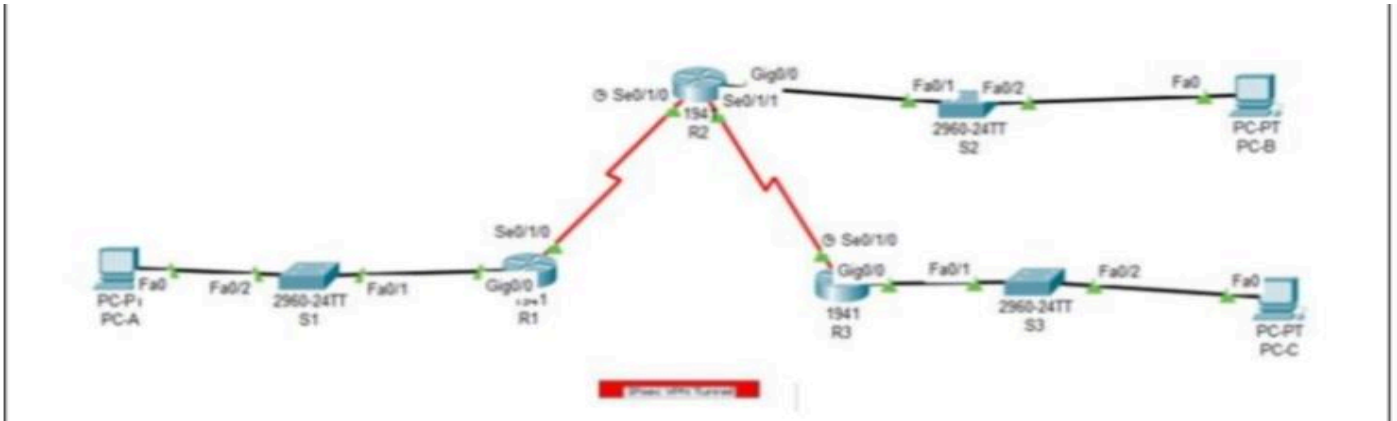
Site_to_site PK

Practical No. 10

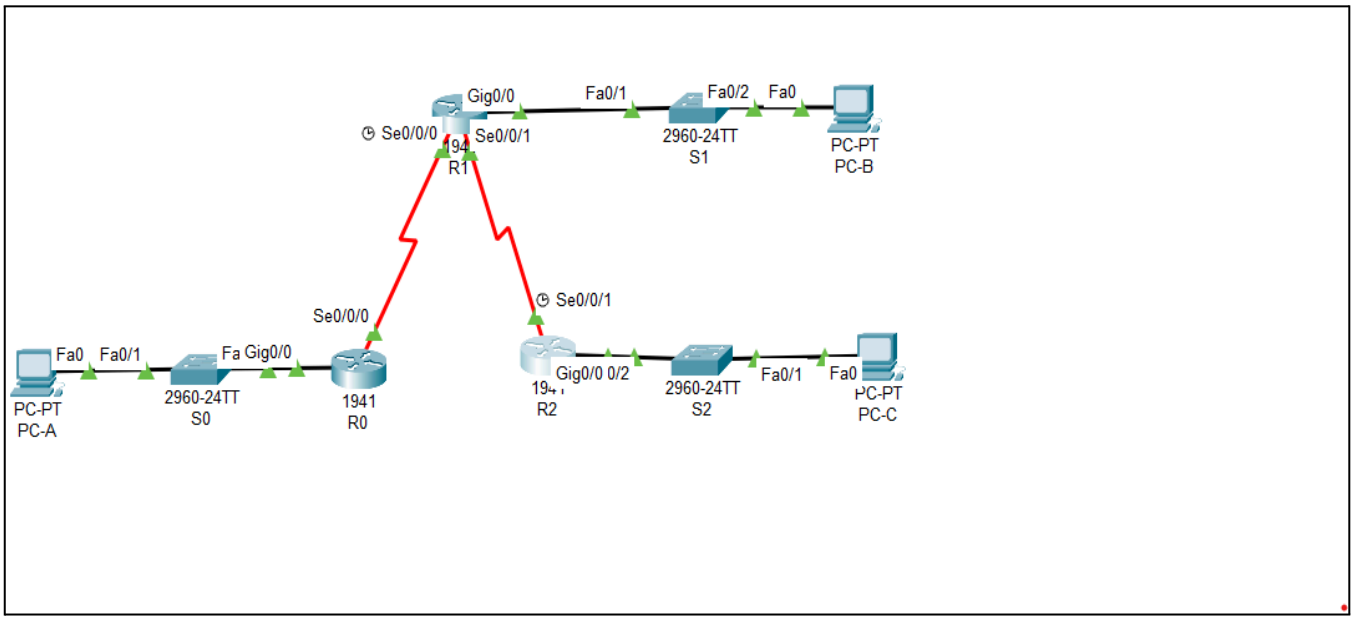
Create the following topology and

- Configure and verify R1 to support a site-to-site IPsec VPN with R3.



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
	se0/1/0	10.1.1.2	255.255.255.252	N/A
R2	gig0/0	192.168.2.1	255.255.255.0	N/A
	se0/1/0	10.1.1.1	255.255.255.252	N/A
	se0/1/1	10.2.2.1	255.255.255.252	N/A
R3	gig0/0	192.168.2.1	255.255.255.0	N/A
	se0/1/0	10.2.2.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1



Part 1: Configure IPsec Parameters on R1
Step 1: Test connectivity.
Ping from PC–A to PC–C.

Step 2: Enable the Security Technology package.
a. Enable the security technology package by using the following command to enable the package.

R1(config)# license boot module c1900 technology–package securityk9

b. Accept the end–user license agreement.

c. Save the running–config and reload the router to enable the security license.

d. Verify that the Security Technology package has been enabled by using the show version command.

Step 3: Identify interesting traffic on R1.
Configure ACL 110 to identify the traffic from the LAN on R1 to the LAN on R3 as interesting. This interesting traffic will trigger the IPsec VPN to be implemented when there is traffic between the R1 to R3 LANs. All other traffic sourced from the LANs will not be encrypted. Because of the implicit deny all, there is no need to configure a deny ip any any statement.

R1(config)# access–list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Step 4: Configure the IKE Phase 1 ISAKMP policy on R1.
Configure the crypto ISAKMP policy 10 properties on R1 along with the shared crypto key vpnpa55. Refer to the ISAKMP Phase 1 table for the specific parameters to configure. Default values do not have to be configured. Therefore, only the encryption method, key exchange method, and DH method must be configured.

Note: The highest DH group currently supported by Packet Tracer is group 5. In a production network, you would configure at least DH 14.

R1(config)# crypto isakmp policy 10

R1(config–isakmp)# encryption aes 256

R1(config–isakmp)# authentication pre–share

R1(config–isakmp)# group 5

R1(config–isakmp)# exit

R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2

Step 5: Configure the IKE Phase 2 IPsec policy on R1.

a. Create the transform-set VPN-SET to use esp-aes and esp-sha-hmac.

R1(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

b. Create the crypto map VPN-MAP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map.

R1(config)# crypto map VPN-MAP 10 ipsec-isakmp

R1(config-crypto-map)# description VPN connection to R3

R1(config-crypto-map)# set peer 10.2.2.2

R1(config-crypto-map)# set transform-set VPN-SET

R1(config-crypto-map)# match address 110

R1(config-crypto-map)# exit

Step 6: Configure the crypto map on the outgoing interface.

Bind the VPN-MAP crypto map to the outgoing Serial 0/0/0 interface.

R1(config)# interface s0/0/0

R1(config-if)# crypto map VPN-MAP

Part 2: Configure IPsec Parameters on R3

Step 1: Enable the Security Technology package.

a. On R3, issue the show version command to verify that the Security Technology package license information has been enabled.

b. If the security technology package has not been enabled, enable the package and reload R3.

Step 2: Configure router R3 to support a site-to-site VPN with R1.

Configure reciprocating parameters on R3. Configure ACL 110 to identify the traffic from the LAN on R3 to the LAN on R1 as interesting.

R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

Step 3: Configure the IKE Phase 1 ISAKMP properties on R3.

Configure the crypto ISAKMP policy 10 properties on R3 along with the shared crypto key vpnpa55.

R3(config)# crypto isakmp policy 10

R3(config-isakmp)# encryption aes 256

R3(config-isakmp)# authentication pre-share

R3(config-isakmp)# group 5

R3(config-isakmp)# exit

R3(config)# crypto isakmp key vpnpa55 address 10.1.1.2

Step 4: Configure the IKE Phase 2 IPsec policy on R3.
c. Create the transform-set VPN-SET to use esp-aes and esp-sha-hmac.

R3(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

d. Create the crypto map VPN-MAP to bind all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map.

R3(config)# crypto map VPN-MAP 10 ipsec-isakmp

R3(config-crypto-map)# description VPN connection to R1

R3(config-crypto-map)# set peer 10.1.1.2

R3(config-crypto-map)# set transform-set VPN-SET

R3(config-crypto-map)# match address 110

R3(config-crypto-map)# exit

Step 5: Configure the crypto map on the outgoing interface.
Bind the VPN-MAP crypto map to the outgoing Serial 0/0/1 interface.

R3(config)# interface s0/0/1

R3(config-if)# crypto map VPN-MAP

Part 3: Verify the IPsec VPN
Step 1: Verify the tunnel prior to interesting traffic.
Issue the show crypto ipsec sa command on R1. Notice that the number of packets encapsulated, encrypted, decapsulated, and decrypted are all set to 0.

Step 2: Create interesting traffic.
Ping PC-C from PC-A.

Step 3: Verify the tunnel after interesting traffic.
On R1, re–issue the show crypto ipsec sa command. Notice that the number of packets is more than 0, which indicates that the IPsec VPN tunnel is working.

Step 4: Create uninteresting traffic.
Ping PC–B from PC–A. Note: Issuing a ping from router R1 to PC–C or R3 to PC–A is not interesting traffic.

Step 5: Verify the tunnel.
On R1, re–issue the show crypto ipsec sa command. Notice that the number of packets has not changed, which verifies that uninteresting traffic is not encrypted.

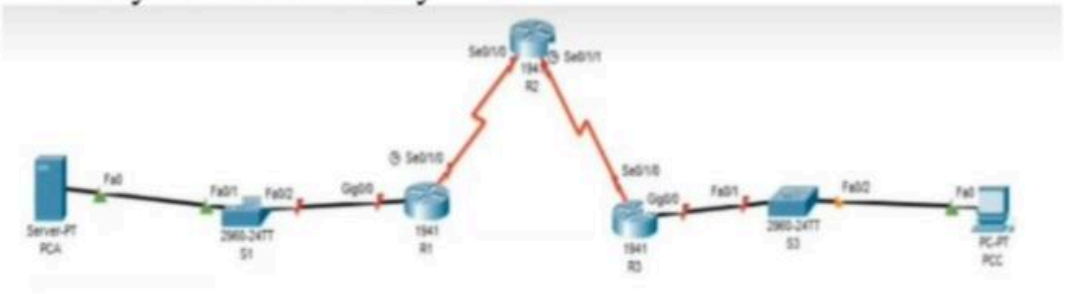
Step 6: Check results.
Your completion percentage should be 100%. Click Check Results to see feedback and verification of which required components have been completed.

Practical 4 VS

Practical No. 4// Vishal

Create the following topology using static routing

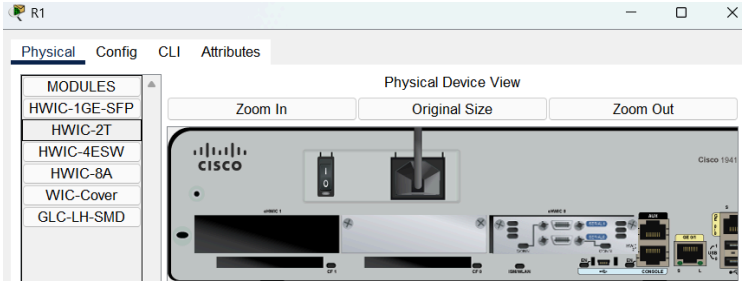
- Configure ACL to allow access to routers R1, R2, and R3 to only be permitted from PC-C, the management station. PC-C is also used for connectivity testing to PC-A, which is a server providing DNS, SMTP, FTP, and HTTPS services.
- Verify ACL functionality



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
	se0/1/0	10.1.1.1	255.255.255.252	N/A
R2	se0/1/0	10.1.1.2	255.255.255.252	N/A
	se0/1/1	10.2.2.2	255.255.255.252	N/A
	lo0	192.168.2.1	255.255.255.0	N/A
R3	gig0/0	192.168.3.1	255.255.255.0	N/A
	se0/1/0	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Create the following topology using statistic routing
Configure according to the table given
Topology
Next this in each router



Add Static Routing to each Router

CLI R1 :

R1(config)#ip route 10.2.2.0 255.255.255.252 10.1.1.2
R1(config)#ip route 192.168.3.0 255.255.255.0 10.1.1.2

CLI R2 :

R2(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1
R2(config)#ip route 192.168.3.0 255.255.255.0 10.2.2.1

CLI R3 :

R3(config)#ip route 192.168.1.0 255.255.255.0 10.2.2.2
R3(config)#ip route 10.1.1.0 255.255.255.252 10.2.2.2

Verify by pinging or sending message

It would result in success.

Add the loopback ip in the R2 with this **:** ip address 192.168.2.1 255.255.255.0

Set ospf

R1 :

Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 10.1.1.0 0.255.255.255 area 0
Router(config-router)#

R2 :

Router(config)#router ospf 1
Router(config-router)#network 10.1.1.0 0.255.255.255 area 0
Router(config-router)#network 100.2.2.0 0.255.255.255 area 0
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0

R3 :

Router(config)#router ospf 1
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#network 100.2.2.0 0.255.255.255 area 0

Change the hostname of routers

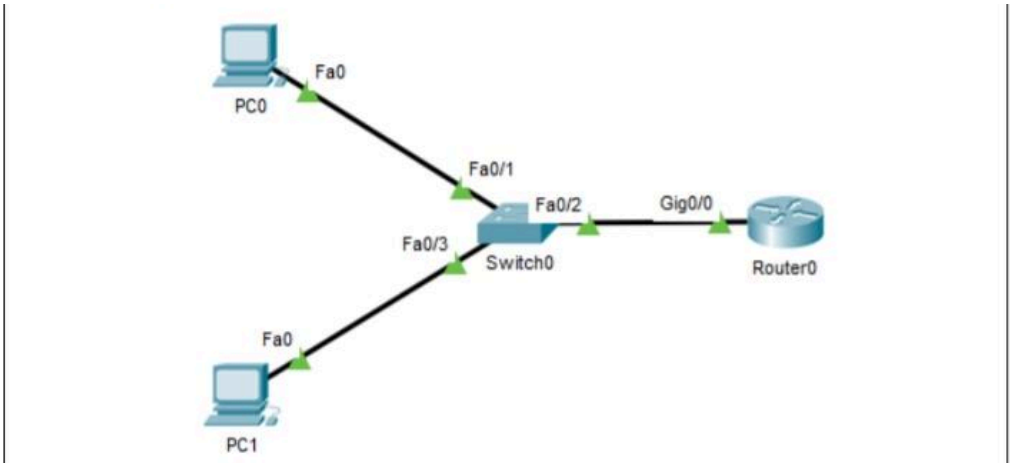
R2(config)#crypto key generate rsa
How many bits in the modulus [512]: 768 .....
R2(config)#username student privilege 15 secret stu
R2(config)#line vty 0 4
R2(config-line)#login local
R2(config-line)#transport input ssh

Now try to login ssh login from server to pc and viceversa

? AC

Practical No. // Ayush Chatterjee

Create the following topology and
▪ Configure OSPF MD5 authentication
▪ Configure a local user account on R1 and configure authenticate on the console and vty lines using local AAA.
▪ Verify local AAA authentication from the R1 console and the PC0 client and PC1 Client.



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
PC0	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC1	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router0	Gig0/0	192.168.1.1	255.255.255.0	-
PC0	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC1	NIC	192.168.1.3	255.255.255.0	192.168.1.1

▪ Configure OSPF MD5 authentication

Step1: Configure all the devices with the given addressing > Go to CLI mode in Router0 > Type these commands:

Router>enable

Router#configure terminal

Router(config)#router ospf 1

Router(config-router)#network 192.168.1.0 0.255.255.255 area 1

Router(config-router)#exit

Router(config)#interface GigabitEthernet0/1

Router(config-if)#ip ospf authentication message-digest

Router(config-if)#ip ospf message-digest-key 1 md5 smile

Router(config-if)#exit

Router(config)#exit

For Output:

Router#show ip ospf interface gigabitEthernet 0/1

Expect the following Output:

GigabitEthernet0/1 is up, line protocol is up Internet address is 192.168.2.1/24, Area 1 Process ID 1, Router ID 192.168.2.1, Network Type BROADCAST, Cost: 1 Transmit Delay is 1 sec, State BDR, Priority 1

Designated Router (ID) 192.168.3.1, Interface address 192.168.2.2

Backup Designated Router (ID) 192.168.2.1, Interface address 192.168.2.1 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:06

Index 2/2, flood queue length 0 Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 1, Adjacent neighbor count is 1 Adjacent with neighbor 192.168.3.1 (Designated Router) Suppress hello for 0 neighbor(s)

Message digest authentication enabled

Youngest key id is 1

Configure a local user account on R1 and configure authenticate on the console and vty lines using local AAA.

Step2: Just to CLI Mode of Router0 > Type these commands :

Router>enable

Router#configure terminal

Router0(config)# username admin privilege 15 secret cisco

Router0(config)# aaa new-model

Router0(config)# aaa authentication login default local

Router0(config)# line console 0

Router0(config-line)# login authentication default

Router0(config-line)# exit

Router0(config)# line vty 0 4

Router0(config-line)# login authentication default

Router0(config-line)# transport input telnet

Router0(config-line)# exit

Router(config)#exit

Router0# write memory

Your given task was accomplished

Verify local AAA authentication from the R1 console and the PC0 client and PC1 Client.

Step: Go to command prompt of any PC; say PC0 > Desktop Tab > Command Prompt > Type command : telnet 192.168.1.1

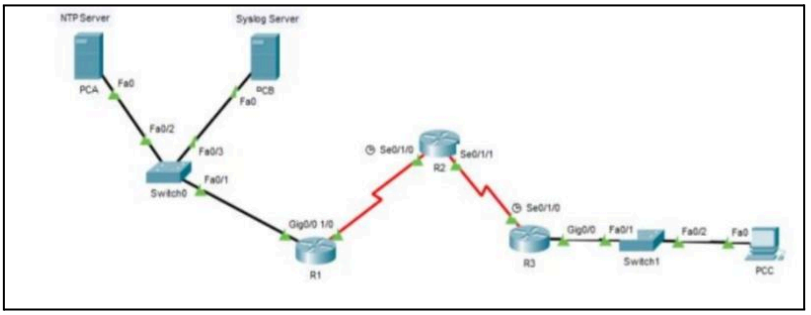
Username: admin

Password: cisco

Pract 1 B AG

Create the following topology with OSPF routing and

- Configure NTP
- Configure Routers to log messages to the syslog server.
- Configure R3 to support SSH connections



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
	se0/1/0	10.1.1.1	255.255.255.252	N/A
R2	se0/1/0	10.1.1.2	255.255.255.252	N/A
	se0/1/1	10.2.2.2	255.255.255.252	N/A
R3	gig0/0	192.168.3.1	255.255.255.0	N/A
	se0/1/0	10.2.2.1	255.255.255.252	N/A
PC–A	NIC	192.168.1.5	255.255.255.0	192.168.1.1
PC–B	NIC	192.168.1.6	255.255.255.0	192.168.1.1
PC–C	NIC	192.168.3.5	255.255.255.0	192.168.3.1

Step 1: Configure the topology according to given data
Step 2: Configure OSPF Routing
On all routers, enable OSPF and define networks.

R1

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface gig0/0
R1(config-if)#ex
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
R1(config-router)#exit
```

R2

```
Router(config-if)#ex
Router(config)#
Router(config)#router ospf 1
Router(config-router)#network 10.1.1.0 0.0.0.3 area 0
Router(config-router)#
00:11:00: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/1/0 from LOADING to FULL,
Loading Done
Router(config-router)#network 10.2.2.0 0.0.0.3 area 0
Router(config-router)#exit
```

R3

```
Router(config)#router ospf 1
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#network 10.2.2.0 0.0.0.3 area 0
Router(config-router)#exit
Router(config)#
```

Step 3: Configure NTP (Network Time Protocol)
Assuming the NTP Server is at 192.168.1.100, apply this to all routers.

```
ntp server 192.168.1.100
```

Step 4: Configure Syslog Logging
Assuming the Syslog Server is at 192.168.1.200, apply this to all routers.

```
logging 192.168.1.200
logging trap informational
```

Step 5: Configure SSH on R3
To secure remote access, enable SSH on R3.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#ip domain-name example.com
R3(config)#crypto key generate rsa
The name for the keys will be: R3.example.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R3(config)#username admin privilege 15 password cisco123
*Mar 1 0:17:10.344: %SSH-5-ENABLED: SSH 1.99 has been enabled
R3(config)#line vty 0 4
R3(config-line)#transport input ssh
R3(config-line)#login local
R3(config-line)#exit
R3(config)#enable secret cisco123
```

Step 7: Testing & Verification
Check OSPF Neighbors

```
show ip ospf neighbor
```

Verify Routing Table

```
show ip route
```

Check NTP Synchronization

```
show ntp status
```

Check Syslog Messages

```
show logging
```

Test SSH Connection to R3
From PC-A or another device, attempt SSH login:

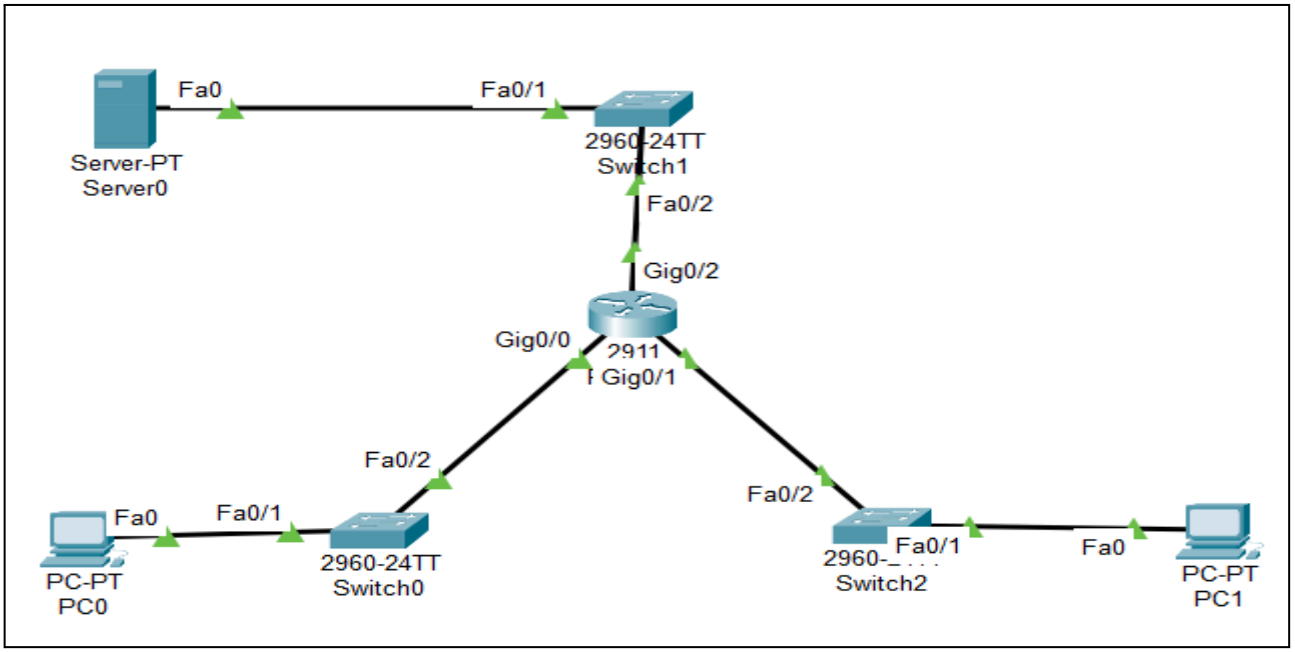
```
ssh -l admin 192.168.3.1
Password: cisco123
```

Practical 3 S1 RJ

Practical No. 3 Rahul Jadhav

Aim : Create the following topology and

- **Configure an ACL that will permit FTP and HTTP access on R1.**
- **Verify the ACL implementation. PC1 (Only FTP). PC2(Only HTTP)**



Devices	Interface	IP Address	Subnet Mask	Default Gateway
Router0	GigabitEthernet0/0	172.22.34.65	255.255.255.224	-
	GigabitEthernet0/1	172.22.34.97	255.255.255.240	-
	GigabitEthernet0/2	172.22.34.1	255.255.255.192	-
Server0	-	172.22.34.62	255.255.255.192	172.22.34.1
PC0	-	172.22.34.66	255.255.255.224	172.22.34.65
PC1	-	172.22.34.98	255.255.255.240	172.22.34.97

Objectives

A] Configure, Apply and Verify an Extended Numbered ACL

B] Configure, Apply and Verify an Extended Named ACL

A] CLI R0:

Router>en
Router#configure terminal
Router(config)#access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62

Step 1: Configure an ACL to permit FTP and ICMP.

CLI R0:

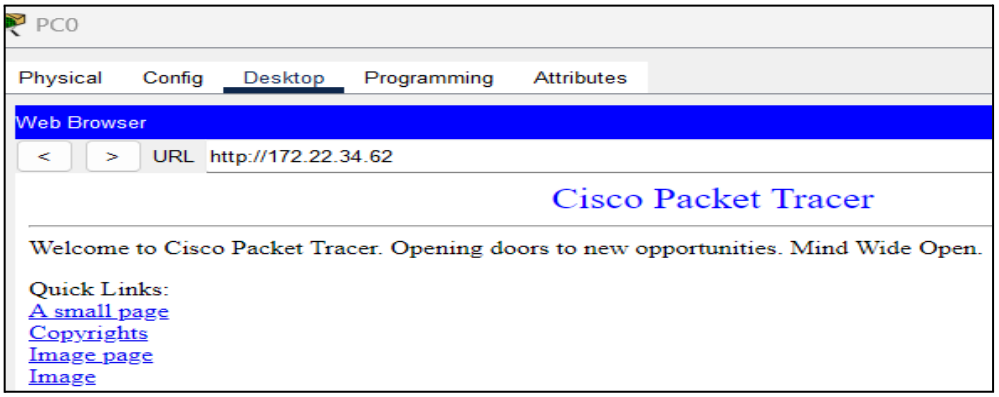
Router(config)#**access-list ?**
Router(config)#access-list **100 ?**
Router(config)#access-list 100 **permit ?**
Router(config)#access-list 100 permit **tcp ?**
Router(config)#access-list 100 permit tcp **172.22.34.64 ?**

[subnet mask. Don't type this only for calculation
11111111.11111111.11111111.11100000 = 255.255.255.224
00000000.00000000.00000000.00011111 = 0.0.0.31]

Router(config)#access-list 100 permit tcp 172.22.34.64 **0.0.0.31 ?**
Router(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 **host 172.22.34.62 ?**
Router(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 **eq ?**
Router(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq **ftp**
Router(config)#**access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62**
Router(config)#**interface g0/0**
Router(config-if)#**ip access-group 100 in**

Step 2: Verify the ACL implementation.

a.Ping from PC0 to Server
Go to PC0->Command Prompt->ping 172.22.34.62
b.FTP from PC0 to Server
> ftp 172.22.34.62
Username:cisco
Password:cisco
ftp> quit
c. Ping from PC0 to PC1
Go to PCO->Web Browser->http://172.22.34.62


PC0
Physical
Config
Desktop
Programming
Attributes
Web Browser
<
>
URL
http://172.22.34.62
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image

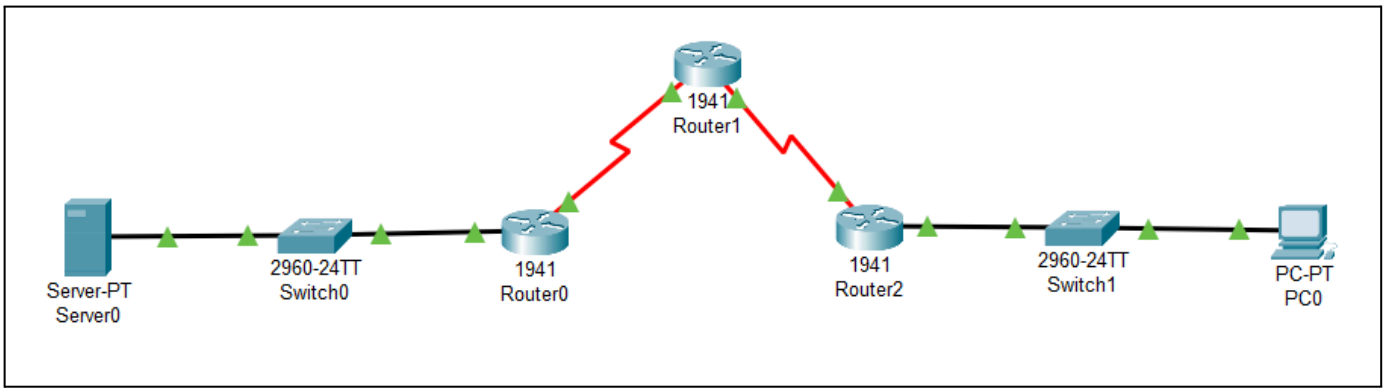
zone-based policy

Practical No. 6 done

Aim : Create the following topology using static routing and configure

- **A zone-based policy (ZPF) firewall on R1**
- **Verify ZPF firewall functionality using ping, SSH and a web browser.**

We use the following Topology for the present case



Addressing table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
	se0/1/0	10.1.1.1	255.255.255.252	N/A
R2	se0/1/0	10.1.1.2	255.255.255.252	N/A
	se0/1/1	10.2.2.2	255.255.255.252	N/A
R3	gig0/0	192.168.3.1	255.255.255.0	N/A
	se0/1/0	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Configuring SSH on all Router :

R1(config)#ip domain-name webpage.com
R1(config)#crypto key generate rsa
⋮
he modulus [512]: 1024
⋮
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#username admin privilege 15 password adminpa55

Add Static Routing to each Router
CLI R1 :
R1(config)#ip route 10.2.2.0 255.255.255.252 10.1.1.2
R1(config)#ip route 192.168.3.0 255.255.255.0 10.1.1.2

CLI R2 :
R2(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1
R2(config)#ip route 192.168.3.0 255.255.255.0 10.2.2.1

CLI R3 :
R3(config)#ip route 192.168.1.0 255.255.255.0 10.2.2.2
R3(config)#ip route 10.1.1.0 255.255.255.252 10.2.2.2

Ping PC-C from PC-A command prompt
Enter following commands PC-A command prompt :
ping 192.168.3.3

ssh -l admin 10.2.2.2
password : adminpa55

Go to PC-A web browser and enter :
192.168.1.3

Create the firewall zones on R3
We first check the weather security package enabled or not on R3
Type the following command in CLI mode on R3

Router#**show version**

As will get a message informing whether the security package is enable or not

R3(config)#license boot module c1900 technology-package securityk9
:
ACCEPT? [yes/no]: yes
:
R3(config)#exit
R3#copy run start
R3#reload

R3>en
R3#show version
:

R3#config t
R3(config)#zone security IN-ZONE

```
R3(config-sec-zone)#exit
R3(config)#zone security OUT-ZONE
R3(config-sec-zone)#exit
R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)#match access-group 101
R3(config-cmap)#exit
R3(config)#
R3(config)#policy-map type inspect IN-2-OUT-PMAP
R3(config-pmap)#class type inspect IN-NET-CLASS-MAP
R3(config-pmap-c)#inspect
R3(config-pmap-c)#exit
R3(config-pmap)#exit
R3(config)#zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
R3(config-sec-zone-pair)#service-policy type inspect IN-2-OUT-PMAP
R3(config-sec-zone-pair)#exit
R3(config)#int gig0/0
R3(config-if)#zone-member security IN-ZONE
R3(config-if)#exit
R3(config)#int se0/1/0
R3(config-if)#zone-member security OUT-ZONE
R3(config-if)#exit
R3(config)#exit
R3#
R3#copy run start
R3#reload
```

Goto PC-C Command prompt & enter following Commands

Ping 192.168.1.3

ssh -l admin 10.2.2.2
password: adminpa55
(Don't close screen)

CLI R3 :
R3#show policy-map type inspect zone-pair sessions
:
Number of Established Sessions = 1

Go to server0(PC-A) web browser and enter :
192.168.1.3
(Don't close screen)

CLI R3 :
R3#show policy-map type inspect zone-pair sessions
:
Number of Established Sessions = 1

Go to server0(PC-A) Command prompt and enter :
ssh -l admin 10.2.2.2
password: adminpa55
exit

ssh -l admin 10.2.2.2
password: adminpa55
(Don't close screen)

CLI R3 :
R3#show policy-map type inspect zone-pair sessions
:
Number of Established Sessions = 1

Go to server0(PC-A) Command prompt and enter :
ping 192.168.3.3
//ping will fail (request time out)

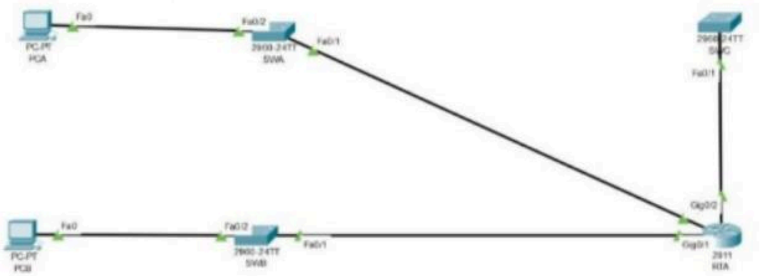
CLI R2 :
R2>ping 192.168.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R2>

permit one LAN s2

Practical No. 3

Aim : Create the following topology and

- Configure an ACL that will permit one LAN to remotely access device in another LAN using SSH Protocol
- Besides ICMP all traffic from other network is denied.
- Verify the ACL implementation.



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	gig0/0	10.101.117.49	255.255.255.248	N/A
	gig0/1	10.101.117.33	255.255.255.240	N/A
	gig0/2	10.101.117.1	255.255.255.224	N/A
PCA	NIC	10.101.117.51	255.255.255.248	10.101.117.49
PCB	NIC	10.101.117.35	255.255.255.240	10.101.117.33
SWA	VLAN 1	10.101.117.50	255.255.255.248	10.101.117.49
SWB	VLAN 1	10.101.117.34	255.255.255.240	10.101.117.33
SWC	VLAN 1	10.101.117.2	255.255.255.224	10.101.117.1

Step 1: Check the connection by sending message from PCA to PCB

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PCA	PCB	ICMP		0.000	N	0	(edit)	
	Successful	PCA	PCB	ICMP		0.000	N	1	(edit)	

Step 2: Configure Switches

-SWA —> (Click on SWA —> Go to CLI)

```
SWA>en
SWA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWA(config)#int vlan 1
SWA(config-if)#ip address 10.101.117.50 255.255.255.248
SWA(config-if)#no shutdown
SWA(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
SWA(config-if)#ip default-gateway 10.101.117.49
```

-SWB —> (Click on SWB —> Go to CLI)

```
SWB>en
SWB#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWB(config)#int vlan 1
SWB(config-if)#ip address 10.101.117.34 255.255.255.240
SWB(config-if)#no shutdown
SWB(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
SWB(config-if)#ip default-gateway 10.101.117.33
SWB(config)#
```

-SWC —> (Click on SWC —> Go to CLI)

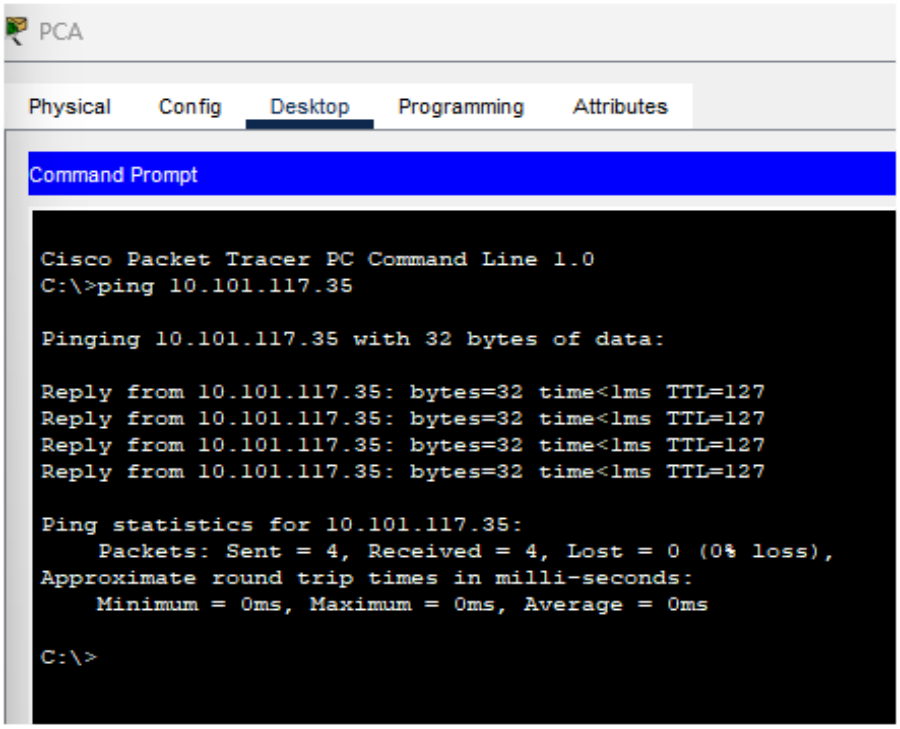
```
SWC>en
SWC#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWC(config)#int vlan 1
SWC(config-if)#ip address 10.101.117.2 255.255.255.224
SWC(config-if)#no shutdown
SWC(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
SWC(config-if)#ip default-gateway 10.101.117.1
SWC(config)#
```

Step 3 : Enable secret password: ciscoenpa55 ,Console password: ciscoconpa55 in all switches.Type these commands in CLI mode of all switches

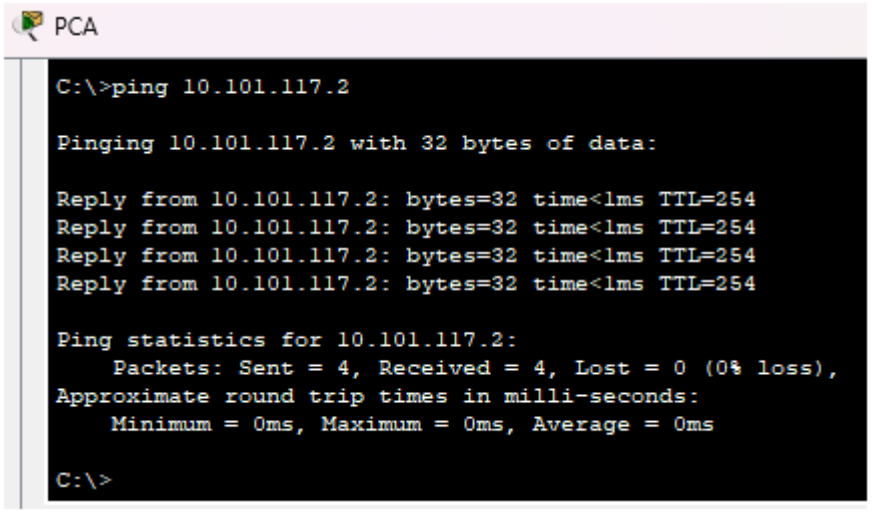
```
SWA>en
SWA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWA(config)#enable secret ciscoenpa55
SWA(config)#line console 0
SWA(config-line)#password ciscoconpa55
SWA(config-line)#login
SWA(config-line)#
```

Step 4:

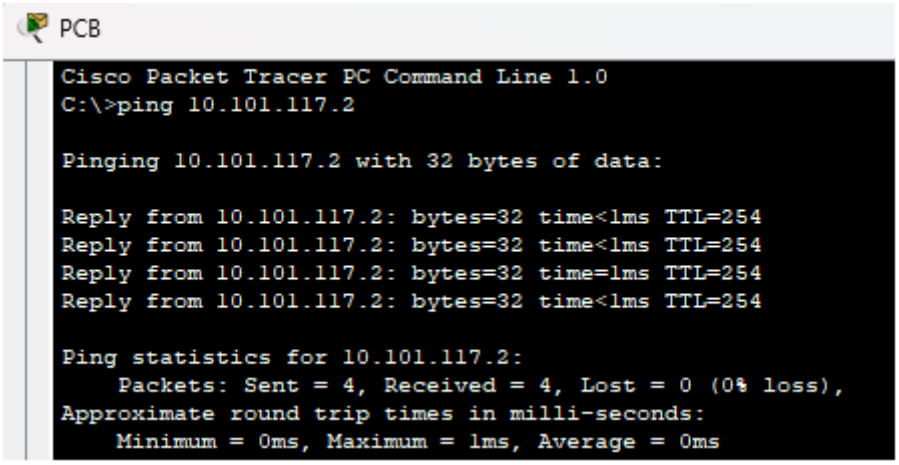
Ping PCB from PCA



Ping SWC from PCA



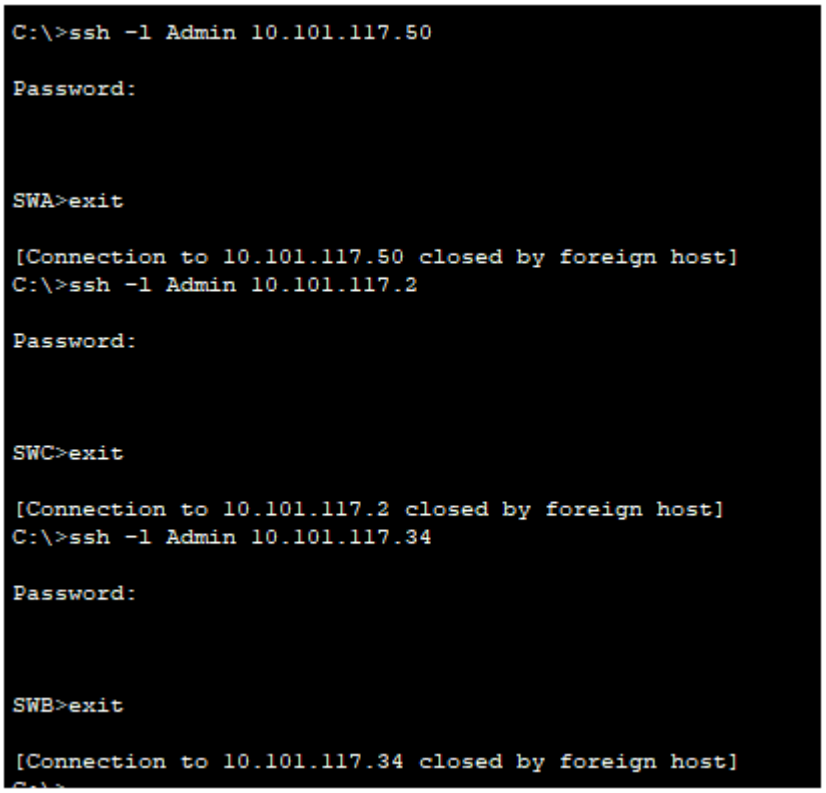
Ping SWC from PCB



Step 5: Generate Security Key .Type these commands in CLI mode of all switches (Note: secret password: ciscoenpa55 , Console password: ciscoconpa55)

User Access Verification
Password:
SWA>en
Password:
SWA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWA(config)#ip domain-name ccnasecurity.com
SWA(config)#username Admin secret Adminpa55
SWA(config)#line vty 0 4
SWA(config-line)#login local
SWA(config-line)#crypto key generate rsa
The name for the keys will be: SWA.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
SWA(config)#

Step 6: From the command prompt, establish an SSH session from PCA using password Admin[a55 . When finished, exit the SSH session.



Step 7 : Type following commands in CLI Mode of router

RTA>en
RTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RTA(config)#access-list 199 permit tcp 10.101.117.32 0.0.0.16 10.101.117.0 0.0.0.31 eq 22
RTA(config)#access-list 199 permit icmp any any
RTA(config)#int gigabitEthernet 0/2
RTA(config-if)#ip access-group 199 out

Step 8 : Check connectivity from PCA to SWB, SWC

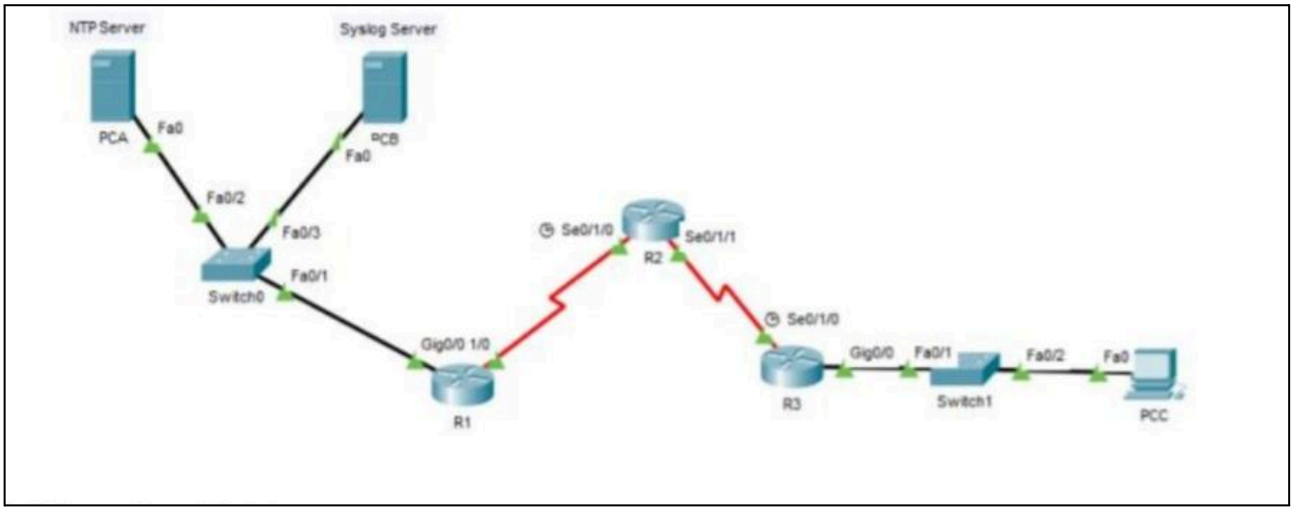
Connectivity from PCA to SWA and SWB is successful, but access to SWC fails because only SSH (port 22) traffic is permitted by the configured access list. Other services or ports are blocked as per the ACL rules.

OSPF_MD5_Syslog Done

Practical No. 1

Create the following topology and

- Configure OSPF MD5 authentication.
- Configure NTP and configure routers to log messages to the Syslog Server



Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
Router0	G0/1	192.168.1.1	255.255.255.0	–	S0 F0/5
	S0/0/0	10.1.1.1	255.255.255.252	–	–
Router1	S0/0/0	10.1.1.2	255.255.255.252	–	–
	S0/0/1	10.2.2.2	255.255.255.252	–	–
Router2	G0/1	192.168.3.1	255.255.255.0	–	S2 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	–	–
Server0	–	192.168.1.5	255.255.255.0	192.168.1.1	S0 F0/6
Server1	–	192.168.1.6	255.255.255.0	192.168.1.1	S1 F0/18
PC0	–	192.168.3.5	255.255.255.0	192.168.3.1	S2 F0/18

Devices	Network	
Router0	192.168.1.0	10.0.0.0
Router1	10.0.0.0	

Router2	192.168.3.0	10.0.0.0

Create the following topology and

- Configure OSPF topology MD5 authentication
- Configure NTP and configure routers to log messages to the Syslog Server

Step 1 : Apply OSPF to all the routers
(For router 1)

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 30.0.0.0 0.255.255.255 area 0
R1(config-router)#exit
R1(config)exit
R1#show ip ospf
R1(config)#exit
R1(config)#exit
```

(For router 2)

```
R2(config)#router ospf 2
R2(config-router)#ex
R2(config)#router ospf 1
R2(config-router)#network 10.1.1.0 0.255.255.255 area 0
R2(config-router)#network 100.2.2.0  0.255.255.255 area 0
R2(config-router)#exit
```

(For router 3)

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0
R3(config-router)#network 100.2.2.0 0.255.255.255 area 0
R3(config-router)#exit
```

Configure OSPF MD5 Authentication

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#area 0 authentication message-digest

R2(config)#router ospf 1
R2(config-router)#area 0 authentication message-digest
R2(config-router)#
```

```
R3(config)#router ospf 1
R3(config-router)#area 0 authentication message-digest
```

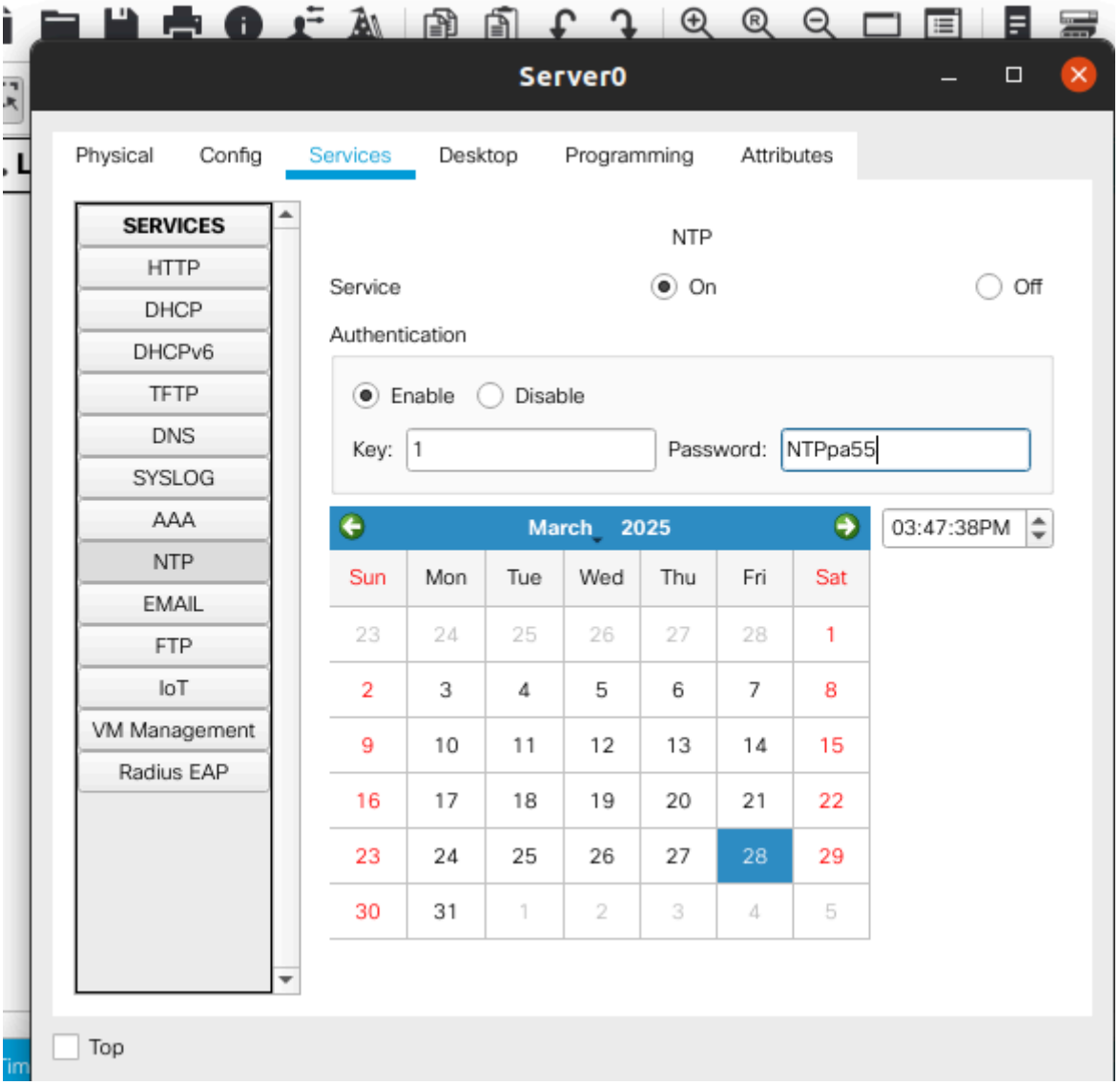
MD5 Key for all the routers

```
R1(config)#router ospf 1
R1(config-router)#area 0 authentication message-digest
R1(config-router)#int s0/0/0
R1(config-if)#ip ospf message-digest-key 1 md5 MD5pa55

R2(config-router)#int s0/0/0
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R2(config-if)#int s0/0/1
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55

R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#area 0 authentication message-digest
R3(config-router)#int s0/0/1
R3(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
```

```
R2#show ip ospf interface
Serial0/0/0 is up, line protocol is up
 Internet address is 10.1.1.2/30, Area 0
 Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT, Cost: 64
 Transmit Delay is 1 sec, State POINT-TO-POINT,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:04
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Suppress hello for 0 neighbor(s)
 Message digest authentication enabled
   Youngest key id is 1
Serial0/0/1 is up, line protocol is up
 Internet address is 10.2.2.2/30, Area 0
 Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT, Cost: 64
```

Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:04
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
  Youngest key id is 1
R2#

Configure NTP



R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ntp server 192.168.1.5
R1(config)#

R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp server 192.168.1.5

R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ntp server 192.168.1.5
R3(config)#

Syslog

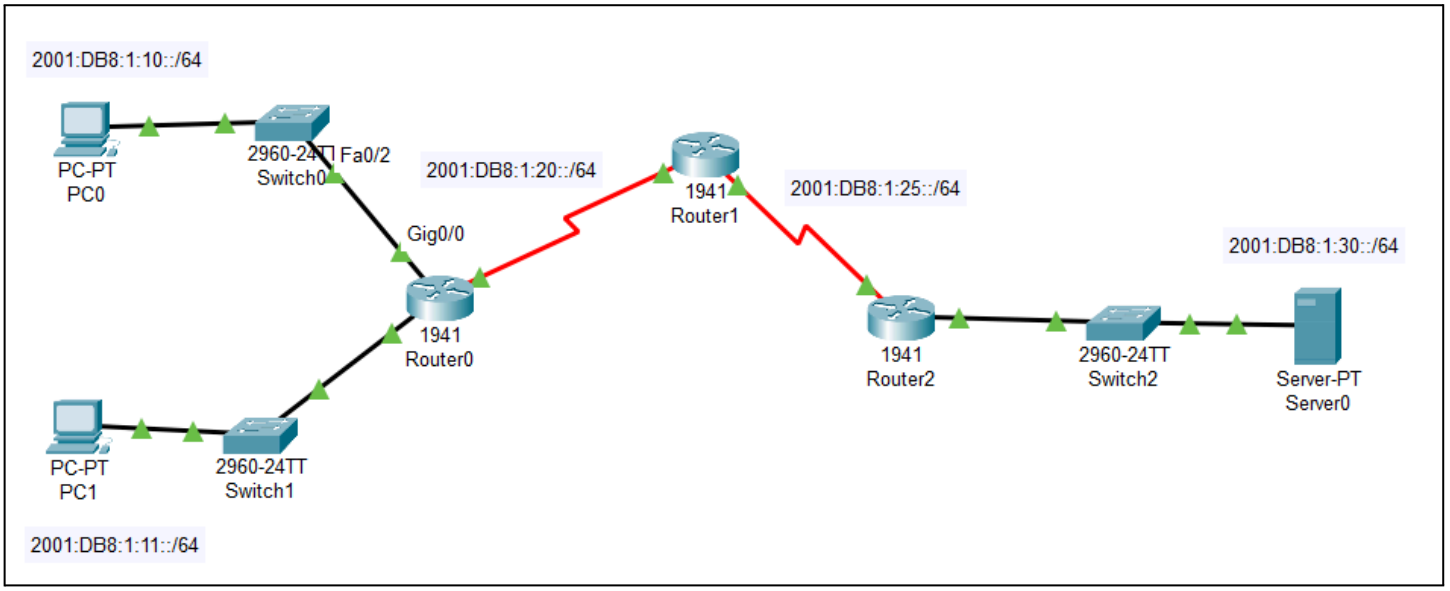
R1(config)#logging host 192.168.1.6
R2(config)#logging host 192.168.1.6
R3(config)#logging host 192.168.1.6

R1#show logging
R2#show logging
R3#show logging

ACL_block_http Done

Practical

Create the following topology using static routing and
Part 1 : Configure, apply and verify an ACL that will block HTTP access on R1
Part 2 : Configure, apply and verify an ACL that will block ICMP access on R3



Part 1 :

Router0 CLI

Router>en
Router#configure terminal
Router(config)#hostname R0
R0(config)#ipv6 unicast-routing

R0(config)#int g0/0
R0(config-if)#ipv6 enable
R0(config-if)#ipv6 address 2001:DB8:1:10::1/64
R0(config-if)#no shut
R0(config-if)#exit

R0(config)#int g0/1
R0(config-if)#ipv6 enable
R0(config-if)#ipv6 address 2001:DB8:1:11::1/64
R0(config-if)#no shut
R0(config-if)#exit

Router2 CLI
Router>en
Router#configure terminal

```
Router(config)#hostname R2
R2(config)#ipv6 unicast-routing
R2(config)#int g0/0
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 address 2001:DB8:1:30::1/64
R2(config-if)#no shut
R2(config-if)#exit
```

Device	IPv6 Address	Default Gateway
PC0	2001:DB8:1:10::2 / 64	2001:DB8:1:10::1
PC1	2001:DB8:1:11::2 / 64	2001:DB8:1:11::1
Server0	2001:DB8:1:30::2 / 64	

Router0 CLI

```
R0>en
R0#configure terminal

R0(config)#int se0/1/0
R0(config-if)#ipv6 enable
R0(config-if)#ipv6 address 2001:DB8:1:20::1/64
R0(config-if)#no shut
R0(config-if)#exit
```

Router1 CLI

```
Router>en
Router#configure terminal
Router(config)#hostname R1
R1(config)#ipv6 unicast-routing

R1(config)#int se0/1/0
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:DB8:1:20::2/64
R1(config-if)#no shut
R1(config-if)#exit

R1(config)#int se0/1/1
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:DB8:1:25::1/64
R1(config-if)#no shut
R1(config-if)#exit
```

Router2 CLI

```
R2(config)#int se0/1/1
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 address 2001:DB8:1:25::2/64
R2(config-if)#no shut
R2(config-if)#exit
```

Static Routing through CLI

Router0 CLI

```
R0(config)#ipv6 route 2001:DB8:1:25::/64 2001:DB8:1:20::2
R0(config)#ipv6 route 2001:DB8:1:30::/64 2001:DB8:1:20::2
```

Router1 CLI

```
R1(config)#ipv6 route 2001:DB8:1:10::/64 2001:DB8:1:20::1
R1(config)#ipv6 route 2001:DB8:1:11::/64 2001:DB8:1:20::1
R1(config)#ipv6 route 2001:DB8:1:30::/64 2001:DB8:1:25::2
```

Router2 CLI

```
R2(config)#ipv6 route 2001:DB8:1:20::/64 2001:DB8:1:25::1
R2(config)#ipv6 route 2001:DB8:1:10::/64 2001:DB8:1:25::1
R2(config)#ipv6 route 2001:DB8:1:11::/64 2001:DB8:1:25::1
```

Now type **2001:DB8:1:30::30** in Both PC0 and PC1 **Web Browser**. You can see both PC's can access the webpage.

Part 1: Configure, Apply, and Verify an IPv6 ACL

Router0 CLI

```
R0(config)#ipv6 access-list BLOCK_HTTP
R0(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R0(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R0(config-ipv6-acl)#permit ipv6 any any
R0(config-ipv6-acl)#exit
R0(config)#int g0/1
R0(config-if)#ipv6 traffic-filter BLOCK_HTTP in
```

Now type **2001:DB8:1:30::30** in PC1 **Web Browser** you will get **Request Timeout.**

Part 2: Configure, Apply, and Verify a Second IPv6 ACL

Router2 CLI

```
R2(config)#ipv6 access-list BLOCK_ICMP
R2(config-ipv6-acl)#deny icmp any any
R2(config-ipv6-acl)#permit ipv6 any any
```

```
R2(config-ipv6-acl)#exit
R2(config)#int g0/0
R2(config-if)#ipv6 traffic-filter BLOCK_ICMP out
```

Now try to ping any PC to Server0 using following command **ping 2001:DB8:1:30::30** you will get **100% loss**

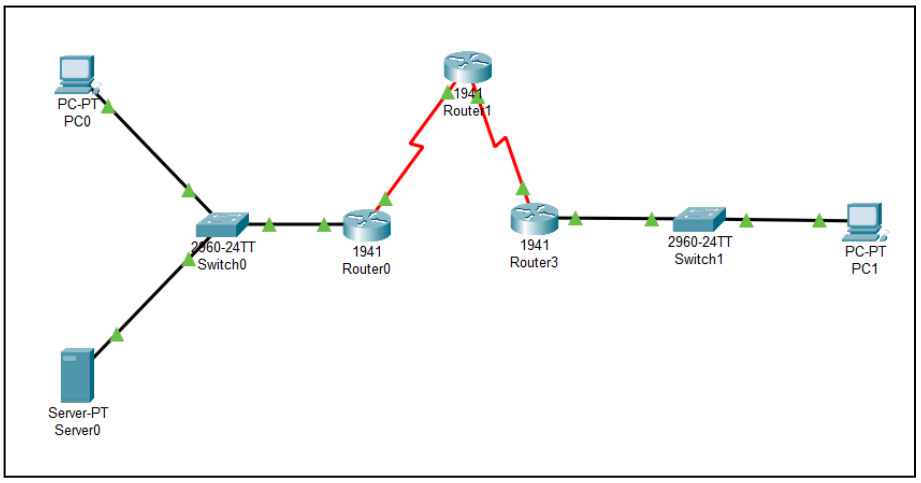
IOS _IPS Done

Practical

Aim : Create the following topology and

- Enable IOS IPS
- Configure logging and verify IPS
- Modify signature and verify again

We use the following Topology for the present case



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
	se0/1/0	10.1.1.1	255.255.255.252	N/A
R2	se0/1/0	10.1.1.2	255.255.255.252	N/A
	se0/1/1	10.2.2.2	255.255.255.252	N/A
R3	gig0/0	192.168.3.1	255.255.255.0	N/A
	se0/1/0	10.2.2.1	255.255.255.252	N/A
Syslog	NIC	192.168.1.50	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.2	255.255.255.0	192.168.3.1

Configuring RIP on each Router

Devices	Network	
Router0	10.0.0.0	192.168.1.0
Router1	10.0.0.0	
Router2	10.0.0.0	192.168.3.0

A]
Router 1 (R1) CLI:

Step 1: Enable the Security Technology package.
Router#show version
Router#conf t
Router(config)#license boot module c1900 technology-package securityk9
Router(config)#do write
Router(config)#exit
Router#reload
Router#show version

Step 2: Verify network connectivity.
*Now Ping Message from PC A to PC-C and vice versa. It should be successful

Step 3: Create an IOS IPS configuration directory in flash. On R1,
Router#mkdir ipsdir
Create directory filename [ipsdir]? //press enter here
Created dir flash:ipsdir

Step 4: Configure the IPS signature storage location. On R1,
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip ips config location flash:ipsdir
Step 5: Create an IPS rule.
Router(config)#ip ips name iosips
Step 6: Enable logging.
Router(config)#ip ips notify log

If necessary, use the clock set command from privileged EXEC mode to reset the clock. R1# clock set 10:20:00 10 january 2014
c. Verify that the timestamp service for logging is enabled on the router using the show run command.
Enable the timestamp service if it is not enabled.

Router(config)# service timestamps log datetime msec

d. Send log messages to the syslog server at IP address 192.168.1.50.

Router(config)#logging host 192.168.1.50

Step 7: Configure IOS IPS to use the signature categories.

Router(config)#ip ips signature-category
Router(config-ips-category)#category all
Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit
Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#exit
Router(config-ips-category)#exit
Do you want to accept these changes? [confirm]

Step 8: Apply the IPS rule to an interface.

Router(config)#interface g0/1
Router(config-if)#ip ips iosips out

B] Modify the Signature

Step 1: Change the event-action of a signature.

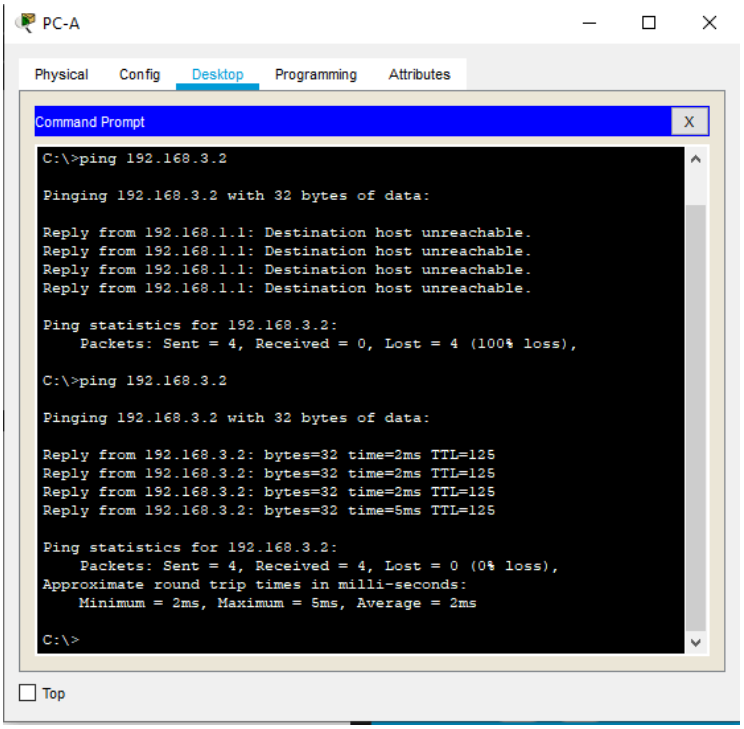
Router(config)#
Router(config)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#exit
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#exit
Router(config-sigdef)#exit

Step 2: Use show commands to verify IPS.

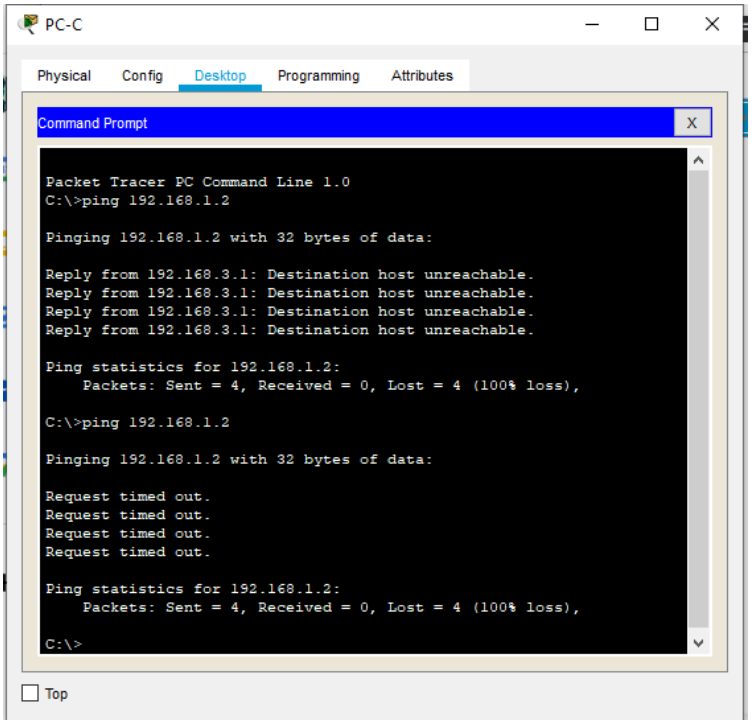
Router#show ip ips all

Step 3: Verify that IPS is working properly.

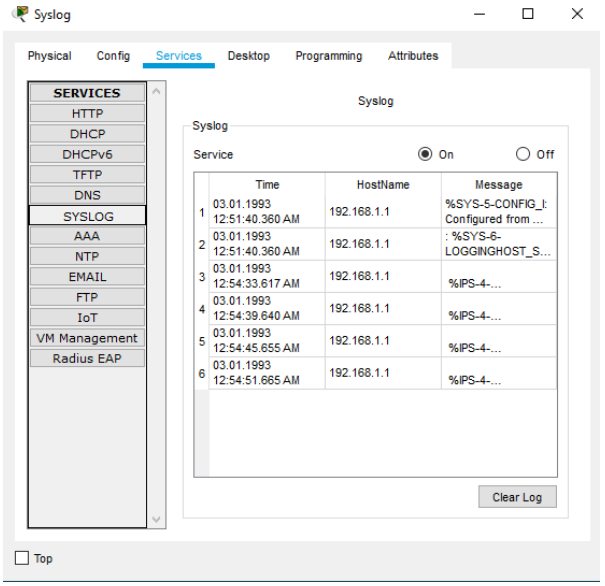
Ping from PC A to PC C will work



From PC C to PCA won't work :



Step 4: see the syslog from the services tab in server

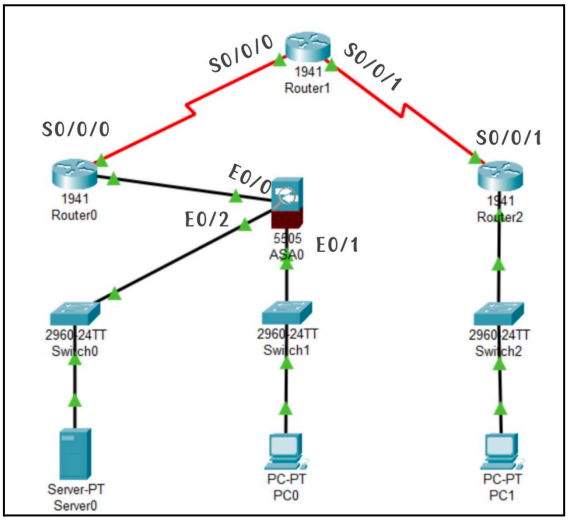

Syslog
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
Syslog
Syslog
Service
On
Off
Time
HostName
Message
1 03.01.1993 12:51:40.360 AM 192.168.1.1 %SYS-5-CONFIG_I: Configured from ...
2 03.01.1993 12:51:40.360 AM 192.168.1.1 : %SYS-6-LOGGINGHOST_S...
3 03.01.1993 12:54:33.617 AM 192.168.1.1 %IPS-4-...
4 03.01.1993 12:54:39.640 AM 192.168.1.1 %IPS-4-...
5 03.01.1993 12:54:45.655 AM 192.168.1.1 %IPS-4-...
6 03.01.1993 12:54:51.665 AM 192.168.1.1 %IPS-4-...
Clear Log
Top

ASA_settings Done

Practical No. 9

Aim : reate the following topology and

- **Configure basic ASA settings and interface security levels using CLI**
- **Configure routing, address translation, and inspection policy using CLI.**
- **Test connectivity to the ASA.**



Step 1 : Configuring PC's

Device Name	IP Address	Subnet Mask	Default Gateway
PC0	192.168.1.3	255.255.255.0	192.168.1.1
PC1	172.16.3.3	255.255.255.0	172.16.3.1

Step 2 : Configuring Server

Device Name	IP Address	Subnet Mask	Default Gateway
Server0	192.168.2.3	255.255.255.0	192.168.2.1

Devices	Interface	IP Address	Subnet Mask
Router0	GigabitEthernet0/0	209.165.200.225	255.255.255.248
	Serial0/0/0	10.1.1.1	255.255.255.252
Router1	Serial0/0/0	10.1.1.2	255.255.255.252
	Serial0/0/1	10.2.2.2	255.255.255.252
Router2	GigabitEthernet0/1	172.16.3.1	255.255.255.0
	Serial0/0/1	10.2.2.1	255.255.255.252

Step3 : Now we check the connectivity by sending a message from PC1 to all routers

So far, the ICMP tests from **PC1** have only been **successful** for **Router2**, while they have **failed** for both **Router1** and **Router0**.

Step4 : Configuring OSPF on Routers

Router0 CLI:

```
Router>en
Router#configure terminal
Router(config)#router ospf 1
Router(config-router)#network 10.1.1.0 0.0.0.3 area 0
Router(config-router)#network 209.165.200.225 0.0.0.7 area 0
Router(config-router)#exit
```

Router1 CLI

```
Router>en
Router#configure terminal
Router(config)#router ospf 1
Router(config-router)#network 10.1.1.0 0.0.0.3 area 0
Router(config-router)#network 10.2.2.0 0.0.0.3 area 0
Router(config-router)#exit
```

Router2 CLI :

```
Router>en
Router#configure terminal
Router(config)#router ospf 1
Router(config-router)#network 10.2.2.0 0.0.0.3 area 0
Router(config-router)#network 172.16.3.0 0.0.0.255 area 0
Router(config-router)#exit
```

Step5 : Now we check the connectivity by sending a message from PC1 to all routers

Now ICMP tests from **PC1** have been **successful** for **all the Routers.**

A] Configure ASA Settings and Interface Security Using the CLI

Step 1 : Configure the hostname and domain name
Step 1.1 : Configure the ASA0 hostname as CCNAS-ASA
ciscoasa#conf t
ciscoasa(config)#

Congif → Hostnae → CCNAS-ASA

Step 1.2 : Configure the domain name as ccnasecurity.com
CCNAS-ASA(config)#domain-name ccnasecurity.com

Step 2 : Configure the enable mobile password
CCNAS-ASA(config)#enable password anpa55

Step 3: Set the date and time.
CCNAS-ASA(config)#clock set 10:23:00 20 mar 2025
CCNAS-ASA(config)#show clock
10:23:9.454 UTC Thu Mar 20 2025

Step 4: Configure the inside and outside interfaces.

Step 4.1 : Configure a logical VLAN 1 interface for the inside network (192.168.1.0/24) and set the security level to the highest setting of 100
CCNAS-ASA(config)#interface vlan 1
CCNAS-ASA(config-if)#nameif inside
CCNAS-ASA(config-if)#ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)#security-level 100
CCNAS-ASA(config-if)#exit

Step 4.2 : Configure a logical VLAN 2 interface for the outside network (209.165.200.224/29) and set the security level to the lowest setting of 0, and enable the VLAN 2 interface.
CCNAS-ASA(config)#interface vlan 2
CCNAS-ASA(config-if)#nameif outside
CCNAS-ASA(config-if)#ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)#security-level 0
CCNAS-ASA(config-if)#exit

Step 4.3 : Use the following verification commands to check your configurations:

```
CCNAS-ASA(config)#show ip address
System IP Addresses:
Interface              Name               IP address      Subnet mask     Method
Vlan1                  inside             192.168.1.1     255.255.255.0   manual
Vlan2                  outside            209.165.200.226 255.255.255.248 manual

Current IP Addresses:
Interface              Name               IP address      Subnet mask     Method
Vlan1                  inside             192.168.1.1     255.255.255.0   manual
Vlan2                  outside            209.165.200.226 255.255.255.248 manual

CCNAS-ASA(config)#show switch vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    inside                           up        Et0/1, Et0/2, Et0/3, Et0/4
                                                Et0/5, Et0/6, Et0/7
2    outside                          up        Et0/0
```

Step 5 : Test connectivity to the ASA0 by sending message from PC0 to ASA0

ICMP tests from **PC0** have been **successful** for **ASA0.**

B] Configure Routing, Address Translation, and Inspection Policy Using the CLI

Step 1: Configure a static default route for the ASA.

```
CCNAS-ASA(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.225
```

Step 2: Configure address translation using PAT and network objects.

```
CCNAS-ASA(config)#object network inside-net
CCNAS-ASA(config-network-object)#subnet 192.168.1.0 255.255.255.0
CCNAS-ASA(config-network-object)#nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)#end
```

Step 3: Modify the default MPF application inspection global service policy.

```
CCNAS-ASA#conf t
CCNAS-ASA(config)#class-map inspection_default
CCNAS-ASA(config-cmap)#match default-inspection-traffic
CCNAS-ASA(config-cmap)#exit
CCNAS-ASA(config)#policy-map global_policy
CCNAS-ASA(config-pmap)#class inspection_default
CCNAS-ASA(config-pmap-c)#inspect icmp
CCNAS-ASA(config-pmap-c)#exit
CCNAS-ASA(config)#service-policy global_policy global
```

C] Configure DHCP, AAA, and SSH

Step 1: Configure the ASA as a DHCP server.
CCNAS-ASA(config)#dhcpd address 192.168.1.5-192.168.1.36 inside
CCNAS-ASA(config)#dhcpd dns 209.165.201.2 interface inside
CCNAS-ASA(config)#dhcpd enable inside

Step 2: Configure AAA to use the local database for authentication.
CCNAS-ASA(config)#username admin password adminpa55
CCNAS-ASA(config)#aaa authentication ssh console LOCA

Step 3 : Configure remote access to the ASA
CCNAS-ASA(config)#crypto key generate rsa modulus 1024
Do you really want to replace them? [yes/no]: **no**
CCNAS-ASA(config)#ssh 192.168.1.0 255.255.255.0 inside
CCNAS-ASA(config)#ssh 172.16.3.3 255.255.255.255 outside
CCNAS-ASA(config)#ssh timeout 10

Step 4 : SSH Connection from PC1 to ASA Firewall

ssh -l admin 209.165.200.226
Password : adminpa55

Step 5 : SSH Connection from PC0 to ASA Firewall

ssh -l admin 192.168.1.1
Password : adminpa55

D] Configure a DMZ, Static NAT, and ACLs

Step 1: Configure the DMZ interface VLAN 3 on the ASA.
CCNAS-ASA(config)#interface vlan 3
CCNAS-ASA(config-if)#ip address 192.168.2.1 255.255.255.0
CCNAS-ASA(config-if)#no forward interface vlan 1
CCNAS-ASA(config-if)#nameif dmz
CCNAS-ASA(config-if)#security-level 70
CCNAS-ASA(config-if)#exit
CCNAS-ASA(config-if)# interface Ethernet0/2
CCNAS-ASA(config-if)# switchport access vlan 3
CCNAS-ASA(config-if)#exit

Step 2: Configure static NAT to the DMZ server using a network object.
CCNAS-ASA(config)# object network dmz-server

CCNAS-ASA(config-network-object)# host 192.168.2.3
CCNAS-ASA(config-network-object)# nat (dmz,outside) static 209.165.200.227
CCNAS-ASA(config-network-object)# exit

Step 3: Configure an ACL to allow access to the DMZ server from the Internet.
CCNAS-ASA#conf t
CCNAS-ASA(config)#access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
CCNAS-ASA(config)#access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
CCNAS-ASA(config)#access-group OUTSIDE-DMZ in interface outside