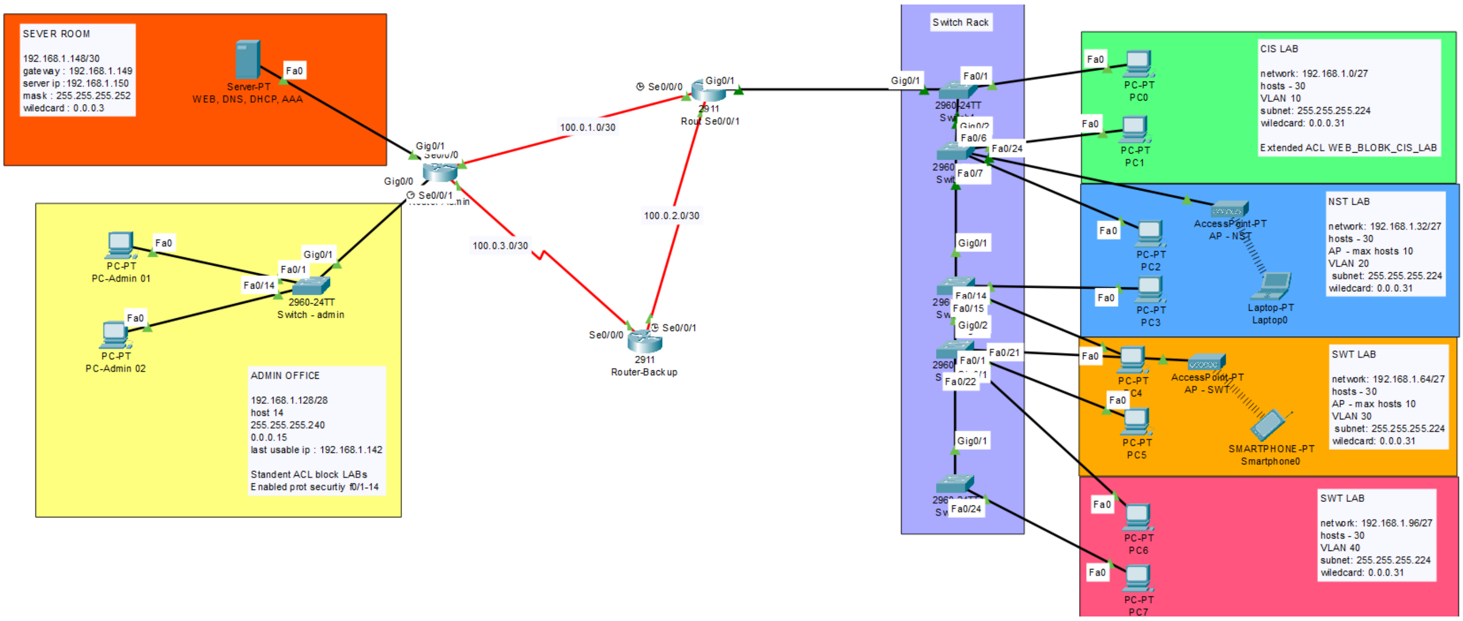
Secure VLAN Network (DHCP, AAA, DNS, WEB, Port Security, ACLs) Design

1. Introduction

This project focuses on designing and implementing a secure, scalable network infrastructure for multiple departments using VLAN segmentation, centralized authentication, access control, and port security. The solution ensures data isolation, controlled access, and network reliability, while supporting secure Wi-Fi communications and redundancy for continuous departmental connectivity.

2. Network Design

- VLANs: Separate VLANs for each department (ADMIN, CIS LAB, NST LAB, SWT LAB, MAC LAB, SERVER ROOM) and Wi-Fi (Students, Guests).
- AAA: Centralized TACACS+ server for network device authentication and management.
- DNS Server: Internal DNS for local and external name resolution (cisco.com -> 192.168.1.150).
- Access Control: ACLs to regulate inter-VLAN traffic and secure sensitive resources.
- Port Security: MAC address limits per port with violation shutdown
- Routing Protocol: OSPFv2 used because it efficiently supports IPv4 networks, offers fast convergence, scalability through multi-area design, robust security with authentication, and is a widely supported.
- Wi-Fi: WPA2-PSK security for Wi-Fi networks, separate SSIDs mapped to VLANs for students and guest access.



SEVER ROOM

192.168.1.148/30
gateway : 192.168.1.149
server ip :192.168.1.150
mask : 255.255.255.252
wiledcard : 0.0.0.3

ADMIN OFFICE

192.168.1.128/28
host 14
255.255.255.240
0.0.0.15
last usable ip : 192.168.1.142

Standent ACL block LABs
Enabled prot securtiy f0/1-14

CIS LAB

network: 192.168.1.0/27
hosts - 30
VLAN 10
subnet: 255.255.255.224
wiledcard: 0.0.0.31

Extended ACL WEB_BLOBK_CIS_LAB

NST LAB

network: 192.168.1.32/27
hosts - 30
AP - max hosts 10
VLAN 20
subnet: 255.255.255.224
wiledcard: 0.0.0.31

SWT LAB

network: 192.168.1.64/27
hosts - 30
AP - max hosts 10
VLAN 30
subnet: 255.255.255.224
wiledcard: 0.0.0.31

SWT LAB

network: 192.168.1.96/27
hosts - 30
VLAN 40
subnet: 255.255.255.224
wiledcard: 0.0.0.31

3. Configurations

Do for Switchers in rack SW01, SW02, SW03, SW04, SW05

```
vlan 10
name CIS
ex
vlan 20
name NST
ex
vlan 30
name SOFT
ex
vlan 40
name MAC
ex
```

SW01 Configurations

```
int range fa0/1 - 24
switchport mode access
switchport access vlan 10
ex
int g0/1
switchport mode trunk
switchport trunk allowed vlan all
```

SW02 Configurations

```
int range fa0/1 - 6
switchport mode access
switchport access vlan 10
ex

int range fa0/7 - 24
switchport mode access
switchport access vlan 20
ex

int g0/2
switchport mode trunk
switchport trunk allowed vlan all
```

SW03 Configurations

```
int range fa0/1 - 14
switchport mode access
switchport access vlan 20
ex

int range fa0/15 - 24
switchport mode access
switchport access vlan 30
ex

int g0/1
switchport mode trunk
switchport trunk allowed vlan all
```

SW04 Configurations

```
int range fa0/1 - 21
switchport mode access
switchport access vlan 30
ex

int range fa0/22 - 24
switchport mode access
switchport access vlan 40
```

```
ex

int g0/2
switchport mode trunk
switchport trunk allowed vlan all
```

SW05 Configurations

```
int range fa0/1 - 24
switchport mode access
switchport access vlan 40
ex

int g0/1
switchport mode trunk
switchport trunk allowed vlan all
```

Admin Switch Configurations

```
enable
configure terminal

hostname admin_switch

vlan 11
name ADMIN
exit

interface range fa0/1 - 14
switchport mode access
switchport access vlan 11
exit
```

```
interface g0/1
switchport mode trunk
switchport trunk allowed vlan 1,11
no shutdown
exit
do wr
```

Port Security Admin-Switch

```
int range fa0/1 - 14
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
ex

int range fa0/15 - 24 , gi0/2
shutdown

ex
do wr
```

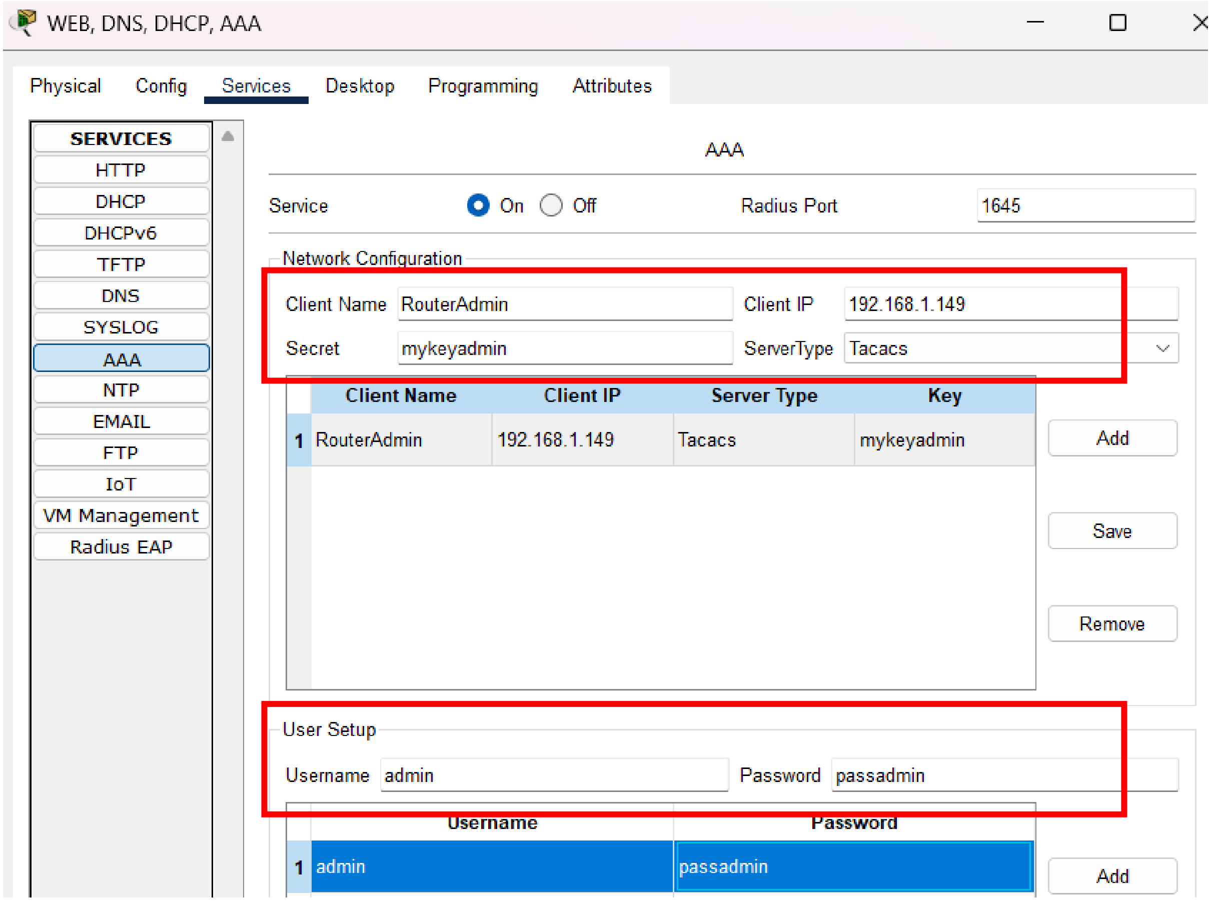
Admin Router Configurations

```
enable
configure terminal

interface g0/0
no shutdown

interface g0/0.11
encapsulation dot1Q 11
```

```
ip address 192.168.1.129 255.255.255.240
ip helper-address 192.168.1.150
no shutdown
exit

interface s0/0/0
ip address 100.0.1.1 255.255.255.252
no shutdown
exit

interface s0/0/1
ip address 100.0.3.1 255.255.255.252
no shutdown
exit

interface g0/1
ip address 192.168.1.149 255.255.255.252
no shutdown
exit

router ospf 1
network 192.168.1.128 0.0.0.15 area 0
network 192.168.1.148 0.0.0.3 area 0
network 100.0.1.0 0.0.0.3 area 0
network 100.0.3.0 0.0.0.3 area 0
exit
do wr
```

AAA with tacacs in Admin-Router

```
enable secret adminclass

tacacs-server host 192.168.1.149 key mykeyadmin

aaa new-model
aaa authentication login authadmin group tacacs+ local

username admin secret passadmin

line vty 0 4
login authentication authadmin
transport input telnet

exit
do wr
```



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name RouterAdmin Client IP 192.168.1.149

Secret mykeyadmin ServerType Tacacs

	Client Name	Client IP	Server Type	Key
1	RouterAdmin	192.168.1.149	Tacacs	mykeyadmin

User Setup

Username admin Password passadmin

	Username	Password
1	admin	passadmin

Admin section block using standard ACL (Router-Admin)

```
ip access-list standard LABS_BLOCK

deny 192.168.1.0 0.0.0.31
deny 192.168.1.32 0.0.0.31
deny 192.168.1.64 0.0.0.31
deny 192.168.1.96 0.0.0.31
permit any
ex

int g0/0.11
ip access-group LABS_BLOCK out
ex
```

WEB (80,443 protocols) BLOCK CIS LAB section block using extended ACL (Router-Admin)

```
ip access-list extended WEB_BLOBK_CIS_LAB

deny tcp 192.168.1.0 0.0.0.31 host 192.168.1.150 eq 80
deny tcp 192.168.1.0 0.0.0.31 host 192.168.1.150 eq 443
permit tcp any any
permit ip any any
ex

int g0/1
ip access-group WEB_BLOBK_CIS_LAB out
ex
```

Main Router Configurations

```
enable
configure terminal
```

```
hostname Router-Main
ex

interface g0/1
no shutdown

interface g0/1.10
encapsulation dot1Q 10
ip address 192.168.1.1 255.255.255.224
ip helper-address 192.168.1.150
no shutdown
exit

interface g0/1.20
encapsulation dot1Q 20
ip address 192.168.1.33 255.255.255.224
ip helper-address 192.168.1.150
no shutdown
exit

interface g0/1.30
encapsulation dot1Q 30
ip address 192.168.1.65 255.255.255.224
ip helper-address 192.168.1.150
no shutdown
exit

interface g0/1.40
encapsulation dot1Q 40
ip address 192.168.1.97 255.255.255.224
ip helper-address 192.168.1.150
no shutdown
exit
```

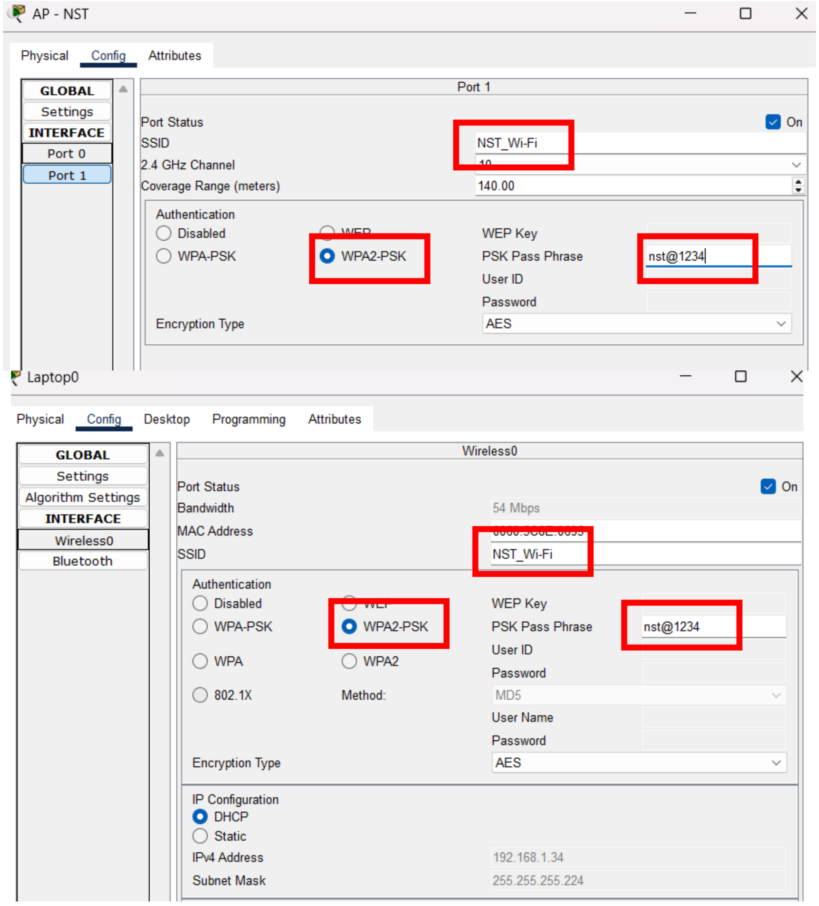
```
interface s0/0/0
ip address 100.0.1.2 255.255.255.252
no shutdown
exit

interface s0/0/1
ip address 100.0.2.1 255.255.255.252
no shutdown
exit

router ospf 1
network 192.168.1.0 0.0.0.31 area 0
network 192.168.1.32 0.0.0.31 area 0
network 192.168.1.64 0.0.0.31 area 0
network 192.168.1.96 0.0.0.31 area 0
network 100.0.1.0 0.0.0.3 area 0
network 100.0.2.0 0.0.0.3 area 0
ex
do wr
```

Backup-router ospf Configurations

```
enable
configure terminal
hostname Backup-Router

interface s0/0/0
ip address 100.0.3.2 255.255.255.252
no shutdown
exit

interface s0/0/1
```

```
ip address 100.0.2.2 255.255.255.252
no shutdown
exit
router ospf 1
network 100.0.3.0 0.0.0.3 area 0
network 100.0.2.0 0.0.0.3 area 0
ex
do wr
```

Wi-Fi Configurations – same like SWT LAB



AP - NST: Port 1

Port Status ☑ On
SSID NST_Wi-Fi
2.4 GHz Channel 10
Coverage Range (meters) 140.00
Authentication
○ Disabled ○ WEP
○ WPA-PSK ● WPA2-PSK
WEP Key
PSK Pass Phrase nst@1234
User ID
Password
Encryption Type AES

Laptop0: Wireless0

Port Status ☑ On
Bandwidth 54 Mbps
MAC Address
SSID NST_Wi-Fi
Authentication
○ Disabled ○ WEP
○ WPA-PSK ● WPA2-PSK
○ WPA ○ WPA2
○ 802.1X Method: MD5
WEP Key
PSK Pass Phrase nst@1234
User ID
Password
User Name
Password
Encryption Type AES
IP Configuration
● DHCP
○ Static
IPv4 Address 192.168.1.34
Subnet Mask 255.255.255.224

4. Conclusion

This project successfully demonstrates the design and implementation of a secure, scalable VLAN-based network infrastructure with centralized TACACS+ authentication, access control, and port security. By leveraging VLAN segmentation, OSPFv2 routing, and WPA2-PSK secured Wi-Fi, the network ensures departmental isolation, secure access, and high availability, meeting the ICT department’s operational and security needs effectively.