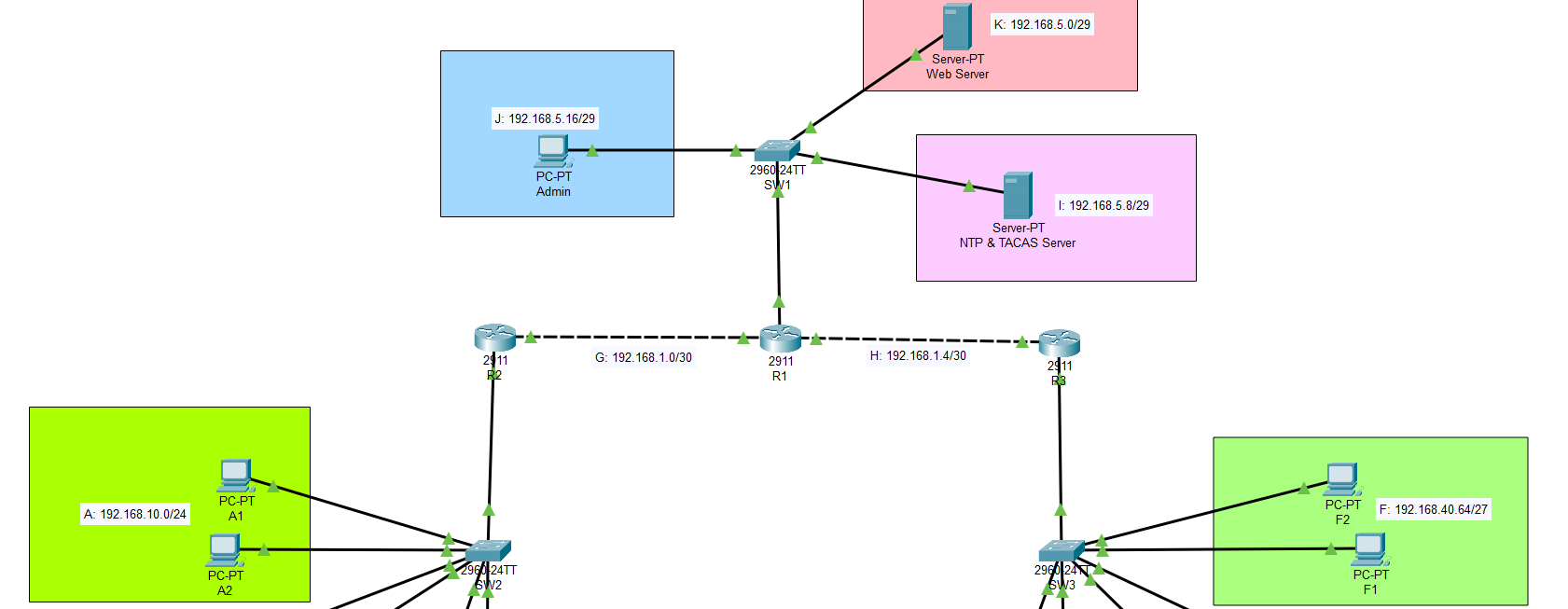
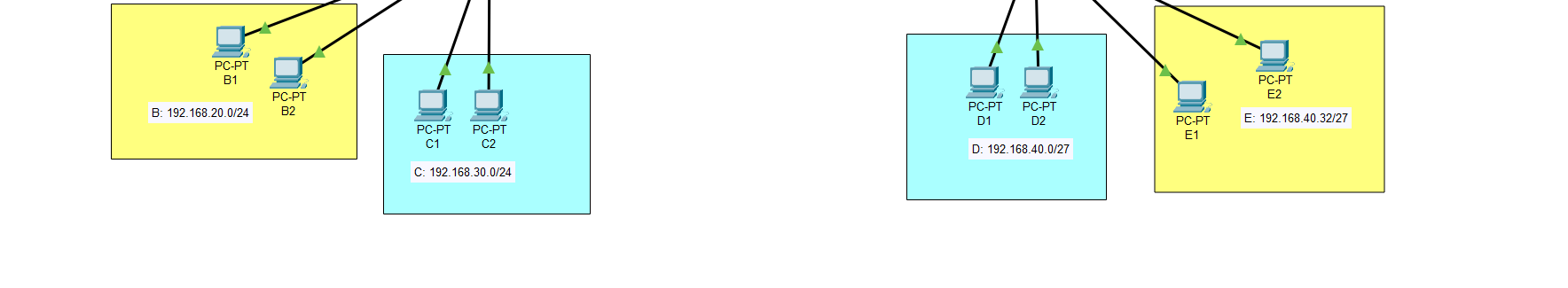
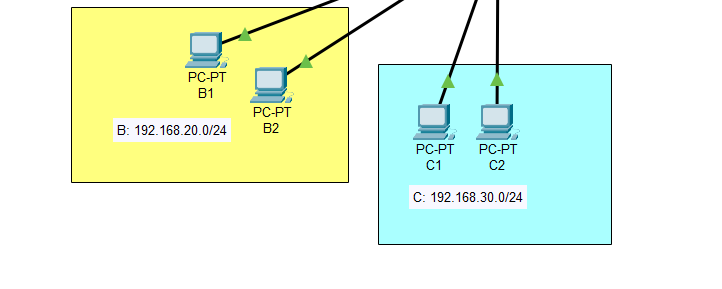
# Cisco Packet Tracer – Secure Network Implementation & Configuration

## Project Overview

This project focuses on designing and configuring a secure multi-network topology in Cisco Packet Tracer. The implementation covers VLANs, inter-VLAN routing, OSPFv2, NTP synchronization, TACACS+ authentication, port security, and ACL-based traffic control.



## Requirements

1. Replicate the given network topology with correct labels.
2. Assign the first usable IP addresses for router interfaces.
3. Enable secure OSPFv2 routing and verify connectivity.
4. Configure a secure NTP server and synchronize devices.
5. Enable secure remote management with a TACACS+ server.
6. Configure port security:  
   - Switch 2 & 3: 2 dynamically learned MACs, restrict violation.  
   - Switch 1: Static MACs for servers/admin PC, shutdown violation.
7. Apply ACLs to allow:  
   - Networks A, B, D, and E → only access the web server.
8. Apply ACLs to allow:  
   - Networks C and F → communicate only with each other.

## IP Addressing Scheme

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | VLAN / Network | IP Address | Subnet Mask |
| R1 | g0/0.10 | VLAN 10 | 192.168.5.1 | 255.255.255.248 |
| R1 | g0/0.20 | VLAN 20 | 192.168.5.9 | 255.255.255.248 |
| R1 | g0/0.30 | VLAN 30 | 192.168.5.17 | 255.255.255.248 |
| R1 | g0/1 | Link to R2 | 192.168.1.1 | 255.255.255.252 |
| R1 | g0/2 | Link to R3 | 192.168.1.5 | 255.255.255.252 |
| R2 | g0/0 | Link to R1 | 192.168.1.2 | 255.255.255.252 |
| R2 | g0/1.10 | VLAN 10 | 192.168.10.1 | 255.255.255.0 |
| R2 | g0/1.20 | VLAN 20 | 192.168.20.1 | 255.255.255.0 |
| R2 | g0/1.30 | VLAN 30 | 192.168.30.1 | 255.255.255.0 |
| R3 | g0/0 | Link to R1 | 192.168.1.6 | 255.255.255.252 |
| R3 | g0/1.10 | VLAN 10 | 192.168.40.1 | 255.255.255.224 |
| R3 | g0/1.20 | VLAN 20 | 192.168.40.33 | 255.255.255.224 |
| R3 | g0/1.30 | VLAN 30 | 192.168.40.65 | 255.255.255.224 |

## Configurations

### VLAN & Inter-VLAN Routing (R1 Example)

en  
conf t  
int g0/0  
no shut  
int g0/0.10  
encapsulation dot1q 10  
ip add 192.168.5.1 255.255.255.248  
no shut  
exit  
int g0/0.20  
encapsulation dot1q 20  
ip add 192.168.5.9 255.255.255.248  
no shut  
exit  
int g0/0.30  
encapsulation dot1q 30  
ip add 192.168.5.17 255.255.255.248  
no shut  
exit  
int g0/1  
ip add 192.168.1.1 255.255.255.252  
no shut  
exit  
int g0/2  
ip add 192.168.1.5 255.255.255.252  
no shut

### OSPFv2 (R1 Example)

router ospf 1  
network 2.2.2.2 0.0.0.0 area 0  
network 192.168.1.0 0.0.0.3 area 0  
network 192.168.1.4 0.0.0.3 area 0  
network 192.168.5.0 0.0.0.7 area 0  
network 192.168.5.8 0.0.0.7 area 0  
network 192.168.5.16 0.0.0.7 area 0  
passive-interface g0/0  
passive-interface loopback 0

### Secure NTP

ntp server 192.168.5.10 key 1  
ntp authentication-key 1 md5 secure

### TACACS+

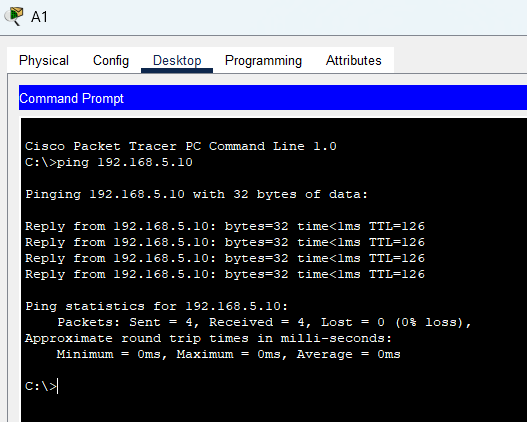
aaa new-model  
tacacs-server host 192.168.5.10 key mykey  
username admin secret cisco  
aaa authentication login auth local group tacacs+ local  
line vty 0 4  
login authentication auth  
transport input telnet  
enable secret cisco

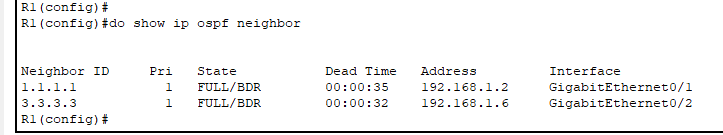
### Port Security (SW2 & SW3)

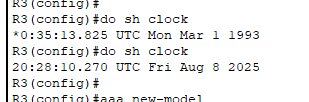
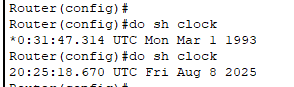
int range f0/1-6  
switchport mode access  
switchport port-security  
switchport port-security maximum 2  
switchport port-security violation restrict  
switchport port-security mac-address sticky

## Verification

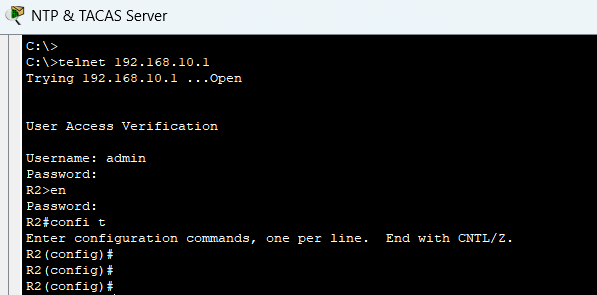
- Ping Tests: Successful communication per ACL rules.

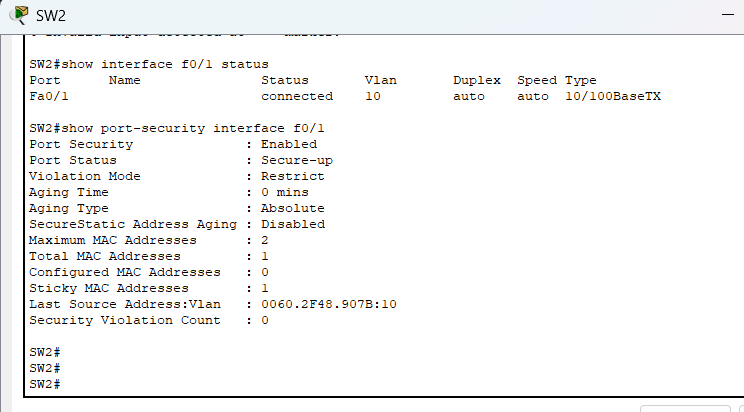
  
- OSPF: Verified adjacency with 'show ip ospf neighbor'.

  
- NTP: Confirmed time sync on all devices.

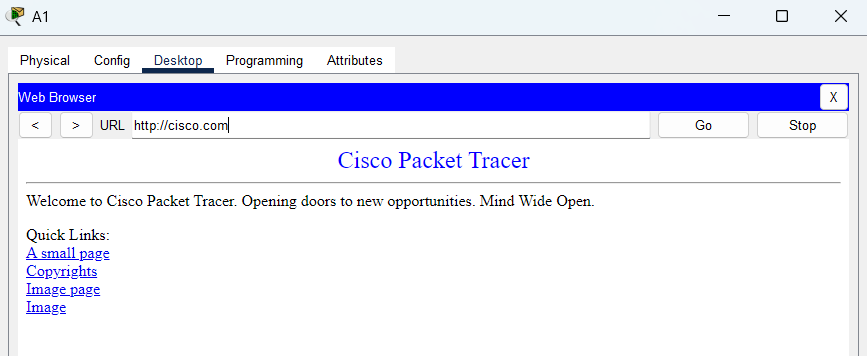
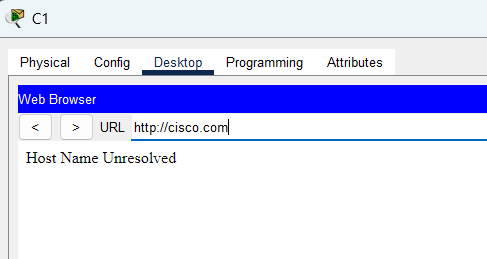


- TACACS+: Telnet access authenticated.

  
- Port Security: Verified shutdown/restrict behavior.



- ACLs: Confirmed traffic filtering matches requirements.



## Author

Chiraji Dilipun  
Final Year – Network & Security Technologies  
South Eastern University of Sri Lanka