NETWORK AND SECURITY DESIGN FOR TECH ZOLUTIONS INC.

Author: Abhi Bhise | Security Architect

Table of Contents

Disclaimer:

1. *This report and the accompanying design represent a proof-of-concept. All the requested connections and features are implemented and work without any issue. However, this does not represent the scale of actual network.*
2. *All the config pasted is from the note taking software (Obsidian) which has a terminal like custom skin applied. I used this tool for note taking and keeping the track of all the commands I implemented. Most of the screenshots are from this app that has code block feature to organise the codes and commands,*
3. *Passwords used on many of the devices are kept simple for ease of use as this is just a proof-of-concept design.*

Introduction

As the employees of Tech Zolutions Inc. relocate to the new site, a comprehensive and detailed Network Security architecture is required. This report is an attempt to fulfil the various requested requirements. Below are the details and base requirements that were addressed in the design and this report.

Network: 172.16.10.0/24

Task 1:

- Network topology design
- Subnetting to address the host device requirements
- Wireless setup for each department
- Server room setup with 4 distinct servers,
    - DHCP server
    - File server
    - Email server
    - Web server
- VLAN setups for each of the following departments
    - Development ------------(50 hosts)
    - Sales and Marketing ----(30 hosts)
    - HR -------------------------(25 hosts)
    - Finance --------------------(25 hosts)
    - IT ----------------------------(15 hosts)
    - Conference room
    - Server room
- Inter-VLAN routing
- OSPF routing
- DHCP setup and IP allocation
- Basic setup for all the devices

Task 2:

- Security measures on each device
- Designing zones of trust
- Implementing ZPF
- ACL setup

Task 3:

- Site-to-Site VPN
- IPsec
- AAA setup

Task 1: Network Design and Configuration

1.1 Network topology

A. **Justification:**

1. All the various departments are segmented into various VLANs. This is to improve security, network performance and scalability.
2. Overall network is configured in the hybrid topology with star for connecting all the VLANs.
3. Being a proof-of-concept design, all the VLANs include just a single PC to test connectivity tests, a Wireless access point and a single Laptop to demonstrate the wireless connectivity.
4. All the VLANs except the server room VLAN includes a Wireless Access Point to WiFi connections. All of these have unique SSID for that department and unique password.
5. All these VLAN connect to the core switch which is a multi-layer switch. This with connecting router provides the inter-VLAN routing using router-on-stick method.
6. Server room is installed with 4 servers. The functionalities of the servers are not configured as it goes out of scope of the network security engineer. The setup is expected from the individual server owner teams. However, connectivity is being established for the servers from other devices.
7. The core router connects to the outer network where there is a gateway router which has zoning and ZPF implemented on it.
8. The design also includes a remote site (on the left of the design) which is connecting to the main site via Site-to-Site VPN. IPSec is also implemented for added security.
9. Internet connection setup and ISP is considered out of scope of this report. However, provisions are made from the gateway router for the connection if needed.
10. Design is structured to visualize the East-West (Internal) and North-South (Bidirectional traffic to internet).
11. Webcam is also configured in the conference room for video conferencing.

B. **Device selection and reasoning:**

1. Switches:
   a. **Department VLAN switches: Cisco 2960**
   Simple and cost-effective switch for small requirements like department VLANs.
   b. **Core switch: Cisco 3650-24PS**
   High density of Gigabit ports which would be helpful in the bandwidth requirements of all the VLAN traffic. It also has the best potential for future scalability.
2. Routers:
   a. **Main/Core router: Cisco 2911**
   Simple and easy router for setup and internal routing purpose. This also has a additional Gigabit ports which could be used in future expansion.
   b. **Gateway/External Router: ISR4331**
   Out of the box VPN capability as well as ideal for the zoning configurations required.

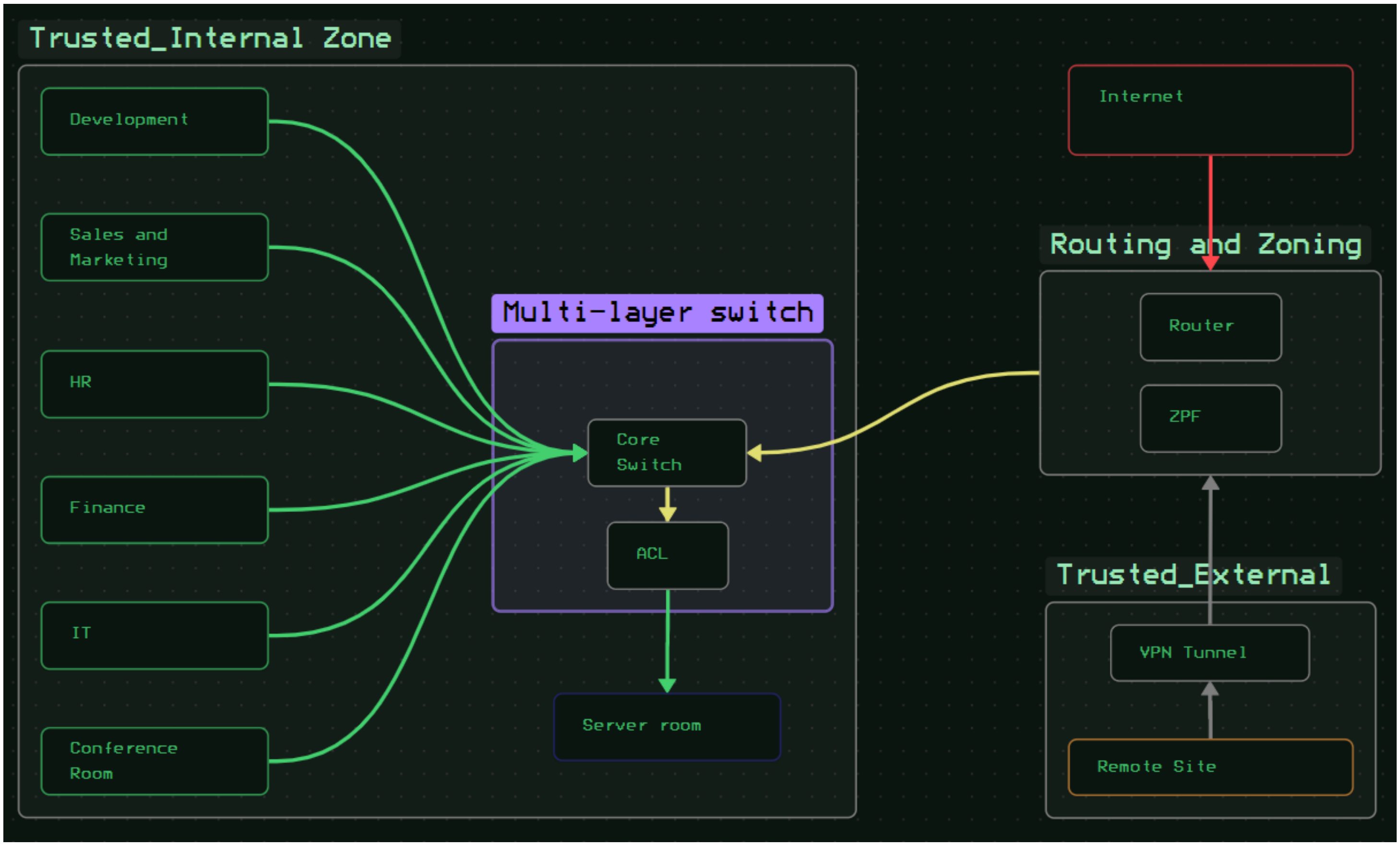


Fig 1. High level Topology of Network

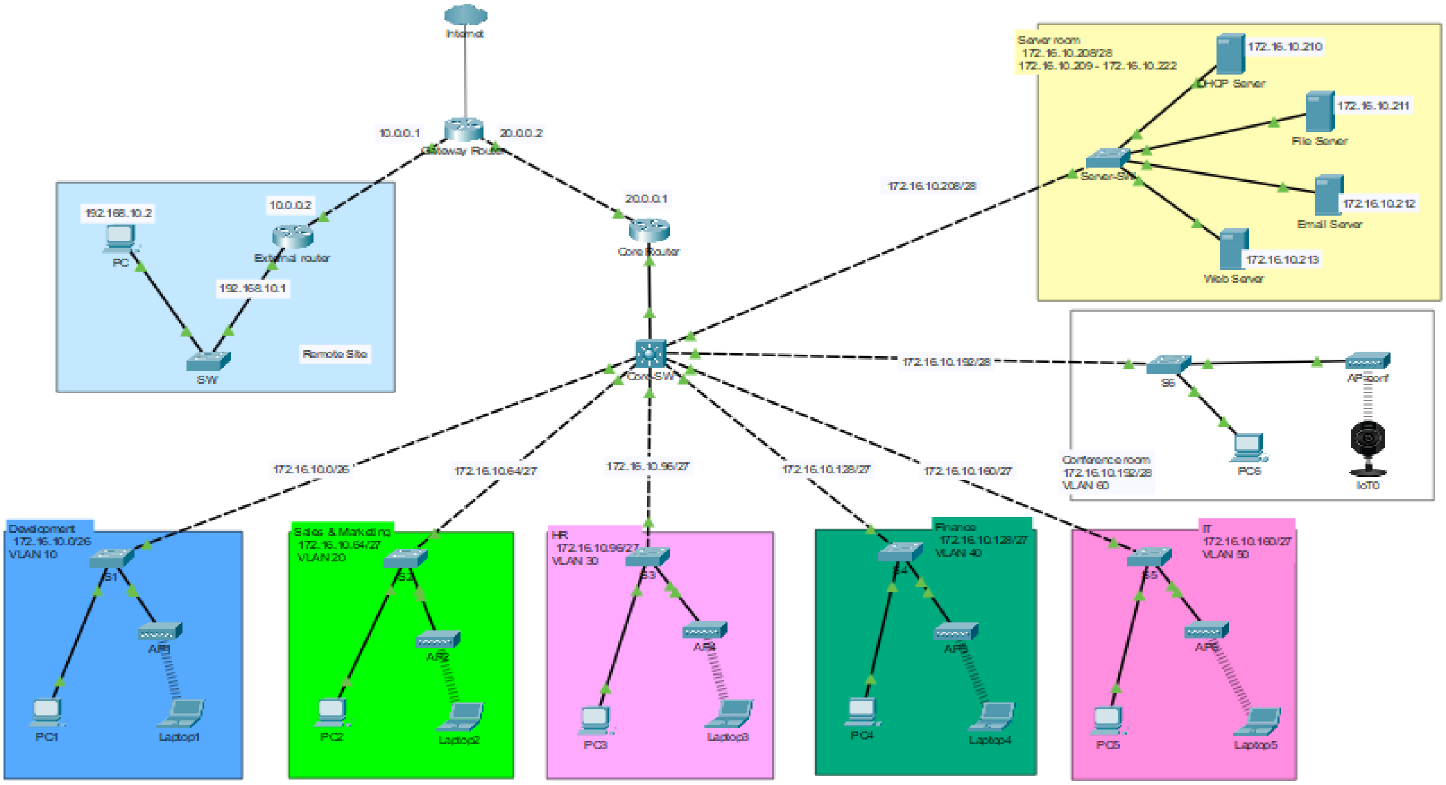


Fig 2. Detailed Network design in packet tracer

1.2 Subnetting and IP Addressing

A. Justification:

Subnets are designed with the IP requirement of each department.

B. Configuration:

Department Name	Hosts needed	Network address	Mask	Usable IPs	Usable range	Broadcast IP
Development	50	172.16.10.0/26	255.255.255.192	62	172.16.10.1 - 172.16.10.62	172.16.10.63
Sales and Marketing	30	172.16.10.64/27	255.255.255.224	30	172.16.10.65 - 172.16.10.94	172.16.10.95
HR	25	172.16.10.96/27	255.255.255.224	30	172.16.10.97 - 172.16.10.126	172.16.10.127
Finance	25	172.16.10.128/27	255.255.255.224	30	172.16.10.129 - 172.16.10.158	172.16.10.159
IT	20	172.16.10.160/27	255.255.255.224	30	172.16.10.161 - 172.16.10.190	172.16.10.191
Conference	8	172.16.10.192/28	255.255.255.240	14	172.16.10.193 - 172.16.10.206	172.16.10.207
Server	8	172.16.10.208/28	255.255.255.240	14	172.16.10.209 - 172.16.10.222	172.16.10.223
Extra for NWs	8	172.16.10.224/28	255.255.255.240	14	172.16.10.225 - 172.16.10.238	172.16.10.239

Table 1. Network segmentation and VLSM table

C. Verification:

All the subnets have enough usable IPs to accommodate all the devices.

1.3 VLAN Configuration

A. Justification:

1. All the departments are segmented into individual VLANs for the security, scalability and performance.

2. All the VLAN switches are connected to the core switch via Gigabit ports for performance and bandwidth. And all the end devices are connected to the FastEthernet ports for limited but enough connection speed and bandwidth.

3. All the connections to the core switch are trunked for the routing and inter-VLAN connections.

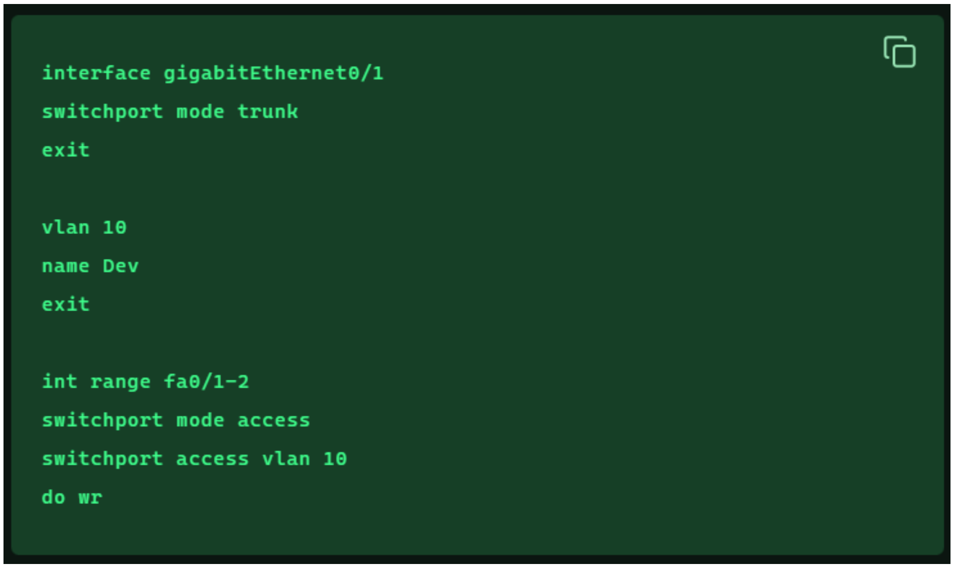
4. All the FastEthernet ports are in the access mode for internal connections to the end devices.

VLAN ID	Name	Department
10	Dev	Development
20	S&M	Sales and marketing
30	HR	HR
40	Fin	Finance
50	IT	IT
60	Conf	Conference room
70	Serv	Server room

Table 2. VLANs

B. Configuration:

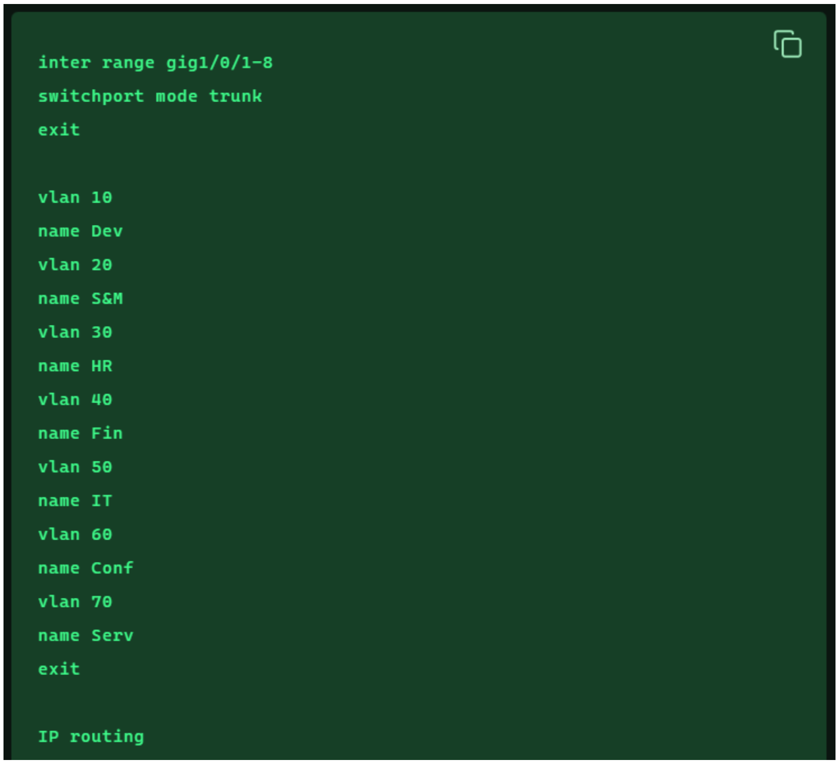
Config for the department VLAN switches.



```
interface gigabitEthernet0/1
switchport mode trunk
exit

vlan 10
name Dev
exit

int range fa0/1-2
switchport mode access
switchport access vlan 10
do wr
```

Fig 3. VLAN config of switch

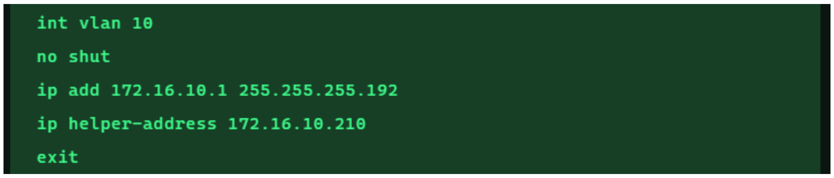
Config for the Core switch (Multilayer switch)



```
inter range gig1/0/1-8
switchport mode trunk
exit

vlan 10
name Dev
vlan 20
name S&M
vlan 30
name HR
vlan 40
name Fin
vlan 50
name IT
vlan 60
name Conf
vlan 70
name Serv
exit

IP routing
```

Fig 4. VLAN config of core switch

Config for one of the VLAN with helper address for DHCP.

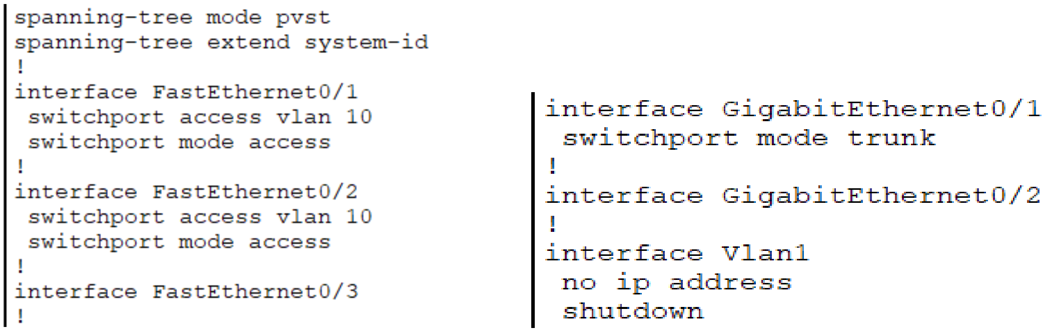


```
int vlan 10
no shut
ip add 172.16.10.1 255.255.255.192
ip helper-address 172.16.10.210
exit
```

Fig 5. Address mapping and helper address setup

C. Verification:

Results from one of the department switches.

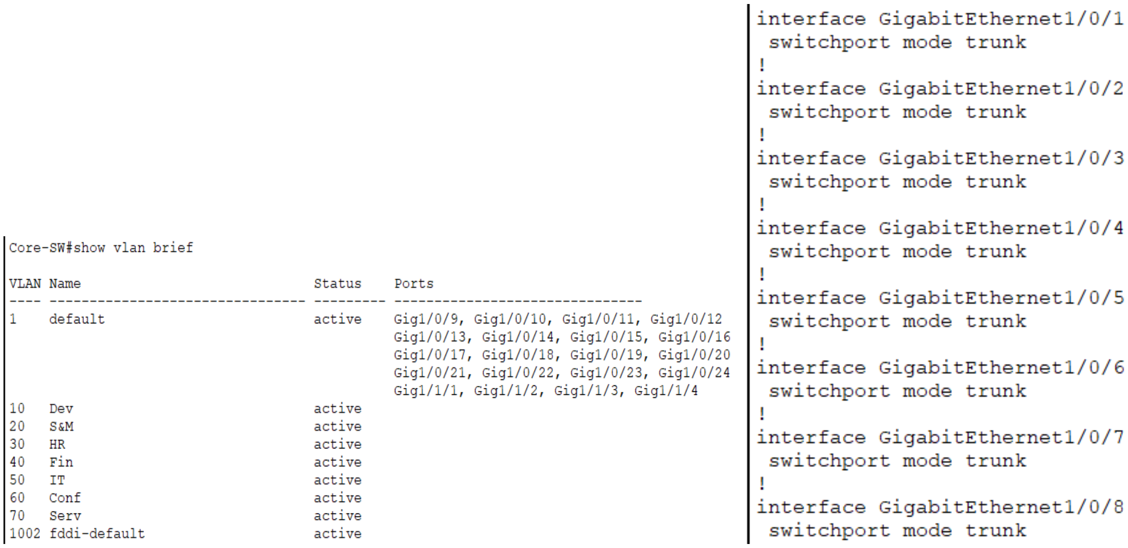


```
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
!
```

```
interface GigabitEthernet0/1
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
```

Fig 6. VLAN results from Dev VLAN

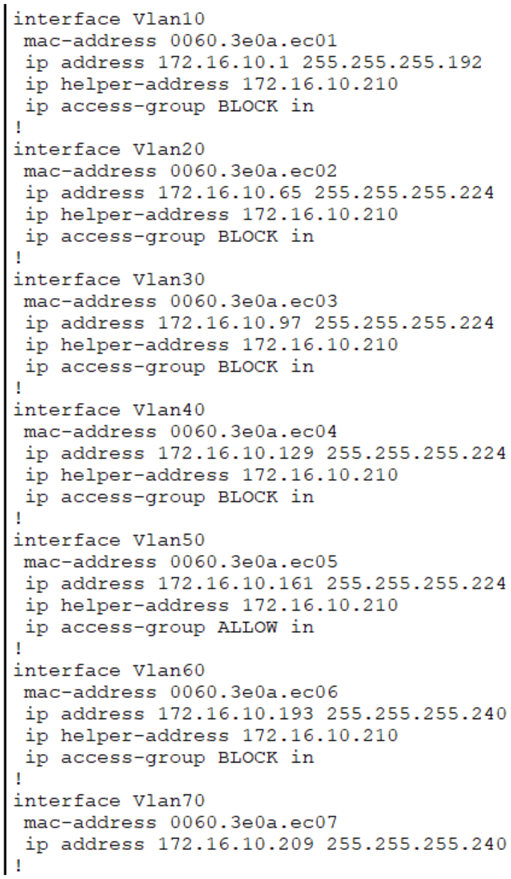
Results from the core switch:



```
Core-SW#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- ------------------------------
1    default                          active    Gig1/0/9, Gig1/0/10, 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   Dev                              active
20   S&M                              active
30   HR                               active
40   Fin                              active
50   IT                               active
60   Conf                             active
70   Serv                             active
1002 fddi-default                     active
```

```
interface GigabitEthernet1/0/1
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport mode trunk
!
interface GigabitEthernet1/0/3
 switchport mode trunk
!
interface GigabitEthernet1/0/4
 switchport mode trunk
!
interface GigabitEthernet1/0/5
 switchport mode trunk
!
interface GigabitEthernet1/0/6
 switchport mode trunk
!
interface GigabitEthernet1/0/7
 switchport mode trunk
!
interface GigabitEthernet1/0/8
 switchport mode trunk
```

Fig 7a. VLANs on core switch



```
interface Vlan10
 mac-address 0060.3e0a.ec01
 ip address 172.16.10.1 255.255.255.192
 ip helper-address 172.16.10.210
 ip access-group BLOCK in
!
interface Vlan20
 mac-address 0060.3e0a.ec02
 ip address 172.16.10.65 255.255.255.224
 ip helper-address 172.16.10.210
 ip access-group BLOCK in
!
interface Vlan30
 mac-address 0060.3e0a.ec03
 ip address 172.16.10.97 255.255.255.224
 ip helper-address 172.16.10.210
 ip access-group BLOCK in
!
interface Vlan40
 mac-address 0060.3e0a.ec04
 ip address 172.16.10.129 255.255.255.224
 ip helper-address 172.16.10.210
 ip access-group BLOCK in
!
interface Vlan50
 mac-address 0060.3e0a.ec05
 ip address 172.16.10.161 255.255.255.224
 ip helper-address 172.16.10.210
 ip access-group ALLOW in
!
interface Vlan60
 mac-address 0060.3e0a.ec06
 ip address 172.16.10.193 255.255.255.240
 ip helper-address 172.16.10.210
 ip access-group BLOCK in
!
interface Vlan70
 mac-address 0060.3e0a.ec07
 ip address 172.16.10.209 255.255.255.240
!
```

Fig 7b. VLANs on core switch

1.4 Inter-VLAN Routing

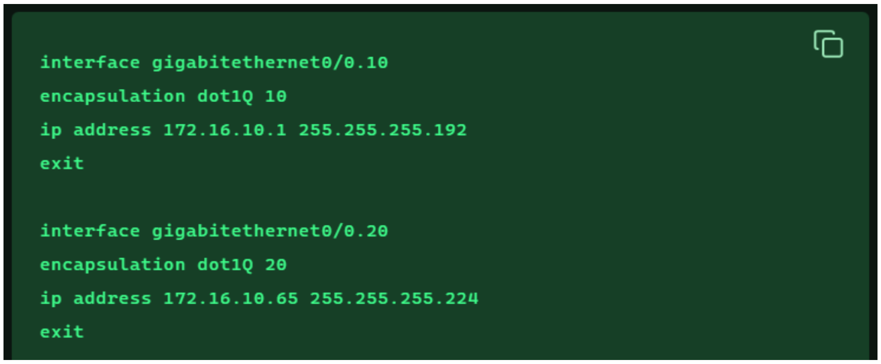
A. Justification:

Router-on-stick method was used for the inter-VLAN routing.

1. Devices should be able to reach out to server for various tasks.
2. IT department also wants to access all the departments.

B. Configuration:

1. Some of the config on the core router:

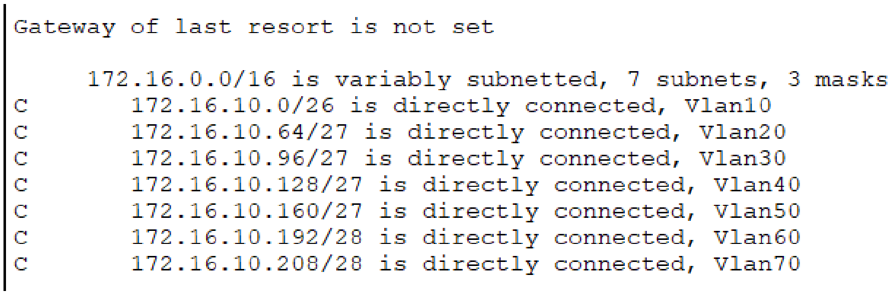


```
interface gigabitethernet0/0.10
encapsulation dot1Q 10
ip address 172.16.10.1 255.255.255.192
exit

interface gigabitethernet0/0.20
encapsulation dot1Q 20
ip address 172.16.10.65 255.255.255.224
exit
```

Fig 8. Sub-interface config on Core router

C. Verification:

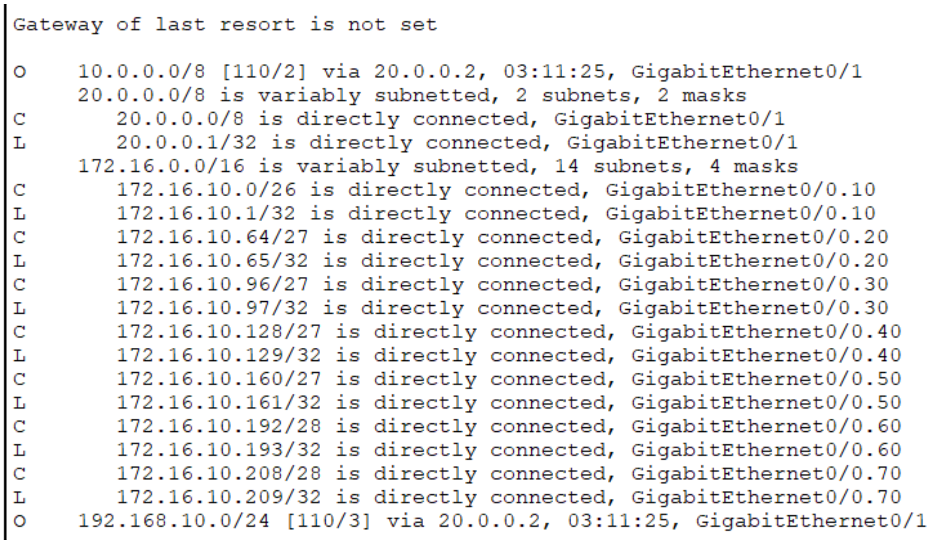
1. Routes mapped on the core switch.



```
Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 7 subnets, 3 masks
C       172.16.10.0/26 is directly connected, Vlan10
C       172.16.10.64/27 is directly connected, Vlan20
C       172.16.10.96/27 is directly connected, Vlan30
C       172.16.10.128/27 is directly connected, Vlan40
C       172.16.10.160/27 is directly connected, Vlan50
C       172.16.10.192/28 is directly connected, Vlan60
C       172.16.10.208/28 is directly connected, Vlan70
```

Fig 9. Core switch routes

C. Routes on the Core router:



```
Gateway of last resort is not set

O    10.0.0.0/8 [110/2] via 20.0.0.2, 03:11:25, GigabitEthernet0/1
     20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       20.0.0.0/8 is directly connected, GigabitEthernet0/1
L       20.0.0.1/32 is directly connected, GigabitEthernet0/1
     172.16.0.0/16 is variably subnetted, 14 subnets, 4 masks
C       172.16.10.0/26 is directly connected, GigabitEthernet0/0.10
L       172.16.10.1/32 is directly connected, GigabitEthernet0/0.10
C       172.16.10.64/27 is directly connected, GigabitEthernet0/0.20
L       172.16.10.65/32 is directly connected, GigabitEthernet0/0.20
C       172.16.10.96/27 is directly connected, GigabitEthernet0/0.30
L       172.16.10.97/32 is directly connected, GigabitEthernet0/0.30
C       172.16.10.128/27 is directly connected, GigabitEthernet0/0.40
L       172.16.10.129/32 is directly connected, GigabitEthernet0/0.40
C       172.16.10.160/27 is directly connected, GigabitEthernet0/0.50
L       172.16.10.161/32 is directly connected, GigabitEthernet0/0.50
C       172.16.10.192/28 is directly connected, GigabitEthernet0/0.60
L       172.16.10.193/32 is directly connected, GigabitEthernet0/0.60
C       172.16.10.208/28 is directly connected, GigabitEthernet0/0.70
L       172.16.10.209/32 is directly connected, GigabitEthernet0/0.70
O    192.168.10.0/24 [110/3] via 20.0.0.2, 03:11:25, GigabitEthernet0/1
```

Fig 10. Core router routes

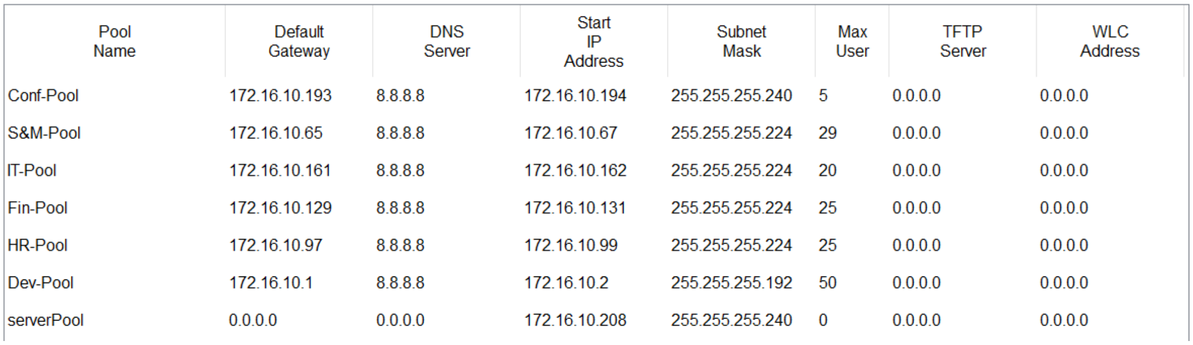
1.5 DHCP Configuration

A. Justification:

1. DHCP server setup is used for the IP allocation.
2. It provides a central management which simplifies IP allocation for all the devices.
3. For mobile devices like Laptop, dynamic allocation IP is required.
4. This should also reduce the errors and overlaps in manual static allocation.

B. Configuration:

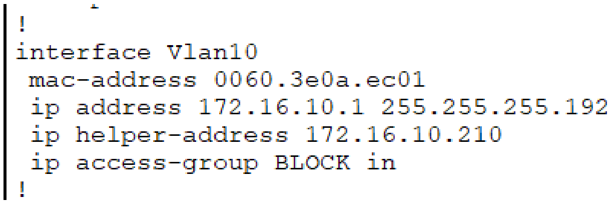
1. DHCP pools are configured on the DHCP server.



Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Conf-Pool	172.16.10.193	8.8.8.8	172.16.10.194	255.255.255.240	5	0.0.0.0	0.0.0.0
S&M-Pool	172.16.10.65	8.8.8.8	172.16.10.67	255.255.255.224	29	0.0.0.0	0.0.0.0
IT-Pool	172.16.10.161	8.8.8.8	172.16.10.162	255.255.255.224	20	0.0.0.0	0.0.0.0
Fin-Pool	172.16.10.129	8.8.8.8	172.16.10.131	255.255.255.224	25	0.0.0.0	0.0.0.0
HR-Pool	172.16.10.97	8.8.8.8	172.16.10.99	255.255.255.224	25	0.0.0.0	0.0.0.0
Dev-Pool	172.16.10.1	8.8.8.8	172.16.10.2	255.255.255.192	50	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	172.16.10.208	255.255.255.240	0	0.0.0.0	0.0.0.0

Fig 11. DHCP pools

2. Helper address is used on the core router to allow DHCPDISCOVER beacon to be sent out to server.

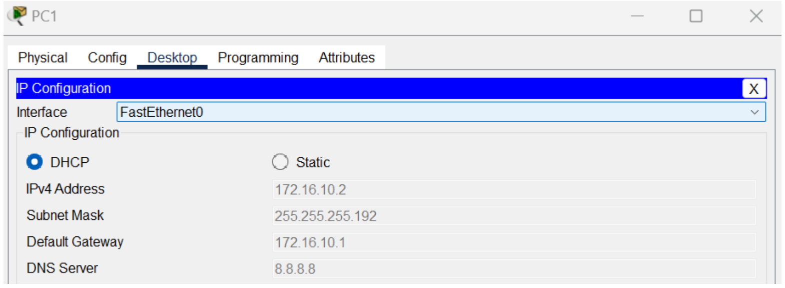


```
!
interface Vlan10
 mac-address 0060.3e0a.ec01
 ip address 172.16.10.1 255.255.255.192
 ip helper-address 172.16.10.210
 ip access-group BLOCK in
!
```

Fig 12. Helper address setup

D. Verification:

Dynamic IPs are being allocated to the end devices when requested.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address	172.16.10.2
Subnet Mask	255.255.255.192
Default Gateway	172.16.10.1
DNS Server	8.8.8.8

Fig 13. DHCP allocation

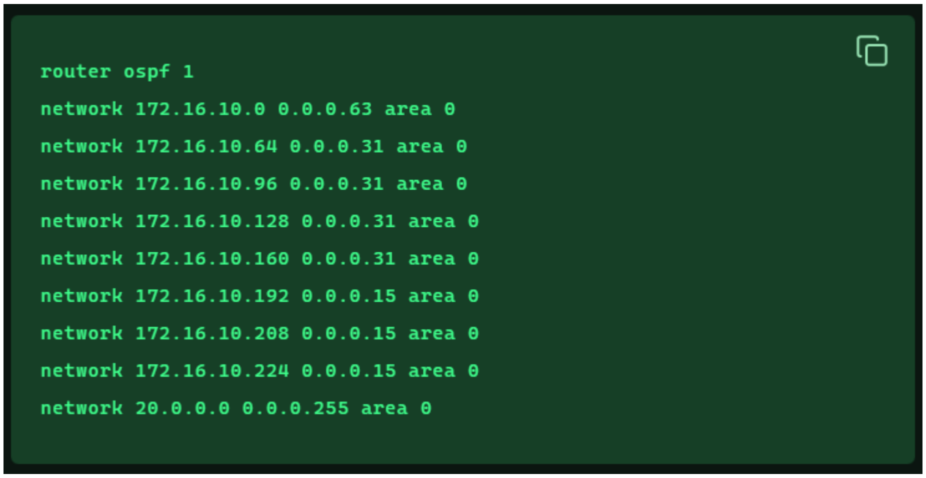
1.6 OSPF Routing Configuration

A. Justification:

1. As there are 3 routers used in the design to connect to the remote site and the main site, OSPF was used.
2. OSPF can adapt to network changes like addition of new VLAN to the network.
3. It also learns the adjacent routes which improves the scalability and efficiency in the routing.

B. Configuration:

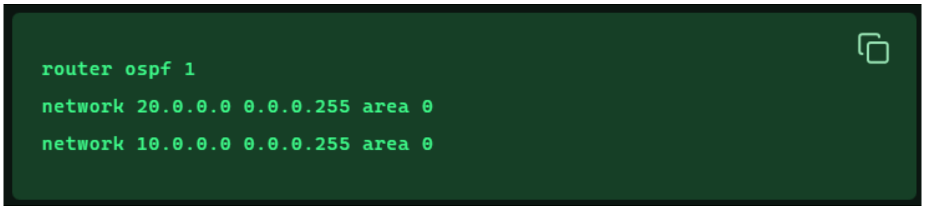
1. OSPF config on the main router:



```
router ospf 1
network 172.16.10.0 0.0.0.63 area 0
network 172.16.10.64 0.0.0.31 area 0
network 172.16.10.96 0.0.0.31 area 0
network 172.16.10.128 0.0.0.31 area 0
network 172.16.10.160 0.0.0.31 area 0
network 172.16.10.192 0.0.0.15 area 0
network 172.16.10.208 0.0.0.15 area 0
network 172.16.10.224 0.0.0.15 area 0
network 20.0.0.0 0.0.0.255 area 0
```

Fig 14. Main router OSPF config

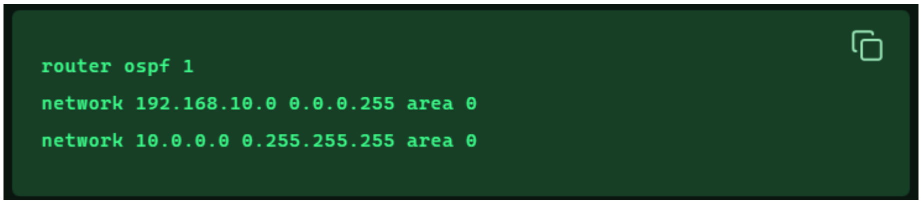
2. OSPF config on the gateway router:



```
router ospf 1
network 20.0.0.0 0.0.0.255 area 0
network 10.0.0.0 0.0.0.255 area 0
```

Fig 15. Gateway router OSPF config

3. OSPF config on the remote site router:

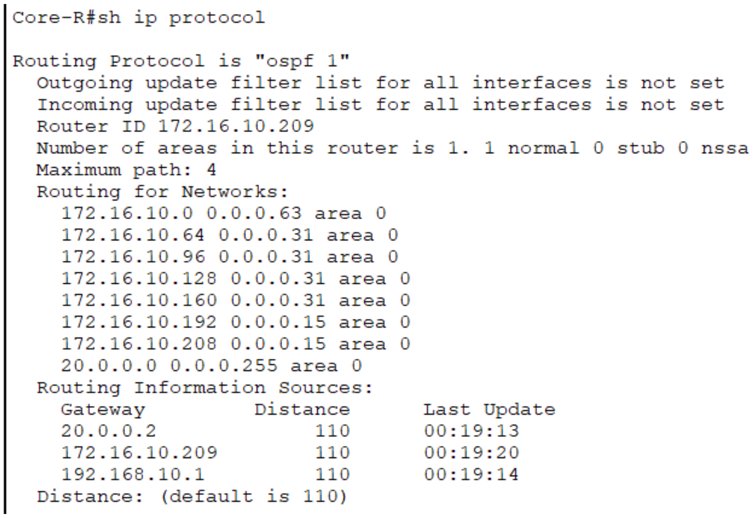


```
router ospf 1
network 192.168.10.0 0.0.0.255 area 0
network 10.0.0.0 0.255.255.255 area 0
```

Fig 16. External router OSPF config

C. Verification:

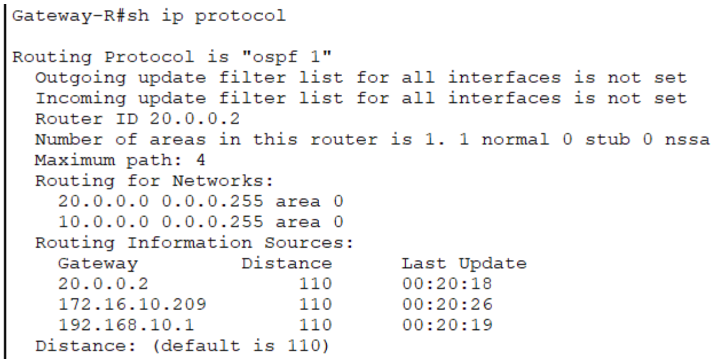
1. Verification on the main router



```
Core-R#sh ip protocol

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.10.209
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.10.0 0.0.0.63 area 0
    172.16.10.64 0.0.0.31 area 0
    172.16.10.96 0.0.0.31 area 0
    172.16.10.128 0.0.0.31 area 0
    172.16.10.160 0.0.0.31 area 0
    172.16.10.192 0.0.0.15 area 0
    172.16.10.208 0.0.0.15 area 0
    20.0.0.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    20.0.0.2             110      00:19:13
    172.16.10.209        110      00:19:20
    192.168.10.1         110      00:19:14
  Distance: (default is 110)
```

Fig 17. OSPF result on main router

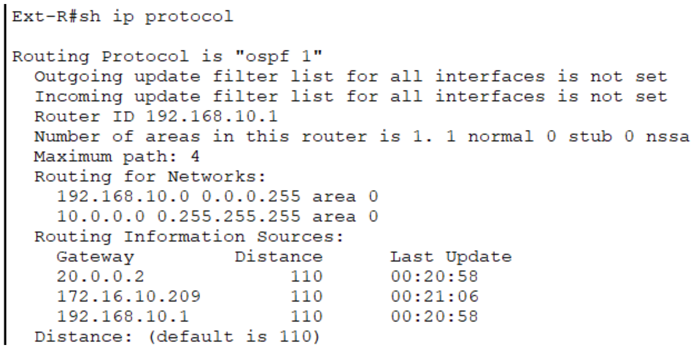
2. Verification on the gateway router:



```
Gateway-R#sh ip protocol

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 20.0.0.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    20.0.0.0 0.0.0.255 area 0
    10.0.0.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    20.0.0.2             110      00:20:18
    172.16.10.209        110      00:20:26
    192.168.10.1         110      00:20:19
  Distance: (default is 110)
```

Fig 18. OSPF result on gateway router

3. Verification on the external router:



```
Ext-R#sh ip protocol

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.10.0 0.0.0.255 area 0
    10.0.0.0 0.255.255.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    20.0.0.2             110      00:20:58
    172.16.10.209        110      00:21:06
    192.168.10.1         110      00:20:58
  Distance: (default is 110)
```

Fig 19. OSPF result on external router

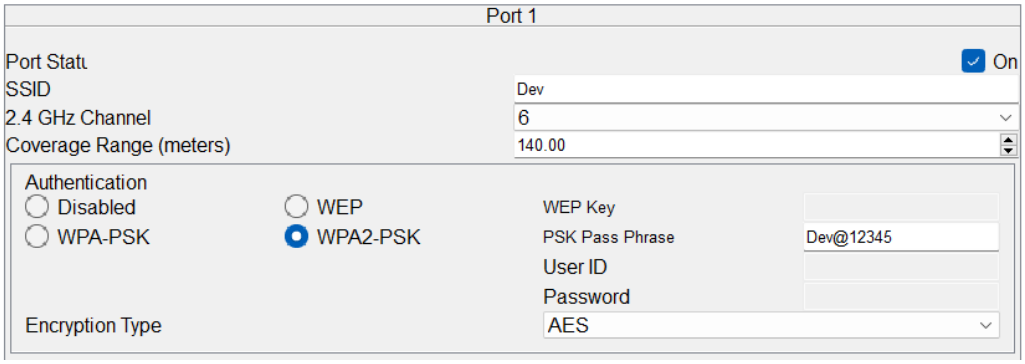
1.7 Wireless Network Configuration

A. Justification:

1. Wireless Access Points are implemented in each VLAN for wireless connectivity like WiFi.
2. SSID of each AP is setup to their departments with unique passwords.
3. WAP2-PSK is used for most possible secure connection setup.
4. Wireless module is used on the laptops for the connections.

B. Configuration:

Configuration on the wireless AP.



Port 1

Port Statı ☑ On

SSID: Dev

2.4 GHz Channel: 6

Coverage Range (meters): 140.00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

WEP Key:

PSK Pass Phrase: Dev@12345

User ID:

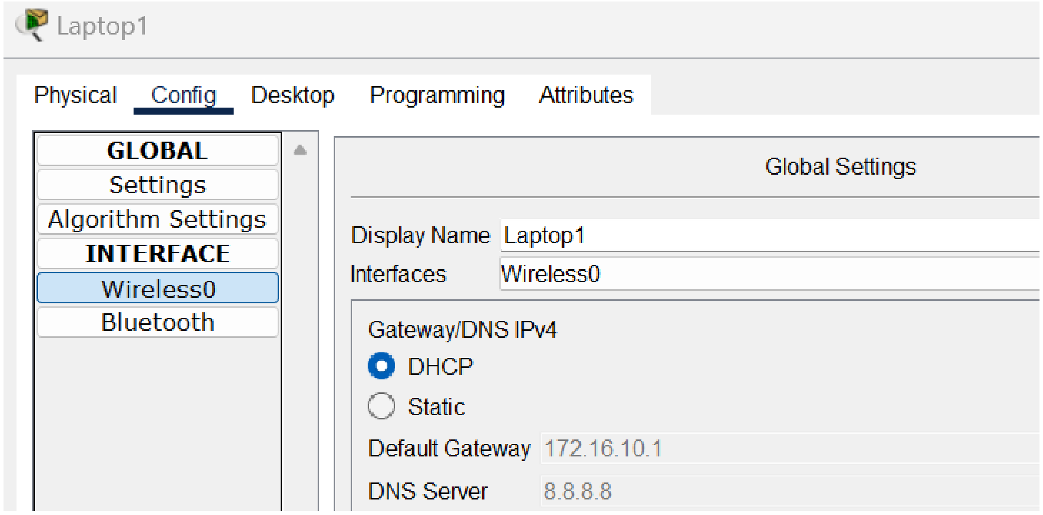
Password:

Encryption Type: AES

Fig 20. WiFi setup

C. Verification:

Results from the laptop showing the active connection to the WiFi.



Laptop1

Global Settings

Display Name: Laptop1

Interfaces: Wireless0

Gateway/DNS IPv4

● DHCP

○ Static

Default Gateway: 172.16.10.1

DNS Server: 8.8.8.8

Fig 21. DHCP allocation on laptop

Task 2: Security and Zones of Trust

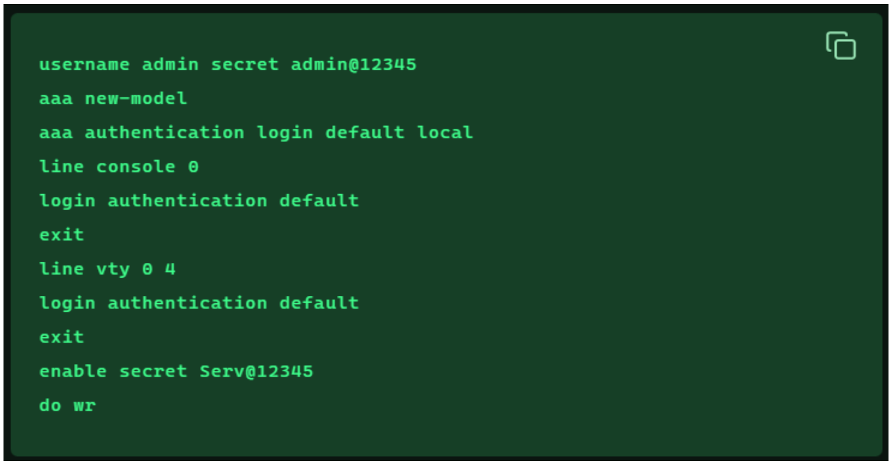
2.1 Security Measures on Network Devices

A. Justification:

1. All the Network devices have “enable password” configured on them for additional security apart from the AAA setup.
2. Security measures are not implemented on the gateway router or remote site router as these would go out of scope for the network security engineer for the current organization.
3. Only main router would reach out to the TACACS server for the authentication.
4. Again, as it is just a proof-of-concept design, convenient passwords were selected to make configuration, designing and testing easy. Stronger password has to be assigned when the NW is being implemented in real life.

B. Configuration:

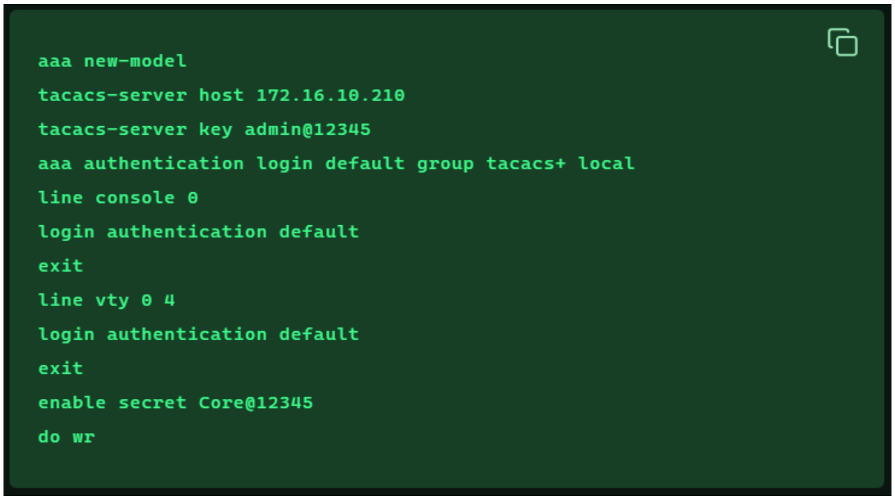
Example config on one of the departmental switches.



```
username admin secret admin@12345
aaa new-model
aaa authentication login default local
line console 0
login authentication default
exit
line vty 0 4
login authentication default
exit
enable secret Serv@12345
do wr
```

Fig 22. Security config on switch

Config on the main router:

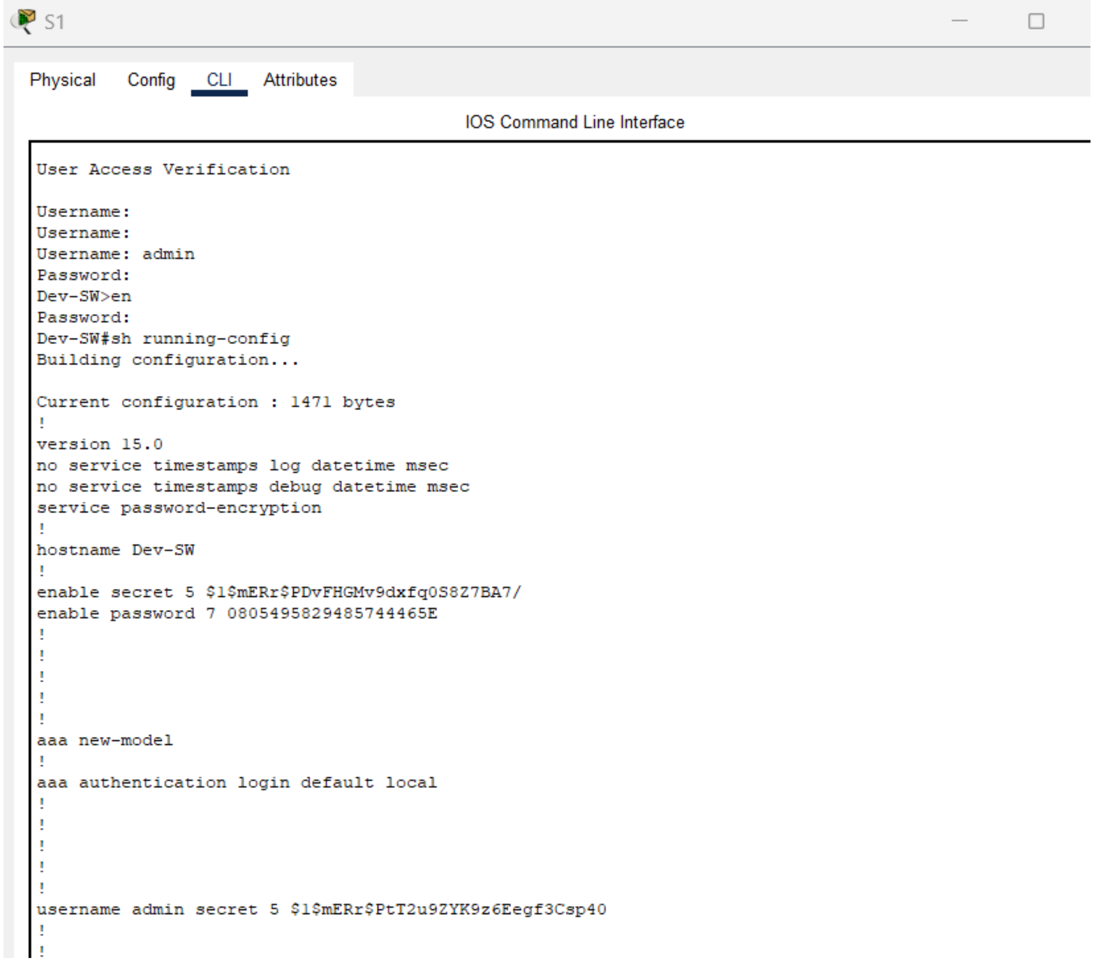


```
aaa new-model
tacacs-server host 172.16.10.210
tacacs-server key admin@12345
aaa authentication login default group tacacs+ local
line console 0
login authentication default
exit
line vty 0 4
login authentication default
exit
enable secret Core@12345
do wr
```

Fig 23. Security config on core router

C. Verification:

1. Authentication required on the departmental switch:



```
User Access Verification

Username:
Username:
Username: admin
Password:
Dev-SW>en
Password:
Dev-SW#sh running-config
Building configuration...

Current configuration : 1471 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Dev-SW
!
enable secret 5 $1$mERr$PDvFHGMv9dxfq0S8Z7BA7/
enable password 7 0805495829485744465E
!
!
!
!
!
aaa new-model
!
aaa authentication login default local
!
!
!
!
!
username admin secret 5 $1$mERr$PtT2u9ZYK9z6Eegf3Csp40
!
!
```

Fig 24. Security measures on the switch

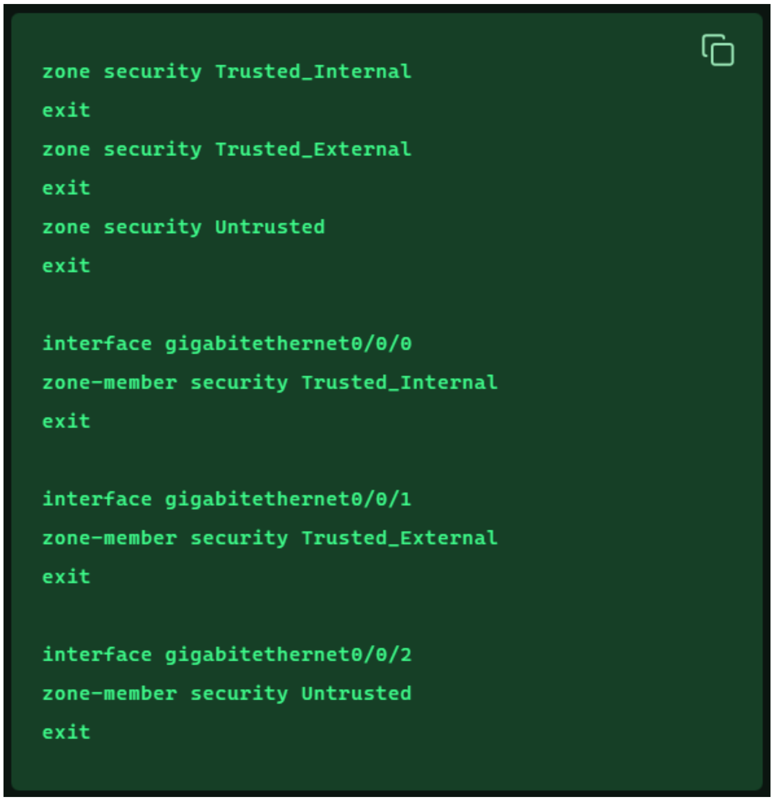
2.2 Zones of Trust Design and ZPF

A. Justification:

1. 3 distinguished zones are defined for the given network.
    1. Trusted_Internal --------- For Internal NW
    2. Trusted_External ---------For Remote site
    3. Untrusted ----------------- For Internet traffic
2. Both main site and remote site are being considered as the trusted as the traffic origin is definable and known.
3. Configuration for the internet traffic is also provisioned however testing is not performed as internet traffic processing was out of scope.
4. Various inspection and polices are set in class maps and policy maps as shown below.

B. Configuration:

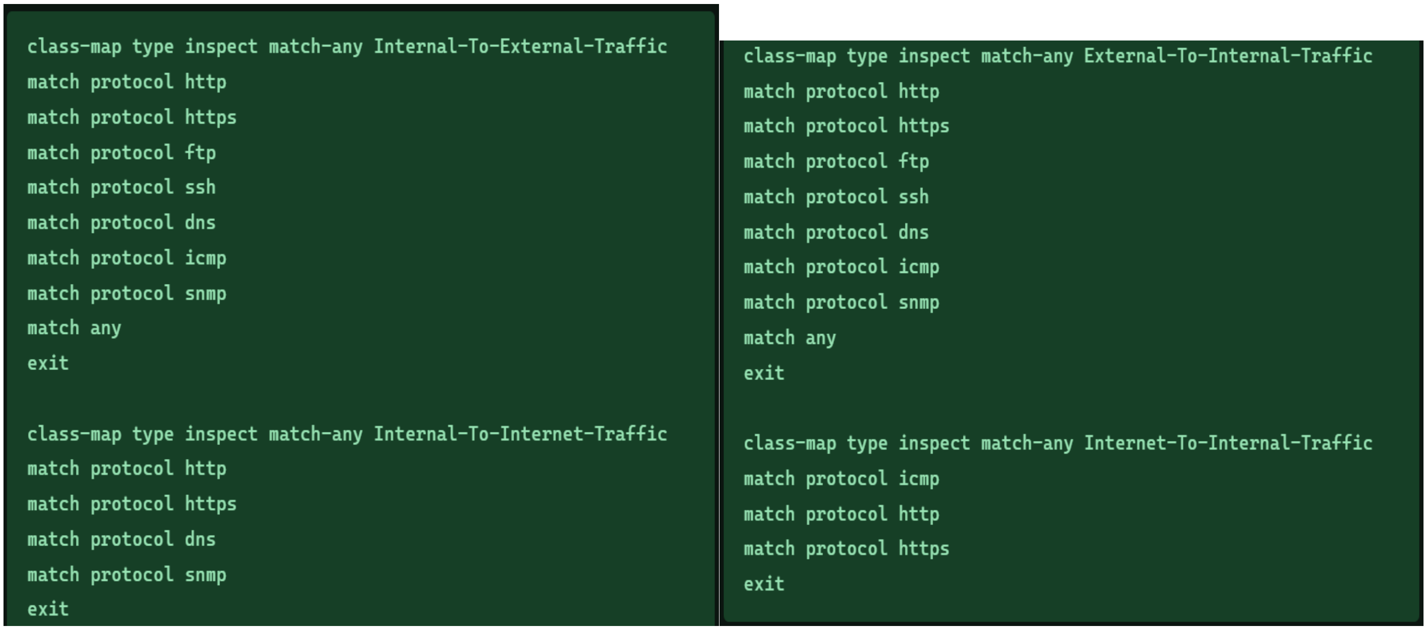
1. Zone creation and assigning Interfaces to Zones



```
zone security Trusted_Internal
exit
zone security Trusted_External
exit
zone security Untrusted
exit

interface gigabitethernet0/0/0
zone-member security Trusted_Internal
exit

interface gigabitethernet0/0/1
zone-member security Trusted_External
exit

interface gigabitethernet0/0/2
zone-member security Untrusted
exit
```

Fig 25. Zone assigning

2. Class maps:

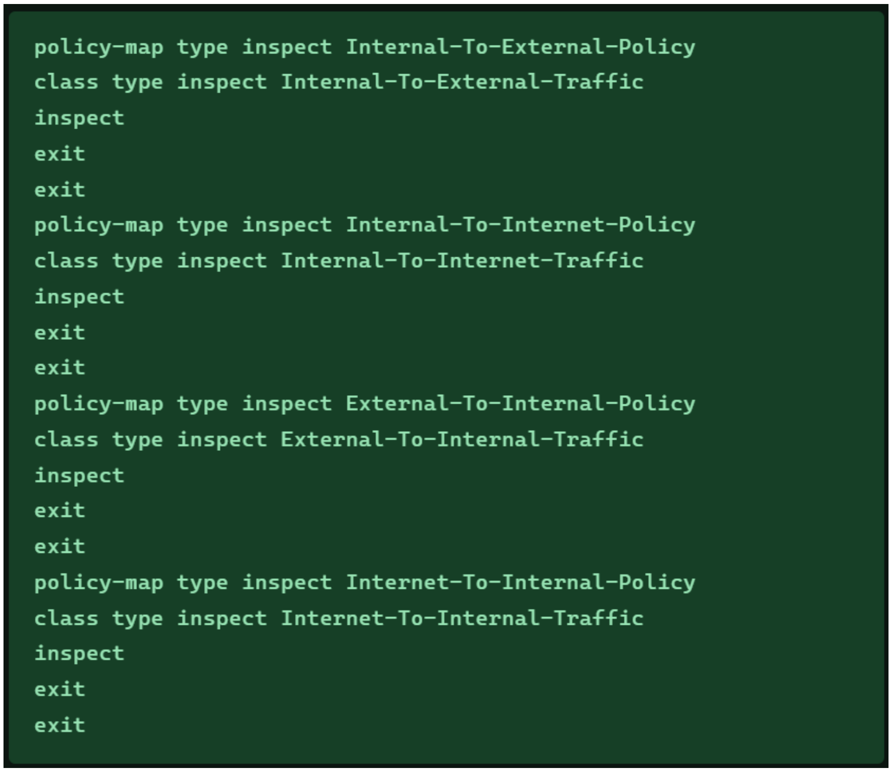


```
class-map type inspect match-any Internal-To-External-Traffic
match protocol http
match protocol https
match protocol ftp
match protocol ssh
match protocol dns
match protocol icmp
match protocol snmp
match any
exit

class-map type inspect match-any Internal-To-Internet-Traffic
match protocol http
match protocol https
match protocol dns
match protocol snmp
exit
```

```
class-map type inspect match-any External-To-Internal-Traffic
match protocol http
match protocol https
match protocol ftp
match protocol ssh
match protocol dns
match protocol icmp
match protocol snmp
match any
exit

class-map type inspect match-any Internet-To-Internal-Traffic
match protocol icmp
match protocol http
match protocol https
exit
```

Fig 26. Class maps

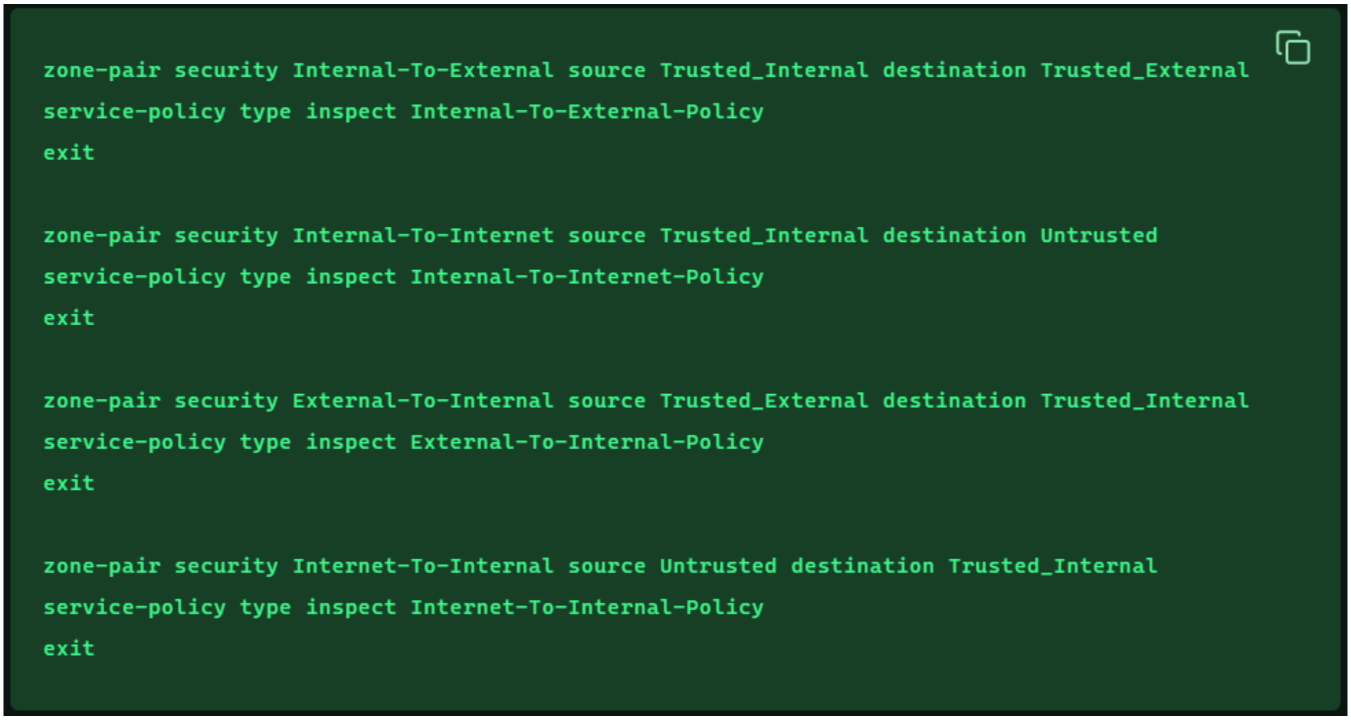
3. Policy maps:



```
policy-map type inspect Internal-To-External-Policy
class type inspect Internal-To-External-Traffic
inspect
exit
exit
policy-map type inspect Internal-To-Internet-Policy
class type inspect Internal-To-Internet-Traffic
inspect
exit
exit
policy-map type inspect External-To-Internal-Policy
class type inspect External-To-Internal-Traffic
inspect
exit
exit
policy-map type inspect Internet-To-Internal-Policy
class type inspect Internet-To-Internal-Traffic
inspect
exit
exit
```

Fig 27. Policy maps

4. Zone pairing:

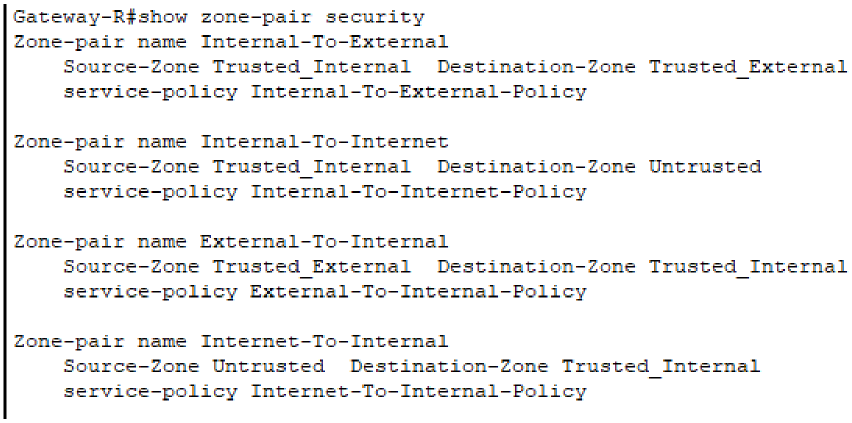


```
zone-pair security Internal-To-External source Trusted_Internal destination Trusted_External
service-policy type inspect Internal-To-External-Policy
exit

zone-pair security Internal-To-Internet source Trusted_Internal destination Untrusted
service-policy type inspect Internal-To-Internet-Policy
exit

zone-pair security External-To-Internal source Trusted_External destination Trusted_Internal
service-policy type inspect External-To-Internal-Policy
exit

zone-pair security Internet-To-Internal source Untrusted destination Trusted_Internal
service-policy type inspect Internet-To-Internal-Policy
exit
```

Fig 28. Zone pairing

C. Verification:

Zone pairing, class and policy maps are correctly implemented on the Gateway router.



```
Gateway-R#show zone-pair security
Zone-pair name Internal-To-External
    Source-Zone Trusted_Internal  Destination-Zone Trusted_External
    service-policy Internal-To-External-Policy

Zone-pair name Internal-To-Internet
    Source-Zone Trusted_Internal  Destination-Zone Untrusted
    service-policy Internal-To-Internet-Policy

Zone-pair name External-To-Internal
    Source-Zone Trusted_External  Destination-Zone Trusted_Internal
    service-policy External-To-Internal-Policy

Zone-pair name Internet-To-Internal
    Source-Zone Untrusted  Destination-Zone Trusted_Internal
    service-policy Internet-To-Internal-Policy
```

Fig 29. ZPF setup on gateway router

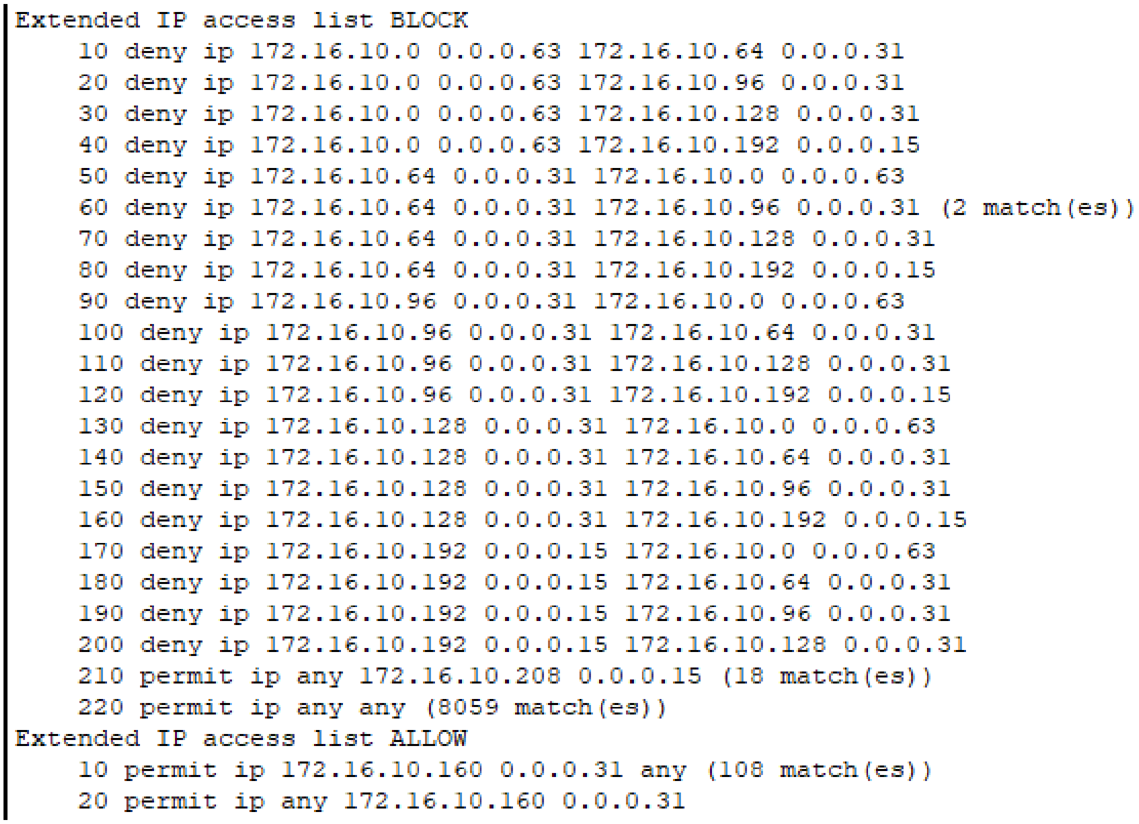
2.3 Access Control Lists (ACLs)

A. Justification:

1. To improve security, no two department should be able to access the devices of each other. Only exception to this is the IT department which needs access to all the devices. Also, all the departments should be able to reach out to all the servers.
2. For the above reason, 2 ACLs are implemented on the core switch which is responsible for the last jump routing for all the VLANs.
3. 2 ACLs are configured, one for allowed connections and one for the block connections.
4. “BLOCK” ACL is designed for blocking all the connections except the connections to the servers and IT VLAN.
5. “ALLOW” ACL is set for the IT to access all the departments.

B. Configuration:

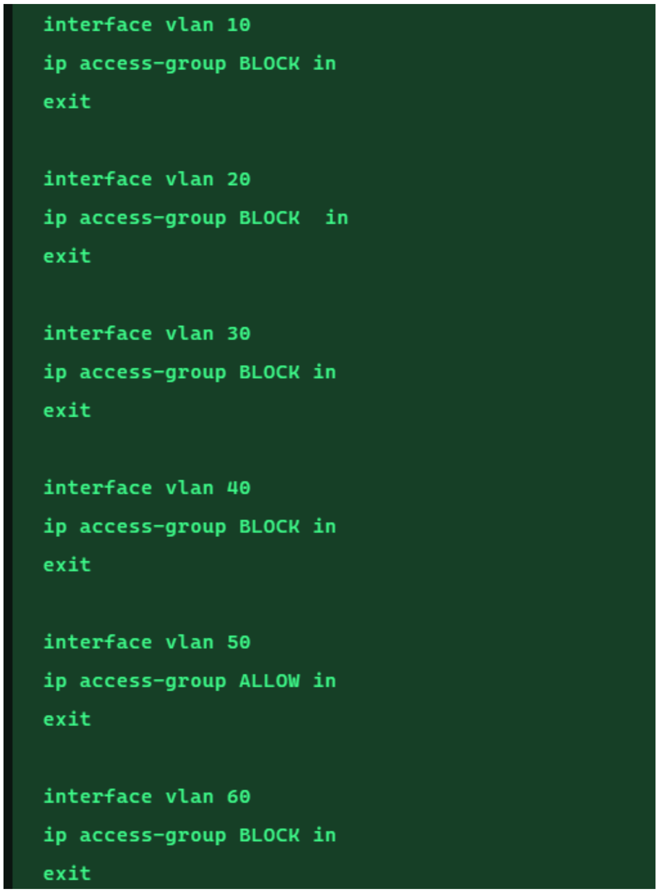
1. ACLs:



```
Extended IP access list BLOCK
    10 deny ip 172.16.10.0 0.0.0.63 172.16.10.64 0.0.0.31
    20 deny ip 172.16.10.0 0.0.0.63 172.16.10.96 0.0.0.31
    30 deny ip 172.16.10.0 0.0.0.63 172.16.10.128 0.0.0.31
    40 deny ip 172.16.10.0 0.0.0.63 172.16.10.192 0.0.0.15
    50 deny ip 172.16.10.64 0.0.0.31 172.16.10.0 0.0.0.63
    60 deny ip 172.16.10.64 0.0.0.31 172.16.10.96 0.0.0.31 (2 match(es))
    70 deny ip 172.16.10.64 0.0.0.31 172.16.10.128 0.0.0.31
    80 deny ip 172.16.10.64 0.0.0.31 172.16.10.192 0.0.0.15
    90 deny ip 172.16.10.96 0.0.0.31 172.16.10.0 0.0.0.63
    100 deny ip 172.16.10.96 0.0.0.31 172.16.10.64 0.0.0.31
    110 deny ip 172.16.10.96 0.0.0.31 172.16.10.128 0.0.0.31
    120 deny ip 172.16.10.96 0.0.0.31 172.16.10.192 0.0.0.15
    130 deny ip 172.16.10.128 0.0.0.31 172.16.10.0 0.0.0.63
    140 deny ip 172.16.10.128 0.0.0.31 172.16.10.64 0.0.0.31
    150 deny ip 172.16.10.128 0.0.0.31 172.16.10.96 0.0.0.31
    160 deny ip 172.16.10.128 0.0.0.31 172.16.10.192 0.0.0.15
    170 deny ip 172.16.10.192 0.0.0.15 172.16.10.0 0.0.0.63
    180 deny ip 172.16.10.192 0.0.0.15 172.16.10.64 0.0.0.31
    190 deny ip 172.16.10.192 0.0.0.15 172.16.10.96 0.0.0.31
    200 deny ip 172.16.10.192 0.0.0.15 172.16.10.128 0.0.0.31
    210 permit ip any 172.16.10.208 0.0.0.15 (18 match(es))
    220 permit ip any any (8059 match(es))
Extended IP access list ALLOW
    10 permit ip 172.16.10.160 0.0.0.31 any (108 match(es))
    20 permit ip any 172.16.10.160 0.0.0.31
```

Fig 30. ACLs

2. ACLs applied to each VLAN:

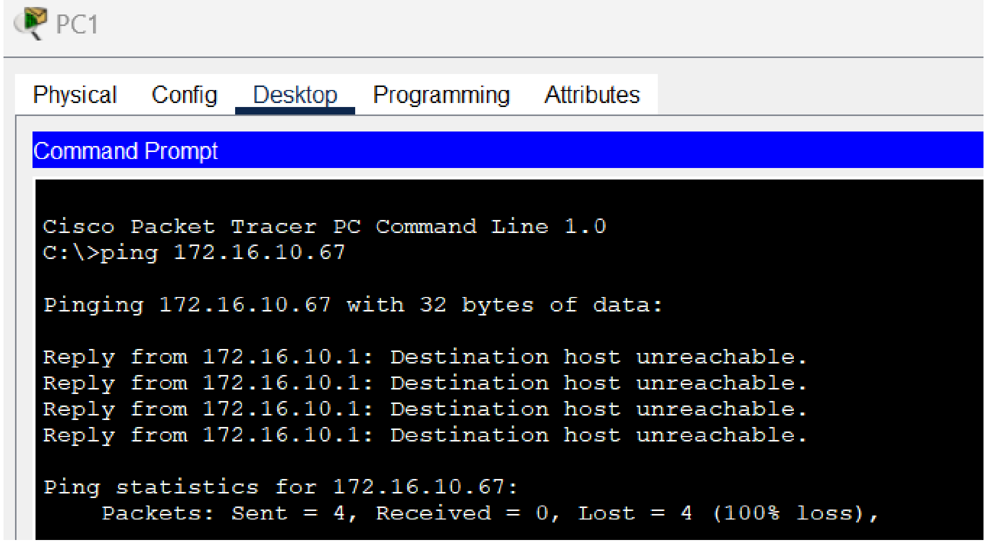


```
interface vlan 10
ip access-group BLOCK in
exit

interface vlan 20
ip access-group BLOCK  in
exit

interface vlan 30
ip access-group BLOCK in
exit

interface vlan 40
ip access-group BLOCK in
exit

interface vlan 50
ip access-group ALLOW in
exit

interface vlan 60
ip access-group BLOCK in
exit
```

Fig 31. ACL application to VLANs

C. Verification:

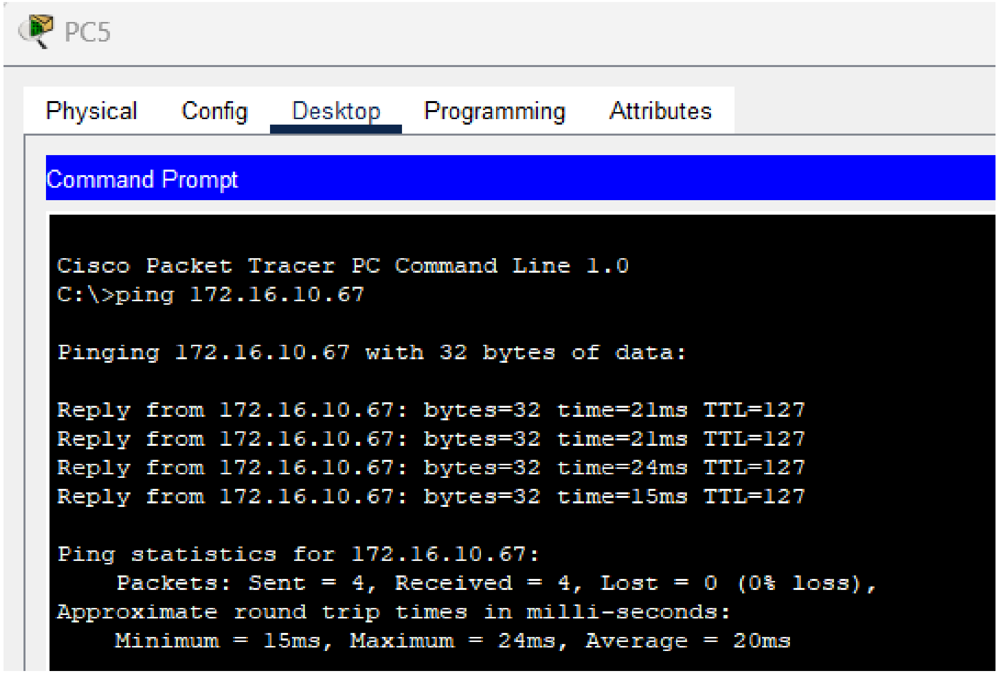
1. Connected not working from the PC from Dev VLAN to the S&M VLAN:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.10.67

Pinging 172.16.10.67 with 32 bytes of data:

Reply from 172.16.10.1: Destination host unreachable.
Reply from 172.16.10.1: Destination host unreachable.
Reply from 172.16.10.1: Destination host unreachable.
Reply from 172.16.10.1: Destination host unreachable.

Ping statistics for 172.16.10.67:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fig 32. ACL refusing the connection between VLANs

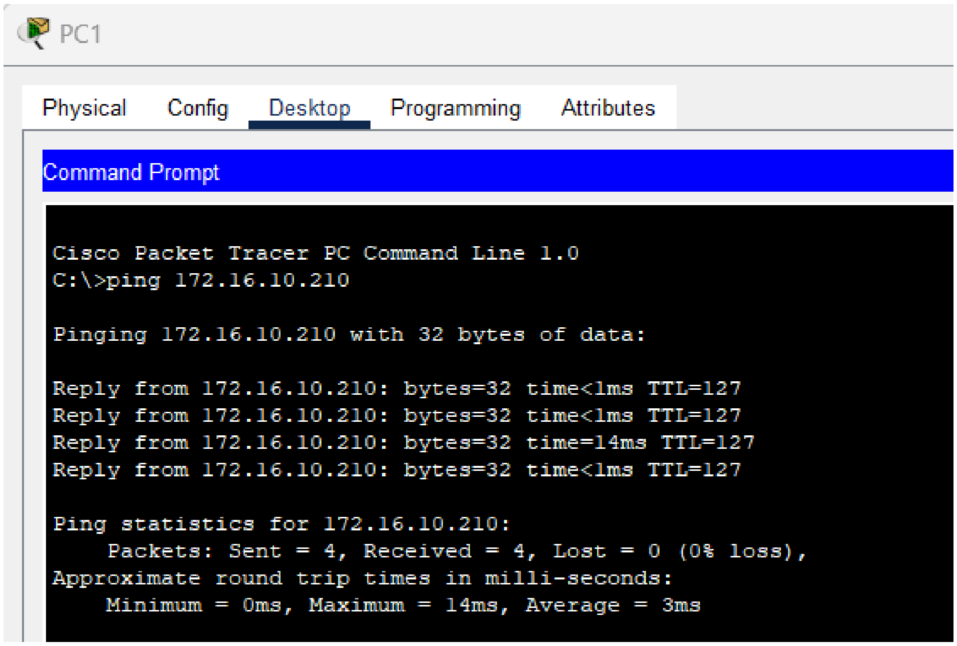
2. Connection working from the IT department.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.10.67

Pinging 172.16.10.67 with 32 bytes of data:

Reply from 172.16.10.67: bytes=32 time=21ms TTL=127
Reply from 172.16.10.67: bytes=32 time=21ms TTL=127
Reply from 172.16.10.67: bytes=32 time=24ms TTL=127
Reply from 172.16.10.67: bytes=32 time=15ms TTL=127

Ping statistics for 172.16.10.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 24ms, Average = 20ms
```

Fig 33a. ACL allowing traffic from IT

3. Traffic is flowing towards the DHCP server from the Dev PC.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.10.210

Pinging 172.16.10.210 with 32 bytes of data:

Reply from 172.16.10.210: bytes=32 time<1ms TTL=127
Reply from 172.16.10.210: bytes=32 time<1ms TTL=127
Reply from 172.16.10.210: bytes=32 time=14ms TTL=127
Reply from 172.16.10.210: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.10.210:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 3ms
```

Fig 33b. ACL allowing traffic from Dev PC to Servers

Task 3: Advanced Security Configuration

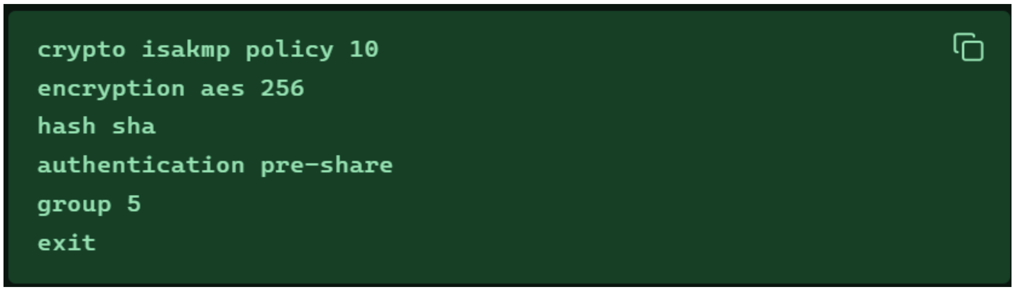
3.1 Site-to-Site VPN Configuration (IPsec)

A. Justification:

1. Remote site has to communicate to the servers in the main site. This is done using Site-to-Site VPN.

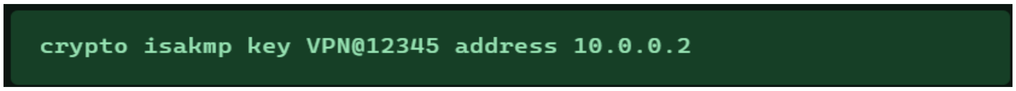
2. IPsec is used for the security. Also, AES-256 is used for the encryption and SHA for hashing.

B. Configuration:



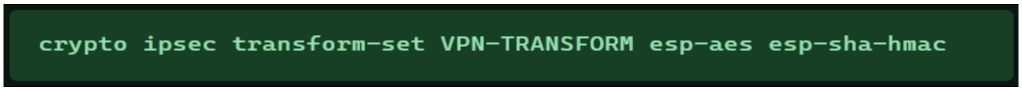
```
crypto isakmp policy 10
encryption aes 256
hash sha
authentication pre-share
group 5
exit
```

Fig 34. ISAKMP Policy



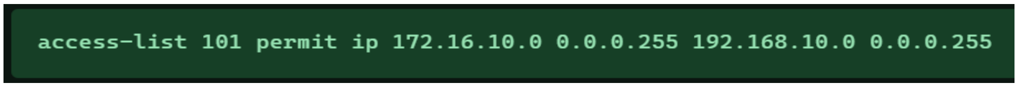
```
crypto isakmp key VPN@12345 address 10.0.0.2
```

Fig 35. Configuration of Pre-Shared Key



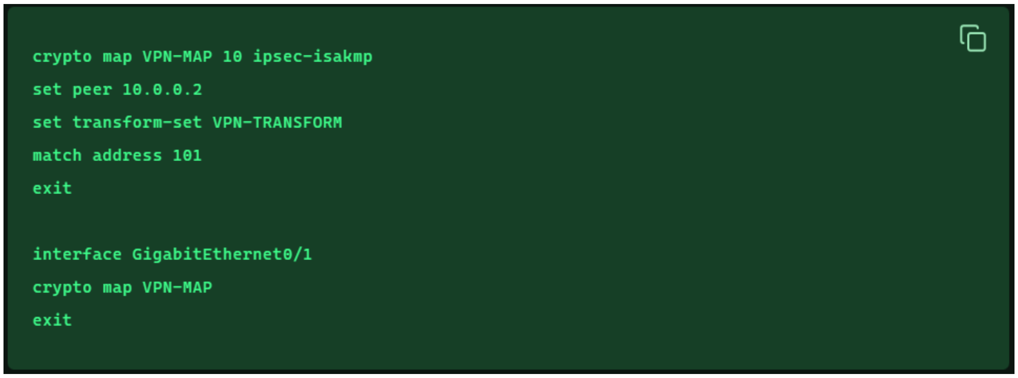
```
crypto ipsec transform-set VPN-TRANSFORM esp-aes esp-sha-hmac
```

Fig 36. IPsec Transform Set



```
access-list 101 permit ip 172.16.10.0 0.0.0.255 192.168.10.0 0.0.0.255
```

Fig 37. Access List for Interesting Traffic

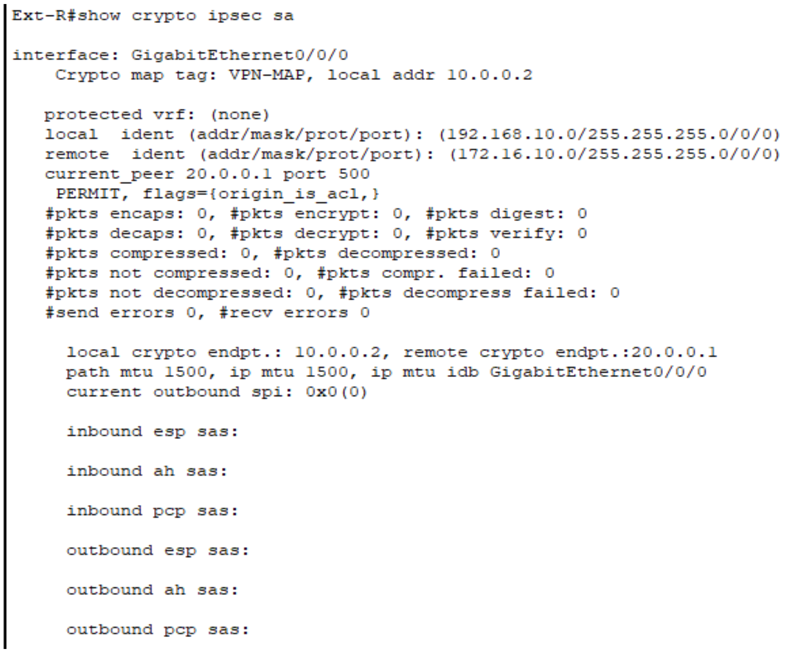


```
crypto map VPN-MAP 10 ipsec-isakmp
set peer 10.0.0.2
set transform-set VPN-TRANSFORM
match address 101
exit

interface GigabitEthernet0/1
crypto map VPN-MAP
exit
```

Fig 38. Crypto Map

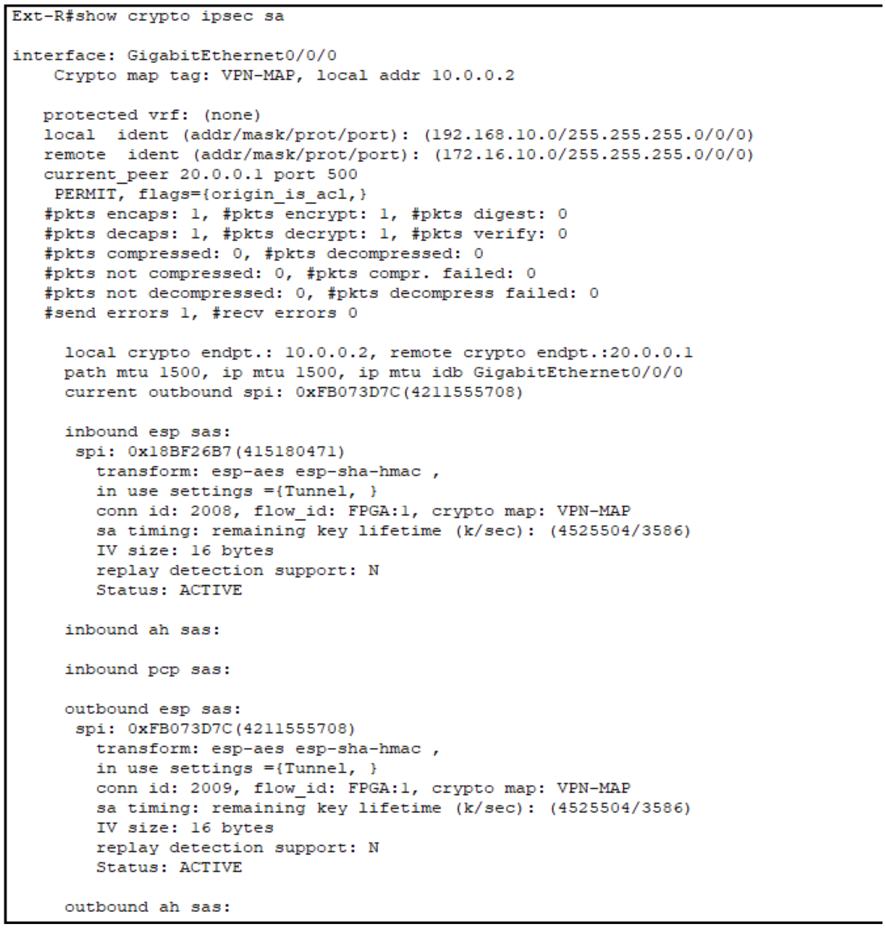
C. Verification:

Packet count changes from the tests:



```
Ext-R#show crypto ipsec sa

interface: GigabitEthernet0/0/0
    Crypto map tag: VPN-MAP, local addr 10.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   current_peer 20.0.0.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #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 0, #recv errors 0

     local crypto endpt.: 10.0.0.2, remote crypto endpt.:20.0.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:
```

Fig 39a. Packet count 0 before the VPN test



```
Ext-R#show crypto ipsec sa

interface: GigabitEthernet0/0/0
    Crypto map tag: VPN-MAP, local addr 10.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   current_peer 20.0.0.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
   #pkts decaps: 1, #pkts decrypt: 1, #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.: 10.0.0.2, remote crypto endpt.:20.0.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
     current outbound spi: 0xFB073D7C(4211555708)

     inbound esp sas:
      spi: 0x18BF26B7(415180471)
        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): (4525504/3586)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xFB073D7C(4211555708)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3586)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:
```

Fig 39b. Increased packet count after the VPN test

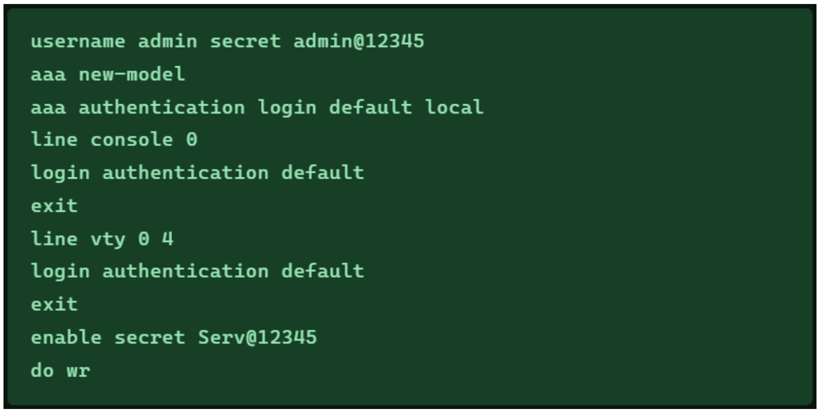
3.2 AAA Server Configuration

A. Justification:

1. AAA, TACACS server is configured on the same server as the DHCP. This is to:
    1. Simplify the design
    2. Security is still maintained as only DHCP and TACACS is allowed on the server with no management access configured to it.
    3. This should also bring the cost of setting up and maintenance down.
    4. Fewer points of failure
2. No security measures are implemented on the gateway and Remote site router as they would be out of scope.

B. Configuration:

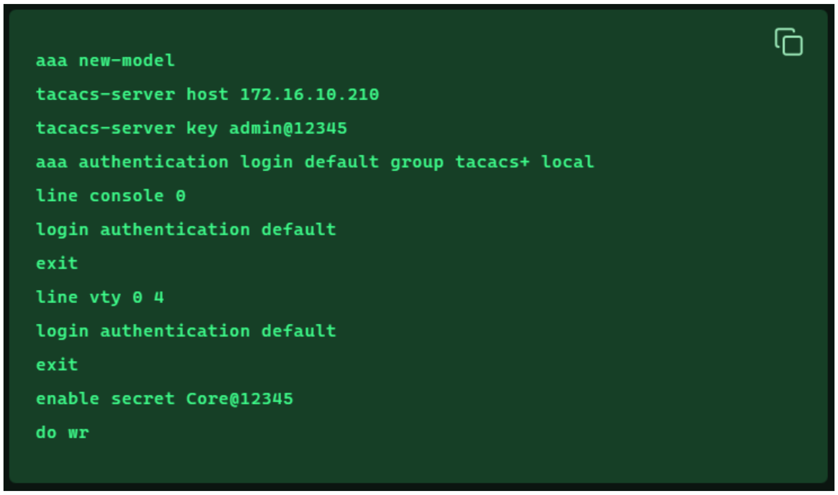
1. AAA setup on switches:



```
username admin secret admin@12345
aaa new-model
aaa authentication login default local
line console 0
login authentication default
exit
line vty 0 4
login authentication default
exit
enable secret Serv@12345
do wr
```

Fig 40. AAA on switch

2. AAA and tacacs setup on router:

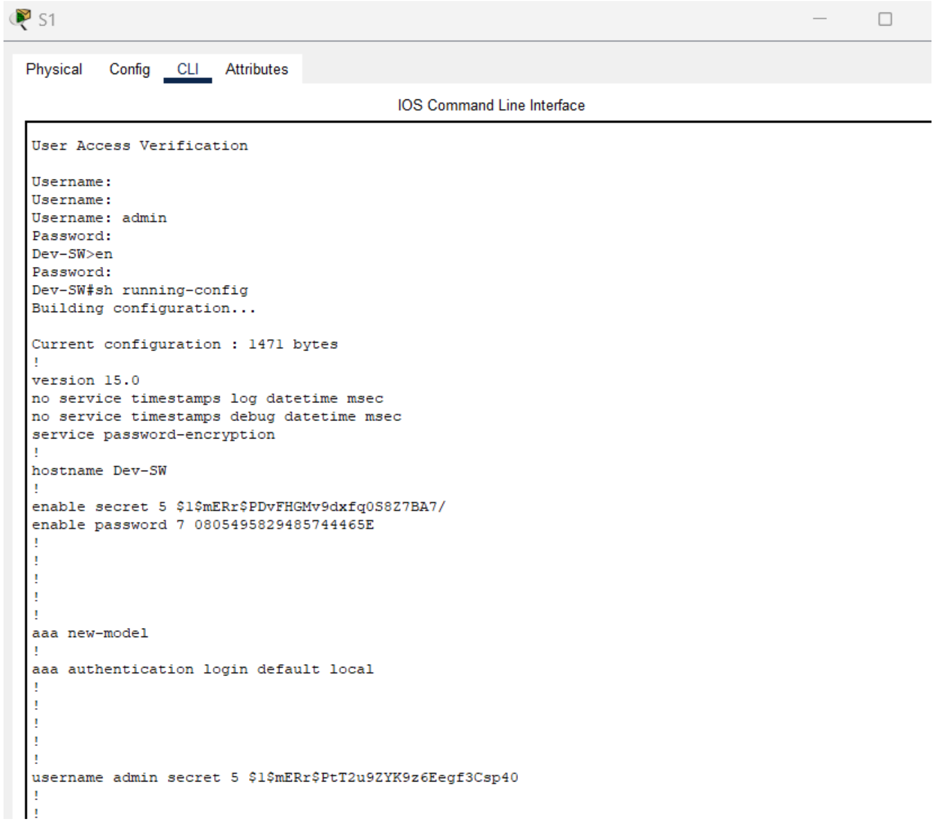


```
aaa new-model
tacacs-server host 172.16.10.210
tacacs-server key admin@12345
aaa authentication login default group tacacs+ local
line console 0
login authentication default
exit
line vty 0 4
login authentication default
exit
enable secret Core@12345
do wr
```

Fig 41. AAA and tacacs on the router

C. Verification:

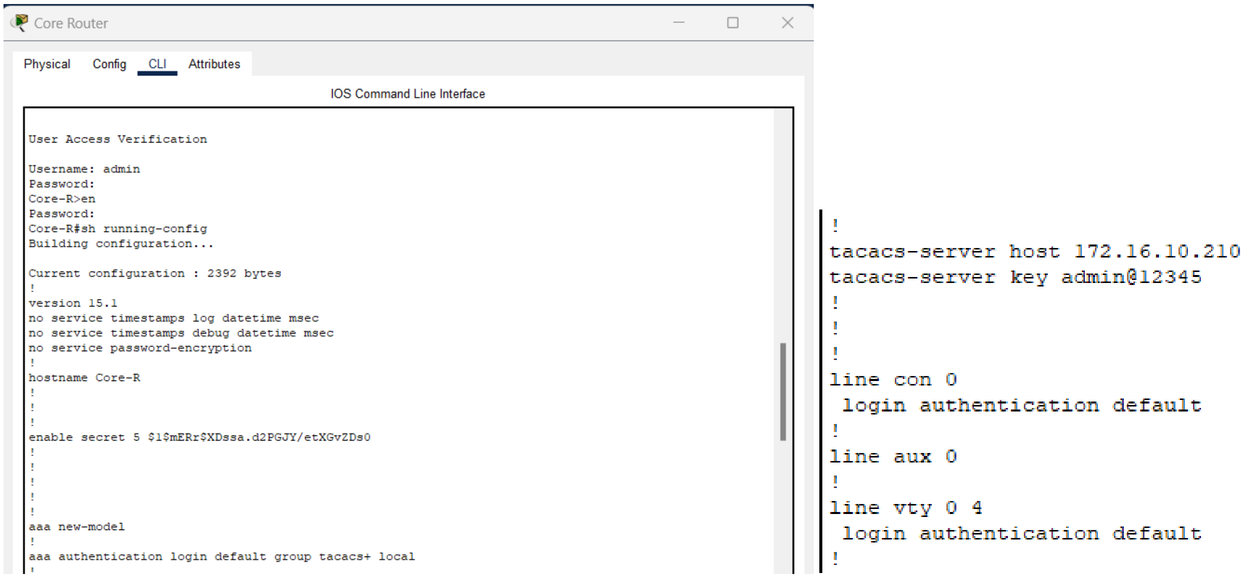
1. AAA on switch:



```
User Access Verification

Username:
Username:
Username: admin
Password:
Dev-SW>en
Password:
Dev-SW#sh running-config
Building configuration...

Current configuration : 1471 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Dev-SW
!
enable secret 5 $1$mERr$PDvFHGMv9dxfq0S8Z7BA7/
enable password 7 0805495829485744465E
!
!
!
!
!
aaa new-model
!
aaa authentication login default local
!
!
!
!
!
username admin secret 5 $1$mERr$PtT2u9ZYK9z6Eegf3Csp40
!
!
```

Fig 42. AAA and security config on the switch

2. AAA and tacacs on the Main Router



```
User Access Verification

Username: admin
Password:
Core-R>en
Password:
Core-R#sh running-config
Building configuration...

Current configuration : 2392 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Core-R
!
!
!
enable secret 5 $1$mERr$XDssa.d2PGJY/etXGvZDs0
!
!
!
!
!
aaa new-model
!
aaa authentication login default group tacacs+ local
!
```

```
!
tacacs-server host 172.16.10.210
tacacs-server key admin@12345
!
!
!
line con 0
 login authentication default
!
line aux 0
!
line vty 0 4
 login authentication default
!
```

Fig 43. AAA and security config on the main router

Appendix

A1. Passwords

Device/Name	**Password**
User: admin	admin@12345
Dev Switch	Dev@12345
Sales and Marketing switch	S&M@12345
HR switch	HR@12345
Finance switch	Fin@12345
IT switch	IT@12345
Conference room switch	Conf@12345
Server switch	Serv@12345
Core switch	Core@12345
Core router	Core@12345
Dev WiFi	Dev@12345
Sales and Marketing WiFi	S&M@12345
HR WiFi	HR@12345
Finance WiFi	Fin@12345
IT WiFi	IT@12345
Conference room WiFi	Conf@12345
VPN PSK	VPN@12345

Disclaimer:

1. *This report and the accompanying design represent a proof-of-concept. All the requested connections and features are implemented and work without any issue. However, this does not represent the scale of actual network.*
2. *All the config pasted is from the note taking software (Obsidian) which has a terminal like custom skin applied. I used this tool for note taking and keeping the track of all the commands I implemented. Most of the screenshots are from this app that has code block feature to organise the codes and commands,*
3. *Passwords used on many of the devices are kept simple for ease of use as this is just a proof-of-concept design.*