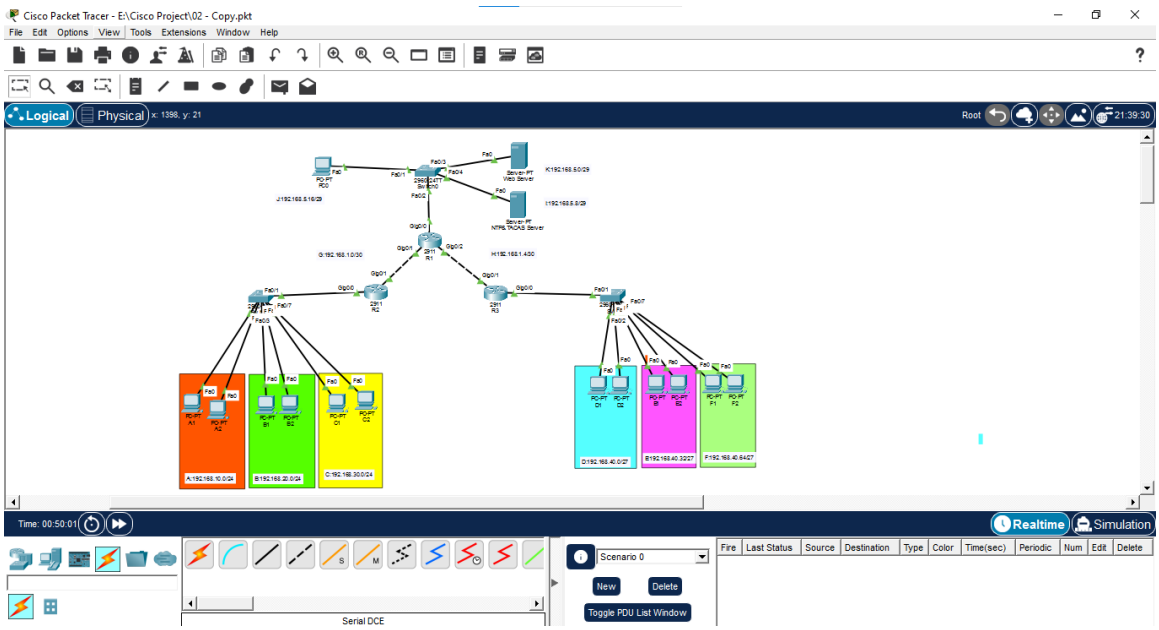
Secure Network Design in Cisco Packet Tracer

1. Topology Diagram

Include a labeled screenshot of the Packet Tracer topology here.



2. IP Addressing

Use the first usable IP addresses for all router interfaces. Example table:

Device	Interface	IP Address	Subnet	Description
R1	G0/1	192.168.1.1	/30	To R2
R1	G0/2	192.168.1.5	/30	To R3
Web_Server	G0/0.10	192.168.5.1	/29	Network K
NTP & Tacas_Server	G0/0.20	192.168.5.9	/29	Network I
Admin PC	G0/0.30	192.168.5.17	/29	Network J
PC A	G0/0.10	192.168.10.1	/24	Network A
PC B	G0/0.20	192.168.20.1	/24	Network B
PC C	G0/0.30	192.168.30.1	/24	Network C
PC D	G0/0.40	192.168.40.1	/24	Network D
PC E	G0/0.50	192.168.40.33	/24	Network E
PC F	G0/0.60	192.168.40.65	/24	Network F

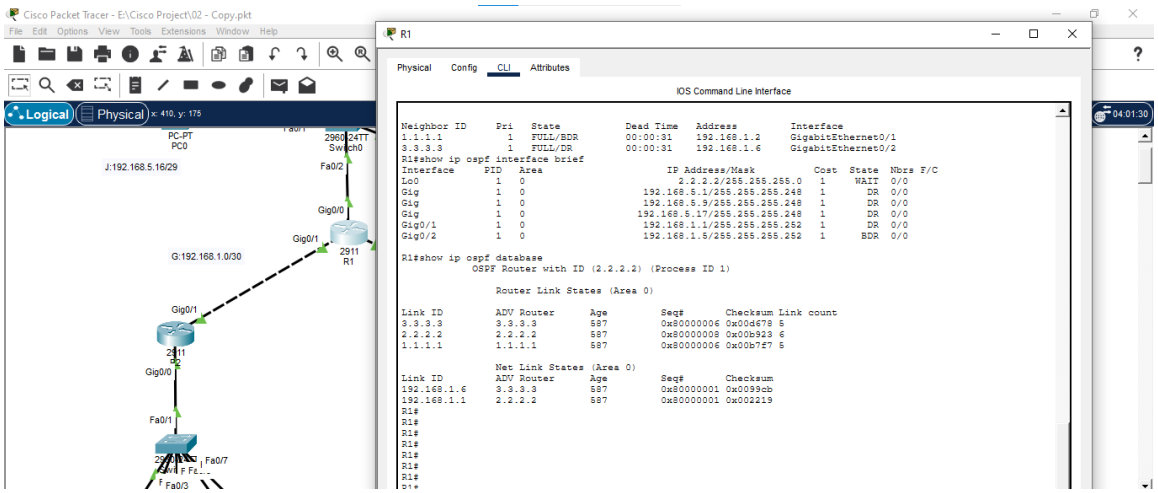
3. Secure OSPFv2 Configuration

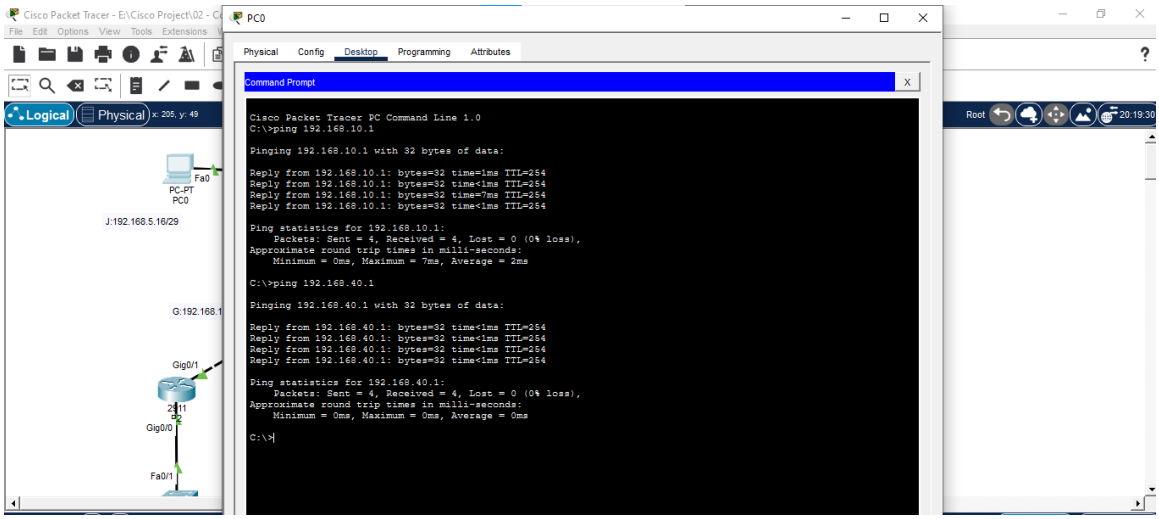
Example configuration:

```
Int loopaback 0
Ip add 1.1.1.1 255.255.255.255
Ex

router ospf 1
 net 1.1.1.1 0.0.0.0 area 0
network 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 g0/0
passive-interface loopaback 0
exit
```

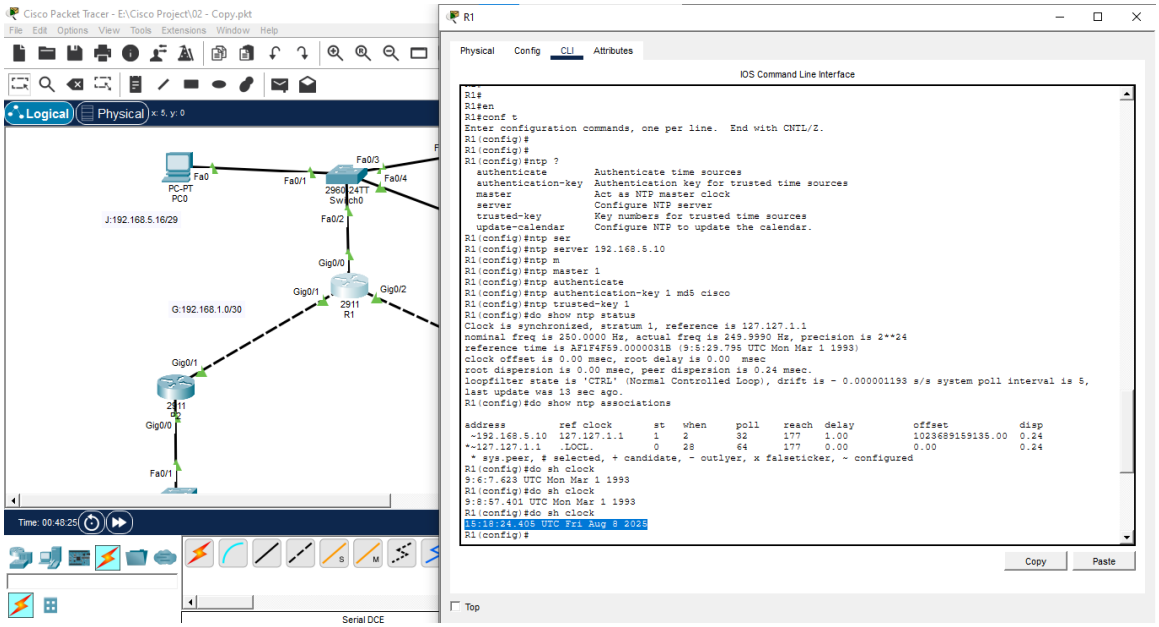
Add PING test results from Network A PC to other devices. Include screenshots.





4. Secure NTP Server

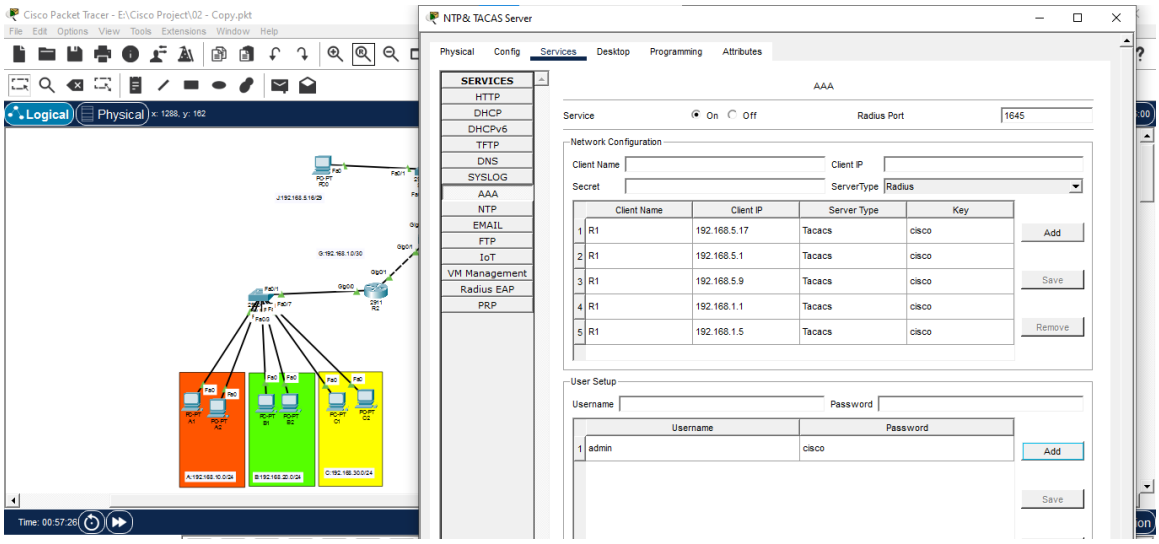
Configure the NTP server. Add screenshots showing synchronized time using "show clock".

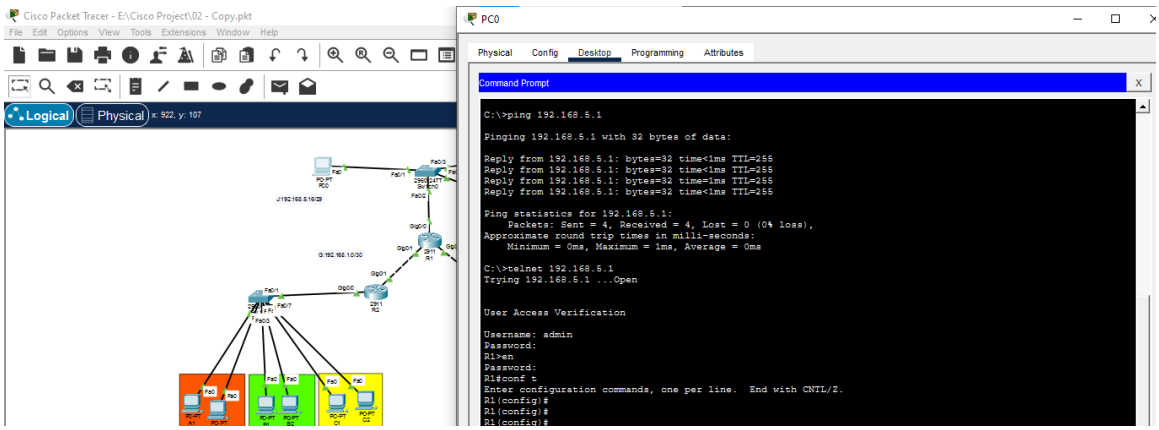


5. Secure Remote Management via TACACS+

Configure the TACACS+ server and device AAA settings. Include a screenshot of login verification.

R1(config)#aaa new-model
R1(config)#tacacs-server host 192.168.5.10 key cisco
R1(config)#username admin secret cisco
R1(config)#aaa authentication login auth local group tacacs+ local
R1(config)#line vty 0 4
R1(config-line)#login authentication auth
R1(config-line)#transport input telnet
R1(config-line)#exit
R1(config)#enable secret cisco
R1(config)#ex



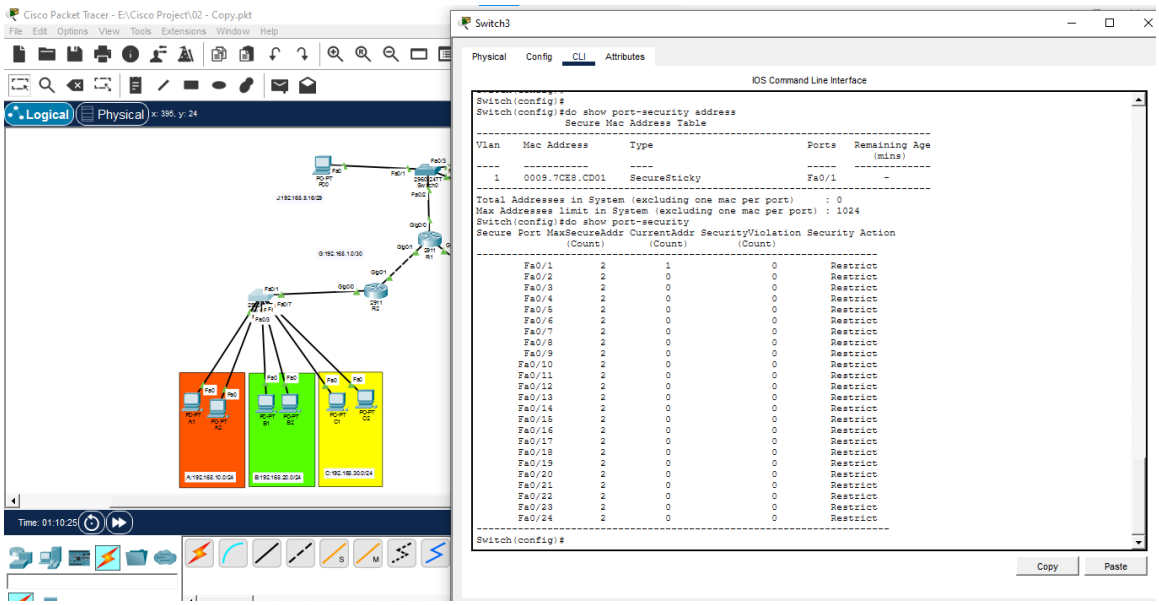


6. Port Security Configuration

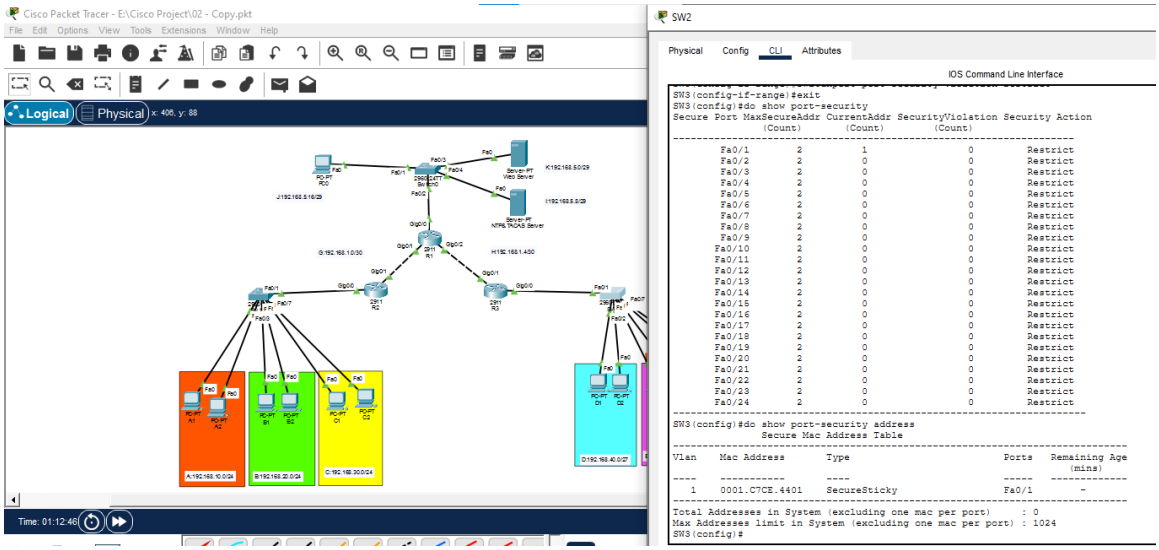
a. Switch 2 and 3 - Dynamic MAC addresses with "restrict" violation mode.

```
int range f0/1-24
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```

SW01

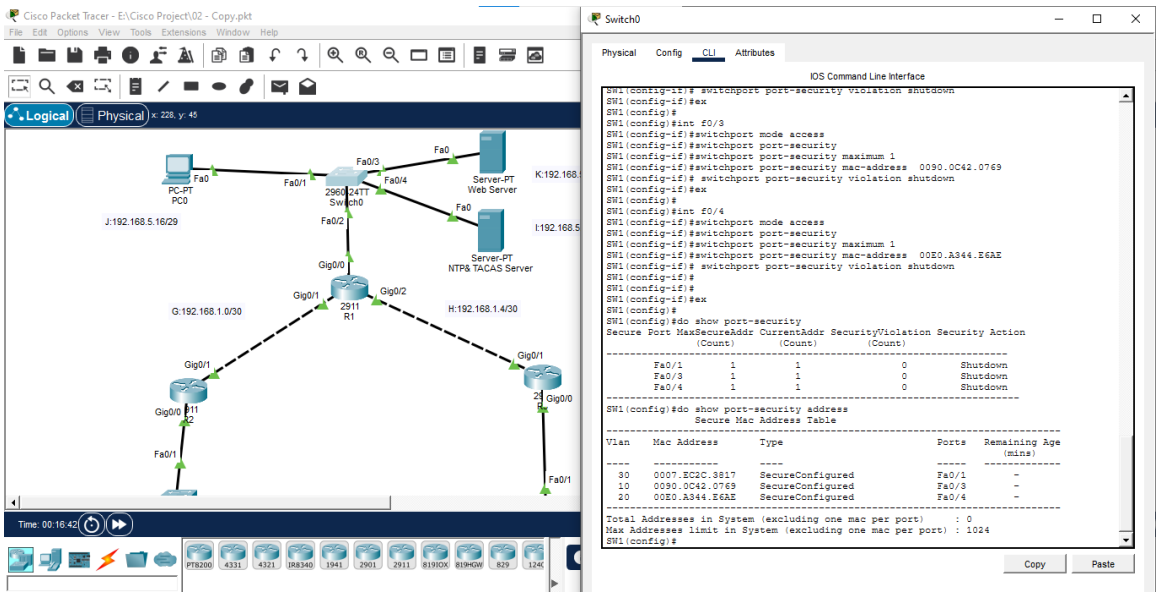


SW02



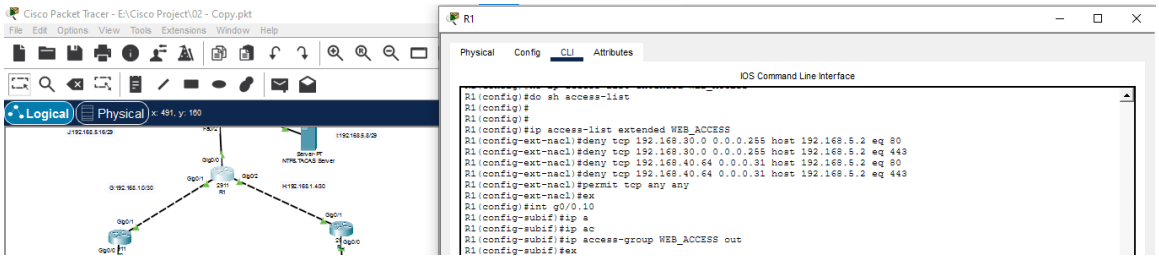
b. Switch 1 - Static MAC addresses with "shutdown" on violation.

int f0/1
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address 0007.EC2C.3817
switchport port-security violation shutdown
exit

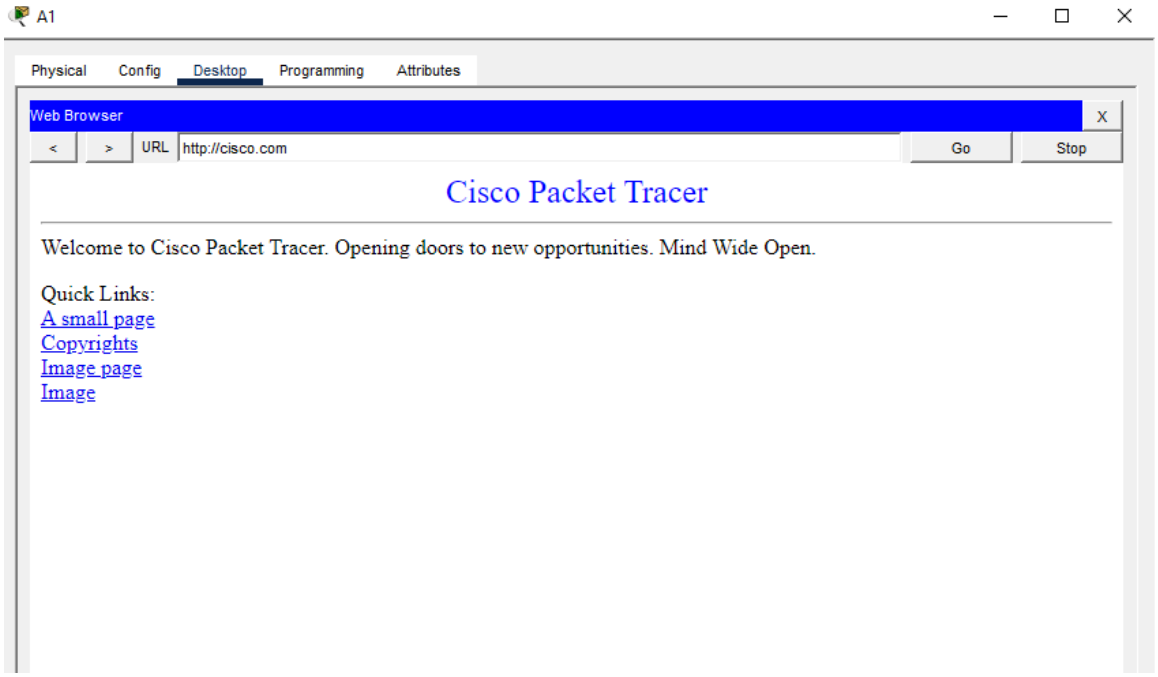


7. Web Access Control

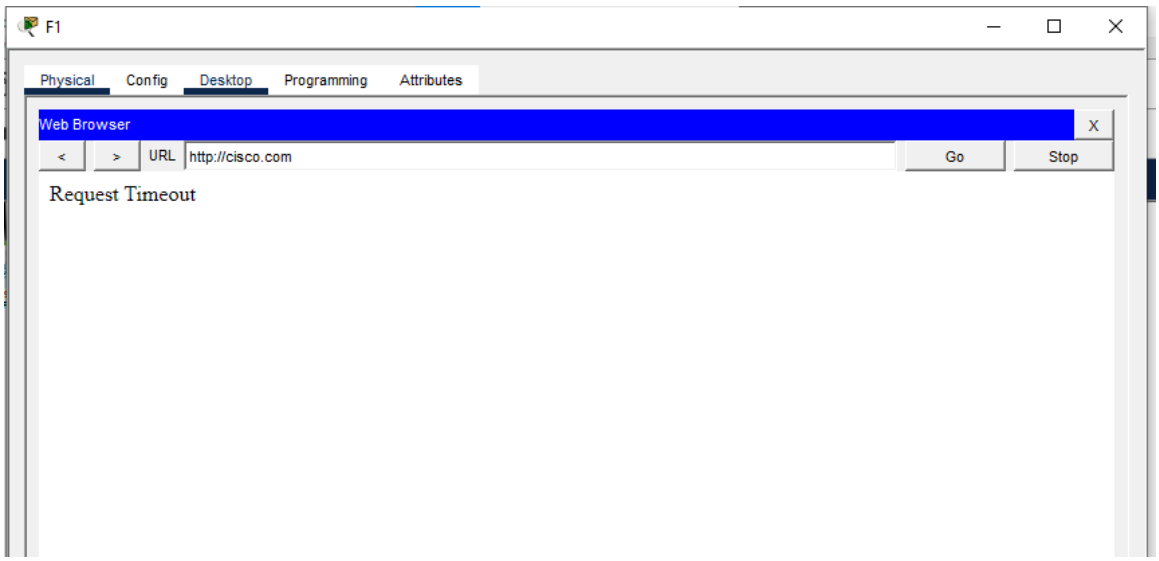
Only Networks A, B, D, and E should access the web server. Use ACLs. Include screenshots.



192.168.10.0



192.168.40.64



Http,Https Not work…..

R.A.J Madhusankha

8. Network Isolation

Only Networks C and F can communicate with each other. Block all other access using ACLs.

```
R2(config)#ip access-list extended C-F-ACCESS
R2(config-ext-nacl)# permit ip 192.168.30.0 0.0.0.255 192.168.40.64 0.0.0.31
R2(config-ext-nacl)# permit ip 192.168.40.64 0.0.0.31 192.168.30.0 0.0.0.255
R2(config-ext-nacl)# deny ip any any
R2(config-ext-nacl)#ex
R2(config)#int g0/0.30
R2(config-if)#ip access-group C-F-ACCESS in
```