Topic: Network Security Implementation for Secure Shop Ltd.

08/04/2025

Middlesex University

Department of Computer Networks and Security

Course Name: Network Security

Course Code: CST3577

Module leader: Dr. Aboubaker Lasebae

Student name : Fisha Goitem

Student ID: M00862650

Network Security Implementation for Secure Shop Ltd.

Introduction

Secure Shop Ltd is a growing eCommerce company that requires a robust, scalable, and secure network infrastructure to support its operations. This report outlines the design, configuration, and security implementation of the network, ensuring data confidentiality, integrity, and availability while considering both technical and physical security.

1. Network Design & Topology

Overview

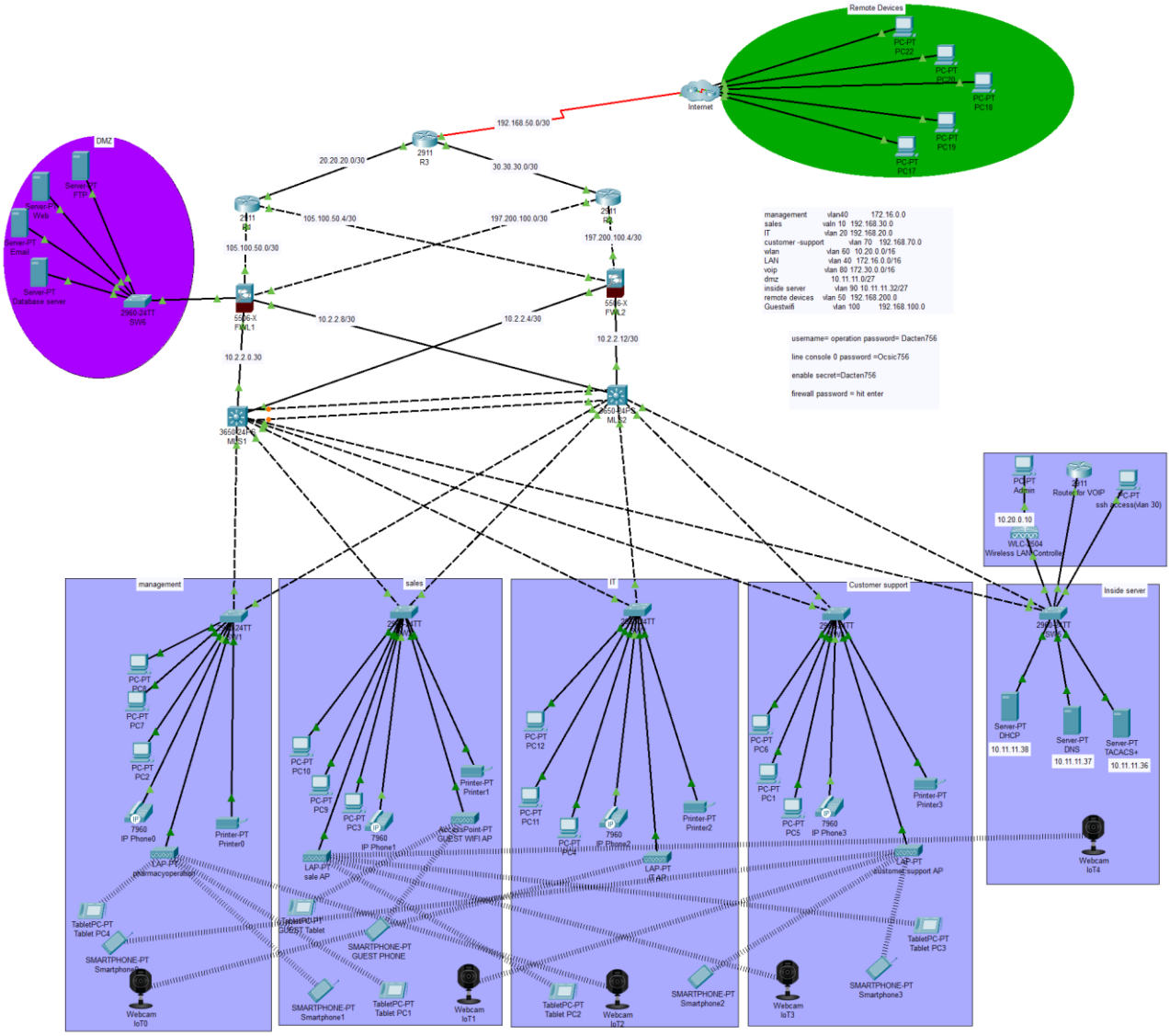
As the Network Security Engineer for Secure Shop Ltd, I designed the network topology to ensure robust security, scalability, and efficiency, which are crucial for our growing eCommerce company. The network is designed to support at least 50 employees onsite and 20 remote users, accommodating the needs of our Management, Sales, IT, and Customer Support departments.

- Segmentation with VLANs: I segmented the network into VLANs for each department to enhance security and efficiency. This isolation reduces the risk of data breaches and minimizes broadcast traffic, improving network performance.
- IP Addressing and Redundancy: I used appropriate IP addressing, including private and public IPs with subnetting, to ensure efficient network communication. To implement redundancy, I configured backup links and secondary routers, ensuring the network remains operational even if a primary link or device fails. This redundancy is critical for maintaining continuous business operations and minimizing downtime.
- Hybrid Routing Strategy: By using both static and dynamic routing (e.g., OSPF), I ensured optimal path selection and adaptability to network changes. This flexibility allows for efficient data routing and quick recovery from network failures.
- Secure Remote Access: I configured IPSec VPNs to provide secure access for remote users, protecting data in transit from interception. This is vital for supporting our remote workforce while maintaining data confidentiality and integrity.
- DMZ for Servers: I placed web and database servers in a DMZ to add an extra layer of security by separating them from the internal network. This setup protects internal resources from external threats while allowing necessary access to public-facing services.

- Comprehensive Security Measures: I configured firewalls and ACLs to filter and restrict traffic, and deployed IDS to monitor for threats, providing a multi-layered security approach. AAA protocols enforce strict authentication and access control policies, ensuring only authorized access.
- Physical Security: I installed CCTV cameras in each of the four departments and the server room to enhance physical security. This deters unauthorized access and provides surveillance for incident response, ensuring critical areas are monitored effectively.

Overall, I designed this topology to provide a secure, scalable, and efficient network infrastructure that supports both current operations and future growth, ensuring the confidentiality, integrity, and availability of our data. Each department has its own VLAN, and there are separate VLANs for phones, staff WiFi, guest WiFi, remote workers, and internal servers. This segmentation enhances security and performance by isolating traffic and ensuring that each segment of the network operates efficiently and securely.

Network Design & Topology for secure shop

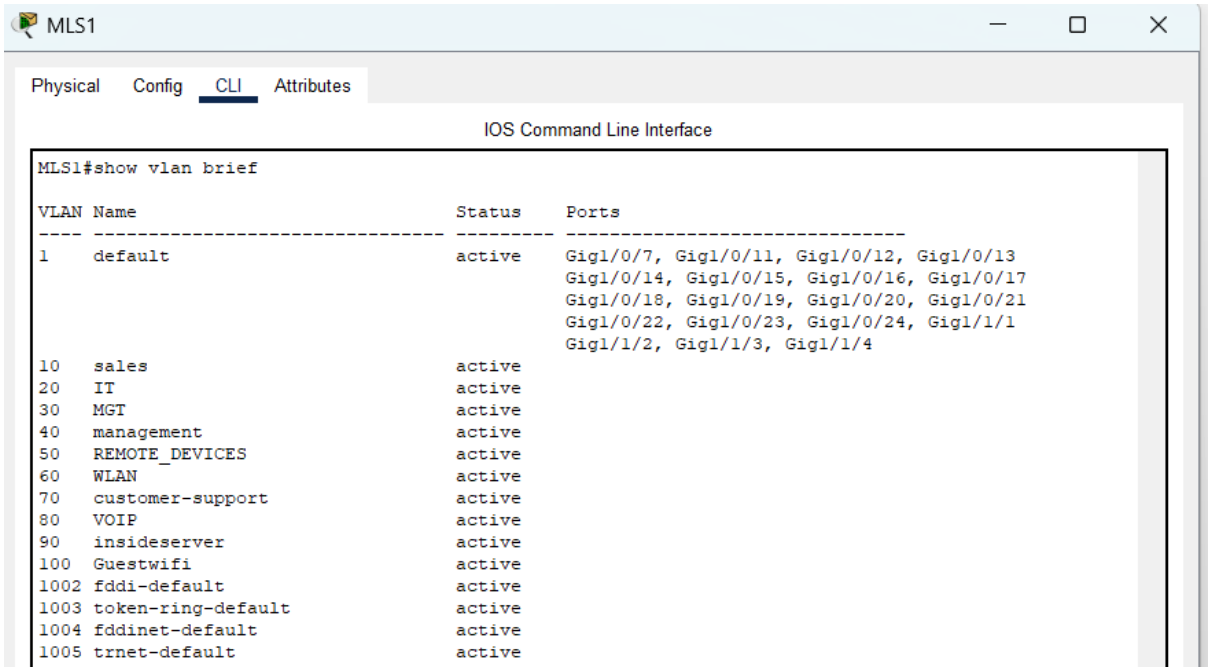


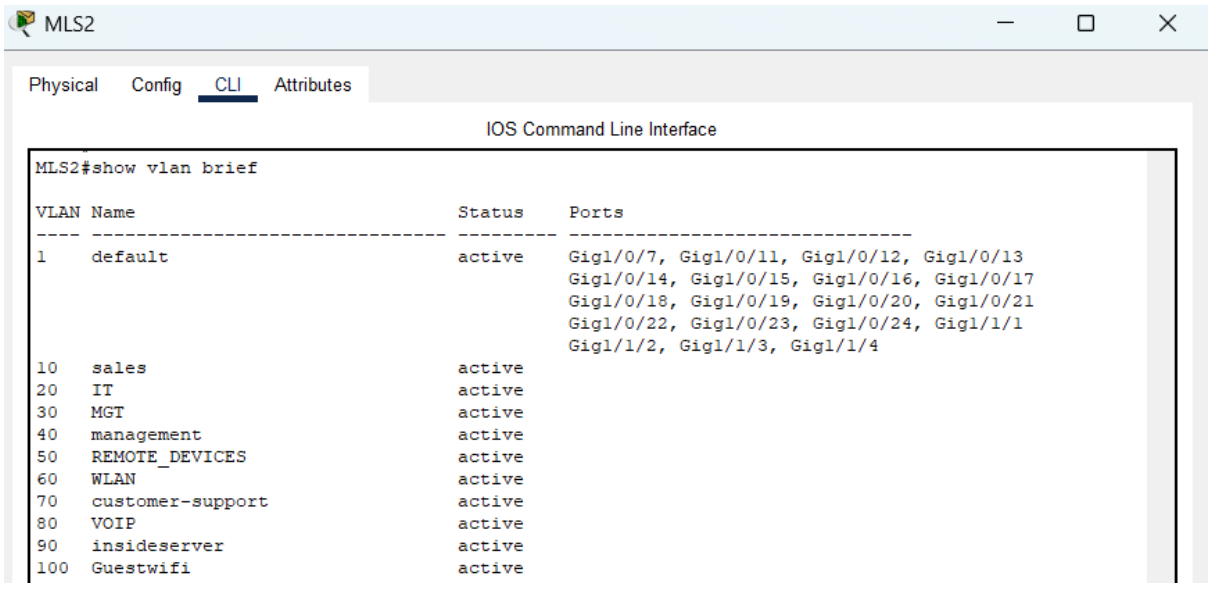
VLAN Segmentation and Private/Public, Subnetting, Explanation

In the network design for Secure Shop Ltd, I implemented VLAN segmentation to enhance both security and efficiency. Each department, including Sales, IT, Management, and Customer

Support, has its own VLAN, ensuring that traffic is isolated and reducing the risk of unauthorized access.

Additionally, separate VLANs are configured for phones, staff WiFi, guest WiFi, remote workers, and internal servers, further enhancing security by segregating different types of traffic. This setup not only improves network performance by minimizing broadcast domains but also simplifies management and troubleshooting.





For IP addressing, I used a combination of public and private IPs. Public IP ranges such as 105.100.50.0/30, 197.200.100.0/30, 197.200.100.4/30, 20.20.20.0/30, and 30.30.30.0/30 are utilized for external communications. Private IPs, as seen in the configuration, include ranges like 192.168.30.2 for VLAN 10 (Sales), 192.168.20.2 for VLAN 20 (IT), and 10.11.11.34 for VLAN 90 (Inside Server). This strategic segmentation and IP addressing scheme are crucial for maintaining a secure and efficient network infrastructure

MLS1

Physical Config CLI Attributes

IOS Command Line Interface

```
MLS1#
MLS1#show ip interface brief | include up
Port-channel1          unassigned      YES unset  up                    up
GigabitEthernet1/0/1   10.2.2.1        YES manual up                    up
GigabitEthernet1/0/2   10.2.2.5        YES manual up                    up
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  up                    up
GigabitEthernet1/0/5   unassigned      YES unset  up                    up
GigabitEthernet1/0/6   unassigned      YES unset  up                    up
GigabitEthernet1/0/8   unassigned      YES unset  up                    up
GigabitEthernet1/0/9   unassigned      YES unset  up                    up
GigabitEthernet1/0/10  unassigned      YES unset  up                    up
Vlan1                  unassigned      YES unset  up                    up
Vlan10                 192.168.30.2    YES manual up                    up
Vlan20                 192.168.20.2    YES manual up                    up
Vlan30                 192.168.10.3    YES manual up                    up
Vlan40                 172.16.0.3      YES manual up                    up
Vlan50                 192.168.50.2    YES manual up                    up
Vlan60                 10.20.0.2       YES manual up                    up
Vlan70                 192.168.70.2    YES manual up                    up
Vlan90                 10.11.11.34     YES manual up                    up
Vlan100                192.168.100.2   YES manual up                    up
MLS1#
```

MLS2

Physical Config CLI Attributes

IOS Command Line Interface

```
MLS2#show ip interface brief | include up
Port-channel1          unassigned      YES unset  up                    up
GigabitEthernet1/0/1   10.2.2.9        YES manual up                    up
GigabitEthernet1/0/2   10.2.2.13       YES manual up                    up
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  up                    up
GigabitEthernet1/0/5   unassigned      YES unset  up                    up
GigabitEthernet1/0/6   unassigned      YES unset  up                    up
GigabitEthernet1/0/8   unassigned      YES unset  up                    up
GigabitEthernet1/0/9   unassigned      YES unset  up                    up
GigabitEthernet1/0/10  unassigned      YES unset  up                    up
Vlan1                  unassigned      YES unset  up                    up
Vlan10                 192.168.30.2    YES manual up                    up
Vlan20                 192.168.20.2    YES manual up                    up
Vlan30                 192.168.10.2    YES manual up                    up
Vlan40                 172.16.0.2      YES manual up                    up
Vlan50                 192.168.50.2    YES manual up                    up
Vlan60                 10.20.0.3       YES manual up                    up
Vlan70                 192.168.70.2    YES manual up                    up
Vlan90                 10.11.11.35     YES manual up                    up
Vlan100                192.168.100.2   YES manual up                    up
MLS2#
```

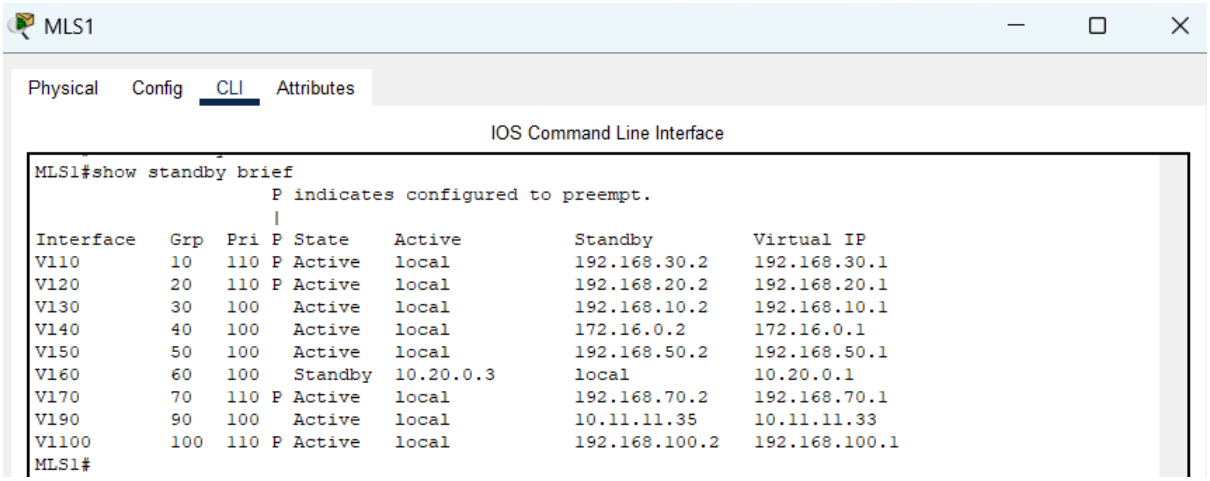
```
R1`#show ip interface brief | include up
GigabitEthernet0/0     20.20.20.1      YES manual up                    up
GigabitEthernet0/1     105.100.50.1    YES manual up                    up
GigabitEthernet0/2     105.100.50.5    YES manual up                    up
```

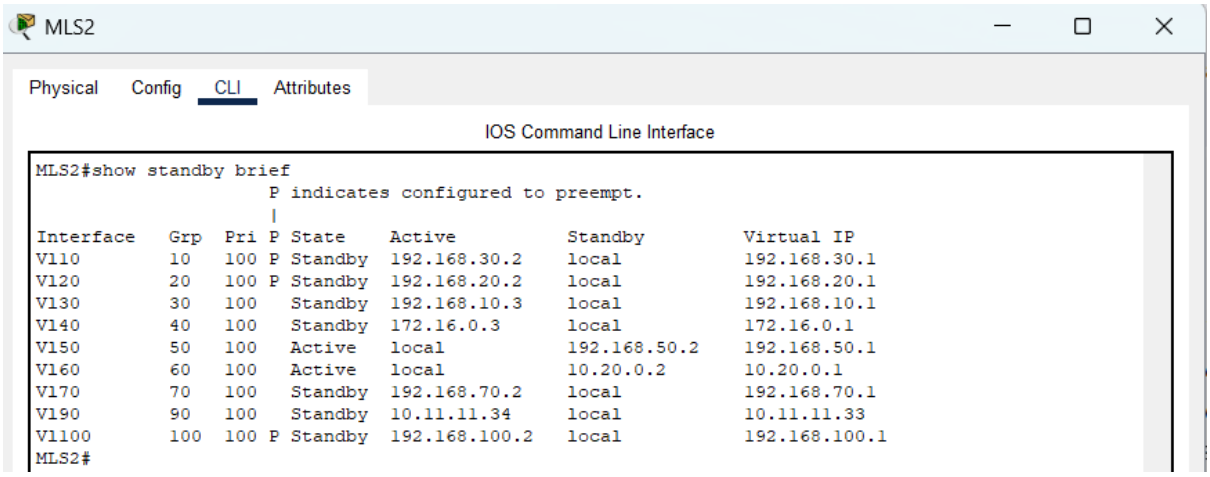
```
R2#show ip interface brief | include up
GigabitEthernet0/0     30.30.30.1      YES manual up                    up
GigabitEthernet0/1     197.200.100.1   YES manual up                    up
GigabitEthernet0/2     197.200.100.5   YES manual up                    up
R2#
```

Network Redundancy

Implementing redundancy in the network design for Secure Shop Ltd is crucial for ensuring high availability and minimizing downtime. The screenshots show the use of Hot Standby Router Protocol (HSRP), which provides redundancy for IP networks by allowing multiple routers to appear as a single virtual router. This setup ensures that if a primary router fails, a standby router can seamlessly take over, maintaining network connectivity without interruption.

By configuring HSRP across various VLANs, such as VLAN 10 (Sales) and VLAN 20 (IT), I ensure that critical network services remain available even in the event of hardware failure. This redundancy is vital for maintaining continuous business operations, especially for an eCommerce company where downtime can lead to significant revenue loss and customer dissatisfaction.

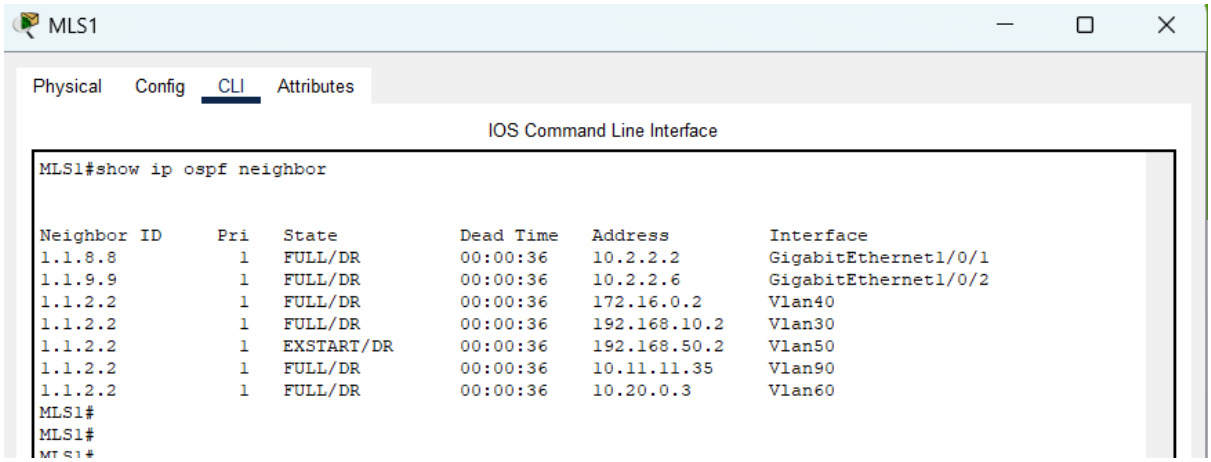


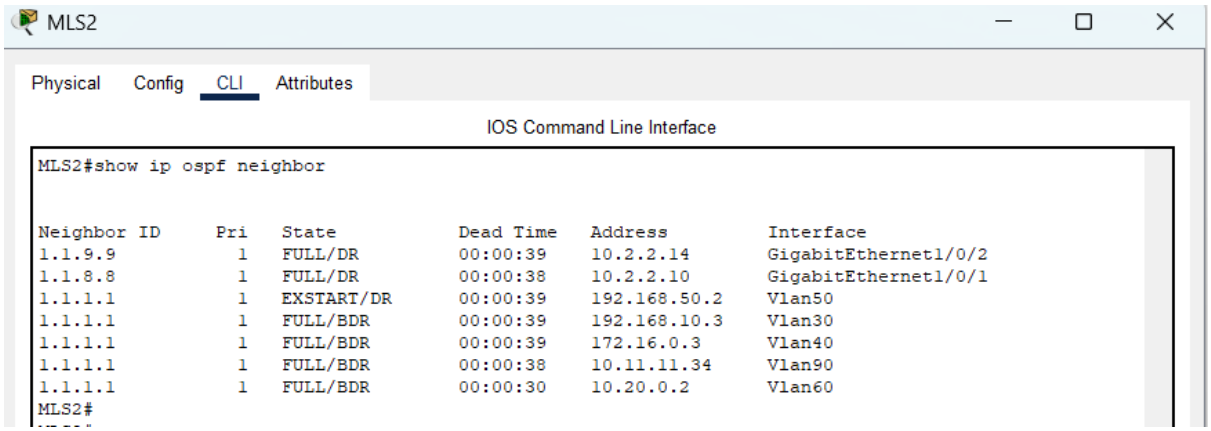


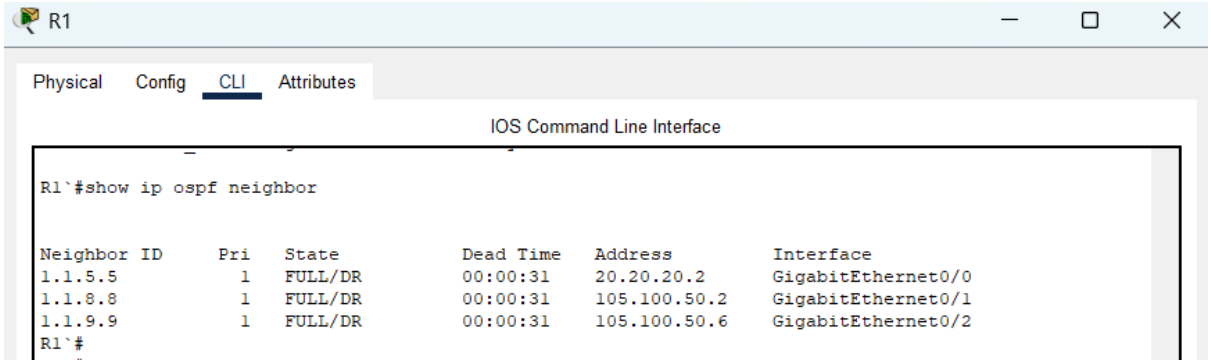
2. Network Configuration

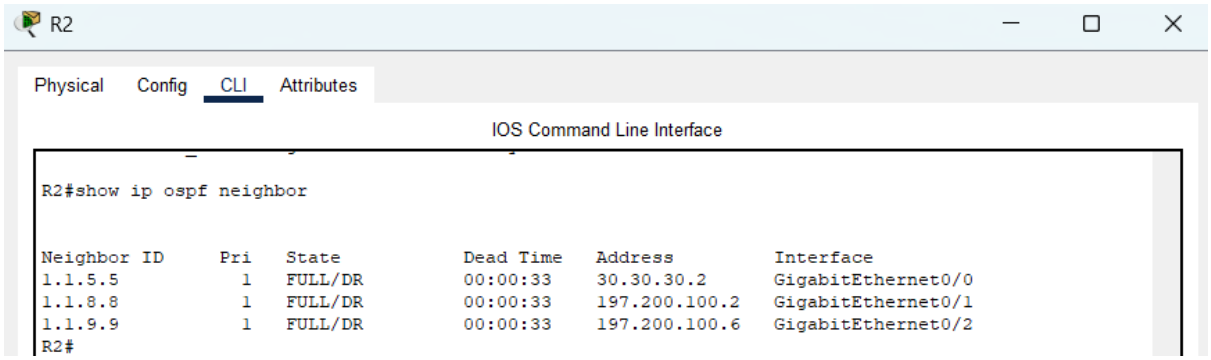
Routing,(OSPF): In the network design for Secure Shop Ltd, I implemented OSPF (Open Shortest Path First) as the dynamic routing protocol, as illustrated in the screenshots. OSPF is ideal for our network because it efficiently manages routing information and adapts quickly to network changes, ensuring optimal path selection. The use of OSPF allows for scalability, which is crucial as our network grows.

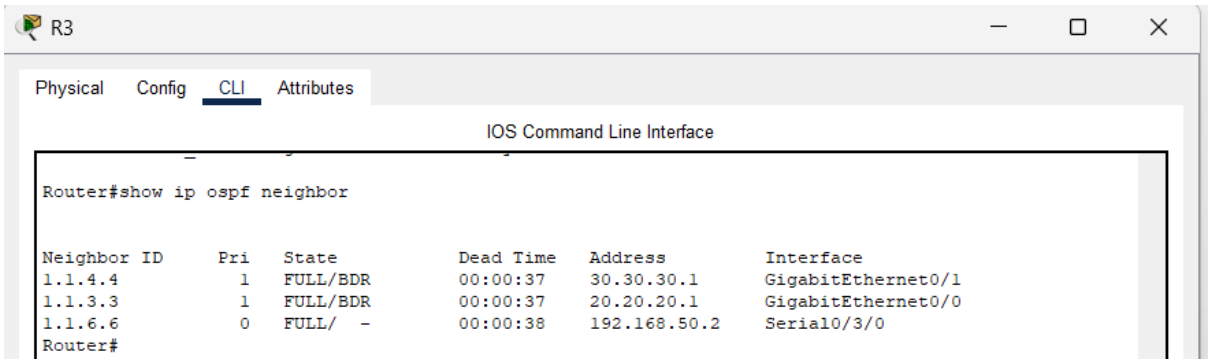
It supports multiple routers and complex topologies, providing fast convergence and reducing downtime. The screenshots show OSPF neighbours in a full state, indicating stable and reliable connections between routers, such as those on interfaces like GigabitEthernet1/0/1 and VLANs 30, 40, and 50. This setup ensures that data is routed efficiently across the network, maintaining high performance and reliability, which are essential for our eCommerce operations.











The OSPF routing configuration for Secure Shop Ltd, as shown in the screenshot, demonstrates a well-structured and efficient routing strategy. OSPF dynamically manages routing information, allowing for quick adaptation to network changes. The routing table includes various subnets, such as 10.2.2.8 and 10.11.11.0, with multiple paths available through interfaces like GigabitEthernet1/0/1 and VLANs 30, 40, and 60.

This setup ensures optimal path selection and redundancy, enhancing network reliability. The use of OSPF allows for scalability, supporting complex topologies and multiple routers, which is crucial for maintaining high performance and minimizing downtime in our eCommerce operations. The configuration also includes public IP subnets like 20.20.20.0/30 and 197.200.100.0/30, facilitating efficient external communications.

MLS1

Physical Config CLI Attributes

IOS Command Line Interface

```
MLS1#show ip route ospf
     10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
O       10.2.2.8 [110/2] via 10.2.2.2, 00:54:07, GigabitEthernet1/0/1
                 [110/2] via 192.168.10.2, 00:54:07, Vlan30
                 [110/2] via 172.16.0.2, 00:54:07, Vlan40
                 [110/2] via 10.20.0.3, 00:54:07, Vlan60
                 [110/2] via 10.11.11.35, 00:54:07, Vlan90
O       10.2.2.12 [110/2] via 10.2.2.6, 00:54:07, GigabitEthernet1/0/2
                  [110/2] via 192.168.10.2, 00:54:07, Vlan30
                  [110/2] via 172.16.0.2, 00:54:07, Vlan40
                  [110/2] via 10.20.0.3, 00:54:07, Vlan60
                  [110/2] via 10.11.11.35, 00:54:07, Vlan90
O       10.11.11.0 [110/2] via 10.2.2.2, 00:54:07, GigabitEthernet1/0/1
     20.0.0.0/30 is subnetted, 1 subnets
O       20.20.20.0 [110/3] via 10.2.2.2, 00:54:07, GigabitEthernet1/0/1
                   [110/3] via 10.2.2.6, 00:54:07, GigabitEthernet1/0/2
     30.0.0.0/30 is subnetted, 1 subnets
O       30.30.30.0 [110/3] via 10.2.2.2, 00:54:07, GigabitEthernet1/0/1
                   [110/3] via 10.2.2.6, 00:54:07, GigabitEthernet1/0/2
     105.0.0.0/30 is subnetted, 2 subnets
O       105.100.50.0 [110/2] via 10.2.2.2, 00:54:07, GigabitEthernet1/0/1
O       105.100.50.4 [110/2] via 10.2.2.6, 00:54:07, GigabitEthernet1/0/2
O    192.168.200.0 [110/68] via 10.2.2.2, 00:54:07, GigabitEthernet1/0/1
                   [110/68] via 10.2.2.6, 00:54:07, GigabitEthernet1/0/2
     197.200.100.0/30 is subnetted, 2 subnets
O       197.200.100.0 [110/2] via 10.2.2.2, 00:54:07, GigabitEthernet1/0/1
O       197.200.100.4 [110/2] via 10.2.2.6, 00:54:07, GigabitEthernet1/0/2
```

MLS2

Physical Config CLI Attributes

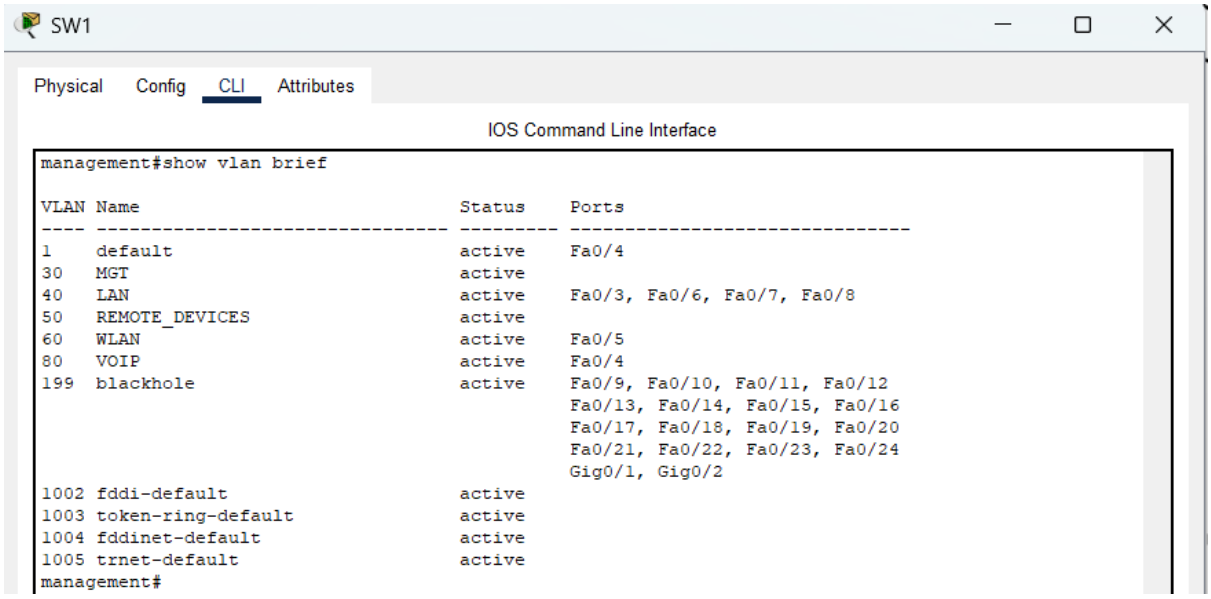
IOS Command Line Interface

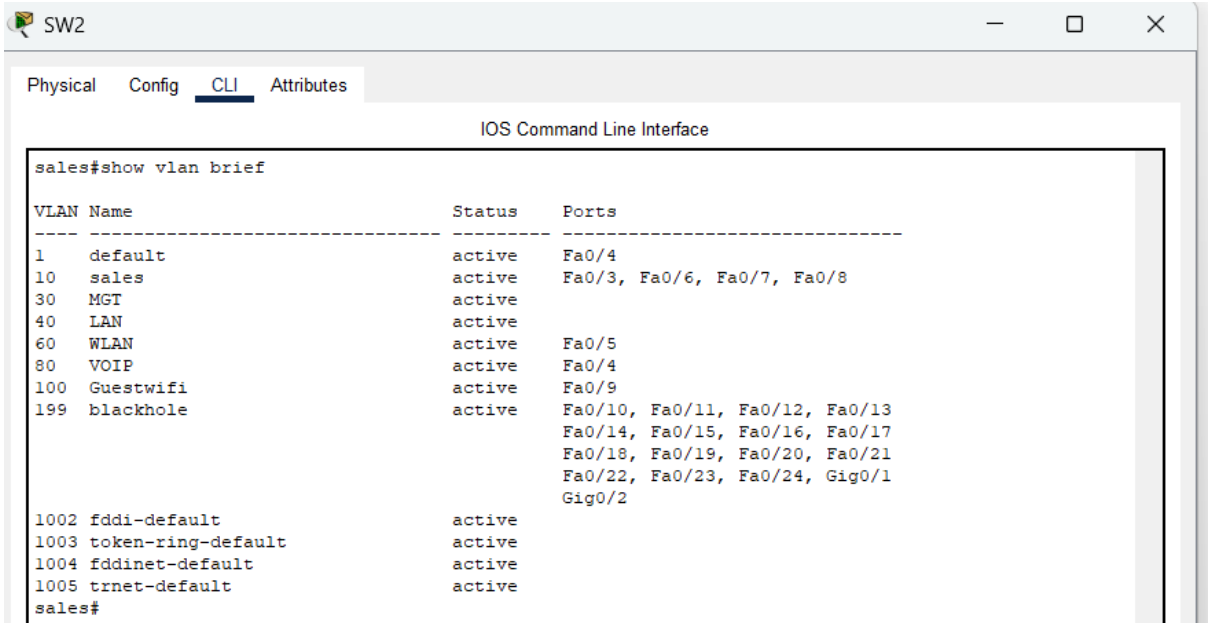
```
MLS2#show ip route ospf
     10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
O       10.2.2.0 [110/2] via 10.2.2.10, 00:54:54, GigabitEthernet1/0/1
                 [110/2] via 192.168.10.3, 00:54:54, Vlan30
                 [110/2] via 172.16.0.3, 00:54:54, Vlan40
                 [110/2] via 10.20.0.2, 00:54:54, Vlan60
                 [110/2] via 10.11.11.34, 00:54:54, Vlan90
O       10.2.2.4 [110/2] via 10.2.2.14, 00:54:54, GigabitEthernet1/0/2
                 [110/2] via 192.168.10.3, 00:54:54, Vlan30
                 [110/2] via 172.16.0.3, 00:54:54, Vlan40
                 [110/2] via 10.20.0.2, 00:54:54, Vlan60
                 [110/2] via 10.11.11.34, 00:54:54, Vlan90
O       10.11.11.0 [110/2] via 10.2.2.10, 00:54:54, GigabitEthernet1/0/1
     20.0.0.0/30 is subnetted, 1 subnets
O       20.20.20.0 [110/3] via 10.2.2.10, 00:54:54, GigabitEthernet1/0/1
                   [110/3] via 10.2.2.14, 00:54:54, GigabitEthernet1/0/2
     30.0.0.0/30 is subnetted, 1 subnets
O       30.30.30.0 [110/3] via 10.2.2.10, 00:54:54, GigabitEthernet1/0/1
                   [110/3] via 10.2.2.14, 00:54:54, GigabitEthernet1/0/2
     105.0.0.0/30 is subnetted, 2 subnets
O       105.100.50.0 [110/2] via 10.2.2.10, 00:54:54, GigabitEthernet1/0/1
O       105.100.50.4 [110/2] via 10.2.2.14, 00:54:54, GigabitEthernet1/0/2
O    192.168.200.0 [110/68] via 10.2.2.10, 00:54:54, GigabitEthernet1/0/1
                   [110/68] via 10.2.2.14, 00:54:54, GigabitEthernet1/0/2
     197.200.100.0/30 is subnetted, 2 subnets
O       197.200.100.0 [110/2] via 10.2.2.10, 00:54:54, GigabitEthernet1/0/1
O       197.200.100.4 [110/2] via 10.2.2.14, 00:54:54, GigabitEthernet1/0/2

MLS2#
```

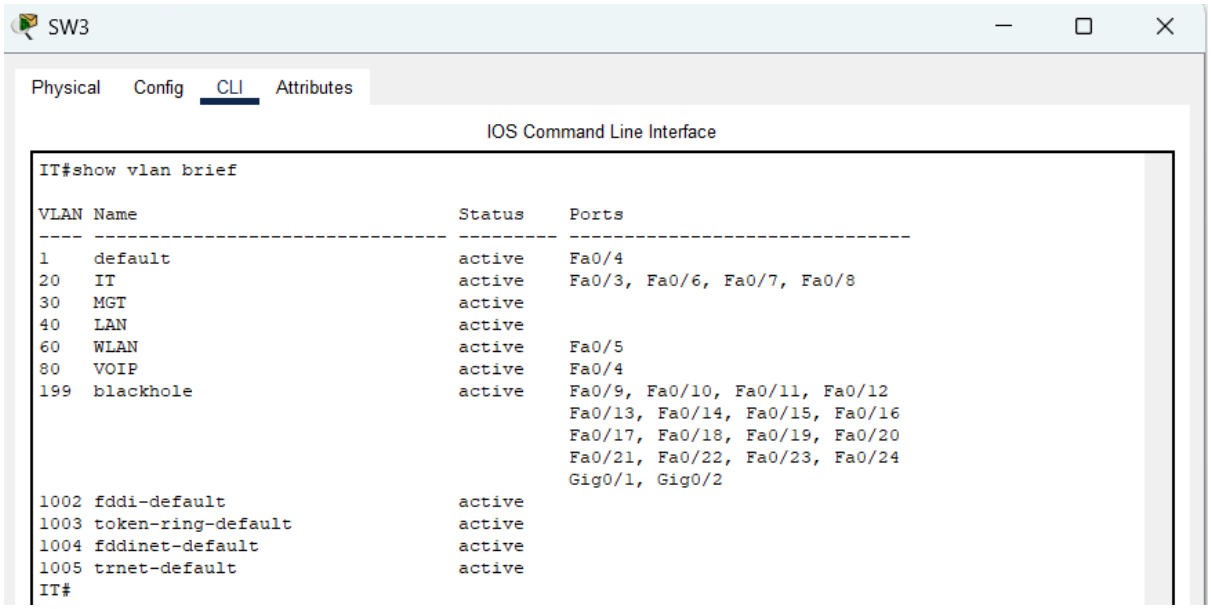
Switching:

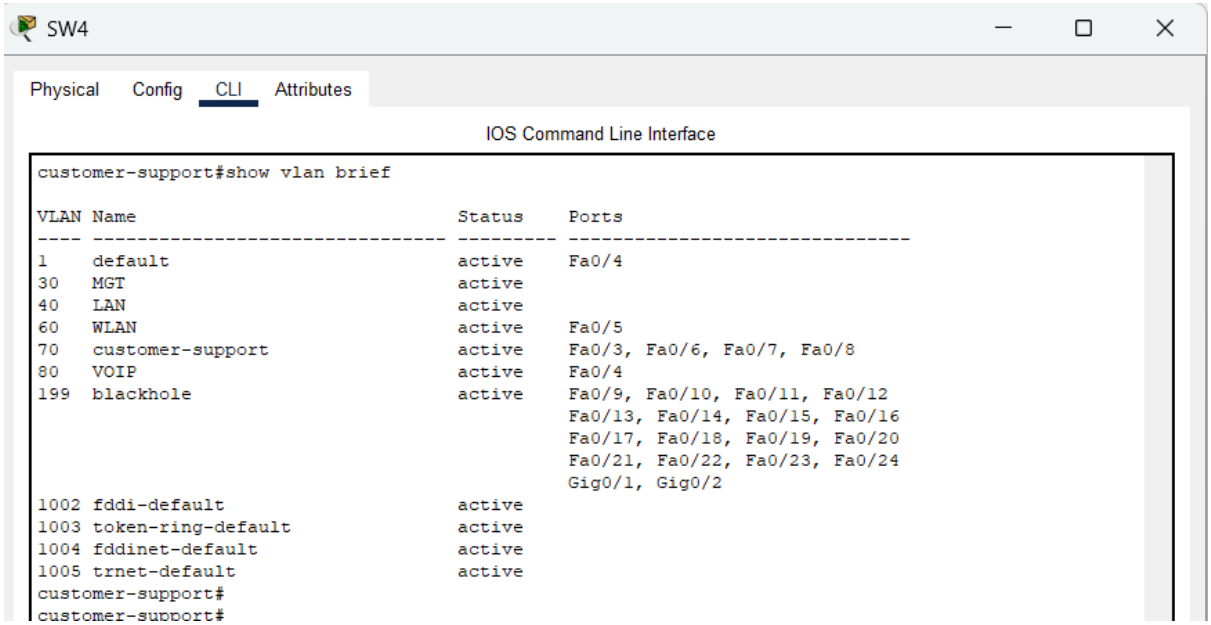
Implement VLANS: In the network design for Secure Shop Ltd, VLANs are strategically implemented to enhance security and efficiency across different departments. Each switch is configured with specific VLANs tailored to departmental needs, such as Sales, IT, Management, and Customer Support. For instance, VLAN 10 is dedicated to Sales, VLAN 20 to IT, and VLAN 30 to Management, ensuring that traffic is isolated and secure.

Additional VLANs, like WLAN for wireless access and VOIP for voice traffic, further optimize network performance by segregating different types of data. The use of VLANs reduces broadcast domains, minimizes congestion, and simplifies network management. This segmentation not only enhances security by limiting access to sensitive data but also improves overall network efficiency, supporting the dynamic needs of our eCommerce operations.









Inter-VLAN routing: Inter-VLAN routing is a crucial component in the network design for Secure Shop Ltd, enabling communication between different VLANs. Each department, such as Sales, IT, and Customer Support, is segmented into its own VLAN for security and efficiency. However, to allow these departments to communicate, inter-VLAN routing is implemented. This is typically achieved using a Layer 3 switch with sub-interfaces configured for each VLAN.

By enabling inter-VLAN routing, I ensure that data can flow seamlessly between departments while maintaining the security benefits of VLAN segmentation. This setup is essential for collaborative tasks and resource sharing across the organization, enhancing overall network functionality and efficiency.

MLS1

Physical Config CLI Attributes

IOS Command Line Interface

```
MLS1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
C       10.2.2.0/30 is directly connected, GigabitEthernet1/0/1
C       10.2.2.4/30 is directly connected, GigabitEthernet1/0/2
O       10.2.2.8/30 [110/2] via 10.2.2.2, 01:09:29, GigabitEthernet1/0/1
                    [110/2] via 192.168.10.2, 01:09:29, Vlan30
                    [110/2] via 172.16.0.2, 01:09:29, Vlan40
                    [110/2] via 10.20.0.3, 01:09:29, Vlan60
                    [110/2] via 10.11.11.35, 01:09:29, Vlan90
O       10.2.2.12/30 [110/2] via 10.2.2.6, 01:09:29, GigabitEthernet1/0/2
                     [110/2] via 192.168.10.2, 01:09:29, Vlan30
                     [110/2] via 172.16.0.2, 01:09:29, Vlan40
                     [110/2] via 10.20.0.3, 01:09:29, Vlan60
                     [110/2] via 10.11.11.35, 01:09:29, Vlan90
O       10.11.11.0/27 [110/2] via 10.2.2.2, 01:09:29, GigabitEthernet1/0/1
C       10.11.11.32/27 is directly connected, Vlan90
C       10.20.0.0/16 is directly connected, Vlan60
     20.0.0.0/30 is subnetted, 1 subnets
O       20.20.20.0 [110/3] via 10.2.2.2, 01:09:29, GigabitEthernet1/0/1
                   [110/3] via 10.2.2.6, 01:09:29, GigabitEthernet1/0/2
     30.0.0.0/30 is subnetted, 1 subnets
O       30.30.30.0 [110/3] via 10.2.2.2, 01:09:29, GigabitEthernet1/0/1
                   [110/3] via 10.2.2.6, 01:09:29, GigabitEthernet1/0/2
     105.0.0.0/30 is subnetted, 2 subnets
O       105.100.50.0 [110/2] via 10.2.2.2, 01:09:29, GigabitEthernet1/0/1
O       105.100.50.4 [110/2] via 10.2.2.6, 01:09:29, GigabitEthernet1/0/2
C    172.16.0.0/16 is directly connected, Vlan40
C    192.168.10.0/24 is directly connected, Vlan30
C    192.168.20.0/24 is directly connected, Vlan20
C    192.168.30.0/24 is directly connected, Vlan10
C    192.168.50.0/24 is directly connected, Vlan50
C    192.168.70.0/24 is directly connected, Vlan70
C    192.168.100.0/24 is directly connected, Vlan100
O    192.168.200.0/24 [110/68] via 10.2.2.2, 01:09:29, GigabitEthernet1/0/1
                      [110/68] via 10.2.2.6, 01:09:29, GigabitEthernet1/0/2
     197.200.100.0/30 is subnetted, 2 subnets
O       197.200.100.0 [110/2] via 10.2.2.2, 01:09:29, GigabitEthernet1/0/1
O       197.200.100.4 [110/2] via 10.2.2.6, 01:09:29, GigabitEthernet1/0/2

MLS1#
MLS1#
MLS1#
MLS1#
```

MLS2

Physical Config CLI Attributes

IOS Command Line Interface

```
MLS2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
O       10.2.2.0/30 [110/2] via 10.2.2.10, 01:10:39, GigabitEthernet1/0/1
                    [110/2] via 192.168.10.3, 01:10:39, Vlan30
                    [110/2] via 172.16.0.3, 01:10:39, Vlan40
                    [110/2] via 10.20.0.2, 01:10:39, Vlan60
                    [110/2] via 10.11.11.34, 01:10:39, Vlan90
O       10.2.2.4/30 [110/2] via 10.2.2.14, 01:10:39, GigabitEthernet1/0/2
                    [110/2] via 192.168.10.3, 01:10:39, Vlan30
                    [110/2] via 172.16.0.3, 01:10:39, Vlan40
                    [110/2] via 10.20.0.2, 01:10:39, Vlan60
                    [110/2] via 10.11.11.34, 01:10:39, Vlan90
C       10.2.2.8/30 is directly connected, GigabitEthernet1/0/1
C       10.2.2.12/30 is directly connected, GigabitEthernet1/0/2
O       10.11.11.0/27 [110/2] via 10.2.2.10, 01:10:39, GigabitEthernet1/0/1
C       10.11.11.32/27 is directly connected, Vlan90
C       10.20.0.0/16 is directly connected, Vlan60
     20.0.0.0/30 is subnetted, 1 subnets
O       20.20.20.0 [110/3] via 10.2.2.10, 01:10:39, GigabitEthernet1/0/1
                   [110/3] via 10.2.2.14, 01:10:39, GigabitEthernet1/0/2
     30.0.0.0/30 is subnetted, 1 subnets
O       30.30.30.0 [110/3] via 10.2.2.10, 01:10:39, GigabitEthernet1/0/1
                   [110/3] via 10.2.2.14, 01:10:39, GigabitEthernet1/0/2
     105.0.0.0/30 is subnetted, 2 subnets
O       105.100.50.0 [110/2] via 10.2.2.10, 01:10:39, GigabitEthernet1/0/1
O       105.100.50.4 [110/2] via 10.2.2.14, 01:10:39, GigabitEthernet1/0/2
C    172.16.0.0/16 is directly connected, Vlan40
C    192.168.10.0/24 is directly connected, Vlan30
C    192.168.20.0/24 is directly connected, Vlan20
C    192.168.30.0/24 is directly connected, Vlan10
C    192.168.50.0/24 is directly connected, Vlan50
C    192.168.70.0/24 is directly connected, Vlan70
C    192.168.100.0/24 is directly connected, Vlan100
O    192.168.200.0/24 [110/68] via 10.2.2.10, 01:10:39, GigabitEthernet1/0/1
                      [110/68] via 10.2.2.14, 01:10:39, GigabitEthernet1/0/2
     197.200.100.0/30 is subnetted, 2 subnets
O       197.200.100.0 [110/2] via 10.2.2.10, 01:10:39, GigabitEthernet1/0/1
O       197.200.100.4 [110/2] via 10.2.2.14, 01:10:39, GigabitEthernet1/0/2

MLS2#
MLS2#
```

Inter-VLAN communication:

From management vlan 40 to IT vlan 20

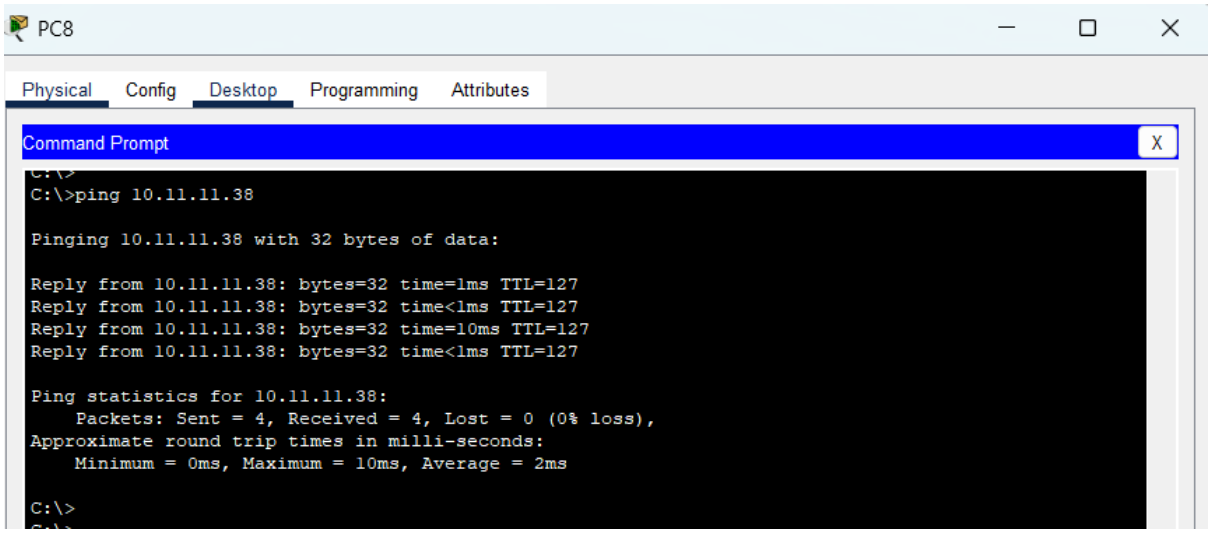
PC8

Physical Config Desktop Programming Attributes

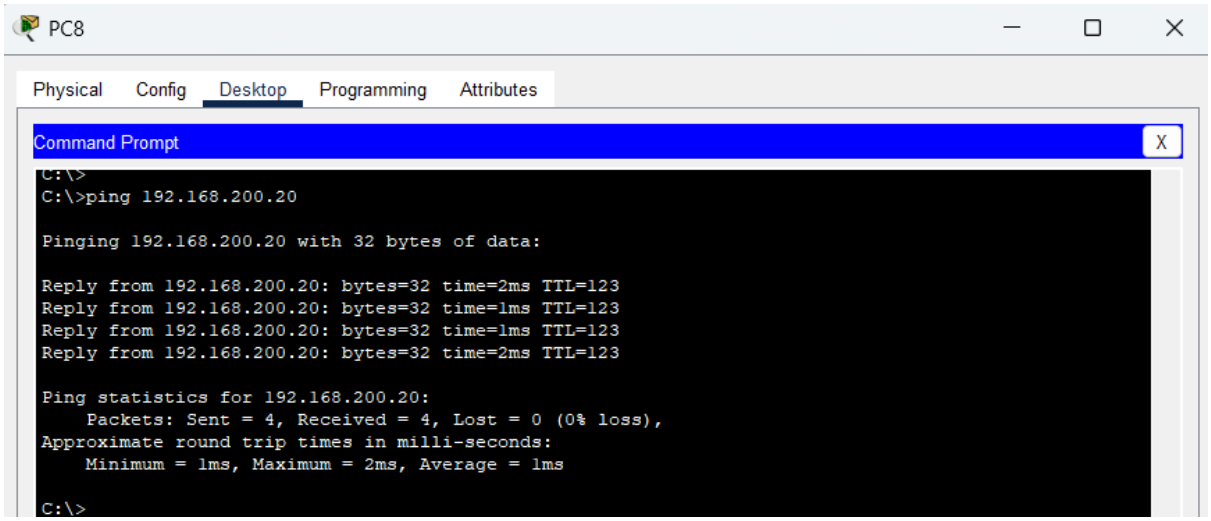
Command Prompt X

```
C:\>ping 192.168.30.18

Pinging 192.168.30.18 with 32 bytes of data:

Reply from 192.168.30.18: bytes=32 time<1ms TTL=127
Reply from 192.168.30.18: bytes=32 time=9ms TTL=127
Reply from 192.168.30.18: bytes=32 time<1ms TTL=127
Reply from 192.168.30.18: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms
```

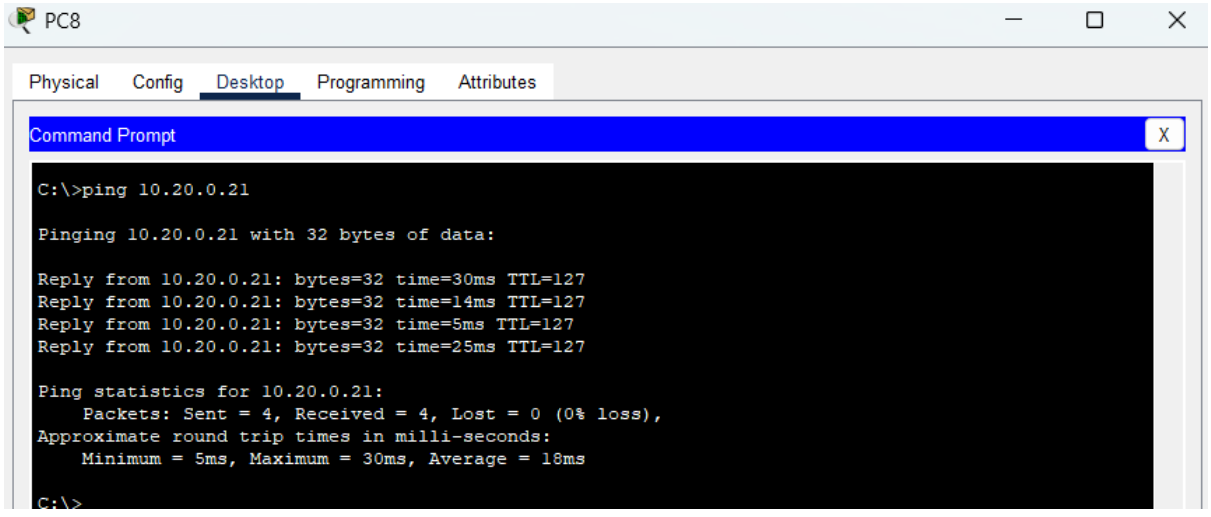
From management vlan 40 to inside server vlan 90



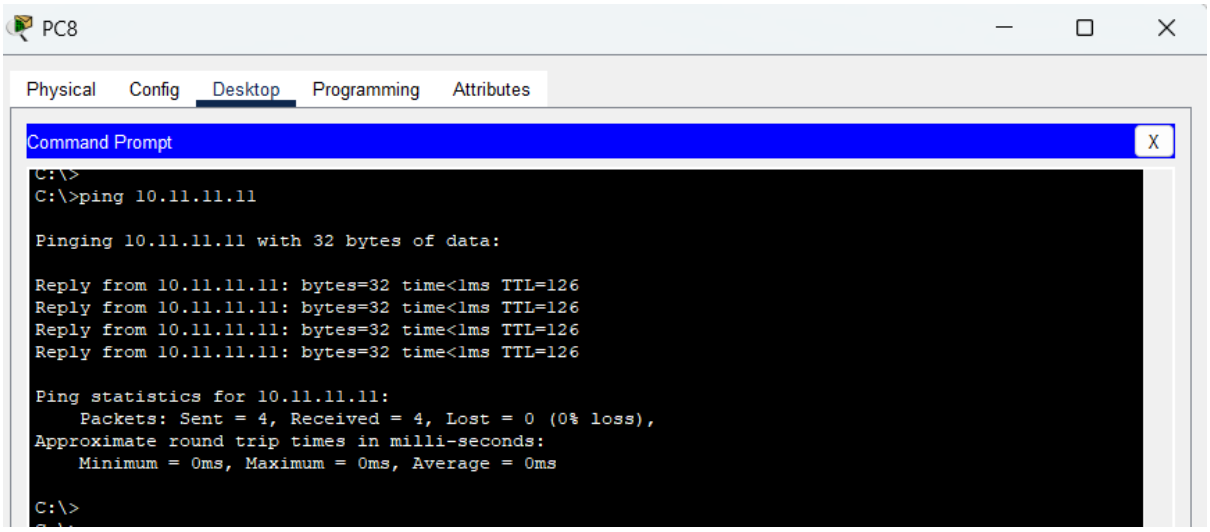
From management vlan 40 to remote user vlan 50



From management vlan 40 to WLAN vlan 60

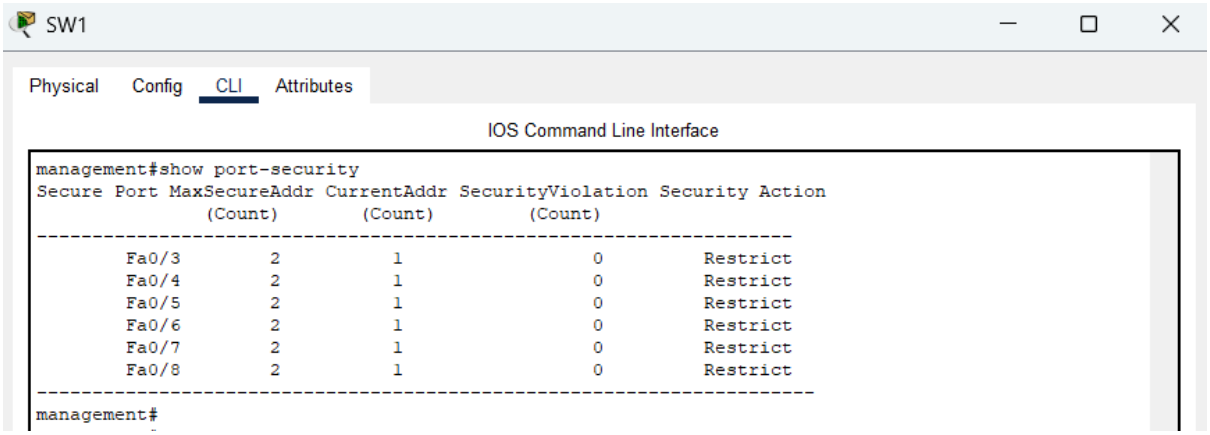


From management vlan 40 to DMZ



Port security: In the network design for Secure Shop Ltd, I implemented port security across the switches for each department—Sales, IT, Management, and Customer Support—to enhance network security. Port security restricts the number of MAC addresses on a port, preventing unauthorized devices from connecting. This is crucial for protecting sensitive data and maintaining network integrity.

By setting a maximum of two secure MAC addresses per port and configuring the security action to "restrict," I ensure that any violation attempts are logged without disrupting legitimate traffic. This setup helps prevent unauthorized access and potential security breaches, safeguarding the network infrastructure and ensuring smooth operations for the company.



SW2

Physical Config CLI Attributes

IOS Command Line Interface

```
sales#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
-------------------------------------------------------------------
        Fa0/3        2           1                0         Restrict
        Fa0/4        2           1                0         Restrict
        Fa0/5        2           1                0         Restrict
        Fa0/6        2           1                0         Restrict
        Fa0/7        2           1                0         Restrict
        Fa0/8        2           1                0         Restrict
        Fa0/9        2           0                0         Restrict
-------------------------------------------------------------------
sales#
sales#
```

SW3

Physical Config CLI Attributes

IOS Command Line Interface

```
IT#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
-------------------------------------------------------------------
        Fa0/3        2           1                0         Restrict
        Fa0/4        2           1                0         Restrict
        Fa0/5        2           1                0         Restrict
        Fa0/6        2           1                0         Restrict
        Fa0/7        2           1                0         Restrict
        Fa0/8        2           1                0         Restrict
-------------------------------------------------------------------
IT#
IT#
```

SW4

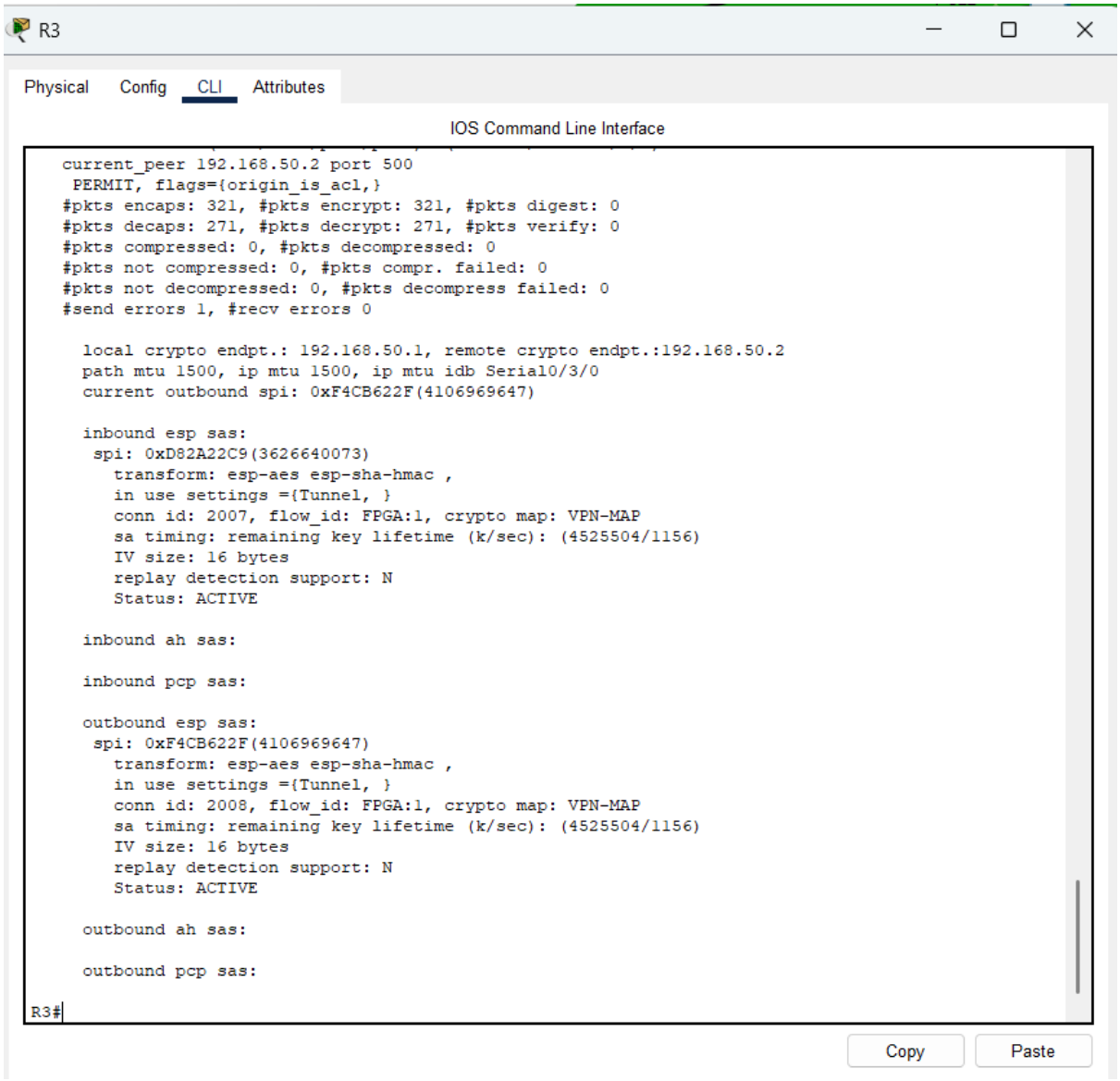
Physical Config CLI Attributes

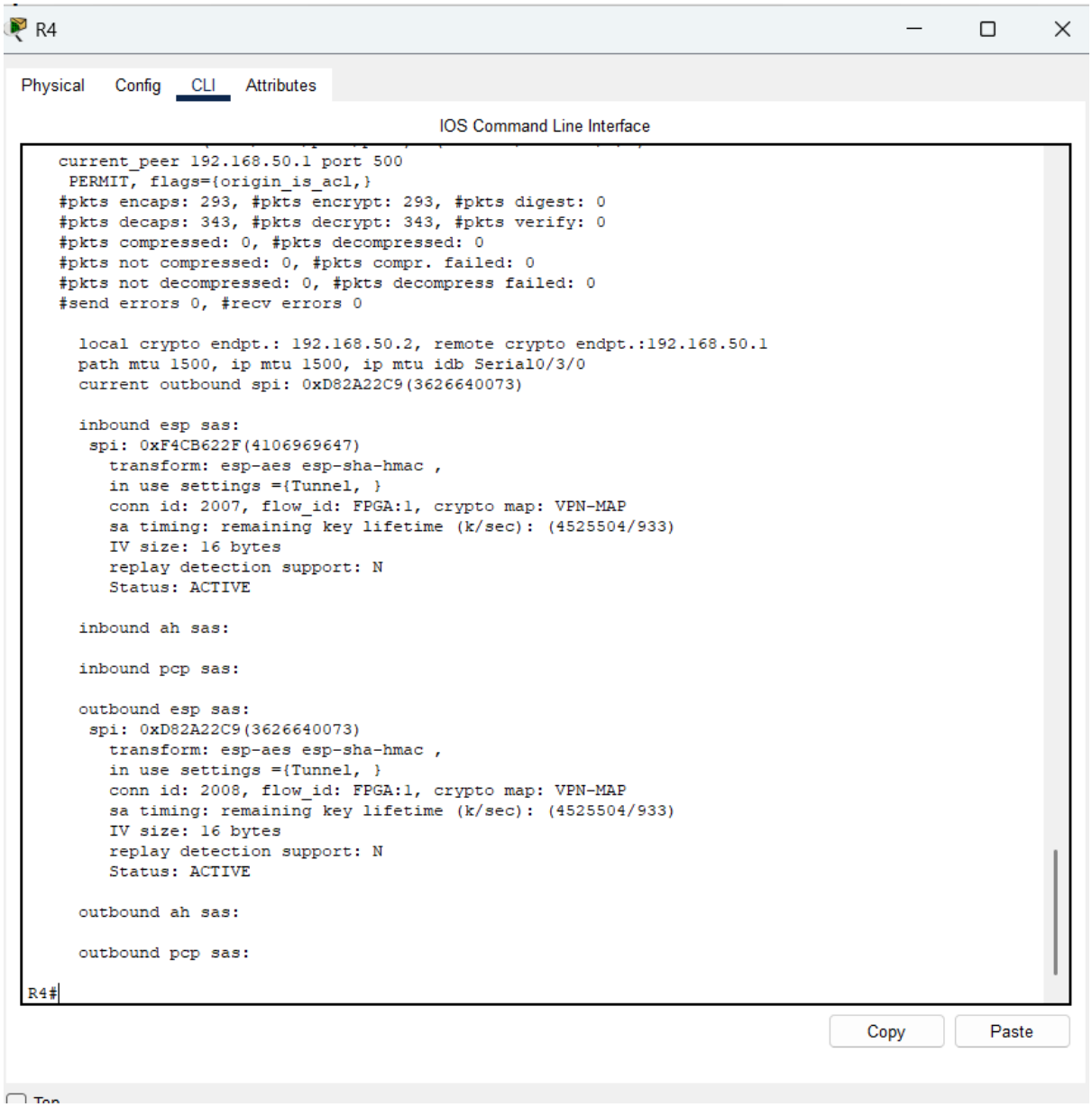
IOS Command Line Interface

```
customer-support#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
-------------------------------------------------------------------
        Fa0/3        2           1                0         Restrict
        Fa0/4        2           1                0         Restrict
        Fa0/5        2           1                0         Restrict
        Fa0/6        2           1                0         Restrict
        Fa0/7        2           0                0         Restrict
        Fa0/8        2           0                0         Restrict
-------------------------------------------------------------------
```

Remote access(IPsec): The screenshot demonstrates the use of IPSec to secure communications between the internal network and remote workers. When a ping is initiated from inside the network to a remote worker or vice versa, the data is encrypted using the ESP-AES and ESP-SHA-HMAC algorithms, ensuring confidentiality and integrity. The active status of the security associations (SAs) indicates that encryption and decryption are functioning correctly, with packets being encapsulated and decapsulated securely.

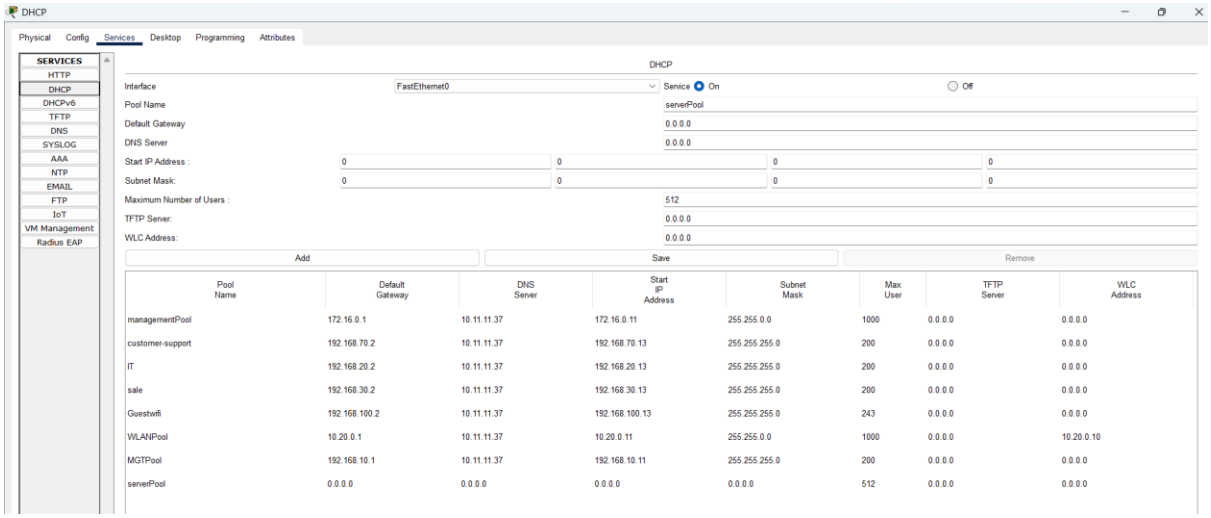
This setup ensures that sensitive information remains protected during transmission, providing a secure communication channel over potentially insecure networks. By using IPSec, I ensure that data exchanged with remote workers is safeguarded against interception and tampering, maintaining the security and privacy of our network operations.

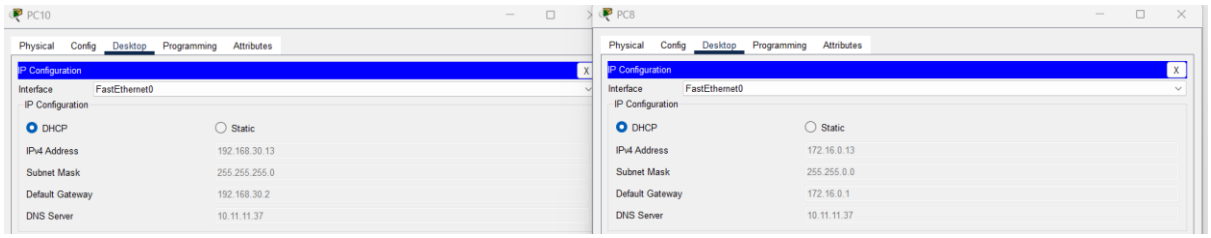

R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
current_peer 192.168.50.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 321, #pkts encrypt: 321, #pkts digest: 0
#pkts decaps: 271, #pkts decrypt: 271, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0
local crypto endpt.: 192.168.50.1, remote crypto endpt.:192.168.50.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/3/0
current outbound spi: 0xF4CB622F(4106969647)
inbound esp sas:
spi: 0xD82A22C9(3626640073)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2007, flow_id: FPGA:1, crypto map: VPN-MAP
sa timing: remaining key lifetime (k/sec): (4525504/1156)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0xF4CB622F(4106969647)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2008, flow_id: FPGA:1, crypto map: VPN-MAP
sa timing: remaining key lifetime (k/sec): (4525504/1156)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE
outbound ah sas:
outbound pcp sas:
R3#
Copy
Paste



DHCP and DNS: Setting up DHCP and DNS is essential for efficient network management and operation at Secure Shop Ltd. DHCP automates IP address allocation, reducing manual configuration errors and ensuring devices can connect seamlessly to the network. The screenshot shows various DHCP pools configured for different departments, such as Management and Sales, each with specific IP ranges and settings. This setup ensures that each department has the necessary IP resources, enhancing network organization and scalability.

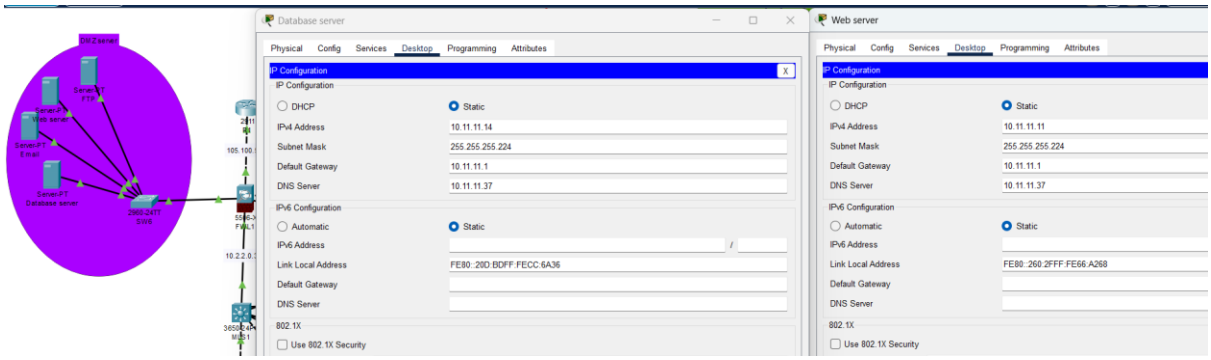
DNS is equally important as it translates domain names into IP addresses, allowing users to access resources using easy-to-remember names instead of numerical IPs. By securing both DHCP and DNS, I ensure that IP allocation and domain resolution are reliable and protected against potential threats, such as IP spoofing or DNS attacks. This comprehensive setup enhances network efficiency, security, and user experience, supporting the dynamic needs of our eCommerce operations.





Web and database server: Placing web and database servers in a secure DMZ zone is a strategic decision to enhance the security of Secure Shop Ltd's network. The DMZ acts as a buffer between the internal network and the external internet, allowing public access to the web server while keeping the database server protected. By positioning these servers behind a firewall, I ensure that they are shielded from direct external threats, reducing the risk of unauthorized access and attacks.

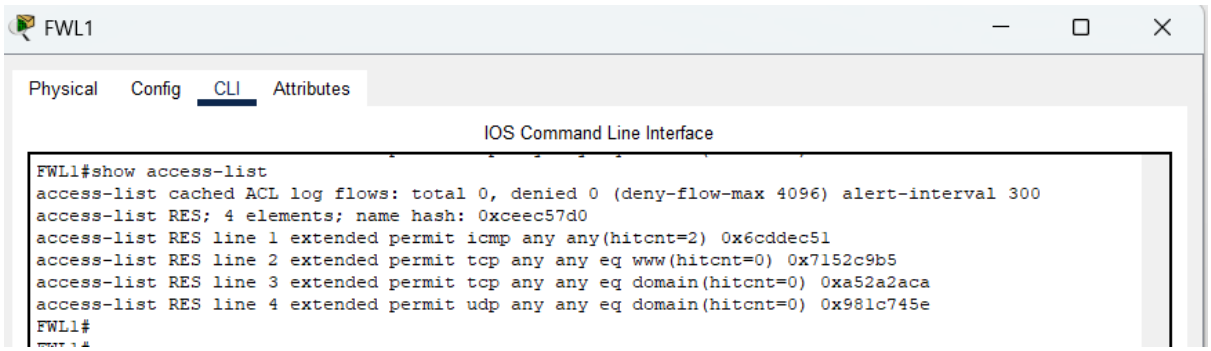
This setup allows the web server to handle public requests while the database server remains secure, accessible only through controlled channels. The benefits include improved security, as sensitive data is protected, and enhanced network performance, as traffic is efficiently managed. This configuration supports the company's eCommerce operations by ensuring that critical services remain available and secure.

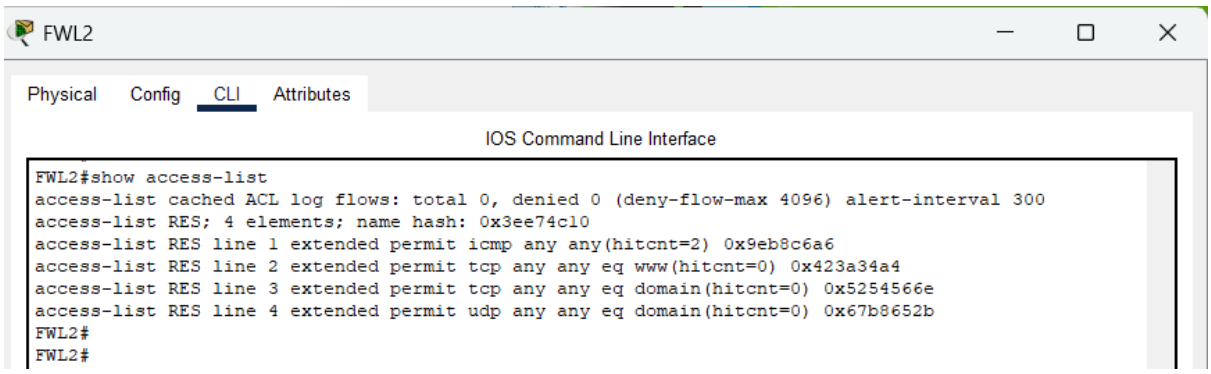


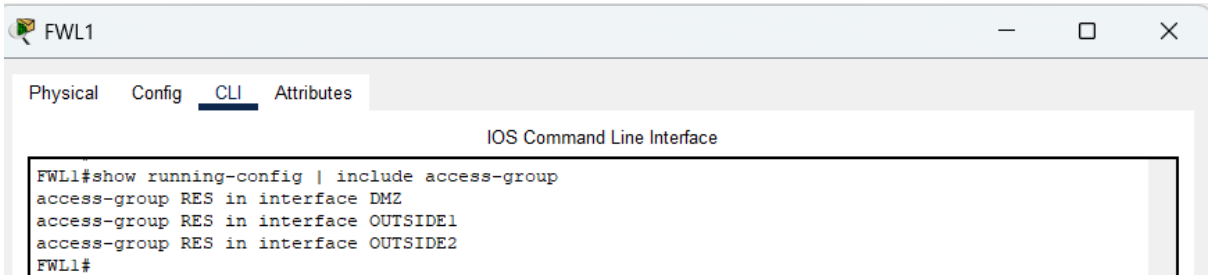
3. Network security implementation

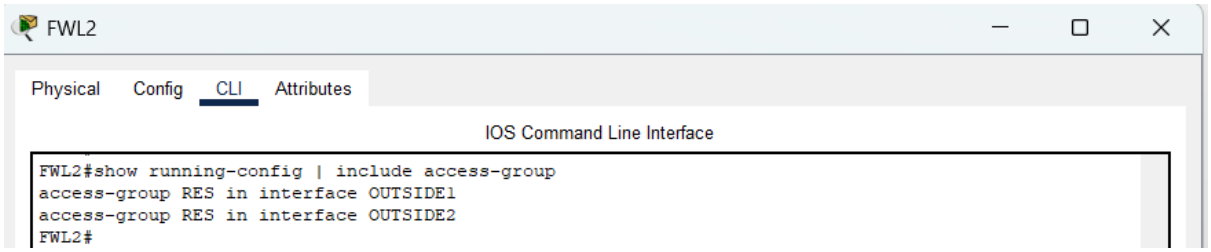
Firewall Configuration: The firewalls in Secure Shop Ltd's network are effectively configured to filter incoming and outgoing traffic, ensuring robust security. The access lists on both FWL1 and FWL2 show that ICMP traffic is permitted, with a hit count of 2, indicating successful pings and active monitoring. This allows for essential network diagnostics while maintaining control over traffic flow. The access lists also permit TCP and UDP traffic for specific services, such as web and domain, ensuring that only authorized traffic is allowed.

The use of access groups, like RES, applied to interfaces such as DMZ and OUTSIDE 1 and 2, further enhances security by segmenting and controlling traffic between different network zones. This configuration ensures that the network is protected against unauthorized access while allowing necessary communication, supporting the secure operation of the company's eCommerce services.

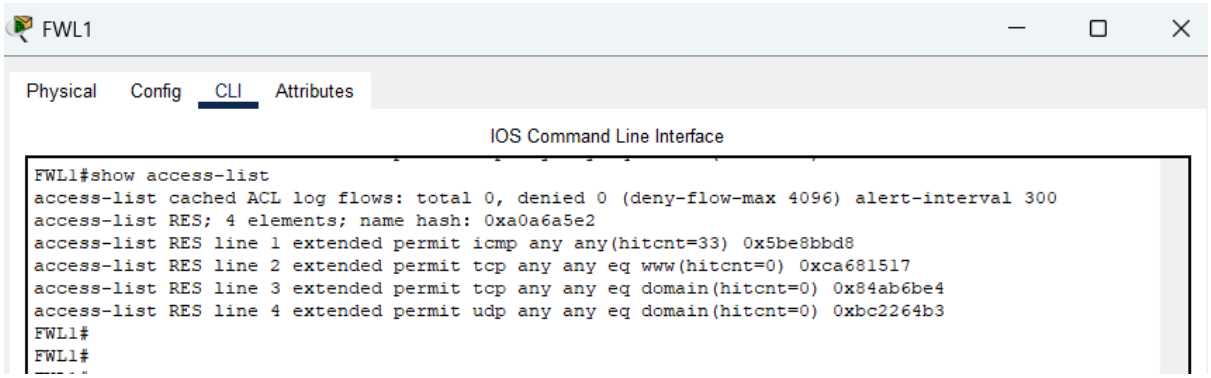


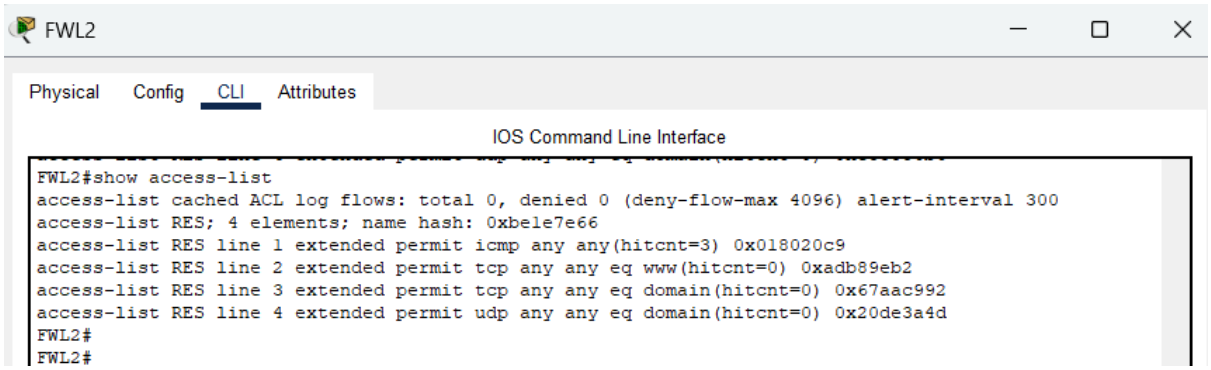






Intrusion prevention(IDS) :The firewalls in Secure Shop Ltd's network are effectively configured to monitor and detect potential threats, as evidenced by the hit counts in the access lists. On FW1, the ICMP traffic shows a hit count of 33, indicating active monitoring and detection of network activity. Similarly, FW2 has a hit count of 3 for ICMP traffic, demonstrating its role in threat detection. These hit counts reflect the firewalls' ability to track and log traffic, allowing for real-time monitoring of network events. By using access lists to permit specific traffic and log attempts, the firewalls act as an Intrusion Detection System (IDS), providing insights into network behavior and enhancing security by identifying potential threats. This setup ensures that the network remains secure and resilient against unauthorized access and attacks.



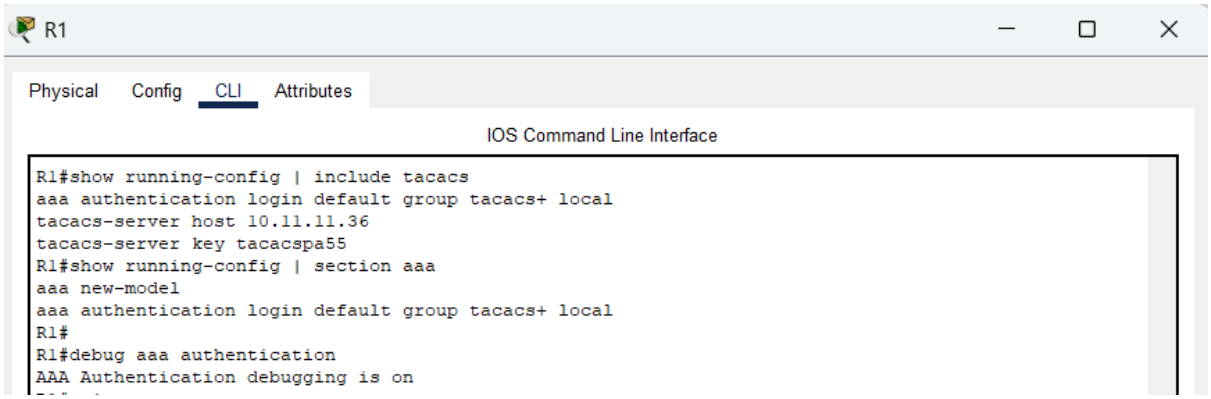


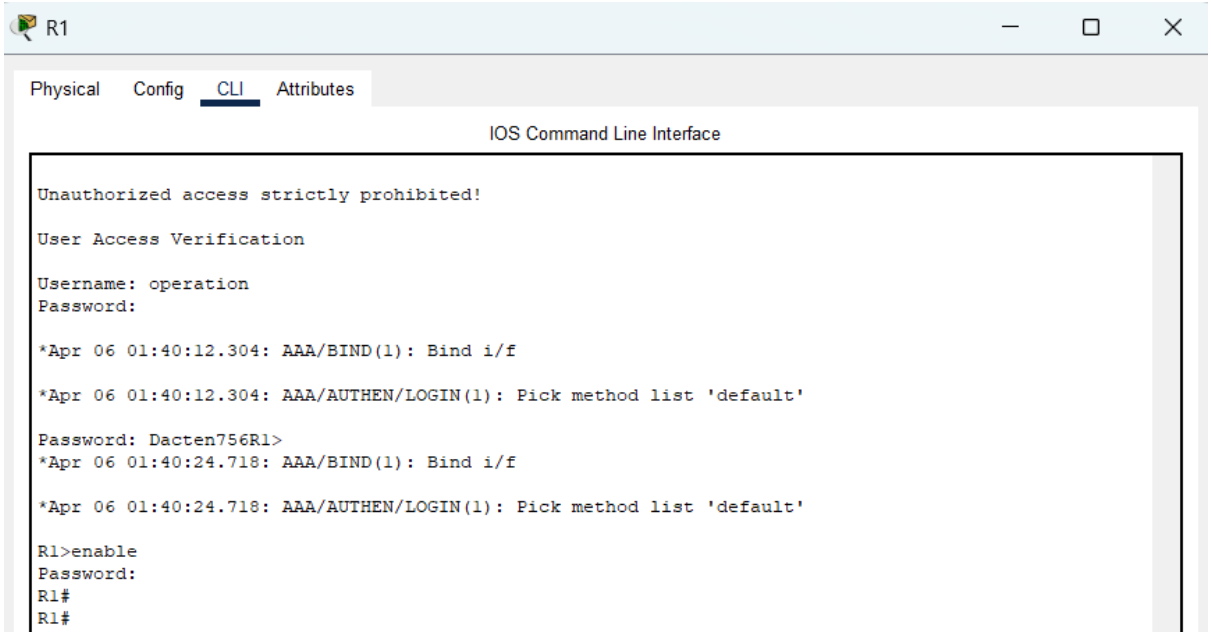
Authentication and Access control:

AAA,TACACS+:TACACS+ (Terminal Access Controller Access-Control System Plus) is a robust protocol used for authentication, authorization, and accounting (AAA) in secure network environments, such as a secure shop. The screenshots illustrate the successful configuration and operation of TACACS+ on a network device via the command-line interface (CLI). The configuration sets up a TACACS+ server at IP address 10.11.11.36 with a shared secret key "tacacspa55," ensuring secure communication. The default authentication method prioritizes TACACS+ and falls back to local authentication if needed.

The login process, shown in the logs, captures user access attempts, providing a detailed audit trail essential for monitoring and compliance. TACACS+ encrypts the entire payload, offering enhanced security over protocols like RADIUS, and allows for centralized authentication, ensuring only authorized personnel access critical resources. This setup not only protects sensitive information but also supports detailed logging for auditing and troubleshooting, enhancing the

overall security posture of the shop's network infrastructure. The logs confirm that TACACS+ is working successfully, effectively managing user access and maintaining security.





Strong password and MFA: I configured Multi-Factor Authentication (MFA) and strong password policies to secure all network devices at Secure Shop Ltd. As part of this setup, I created specific user accounts with unique passwords and enabled passwords for additional security layers for all devices . This approach ensures that accessing devices like access layer switches, multi-layer switch and routers requires both a username and a password, effectively implementing MFA.

The password policies enforce complexity and minimum length, reducing the risk of unauthorized access. These measures are essential for protecting sensitive data and maintaining network integrity, ensuring that only authorized personnel can manage and configure network resources. This comprehensive security strategy supports the overall security posture of the company.

R1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router(config-line)#line console 0
Router(config-line)#pass
Router(config-line)#password ciscol2
% Password too short - must be at least 8 characters. Password not configured.
Router(config-line)#line vty 0 4
Router(config-line)#password netcad7
% Password too short - must be at least 8 characters. Password not configured.
Router(config-line)#enable password boot123
% Password too short - must be at least 8 characters. Password not configured.
Router(config)#username boot password IT123
% Password too short - must be at least 8 characters. Password not configured.
Router(config)#
```

SW1

Physical Config CLI Attributes

IOS Command Line Interface

```
 Unauthorized Access Strictly Prohibited!

User Access Verification

Username: operation
Password:

management>enable
Password:
management#conf
management#configure ter
management#configure terminal
```

MLS1

Physical Config CLI Attributes

IOS Command Line Interface

```
 Unauthorized Access Strictly Prohibited!

User Access Verification

Username: operation
Password:

MLS1>enable
Password:
MLS1#conf
MLS1#configure ter
MLS1#configure terminal
```

R1

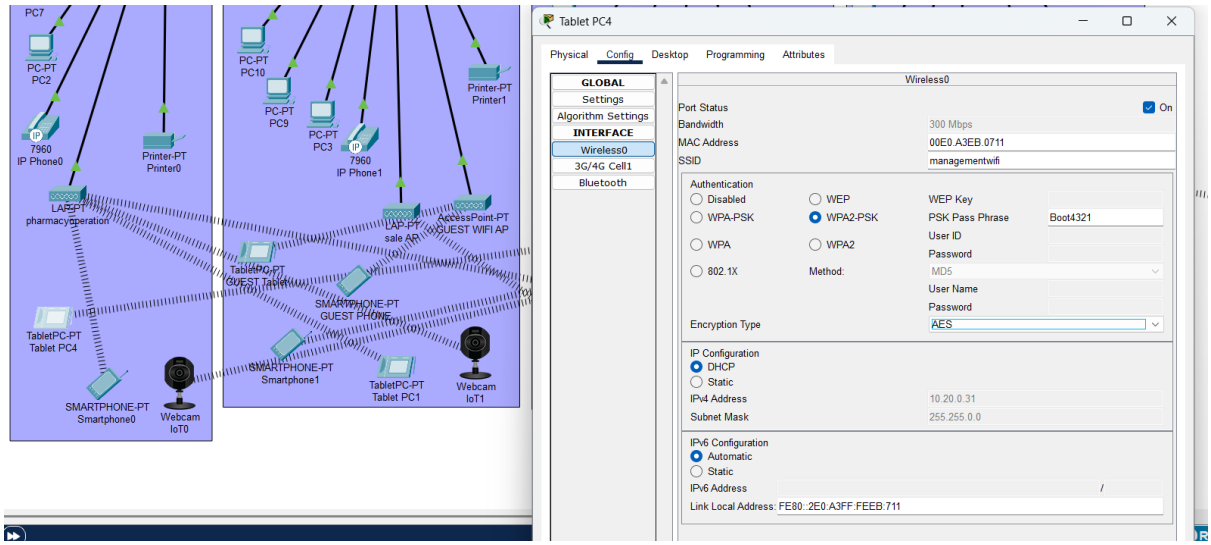
Physical Config CLI Attributes

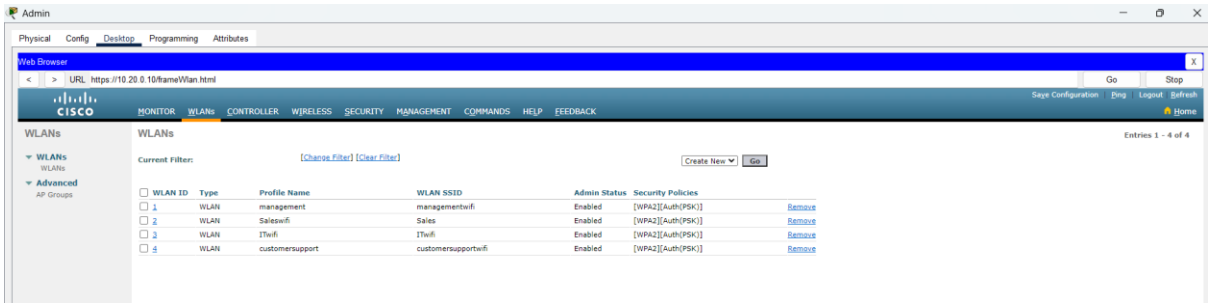
IOS Command Line Interface

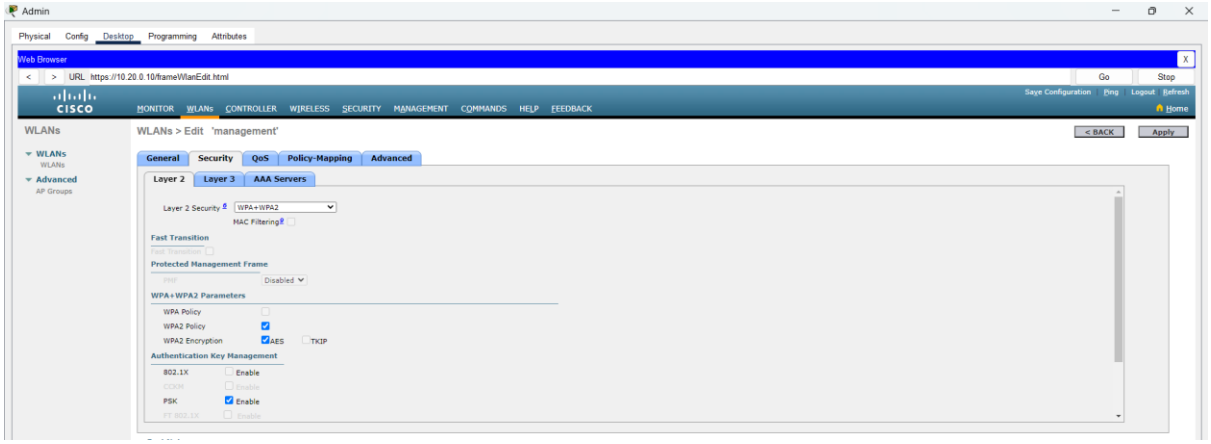
```
Unauthorized access strictly prohibited!

User Access Verification

Username: operation
Password:

R1`>enable
Password:
R1`#conf
R1`#configure ter
R1`#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1`(config)#
```

Wireless security: The wireless security setup for Secure Shop Ltd is robust, ensuring secure connectivity across all departments, including Sales, IT, Management, and Customer Support. Each department has its own SSID, and the network uses WPA2 with AES encryption, providing strong protection against unauthorized access. This encryption standard is highly secure, safeguarding data transmitted over the wireless network.

Additionally, MAC filtering is implemented, allowing only approved devices to connect, further enhancing security by preventing unauthorized devices from accessing the network. This comprehensive approach ensures that the Wi-Fi network is secure, protecting sensitive company data and maintaining the integrity of network communications. By implementing these measures, I ensure that the wireless infrastructure supports secure and efficient operations for all departments.

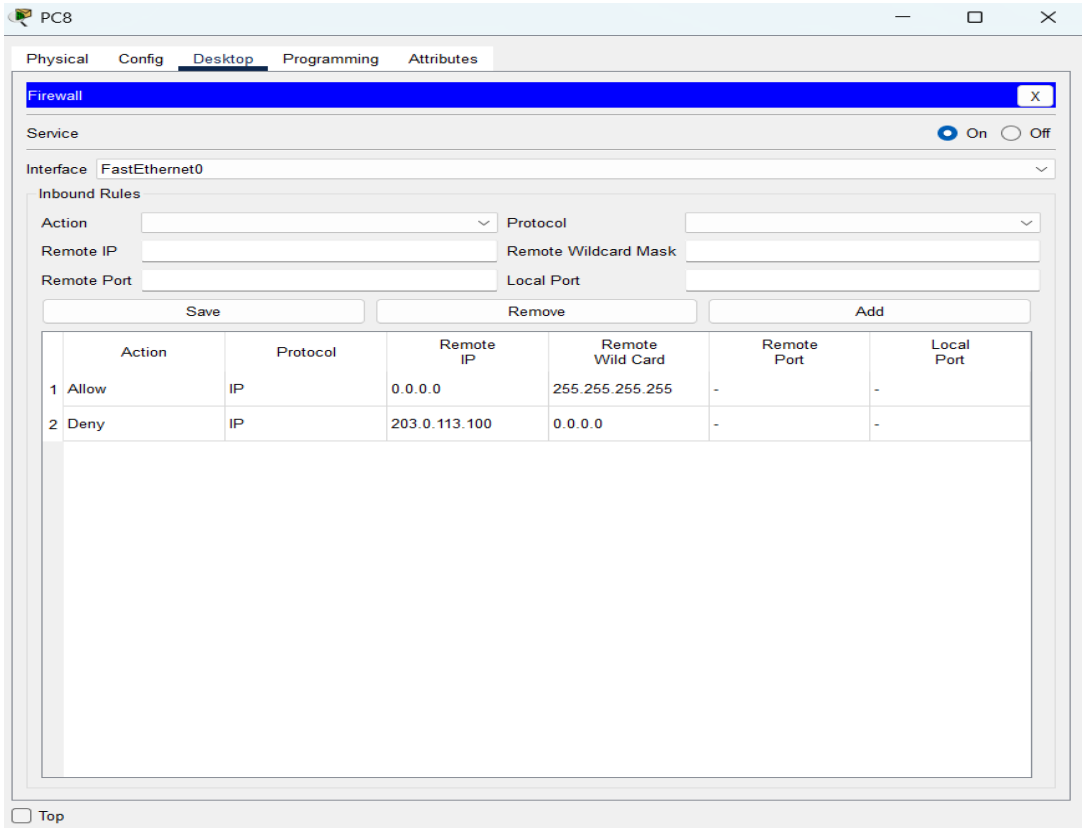




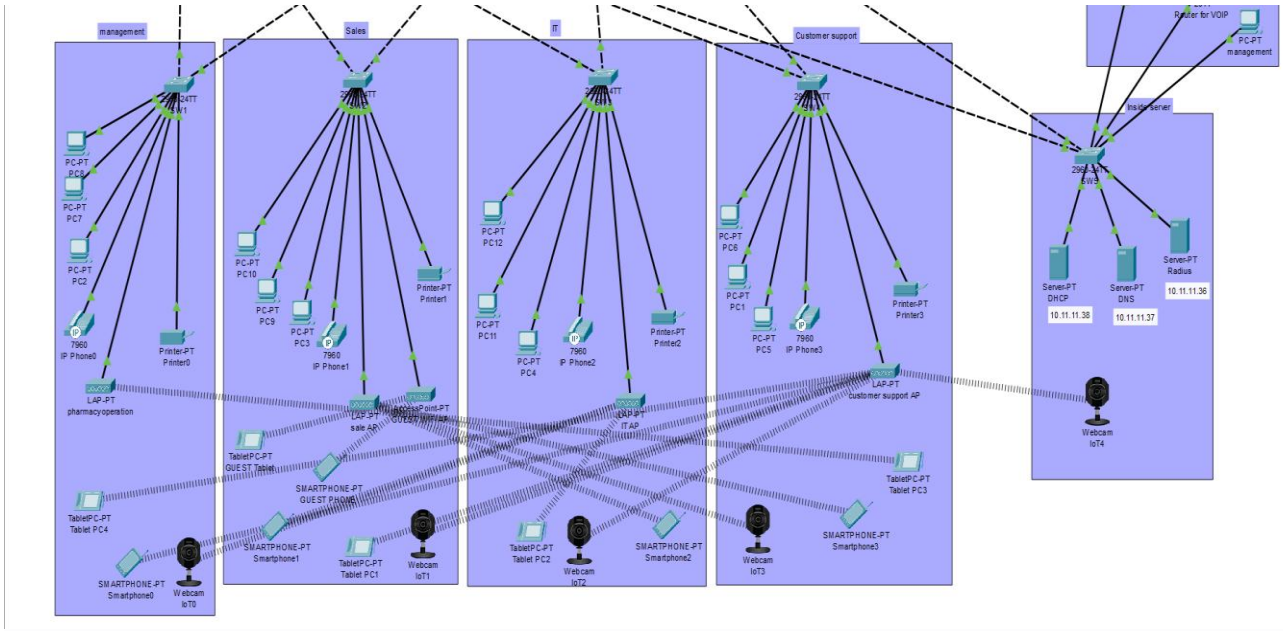


Endpoint Protection: Endpoint protection is a critical component of Secure Shop Ltd's network security strategy. By ensuring that all devices, including those in Sales, IT, Management, and Customer Support, have up-to-date antivirus software and patch management, I protect the network from malware and vulnerabilities. Regular updates and patches are essential to address security flaws and prevent exploitation by attackers. This proactive approach minimizes the risk of infections and data breaches, maintaining the integrity and confidentiality of sensitive information. By implementing comprehensive endpoint protection, I ensure that all devices are secure, supporting the overall resilience and security of the company's network infrastructure.

Firewall**:** Additionally, I utilize a firewall to control incoming and outgoing network traffic based on predetermined security rules. This enhances our network security by blocking unauthorized access while allowing legitimate communications, ensuring the safety of our internal network from external threats.



Physical security: In Secure Shop Ltd, I have implemented comprehensive physical security measures to protect critical assets and data. CCTV cameras are installed in all four departments,Sales, IT, Management, and Customer Support as well as inside the server room. This constant monitoring deters unauthorized access and provides real-time surveillance, enhancing security and enabling quick response to incidents. Additionally, securing server rooms with biometric access ensures that only authorized personnel can enter, further protecting sensitive equipment and data. To prevent data breaches, I also implemented measures to block unauthorized USB device connections. These physical security strategies collectively safeguard the company's infrastructure, ensuring a secure environment for operations.



4. Network Access policy:

- Define who can access what and from where.
- Implement a least privilege model (only necessary access is granted).

Privilege Levels and Access Control

IT Department (Privilege Level 15): The IT department has the highest privilege level, allowing full control over network configurations, security settings, and troubleshooting. They can execute commands like show running-config, show vlan, configure terminal, and copy running-config startup-config, ensuring smooth and secure network operations.

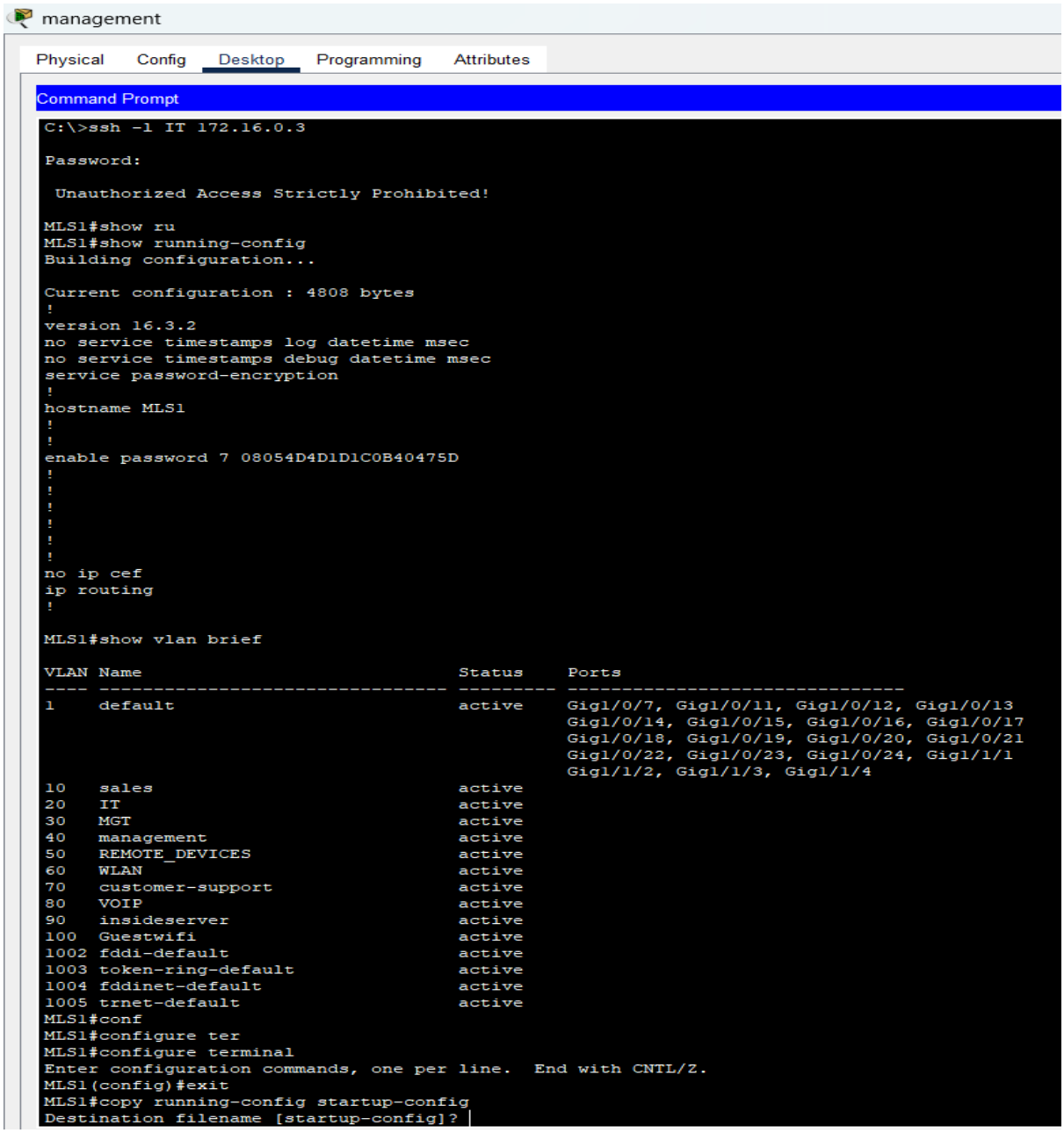
Customer Support (Privilege Level 5): Customer support has limited access to assist users and perform basic troubleshooting. They can use commands like show vlan to view network segmentation but cannot modify configurations or execute commands like show running-config and configure terminal, maintaining system integrity.

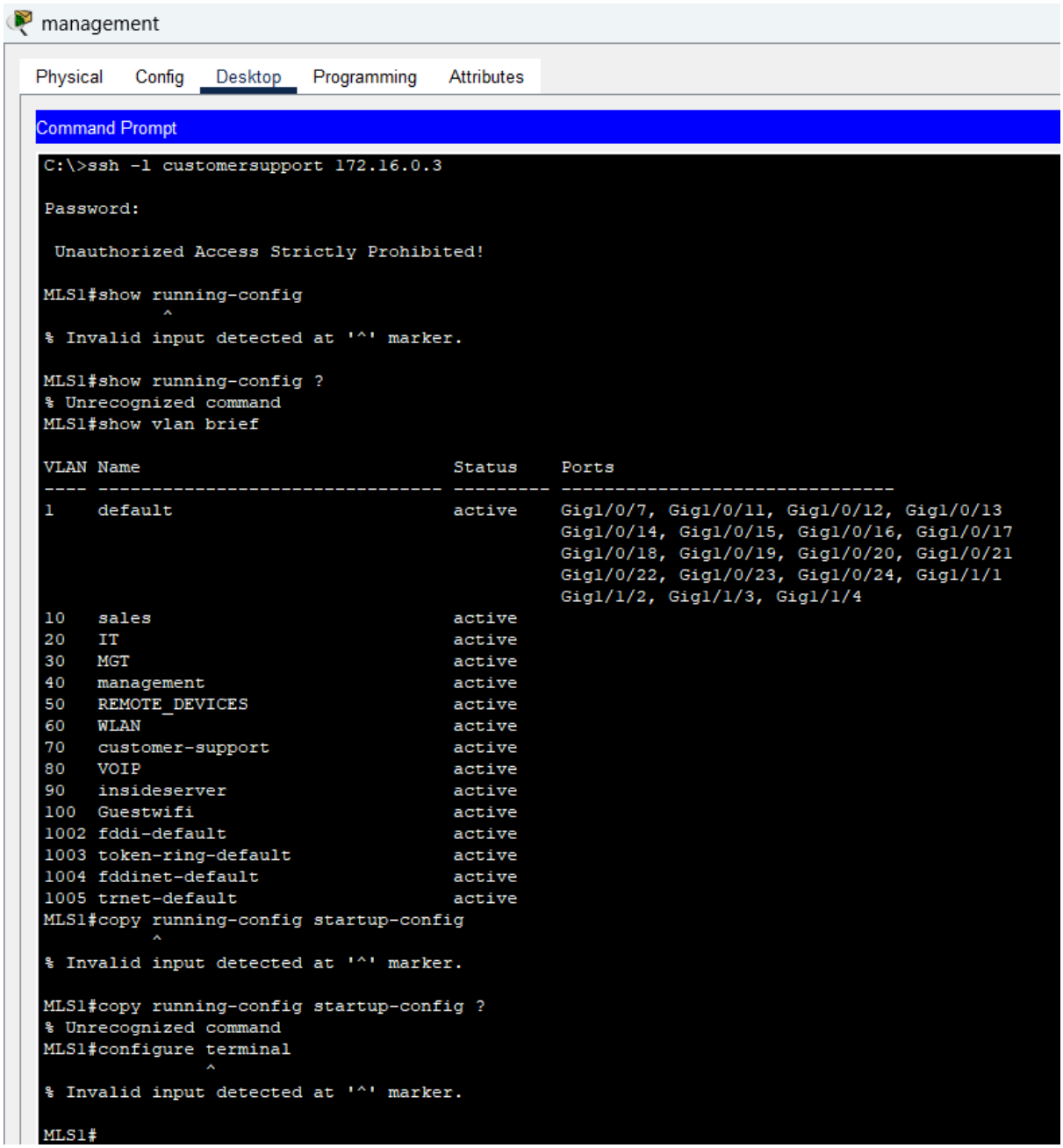
Management (Privilege Level 10): Management needs access to system reports and network performance data for informed decision-making. While they can view configurations, they cannot make major changes, ensuring oversight without compromising security.

Sales (Privilege Level 2): Sales staff have minimal access, allowing them to view only the information necessary for their role, such as customer data and sales analytics. They do not have access to network settings, ensuring security while supporting their workflow.

Summary:-In the screenshots as we can see, the IT department can execute commands like show running-config, show vlan, configure terminal, and copy running-config startup-config, allowing them to manage and secure the network effectively. This ensures smooth and efficient operations. Meanwhile, customer support can execute commands such as show vlan, enabling them to view network segmentation for troubleshooting purposes.

However, customer supports don't have privilege to use commands like show run, configure terminal. This limited access helps maintain system integrity by preventing unauthorized changes while still allowing effective user support.


management
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>ssh -l IT 172.16.0.3
Password:
Unauthorized Access Strictly Prohibited!
MLS1#show ru
MLS1#show running-config
Building configuration...
Current configuration : 4808 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MLS1
!
!
enable password 7 08054D4D1D1C0B40475D
!
!
!
!
!
!
no ip cef
ip routing
!
MLS1#show vlan brief
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Gig1/0/7, Gig1/0/11, Gig1/0/12, Gig1/0/13
Gig1/0/14, Gig1/0/15, Gig1/0/16, Gig1/0/17
Gig1/0/18, Gig1/0/19, Gig1/0/20, Gig1/0/21
Gig1/0/22, Gig1/0/23, Gig1/0/24, Gig1/1/1
Gig1/1/2, Gig1/1/3, Gig1/1/4
10 sales active
20 IT active
30 MGT active
40 management active
50 REMOTE_DEVICES active
60 WLAN active
70 customer-support active
80 VOIP active
90 insideserver active
100 Guestwifi active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
MLS1#conf
MLS1#configure ter
MLS1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MLS1(config)#exit
MLS1#copy running-config startup-config
Destination filename [startup-config]?



Incident Response Plan for Secure Shop Ltd

Secure Shop Ltd is committed to maintaining a secure network infrastructure to protect its eCommerce operations. This Incident Response Plan (IRP) outlines the steps to be taken in the event of a security breach, ensuring a swift and effective response to minimize damage and restore normal operations.

1. Preparation, Security Measures in Place:

- Network Segmentation with VLANs: Each department (Sales, IT, Management, Customer Support) is assigned separate VLANs to prevent unauthorized access and limit the impact of breaches.

- Firewall Configuration: Firewalls (FWL1 & FWL2) restrict unauthorized traffic using access control lists (ACLs) and intrusion detection systems (IDS/IPS).
- Authentication & Access Control: Multi-Factor Authentication (MFA), TACACS+, and strict password policies ensure only authorized users can access network resources.
- Physical Security: CCTV cameras monitor the premises, and biometric access controls secure the server room.
- Endpoint Protection: All devices are secured with updated antivirus software and patch management to mitigate malware threats.
- Secure Remote Access: IPSec VPN ensures encrypted communication for remote employees, reducing the risk of data interception.

2. Identification, Detecting Security Breaches:

- Intrusion Detection System (IDS): Monitors network traffic for anomalies, such as unauthorized access attempts.
- Firewall Logs: Analysing access logs to identify potential security threats.
- Unusual Network Activity: Sudden spikes in traffic or unauthorized login attempts trigger alerts.
- User Reports: Employees report suspicious emails, unauthorized access, or system anomalies.

3. Containment, Immediate Actions:

- Isolate Affected Systems:
    - If an attack is detected in a VLAN (e.g., IT, Management), it will be temporarily isolated.
    - If an endpoint is compromised, network access will be revoked.
- Disable Compromised Accounts: Any accounts suspected of being compromised will be locked and investigated.
- Firewall Rule Adjustments: ACLs will be updated to block malicious traffic and restrict external access if necessary.
- Restrict Remote Access: Disable VPN access for compromised accounts or devices.

4. Eradication, Removing Threats:

- Malware Removal: Endpoint security software will be used to scan and remove malware.
- Patch Vulnerabilities: Update all affected software, routers, and switches to the latest secure versions.
- Reset Credentials: Force password resets for compromised accounts and reapply MFA.
- Audit Network Devices: Ensure all routers, switches, and firewalls have not been tampered with.

5. Recovery, Restoring Normal Operations:

- Restore from Backups: Use secure backups to restore affected systems (e.g., database, web servers).
- Reinstate Network Connectivity: After thorough security checks, re-enable VLANs and remote access.
- Monitor for Residual Threats: Continue monitoring logs and IDS for any signs of lingering threats.
- Confirm Security Fixes: Conduct vulnerability assessments to ensure all threats have been mitigated.

6. Lessons Learned, Post-Incident Analysis:

- Incident Review: Document the attack vector, affected systems, and response effectiveness.
- Policy Updates: Improve firewall rules, access control policies, and authentication methods if necessary.
- Employee Training: Educate employees on recognizing phishing attempts and security best practices.
- Security Enhancements: Upgrade network security, such as additional monitoring tools or stricter privilege levels.

7. Roles & Responsibilities

- IT Department (Privilege Level 15): Leads response efforts, mitigates security threats, and updates network security configurations.
- Customer Support (Privilege Level 5): Reports potential incidents and assists users in security-related queries.
- Management (Privilege Level 10): Oversees incident impact, ensures business continuity, and enforces security policies.
- Sales (Privilege Level 2): Reports suspicious activities and follows security guidelines to protect customer data.

Summary

Secure Shop Ltd, a growing eCommerce company, requires a robust and secure network infrastructure to support its operations. The network design includes VLAN segmentation for each department, enhancing security and efficiency by isolating traffic. A combination of public and private IP addressing ensures efficient communication, while redundancy measures like HSRP maintain high availability. OSPF is used for dynamic routing, supporting scalability and optimal path selection.

Secure remote access is provided via IPSec VPNs, and a DMZ protects web and database servers. Comprehensive security measures include firewalls, IDS/IPS, and TACACS+ for authentication, ensuring only authorized access. Physical security is enhanced with CCTV and biometric access controls. The network supports current operations and future growth,

maintaining data confidentiality, integrity, and availability. An incident response plan outlines steps for swift action in case of security breaches, ensuring resilience and continuous operation.