Summer Intern Final Project NETSEC

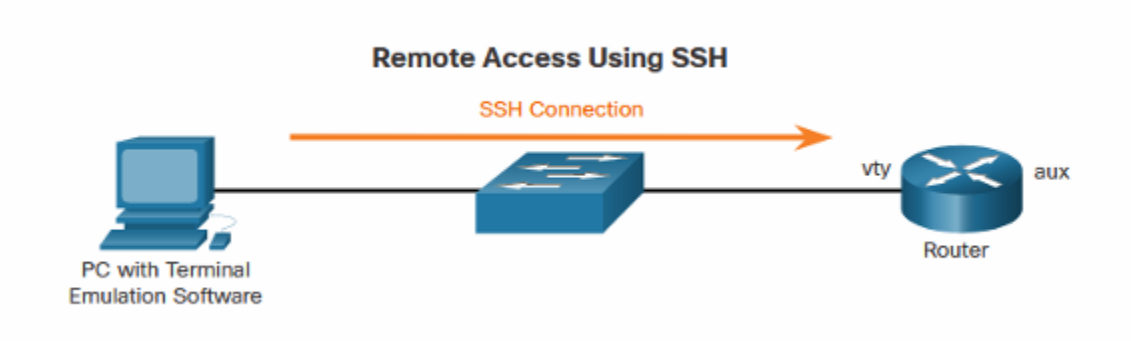
Prepared by: Habiba Mahmoud Abd-Elmoneim

❖ CHECKLIST

Task	Done?
1. Subnet the network 192.168.1.0/24	☑
2. Assign IP addresses to all interfaces	☑
3. Assign IP addresses to all devices (Pcs-Sw-Router)	☑
4. Implement Basic Configurations	☑
5. Enable SSH on routers	☑
6. Configure Role-Based CLI	☑
7. Configure routing protocol OSPF	☑
8. Test connectivity	☑
9. Configure AAA authentication (local or server-based)	☑
10. Configure NTP, SYSLOG	☑
11. Apply ACL	☑
12. Apply ZPF	☑
13.Configure Vlans and L2 port Security	☑
14.VPN Implementation	☑
15.Write the final project report	☑

➢ Secure Remote Access (SSH) :

- SSH enables users to connect to and manage remote servers securely.
- SSH uses strong authentication methods, such as public-key cryptography, to verify the identity of users and systems.



Configuration:

```
R2(config)#Hostname R2
R2(config)#no ip domain lookup
R2(config)#ip domain-name netsec.com
R2(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R2.netsec.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:10:11.850: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#username Habiba secret cisco
R2(config)#line vty 0 15
R2(config-line)#login local
R2(config-line)#transport input ssh
R2(config-line)#exit
R2(config)#
```

Verification:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l Habiba 10.0.0.25

Password:
```

- **OSPF Routing:**

Router	Connected Networks
R0	1. 192.168.1.100/30 2. 192.168.1.32/29 3. 192.168.1.40/29
R1	1. 192.168.1.112/30 2. 192.168.1.116/30 3. 192.168.1.104/30 4. 192.168.1.108/30
R2	1. 192.168.1.64/29 2. 192.168.1.112/30
R3	1. 192.168.1.16/29 2. 192.168.1.24/29 3. 192.168.1.96/30
R4	1. 192.168.1.48/29 2. 192.168.1.56/29 3. 192.168.1.108/30
R5	1. 192.168.1.80/29 2. 192.168.1.88/30 3. 192.168.1.92/30
R6	1. 192.168.1.116/30 2. 192.168.1.0/28
R7	1. 192.168.1.92/30 2. 192.168.1.100/30 3. 192.168.1.104/30 4. 192.168.1.96/30
R8	1. 192.168.1.88/30 2. 192.168.1.72/29

Configuration:

```
R3(config)#router ospf 1
R3(config-router)#network 192.168.1.88 0.0.0.3 area 0
R3(config-router)#network 192.168.1.72 0.0.0.7 area 0
R3(config-router)#
```

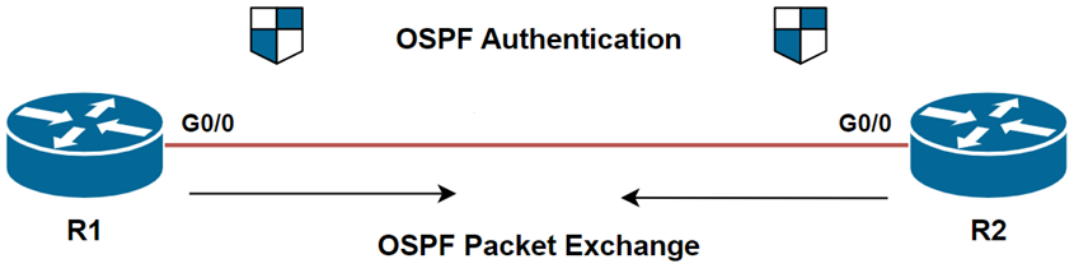
Verification:

```
R1#sh ip ospf neighbor
```

➢ Ospf Authentication:

• Enable OSPF authentication to protect routing updates from tampering or spoofing.

• This ensures only trusted routers with the correct key can participate in OSPF neighbor relationships.



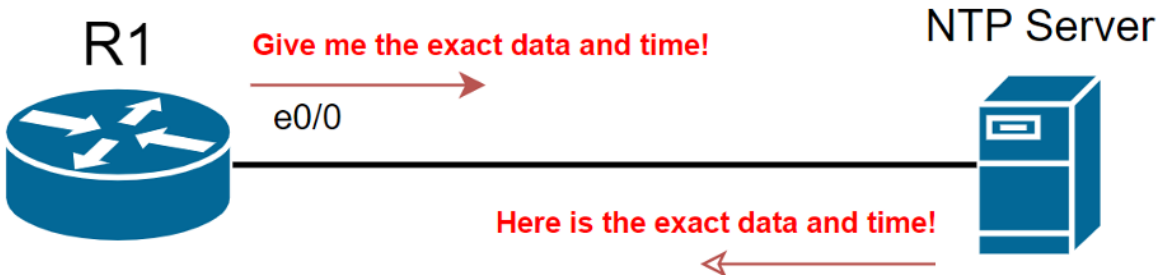
Configuration:

```
R1(config)#int s0/1/0
R1(config-if)#ip ospf message-digest-key 1 md5 cisco
R1(config-if)#ip ospf authentication message-digest
R1(config-if)#
```

```
R1(config)#router ospf 1
R1(config-router)#passive
R1(config-router)#passive-interface g0/0/0
R1(config-router)#
```

➢ NTP Configuration:

- Ensure all network devices maintain synchronized and accurate time.



Configuration:

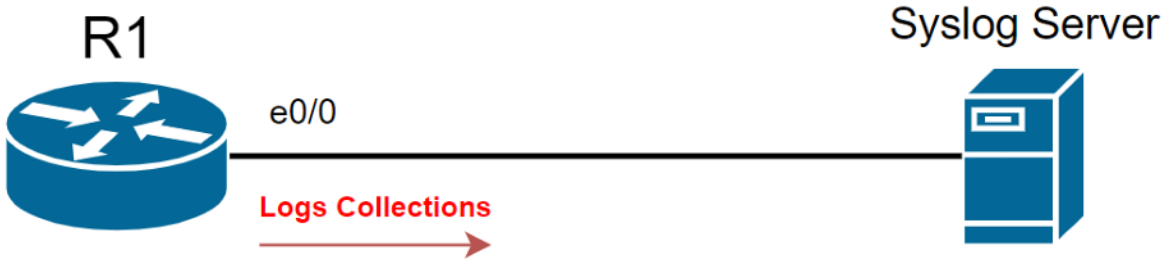
```
R7#sh running-config | include ntp
ntp server 192.168.1.27
R7#
```

Verification:

```
R7#sh clock detail
*22:46:36.509 UTC Sat Jul 19 2025
Time source is hardware calendar
R7#
```

➢ Syslog Configuration:

• To send system logs from network devices to a centralized Syslog server for storage and analysis.

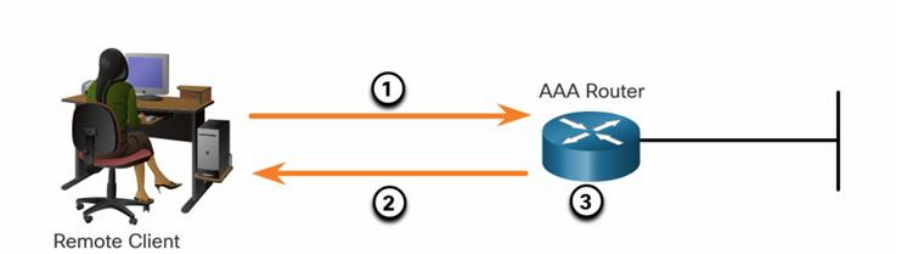


Configuration:

```
R7(config)#logging 192.168.1.26
R7(config)#loggng on
```

- **Local AAA Authentication** (R1,R7) :

It means verifying user credentials directly on the device (like a router or switch) without relying on an external authentication server.



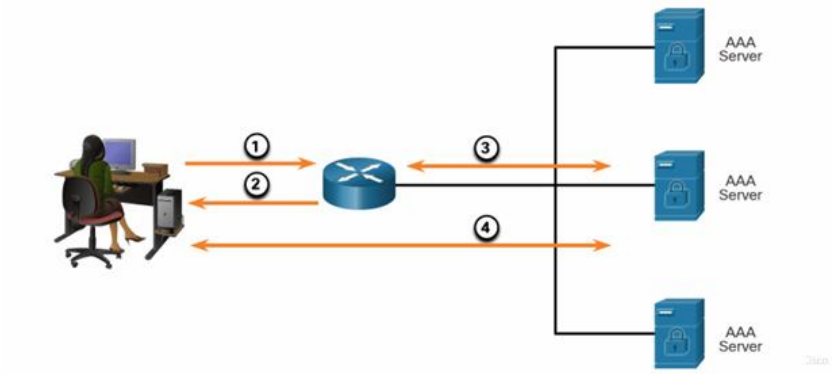
Configuration:

```
R2(config)#username Habiba secret cisco
R2(config)#aaa new-model
R2(config)#aaa authentication login default local enable
R2(config)#end
```

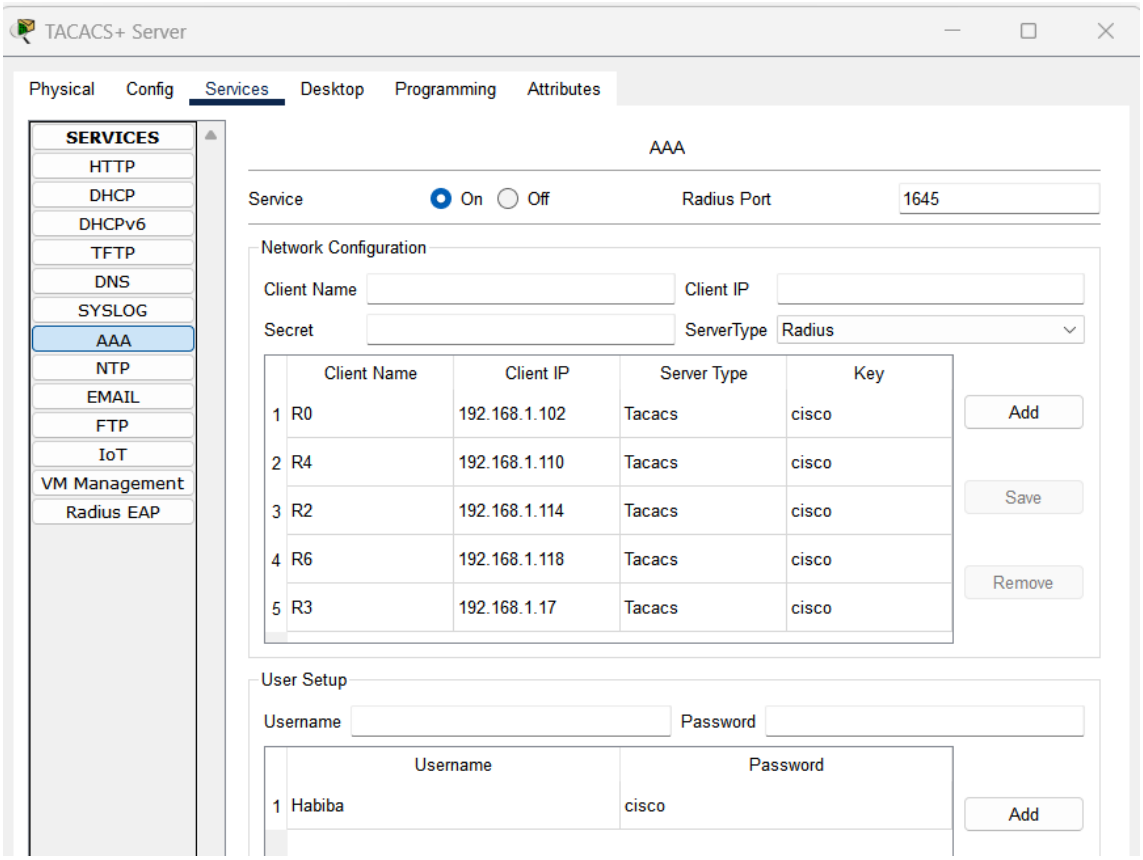
1. enable: Uses the enable password for authentication.
2. local: Uses the local username database for authentication.

- **Server-Based AAA:**

It means verifying user credentials through an external authentication server (such as a RADIUS or TACACS+ server.

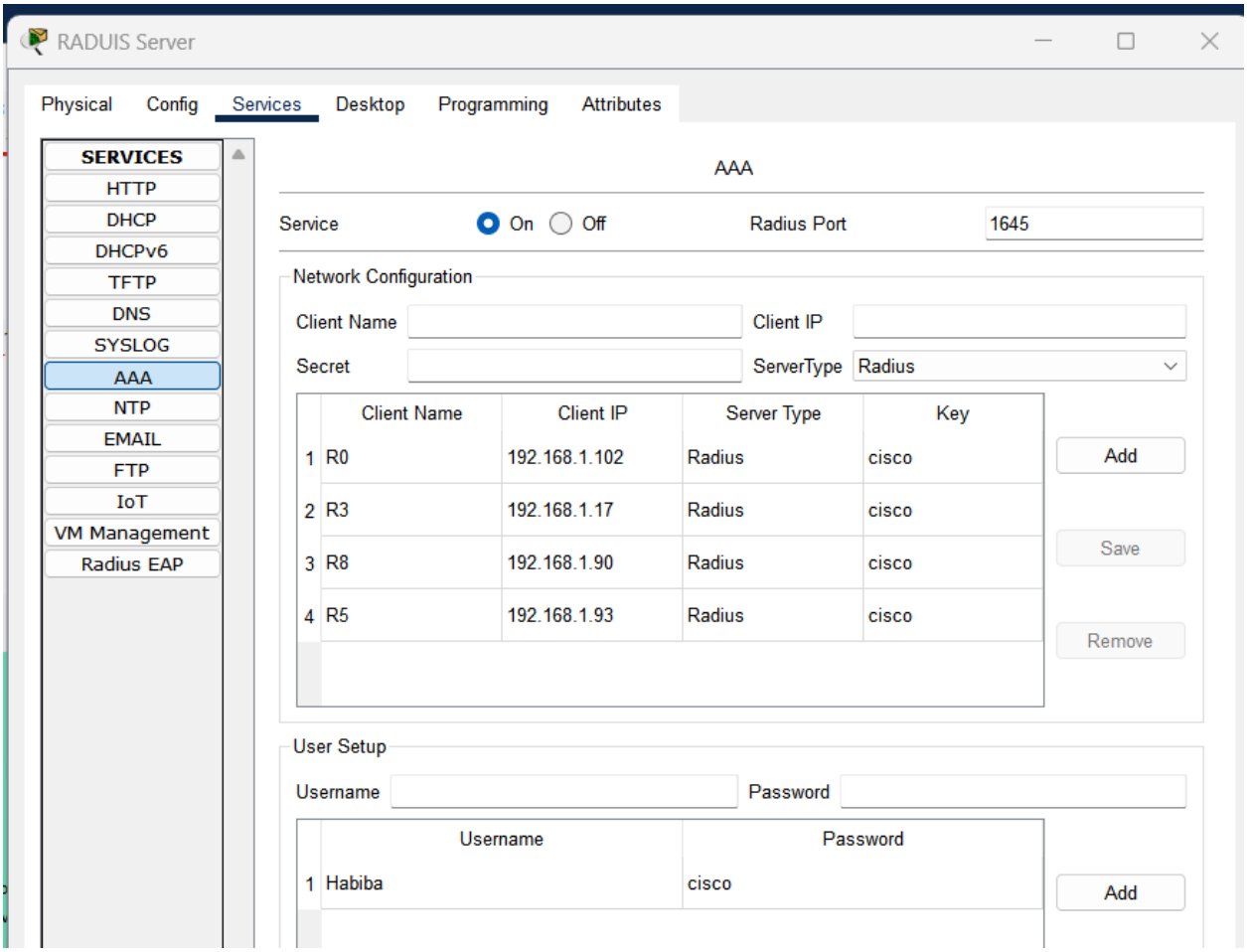


Configure TACACS+ Servers :




```
R2(config)#username Habiba secret cisco
R2(config)#aaa new-model
R2(config)#tacacs-server host 192.168.1.19
R2(config)# tacacs-server key cisco
R2(config)#aaa authentication login default group tacacs+ local
R2(config)#
```

Configure RADIUS Servers :




```
R3(config)#username Habiba secret cisco
R3(config)#aaa new-model
R3(config)#radius server RADIUS_SERVER
R3(config-radius-server)#address ipv4 192.168.1.18 auth-port 1645
R3(config-radius-server)#key cisco
```

```
R2(config-radius-server)#
R2(config-radius-server)#aaa authentication login default group tacacs+ local
R2(config)#
```

➢ Access Control Lists (ACLs) :

• ACLs are used to filter and control traffic between VLANs, and between LAN and WAN.

• To filter and control traffic flow based on IP addresses and protocols.

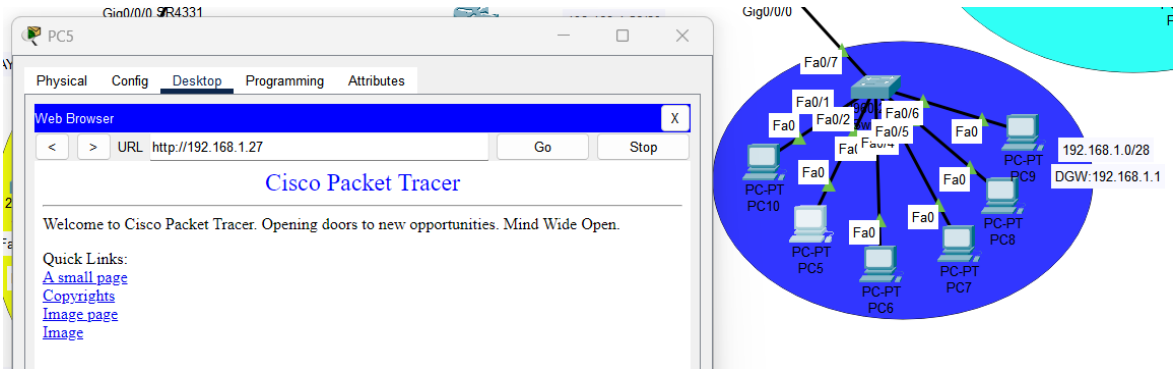
Extended ACLS:

• SURFING - This will permit inside HTTP and HTTPS traffic to exit to the internet.

```
Extended IP access list SURFING
    10 permit tcp 192.168.1.0 0.0.0.15 any eq www
    20 permit tcp 192.168.1.0 0.0.0.15 any eq 443
    30 deny ip any any
```

• BROWSING :
This will only permit returning web traffic to the inside hosts while all
other traffic exiting the R1 G0/0/0 interface is implicitly denied .

```
Extended IP access list BROWSING
    10 permit tcp any 192.168.1.0 0.0.0.15 established
```



Extended ACL 150 :

For Mitigate Spoofing Attacks

- All zeros addresses
- Broadcast addresses
- Local host addresses (127.0.0.0/8)
- Reserved private addresses (RFC 1918)
- IP multicast address range (224.0.0.0/4)

```
Extended IP access list 150
    10 deny ip host 0.0.0.0 any
    20 deny ip 10.0.0.0 0.255.255.255 any
    30 deny ip 127.0.0.0 0.255.255.255 any
    40 deny ip 172.16.0.0 0.15.255.255 any
    50 deny ip 224.0.0.0 15.255.255.255 any
    60 deny ip host 255.255.255.255 any
```

Extended ACL 107:
For Mitigate ICMP Attacks: Deny all

```
Extended IP access list 107
    10 deny icmp any any echo-reply
    20 deny icmp any any unreachable
    30 deny icmp any any
    40 permit icmp any any
```

Standard ACL:
For Permit Necessary Traffic (SSh)

```
Standard IP access list VTY_ACCESS_SSH
    10 permit any
    20 deny any
```

Verification:

```
show access-lists

show ip interface G0/0
```

- **Zone-Based Policy Firewalls(ZPF):**
- **IN-to-Out policy:**

Step 1.2. Create Zones and Assign Zones to Interfaces

```
zone INSIDE
  Member Interfaces:
    GigabitEthernet0/0/1


zone OUTSIDE
  Member Interfaces:
    Serial0/1/0


zone DMZ
  Member Interfaces:
    GigabitEthernet0/0/0
```

```
Class-map: IN-OUT-CLASS-MAP (match-any)
  Match: protocol http
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol https
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol ssh
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol icmp
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol ntp
    42 packets, 8274 bytes
    30 second rate 0 bps
  Match: protocol syslog
    0 packets, 0 bytes
    30 second rate 0 bps
  Inspect
```

Step 3. Identify Traffic (Http/Https/SSh/ntp/syslog)

Step 4. Define an Action (inspect)

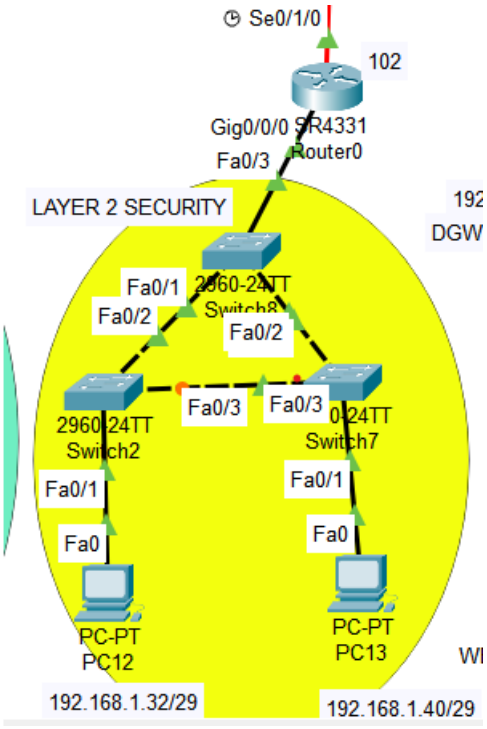
Step 5. Identify a Zone-Pair and Match to a Policy

```
policy exists on zp IN-OUT-ZPAIR
 Zone-pair: IN-OUT-ZPAIR

  Service-policy inspect : IN-OUT-POLICY-MAP
```

And the Same for OUT-to-DMZ policy.

➢ Layer 2 Security:



1- Create vlans

- Vlan 10(pc12-pc13)
  192.168.1.32/29
- Vlan 99 (managment)
  (for switches)
  (192.168.1.40/29)

2-Configure a trunk port between

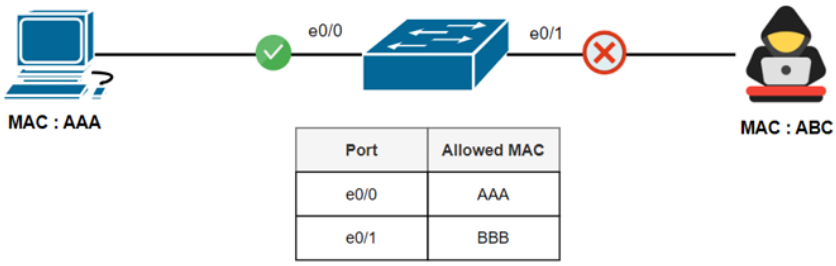
- Switchport mode access :fa0/1
- Switchport mode trunk between switches and router
  (Trunk allowed for vlan 10,99)

3-Inter-VLAN routing:

G0/0/0

1- G0/0/0.10 192.168.1.33/29
2- G0/0/0.99 192.168.1.41/29

4-Applying port security for vlan 10:



Port	Allowed MAC
e0/0	AAA
e0/1	BBB

• Port Security restricts access to the switch ports based on MAC addresses, protecting against unauthorized devices.

```
sw2(config-if)#int fa0/1
sw2(config-if)#switchport mode access
sw2(config-if)#switchport port-security
sw2(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
sw2(config-if)#switchport port-security violation shutdown
sw2(config-if)#
```

Verification:

```
show port-security

show port-security interface e0/1
```

➢ VPN Implementation :

VPN Configurations Steps

➢ Define ISAKMP/IKE Phase 1 Policy

• Define encryption, hashing, authentication method, and Diffie-Hellman group.

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encr aes
R2(config-isakmp)#hash sha
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)#group 5
R2(config-isakmp)#lifetime 700
R2(config-isakmp)#
```

➢ Define Pre-shared Key

• Set a shared key for peer authentication.

```
R2(config-isakmp)#crypto isakmp key cisco address 192.168.1.114
```

➢ Configure IPsec Phase 2 Transform Set

• Define encryption and integrity methods used in IPsec tunnel.

```
R2(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R2(config)#
```

➢ Configure IPsec Phase 2 Transform Set

• Specify which traffic should be encrypted over the VPN.

```
R2(config)#access-list 140 permit ip 192.168.1.72 0.0.0.7 192.168.1.64 0.0.0.7
R2(config)#
```

➢ Create Crypto Map

• Bind IPsec settings to the crypto map and link to the access list.

```
R2(config-crypto-map)#crypto map VPN-MAP 10 ipsec-isakmp
R2(config-crypto-map)#set peer 192.168.1.90
R2(config-crypto-map)#set transform-set VPN-SET
R2(config-crypto-map)#match address 140
R2(config-crypto-map)#exit
R2(config)#
```

➢ Bind Crypto Map to WAN Interface

• Apply the crypto map to the outbound interface.

```
R2(config)#int s0/1/0
R2(config-if)#crypto map VPN-MAP
```

Security Measures for VPN

• Strong encryption algorithms (AES 256)

• SHA hashing for integrity

• Pre-Shared Keys with complexity

• Lifetime and session monitoring

• ACL to limit interesting traffic only

• Logging VPN events