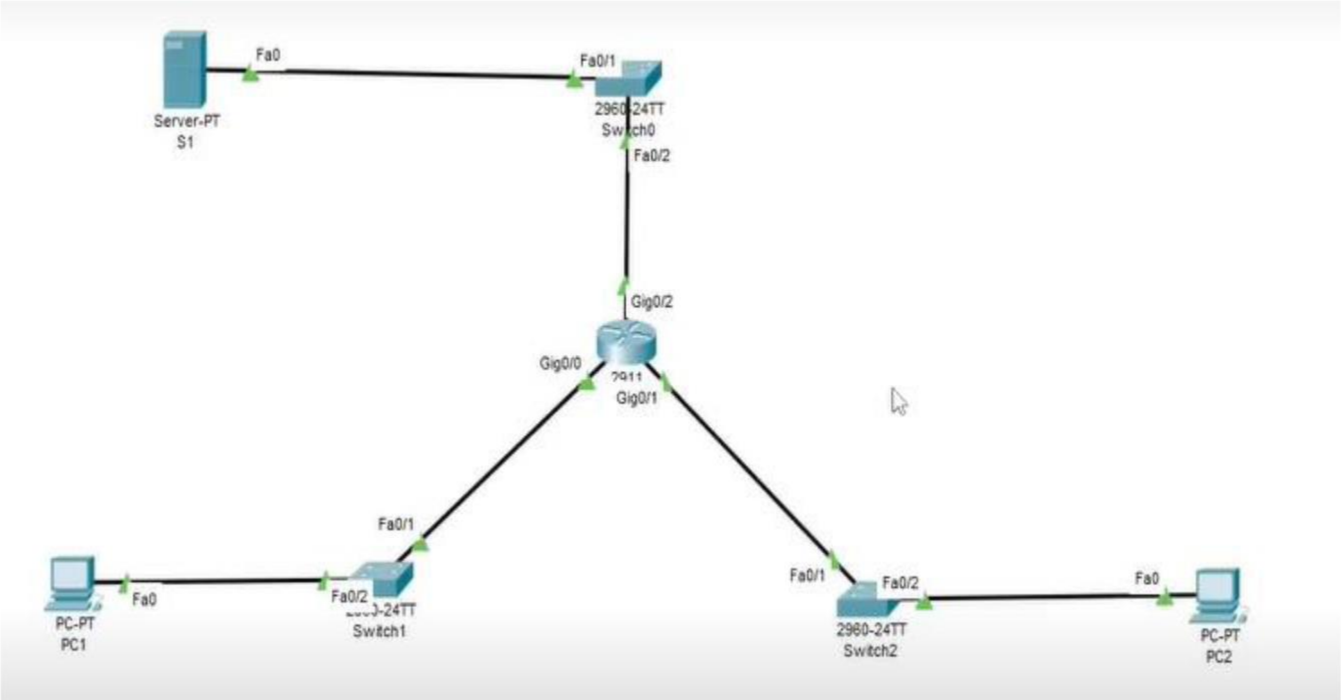
Security In Computing Practical

Practical 3: Configuring Extended ACLs

A]

Topology:



Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	172.22.34.65	255.255.255.224	N/A
	gig0/1	172.22.34.97	255.255.255.240	N/A
	gig0/2	172.22.34.1	255.255.255.192	N/A
Server	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

Objectives:

- **Configure, Apply and Verify an Extended Numbered ACL**
- **Configure, Apply and Verify an Extended Named ACL**

Scenario:

- PC1 Should be allowed only FTP access
- PC2 Should be allowed only web access
- Both PCs must ping server but not each other’s

Configure Router:

Step 1: Configure password for vty lines

```
R1(config) # line vty 0 4
R1(config-line) #password vtypa55
R1(config-line) #login
```

Step 2: Configure secret on router

```
R1(config) # enable secret enpa55
```

Part 1: Configure, Apply and Verify an Extended Numbered ACL

Step 1: Configure an ACL to permit FTP and ICMP. (Use Router 2911)

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
```

Step 2: Apply the ACL on the correct interface to filter traffic.

```
R1(config)# int gig 0/0
R1(config-if)# ip access-group 100 in
```

Step 3: Verify the ACL implementation.

a. Ping from PC1 to Server. PC1> ping 172.22.34.62 (Successful)

b. FTP from PC1 to Server. The username and password are both cisco.

```
PC1> ftp 172.22.34.62
```

c. Exit the FTP service of the Server.

```
ftp> quit
```

d. Ping from PC1 to PC2.

```
PC1> ping 172.22.34.98
```

(Unsuccessful) destination host unreachable

Part 2: Configure, Apply and Verify an Extended Named ACL

Step 1: Configure an ACL to permit HTTP access and ICMP.

```
R1(config)# ip access-list extended HTTP_ONLY
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62
eq www
R1(config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
```

Step 2: Apply the ACL on the correct interface to filter traffic.

```
R1(config)# int gig0/1
R1(config-if)# ip access-group HTTP_ONLY in
```

Step 3: Verify the ACL implementation.

a. Ping from PC2 to Server. PC2> ping 172.22.34.62 (Successful)

b. FTP from PC2 to Server

PC2> ftp 172.22.34.62

(Unsuccessful)

c. **Open the web browser on PC2.**

URL -> http://172.22.34.62

(Successful)

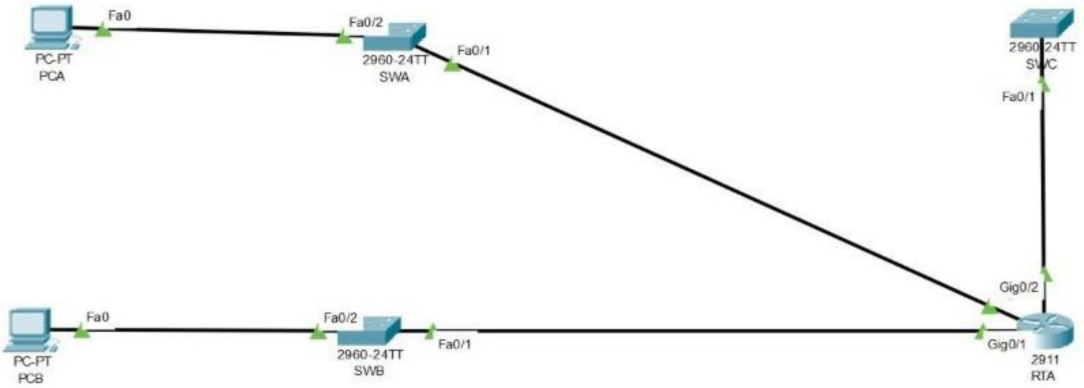
d. Ping from PC2 to PC1.

PC> ping 172.22.34.66

(Unsuccessful)

B]

Topology:



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

Objectives:

- **Configure, Apply and Verify an Extended Numbered ACL**

Scenario:

- Device on one LAN are allowed to remotely access device in another LAN using SSH protocol
- Besides ICMP all traffic from other network is denied

Configure Switch and Router:

Step 1: Configure the IP address on switch

```
SWA(config)# int vlan 1
SWA(config-if)# ip address 10.101.117.50 255.255.255.248
SWA(config-if)# no shut
SWA(config-if)# ip default-gateway 10.101.117.49

SWB(config)# int vlan 1
SWB(config-if)# ip address 10.101.117.34 255.255.255.240
SWB(config-if)# no shut
SWB(config-if)# ip default-gateway 10.101.117.33

SWC(config)# int vlan 1
SWC(config-if)# ip address 10.101.117.2 255.255.255.224
SWC(config-if)# no shut
SWC(config-if)# ip default-gateway 10.101.117.1
```

Step 2: Configure the secret on router and switch

```
RTA/SW(config)# enable secret enpa55
```

Step 3: Configure the console password on router and switch

```
RTA/SW(config)# line console 0
RTA/SW(config)# password tyit
RTA/SW(config)# login
```

Step 4: Test connectivity

Ping from PCA to PC-B.

```
PCA>ping 10.101.117.35
(Successful)
```

Ping from PCA to SWC.

```
PCA>ping 10.101.117.2
(Successful)
```

Ping from PCB to SWC.

```
PCB>ping 10.101.117.2
(Successful)
```

Part 1: Configure Switch and Router to support SSH Connection

Step 1: Configure domain name and crypto key for use with SSH. RTA/SW(config)# ip domain-name ccnasecurity.com

Step 2: Configure users to login to SSH

```
RTA/SW(config)# username admin secret adminpa55
```

Step 3: Configure incoming vty lines

```
RTA/SW(config)# line vty 0 4
RTA/SW(config-line)# login local
RTA/SW(config)# crypto key generate rsa
How many bits in the modulus [512]:
```

1024 **Step 4: Verify the SSH Connection**

```
PCA> ssh -l Admin 10.101.117.34
Password: adminpa55
```

```
SWB>
PCA> ssh -l Admin 10.101.117.2
Password: adminpa55
SWC>
PCB> ssh -l Admin 10.101.117.50
Password: adminpa55
SWA>
PCB> ssh -l Admin 10.101.117.2
Password: adminpa55
SWC>
SWC> ssh -l Admin 10.101.117.50
Password: adminpa55
SWA>
SWC> ssh -l Admin 10.101.117.34
Password: adminpa55
SWB>
SWB> exit
```

Part 2: Configure, Apply and Verify an Extended Numbered ACL

Step 1: Configure the extended ACL.

```
RTA(config)# access-list 199 permit tcp 10.101.117.32 0.0.0.15 10.101.117.0 0.0.0.31 eq 22
RTA(config)# access-list 199 permit icmp any any
```

Step 2: Apply the extended ACL.

```
RTA(config)# int gig0/2 RTA(config-
if)# ip access-group 199 out
```

Step 3: Verify the extended ACL implementation.

a. Ping from PCB to all of the other IP addresses in the network.

```
PCB> ping 10.101.117.51
(Successful)
PCB> ping 10.101.117.2
(Successful)
```

b. SSH from PCB to SWC.

```
PCB> ssh -l Admin 10.101.117.2
Password:adminpa55
SWC>
```

c. Exit the SSH session to SWC.

```
SWC>exit
```

d. Ping from PCA to all of the other IP addresses in the network.

```
PCA> ping 10.101.117.35
(Successful)
PCA> ping 10.101.117.2
(Successful)
```

e. SSH from PCA to SWC

```
PCA> ssh -l Admin 10.101.117.2
```

```
Connection timed out. Remote host not responding
```

f. SSH from PCA to SWB.

```
PCA> ssh -l Admin 10.101.117.34

Password: adminpa55

SWB>
```

g. After logging into SWB, do not log out. SSH to SWC in privileged EXEC mode.

```
SWB# ssh -l Admin 10.101.117.2

Password: adminpa55

SWC>
```