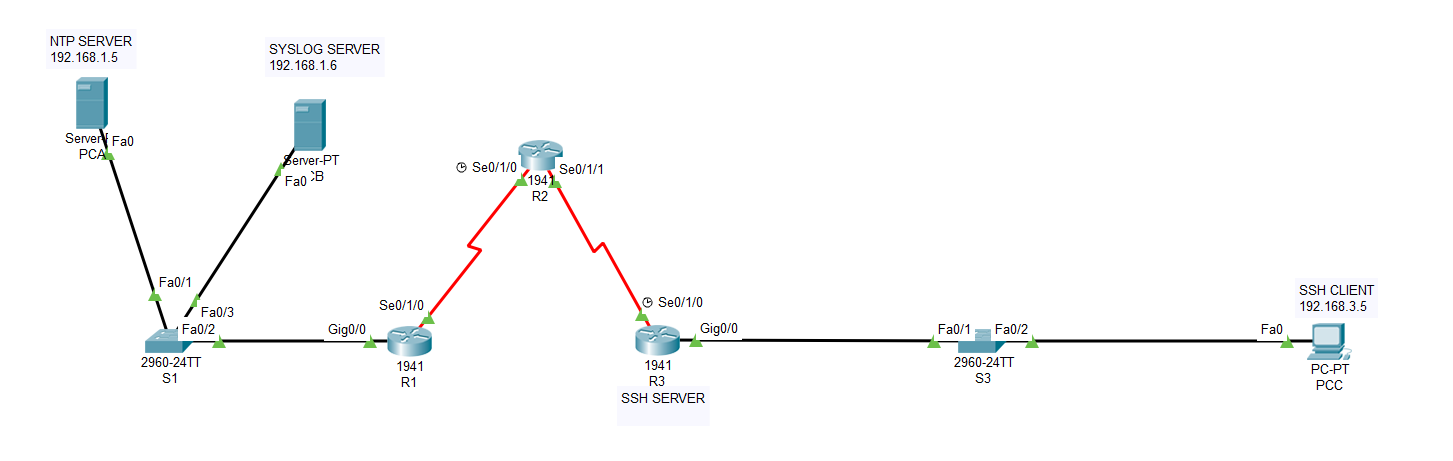
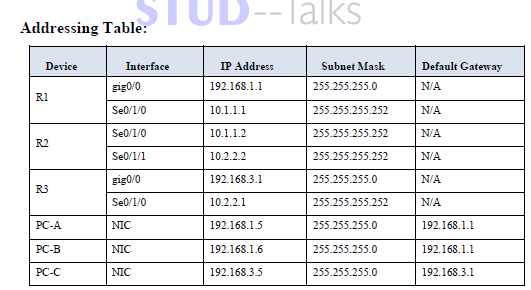
**Practical 1**

**Configure Routers For Syslog , NTP And SSH Operation**

**S2Q2 , S13Q13 S15Q18**

****

****

**Objectives:**

**. Configure OSPF MD5 authentication.**

**. Configure NTP.**

**. Configure routers to log messages to the syslog server.**

**. Configure R3 to support SSH connections.**

**Part 1 : Configure Router**

Step 1: Configure password for vty lines on all Routers

R(config) # line vty 0 4

R(config - line) #password vtypa55

R(config - line ) #login

Step 2 : Configure Secret on all Router

R(config)# enable secret enpa55

Step 3 : Configure ospf on routers

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

R2(config)# router ospf 1

R2(config-router) # network 10.1.1.0 0.0.0.3 area 0

R2(config-router) # network 10.2.2.0 0.0.0.3 area 0

R3(config)# router ospf 1

R3(config-router) # network 192.168.3.0 0.0.0.255 area 0

R3(config-router) # network 10.2.2.0 0.0.0.3 area 0

Step 4 : Test connectivity

PCA > ping 192.168.3.5 (pcc)

Sucessful

PCB > ping 192.168.3.5 (pcc)

Sucessful

**Part 2: Configure OSPF MD5 Authentication**

Step 1: Configure OSPF MD5 Authentication for all routers in area 0

Execute Command On all Routers

R(config) # router ospf 1

R(config-router)# area 0 authentication message-digest

Step 2: Configure the MD5 Key for all router in area 0 . configure an MD5 KEY on all the serial interfaces on R1 , R2 and R3 . use the password MD5pa55 for key 1.

R1(config)# int se0/1/0

R1(config-if)#ip ospf message-digest-key 1 md5 MD5pa55

R2(config)# int se0/1/0

R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55

R2(config)# int se0/1/1

R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55

R3(config)# int se0/1/0

R3(config-if)#ip ospf message-digest-key 1 md5 MD5pa55

Step 3: Verify Configurations

a. Verify the MD5 authentication configurations using the commands show ip ospf interface.

b. Verify end-to-end connectivity.

Output should be shown in all the routers :

R# show ip ospf interface

Message-digest Authentication Enabled

Youngest key ID is 1

**Part 3: Configure NTP**

Step 1: Enable Authentication On Pc-A

1. On PcA , click NTP under the services to verify NTPservice is enabled
2. To Configure NTP authentication , click Enable under Authentication use Key 1 and password NTPpa55 for authentication

Step 2 : Configure R1,R2,R3 as NTP clients

Execute Command On all Routers

R(config)# ntp server 192.168.1.5

Verify client configuration using the command show ntp status.

Step 3: Configure Routers to update hardware clock

Execute command on all routers

R(config)# ntp update-calendar

Verify that the hardware clock was updated

R#show clock

Step 4: Configure NTP authentication on the routers

Execute command on all routers

R(config)# ntp authenticate

R(config)# ntp trusted-key 1

R(config)# ntp authentication-key 1 md5 NTPpa55

Step 5: Configure Routers to timestamp log messages

Execute command on all routers

R(config)# service timestamp log datetime msec

**Part 4 : Configure Routers to log messages to the syslog server**

Step 1: Configure the routers to identify the remote host

(syslog-server) that will receive logging messages

Execute command on all routers

R(config)# logging host 192.168.1.6

Step 2: Verify Logging Configurations

Execute command on all routers

R# show logging

Step 3 : Examine logs of the syslog server

From the services tab of the syslog servers dialouge box, select the syslog services button observe the logging messages received from the routers .

Note: Log messages can be generated on the server by executing commands on the router. For example, entering and exiting global configuration mode will generate an informational configuration message. You may need to click a different service and then click Syslog again to refresh the message display.

**Part 5 : Configure R3 to support SSH connections**

Step 1 : Configure a domain-name

R3(config)# ip domain-name ccnasecurity.com

Step 2: Configure users for login to the ssh server R3

R3(config) # username SSHadmin privilege 15 secret sshpa55

Step 3: Configure the incoming vty lines on R3

R3(config)# line vty 0 4

R3(config-line)# login local

R3(config-line) # transport input ssh

Step 4: Erase existing key pairs on R3

R3(config)# crypto key zeroize rsa

Step 5: Generate the RSA encryption key pair for R3

R3(config)# crypto key generate rsa

Step 6: Verify the ssh configuration

R3# show ip ssh

SSH enabled-version 1.99

Authentication time out: 120 secs; Authentication retries : 3

Step 7: Configure SSH timeouts and authentication parameters

R3(config)# ip ssh time-out 90

R3(config)# ip ssh authentication-retries 2

R3(config)#ip ssh version 2

Step 8: Verify the SSH configurations

R3# show ip ssh

Step 9: Attempt to connect to R3 via Telnet from pc-c open the desktop of pc-c , select the command prompt icon

Pcc> telnet 192.168.3.1

This connection should fail because R3 has been configured to accept only SSH connections on the virtual terminal lines.

Step 10: connect to R3 using SSH on pc-c

Pcc> ssh -l SSHadmin 192.168.3.1

Password: sshpa55

Step 11: Connect to R3 using SSH on R2

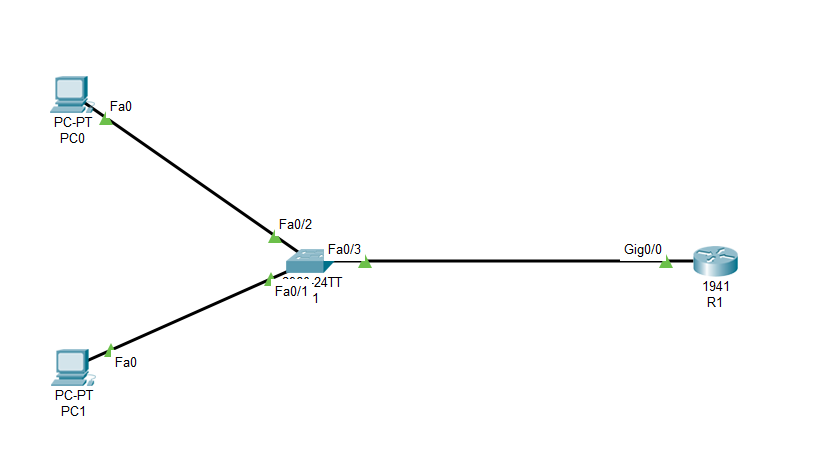
R2# ssh -v 2 -l SSHadmin 10.2.2.1

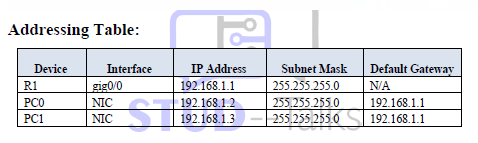
Password: sshpa55

**Practical 2**

**Configure AAA Authentication on Router**

**S7Q7 S18Q24**

****

****

**Objectives:**

**▪ 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.**

**Part 1: Configure Router**

Step 1 : Configure secret on router

R(config) # enable secret enpa55

Step 2 : Configure password for vty lines

R(config) # line vty 0 4

R(config-line) # password vtypa55

R(config-line)# login

Step 3: Configure OSPF on router

R1(config) # router ospf 1

R1(config – router) # network 192.168.1.0 0.0.0.255 area 0

Step 4: Configure ospf md5 authentication for all router in area 0

R1(config)# router ospf 1

R1(config-router)# area 0 authentication message-digest

Step 5: Configure the md5 key for all the router in area 0

R1(config)# int gig0/0

R1(config-if)#ip ospf message-digest-key 1 md5 md5pa55

Step 6: Verify Configuration

a. Verify the MD5 authentication configurations using the commands show ip ospf interface.

b. Verify end-to-end connectivity.

Output should be shown in all the routers :

R# show ip ospf interface

Message-digest Authentication Enabled

Youngest key ID is 1

**Part 2: Configure local AAA Authentication for console access on R1**

Step 1: Test Connectivity

PC0> ping 192.168.1.3 (pc0)

Successful

PC1> ping 192.168.1.2 (pc1)

Succesful

Step 2: Configure a local username on R1

R1(config)# username admin secret adminpa55

Step 3: Configure local AAA Authentication for console access on R1

R1(config)# aaa new-model

R1(config)#aaa authentication login default local

Step 4: Configure the line console to use the defined AAA authentication method

R1(config)# line console 0

R1(config-line)# login authentication default

Step 5: Verify the AAA authentication method

R1(config-line)# end

Username : admin

Password: adminpa55

R1>

**Part 3: configure local AAA authentication for vty lines on R1**

Step 1: Configure domain name and crypto key for user with ssh

R1(config)# ip domain-name ccnasecurity.com

R1(config)# crypto key generate rsa

How many bits in the modulus [512]: 1024

Step 2: Configure a named list AAA authentication method for the vty lines on R1

R1(config)# aaa authentication login SSH-login local

Step 3: Configure the vty lines to use the defined AAA authentication method

R1(config)# line vty 0 4

R1(config-line)# login authentication SSH-LOGIN

R1(config-line)# transport input ssh

R1(config-line)#end

Step 4: Verify the AAA authentication method

Pc0> ssh -l admin 192.168.1.1

Password: adminpa55

R1>

Pc1> ssh -l admin 192.168.1.1

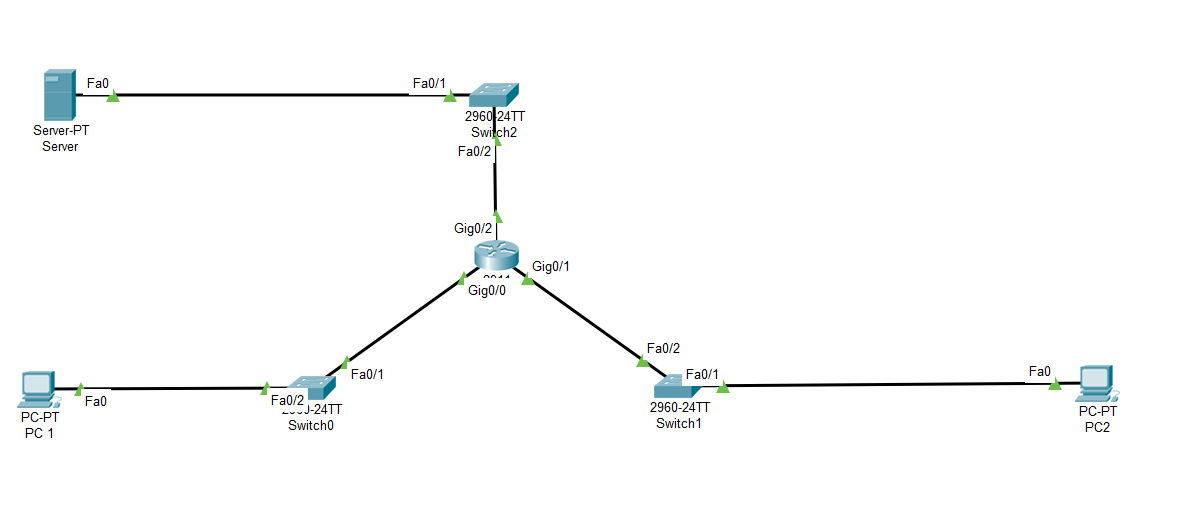
Password: adminpa55

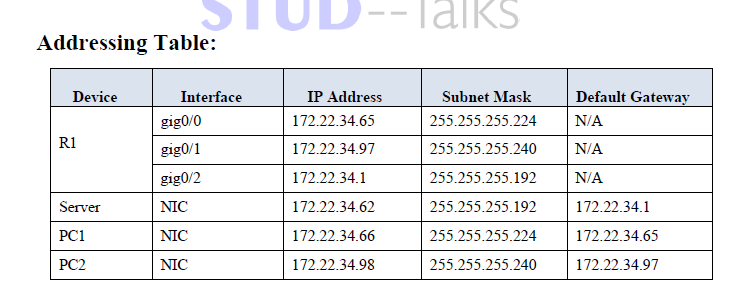
R1>

**Practical 3**

**Configuring extended ACLs**

**A] S6Q6 , S14Q16**

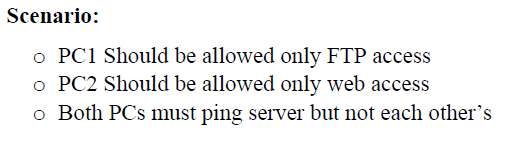
****

****

**Objectives:**

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

**▪ Configure, Apply and Verify an Extended Named ACL**

****

**Part 1: 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: Enable Secret on router

R1(config)# enable secret enpa55

**Part 2: Configure , Appply and verify an extended Numbered ACL**

Step 1: Configure an ACL to permit FTP and ICMP

R1(config)# access-list 100 permit tcp 172.22.34.65 0.0.0.31 host 172.22.34.62 eq ftp

R1(config)#access-list 100 permit icmp 172.22.34.65 0.0.0.31 host 172.22.34.62

Step 2: Apply the ACL on the correct ibnterface filter traffic

R1(config)# int gig0/0

R1(config-if)#ip access-group HTTP\_ONLY in

Step 3: Verify the ACL implementation

1. Ping from pc1 to server

Pc1> ping 172.22.34.62

Successful

1. ftp from pc1 to server the username and password are both cisco

Pc1> ftp 172.22.34.62

1. exit the ftp service of the server

ftp>quit

1. ping from pc1 to pc2

pc1> ping 172.22.34.98

UnSuccessful destination host unreachable

**Part 3: Configure , Appply 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-exte-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www

R1(config-exte-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

1. ping from pc2 to server

pc2> ping 172.22.34.62

successful

1. ftp from pc2 to server

pc2> ftp 172.22.34.62

unsuccessful

1. open the web browser on pc2

url-> http://172.22.34.62

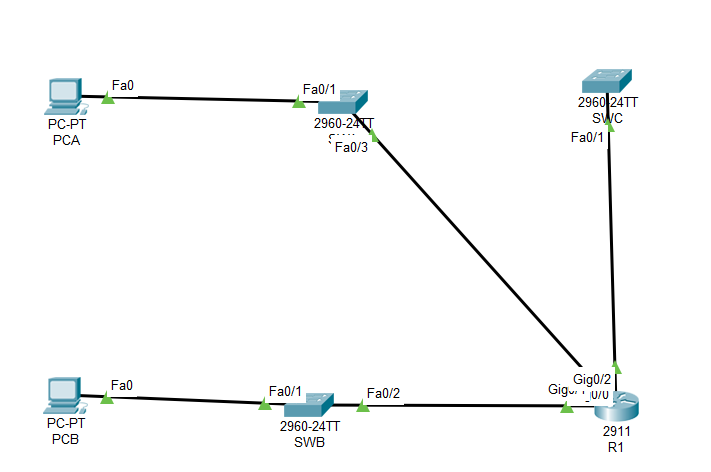
Successful

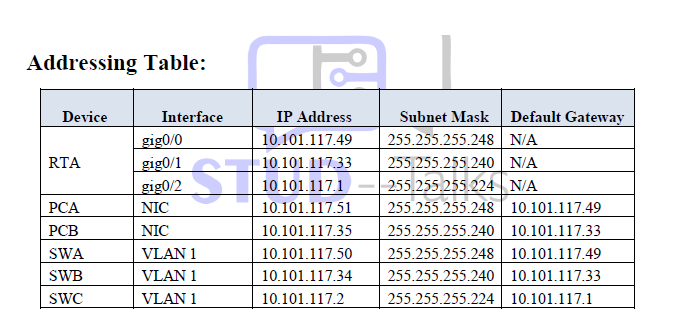
1. ping from pc2 to pc1

pc2> ping 172.22.34.66

unsuccessful

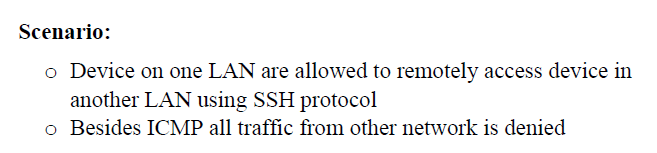
**B] S18Q23**

****

****

**Objectives:**

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

****

**Part 1: 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 vlan1

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 a secret on router and switch

RTA/SW (config)# enable secret enpa55

Step 3: Configure a console password on router and switch

RTA/SW (config)# line console 0

RTA/SW (config-line)# password tyit

RTA/SW (config-line)# login

Step 4: Test Connectivity

Ping from PCA to PCB

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 2: Configure a switch and router to support ssh connection**

Step 1: Configure a 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 modules[512]:1024

Step 4: Verify the SSH connection

PCA> ssh -l admin 10.101.117.34

Password: adminpa55

SWB>

SWB>exit

PCA> ssh -l admin 10.101.117.2

Password: adminpa55

SWC>

SWC>exit

PCB> ssh -l admin 10.101.117.50

Password: adminpa55

SWA>

SWA>exit

PCB> ssh -l admin 10.101.117.2

Password: adminpa55

SWC>

SWC>exit

SWC> ssh -l admin 10.101.117.50

Password: adminpa55

SWC>

SWC>exit

SWC> ssh -l admin 10.101.117.34

Password: adminpa55

SWB>

SWB>exit

**Part 3: Configure, apply and verify an extended numbered ACL**

Step 1: Configure the extended ACL

RTA/SW(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/SW(config)# access-list 199 permit icmp any any

Step 2: Apply the extended ACL

RTA/SW(config)# int gig0/2

RTA/SW(config-if)# ip access-group 199 out

Step 3: Verify the extended ACL implementation

1. Ping from pcb to all of other ip address in network

PCB> ping 10.101.117.51

Successful

PCB> ping 10.101.117.2

Successful

1. Ssh from pcb to swc

PCB> ssh -l admin 10.101.117.2

Password: adminpa55

Swc>

1. Exit the ssh session to swc

Swc>exit

1. Ping from pca to all the other ip address in the network

PCA> ping 10.101.117.35

Successful

PCA> ping 10.101.117.2

Successful

1. SSH from PCA to SWB

PCA> ssh -l admin 10.101.117.2

Connection timed out

1. Ssh from pca to swb

PCA> ping 10.101.117.34

Password: adminpa55

SWB>

1. After logging into swb do not logout swa to ssc in priviliged exec code

SWB# ssh -l admin 10.101.117.2

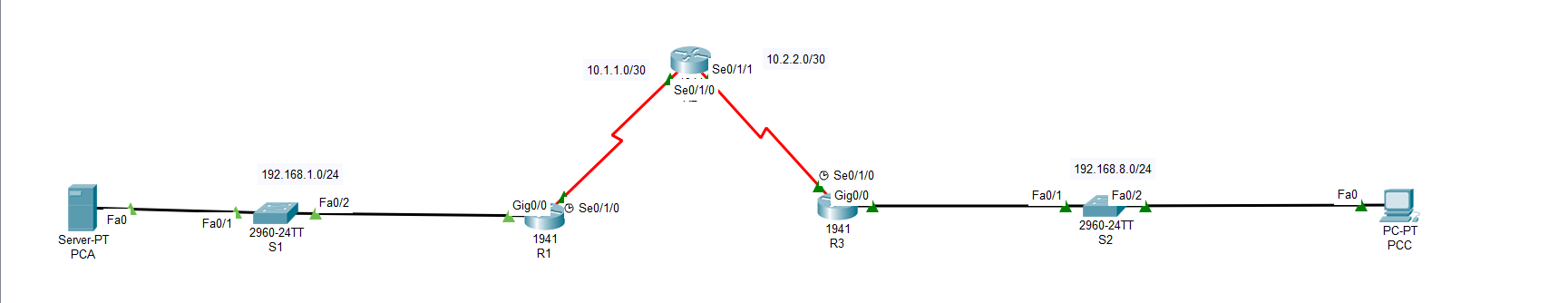
Password: adminpa55

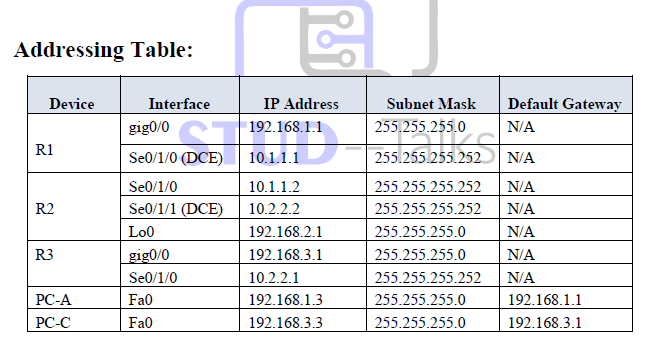
SWC>

**Practical 4**

**Configure IP Acls To Mitigate Attacks**

**A] S8Q8 S14Q15 S15Q17**

****

****

**Objectives:**

* + Verify connectivity among devices before firewall configuration.
  + Use ACLs to ensure remote access to the routers is available only from management station PC-C.
  + Configure ACLs on R1 and R3 to mitigate attacks.
  + Verify ACL functionality.

**Part 1: Configure router**

Step 1: Configure a secret on router

R(config)# enable secret enpa55

Step 2: Configure a console password on router

R(config)# line console 0

R(config-line)# password conpa55

R(config-line)# login

Step 3: Configure SSH login on router

R(config)# ip domain-name ccnasecurity.com

R(config)# username admin secret adminpa55

R(config)# line vty 0 4

R(config-line)#login local

R(config)# crypto key generate rsa

How many bits in the modules [512] : 1024

Step 4: Configure loop back address on router 2

R2(config)# int loopback 0

R2(config-if)# ip address 192.168.2.1 255.255.255.0

R2(config-if)# no shut

Step 5: configure state routing on router

R1(config)# ip route 192.168.3.0 255.255.255.0 10.1.1.2

R1(config)# ip route 10.2.2.0 255.255.255.252 10.1.1.2

R1(config)# ip route 192.168.2.0 255.255.255.0 10.1.1.2

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

R3(config)# ip route 192.168.1.0 255.255.255.0 10.2.2.2

R3(config)# ip route 192.168.2.0 255.255.255.0 10.2.2.2

R3(config)# ip route 10.1.1.0 255.255.255.252 10.2.2.2

**Part 2 : Verify Basic Network Connectivity**

Step 1: From PCA , verify connectivity to PCC and R2

PCA>ping 192.168.3.3

Successful

PCA>ping 192.168.2.1

Successful

PCA>ssh -l admin 192.168.2.1

password: adminpa55

R2>exit

Step 2: from PCC verify connectivity to PCA and R2

PCC> ping 192.168.1.3

successful

PCC> ping 192.168.2.1

successful

PC-C>ssh -l admin 192.168.2.1

password: adminpa55

R2> exit

Open web browser to PCA server (192.168.1.3 ) to display web page

Close the browser when done

Desktop -> web browser -> 192.168.1.3

Successful

**Part 3: secure access to router**

Step 1: configure ACL 10 to block all remote access to router except PCC execute command on all routers

R(config)# access-list 10 permit host 192.168.3.3

Step 2: Apply ACL 10 to traffic on vty lines execute command on all routers

R(config)# line vty 0 4

R(config)# access-class 10 in

Step 3: verify exclusive access from management statcon

PCC> ssh -l admin 192.168.2.1

Password: adminpa55

R2> exit

Step 4 : Verify denial from PCA

PCA> ssh -l admin 192.168.2.1

Unsuccessful : Connection refused by remote host

**Part 4: Create a numbered 10 ACL 120 on R1**

Step 1: verify that PCC can access the PCA via the HTTPS using the web browser

Be sure to disable the HTTP and enable HTTPS on server PCA in service tab

Step 2: config ACL 120 to specifically permit and deny the specified traffic

R1(config)# access-list 120 permit udp any host 192.168.1.3 eq domain

R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq smtp

R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq ftp

R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq 443

R1(config)# access-list 120 permit tcp any host 192.168.3.3 eq 22

Step 3 : Apply the ACL 10 interface

R1(config)#int se 0/1/0

R1(config)#ip access-group 120 in

Step 4: Verify that PCC cannot access PCA via HTTPS using the web browser

Desktop -> web Browser -> 192.168.1.3

Unsuccessful request timed out

**Part 5: Modify an existing ACL on R1**

Step 1: Verify that PCA cannot successfully ping the loopback interface on R2

PCA> ping 192.168.2.1

Unsuccessful request timed out

Step 2: Make any necessary changes to ACL 120 to permit and deny the specified traffic

R1(config)#access-list 120 permit icmp any any echo-reply

R1(config)#access-list 120 permit icmp any any unreachable

R1(config)#access-list 120 deny icmp any any

R1(config)#access-list 120 permit ip any any

Step 3: Verify that PCA can successfully ping the loopback interface on R2

Pca> ping 192.168.2.1

Successful

Part 6: Create a numbered IP ACL 110 on R3

Step 1: configure ACL 110 to permit only traffic from inside network

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

Step 2: Apply the ACL to interface

R3(config)# int gig0/1

R3(config)# ip access-group 110 in

Part 7: Create a Numbered IP ACL 100 on R3

Step 1: Configure ACL 100 to block all the specified traffic from the outside network

R3(config)# access-list 100 permit tcp 10.0.0.0 0.255.255.255 host 192.168.3.3 eq 22

R3(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any

R3(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any

R3(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any

R3(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any

R3(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any

R3(config)# access-list 100 permit ip any any

Step 2 : Apply the ACL to interface

R3(config)# int se0/1/0

R3(config-if)# ip access-group 100 in

Step 3: Confirm that the specified traffic entering interface serial is handled

pcc> ping 192.168.1.3

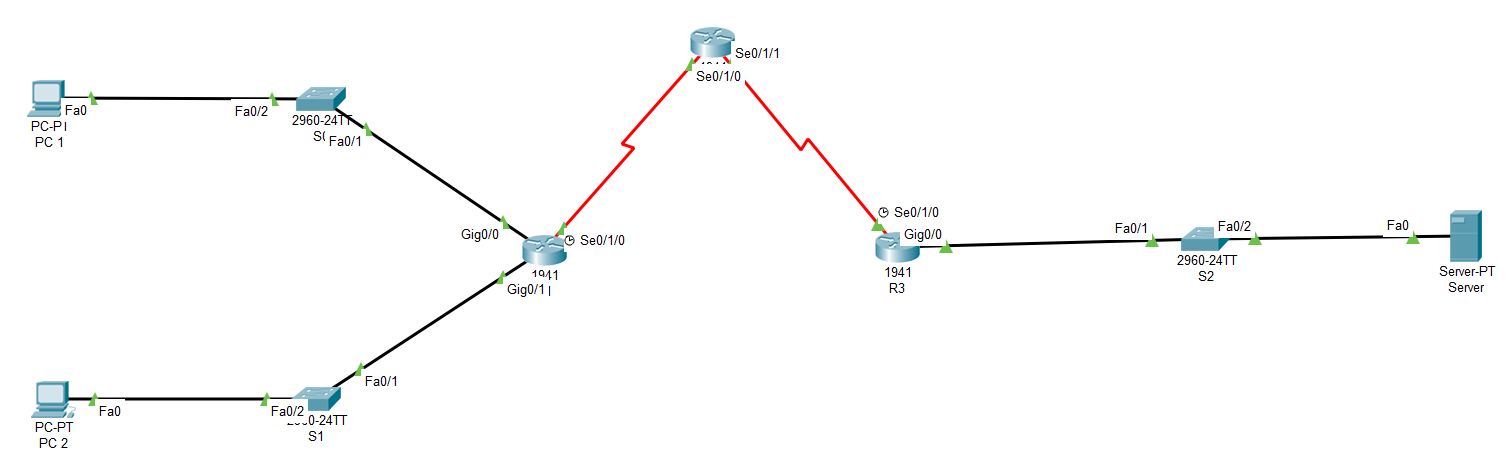
unsuccessful request timed out

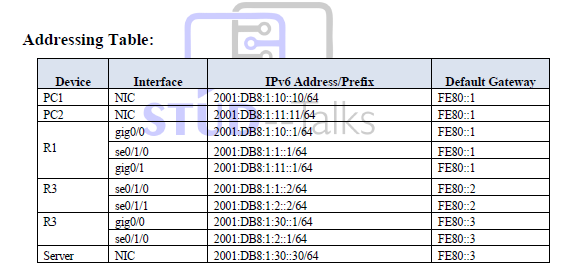
pcc>ssh -l admin 192.168.2.1

password: adminpa55

R2>exit

**B] S3Q3 , S10Q10**

****

****

**Objective:**

* • Configure, Apply, and Verify an IPv6 ACL
* • Configure, Apply, and Verify a Second IPv6 ACL

**Part 1: Configure Router**

Step 1: Configure Secret on Router

R(config)# enable secret enpa55

Step 2: Assign static ipv6 address

R1(config)# int gig 0/0

R1(config - if)# ipv6 address 2001:DB8:1:10::1/64

R1(config - if)# ipv6 address FE80::1 link-local

R1(config - if)# no shut

R1(config - if)# exit

R1(config)# int gig 0/1

R1(config - if)# ipv6 address 2001:DB8:1:11::1/64

R1(config - if)# ipv6 address FE80::1 link-local

R1(config - if)# no shut

R1(config - if)# exit

R1(config)# int se 0/1/0

R1(config - if)# ipv6 address 2001:DB8:1:1::1/64

R1(config - if)# ipv6 address FE80::1 link-local

R1(config - if)# no shut

R1(config - if)# exit

Step 3: Enable Ipv6 Routing

R1(config)# ipv6 unicast-routing

R1(config-if)# ipv6 route 2001:DB8:1:2::0/64 2001:DB8:1:1::2

R1(config-if)# ipv6 route 2001:DB8:1:30::0/64 2001:DB8:1:1::2

R2(config)# ipv6 unicast-routing

R2(config-if)# ipv6 route 2001:DB8:1:10::0/64 2001:DB8:1:1::1

R2(config-if)# ipv6 route 2001:DB8:1:11::0/64 2001:DB8:1:1::1

R2(config-if)# ipv6 route 2001:DB8:1:30::0/64 2001:DB8:1:2::1

R3(config)# ipv6 unicast-routing

R3(config-if)# ipv6 route 2001:DB8:1:10::0/64 2001:DB8:1:2::2

R3(config-if)# ipv6 route 2001:DB8:1:11::0/64 2001:DB8:1:2::2

R3(config-if)# ipv6 route 2001:DB8:1:1::0/64 2001:DB8:1:2::2

Step 4: Verify Connectivity

pc1> ping 2001:DB8:1:30::30

successful

pc2> ping 2001:DB8:1:30::30

successful

**Part 2: Configure, apply and verify an ipv6 ACL**

Step 1 : configure an ACL that will block HTTP and HTTPS access

R1(config)# ipv6 access-list BLOCK\_HTTP

R1(config-ipv6-acl)# deny tcp any host 2001:DB8:1:30::30 eq www

R1(config-ipv6-acl)# deny tcp any host 2001:DB8:1:30::30 eq 443

R1(config-ipv6-acl)# permit ipv6 any any

R1(config-ipv6-acl)# exit

Step 2: Apply the ACL to the correct Interface

R1(config)# int gig 0/1

R1(config-if)# ipv6 traffic-filter BLOCK\_HTTP in

Step 3: Verify the ACL implementations

Open a web browser to the pc1 to display the webpage.

Desktop-> web browser -> <http://2001:DB8:1:30::30>

Successful

Desktop-> web browser -> <https://2001:DB8:1:30::30>

Successful

Open a web browser to the pc2 to display the web page

Desktop-> web browser -> <http://2001:DB8:1:30::30>

Unsuccessful-Request-Timeout

Desktop-> web browser -> <https://2001:DB8:1:30::30>

Unsuccessful-Request-Timeout

Pc2> ping 2001:DB8:1:30::30

Successful

**Part 3: Configure , Apply and Verify a second ipv6 ACL**

Step 1: Create an access-list to block ICMP

R3(config)# ipv6 access-list BLOCK\_ICMP

R3(config-ipv6-acl)# deny ICMP any any

R3(config-ipv6-acl)# permit ipv6 any any

R1(config-ipv6-acl)# exit

Step 2: Apply the ACL to the correct Interface

R3(config)# int gig 0/0

R3(config-if)# ipv6 traffic-filter BLOCK\_ICMP out

Step 3: Verify that a proper access lists functions

pc2> ping 2001:DB8:1:30::30

unsuccessful – Destination host unreachable

pc1> ping 2001:DB8:1:30::30

unsuccessful – Destination host unreachable

open a web browser to the pc1 to display the web page

pc1->Desktop->web browser-><http://2001:DB8:1:30::30>

successful

pc1->Desktop->web browser-><https://2001:DB8:1:30::30>

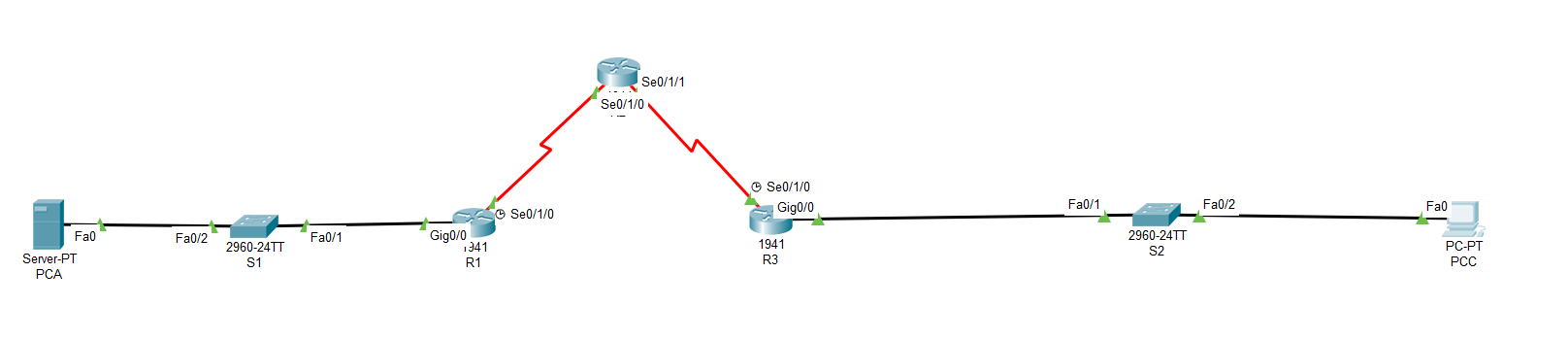
successful

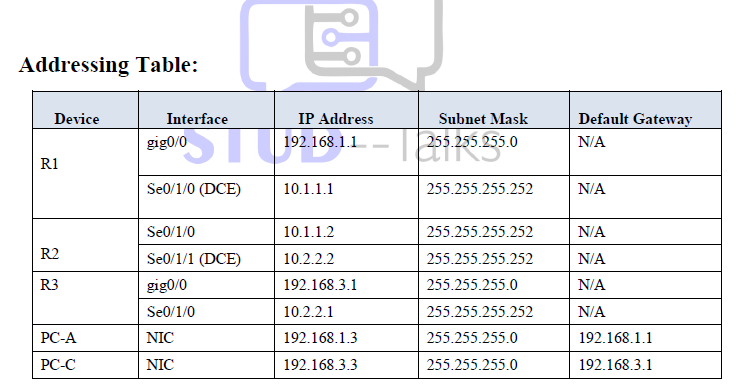
**Practical 5**

**Configure a Zone-Based Policy Firewall**

**S1Q1 S17Q21**

**A]**

****

****

**Objectives:**

 Verify connectivity among devices before firewall configuration.

 Configure a zone-based policy (ZPF) firewall on R3.

 Verify ZPF firewall functionality using ping, SSH, and a web browser.

**Part 1: Configure Router**

Step 1: Configure console password on router Execute command on all router

R(config) # line console 0

R(config-line) # password conpa55

R(config-line) # login

Step 2: Configure Password for vty lines .

Execute command on all routers

R(config) # line vty 0 4

R(config-line) # password vtypa55

R(config-line) # login

Step 3: Configure a secret on router . Execute Command on all router

R(config)# enable secret enpa55

Step 4: Configure SSH login on routers

Execute command on all router

R(config) # ip domain-name ccnasecurity.com

R(config) # username admin secret adminpa55

R(config) # line vty 0 4

R(config-line) # login local

R(config-line) # crypto key generate rsa

How many bits in the module : 1024

Step 5 : Configure static routing on routers

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

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

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 10.2.2.0

**Part 2: Verify Basic Network Connectivity**

Step 1: Check Connectivity from pca to pcc

PC-A>ping 192.168.3.3

Successful

Step 2: Access R2 using SSH

Pcc>ssh -l admin 10.2.2.2

password: adminpa55

R2> exit

Step 3: From pcc open a web browser to pca server

pcc>desktop-> web browser -><http://192.168.1.3>

successful

**Part 3 : Create the firewall Zone on R3**

Step 1: Verify that security Technology package

R3# show version

(security not enabled )

Step 2: Enable security Technology Package

R3(config)# license boot module c1900 technology-package securityk9

Step 3: save the running config and reload the router

R3# copy run start

R3# reload

Step 4: Verify the security Technology Package

R3# show version

(Security enabled )

Step 5 : Create an Internal zone

R3(config)# zone security IN-ZONE

R3(config-sec-zone)# exit

R3(config)# zone security OUT-ZONE

R3(config-sec-zone)# exit

**Part 4 : Identify Traffic using a class-map**

Step 1 : Create ACL that defines internal traffic

R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 any

Step 2 : create a class Map

R3(config)# class-map type inspect match-all IN-NET-CLASS-MAP

R3(config-cmap)# match access-group 101

R3(config-cmap)# exit

**Part 5 : specify Firewall Poilicies**

Step 1: Create a policy map to determine what to do with matched traffic

R3(config) # policy-map type inspect IN-2-OUT-PMAP

Step 2 : Specify a class – type of inspect and reference class map IN NET-CLASS-MAP

R3(config-cmap)# class type inspect IN-NET-CLASS-MAP

Step 3 : specify the action of inspect for the policy map

R3(config-cmap-c)# inspect

R3(config-cmap-c)# exit

R3(config-cmap-c)# exit

**Part 6 : Apply Firewall Policies**

Step 1 : create a pair of zone

R3(config)# zone-pair security IN-2-OUT-ZPAIR source IN-ZONE

destination OUT-ZONE

Step 2 : specify the policy map for handling traffic between 2 zones

R3(config-sec-zone-pair)# service-policy type inspect IN-2-OUT-PMAP

R3(config-sec-zone-pair)# exit

R3(config)#

Step 3 : Assign interfaces to appropriate security zones

R3(config)# int gig 0/0

R3(config-if)# zone-member security IN-ZONE

R3(config-if)# exit

R3(config-if)# int se 0/1/0

R3(config-if)# zone-member security OUT-ZONE

R3(config-if)# exit

Step 4 : Copy the running configuration to startup config

R3# copy run start

R3# reload

**Part 7 : Test firewall functionality from IN-ZONE to OUT-ZONE**

Step 1 : From internal pcc-c ping external pc-a server

PC-C>ping 192.168.1.3

successful

Step 2 : Access R2 using SSH

PC-C>ssh -l admin 10.2.2.2

password: adminpa55

R2>

Step 3 : View established sessions

R3# show policy-map type inspect zone-pair sessions

Session 175216232 ( 192.168.3.3 : K28 -> (10.2.2.2:22) tcp SIS-OPEN/TCP-ESTB

Step 4 : from pcc exit the ssh session on R2 and close the command prompt

R2> exit

Step 5 : from internal PCA ping external PCC server

PCA > <http://192.168.1.3>

Successful

Step 6 : view established session

R3# show policy-map type inspect zone-pair sessions

Session 555266534 ( 192.168.3.3:1036 -> (192.168.1.3:10) tcp SIS-OPEN/TCP-ESTB

**Part 8 : Test firewall functionality from OUT-ZONE to IN-ZONE**

Step 1 : from internal PCA ping external PCC server

PCA> ping 192.168.3.3

Unsuccessful - request timed out

Step 2 : from R2 ping PCC

R2# ping 192.168.3.3

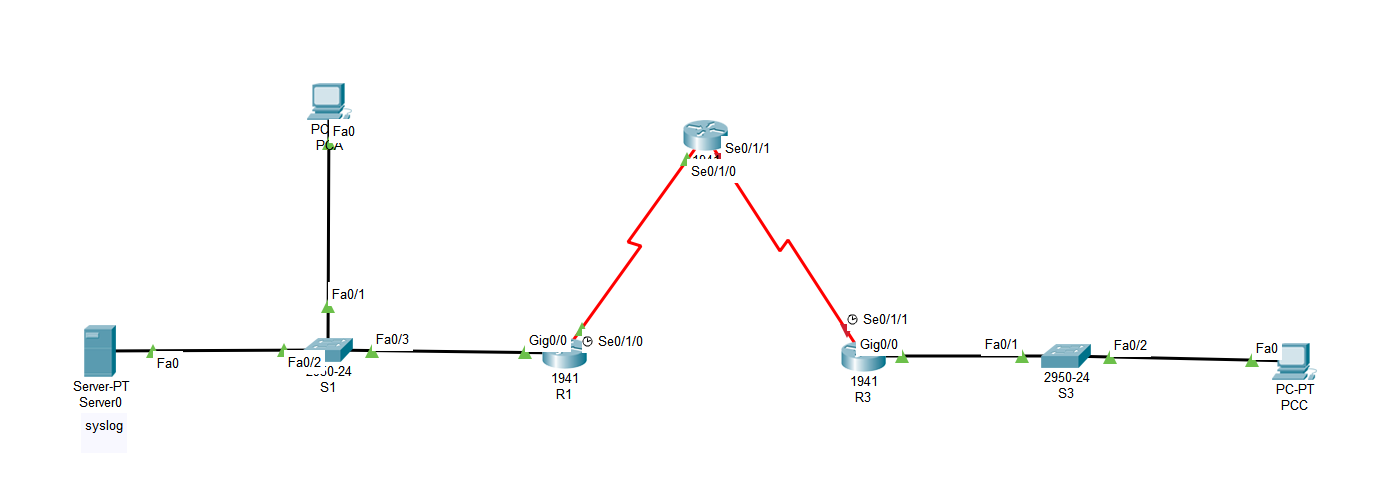
Unsuccessful – request timed out

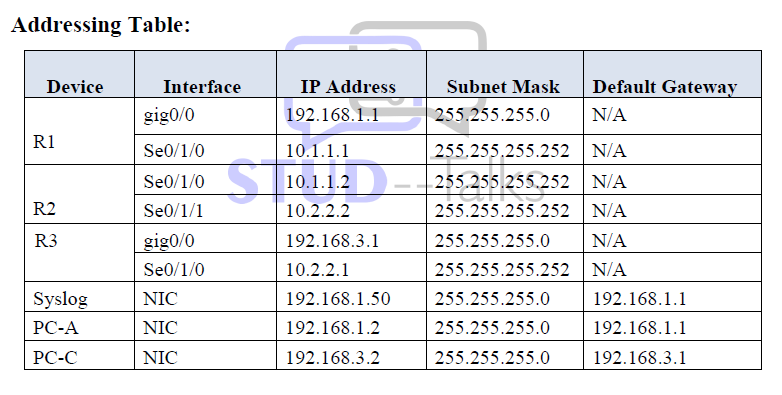
**Practical 6**

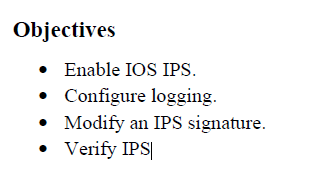
**Configure IOS Intrusion prevention system ( IPS ) using the CLI**

**S5Q5 S16Q19**

**A]**

****





**Part 1 : Configure Router**

Step 1 : Configure secret on router

Execute Command on all Router

R(config) # enable secret enpa55

Step 2 : Configure Console password on router

Execute command on all Router

R(config)# line console 0

R(config-line)# password conpa55

R(config)# login

Step 3 : Configure SSH login on router

Execute Command on all router

R(config)# ip domain-name ccnasecurity.com

R(config)# username admin secret adminpa55

R(config)# line vty 0 4

R(config-line)# login local

R(config)# crypto key generate rsa

How many bits in modules [512] : 1024

Step 4 : Configure OSPF on Router

R1 (config) # router ospf 1

R1(config-router)# network 192.268.1.0 0.0.0.255 area 0

R1(config-router)# network 10.1.1.0 0.0.0.3 area 0

R2(config)# router ospf 1

R2(config-router)# network 10.1.1.0 0.0.0.3 area 0

R2(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3(config)# router ospf 1

R3(config-router)# network 10.2.2.0 0.0.0.3 area 0

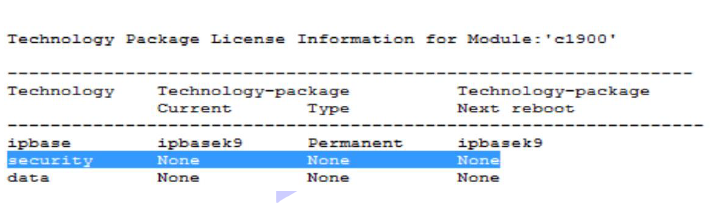
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0

**Part 2 : Enable IOS PIS**

Step 1 : Enable the security Technology package

R1# show version

Security not enabled



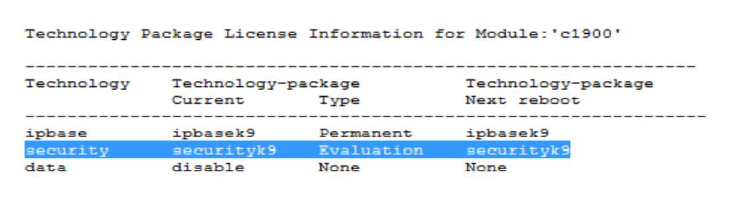
R1 (config) # license boot module c1900 technology-package securityk9

R1# copy run start

R1 # reload

R1 # show version

Security enabled



Step 2 : verify network connectivity

Pca > ping 192.168.3.2

(successful )

Pcc> ping 192.168.1.2

(successful )

Step 3 : Create an IOS IPS configuration directory in flash

R1# mkdir ipsdir

Create directory file name [ipsdir] ? <Enter>

Step 4 : Configure the IPS signature storage location

R1 (config) # ip ips config location flash:ipsdir

Step 5 : Create an IPS rule

R1 (config) # ip ips name iospis

Step 6 : Enable Logging

R1 (config) # ip ips notify log

R1 # clock set 19:40:00 08 April 2022

R1 (config) # service timestamp log datetime msec

R1 (config) # logging host 192.168.1.50

Step 7 : Configure IOS IPS to use signature categories

R1 (config) # ip ips signature-category

R1 (config-ips-category-action) #category all

R1 (config-ips-category-action)# retired true

R1 (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-category)# exit

Do You Want To Accept The changes ? [confirm] < Enter >

Step 8 : Apply the IPS rule to an Interface

R1 (config) # int gig 0/0

R1 (config-if) # ip ips iosips out

Step 9 : use show command to verify IPS

R1# show ip ips all

Step 10 : view syslog messages

Click the syslog server -> service tab -> SYSLOG

**Part 3 : Modify the Signature**

Step 1 : change the event action of signature

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

Do You want to accept these changes ? [confirm ] < Enter >

Step 2 : Use show command to verify IPS

R1# show ip ips all

Step 3 : Verify that IPS is working properly

a)from pc-c attempt to ping pca

pcc> ping 192.168.1.2

request timeout

pca> ping 192.168.3.2

successful

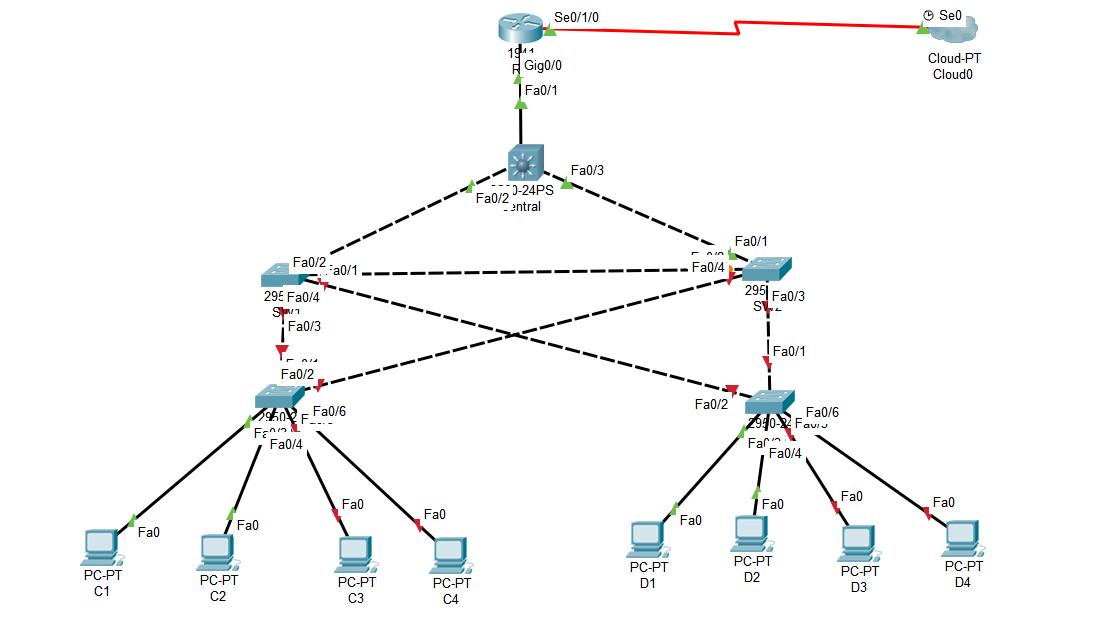
Step 4 : view the syslog message

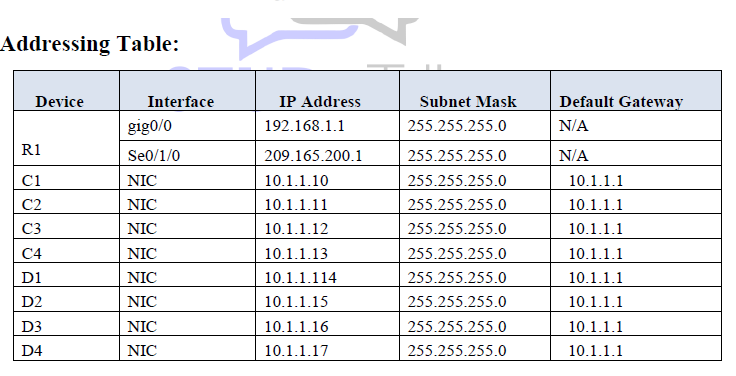
Click syslog server -> service tab -> syslog server to view log file

**Practical 7**

**Packet -Tracer Layer 2 Security**

**S9Q9 S16Q20**





**Objectives:**

* • Assign the Central switch as the root bridge.
* • Secure spanning-tree parameters to prevent STP manipulation attacks.
* • Enable port security to prevent CAM table overflow attacks

**Part 1 : Configure switch/router**

Step 1 : Configure secret

Execute command on all router and all switches

R1/sw(config)# enable secret enpa55

Step 2 : Configure Console Password

Execute Command on all router and all switches

R1/sw(config)# line console 0

R1/sw(config-line)# password conpa55

R1/sw(config-line)# login

Step 3 : Configure SSH login

Execute command on all router and all switches

R1/sw(config)# ip domain-name ccnasecurity.com

R1/sw(config)# username admin secret adminpa55

R1/sw(config)# line vty 0 4

R1/sw(config-line)# login local

R1/sw(config-line)# crypto key generate rsa

How many bits in the module [512]: 1024

**Part 2 : Configure root bridge**

Step 1 : Determine the current root bridge

Central# show spanning-tree

Sw1# show spanning-tree

Step 2 : Assign central as the primary root bridge

Central(config)# spanning-tree vlan 1 root primary

Central# show spanning-tree

Step 3 : Assign sw-l as a secondary root bridge

Sw1(config)# spanning-tree vlan 1 root secondary

Sw1# show spanning-tree

**Part 3 : Project Against STP attacks**

Step 1 : Enable port fast on all access ports

SWA/B(config)# int range fa 0/1 -4

SWA/B(config-if-range)# spanning-tree portfast

Step 2 : Enable BPDU guard on all access ports

SWA/B(config)# int range fa0/1 -4

SWA/B(config-if-range)# spanning-tree bpduguard enable

Step 3 : Enable root guard

SW1/2(config)# int range fa0/23-24

SW1/2(config-if-range)# spanning-tree guard root

**Part 4 : Configure Port security and disable unused ports**

Step 1 : Configure basic port security on all ports connected to host devices

SWA/B(config)# int range fa 0/1-22

SWA/B(config-if-range)#switchport mode access

SWA/B(config-if-range)# switchport port-security

SWA/B(config-if-range)# switchport port-security maximum 2

SWA/B(config-if-range)# switchport port-security violation shutdown

SWA/B(config-if-range)# switchport port-security mac-address sticky

Step 2 : Verify Port security

SWA/B#show port-security interface fa0/1

Step 3 : Disable unused ports

SWA/B(config)# int range fa0/5-22

SWA/B(config)# shutdown

Step 4 : Verify connectivity

C1> ping 10.1.1.11 (C2)

successful

C1> ping 10.1.1.14 (D1)

Successful

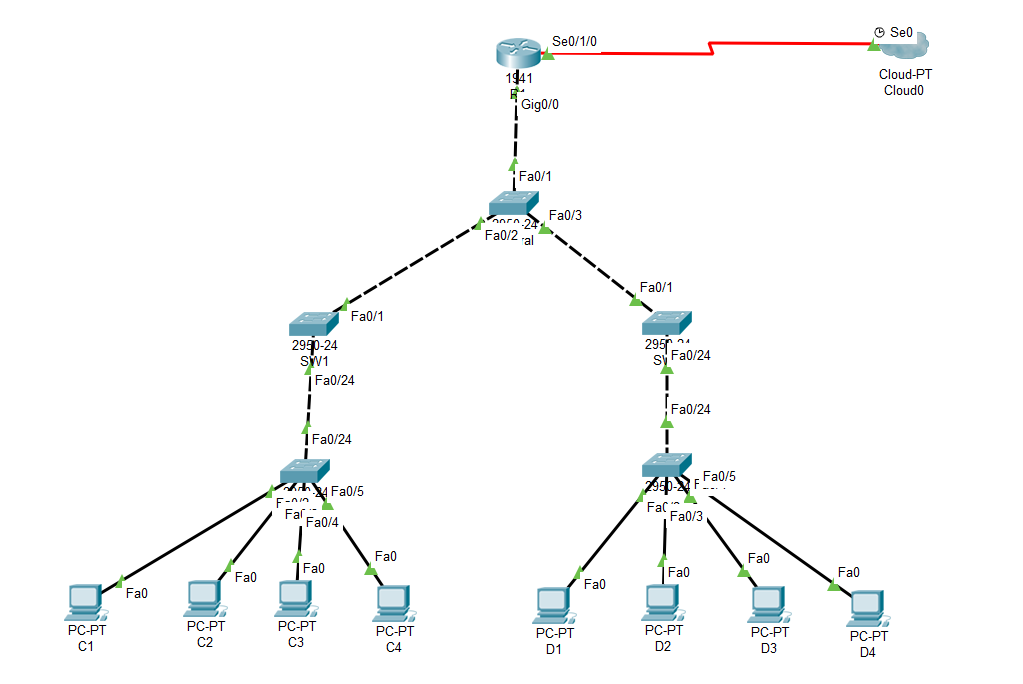
Step 5 : Verify port security

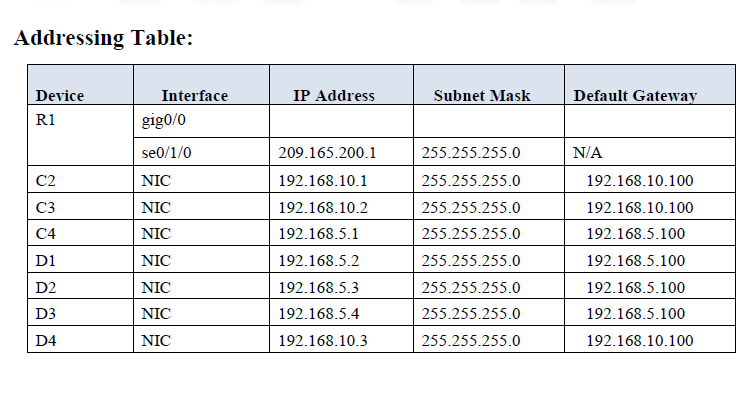
SWA/B# show port-security int fa0/1

**Practical 8**

**Layer 2 VLAN Security**

**S11Q11 , S13Q14 , S17Q22**

****

****

**Objectives**

* • Connect a new redundant link between SW-1 and SW-2.
* • Enable trunking and configure security on the new trunk link between SW-1 and SW-2.
* • Create a new management VLAN (VLAN 20) and attach a management PC to that VLAN.
* • Implement an ACL to prevent outside users from accessing the management VLAN

**Scenario**

A company’s network is currently set up using two separate VLANs: VLAN 5 and VLAN 10. In addition, all trunk ports are configured with native VLAN 15.

**Part 1 : Configure switch/Router**

Step 1 : Configure secret

Execute Command on all router& switches

SW/R1(config)# enable secret enpa55

Step 2 : Configure console password

Execute command on all switches/routers

SW/R1(config)# line console 0

SW/R1(config-line)# password conpa55

SW/R1(config-line)# login

Step 3 : Configure SSH login

Execute command on all switches/routers

SW/R1(config)# ip domain-name ccnasecurity.com

SW/R1(config)# username admin secret adminpa55

SW/R1(config)# line vty 0 4

SW/R1(config-line)# login local

SW/R1(config-line)#crypto key generate rsa

How many bits in the modules [512] : 1024

**Part 2 : Create VLAN & assign access mode and trunk mode to interfaces**

Step 1 : Check existing vlan

Execute command on all switches

SW# show vlan brief

Step 2 : Create new VLAN

Execute command on all switches

SW(config)# vlan 5

SW(config-vlan)#exit

SW(config)# vlan 10

SW(config-vlan)#exit

SW(config)# vlan 15

SW(config-vlan)#exit

Step 3 : check the new VLAN

Execute command on all switches

SW# show vlan brief

Step 4 : Assign access mode to vlan switch interfaces

Execute command on switches SWA/SWB

SWA(config)# int fa 0/2

SWA(config-if)# switchport mode access

SWA(config-if)# switchport access vlan 10

SWA(config)# int fa 0/3

SWA(config-if)# switchport mode access

SWA(config-if)# switchport access vlan 10

SWA(config)# int fa 0/4

SWA(config-if)# switchport mode access

SWA(config-if)# switchport access vlan 5

SWB(config)# int fa 0/1

SWB(config-if)#switchport mode acccess

SWB(config-if)#switchport access vlan 5

SWB(config)# int fa 0/2

SWB(config-if)#switchport mode acccess

SWB(config-if)#switchport access vlan 5

SWB(config)# int fa 0/3

SWB(config-if)#switchport mode acccess

SWB(config-if)#switchport access vlan 5

SWB(config)# int fa 0/4

SWB(config-if)#switchport mode acccess

SWB(config-if)#switchport access vlan 10

Step 5 : check the access mode allocations

SWA# show vlan brief

SWB# show vlan brief

Step 6 : Assign trunk mode to another switch interfaces

SWA(config)# int fa 0/24

SWA(config-if)# switchport mode trunk

SWA(config-if)# switchport trunk native vlan 15

SWB(config)# int fa 0/24

SWB(config-if)# switchport mode trunk

SWB(config-if)# switchport trunk native vlan 15

SW1(config)# int fa 0/24

SW1config-if)#switchport mode trunk

SW1(config-if)#switchport trunk native vlan 15

SW1(config)# int gig0/1

SW1config-if)#switchport mode trunk

SW1(config-if)#switchport trunk native vlan 15

SW2(config)# int fa 0/24

SW2(config-if)#switchport mode trunk

SW2(config-if)#switchport trunk native vlan 15

SW2(config)# int gig 0/1

SW2config-if)#switchport mode trunk

SW2config-if)#switchport trunk native vlan 15

Central(config)#int range gig0/1-2

Central(config-if-range)#switchport mode trunk

Central(config-if-range)#switchport trunk native vlan 15

Central(config)# int fa0/1

Central(config –if)# switchport mode trunk

Central(config –if)# switchport trunk native vlan 15

Step 7 : check the trunk mode allocations

Central# show int trunk

SW1/2# show int trunk

SWA/B#show int trunk

Step 8 : Create sub interfaces on routers to support vlan

R1(config) # int gig 0/0.1

R1(config-subif) # encapsulation dotlq 5

R1(config-subif) # ip address 192.168.5.100 255.255.255.0

R1(config) # int gig 0/0.2

R1(config-subif) # encapsulation dotlq 5

R1(config-subif) # ip address 192.168.5.100 255.255.255.0

R1(config) # int gig 0/0.15

R1(config-subif) #encapsulation dotlq 5

R1(config-subif) # ip address 192.168.5.100 255.255.255.0

**Part 3 : Verify Connectivity**

Step 1 : Verify connectivity between c2(vlan 10) and c3(vlan 10)

C2> ping 192.168.10.2

Successful

Step 2 : Verify connectivity between c2(vlan 10) and D1(vlan 5)

PC2> ping 192.168.5.2

successful

**Part 4 : Create a redundant link between SW-1 & SW-2**

Step 1 : Connect SW1 & SW2 using Crossover Copper Cable connect Wired port fa0/23 on SW2

Step 2 : Enable trunking , including all trunk security mechanisms on link between sw-1 and sw-2

Execute command on SW-1 , SW-2

SW1/2(config)# int fa 0/23

SW1/2(config-if)# switchport mode trunk

SW1/2(config-if)# switchport trunk native vlan 15

SW1/2(config-if)# switchport nonegotiate

**Part 5 : Enable VLAN20 as a management VLAN**

Step 1 : Enable a management VLAN ( VLAN 20) as swa

SWA(config)#vlan 20

SWA(config-vlan)#exit

SWA(config)#int vlan 20

SWA(config-if)#ip address 192.168.20.1 255.255.255.0

Step 2 : Enable same management VLAN on all other switch execute command on SWB ,SW1,SW2 and central

SW(config)#vlan 20

SW(config-vlan)#exit

Create an interface VLAN 20 on all switches and assign an ip address within the 192.168.20.0/24 network

SWB(config)# int vlan 20

SWB(config-if)#ip address 192.168.20.2 255.255.255.0

SW1(config)#int vlan 20

SW1(config-if)#ip address 192.168.20.3 255.255.255.0

SW2(config)#int vlan 20

SW2(config-if)#ip address 192.168.20.4 255.255.255.0

Central(config)# int vlan 20

Central(config-if)# ip address 192.168.20.5 255.255.255.0

Step 3 : Connect and configure the management PC .

Connect the management PC to SWA port fa0/1 and ensure that it is assigned on available IP ADDRESS

note : C1 (IP ADDRESS)> 192.168.20.50

Step 4 : on SWA ensure managementPCC is part of VLAN20

SWA(config)#int fa 0/1

SWA(config)switchport mode access

SWA(config-if)switchport access vlan 20

Step 5 : verify connectivity of management PCC to all switches

C1>ping 192.168.20.1 (SWA)

Successful

C1>ping 192.168.20.2 (SWB)

Successful

C1>ping 192.168.20.3 (SW1)

Successful

C1>ping 192.168.20.4 (SW2)

Successful

C1> ping 192.168.20.5 ( Central)

Successful

**Part 6 : Enable management PC to access Router R1**

Step 1 : Enable a new sub-interface on router R1

R1(config)#int gig 0/0.3

R1(config)#encapsulation dot1q 20

R1(config-subif)#ip address 192.168.10.100 255.255.255.0

Step 2 : set default gateway in management PC

C1 default gateway : 192.168.20.100

Step 3 : Verify connectivity between management PC and R1

C1>ping 192.168.20.100

successful

Step 4 : Enable security

R1(config)#access-list 101 deny ip any 192.168.20.0 0.0.0.255

R1(config)#access-list 101 permit ip any any

R1(config)#access-list 102 permit ip host 192.168.20.50 any

Step 5 : Apply ACL on correct interfaces

R1(config)#interface gig0/0.1

R1(config-subif)# ip access-group 101 in

R1(config)#interface gig0/0.2

R1(config-subif)# ip access-group 101 in

R1(config-subif)# line vty 0 4

R1(config-subif)#access-class 102 in

Step 6 : Verify security

C1> ssh -l admin 192.168.20.100

password: adminpa55

R1> exit

Step 7 : Verify Connectivity between management PC and SWA , SWB , R1

C1>ping 192.168.20.1 (SWA)

successful

C1>ping 192.168.20.2 (SWB)

Successful

C1>ping 192.168.20.100 (R1)

Successful

Step 8 : Verify connectivity between D1 & management PC

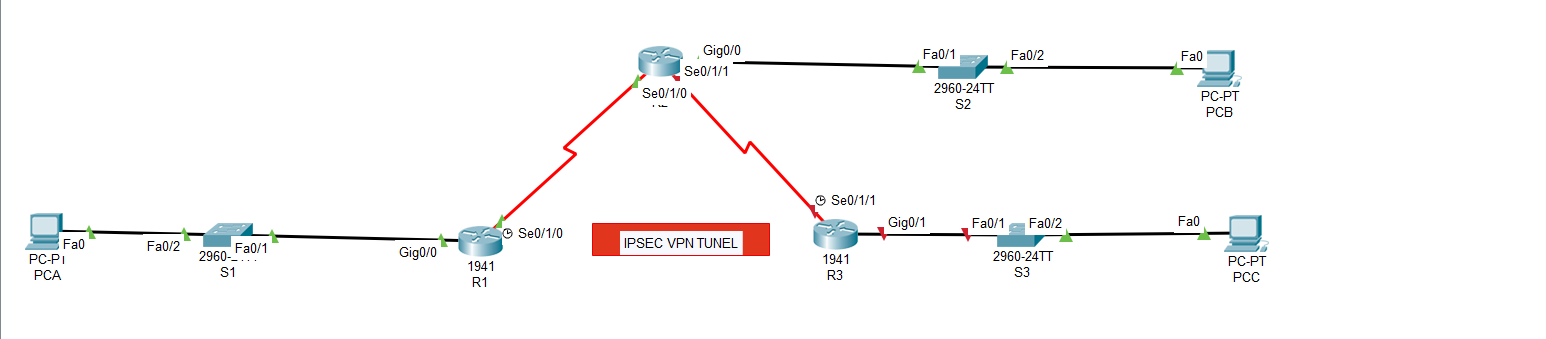
D1> ping 192.168.20.50

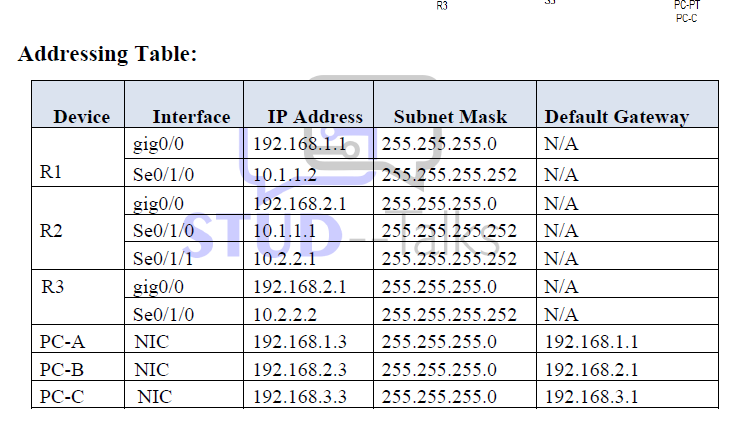
(unsuccessful – Destination host unreachable)

**Practical 9**

**Configure And Verify Site-To-Site Ip Sec Vpn Using CLI**

**S4Q4**

****

****

**Objectives:**

* • Verify connectivity throughout the network.
* • Configure R1 to support a site-to-site IPsec VPN with R3.

**Part 1 : Configure Router**

Step 1 : Configure secret on router

R(config)# enable secret enpa55

Step 2 : Configure console password on router

Execute command on all routers

R(config)#line console 0

R(config-line)#password conpa55

R(config-line)#login

R(config)#ip domain-name ccnasecurity.com

R(config)#username admin secret adminpa55

R(config)#line vty 0 4

R(config-line)#login local

R(config)#crypto key generate rsa

How many bits in the module : 1024

Step 3 : Configure OSPF on routers

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

R2(config)#router ospf 1

R2(config-router)#network 192.168.2.0 0.0.0.255 area 0

R2(config-router)#network 10.1.1.0 0.0.0.3 area 0

R2(config-router)#network 10.2.2.0 0.0.0.3 area 0

R3(config)#router ospf 1

R3(config-router)#network 10.2.2.0 0.0.0.3 area 0

R3(config-router)#network 192.168.3.0 0.0.0.255 area 0

**Part 2 : Configure IPSEC parameters on R1**

Step 1 : from pc-a verify connectivity to pc-c and pc-b

PCA> ping 192.168.3.3

successful

PCA> ping 192.168.2.3

successful

PCB> ping 192.168.3.3

successful

Step 2 : check if security Technology package is enabled

R1#show version

Technology not enabled table

Step 3 : Enable the security Technology package

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

Step 4 : save the running config and reload router to enable security license

R1#copy run start

R1#reload

Step 5 : verify security Technology package is enabled

R1#show version

Technology enabled table

Step 6 : Identify interesting traffic on R1

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

Step 7 : Configure the IKE phase 1 ISAKMP policy on R1

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 8 : Configure the IKE phase 2 IPSEC policy on R1

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

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 9 : Configure the crypto map on outgoing interface

R1(config)#int se0/1/0

R1(config)#crypto map VPN-MAP

**Part 3 : Configure IPSEC parameters on R3**

Step 1 : check if security package is enabled

R3#show version

Technology not enabled

Step 2 : Enable Security Technology package

R3(config)#license boot module c1900 technology-package securityk9

Step 3 : save the running config and reload router to enable the security license

R3#copy run start

R3#reload

Step 4 : Verify security technology package is enabled

R3# show version

Technology package is enabled

Step 5 : Configure R3 to support site-site VPN with R1

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

Step 6 : Configure the IKE phase 1 ISAKMP properties on R3

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 7 : Configure the IKE phase 2 IPSEC policy on R3

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

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

R3(config)# int se0/1/0

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

**Part 4 : Verify the IPSEC VPN**

Step 1 : Verify the tunnel prior to interesting traffic

show crypto ipsec sa

Step 2 : create interesting traffic

pcc> ping 192.168.1.3

successful

Step 3 : Verify the tunnel after interesting traffic

R1# show crypto ipsec sa

Step 4 : create uninteresting traffic

pcb > ping 192.168.1.3

successful

r1# ping 192.168.3.3

successful

r3# ping 192.168.1.3

successful

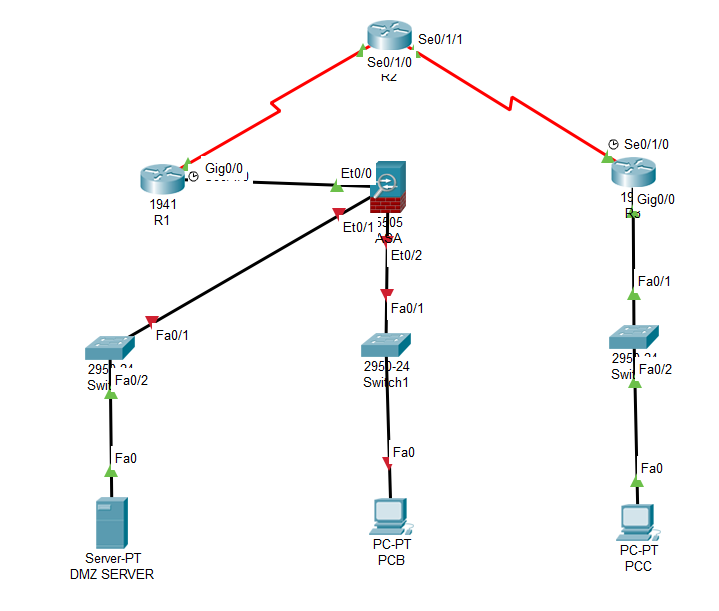
Step 5 : verify the tunnel

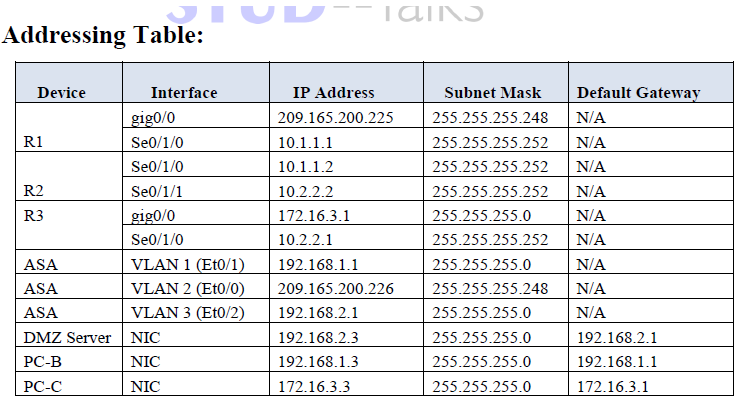
R1#show crypto ipsec sa

**Practical 10**

**Configuring ASA Basic setting and firewall using CLI**

**S12Q12**

****

****

**Objectives:**

* • Verify connectivity and explore the ASA
* • Configure basic ASA settings and interface security levels using CLI
* • Configure routing, address translation, and inspection policy using CLI
* • Configure DHCP, AAA, and SSH
* • Configure a DMZ, Static NAT, and ACLs

**Part 1 : Configure router**

Step 1 : Configure secret on All routers

Execute Command on all routers

R(config)# enable secret enpa55

Step 2 : Configure a console password on router

Execute command on all routers

R(config)# line console 0

R(config-line)# password conpa55

R(config-line)# login

Step 3 : configure SSH login on all router

Execute command on all routers

R(config)# ip domain-name ccnasecurity.com

R(config)# username admin secret adminpa55

R(config)# line vty 0 4

R(config-line)# login local

R(config)# crypto key generate rsa

How many bits in the module : 1024

Step 4 : Configure OSPF on router

Execute command on all routers

R1(config)# router ospf 1

R1(config-router)# network 10.1.1.0 0.0.0.3 area 0

R1(config-router)# network 209.165.200.0 0.0.0.7 area 0

R2(config)#router ospf 1

R2(config-router)# network 10.1.1.0 0.0.0.3 area 0

R2(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3(config)#router ospf 1

R3(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3(config-router)# network 172.16.3.0 0.0.0.255 area 0

**Part 2 : Verify the Connectivity and explore the ASA**

Step 1 : Verify Connectivity

pcc> R1,R2,R3 (successful)

pcc>ASA,DMZ,PCB (Unsuccessful)

Step 2 : Determine ASA Version interface and license

Enter priviledge EXEC mode . A password has not been set . press Enter when promoted for a password

ASA# show version

Step 3 : Determine the file system and content of flash memory

ASA# show file system

ASA# show flash

**Part 3 : Configure ASA settings and interface security using CLI**

Step 1 : Configuring the hostname and domain name

ASA(config)#hostname CCNAS-ASA

CCNAS-ASA(config)# domain-name ccnasecurtiy.com

Step 2 : Configure the enable mode

CCNAS-ASA(config)#enable password enpa55

Step 3 : set date and time

clock set 13:06:00 08 April 2022

Step 4 : Configure inside and outside interface

CCNAS-ASA(config)#int 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)#int 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

Step 5 :Check the Configuration

CCNAS-ASA #show int ip brief

CCNAS-ASA #show ip address

CCNAS-ASA #show switch vlan

Step 6 : Test connectivity to the ASA

pcb > ASA (successful )

pcb> R1 ( unsuccessful)

**Part 4 : Configure routing, address Translation and inspection policy using the CLI**

Step 1 : Configure static default router for the ASA

CCNAS-ASA # show route

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

CCNAS-ASA #show route

Step 2 : Test Connectivity

ASA-> R1(successful)

Step 3 : Configure address translation using PAT & Network Object

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 4 : Test Connectivity

CCNAS-ASA # #show run

PCB-> R1 (Unsuccessful )

CCNAS-ASA # #show nat

Step 5 : Modify the default MPF application inspection global secure policy

CCNAS(config)# class-map inspection-default

CCNAS(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

Step 6 : Test Connectivity

PCB-> R1 ( Successful )

**Part 5 : Configure DHCP , AAA & 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 int inside

CCNAS-ASA(config)# dhcpd enable inside

Change pcb from a static IP address to a DHCP client and verify that it recieves IP addressing information

Step 2 : Configure AAA to use local database for authentication

CCNAS-ASA(config)# username admin password adminpa55

CCNAS-ASA(config)# aaa authentication ssh console login

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 : Verify SSH session

pcc> ssh -l admin 209.165.200.226

password : adminpa55

CCNAS-ASA> exit

pcb> ssh -l admin 192.168.1.1

password : adminpa55

CCNAS-ASA> exit

**Part 6 : Configure DMZ static NAT & ACLs**

Step 1 : Configure the DMZ interface VLAN3 on all ASA

CCNAS-ASA(config)# int vlan 3

CCNAS-ASA(config-if)# ip address 192.168.2.1 255.255.255.0

CCNAS-ASA(config-if)# no forward int vlan 1

CCNAS-ASA(config-if)# nameif dmz

CCNAS-ASA(config-if)# security-level 70

CCNAS-ASA(config-if)# int et 0/2

CCNAS-ASA(config-if)# switchport access vlan 3

Step 2 : check IO Configuration

CCNAS-ASA #show int ip brief

CCNAS-ASA #show ip address

CCNAS-ASA #switch vlan

Step 3 : Configure static NAT DHZ server using 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)

CCNAS-ASA(config-network-object)# static 209.165.200.225

CCNAS-ASA(config-network-object)# exit

Step 4 : Configure an ACL to allow access to DMZ server from internet

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 int outside

Step 5 : Test access to DMZ server

The ability to successfully test outside access to the DMZ web server not in place , therefore , successfully testing is not required .