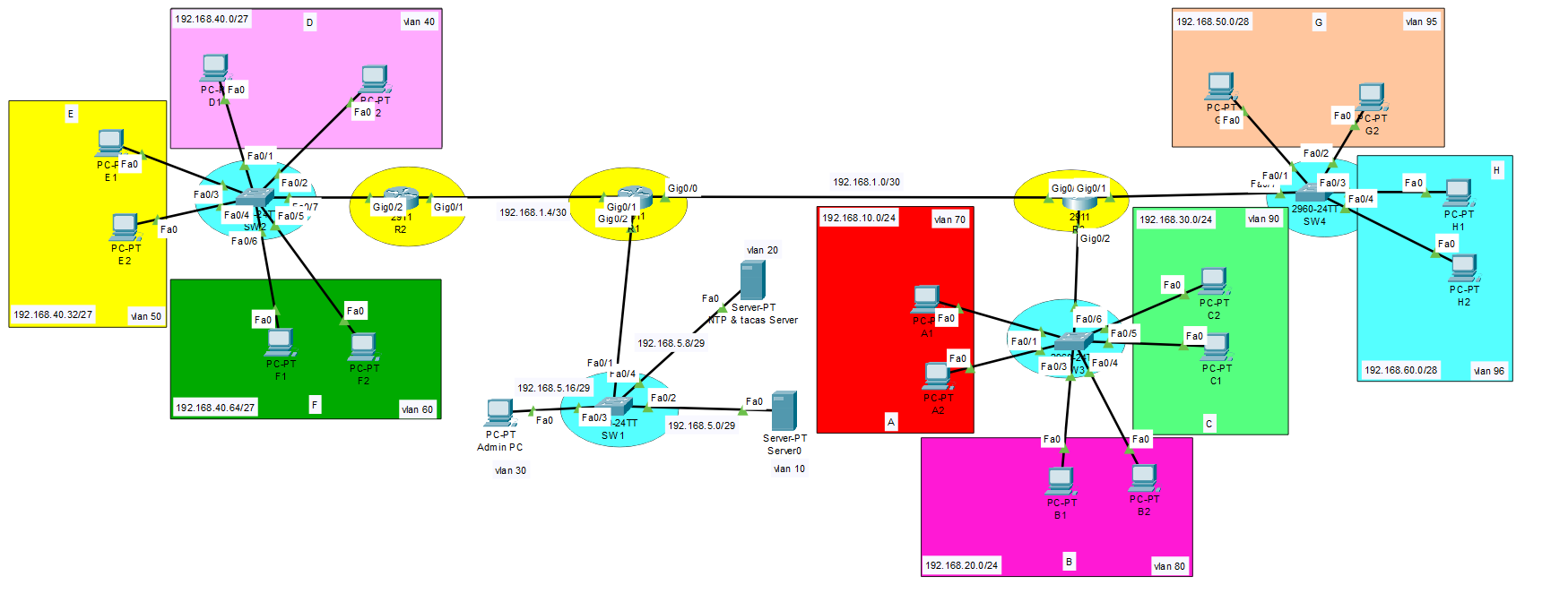
**Secure Multi-Segment Enterprise Network with OSPFv2, NTP, TACACS+, and Advanced Access Control**



**Project Overview**

In this project, I designed and implemented a **secure, multi-network topology** in Cisco Packet Tracer, following strict enterprise-grade requirements. The network integrates **dynamic routing (OSPFv2)**, **secure time synchronization (NTP)**, **centralized authentication (TACACS+)**, **advanced switch port security**, and **granular access control lists (ACLs)** to meet specific communication and security policies.

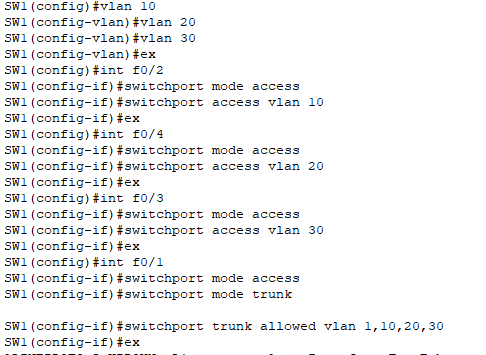
**Objectives**

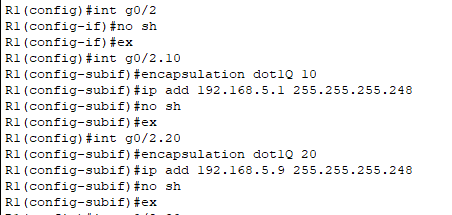
1. **Topology Replication** – Recreated the enterprise network shown in the given specification with proper device labels.
2. **IP Addressing Scheme** – Assigned the **first usable IP** to router interfaces for efficient address allocation.
3. **Dynamic Routing** – Configured **secure OSPFv2** across all routers to enable fast and reliable inter-network communication.
4. **Connectivity Validation** – Successfully tested end-to-end communication from **Network A’s PC** to all devices.
5. **Time Synchronization** – Deployed a **secure NTP server**, synchronizing all devices to a unified clock.
6. **Centralized Authentication** – Configured **TACACS+** for secure remote management of all network devices.
7. **Port Security** – Applied strict policies:
   * Switches 2 & 3: **Dynamic MAC learning (max 2)**, restrict on violation.
   * Switch 1: **Static MAC binding** for servers and admin PC, shutdown on violation.
8. **Traffic Segmentation** – Implemented ACLs:
   * Networks A, B, D, and E → Web server only.
   * Networks C and F → Communicate only with each other.

**Implementation Steps**

**1. Topology Design**

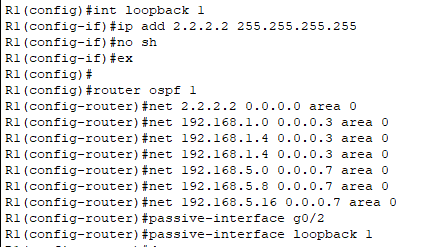
* Used Cisco Packet Tracer to design the layout.
* Proper labels assigned to routers, switches, servers, and end devices.
* Subnetting completed with the **first usable IP** allocated to each router interface.





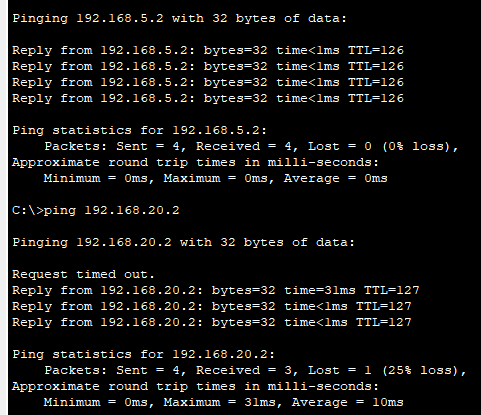
**2. Dynamic Routing (OSPFv2)**

* Configured **OSPFv2 with authentication**.
* Enabled routing between all networks except where restricted by ACLs.
* Verified routing tables with show ip route ospf.

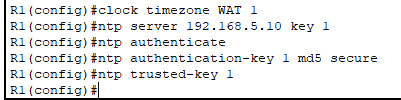


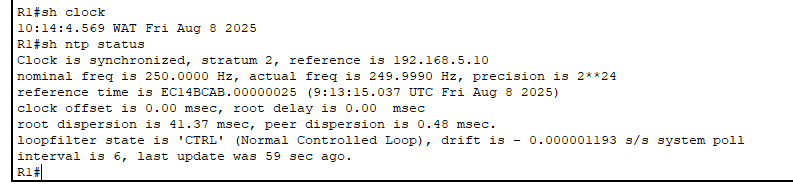
**3. Connectivity Testing**

* Sent **ICMP PINGs** from Network A’s PC to all devices — 100% success.



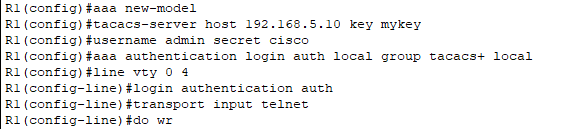
**4. Secure NTP Configuration**

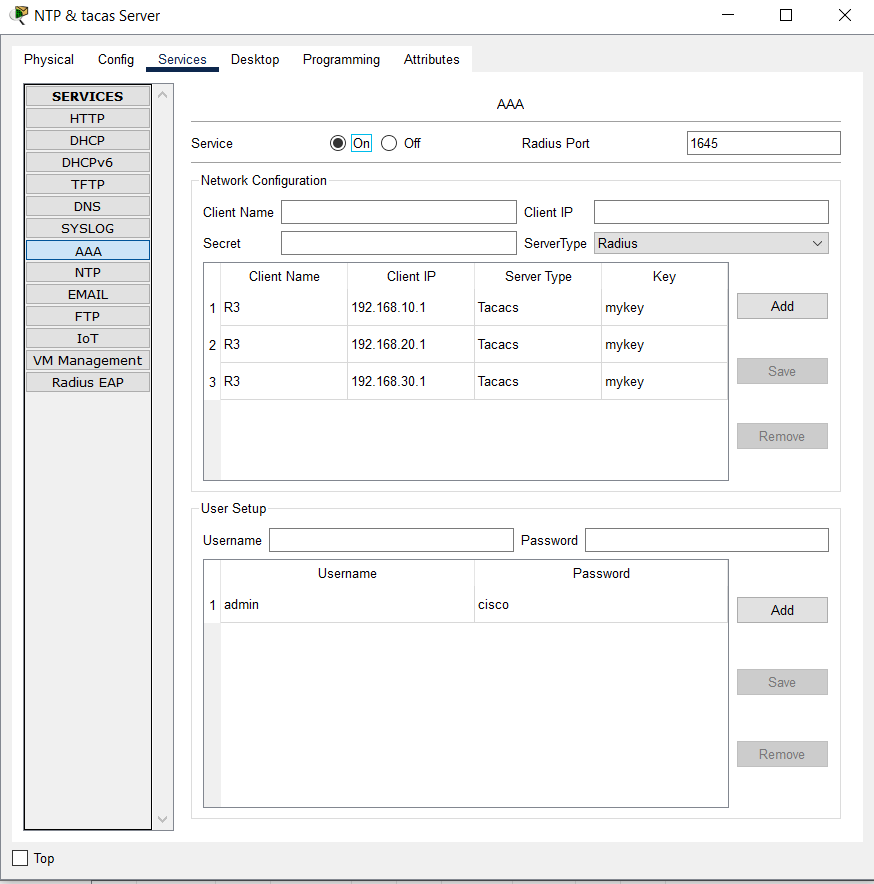
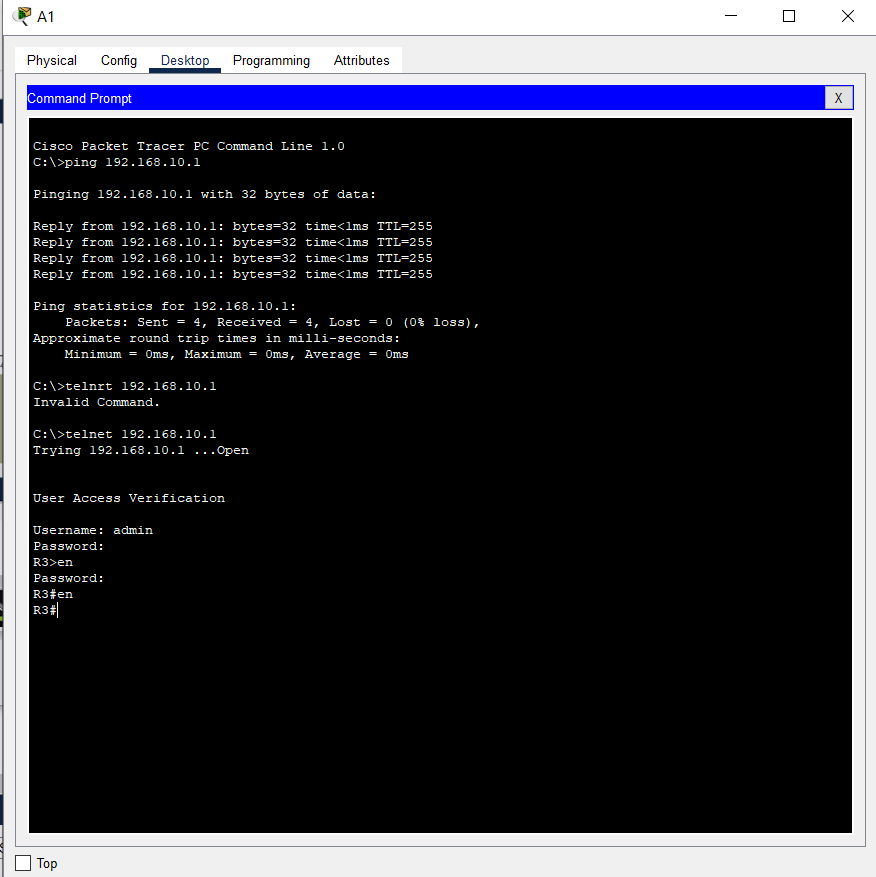
* NTP server set up with authentication keys.
* All routers synchronized to the central clock.
* Verified with show clock and show ntp status.



**5. TACACS+ Remote Management**

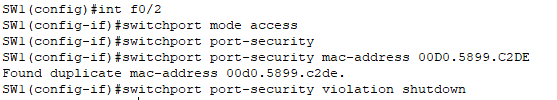
* Deployed a TACACS+ server for secure login.
* Configured all network devices to use centralized credentials.
* Tested SSH remote management — login access granted only via TACACS+.

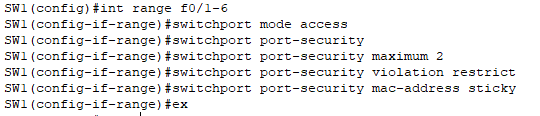




**6. Port Security**

* **Switch 1:** Static MAC binding for servers and admin PC with shutdown violation mode.
* **Switches 2 & 3:** Dynamic MAC learning (2 addresses max) with restrict violation mode.
* Tested violation scenarios — ports responded according to security mode.





**7. ACL-Based Traffic Filtering**

* Created and applied ACLs to meet requirements:
  + **A, B, D, E → Web server only**
  + **C ↔ F communication allowed, blocked from others**
* Tested HTTP access and ICMP requests to confirm filtering worked.

**Results**

✅ **Full connectivity** where required.  
✅ **Centralized authentication** and **time synchronization** working perfectly.  
✅ **Port security** and **ACL rules** enforced exactly as per requirements.  
✅ All configurations saved and backed up for disaster recovery.

**Skills & Technologies Used**

* **Cisco Packet Tracer** for network simulation
* **OSPFv2** with authentication
* **NTP server configuration**
* **TACACS+ secure authentication**
* **Switch port security (static & dynamic)**
* **Access Control Lists (ACLs)**
* **IP subnetting & allocation strategies**

**Screenshots & Evidence**

*(In GitHub repo: /screenshots folder)*

* Topology diagram
* Routing table outputs
* Ping test results
* NTP sync verification
* TACACS+ login verification
* Port security violation tests
* ACL filtering test results

**All codes**

Router 1 (R1)

en

hostname R1

conf t

int g0/2

no sh

ex

............... sub interface

int g0/2.10

encapsulation dot1Q 10

ip add 192.168.5.1 255.255.255.248

no sh

ex

int g0/2.20

encapsulation dot1Q 20

ip add 192.168.5.9 255.255.255.248

no sh

ex

int g0/2.30

encapsulation dot1Q 30

ip add 192.168.5.17 255.255.255.248

no sh

ex

int g0/1

ip add 192.168.1.5 255.255.255.252

no sh

ex

int g0/0

ip add 192.168.1.1 255.255.255.252

no sh

do wr

............... ospf

int loopback 1

ip add 2.2.2.2 255.255.255.255

no sh

ex

router ospf 1

net 2.2.2.2 0.0.0.0 area 0

net 192.168.1.0 0.0.0.3 area 0

net 192.168.1.4 0.0.0.3 area 0

net 192.168.1.4 0.0.0.3 area 0

net 192.168.5.0 0.0.0.7 area 0

net 192.168.5.8 0.0.0.7 area 0

net 192.168.5.16 0.0.0.7 area 0

passive-interface g0/2

passive-interface loopback 1

do wr

............... ntp server

clock timezone WAT 1

ntp server 192.168.5.10 key 1

ntp authenticate

ntp authentication-key 1 md5 secure

ntp trusted-key 1

............... extended acl

ip access-list extended web\_server

permit ip 192.168.10.0 0.0.0.255 host 192.168.5.2

permit ip 192.168.20.0 0.0.0.255 host 192.168.5.2

permit ip 192.168.40.0 0.0.0.31 host 192.168.5.2

permit ip 192.168.40.32 0.0.0.31 host 192.168.5.2

permit ip 192.168.50.0 0.0.0.15 host 192.168.5.2

permit tcp 192.168.10.0 0.0.0.255 host 192.168.5.2 eq 80

permit tcp 192.168.10.0 0.0.0.255 host 192.168.5.2 eq 443

permit tcp 192.168.20.0 0.0.0.255 host 192.168.5.2 eq 80

permit tcp 192.168.20.0 0.0.0.255 host 192.168.5.2 eq 443

permit tcp 192.168.40.0 0.0.0.31 host 192.168.5.2 eq 443

permit tcp 192.168.40.0 0.0.0.31 host 192.168.5.2 eq 80

permit tcp 192.168.40.32 0.0.0.31 host 192.168.5.2 eq 80

permit tcp 192.168.40.32 0.0.0.31 host 192.168.5.2 eq 443

permit tcp 192.168.50.0 0.0.0.15 host 192.168.5.2 eq 80

permit tcp 192.168.50.0 0.0.0.15 host 192.168.5.2 eq 443

deny ip any any

deny tcp any any

ex

int g0/2.10

ip access-group web\_server out

ex

int g0/2.20

ip access-group web\_server out

ex

int g0/2.30

ip access-group web\_server out

ex

............... tacas server

aaa new-model

tacacs-server host 192.168.5.10 key mykey

username admin secret cisco

aaa authentication login auth local group tacacs+ local

line vty 0 4

login authentication auth

transport input telnet

do wr

exit

enable secret cisco

------------------------------------------------------

Router 2 (R2)

en

hostname R2

conf t

int g0/2

no sh

ex

............... sub interface

int g0/2.40

encapsulation dot1Q 40

ip add 192.168.40.1 255.255.255.224

no sh

ex

int g0/2.50

encapsulation dot1Q 50

ip add 192.168.40.33 255.255.255.224

no sh

ex

int g0/2.60

encapsulation dot1Q 60

ip add 192.168.40.65 255.255.255.224

no sh

ex

do wr

............... ospf

int loopback 2

ip add 3.3.3.3 255.255.255.255

no sh

ex

router ospf 1

net 3.3.3.3 0.0.0.0 area 0

net 192.168.1.4 0.0.0.3 area 0

net 192.168.1.4 0.0.0.3 area 0

net 192.168.40.0 0.0.0.31 area 0

net 192.168.40.32 0.0.0.31 area 0

net 192.168.40.64 0.0.0.31 area 0

passive-interface g0/2

passive-interface loopback 2

do wr

............... standerd acl

ip access-list standard pc\_access

permit 192.168.30.0 0.0.0.255

deny any

ex

int g0/2.10

ip acc

ip access-group pc\_access out

ex

int g0/2.20

ip access-group pc\_access out

ex

int g0/2.30

ip access-group pc\_access out

ex

do wr

............... ntp server

clock timezone WAT 1

ntp server 192.168.5.10 key 1

ntp authenticate

ntp authentication-key 1 md5 secure

ntp trusted-key 1

............... tacas server

aaa new-model

tacacs-server host 192.168.5.10 key mykey

username admin secret cisco

aaa authentication login auth local group tacacs+ local

line vty 0 4

login authentication auth

transport input telnet

do wr

exit

enable secret cisco

------------------------------------------------------

Router 3 (R3)

en

hostname R3

conf t

int g0/2

no sh

ex

............... sub interface

int g0/2.70

encapsulation dot1Q 70

ip add 192.168.10.1 255.255.255.0

no sh

ex

int g0/2.80

encapsulation dot1Q 80

ip add 192.168.20.1 255.255.255.0

no sh

ex

int g0/2.90

encapsulation dot1Q 90

ip add 192.168.30.1 255.255.255.0

no sh

ex

int g0/1

no sh

int g0/1.95

encapsulation dot1Q 95

ip add 192.168.50.1 255.255.255.240

no sh

ex

int g0/1.96

encapsulation dot1Q 96

ip add 192.168.60.1 255.255.255.240

no sh

ex

do wr

............... ospf

int loopback 0

ip add 1.1.1.1 255.255.255.255

no sh

do wr

router ospf 1

net 1.1.1.1 0.0.0.0 area 0

net 192.168.1.0 0.0.0.3 area 0

net 192.168.10.0 0.0.0.255 area 0

net 192.168.20.0 0.0.0.255 area 0

net 192.168.30.0 0.0.0.255 area 0

net 192.168.50.0 0.0.0.15 area 0

net 192.168.60.0 0.0.0.15 area 0

passive-interface g0/1

passive-interface g0/2

passive-interface loopback 0

............... standerd acl

ip access-list standard pc\_access

permit 192.168.40.64 0.0.0.31

deny any

ex

int g0/2.10

ip access-group pc\_access out

ex

int g0/2.20

R3(config-subif)#

ip access-group pc\_access out

int g0/2.30

ip access-group pc\_access out

ex

do wr

............... ntp server

clock timezone WAT 1

ntp server 192.168.5.10 key 1

ntp authenticate

ntp authentication-key 1 md5 secure

ntp trusted-key 1

............... tacas server

aaa new-model

tacacs-server host 192.168.5.10 key mykey

username admin secret cisco

aaa authentication login auth local group tacacs+ local

line vty 0 4

login authentication auth

transport input telnet

do wr

exit

enable secret cisco

------------------------------------------------------

Switch 1 (SW1)

en

conf t

hostname SW1

............... vlan

vlan 10

vlan 20

vlan 30

ex

int f0/2

switchport mode access

switchport access vlan 10

ex

int f0/4

switchport mode access

switchport access vlan 20

ex

int f0/3

switchport mode access

switchport access vlan 30

ex

............... trunk

int f0/1

switchport mode access

switchport mode trunk

switchport trunk allowed vlan 1,10,20,30

ex

do wr

............... port security

int f0/2

switchport mode access

switchport port-security

switchport port-security mac-address 00D0.5899.C2DE

switchport port-security violation shutdown

ex

int f0/3

switchport mode access

switchport port-security

switchport port-security mac-address 00D0.979C.8E30

switchport port-security violation shutdown

ex

int f0/4

switchport mode access

switchport port-security

switchport port-security mac-address 000C.CFE7.CAEB

switchport port-security violation shutdown

ex

do wr

------------------------------------------------------

Switch 2 (SW2)

en

conf t

hostname SW2

............... vlan

vlan 40

vlan 50

vlan 60

ex

int range f0/1-2

switchport mode access

switchport access vlan 40

ex

int range f0/3-4

switchport mode access

switchport access vlan 50

ex

int range f0/5-6

switchport mode access

switchport access vlan 60

ex

............... trunk

int f0/7

switchport mode trunk

switchport trunk allowed vlan 1,40,50,60

ex

do wr

............... port security

int range f0/1-6

switchport mode access

switchport port-security

switchport port-security maximum 2

switchport port-security violation restrict

switchport port-security mac-address sticky

ex

do wr

------------------------------------------------------

Switch 3 (SW3)

en

conf t

hostname SW3

............... vlan

vlan 70

vlan 80

vlan 90

ex

int range f0/1-2

switchport mode access

switchport access vlan 70

ex

int range f0/3-4

switchport mode access

switchport access vlan 80

ex

int range f0/5-6

switchport mode access

switchport access vlan 90

ex

............... trunk

int f0/7

switchport mode trunk

switchport trunk allowed vlan 1,70,80,90

ex

do wr

............... port security

int range f0/1-6

switchport mode access

switchport port-security

switchport port-security maximum 2

switchport port-security violation restrict

switchport port-security mac-address sticky

ex

do wr

------------------------------------------------------

Switch 4 (SW4)

en

conf t

hostname SW4

............... vlan

vlan 65

ex

no vlan 65

vlan 95

vlan 96

ex

int range f0/1-2

switchport mode access

switchport access vlan 95

ex

int range f0/3-4

switchport mode access

switchport access vlan 96

ex

............... trunk

int f0/7

switchport mode trunk

switchport trunk allowed vlan 1,95,96

ex

do wr

............... port security

int range f0/1-4

switchport mode access

switchport port-security

switchport port-security maximum 2

switchport port-security violation restrict

switchport port-security mac-address sticky

ex

do wr

------------------------------------------------------