Project Name:

Secure Network Infrastructure with Cisco ASA and VPN Integration.

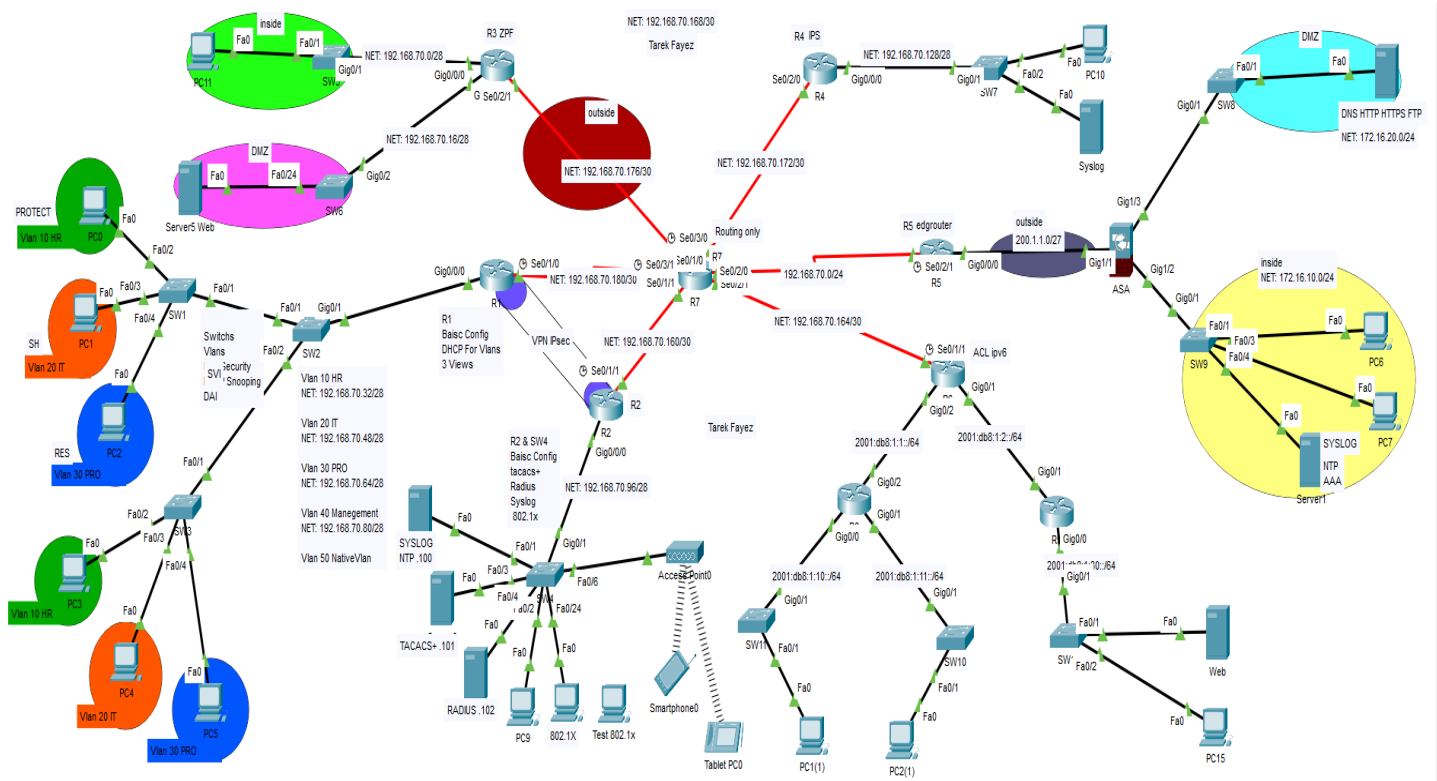
Description:

Designed and implemented a secure network architecture with Cisco ASA, configuring IPS to detect and block malicious traffic. Deployed secure IPsec VPNs for encrypted remote communication, implemented AAA protocols for access control, and applied Layer 2 security measures to protect against threats like VLAN hopping and MAC spoofing and IEEE 802.1x..

Supervised by Dr Sahar El-Shazly at NTI.

This project is designed by Dr Sahar El-Shazly.

Project is configured and implemented by Tarek Fayez Mohamed.



tarekfayez99@gmail.com

First, we have network 192.168.70.0/24 and I will make subnetting for this network.

1. Creating 11 Networks from 192.168.70.0/24.

To create 11 subnets from the 192.168.70.0/24 network, we need to determine the subnet mask that provides at least 11 subnets.

- The original network is 192.168.70.0/24 (256 total IPs).
- To create 11 subnets, we need at least 4 additional bits (since 24=16≥1124=16≥11).
- The new subnet mask will be /28 (24 + 4 = 28).

Each subnet will have 232−28=16232−28=16 IPs, with 14 usable hosts per subnet (excluding network and broadcast addresses).

Subnet Ranges:

No.	Networks		First	Last	Broadcast	Subnet mask
1.		**192.168.70.0/28**	192.168.70.1	192.168.70.14	192.168.70.15	**255.255.255.240**
2.		**192.168.70.16/28**	192.168.70.17	192.168.70.30	192.168.70.31	
3.		**192.168.70.32/28**	192.168.70.33	192.168.70.46	192.168.70.47	
4.		**192.168.70.48/28**	192.168.70.49	192.168.70.62	192.168.70.63	
5.		**192.168.70.64/28**	192.168.70.65	192.168.70.78	192.168.70.79	
6.		**192.168.70.80/28**	192.168.70.81	192.168.70.94	192.168.70.95	
7.		**192.168.70.96/28**	192.168.70.97	192.168.70.110	192.168.70.111	
8.		**192.168.70.112/28**	192.168.70.113	192.168.70.126	192.168.70.127	
9.		**192.168.70.128/28**	192.168.70.129	192.168.70.142	192.168.70.143	
10.		**192.168.70.144/28**	192.168.70.145	192.168.70.158	192.168.70.159	

---

2. Creating 6 Networks (Between Routers)

From the last subnet (192.168.70.160/28), we need to create 6 subnets, each with 2 usable hosts.

- To accommodate 2 hosts, we need 22=422=4 IPs per subnet (2 usable hosts + network + broadcast).
- The subnet mask for each subnet will be /30 (32 - 2 = 30).

Subnet Ranges:

No.	Networks	First	Last	Broadcast	Subnet mask
11.	**192.168.70.160/30**	192.168.70.161	192.168.70.162	192.168.70.163	**255.255.255.252**
12.	**192.168.70.164/30**	192.168.70.165	192.168.70.166	192.168.70.167	
13.	**192.168.70.168/30**	192.168.70.169	192.168.70.170	192.168.70.171	
14.	**192.168.70.172/30**	192.168.70.173	192.168.70.174	192.168.70.175	
15.	**192.168.70.176/30**	192.168.70.177	192. 168.70.178	192.168.70.179	
16.	**192.168.70.180/30**	192.168.70.181	192.168.70.182	192.168.70.183	

tarekfayez99@gmail.com

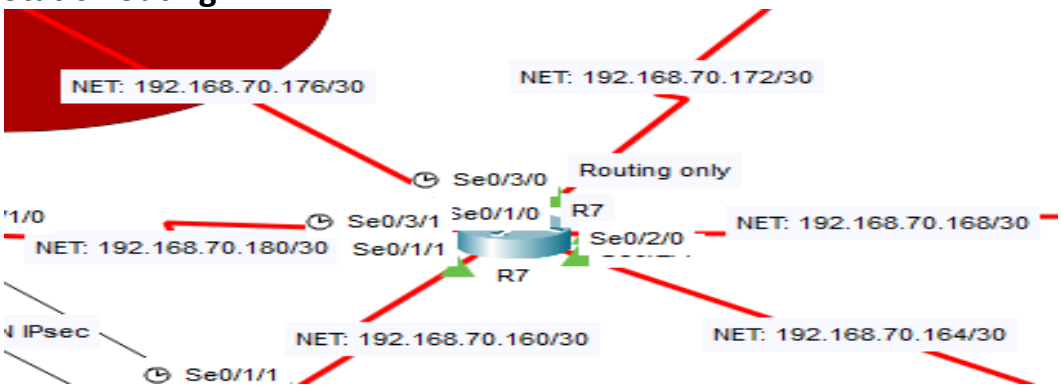
Basic Configuration

```
enable
configure terminal
hostname SW8
enable secret 12345
no ip domain-lookup
ip domain-name cisco.com
security passwords min-length 5
login block-for 10 attempts 5 within 30
crypto key generate rsa general-keys modulus 1024

ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2
username adminSW8 secret 12345
service password-encryption
service timestamps log datetime msec
banner motd #
************ AUTHORIZED ACCESS ONLY **************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED *
************************************************
                  Tarek Fayez
************************************************
#

line console 0
login local
exec-timeout 2 5
logging synchronous
exit

line vty 0 15
login local
transport input ssh
exec-timeout 2 5
logging synchronous
exit
do write memory
```

tarekfayez99@gmail.com

R7 Configuration

- **Basic Configuration**
- **R7 will only handle routing configurations**
- **Make Static Routing**



!!!! Configure Basic Configuration

```
enable
configure terminal
hostname R7
enable secret 12345
no ip domain-lookup
ip domain-name cisco.com
security passwords min-length 5
login block-for 10 attempts 5 within 30
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2
username adminR7 secret 12345
service password-encryption
service timestamps log datetime msec
```

!!!! Configure IP to each interface

```
interface Serial0/1/0
ip address 192.168.70.181 255.255.255.252
no sh
interface Serial0/1/1
ip address 192.168.70.161 255.255.255.252
no sh
interface Serial0/2/0
ip address 192.168.70.165 255.255.255.252
no sh
interface Serial0/2/1
ip address 192.168.70.169 255.255.255.252
no sh
interface Serial0/3/0
ip address 192.168.70.173 255.255.255.252
no sh
interface Serial0/3/1
ip address 192.168.70.177 255.255.255.252
```

tarekfayez99@gmail.com

no sh

!!!! Static Routing

ip route 192.168.70.0 255.255.255.240 192.168.70.178
ip route 192.168.70.16 255.255.255.240 192.168.70.178
ip route 192.168.70.32 255.255.255.240 192.168.70.182
ip route 192.168.70.48 255.255.255.240 192.168.70.182
ip route 192.168.70.64 255.255.255.240 192.168.70.182
ip route 192.168.70.80 255.255.255.240 192.168.70.182
ip route 192.168.70.96 255.255.255.240 192.168.70.162
ip route 192.168.70.112 255.255.255.240 192.168.70.166
ip route 192.168.70.128 255.255.255.240 192.168.70.174
ip route 200.1.1.0 255.255.255.224 192.168.70.170

!!!! Syslog Server

logging trap debugging
logging 192.168.70.100

!!!! NTP Server

ntp server 192.168.70.100
ntp authentication-key 1 md5 cisco123
ntp authenticate
ntp trusted-key 1
ntp update-calendar

!!!! tacacs+ Server

tacacs-server host 192.168.70.101
tacacs-server key cisco123

!!!! radius Server

aaa new-model
radius server RADIUS_SERVER
address ipv4 192.168.70.102
key cisco123

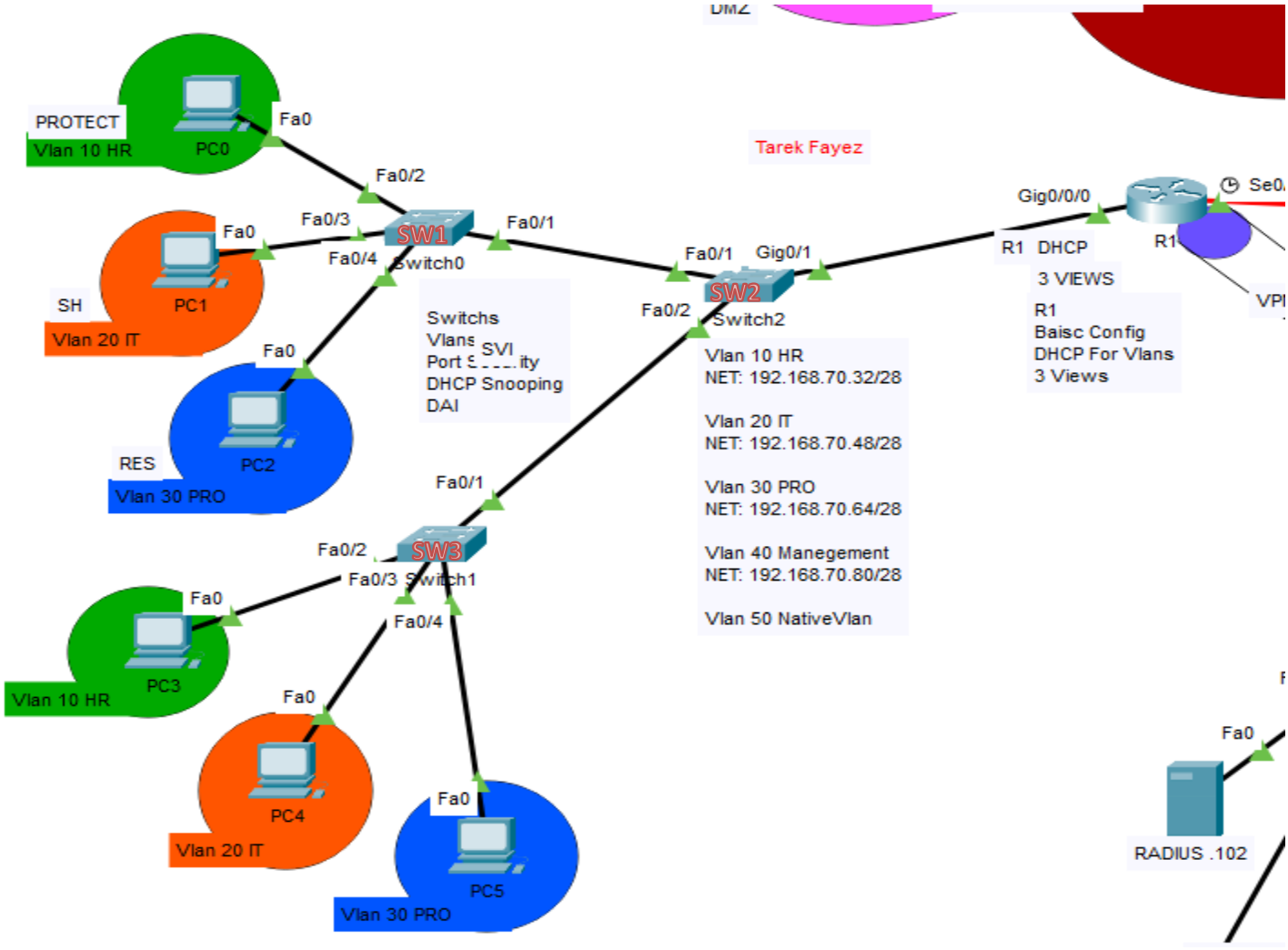
!!!! Enable authentication and ssh

aaa authentication login default group tacacs+ group radius local
line console 0
login authentication default
exec-timeout 2 5
exit
line vty 0 4
login authentication default
transport input ssh
exec-timeout 2 5
exit

tarekfayez99@gmail.com

R1 Configuration

- Basic configuration
- Configure VLANs:
  - **VLAN 10, 20, 30** for data
  - **VLAN 40** for management
  - **VLAN 50** Native Vlan
  - **A dedicated VLAN** for the native VLAN
- Apply **VLAN security** and **STP security mechanisms**.
- Implement **port security**:
  - First detected device: **Protect mode**
  - Second device: **Shutdown mode**
  - Third device: **Restrict mode**
- **R1 will function as a DHCP server** and maintain **three separate DHCP pools** for the three VLANs.
- SVI requires a static IP.
- On router Configure **three user views**: **Admin, Senior, and Junior**.
- **Implement all Layer 2 security measures will Configured on switches.**
  - Port Security.
  - Enable **DHCP Snooping** for network security.
  - Enable **DAI**



tarekfayez99@gmail.com

!!!! Configure Basic Configuration

```
enable
configure terminal
hostname R1
no ip domain-lookup
ip domain-name cisco.com
security passwords min-length 5
crypto key generate rsa general-keys modulus 1024
enable secret 12345
username adminR1 privilege 15 secret 12345
service password-encryption
service timestamps log datetime msec
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2
```

!!!! Configure IP to each interface

```
interface Serial0/1/0
ip address 192.168.70.182 255.255.255.252
exit
interface GigabitEthernet0/0/0
sn sh
exit
interface GigabitEthernet0/0/0.10
encapsulation dot1Q 10
ip address 192.168.70.33 255.255.255.240
exit
interface GigabitEthernet0/0/0.20
encapsulation dot1Q 20
ip address 192.168.70.49 255.255.255.240
exit
interface GigabitEthernet0/0/0.30
encapsulation dot1Q 30
ip address 192.168.70.65 255.255.255.240
exit
interface GigabitEthernet0/0/0.40
encapsulation dot1Q 40
ip address 192.168.70.81 255.255.255.240
exit
interface GigabitEthernet0/0/0.50
encapsulation dot1Q 50
exit

ip route 0.0.0.0 0.0.0.0 192.168.70.181
```

tarekfayez99@gmail.com

!!!! DHCP For Vlans

```
ip dhcp excluded-address 192.168.70.33 192.168.70.34
ip dhcp excluded-address 192.168.70.49 192.168.70.50
ip dhcp excluded-address 192.168.70.65 192.168.70.66

ip dhcp pool VLAN10
 network 192.168.70.32 255.255.255.240
 default-router 192.168.70.33
 dns-server 8.8.8.8
exit
ip dhcp pool VLAN20
 network 192.168.70.48 255.255.255.240
 default-router 192.168.70.49
 dns-server 8.8.8.8
exit
ip dhcp pool VLAN30
 network 192.168.70.64 255.255.255.240
 default-router 192.168.70.65
 dns-server 8.8.8.8
exit
```

!!!! Create 3 Views (ADMIN, JUNIOR, SENIOR)

```
aaa new-model
parser view ADMIN
 secret 12345
 commands exec include setup
 commands exec include all show
 commands exec include telnet
 commands exec include terminal
 commands exec include traceroute

parser view JUNIOR
 secret 12345
 commands exec include ping
 commands exec include reload
 commands exec include ssh

parser view SENIOR
 secret 12345
 commands exec include dir
 commands exec include show
 commands exec include show arp
 commands exec include show ip
 commands exec include show ip interface
 commands exec include show version
```

tarekfayez99@gmail.com

!!!! Syslog Server
logging trap debugging
logging 192.168.70.100

!!!! NTP Server
ntp server 192.168.70.100
ntp authentication-key 1 md5 cisco123
ntp authenticate
ntp trusted-key 1
ntp update-calendar

!!!! tacacs+ Server
tacacs-server host 192.168.70.101
tacacs-server key cisco123

!!!! radius Server
aaa new-model
radius server RADIUS_SERVER
address ipv4 192.168.70.102
key cisco123

!!!! Enable authentication and ssh
aaa authentication login default group tacacs+ group radius local
line console 0
login authentication default
exec-timeout 2 5
exit
line vty 0 4
login authentication default
transport input ssh
exec-timeout 2 5
exit

tarekfayez99@gmail.com

!!!! VPN IPsec on R1

```
access-list 100 permit ip 192.168.70.32 0.0.0.15 192.168.70.96 0.0.0.15
access-list 100 permit ip 192.168.70.48 0.0.0.15 192.168.70.96 0.0.0.15
access-list 100 permit ip 192.168.70.64 0.0.0.15 192.168.70.96 0.0.0.15
access-list 100 permit ip 192.168.70.80 0.0.0.15 192.168.70.96 0.0.0.15

crypto isakmp enable
crypto isakmp policy 10
hash sha
authentication pre-share
group 5
encryption aes 256
lifetime 3600
exit

crypto isakmp key cisco123 address 192.168.70.162
crypto ipsec transform-set R1_R2 esp-aes esp-sha-hmac

crypto map VPN_IPSEC 10 ipsec-isakmp
set peer 192.168.70.162
set pfs group5
set security-association lifetime seconds 900
set transform-set R1_R2
match address 100
exit

interface Serial0/1/0
crypto map VPN_IPSEC
```

tarekfayez99@gmail.com

SW2

!!! DHCP Snooping and Dynamic arp inspection

```
no ip dhcp snooping information option
ip dhcp snooping
ip dhcp snooping vlan 10,20,30,40
ip arp inspection vlan 10,20,30,40

interface range FastEthernet0/1-2
switchport trunk native vlan 50
ip dhcp snooping limit rate 10
switchport mode trunk
switchport nonegotiate

interface GigabitEthernet0/1
switchport trunk native vlan 50
switchport trunk allowed vlan 10,20,30,40
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
```

!!!!STP Security

```
spanning-tree portfast default
spanning-tree portfast bpduguard default
```

!!!! SVI (Management Vlan)

```
interface Vlan40
ip address 192.168.70.83 255.255.255.240
exit
ip default-gateway 192.168.70.81
```

!!!! implement Vlan Security (in all Switches)

```
interface range FastEthernet0/3-24
switchport access vlan 999
switchport mode access
shutdown
```

tarekfayez99@gmail.com

SW1 and SW3

!!! DHCP Snooping and Dynamic arp inspection

ip arp inspection vlan 10,20,30,40
ip dhcp snooping vlan 10,20,30,40
no ip dhcp snooping information option
ip dhcp snooping

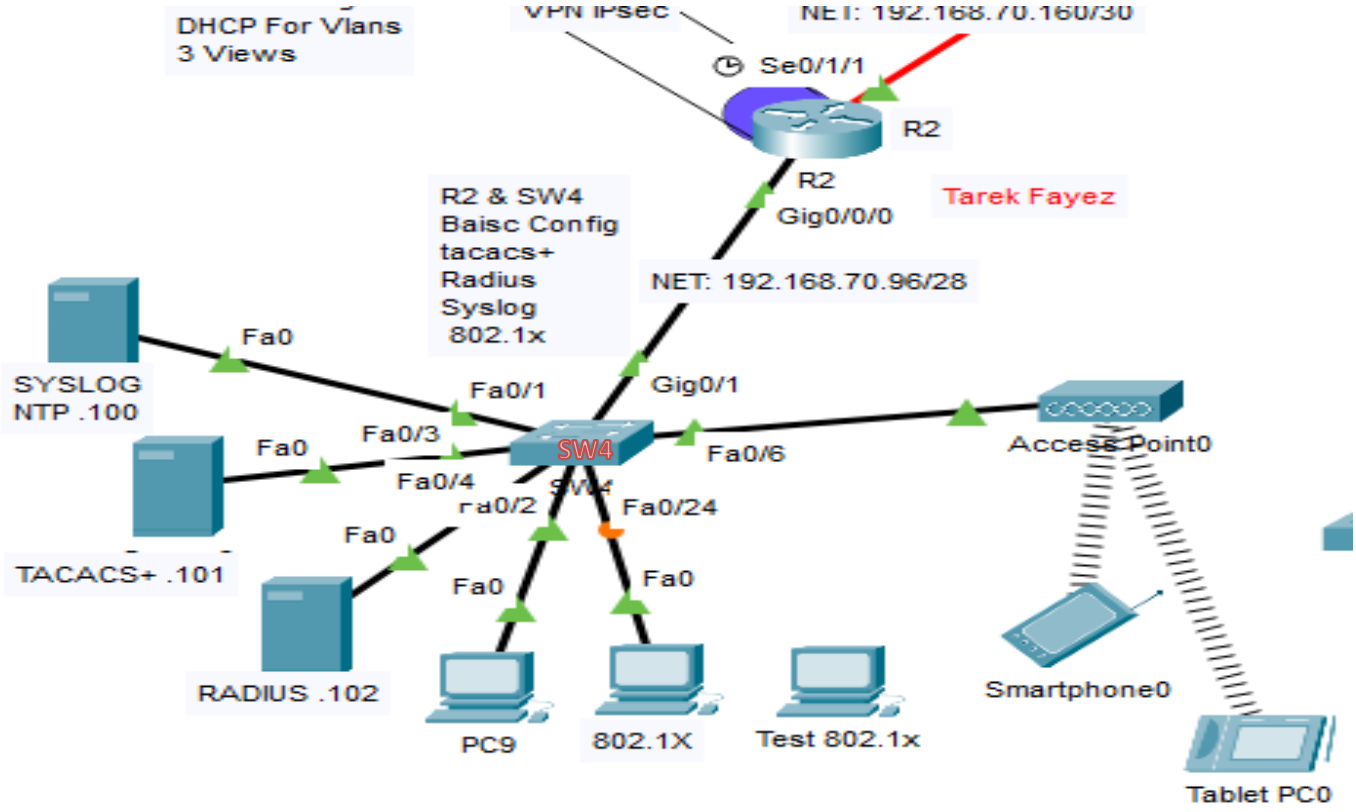
!!!!STP Security

spanning-tree portfast default
spanning-tree portfast bpduguard default
interface FastEthernet0/1
switchport trunk native vlan 50
ip arp inspection trust
ip dhcp snooping trust
switchport mode trunk
interface FastEthernet0/2
switchport access vlan 10
ip dhcp snooping limit rate 10
switchport mode access
switchport port-security
switchport port-security violation protect
interface FastEthernet0/3
switchport access vlan 20
ip dhcp snooping limit rate 10
switchport mode access
switchport port-security
switchport port-security violation shutdown
interface FastEthernet0/4
switchport access vlan 30
ip dhcp snooping limit rate 10
switchport mode access
switchport port-security
switchport port-security violation restrict
interface FastEthernet0/4
switchport access vlan 30
ip dhcp snooping limit rate 10
switchport mode access
interface Vlan40
ip address 192.168.70.82 255.255.255.240
exit
ip default-gateway 192.168.70.81

tarekfayez99@gmail.com

R2 Configuration (Wired & Wireless LANs)

- Enhance **wireless LAN security** by **changing SSID name** and **modifying encryption protocols**.
- Implement a **authentication** approach for login:
    1. **Primary method:** TACACS+
    2. **Secondary method:** RADIUS
    3. **Tertiary method:** Local database
- All routers **(except R5)** must use **AAA authentication** with **TACACS+ as the primary method** and **RADIUS as the secondary method**.
- All routers must **send logs to a Syslog server** located on R2's network.
- Implement **802.1x authentication** for PC 8
- Establish a **site-to-site IPsec VPN** between R1 and R2.




```
enable
configure terminal
hostname R2
enable secret 12345
no ip domain-lookup
ip domain-name cisco.com
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2
username adminR2 privilege 15 secret 12345
service password-encryption
service timestamps log datetime msec
```

tarekfayez99@gmail.com

interface GigabitEthernet0/0/0
ip address 192.168.70.97 255.255.255.240
no sh
interface Serial0/1/1
ip address 192.168.70.162 255.255.255.252
no sh
ip route 0.0.0.0 0.0.0.0 192.168.70.161

logging trap debugging
logging 192.168.70.100

ntp server 192.168.70.100
ntp authentication-key 1 md5 cisco123
ntp authenticate
ntp trusted-key 1
ntp update-calendar

tacacs-server host 192.168.70.101
tacacs-server key cisco123
aaa new-model
radius server RADIUS_SERVER
address ipv4 192.168.70.102
key cisco123
ex
aaa authentication login default group tacacs+ group radius local

line console 0
login authentication default
exec-timeout 2 5
exit
line vty 0 4
login authentication default
transport input ssh
exec-timeout 2 5
exit

!!!! DHCP for wireless

ip dhcp excluded-address 192.168.70.97 192.168.70.105
ip dhcp pool pool_Wireless
network 192.168.70.96 255.255.255.240
default-router 192.168.70.97
dns-server 8.8.8.8
exit

tarekfayez99@gmail.com

!!!! VPN IPsec on R2

```
access-list 100 permit ip 192.168.70.96 0.0.0.15 192.168.70.32 0.0.0.15
access-list 100 permit ip 192.168.70.96 0.0.0.15 192.168.70.48 0.0.0.15
access-list 100 permit ip 192.168.70.96 0.0.0.15 192.168.70.64 0.0.0.15
access-list 100 permit ip 192.168.70.96 0.0.0.15 192.168.70.80 0.0.0.15

crypto isakmp enable
crypto isakmp policy 10
hash sha
authentication pre-share
group 5
encryption aes 256
lifetime 3600
exit

crypto isakmp key cisco123 address 192.168.70.182
crypto ipsec transform-set R1_R2 esp-aes esp-sha-hmac

crypto map VPN_IPSEC 10 ipsec-isakmp
set peer 192.168.70.182
set pfs group5
set security-association lifetime seconds 900
set transform-set R1_R2
match address 100
exit

interface Serial0/1/1
crypto map VPN_IPSEC
```

**********SW4**********

```
enable
configure terminal
hostname SW4
enable secret 12345
no ip domain-lookup
ip domain-name cisco.com
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2
username adminSW4 secret 12345
service password-encryption
service timestamps log datetime msec

aaa new-model
```

!!!! Configure RADIUS Server

```
radius-server host 192.168.70.102 auth-port 1645
radius-server key cisco123
```

tarekfayez99@gmail.com

!!!! Configure AAA for 802.1X

aaa authentication dot1x default group radius
aaa authentication login default group radius local

!!!! Enable 802.1X Globally

dot1x system-auth-control

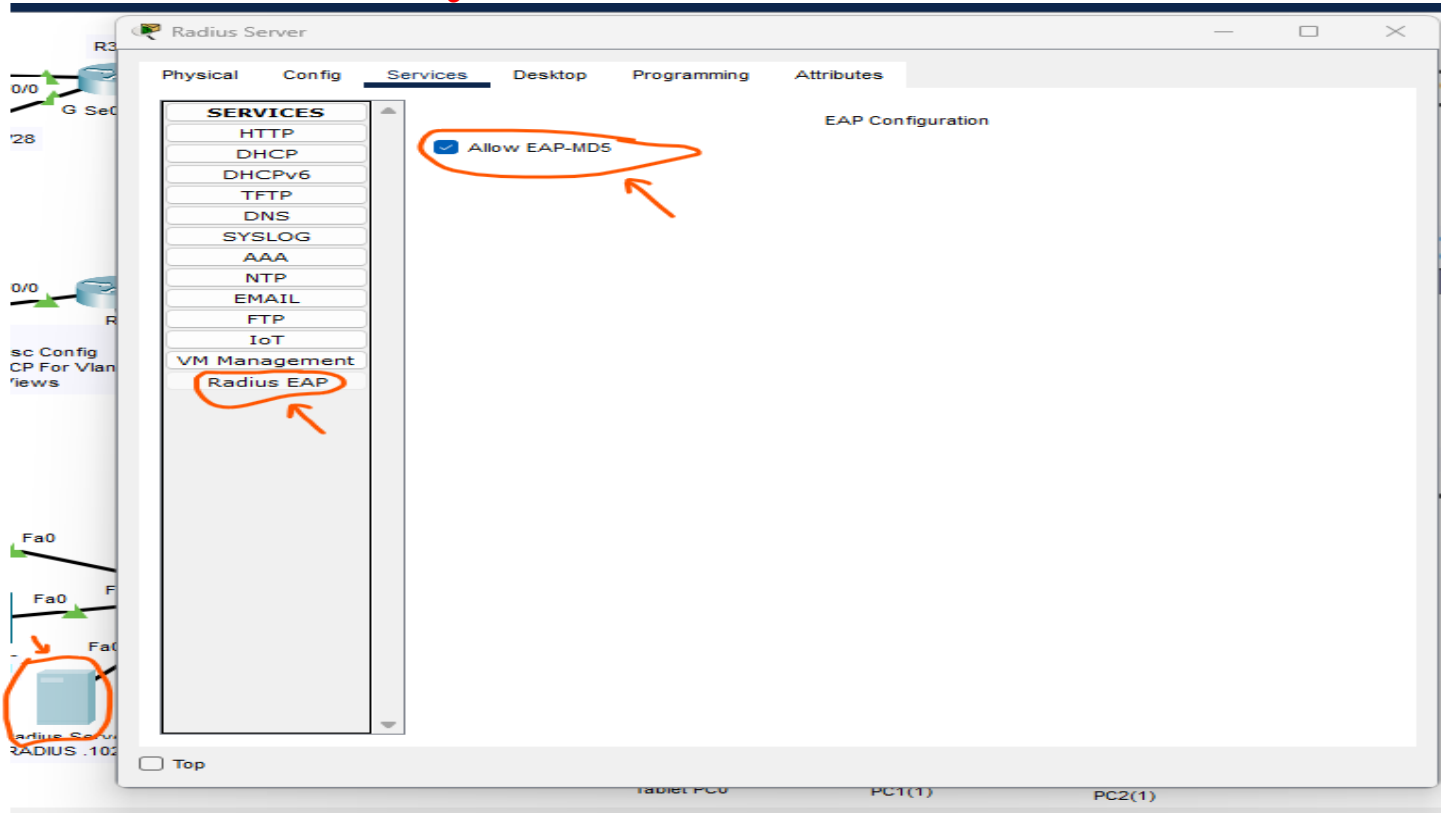
!!!! Configure Interface for 802.1X

interface fas0/5
switchport mode access
authentication port-control auto
dot1x pae authenticator
exit

line console 0
login authentication default
exec-timeout 2 5
exit

line vty 0 4
login authentication default
transport input ssh
exec-timeout 2 5
exit

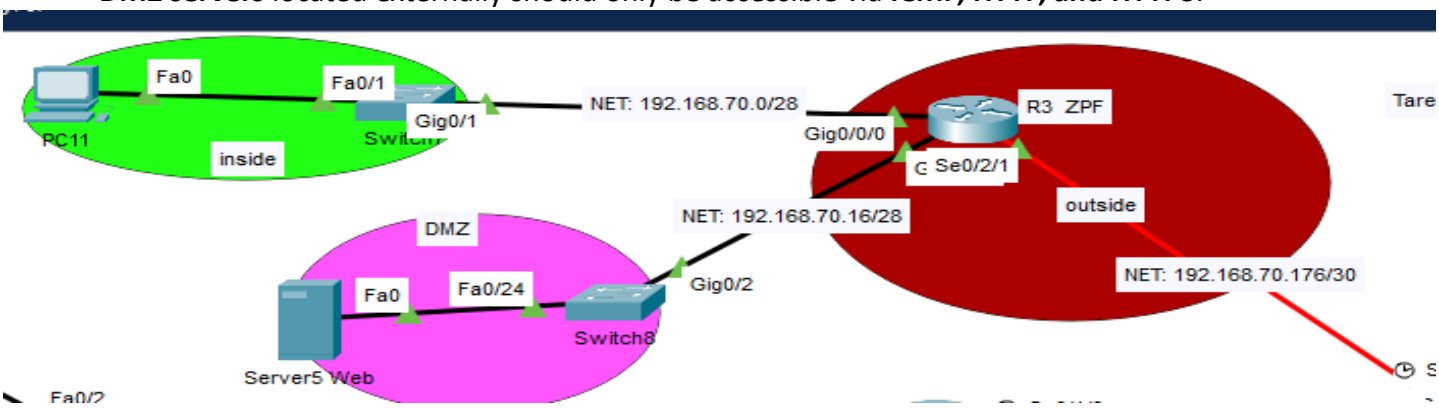
To enable 802.1x you should enable Allow EAP-MD5



tarekfayez99@gmail.com

R3 Configuration (Zone-Based Firewall)

- **Internal users** can access **all external traffic types**.
- **DMZ servers** located externally should only be accessible via **ICMP, HTTP, and HTTPS**.



enable
configure terminal
hostname R3
no ip domain-lookup
ip domain-name cisco.com
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2
security passwords min-length 5
enable secret 12345
username adminR3 secret 12345
service password-encryption
service timestamps log datetime msec

logging trap debugging
logging 192.168.70.100
ntp server 192.168.70.100
ntp authentication-key 1 md5 cisco123
ntp authenticate
ntp trusted-key 1
ntp update-calendar
tacacs-server host 192.168.70.101
tacacs-server key cisco123
aaa new-model
radius server RADIUS_SERVER
address ipv4 192.168.70.102
key cisco123
ex
aaa authentication login default group tacacs+ group radius local
line console 0
login authentication default
exec-timeout 2 5
exit

tarekfayez99@gmail.com

line vty 0 4
login authentication default
transport input ssh
exec-timeout 2 5
exit

interface GigabitEthernet0/0/0
ip address 192.168.70.1 255.255.255.240
no sh
exit
interface GigabitEthernet0/0/1
ip address 192.168.70.17 255.255.255.240
no sh
exit
interface Serial0/2/1
ip address 192.168.70.178 255.255.255.252
no sh
exit
ip route 0.0.0.0 0.0.0.0 192.168.70.177
zone security INSIDE
exit
zone security DMZ
exit
zone security PUBLIC
exit

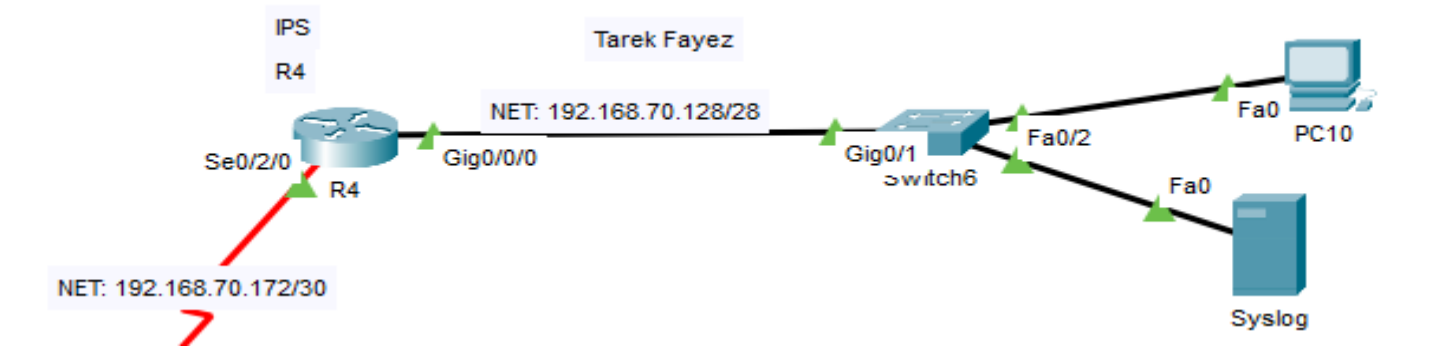
class-map type inspect match-any DMZ_PROTOCOLS match protocol http match protocol https match protocol icmp exit	class-map type inspect match-any INSIDE_PROTOCOLS match protocol icmp match protocol tcp match protocol udp exit
policy-map type inspect DMZ_TO_PUBLIC class type inspect DMZ_PROTOCOLS inspect exit exit	policy-map type inspect INSIDE_TO_PUBLIC class type inspect INSIDE_PROTOCOLS inspect exit exit
zone-pair security PUBLIC_TO_DMZ source PUBLIC destination DMZ service-policy type inspect DMZ_TO_PUBLIC exit	zone-pair security INSIDE_TO_PUBLIC source INSIDE destination PUBLIC service-policy type inspect INSIDE_TO_PUBLIC exit

interface g0/0/1
zone-member security DMZ
interface g0/0/0
zone-member security INSIDE
interface s0/2/0
zone-member security PUBLIC

tarekfayez99@gmail.com

R4 Configuration (IPS - Intrusion Prevention System)

- Internal devices can **ping external networks**, but external networks **cannot initiate pings** to internal devices.




```
enable
configure terminal
hostname R4
enable secret 12345
no ip domain-lookup
ip domain-name cisco.com

crypto key generate rsa general-keys modulus 1024
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2

username adminR4 secret 12345
service password-encryption
service timestamps log datetime msec

interface GigabitEthernet0/0/0
ip address 192.168.70.129 255.255.255.240
no sh

interface Serial0/2/0
ip address 192.168.70.174 255.255.255.252
no sh

ip route 0.0.0.0 0.0.0.0 192.168.70.173

logging trap debugging
logging 192.168.70.100

ntp server 192.168.70.100
ntp authentication-key 1 md5 cisco123
ntp authenticate
ntp trusted-key 1
ntp update-calendar
```

tarekfayez99@gmail.com

tacacs-server host 192.168.70.101
tacacs-server key cisco123
aaa new-model
radius server RADIUS_SERVER
address ipv4 192.168.70.102
key cisco123
ex
aaa authentication login default group tacacs+ group radius local
line console 0
login authentication default
exec-timeout 2 5
exit
line vty 0 4
login authentication default
transport input ssh
exec-timeout 2 5
exit

!!!! Configure IPs IOS

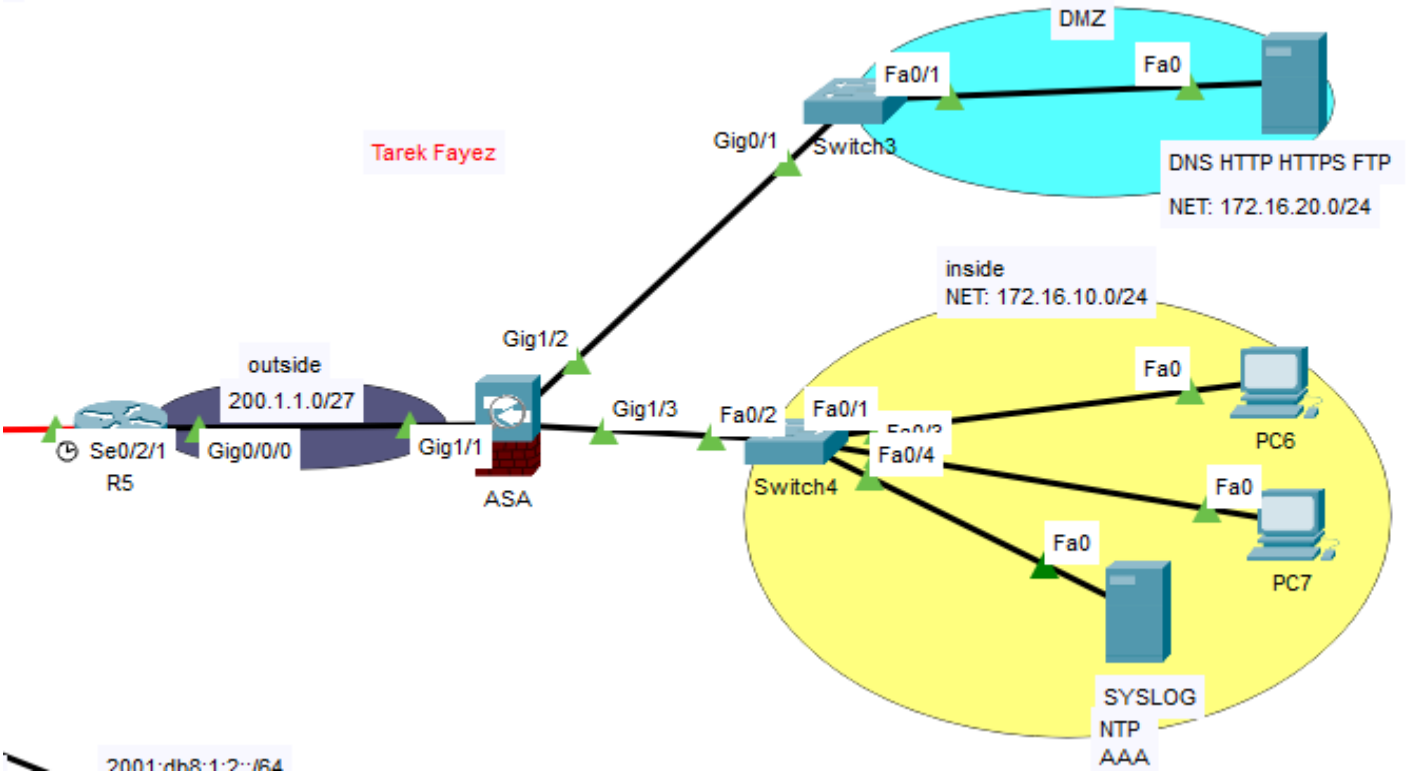
show version
Save the running-config and reload
show version
R1# **mkdir ipsdir**
R1(config)# **ip ips config location flash:ipsdir**
R1(config)# **ip ips name iosips**
R1(config)# **ip ips notify log**
R1(config)# **ip ips signature-category**
R1(config-ips-category)# **category all**
R1(config-ips-category-action)# **retired true**
(config-ips-category-action)# **exit**
R1(config-ips-category)# **category ios_ips basic**
R1(config-ips-category-action)# **retired false**
R1(config-ips-category-action)# **exit**
R1(config-ips-cateogry)# **exit**
Do you want to accept these changes? [confirm] **<Enter>**
R1(config)# **interface g0/0/0**
R1(config-if)# **ip ips iosips out**
R1(config)# **ip ips signature-definition**
R1(config-sigdef)# **signature 2004 0**
R1(config-sigdef-sig)# **status**
R1(config-sigdef-sig-status)# **retired false**
R1(config-sigdef-sig-status)# **enabled true**
R1(config-sigdef-sig-status)# **exit**
R1(config-sigdef-sig)# **engine**
R1(config-sigdef-sig-engine)# **event-action produce-alert**
R1(config-sigdef-sig-engine)# **event-action deny-packet-inline**
R1(config-sigdef-sig-engine)# **exit**
R1(config-sigdef-sig)# **exit**
R1(config-sigdef)# **exit**

tarekfayez99@gmail.com

R5 Configuration (Firewall - Edge Router)

- **R5 acts as the network's edge router**.
- Define three zones:
  - **DMZ (Blue)**
  - **Inside Network (Yellow)**
  - **Outside Network (Purple)**
- Implement **complete firewall configuration** from **hostname setup** to **AAA, Syslog, and NTP server integration**.

8



!!!!R5

```
enable
configure terminal
hostname R5
no ip domain-lookup
ip domain-name cisco.com
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2
security passwords min-length 5
enable secret 12345
username adminR5 secret 12345
service password-encryption
service timestamps log datetime msec
line console 0
login local
exec-timeout 2 5
logging synchronous
```

tarekfayez99@gmail.com

```
exit
line vty 0 15
login local
transport input ssh
exec-timeout 2 5
logging synchronous
exit
do write memory
interface GigabitEthernet0/0/0
ip address 200.1.1.1 255.255.255.224
no sh
interface Serial0/2/1
ip address 192.168.70.170 255.255.255.252
no sh

ip classless
ip route 0.0.0.0 0.0.0.0 192.168.70.169
```

!!!! Syslog Server !!!!!!!

logging trap debugging
logging 172.16.10.2

!!!! NTP Server !!!!!!!!

ntp server 172.16.10.2
ntp authentication-key 1 md5 cisco123
ntp authenticate
ntp trusted-key 1
ntp update-calendar

!!!! tacacs+ Server !!!!!!!!

tacacs-server host 172.16.10.2
tacacs-server key cisco123

!!!! radius Server !!!!!!!!

aaa new-model
radius server RADIUS_SERVER
address ipv4 192.168.70.102
key cisco123

!!!! Enable authentication and ssh !!!!!!!!

aaa authentication login default group tacacs+ group radius local
line console 0
login authentication default
exec-timeout 2 5
exit
line vty 0 4
login authentication default
transport input ssh
exec-timeout 2 5

tarekfayez99@gmail.com

!!! Firewall

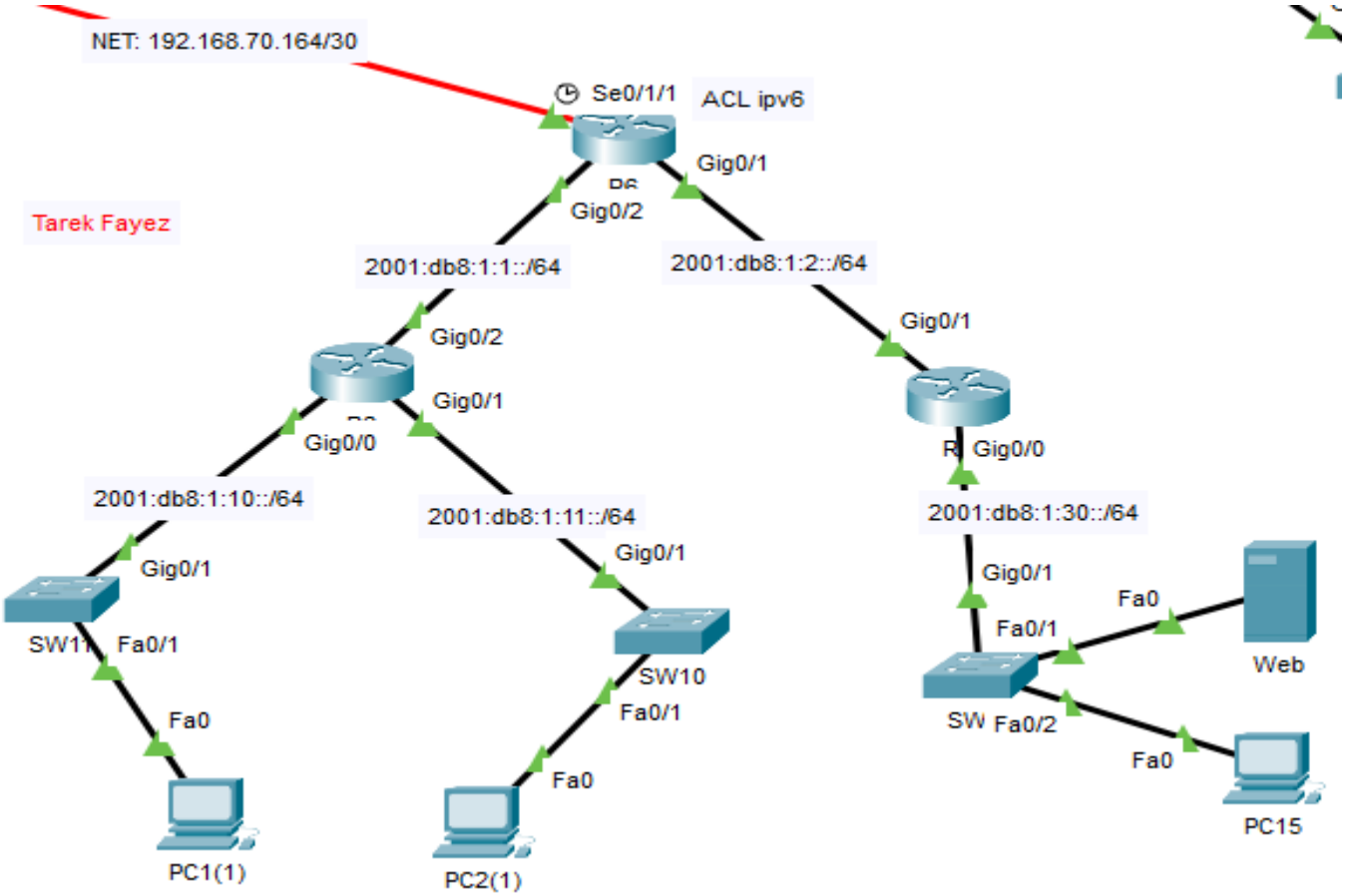
```
hostname ASA
domain-name cisco.com
enable password 12345
username admin password 12345
aaa authentication ssh console LOCAL
crypto key generate rsa modulus 1024
yes
!
interface GigabitEthernet1/1
 nameif OUTSIDE
 security-level 0
 ip address 200.1.1.2 255.255.255.224
 exit
!
interface GigabitEthernet1/2
 nameif INSIDE
 security-level 100
 ip address 172.16.10.1 255.255.255.0
 exit
!
interface GigabitEthernet1/3
 nameif DMZ
 security-level 70
 ip address 172.16.20.1 255.255.255.0
 exit
!
object network INSIDE-NET
 subnet 172.16.10.0 255.255.255.0
 nat (INSIDE,OUTSIDE) dynamic interface

object network DMZ-SERVER
 host 172.16.20.2
 nat (DMZ,OUTSIDE) static 200.1.1.10

!
route OUTSIDE 0.0.0.0 0.0.0.0 200.1.1.1 1
!
access-list dmz extended permit udp any host 172.16.20.2 eq ftp
!
!
yes
ssh 172.16.10.0 255.255.255.0 INSIDE
ssh 200.1.1.1 255.255.255.255 OUTSIDE
ssh timeout 10
```

tarekfayez99@gmail.com

```
!
dhcpd address 172.16.10.5-172.16.10.20 INSIDE
dhcpd dns 8.8.8.8 interface INSIDE
dhcpd lease 20000
dhcpd enable INSIDE

access-list OUTSIDE_DMZ permit icmp any host 172.16.20.2
access-list OUTSIDE_DMZ permit tcp any host 172.16.20.2 eq 80
access-list OUTSIDE_DMZ permit tcp any host 172.16.20.2 eq 443
access-list OUTSIDE_DMZ permit udp any host 172.16.20.2 eq 20
access-list OUTSIDE_DMZ permit tcp any host 172.16.20.2 eq 21
access-list OUTSIDE_DMZ permit udp any host 172.16.20.2 eq 53
access-list OUTSIDE_DMZ permit tcp any host 172.16.20.2 eq 53
access-group OUTSIDE_DMZ in interface OUTSIDE
```

tarekfayez99@gmail.com

R6 Using IPv6 ACL and routing OSPF




```
enable
configure terminal
hostname R6
enable secret 12345
no ip domain-lookup
ip domain-name cisco.com
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2
username adminR6 privilege 15 secret 12345
service password-encryption
service timestamps log datetime msec

interface GigabitEthernet0/0/1
ip address 192.168.70.113 255.255.255.240
no sh

logging trap debugging
logging 192.168.70.100
ntp server 192.168.70.100
ntp authentication-key 1 md5 cisco123
```

tarekfayez99@gmail.com

```
ntp authenticate
ntp trusted-key 1
ntp update-calendar

tacacs-server host 192.168.70.101
tacacs-server key cisco123
aaa new-model
radius server RADIUS_SERVER
address ipv4 192.168.70.102
key cisco123
ex
aaa authentication login default group tacacs+ group radius local

line console 0
login authentication default
exec-timeout 2 5
exit
line vty 0 4
login authentication default
transport input ssh
exec-timeout 2 5
exit
```

tarekfayez99@gmail.com