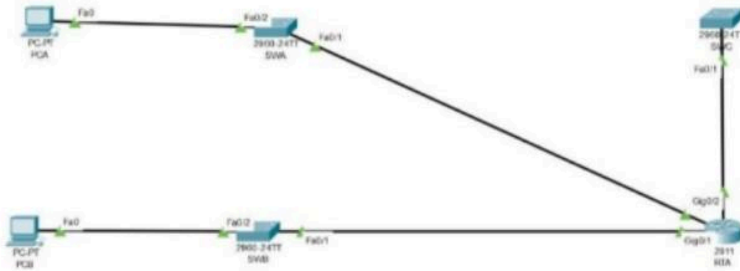


## Practical No. 3

**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

```
PCA
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.101.117.35

Pinging 10.101.117.35 with 32 bytes of data:

Reply from 10.101.117.35: bytes=32 time<1ms TTL=127
Reply from 10.101.117.35: bytes=32 time<1ms TTL=127
Reply from 10.101.117.35: bytes=32 time<1ms TTL=127
Reply from 10.101.117.35: bytes=32 time<1ms TTL=127

Ping statistics for 10.101.117.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

### Ping SWC from PCA

```
PCA

C:\>ping 10.101.117.2

Pinging 10.101.117.2 with 32 bytes of data:

Reply from 10.101.117.2: bytes=32 time<1ms TTL=254
Reply from 10.101.117.2: bytes=32 time<1ms TTL=254
Reply from 10.101.117.2: bytes=32 time<1ms TTL=254
Reply from 10.101.117.2: bytes=32 time<1ms TTL=254

Ping statistics for 10.101.117.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

### Ping SWC from PCB

```
PCB

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.101.117.2

Pinging 10.101.117.2 with 32 bytes of data:

Reply from 10.101.117.2: bytes=32 time<1ms TTL=254
Reply from 10.101.117.2: bytes=32 time<1ms TTL=254
Reply from 10.101.117.2: bytes=32 time<1ms TTL=254
Reply from 10.101.117.2: bytes=32 time<1ms TTL=254

Ping statistics for 10.101.117.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

**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.**

```
C:\>ssh -l Admin 10.101.117.50
Password:

SWA>exit

[Connection to 10.101.117.50 closed by foreign host]
C:\>ssh -l Admin 10.101.117.2
Password:

SWC>exit

[Connection to 10.101.117.2 closed by foreign host]
C:\>ssh -l Admin 10.101.117.34
Password:

SWB>exit

[Connection to 10.101.117.34 closed by foreign host]
```

**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.

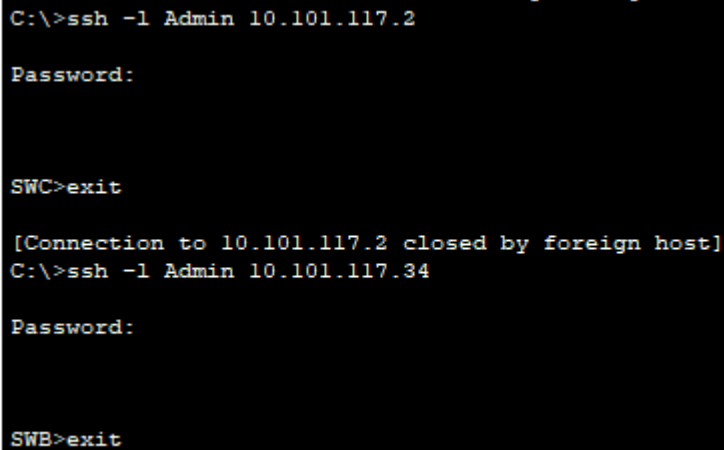
RTA(config)#access-list 199 permit tcp 10.101.117.32 0.0.0.16 10.101.117.0 0.0.0.31 eq 22

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**



```
C:\>ssh -l Admin 10.101.117.2

Password:

SWC>exit

[Connection to 10.101.117.2 closed by foreign host]
C:\>ssh -l Admin 10.101.117.34

Password:

SWB>exit
```

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.