testing and Validation

9.1 Simulation

For the **XYZ Farmer-to-Customer Sales Platform**, testing and validation were performed usinga network simulation tool. The simulation involved the following steps:

- **Network Topology Design**: A virtual network was built, including key components like routers, switches, PCs, and servers. The topology reflected the actual design proposed forthe project.
- **Configuration Implementation**: Configurations were applied to routers, switches, and other devices according to the planned network setup. This was done to simulate real- world operations and verify hat configurations aligned with the

project's goals.

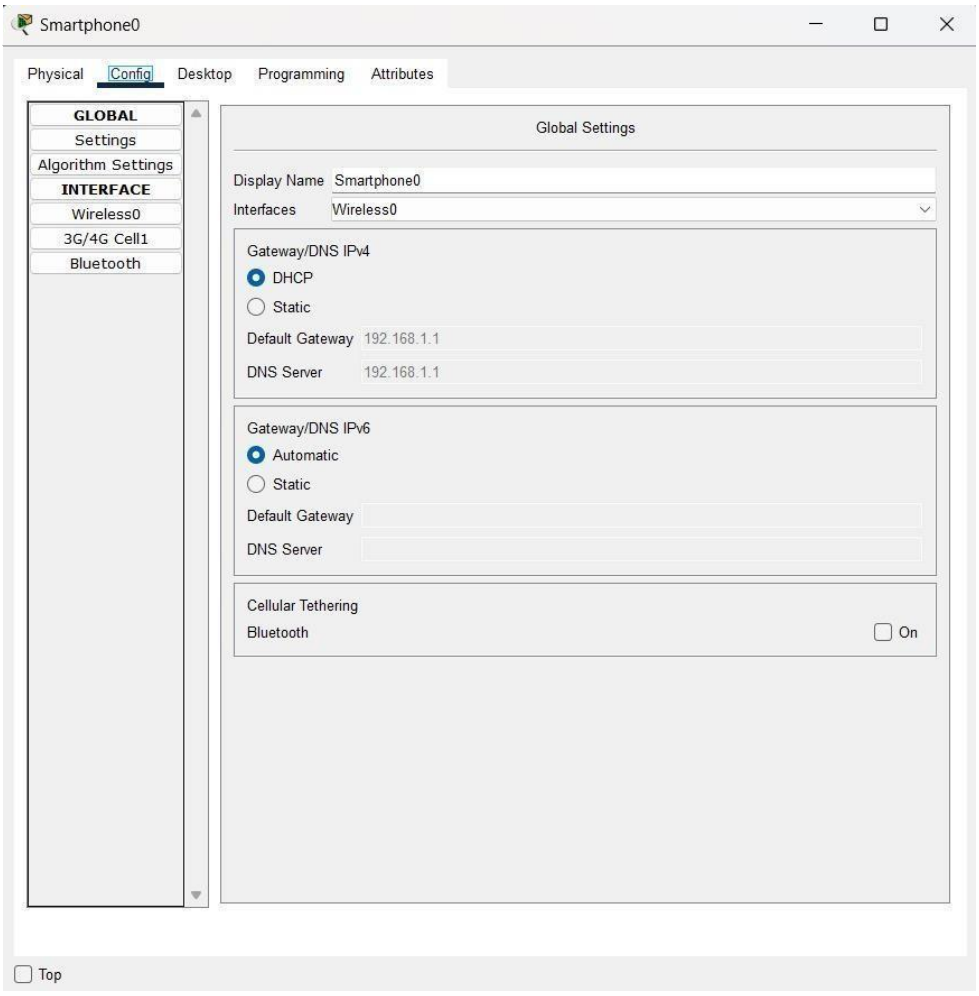
- **Traffic Simulation**: The simulation included generating network traffic to test connectivityand communication across different VLANs and between departments (sales and management teams).

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Tablet PC0	ICMP		0.000	N	5	(edit)	(delete)
	Successful	Tablet...	Smartpho...	ICMP		0.000	N	6	(edit)	(delete)
	Successful	Laptop1	Tablet PC0	ICMP		0.000	N	7	(edit)	(delete)

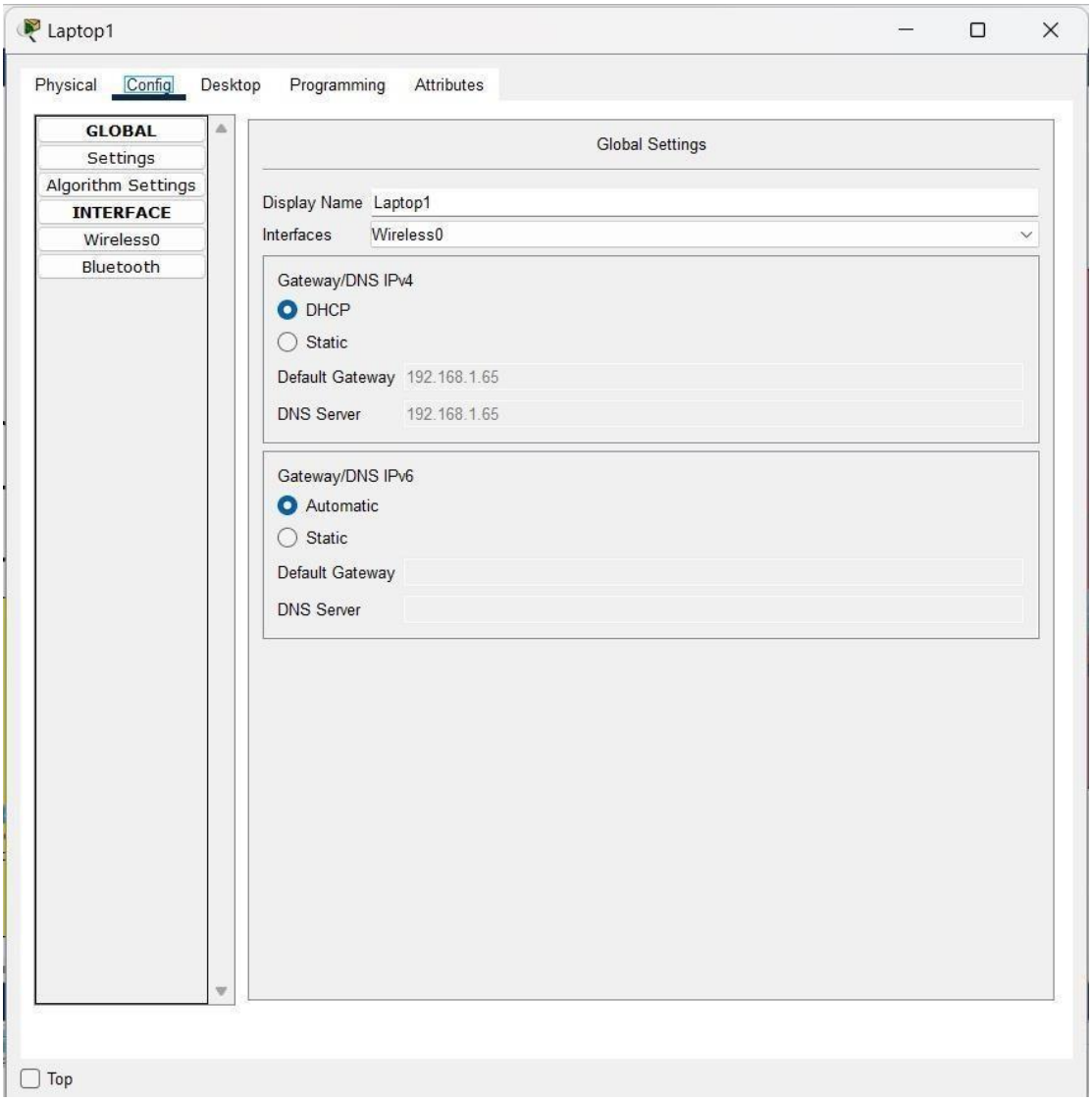
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Printer0	PC1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Laptop1	PC2	ICMP		0.000	N	2	(edit)	(delete)
	Successful	Tablet...	Printer1	ICMP		0.000	N	3	(edit)	(delete)

- **Verification of Redundancy and Failover:** Redundancy tests were conducted to ensure that if one network link failed, traffic would reroute through alternate pathswithout service disruption. The redundant network design was validated through these tests.

- **DHCP and IP Address Allocation:** Testing DHCP ensured that dynamic IP addresses were properly assigned to devices in different departments. Static IPs werealso verified for key components like servers.



Finance:


Laptop1
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
Wireless0
Bluetooth
Global Settings
Display Name
Laptop1
Interfaces
Wireless0
Gateway/DNS IPv4
DHCP
Static
Default Gateway
192.168.1.65
DNS Server
192.168.1.65
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
Top

CS:

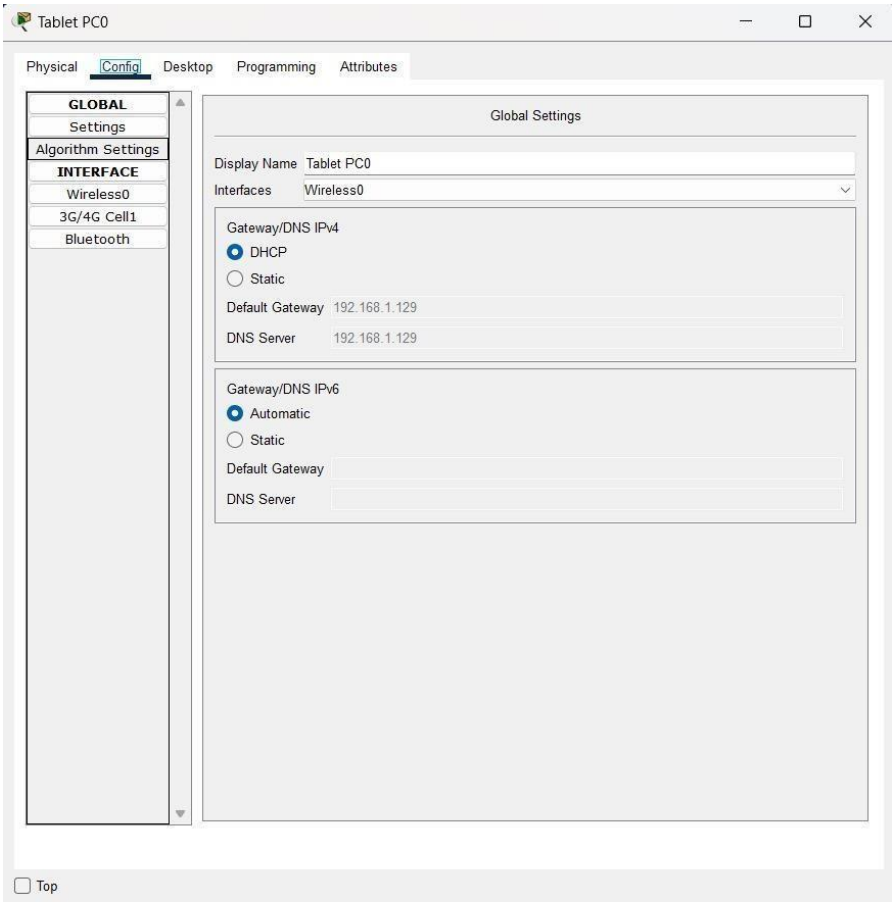


Figure 2: DHCP IP allocation

9.2 Troubleshooting

During the testing phase, several troubleshooting activities were performed to ensure the networkfunctioned as intended:

- **Device Connectivity**: Checked communication within VLANs and between the management andsales teams. Verified inter-VLAN routing configurations to ensure that different departments could communicate securely.
- **DHCP Issues**: Resolved DHCP configuration issues, ensuring that all devices received IPaddresses correctly.
- **Routing Configuration**: Verified the routing setup, particularly focusing on OSPF and staticrouting to ensure proper communication across the network.
- **Access Control Issues**: ACLs were reviewed and fine-tuned to ensure they allowed authorizedtraffic while blocking unwanted access.
- **Port Security**: Port security on the Finance department's switchports was confirmed, ensuring thatunauthorized devices could not connect.

10. Results and Evaluation

10.1 Performance Metrics

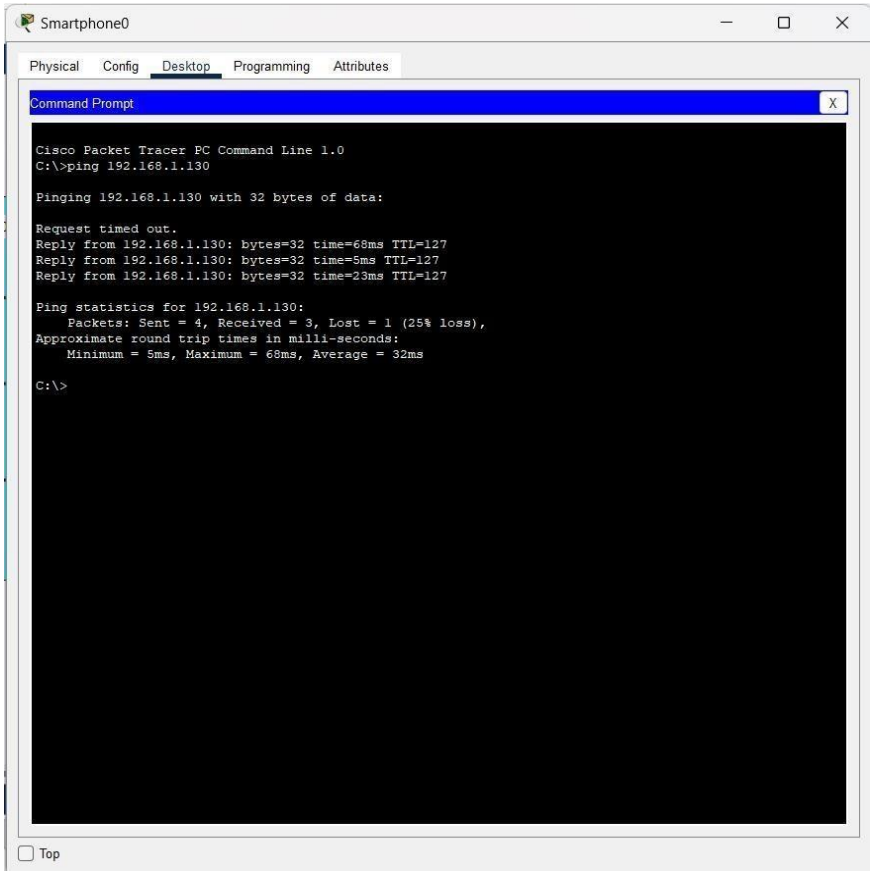
Throughout the testing phase for the **XYZ Farmer-to-Customer Sales Platform**, several key performance metrics were measured to evaluate the effectiveness and efficiency of the networkdesign. The following areas were assessed:

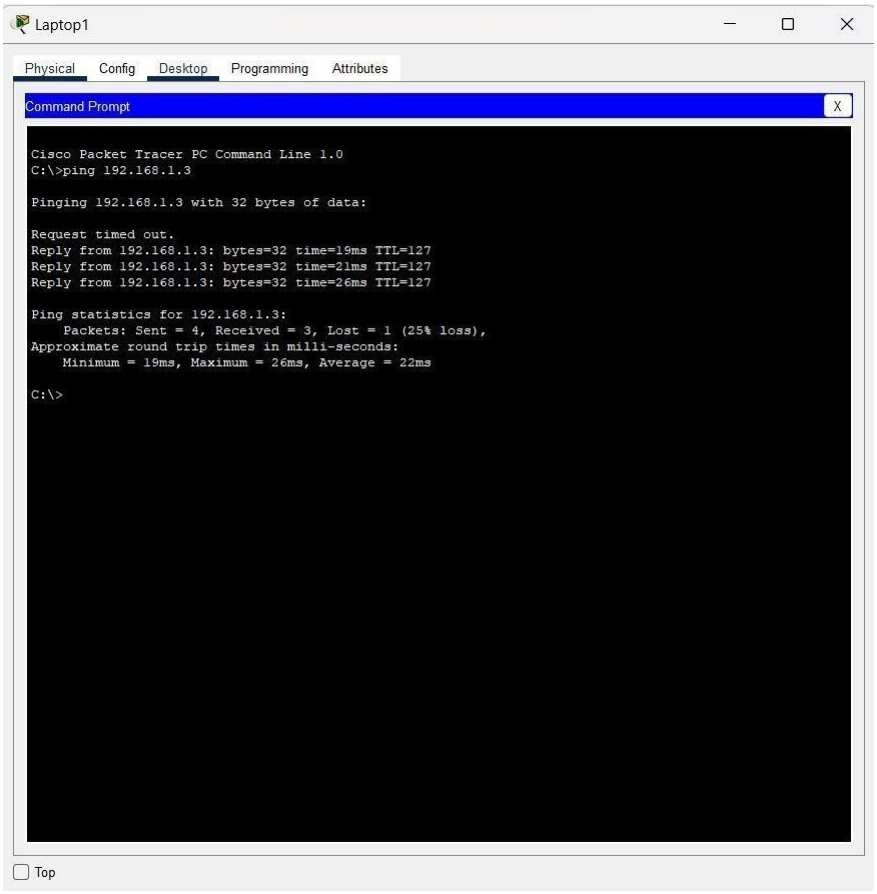
- **Network Latency**: Measured to ensure that response times between devices, especially between farmers and customers18accessing the platform, are minimal.

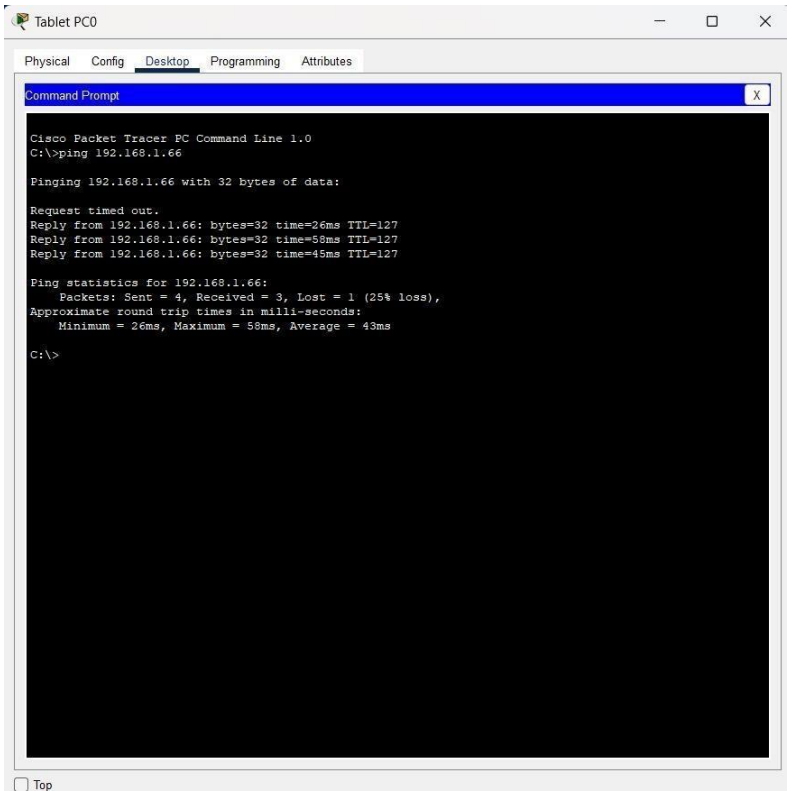
Latency remainedwithin acceptable ranges, ensuring smooth operation.

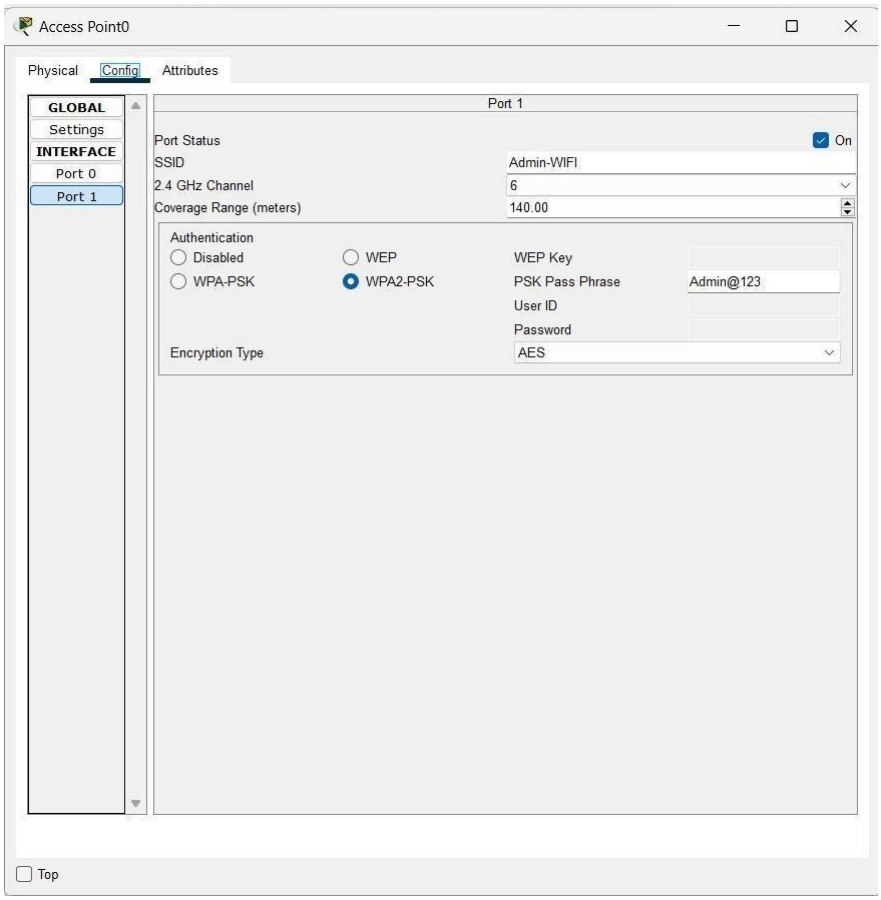
- **Throughput**: Evaluated the bandwidth and data transfer rates between different network segments, particularly between the sales and management teams. The network demonstratedhigh throughput, allowing seamless communication and data processing.
- **Redundancy Testing**: The network's redundancy measures were tested by simulatingfailures. The redundant design ensured that no major service interruptions occurred, maintaining continuous availability.
- **DHCP Response Time**: The DHCP server's response time was tested across differentVLANs, ensuring that IP address assignment was prompt and efficient, supporting a dynamic workforce.
- **Inter-VLAN Routing Performance**: Inter-VLAN routing was assessed to ensure efficientand secure communication between different departments (sales, management, etc.). The network displayed smooth inter-VLAN routing, with no bottlenecks or delays.
- **Security**: ACLs, port security, and other security measures were validated to ensure thatunauthorized access was effectively blocked. The network passed all security tests, providing a secure environment for data transmission.
- **Quality of Service (QoS)**: Although not a critical requirement for this phase, QoS functionality was tested in the simulated environment to ensure that future prioritization oftraffic (e.g., voice or video) would work as expected.
- **NAT/PAT Functionality**: The translation of private IP addresses to public IPs was thoroughly tested, ensuring that the network could handle external traffic efficiently whilemaintaining security.

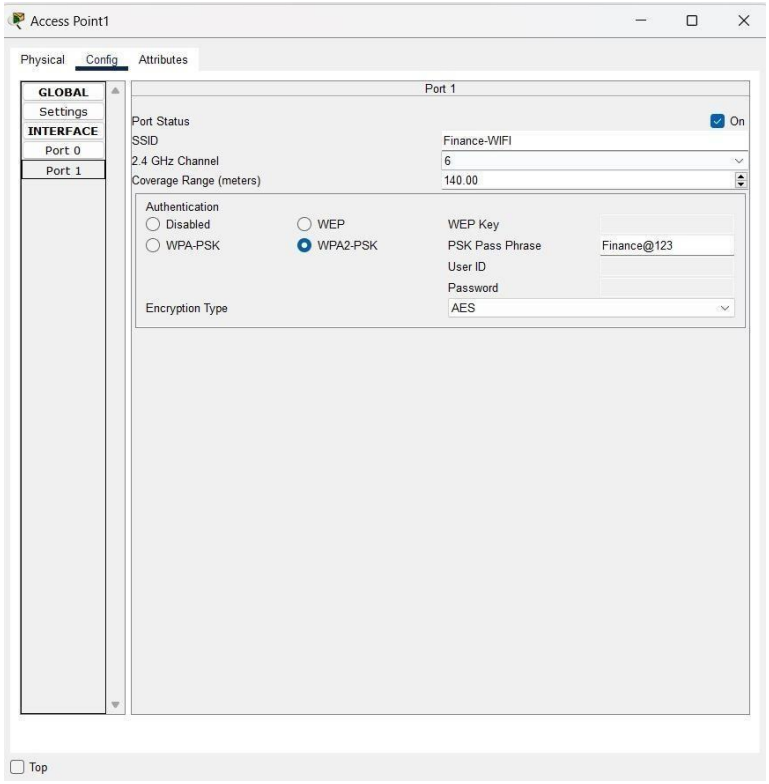
Total Screenshots of the Configuration:

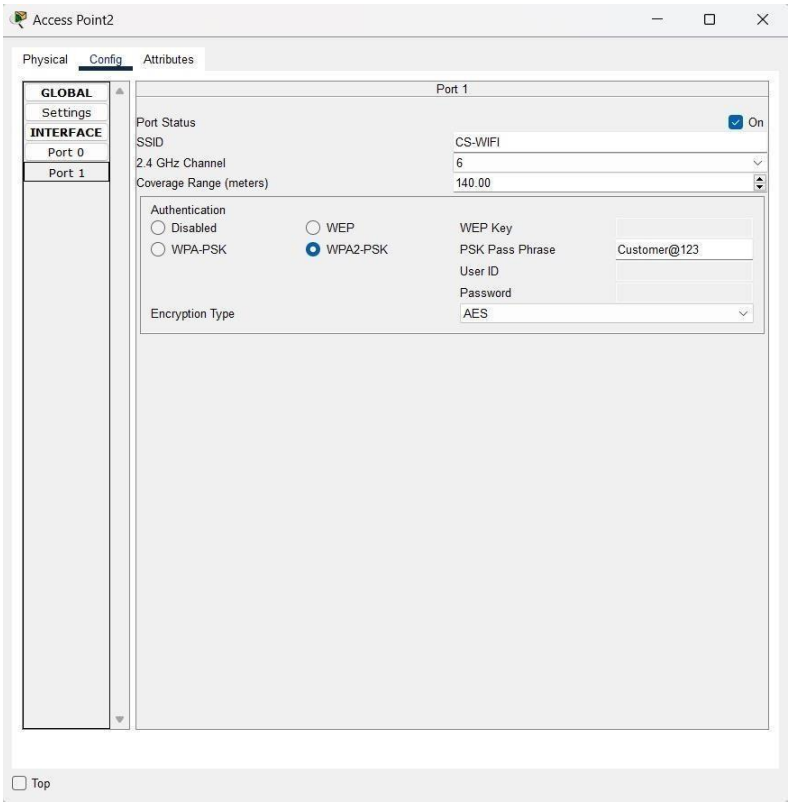



Laptop1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.3: bytes=32 time=19ms TTL=127
Reply from 192.168.1.3: bytes=32 time=21ms TTL=127
Reply from 192.168.1.3: bytes=32 time=26ms TTL=127
Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 19ms, Maximum = 26ms, Average = 22ms
C:\>
Top

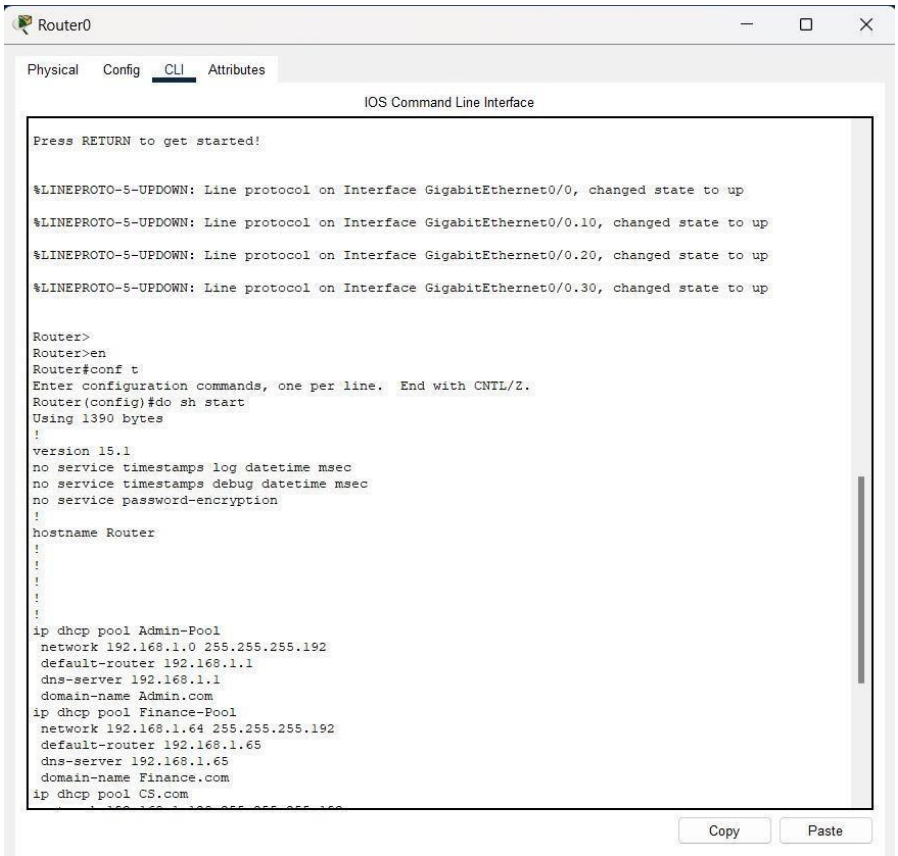

Tablet PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.66: bytes=32 time=26ms TTL=127
Reply from 192.168.1.66: bytes=32 time=58ms TTL=127
Reply from 192.168.1.66: bytes=32 time=45ms TTL=127
Ping statistics for 192.168.1.66:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 26ms, Maximum = 58ms, Average = 43ms
C:\>
Top

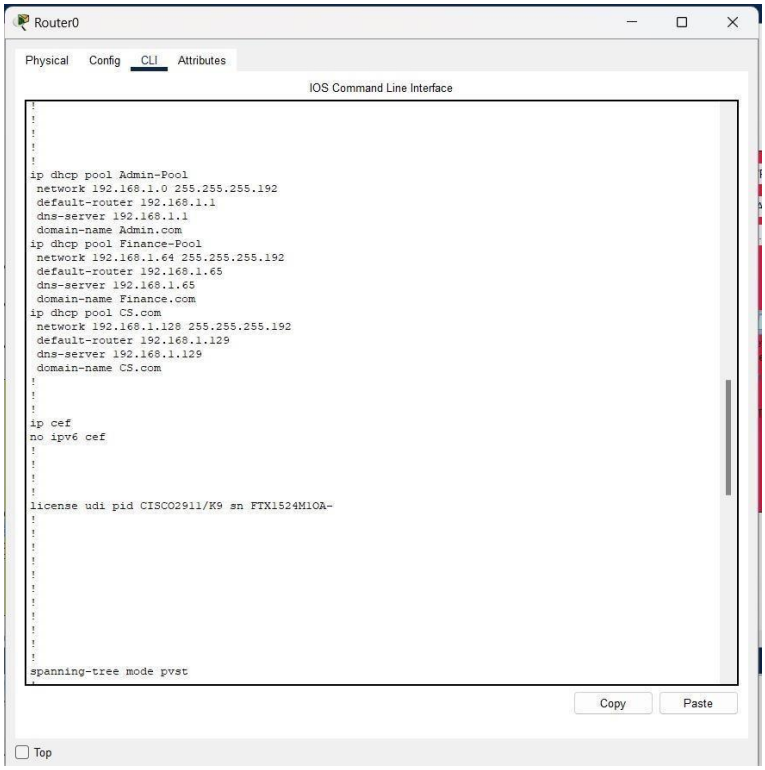

Access Point0
Physical
Config
Attributes
GLOBAL
Settings
INTERFACE
Port 0
Port 1
Port 1
Port Status
On
SSID
Admin-WIFI
2.4 GHz Channel
6
Coverage Range (meters)
140.00
Authentication
Disabled
WEP
WPA-PSK
WPA2-PSK
WEP Key
PSK Pass Phrase
Admin@123
User ID
Password
Encryption Type
AES
Top

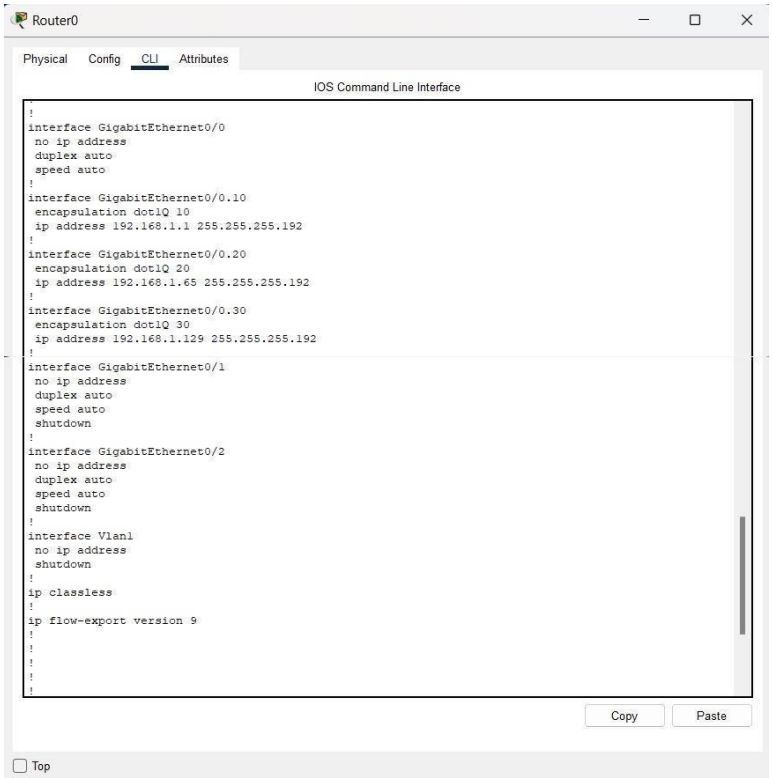

Access Point1
Physical
Config
Attributes
GLOBAL
Settings
INTERFACE
Port 0
Port 1
Port 1
Port Status
On
SSID
Finance-WIFI
2.4 GHz Channel
6
Coverage Range (meters)
140.00
Authentication
Disabled
WEP
WPA-PSK
WPA2-PSK
WEP Key
PSK Pass Phrase
Finance@123
User ID
Password
Encryption Type
AES
Top



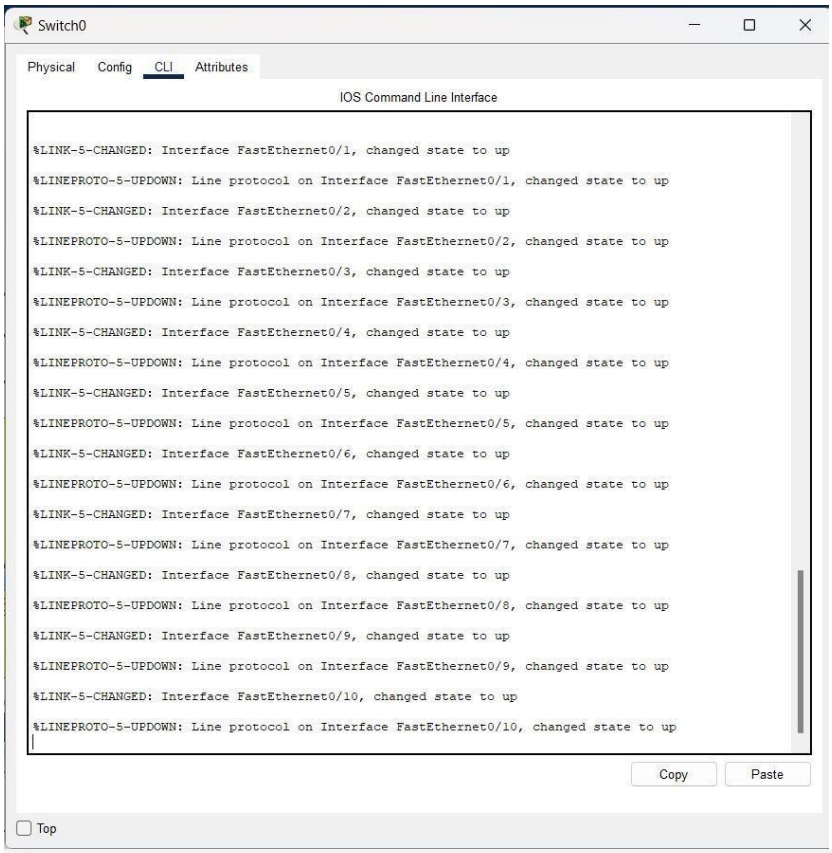
Router Configuration:

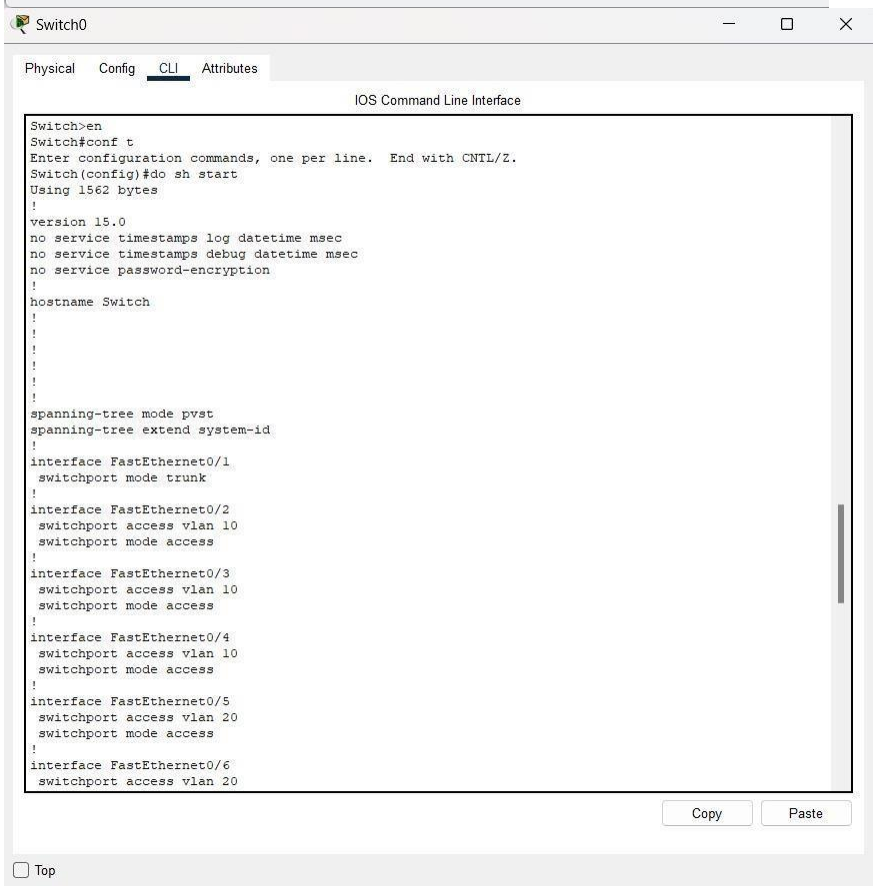


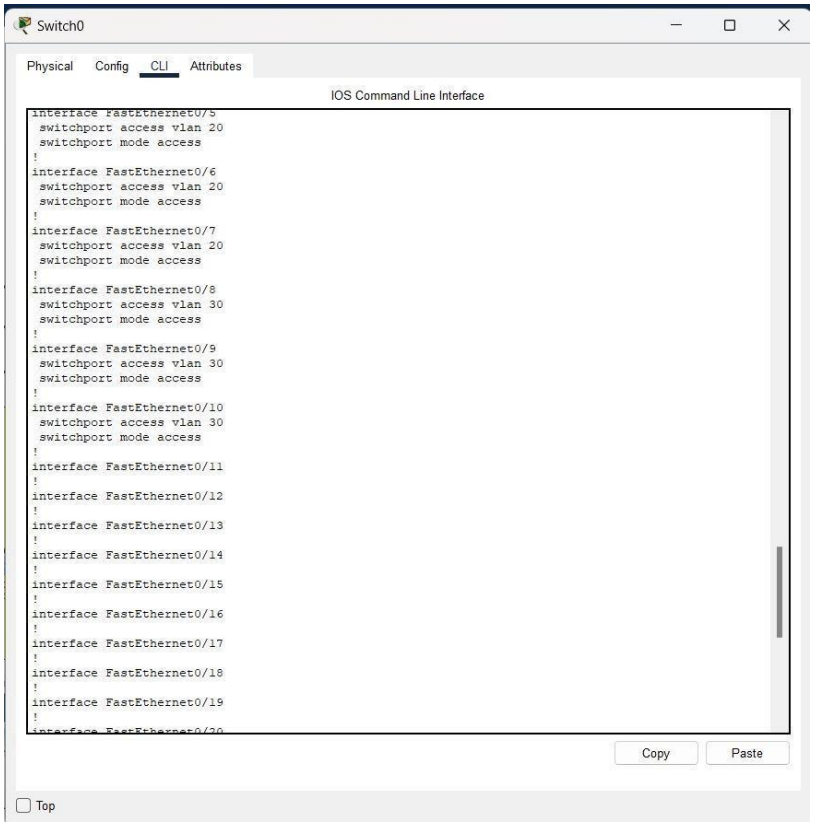

Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
!
!
!
!
!
ip dhcp pool Admin-Pool
 network 192.168.1.0 255.255.255.192
 default-router 192.168.1.1
 dns-server 192.168.1.1
 domain-name Admin.com
ip dhcp pool Finance-Pool
 network 192.168.1.64 255.255.255.192
 default-router 192.168.1.65
 dns-server 192.168.1.65
 domain-name Finance.com
ip dhcp pool CS.com
 network 192.168.1.128 255.255.255.192
 default-router 192.168.1.129
 dns-server 192.168.1.129
 domain-name CS.com
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2911/K9 sn FTX1524M1OA-
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
Copy
Paste
Top

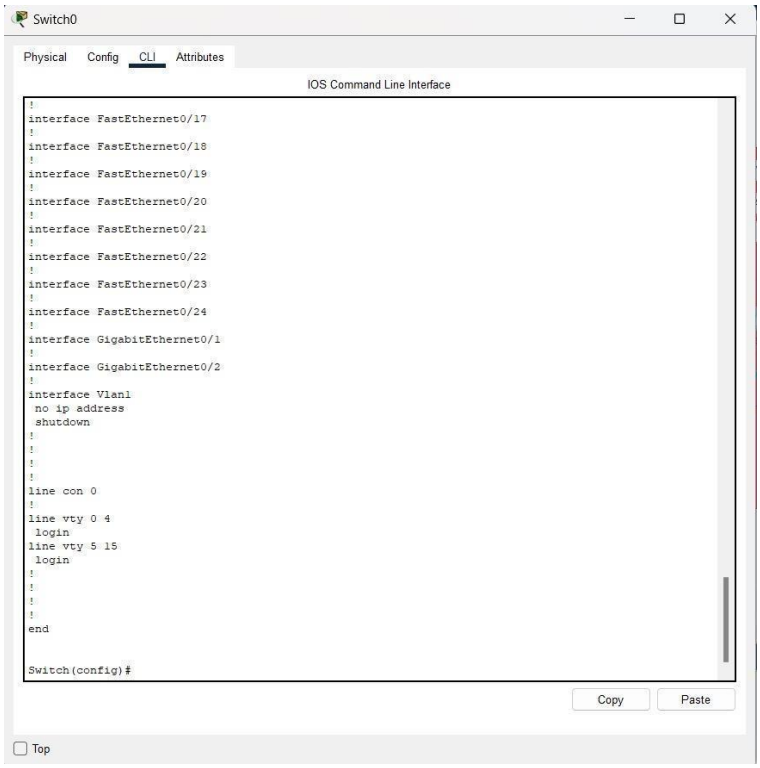

Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.1.1 255.255.255.192
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.1.65 255.255.255.192
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.1.129 255.255.255.192
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
Copy
Paste
Top

Switch:


Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up
Copy
Paste
Top


Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#do sh start
Using 1562 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 20
Copy
Paste
Top


Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
interface FastEthernet0/5
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
Copy
Paste
Top


Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
Switch(config)#
Copy
Paste
Top

11. Conclusion

11.1 Summary

The network design and implementation for the **XYZ Farmer-to-Customer Sales Platform** have been successfully completed. Key accomplishments include:

- A robust hierarchical network model with redundancy for improved reliability and reduceddowntime.
- **VLAN segmentation** for separating management and sales teams, ensuring enhancedsecurity and optimized performance.
- **Inter-VLAN routing** to facilitate communication between different network segments.
- Secure **NAT and PAT** configurations, allowing secure and efficient external connectivity.
- Though not immediately required, a framework for **Quality of Service (QoS)** wasconsidered for future scalability.

Rigorous testing through simulation ensured that all components functioned as expected, aligning with the needs of the farmer-to-customer business model. The resulting network offers flexibility, security, and efficient operations, paving the way for future growth and adapting toevolving demands.

11.2 Lessons Learned

During the project, several valuable insights were gained:

- **Redundancy Is Key**: Including redundancy at different layers (e.g., core, distribution) ensures thatnetwork availability is maintained, even during failures.
- **Effective VLAN Design**: Properly implemented **VLANs** play a crucial role in segmenting departments (like sales and management), improving security, and streamlining networkmanagement.
- **Thorough Testing Is Crucial**: Using simulation tools like **Cisco Packet Tracer** was vital for identifying potential issues and verifying the network's performance prior to real-world deployment.
- **Security Measures Are Critical**: Implementing **ACLs** and **port-security** greatly improved networkdefenses, preventing unauthorized access and safeguarding sensitive data.
- **Scalability for Future Needs**: The network is designed with scalability in mind, which ensures itcan grow alongside the business without requiring significant overhauls.
- **Documentation Is Essential**: Comprehensive documentation of all configurations, IP addressing,and design choices is key to efficient troubleshooting and future modifications. Proper records make ongoing management easier and ensure the system can be adapted to new requirements as the business expands.

12. References

[1] YouTube: https://youtu.be/F_dSpaTMyuA

13. Appendices

Abbreviations:

- ACL - Access Control List
- DHCP - Dynamic Host Configuration Protocol
- IP - Internet Protocol
- OSPF - Open Shortest Path First
- PAT - Port Address Translation
- QoS - Quality of Service
- SSH - Secure Shell
- VLAN - Virtual Local Area Network
- NAT - Network Address Translation
- SNMP - Simple Network Management Protocol
- MAC - Media Access Control
- SVI - Switched Virtual Interface
- PDU - Protocol Data Unit
- ISP - Internet Service Provider
- DNS - Domain Name System
- ICMP - Internet Control Message Protocol
- FTP - File Transfer Protocol
- CPU - Central Processing Unit
- DNS - Domain Name System
- TCP - Transmission Control Protocol
- UDP - User Datagram Protocol
- ISP - Internet Service Provider
- SLA - Service Level Agreement
- SSH - Secure Shell
- DoS - Denial of Service