INFORMATION SECURITY

PRACTICALS

BSc.IT
SEMESTER 6

NAME: ALISHA SHAIKH

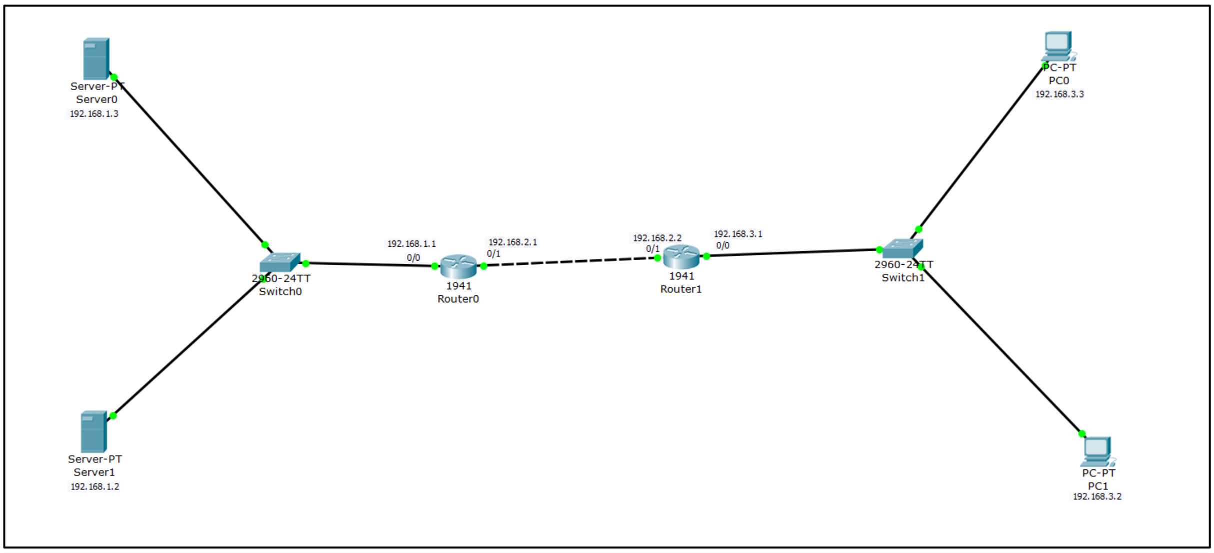
ROLL NO: B20222507

COLLEGE: SASMIRA'S INSTITUTE OF COMMERCE & SCIENCE

YEAR: 2025

Sr. No	Practical Name	Date of Performance	Date of Submission	Grade
1	**Configure Routers** a) OSPF MD5 authentication. b) NTP. c) to log messages to the syslog server. d) to support SSH connections.			
2	**Configure AAA Authentication** a) Configure a local user account on Router and configure authenticate on the console and vty lines using local AAA b) Verify local AAA authentication from the Router console and the PC-A client			
3	**Configuring Extended ACLs** a) Configure, Apply and Verify an Extended Numbered ACL			
4	**Configure IP ACLs to Mitigate Attacks and IPV6 ACLs** a) Verify connectivity among devices before firewall configuration. b) Use ACLs to ensure remote access to the routers is available only from management station PC-C. c) Configure ACLs on to mitigate attacks. d) Configuring IPv6 ACLs			
5	**Configuring a Zone-Based Policy Firewall**			
6	**Configure IOS Intrusion Prevention System (IPS) Using the CLI** a) Enable IOS IPS. b) Modify an IPS signature.			
7	**Layer 2 Security** a) Assign the Central switch as the root bridge. b) Secure spanning-tree parameters to prevent STP manipulation attacks. c) Enable port security to prevent CAM table overflow attacks.			
8	**Layer 2 VLAN Security**			
9	**Configure and Verify a Site-to-Site IPsec VPN Using CLI**			
10	**Configuring ASA Basic Settings and Firewall Using CLI** a) Configure basic ASA settings and interface security levels using CLI b) Configure routing, address translation, and inspection policy using CLI c) Configure DHCP, AAA, and SSH d) Configure a DMZ, Static NAT, and ACLs			

PRACTICAL 1: CONFIGURE ROUTERS



Connect the server to switch with [copper straight through wire]

Server (Fastethernet) to switch0 (any ethernet connections 0/1 to 0/20)

Repeat the same for all connections of server and pc

Connect switch0 to router 0 using [copper straight through wire] (gigabitethernet 0/0)

Connect switch1 to router 1[copper straight through wire] (gigabitethernet 0/0)

Connect routers using [copper cross -over wire] (gigabitEthernet 0/1]

Step 1: server 0 > desktop > IP configuration:

IP address: (192.168.1.3) > enter >

subnet mask (will get by default) >

default gateway: (192.168.1.1)

close

Step 2: server 1 > desktop > IP configuration:

IP address: (192.168.1.2) > enter >

subnet mask (will get by default) >

default gateway: (192.168.1.1)

close

Step 3: PC 0 > desktop > IP configuration:

IP address: (192.168.3.3) > enter >

subnet mask (will get by default) >

default gateway: (192.168.3.1)

close

Step 4: PC 1 > desktop > IP configuration:

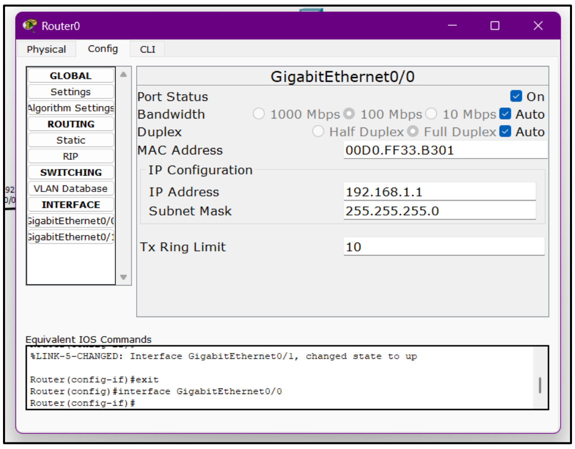
IP address: (192.168.3.2) > enter >

subnet mask (will get by default) >

default gateway: (192.168.3.1)

close

step 5: Router 0 > config > interface > gigabitEthernet 0/0 & gigabitEthernet 0/1

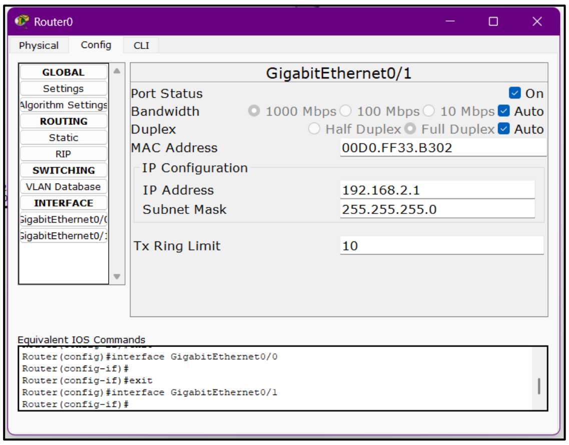


GigabitEthernet0/0

Port Status ☑ On
Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address 00D0.FF33.B301
IP Configuration
IP Address 192.168.1.1
Subnet Mask 255.255.255.0
Tx Ring Limit 10

Equivalent IOS Commands

```
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
```



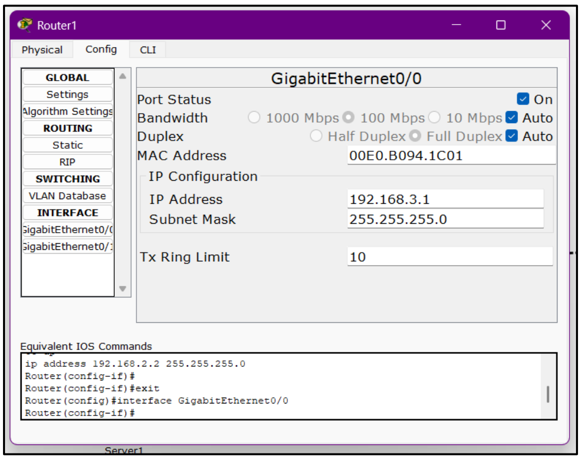
GigabitEthernet0/1

Port Status ☑ On
Bandwidth ○ 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ○ Full Duplex ☑ Auto
MAC Address 00D0.FF33.B302
IP Configuration
IP Address 192.168.2.1
Subnet Mask 255.255.255.0
Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
```

Step 6: Router 1 > config > interface > gigabitEthernet 0/0 & gigabitEthernet 0/1

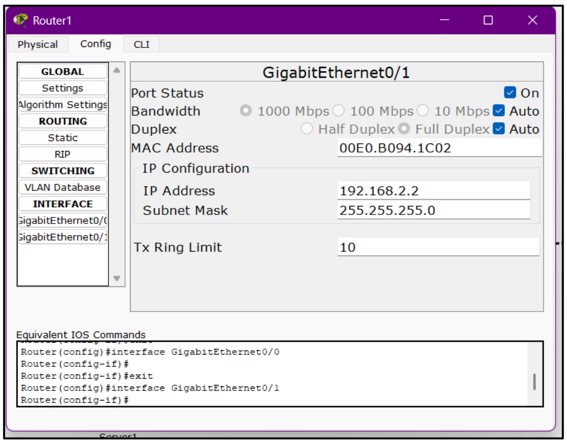


GigabitEthernet0/0

Port Status ☑ On
Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address 00E0.B094.1C01
IP Configuration
IP Address 192.168.3.1
Subnet Mask 255.255.255.0
Tx Ring Limit 10

Equivalent IOS Commands

```
ip address 192.168.2.2 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
```



GigabitEthernet0/1

Port Status ☑ On
Bandwidth ○ 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ○ Full Duplex ☑ Auto
MAC Address 00E0.B094.1C02
IP Configuration
IP Address 192.168.2.2
Subnet Mask 255.255.255.0
Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
```

Step 7: Configure Command for ospf for router 0

Router 0> CLI

Type the following commands:

Router> enable

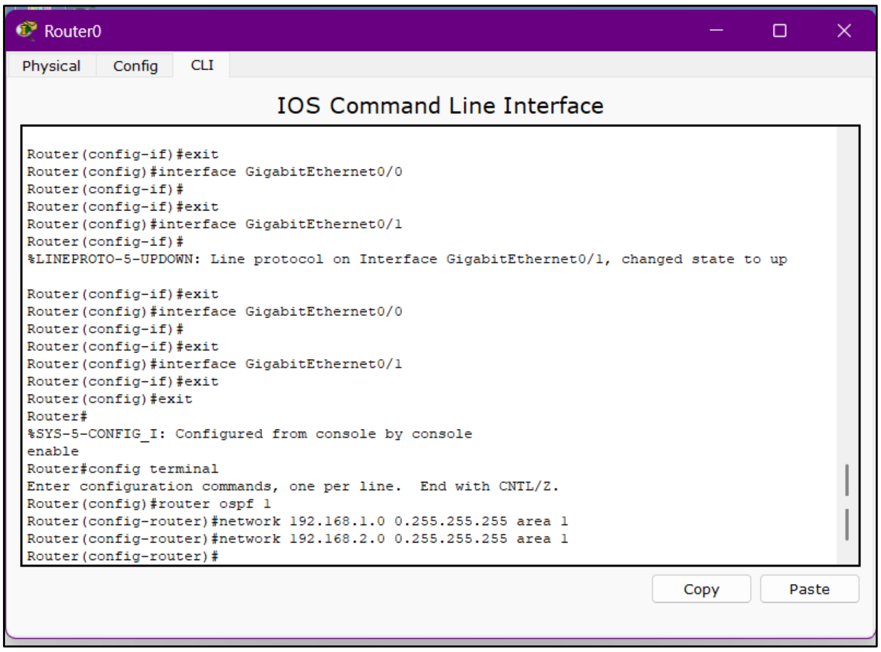
Router# config terminal

Router(config)# router ospf 1

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

Router(config-router)# Network 192.168.2.0 0.255.255.255 area 1

>Close the command prompt



```
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.255.255.255 area 1
Router(config-router)#network 192.168.2.0 0.255.255.255 area 1
Router(config-router)#
```

Step 8: Configure Command for ospf for router 1

Router 1> CLI

Type the following commands:

Router> enable

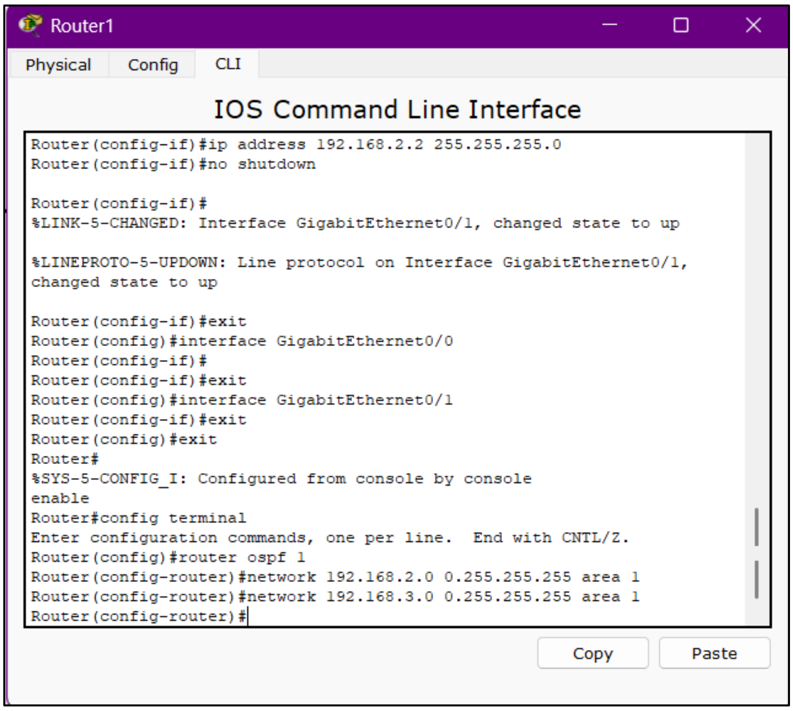
Router# config terminal

Router(config)# router ospf 1

Router(config-router)# Network 192.168.2.0 0.255.255.255 area 1

Router(config-router)# Network 192.168.3.0 0.255.255.255 area 1

>Close the command prompt



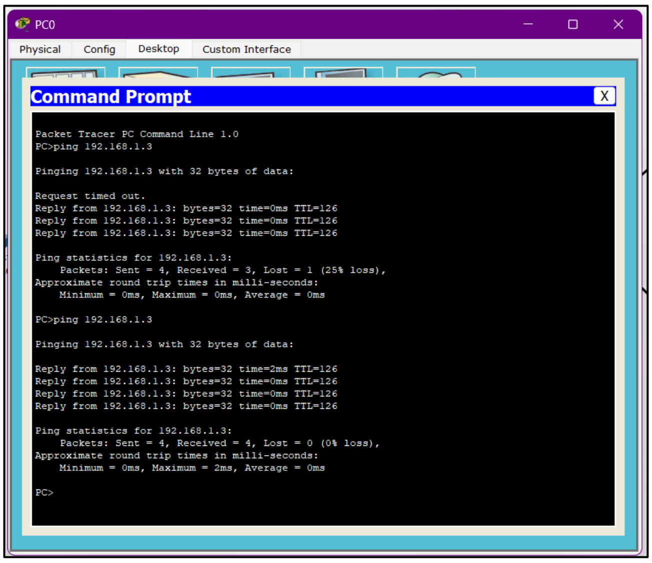
```
Router(config-if)#ip address 192.168.2.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.2.0 0.255.255.255 area 1
Router(config-router)#network 192.168.3.0 0.255.255.255 area 1
Router(config-router)#
```

Step 9: open PC 0 > desktop > command prompt

Type the command:

Ping 192.168.1.3 > enter

Type the command again:



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time=0ms TTL=126
Reply from 192.168.1.3: bytes=32 time=0ms TTL=126
Reply from 192.168.1.3: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=2ms TTL=126
Reply from 192.168.1.3: bytes=32 time=0ms TTL=126
Reply from 192.168.1.3: bytes=32 time=0ms TTL=126
Reply from 192.168.1.3: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

PC>
```

a) Configure md5 message digest for both routers:

Step 1: router 0 > CLI

Type the following commands:

Router> enable

Router# config terminal

Router(config)# interface gigabitEthernet 0/1

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

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

Router(config-if)# exit

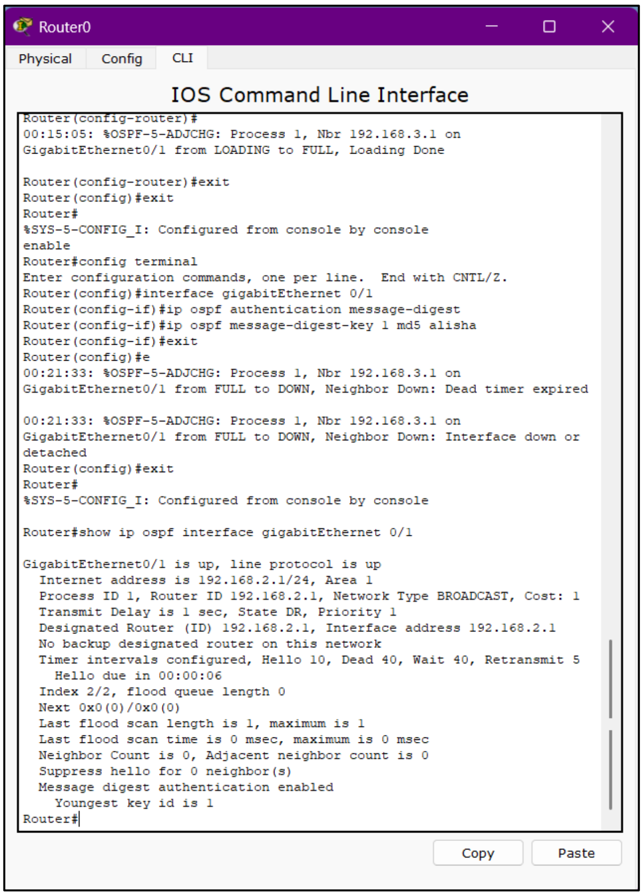
Router (config)# exit

[checking whether the message digest is enables]

Type command:

enable

Router# show ip ospf interface gigabitEthernet 0/1

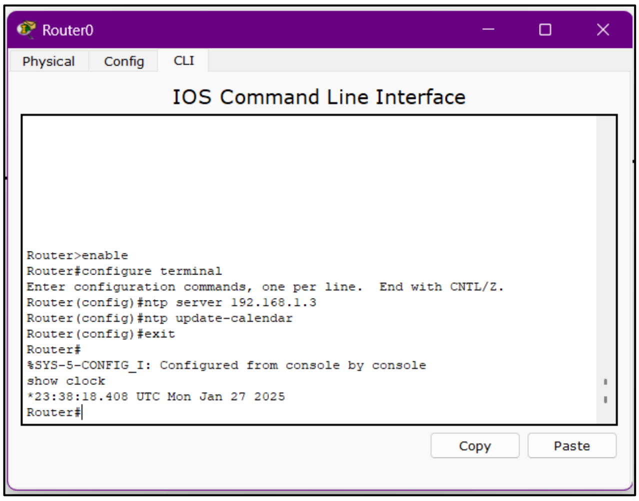


```
Router(config-router)#
00:15:05: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on
GigabitEthernet0/1 from LOADING to FULL, Loading Done

Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 alisha
Router(config-if)#exit
Router(config)#e
00:21:33: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on
GigabitEthernet0/1 from FULL to DOWN, Neighbor Down: Dead timer expired

00:21:33: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on
GigabitEthernet0/1 from FULL to DOWN, Neighbor Down: Interface down or
detached
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip ospf interface gigabitEthernet 0/1

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 DR, Priority 1
  Designated Router (ID) 192.168.2.1, Interface address 192.168.2.1
  No backup designated router on this network
  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 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
Router#
```

b) Config command for NTP update-calendar: both routers 0 and 1:

CLI> type the following command

- enable
- configure terminal
- ntp server 192.168.1.3
- ntp update-calendar
- exit
- exit



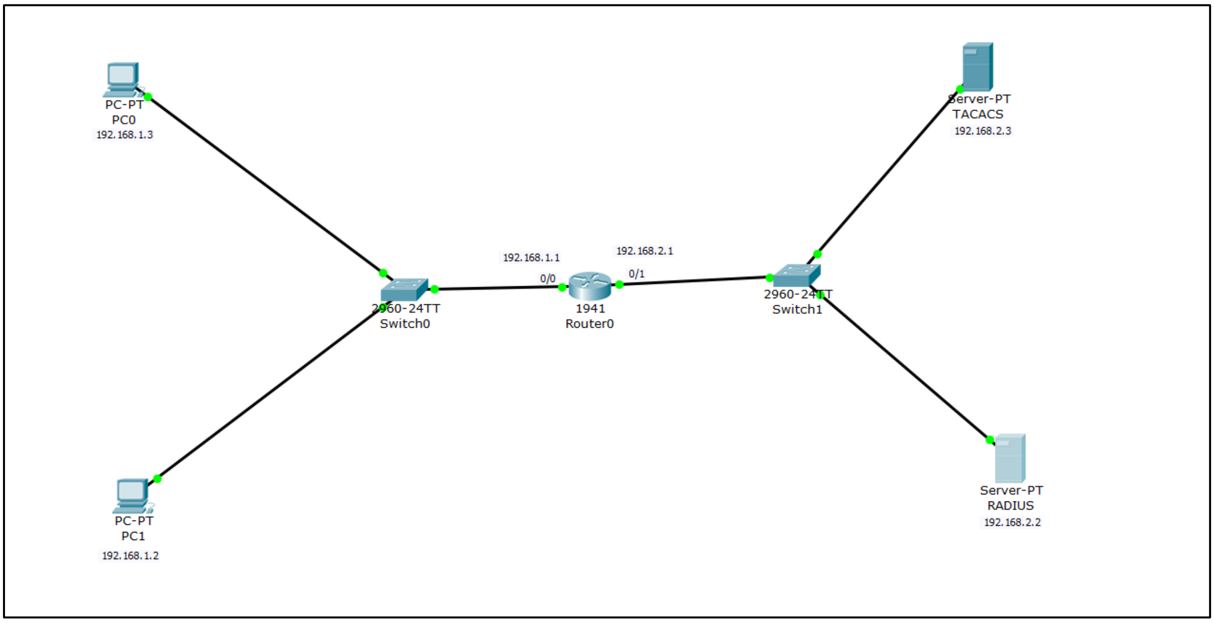
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ntp server 192.168.1.3
Router(config)#ntp update-calendar
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
show clock
*23:38:18.408 UTC Mon Jan 27 2025
Router#
```

c) **<u>config the loggong command on both routers.logging should be syslog ip 192.168.1.2. check the logging activity in syslog server:</u>**

router 0 > CLI> type the following command:

- enable
- configure terminal
- logging 192.168.1.2
- exit
- exit

PRACTICAL 2: CONFIGURE AAA AUTHENTICATION



Connect the server to switch with [copper straight through wire]

Server (Fastethernet) to switch0 (any ethernet connections 0/1 to 0/20)

Repeat the same for all connections of server and pc

Connect switch0 to router 0 using [copper straight through wire] (gigabitethernet 0/0)

Connect switch1 to router 0[copper straight through wire] (gigabitethernet 0/1)

Step 1: TACACS > desktop > IP configuration:

IP address: (192.168.2.3) > enter >

subnet mask (will get by default) >

default gateway: (192.168.2.1)

close

Step 2: RADIUS > desktop > IP configuration:

IP address: (192.168.2.2) > enter >

subnet mask (will get by default) >

default gateway: (192.168.2.1)

close

Step 3: PC 0 > desktop > IP configuration:

IP address: (192.168.1.3) > enter >

subnet mask (will get by default) >

default gateway: (192.168.1.1)

close

Step 4: PC 1 > desktop > IP configuration:

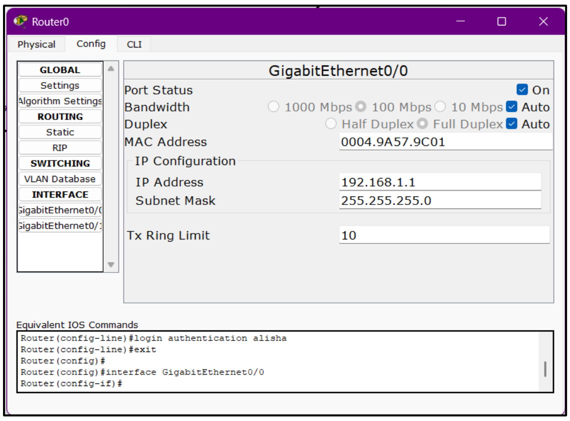
IP address: (192.168.1.2) > enter >

subnet mask (will get by default) >

default gateway: (192.168.1.1)

close

Step 5: Router 0 > config > interface > gigabitEthernet 0/0 & gigabitEthernet 0/1



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0004.9A57.9C01

IP Configuration

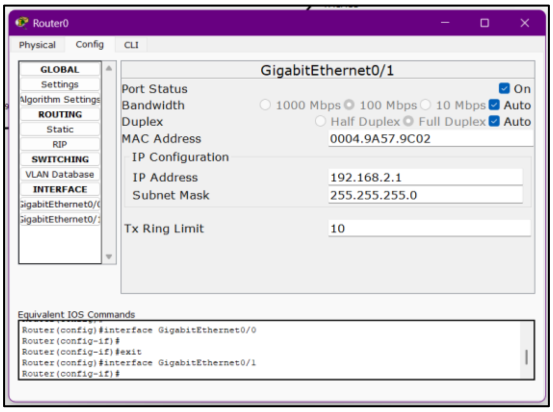
IP Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-line)#login authentication alisha
Router(config-line)#exit
Router(config)#
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
```



GigabitEthernet0/1

Port Status ☑ On

Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0004.9A57.9C02

IP Configuration

IP Address 192.168.2.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
```

a) **Configure a local user account on Router and configure authenticate on the console and vty lines using local AAA**

Step 6: TACACS > service > AAA > on

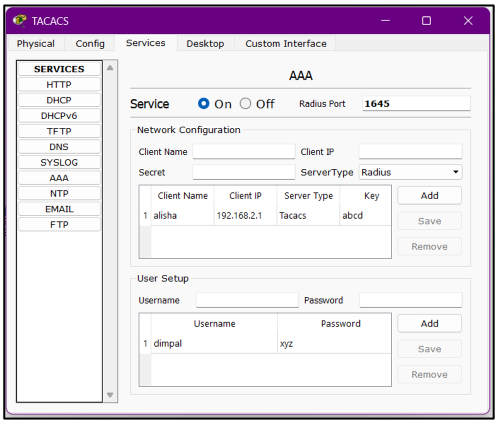
Client name: alisha client ip: 192.168.2.1

Secret: abcd server type : tacacs

Add

>username : dimpal password: xyz

Add



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name Client IP

Secret ServerType Radius

	Client Name	Client IP	Server Type	Key
1	alisha	192.168.2.1	Tacacs	abcd

User Setup

Username Password

	Username	Password
1	dimpal	xyz

Step 7: RADIUS > service > AAA > on

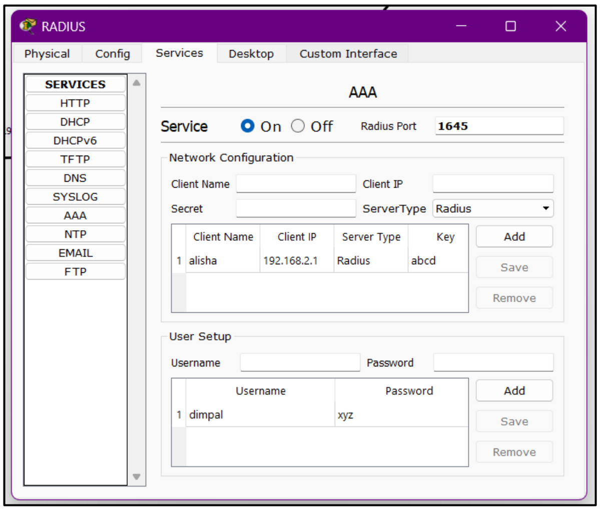
Client name: alisha client ip: 192.168.2.1

Secret: abcd server type : tacacs

Add

>username : dimpal password: xyz

Add



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name Client IP

Secret ServerType Radius

	Client Name	Client IP	Server Type	Key
1	alisha	192.168.2.1	Radius	abcd

User Setup

Username Password

	Username	Password
1	dimpal	xyz

Step 8: router 0 > CLI >

Type following command:

- enable
- configure terminal
- aaa new-model
- tacacs-server host 192.168.2.3 key abcd
- radius-server host 192.168.2.2 key abcd
- aaa authentication login alisha group tacacs+ group radius local
- line vty 0 4
- login authentication alisha
- exit

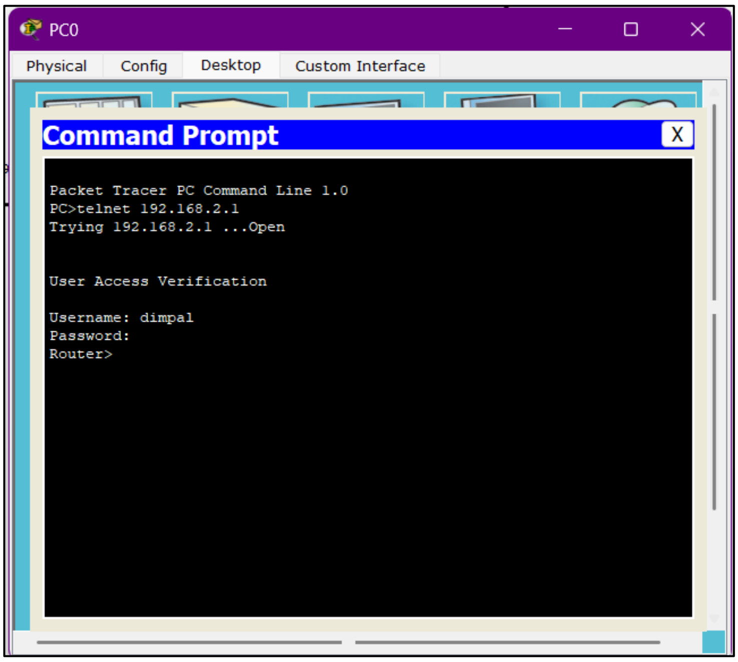
Step 9: PC 0 > desktop > command prompt >

Type the command:

telnet 192.168.2.1

username: dimpal

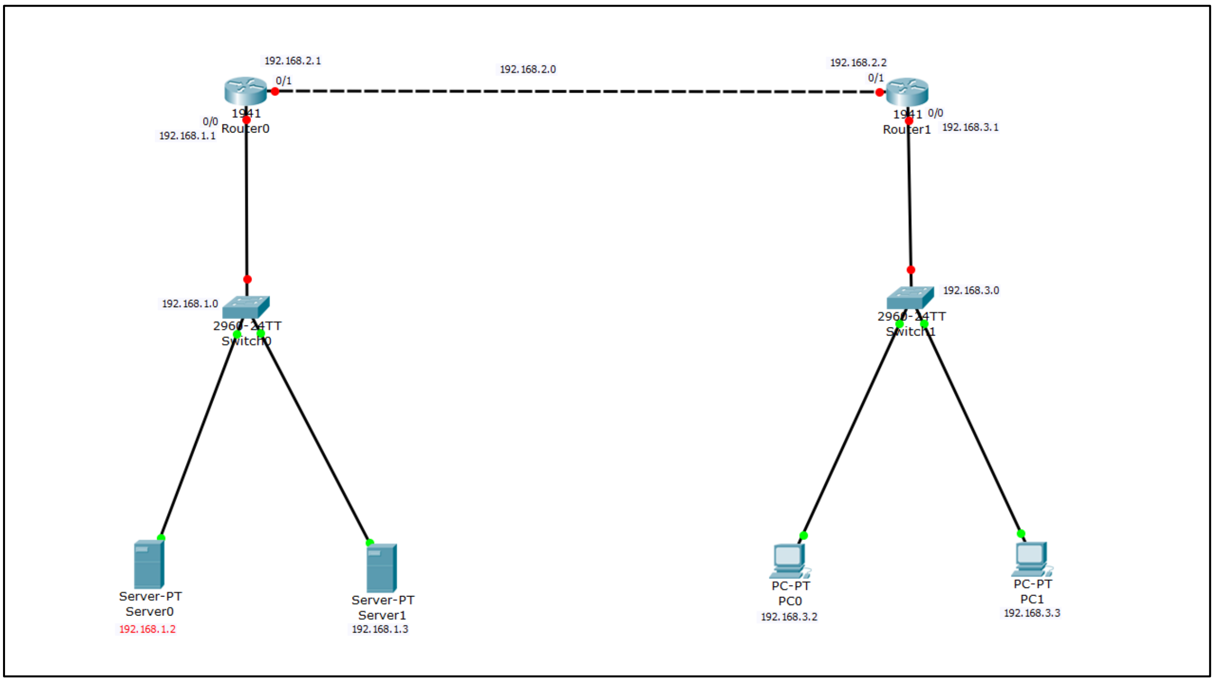
password: xyz [note: the password cannot be seen while typing on cmd]



```
Packet Tracer PC Command Line 1.0
PC>telnet 192.168.2.1
Trying 192.168.2.1 ...Open


User Access Verification

Username: dimpal
Password:
Router>
```

PRACTICAL 3: CONFIGURING EXTENDED ACLs

a) Configure, Apply and verify an Extended Numbered ACL



Connect the server to switch with [copper straight through wire]

Server (Fastethernet) to switch0 (any ethernet connections 0/1 to 0/20)

Repeat the same for all connections of server and pc

Connect switch0 to router 0 using [copper straight through wire] (gigabitethernet 0/0)

Connect switch1 to router 1[copper straight through wire] (gigabitethernet 0/0)

Connect routers using [copper cross -over wire] (gigabitEthernet 0/1]

Step 1: server 0 > desktop > IP configuration:

IP address: (192.168.1.2) > enter >

subnet mask (will get by default) >

default gateway: (192.168.1.1)

close

Step 2: server 1 > desktop > IP configuration:

IP address: (192.168.1.3) > enter >

subnet mask (will get by default) >

default gateway: (192.168.1.1)

close

<u>Step 3</u>: PC 0 > desktop > IP configuration:

IP address: (192.168.3.2) > enter >

subnet mask (will get by default) >

default gateway: (192.168.3.1)

close

<u>Step 4</u>: PC 1 > desktop > IP configuration:

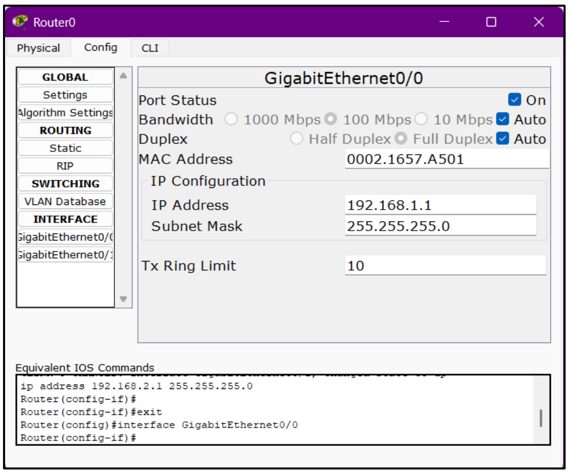
IP address: (192.168.3.3) > enter >

subnet mask (will get by default) >

default gateway: (192.168.3.1)

close

<u>step 5</u>: Router 0 > config > interface > gigabitEthernet 0/0 & gigabitEthernet 0/1



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0002.1657.A501

IP Configuration

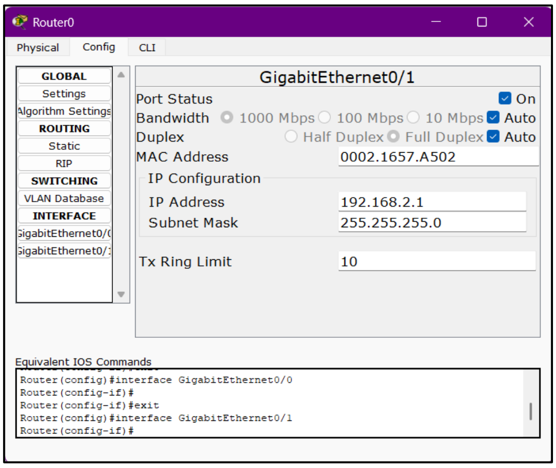
IP Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
ip address 192.168.2.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
```



GigabitEthernet0/1

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0002.1657.A502

IP Configuration

IP Address 192.168.2.1

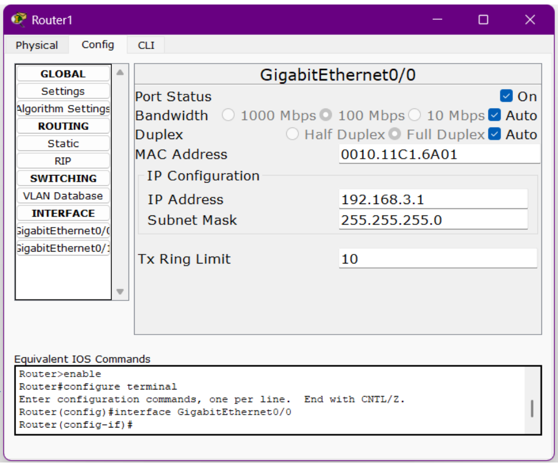
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
```

<u>step 6</u>: Router 1 > config > interface > gigabitEthernet 0/0 & gigabitEthernet 0/1



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0010.11C1.6A01

IP Configuration

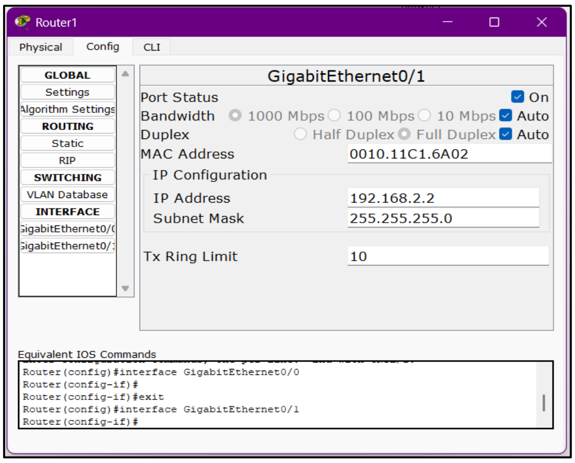
IP Address 192.168.3.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
```



GigabitEthernet0/1

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0010.11C1.6A02

IP Configuration

IP Address 192.168.2.2

Subnet Mask 255.255.255.0

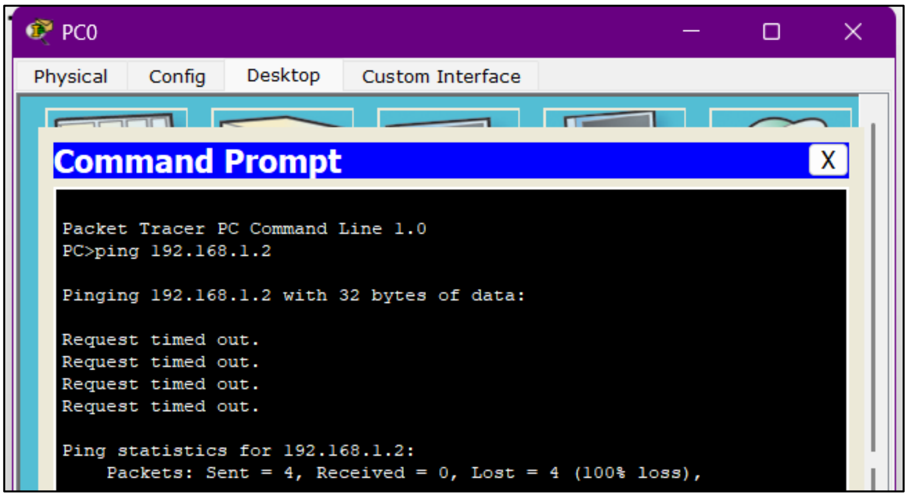
Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
```

step 7: pc 0 > command prompt > (type) ping 192.168.1.2

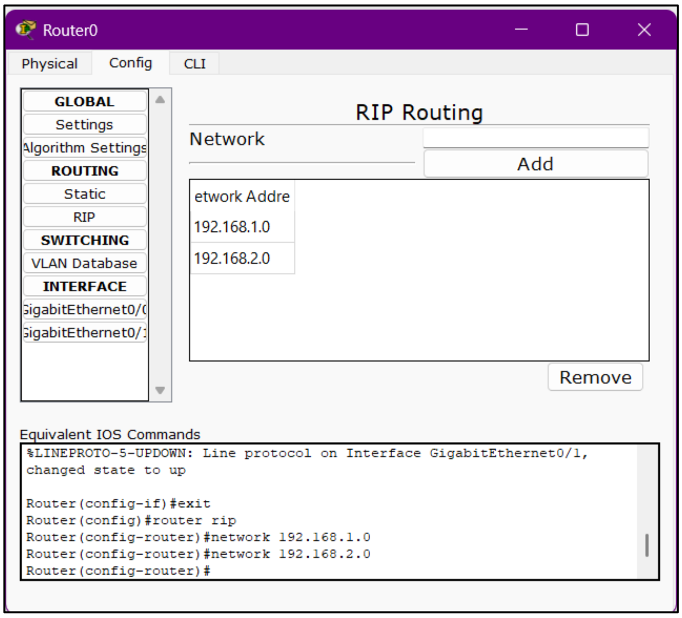
(ping from one network to other. Ping is unsuccessful)



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

{need to configure the router with some protocol (RIP) (i.e informing router which network it is connected) }

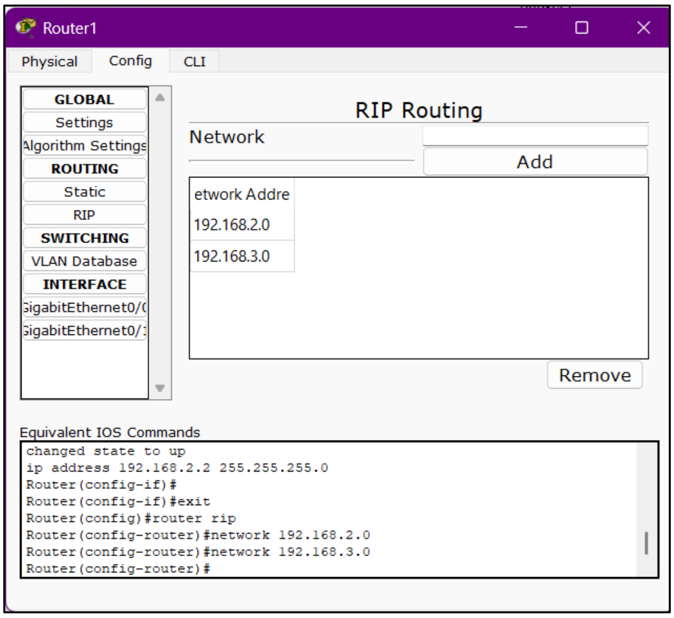
step 8: Router 0 > config > RIP > add two networks 192.168.1.0 and 192.168.2.0



etwork Addre
192.168.1.0
192.168.2.0

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
Router(config-router)#
```

step 9: Router 1 > config > RIP > add two networks 192.168.2.0 and 192.168.3.0



RIP Routing

Network

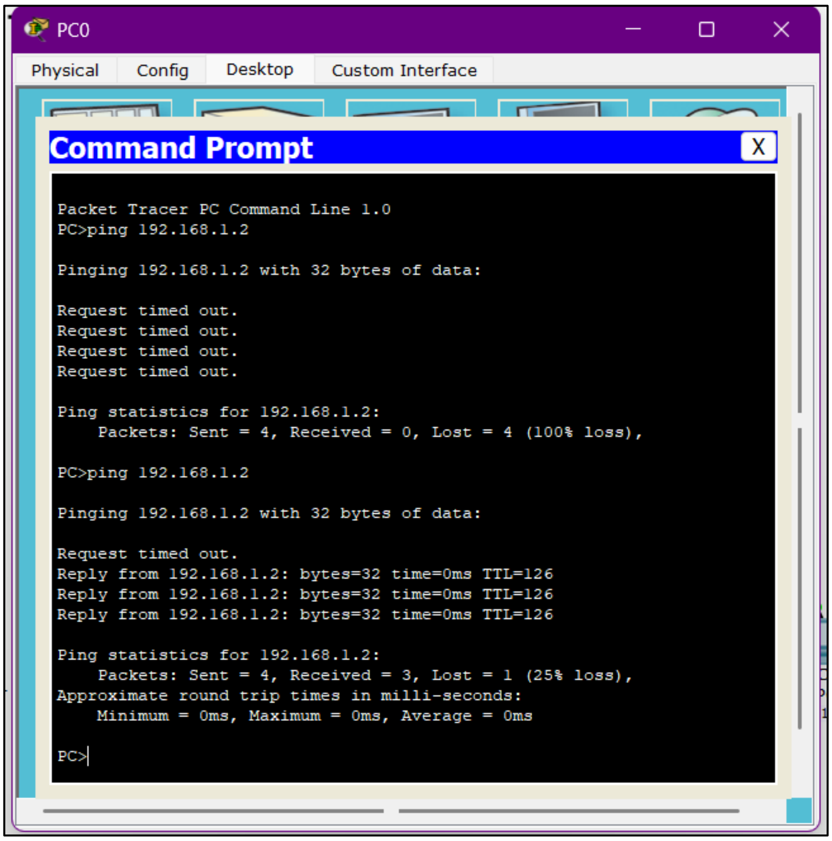
etwork Addre
192.168.2.0
192.168.3.0

Equivalent IOS Commands

```
changed state to up
ip address 192.168.2.2 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.3.0
Router(config-router)#
```

step 10: pc 0 > command prompt > (type command again) ping 192.168.1.2

(Ping from one network to other. Ping is successful)



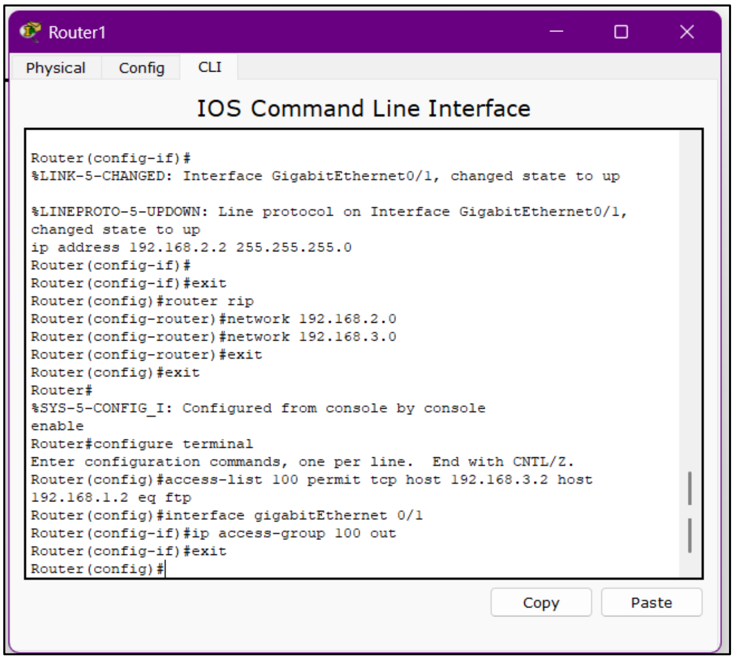
```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```

Configure access control list router 1- (eg: pc 0 have access to FTP service of server 0 but pc1 does not have access to FTP service of server 1)

Check whether the FTP service is ON on server1 along with username and password (by default it is – cisco (username & password)

step 11: Router 1 > CLI > type the commands:

- enable
- configure terminal
- access-list 100 permit tcp host 192.168.3.2 host 192.168.1.2 eq ftp
  (Note: the fir host is the PC which will have access to ftp service and the second host is the server providing ftp service)
- ip access-group 100 out (command to apply policy)
- exit

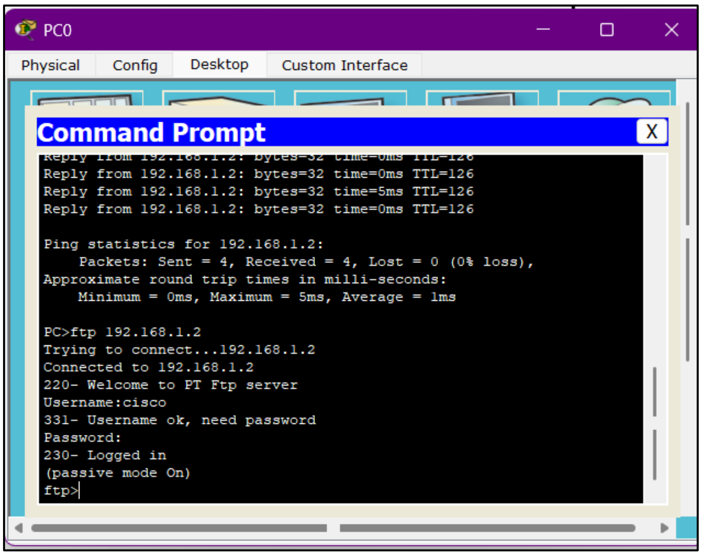


```
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
ip address 192.168.2.2 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.3.0
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit tcp host 192.168.3.2 host
192.168.1.2 eq ftp
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip access-group 100 out
Router(config-if)#exit
Router(config)#
```

step 12: PC 0 > command prompt > (type) ftp 192.168.1.2 (this is the server0 IP where the FTP service is ON)

enter the username Password (by default- cisco)

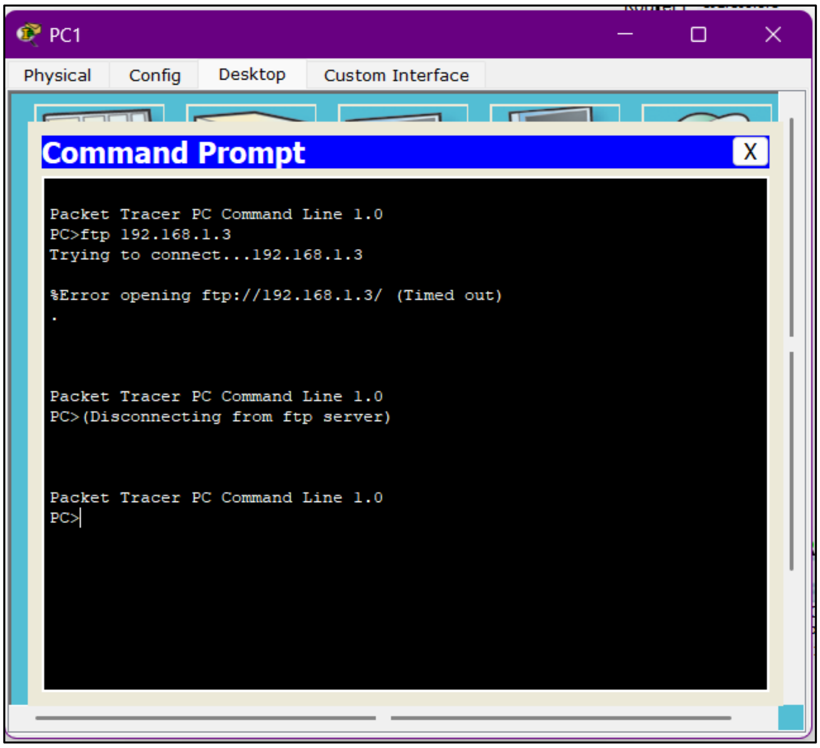
FTP service is accessible from PC0



```
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=5ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 1ms

PC>ftp 192.168.1.2
Trying to connect...192.168.1.2
Connected to 192.168.1.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

<u>Step 13</u>: try with pc 1: ftp 192.168.1.2

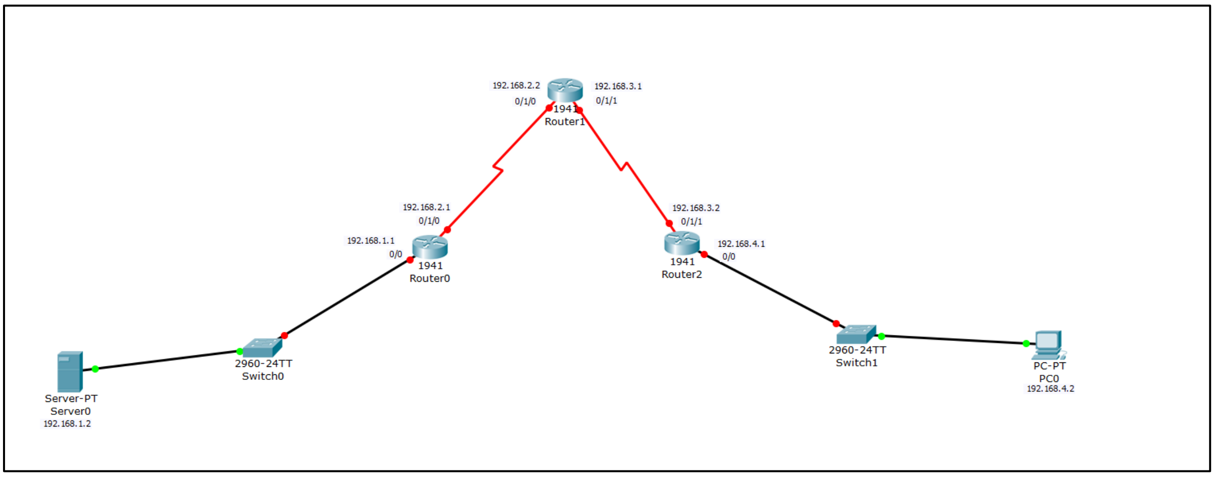
It doesn't connect



```
Packet Tracer PC Command Line 1.0
PC>ftp 192.168.1.3
Trying to connect...192.168.1.3

%Error opening ftp://192.168.1.3/ (Timed out)
.


Packet Tracer PC Command Line 1.0
PC>(Disconnecting from ftp server)


Packet Tracer PC Command Line 1.0
PC>
```

PRACTICAL 4:

CONFIGURE IP ACLs TO MITIGATE ATTACKS AND IPV6 ACLs



a) Connect the server to switch with [copper straight through wire]
Server (Fastethernet) to switch0 (any ethernet connections 0/1 to 0/20)
Switch 0 (any ethernet connections 0/1 to 0/20) to R0 (gigbitEthernet 0/0)
Repeat the same for other side connections of pc, switch, and router.

b) To connect routers with red serial interface:
Step1: goto router 0> physical tab> zoom in> turn off the switch> drag the serial interface module “HWIC-2T” to the model > turn on the switch> zoom out
Step2: repeat the same with all routers (R0, R1, and R2)
Step3: connect the routers with serial wire (red one without timer):
R0 serial 0/1/0 to R1 serial 0/1/0
R1 serial 0/1/1 to R2 serial 0/1/1

Step 1: server 0 > desktop > IP configuration:

IP address: (192.168.1.2) > enter >

subnet mask (will get by default) >

default gateway: (192.168.1.1)

close

Step 2: PC 0 > desktop > IP configuration:

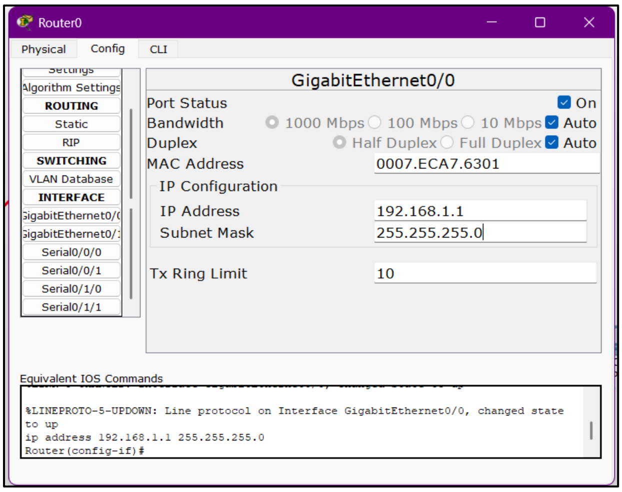
IP address: (192.168.4.2) > enter >

subnet mask (will get by default) >

default gateway: (192.168.4.1)

close

Step 3: router 0 > config > interface > gigabitEthernet 0/0 & serial 0/1/0



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ○ 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address 0007.ECA7.6301

IP Configuration

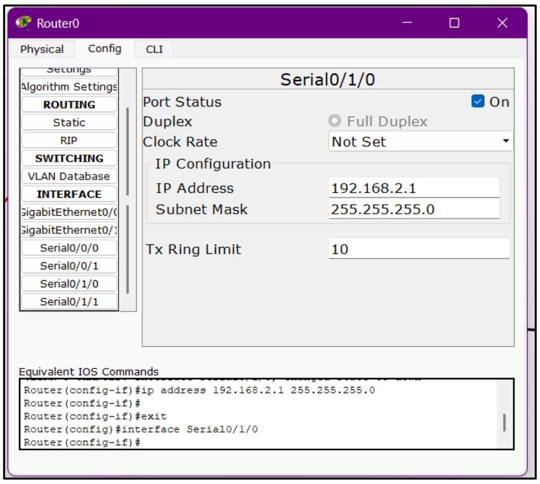
IP Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up
ip address 192.168.1.1 255.255.255.0
Router(config-if)#
```



Serial0/1/0

Port Status ☑ On

Duplex ○ Full Duplex

Clock Rate Not Set

IP Configuration

IP Address 192.168.2.1

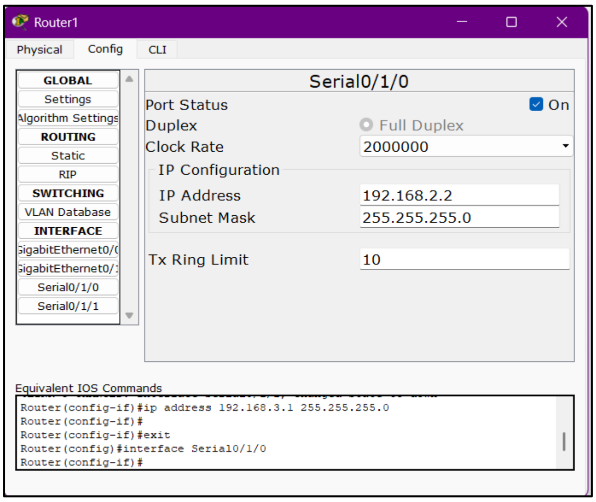
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#
```

Step 4: router 1 > config > interface > serial 0/1/0 & serial 0/1/1



Serial0/1/0

Port Status ☑ On

Duplex ○ Full Duplex

Clock Rate 2000000

IP Configuration

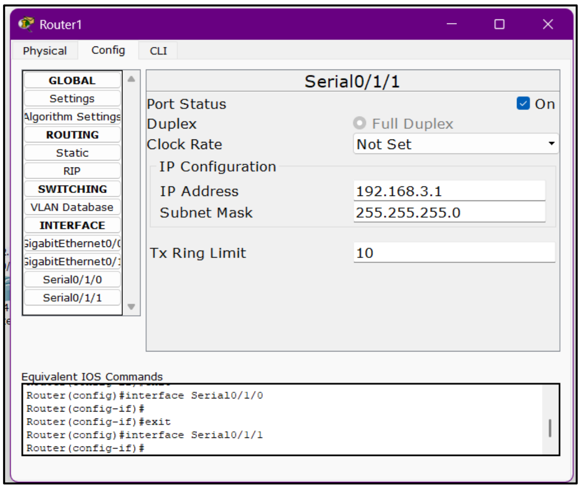
IP Address 192.168.2.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#
```



Serial0/1/1

Port Status ☑ On

Duplex ○ Full Duplex

Clock Rate Not Set

IP Configuration

IP Address 192.168.3.1

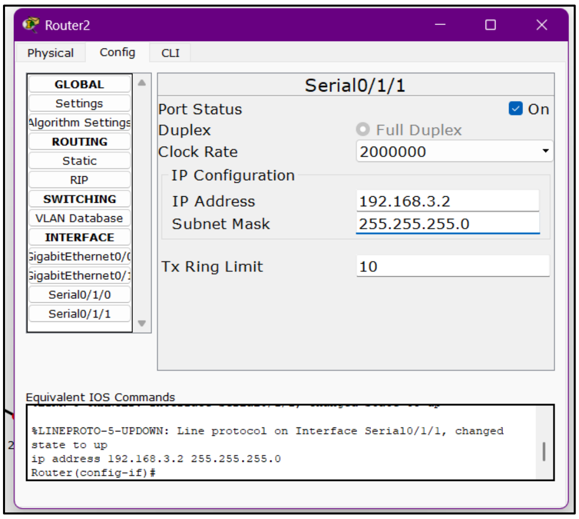
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/1
Router(config-if)#
```

Step 5: router 2 > config > interface > serial 0/1/1 & gigabitEthernet 0/0



Serial0/1/1

Port Status ☑ On

Duplex ○ Full Duplex

Clock Rate 2000000

IP Configuration

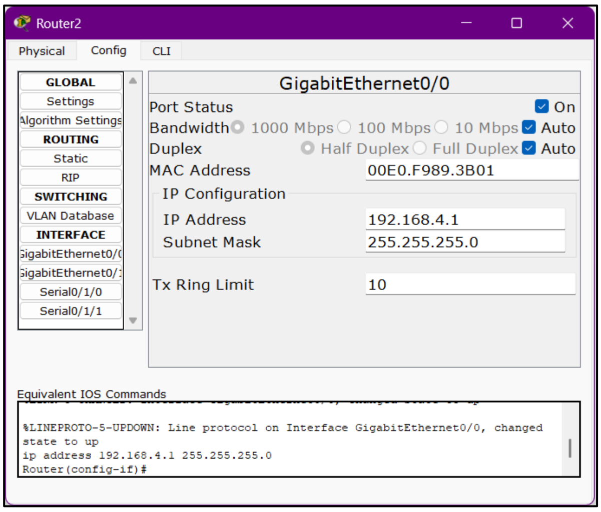
IP Address 192.168.3.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed
state to up
ip address 192.168.3.2 255.255.255.0
Router(config-if)#
```



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ○ 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address 00E0.F989.3B01

IP Configuration

IP Address 192.168.4.1

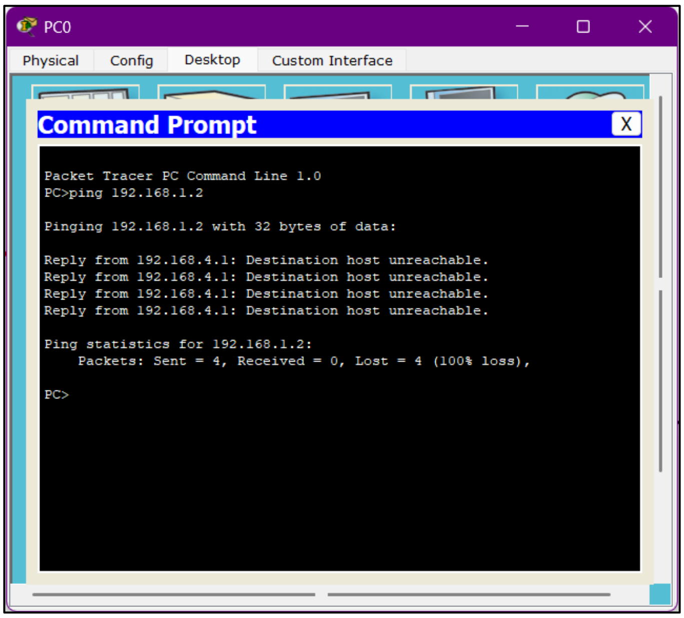
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up
ip address 192.168.4.1 255.255.255.0
Router(config-if)#
```

Step 6: PC 0> command prompt> ping 192.168.1.2 (ping pc to server 1. Ping is unsuccessful)

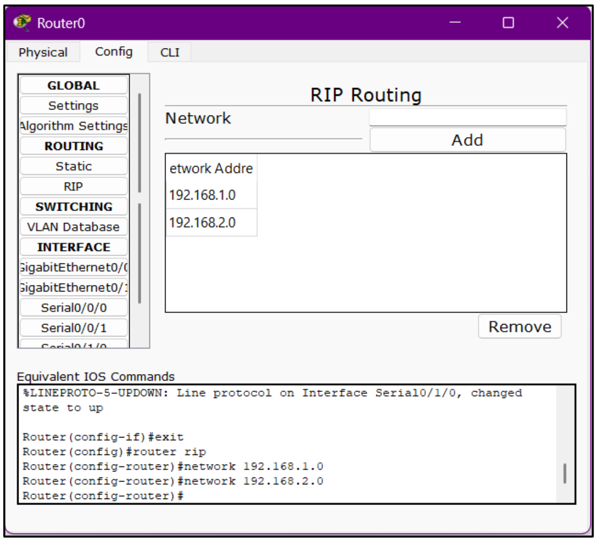


```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

whenever we have 2 or more routers we need to configure the path using some protocol:-

Configure RIP for all routers (R0, R1 & R2)

Step 7: router 0> RIP > add two networks 192.168.1.0 and 192.168.2.0

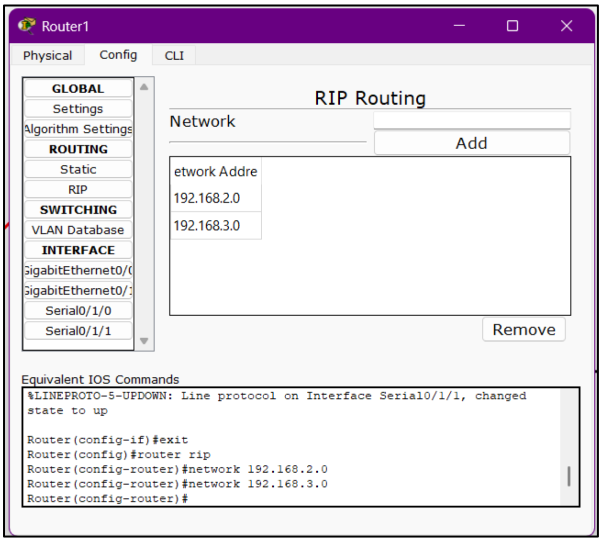


etwork Addre
192.168.1.0
192.168.2.0

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed
state to up

Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
Router(config-router)#
```

Step 8: router 1 > RIP > add two networks 192.168.2.0 and 192.168.3.0

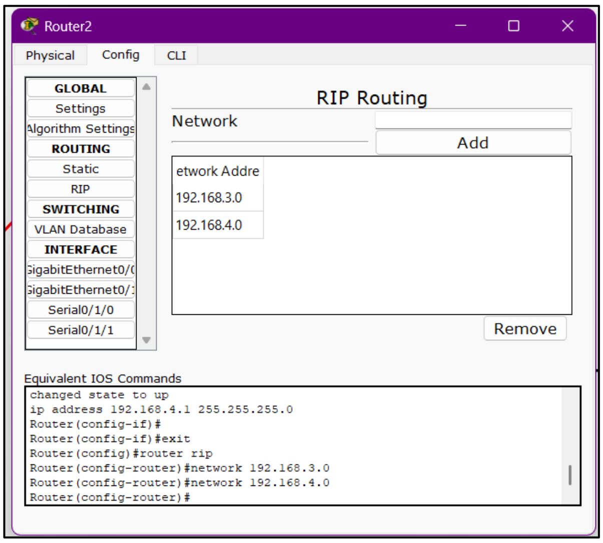


etwork Addre
192.168.2.0
192.168.3.0

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed
state to up

Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.3.0
Router(config-router)#
```

Step 9: router 2> RIP > add two networks 192.168.3.0 and 192.168.4.0

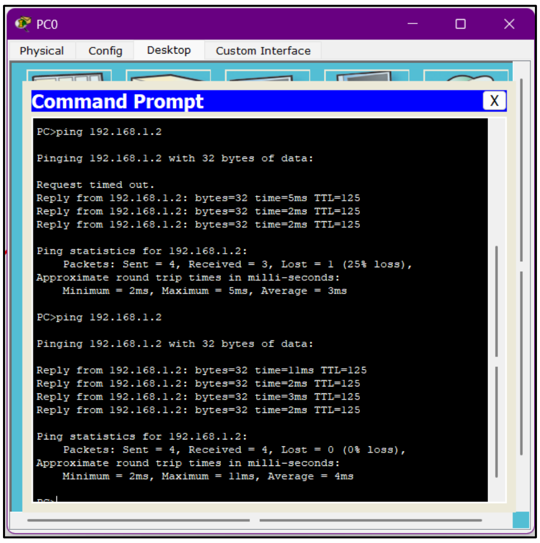


etwork Addre
192.168.3.0
192.168.4.0

Equivalent IOS Commands

```
changed state to up
ip address 192.168.4.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.3.0
Router(config-router)#network 192.168.4.0
Router(config-router)#
```

Step 10: PC 0> command prompt> ping 192.168.1.2 (ping pc to server 1. Ping is successful)



```
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=5ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 5ms, Average = 3ms

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=11ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=3ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 11ms, Average = 4ms

PC>
```

Configure routers for ACL (Access Control List).

Step 11: repeat the command for all routers (R0, R1, & R2) in CLI

- enable
- configure terminal
- ip domain-name sics.com
- hostname S0
- crypto key generate rsa
- yes
- 512
- line vty 0 4
- transport input ssh
- login local
- exit
- username admin privilege 15 password xyz
- exit

(Note: there are 16 levels, 0-15 by default, privilege level 1 users can issue all commands, while a privilege level 1 user can issue most show commands)

Create the ACL on all routers (R0, R1, & R2). We want to allow the command from PC to all routers and disallow the comm from server through routers.

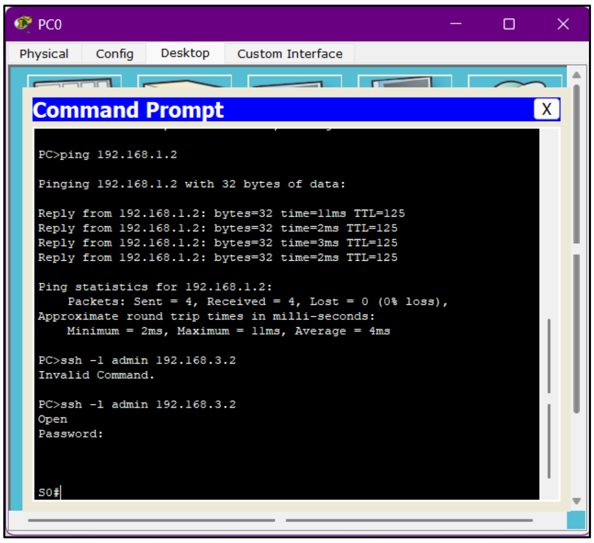
Step 12: type the same commands to all routers (R0, R1, & R2):

- enable
- configure terminal
- access-list 10 permit host 192.168.4.2 (PC IP address)
- line vty 0 4
- access-class 10 in
- exit

verify the command from pc and server

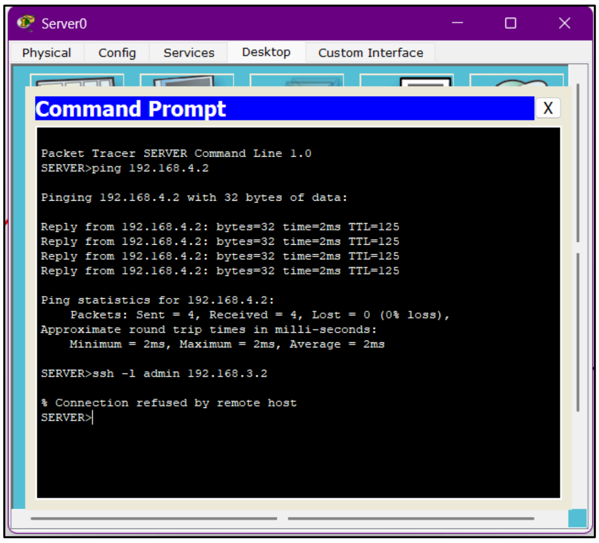
Step 13: PC 0 > command prompt > ssh -l admin 192.168.3.2

Password: xyz



```
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=11ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=3ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 11ms, Average = 4ms

PC>ssh -l admin 192.168.3.2
Invalid Command.

PC>ssh -l admin 192.168.3.2
Open
Password:



S0#
```

Step 14: server 0 > command prompt> ssh -l admin 192.168.3.2



```
Packet Tracer SERVER Command Line 1.0
SERVER>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=2ms TTL=125
Reply from 192.168.4.2: bytes=32 time=2ms TTL=125
Reply from 192.168.4.2: bytes=32 time=2ms TTL=125
Reply from 192.168.4.2: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

SERVER>ssh -l admin 192.168.3.2

% Connection refused by remote host
SERVER>
```

Practical 5: Configuring a Zone-Based Policy Firewall (ZPF)

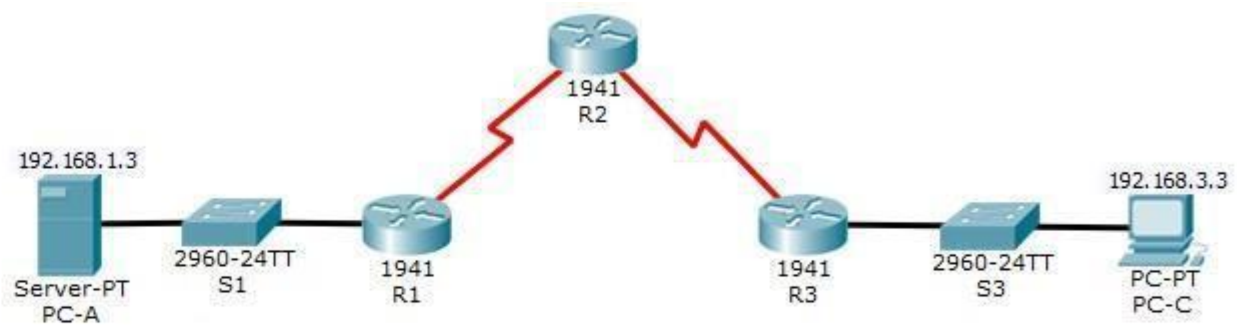
1) **Prior Concepts:**
   a. AAA Authentication
   b. MD5 Authentication and Hash
   c. Telnet
   d. SSH
   e. RADIUS and TACACS + Server
2) **New Concepts:**
   ZPFs are the latest development in the evolution of Cisco firewall technologies. In this activity, you will configure a basic ZPF on an edge router R3 that allows internal hosts access to external resources and blocks external hosts from accessing internal resources. You will then verify firewall functionality from internal and external hosts. If user access verification, password is asked in the router while writing command then Password: ciscoconpa55.If just password is asked in the router while writing command then Password: ciscoenpa55.For SSH username: Admin Password: Adminpa55

3) **Objectives:**

a. Verify connectivity among devices before firewall configuration.
b. Configure a zone-based policy (ZPF) firewall on R3.
c. Verify ZPF firewall functionality using ping, SSH, and a web browser.

4) **Procedure:**
   a. Verify Basic Network Connectivity
   b. Create the Firewall Zones on R3
   c. Identify Traffic Using a Class-Map
   d. Specify Firewall Policies
   e. Apply Firewall Policies
   f. Test Firewall Functionality from IN-ZONE to OUT-ZONE
   g. Test Firewall Functionality from OUT-ZONE to IN-ZONE

5) **Implementation :**
   a. Done by students in the lab.
6) **Results:**
   a. O/P of the program
7) **Application:**
   a. Real life application in network designing
8) **Questions:**



Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
R3	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Part 1: Verify Basic Network Connectivity-Verify network connectivity prior to configuring the zone-based

policy firewall.

```
R1(config)#router rip

R1(config-router)#network 192.168.1.0

R1(config-router)#network 10.1.1.0

R1(config-router)#network 10.2.2.0

R1(config-router)#network 192.168.3.0

R1(config-router)#exit

R1(config)#
```

R2(config)#router rip

R2(config-router)#network 192.168.1.0

R2(config-router)#network 10.1.1.0

R2(config-router)#network 10.2.2.0

R2(config-router)#network 192.168.3.0

R2(config-router)#exit

R2(config)#

R3(config)#router rip

R3(config-router)#network 192.168.1.0

R3(config-router)#network 10.1.1.0

R3(config-router)#network 10.2.2.0

R3(config-router)#network 192.168.3.0

R3(config-router)#exit

R3(config)#

Step 1: From the PC-A –ping 192.168.1.3, Ping 192.168.1.1, ping 10.1.1.1, ping 10.1.1.2, ping 10.2.2.2, ping

10.2.2.1, ping 192.168.3.1, ping 192.168.3.3 (all should be successful).From PC-C –ping 192.168.1.3, Ping

192.168.1.1, ping 10.1.1.1, ping 10.1.1.2, ping 10.2.2.2, ping 10.2.2.1, ping 192.168.3.1, ping 192.168.3.3 (all

should be successful).

Step 2: Access R2 using SSH. To configure SSH in any router:

R2(config)# ip domain-name ccnasecurity.com

R2(config)# username Admin privilege 15 secret Adminpa55

R2(config)# line vty 0 4

R2(config-line)# login local

R2(config-line)# transport input ssh

Check :Connect to Router using SSH on PC. Go to the PC-C ->desktop->command prompt, type

PC> ssh -l Admin 10.2.2.2(ip address of the router where SSH is configured). If passwords is asked then enter Adminpa55 and it is successful else connection by foreign host is closed.

Step 3: From PC-C, open a web browser to the PC-A server.

a. Click the Desktop tab and then click the Web Browser application. Enter the PC-A IP address 192.168.1.3 as the URL. The Packet Tracer welcome page from the web server should be displayed.

b.Close the browser on PC-C.

Part 2: Create the Firewall Zones on R3 Note: For all configuration tasks, be sure to use the exact names as specified.

Step 1: Enable the Security Technology package.

a. On R3, issue the show version command to view the Technology Package license information.

b. If the Security Technology package has not been enabled, use the following command to enable the package.

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

c. Accept the end-user license agreement.

d. Save the running-config and reload the router to enable the security license. for this go to

```
R3#copy run start

R3# reload

R3#
```

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

Step 2: Create an internal zone. Use the zone security command to create a zone named IN-ZONE.

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

 R3(config-sec-zone) exit
```

Step 3: Create an external zone. Use the zone security command to create a zone named OUT-ZONE.

```
R3(config-sec-zone)# zone security OUT-ZONE

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

Part 3: Identify Traffic Using a Class-Map

Step 1: Create an ACL that defines internal traffic.

Use the access-list command to create extended ACL 101 to permit all IP protocols from the 192.168.3.0/24 source network to any destination.

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

Step 2: Create a class map referencing the internal traffic AC.

```
R3(config)#class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)# match access-group 101
R3(config-cmap)# exit
```

Part 4: Specify Firewall Policies

Step 1: Create a policy map to determine what to do with matched traffic. Use the policy-map type inspect command and create a policy map named IN-2-OUT-PMAP.

```
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-pmap)# class type inspect IN-NET-CLASS-MAP
```

Step 3: Specify the action of inspect for this policy map.The use of the inspect command invokes contextbased access control (other options include pass and drop).

```
R3(config-pmap-c)# inspect
```

%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols will be inspected. Issue the exit command twice to leave config-pmap-c mode and return to config mode.

```
R3(config-pmap-c)# exit
R3(config-pmap)# exit
```

Part 5: Apply Firewall Policies

Step 1: Create a pair of zones.

Using the zone-pair security command, create a zone pair named IN-2-OUT-ZPAIR. Specify the source and destination zones that were created in Task 1.

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

Step 2: Specify the policy map for handling the traffic between the two zones-Attach a policy-map and its associated actions to the zone pair using the service-policy type inspect command and reference the policy map previously created, IN-2-OUT-PMAP.

```
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 the appropriate security zones.

Use the zone-member security command in interface configuration mode to assign G0/1 to IN-ZONE and S0/0/1 to OUT-ZONE.

```
R3(config)# interface g0/1

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

R3(config-if)# exit

R3(config)# interface s0/0/1

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

R3(config-if)# exit
```

Step 4: Copy the running configuration to the startup configuration.

Part 6: Test Firewall Functionality from IN-ZONE to OUT-ZONE

Verify that internal hosts can still access external resources after configuring the ZPF.

Step 1: From internal PC-C, ping the external PC-A server.

From the PC-C command prompt, ping PC-A at 192.168.1.3. The ping should succeed.

Step 2: From internal PC-C, SSH to the R2 S0/0/1 interface.

a. From the PC-C command prompt, SSH to R2 at 10.2.2.2. Use the username Admin and the password Adminpa55 to access R2. The SSH session should succeed.

b. While the SSH session is active, issue the command show policy-map type inspect zone-pair sessions on R3 to view established sessions.

```
R3# show policy-map type inspect zone-pair sessions policy exists on zp IN-2-OUT-ZPAIR

Zone-pair: IN-2-OUT-ZPAIR

Service-policy inspect : IN-2-OUT-PMAP

Class-map: IN-NET-CLASS-MAP (match-all)

Match: access-group 101

Inspect

Number of Established Sessions = 1

Established Sessions

Session 175216232 (192.168.3.3:1028)=>(10.2.2.2:22) tcp SIS_OPEN/TCP_ESTAB

Created 00:00:25, Last heard 00:00:20

Bytes sent (initiator:responder) [1195:1256] Classmap: class-default (match-any)

Match: any
```

```
Drop (default action)
0 packets, 0 bytes
```

192.168.3.3:1028 (port 1028 is random)

10.2.2.2:22 (SSH = port 22)

Step 3: From PC-C, exit the SSH session on R2 and close the command prompt window.

Step 4: From internal PC-C, open a web browser to the PC-A server web page.

Enter the server IP address 192.168.1.3 in the browser URL field, and click Go. The HTTP session should succeed. While the HTTP session is active, issue the command show policy-map type inspect zone-pair sessions on R3 to view established sessions.

Note: If the HTTP session times out before you execute the command on R3, you will have to click the Go button on PC-C to generate a session between PC-C and PC-A.

```
R3# show policy-map type inspect zone-pair sessions
policy exists on zp IN-2-OUT-ZPAIR
Zone-pair: IN-2-OUT-ZPAIR
Service-policy inspect : IN-2-OUT-PMAP
Class-map: IN-NET-CLASS-MAP (match-all)
Match: access-group 101
Inspect
Number of Established Sessions = 1
Established Sessions
Session 565266624 (192.168.3.3:1031)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
Created 00:00:01, Last heard 00:00:01
Bytes sent (initiator:responder) [284:552]
Class-map: class-default (match-any)
Match: any
Drop (default action)
0 packets, 0 bytes
```

Step 5: Close the browser on PC-C.

Part 7: Test Firewall Functionality from OUT-ZONE to IN-ZONE

Verify that external hosts CANNOT access internal resources after configuring the ZPF.

Step 1: From the PC-A server command prompt, ping PC-C.

From the PC-A command prompt, ping PC-C at 192.168.3.3. The ping should fail.

Step 2: From R2, ping PC-C.

From R2, ping PC-C at 192.168.3.3. The ping should fail.

Step 3: Output :Check results:Your completion percentage should be 100%. Click Check Results to see feedback and verification of which required components have been completed.

Notes :

➢ What is an access control list?

An access control list is a record that identifies and manages traffic. There are two types of IP ACLs: standard and extended. Standard IP ACLs can only control traffic based on the SOURCE IP address. Extended IP ACLs are far more powerful; they can identify traffic based on source IP, source port, destination IP, and destination port.

➢ The most common numbers used for IP ACLs are 1 to 99 and 1300 to 1999 for standard lists.100 to 199 and 2000 to 2699 for extended lists.

Practical: 6

1.Title: Configure IOS Intrusion Prevention System (IPS) Using the CLI

2. Prior Concepts:

a. Telnet

b. SSH

3. New Concepts:

Your task is to enable IPS on R1 to scan traffic entering the 192.168.1.0 network.The server labeled Syslog is used to log IPS messages. You must configure the router to identify the syslog server to receive logging messages. Displaying the correct time and date in syslog messages is vital when using syslog to monitor the network. Set the clock and configure the timestamp service for logging on the routers. Finally, enable IPS to produce an alert and drop ICMP echo reply packets inline.The server and PCs have been preconfigured. The routers have also been preconfigured with the following: Enable password: ciscoenpa55 . Console password: ciscoconpa55 . SSH username and password: SSHadmin / ciscosshpa55 .OSPF 101

4.Objectives:

a. Enable IOS IPS.

b. Configure logging.

c. Modify an IPS signature.

d. Verify IPS.

5. Procedure:

a. Enable IOS IPS

b. Modify the Signature

6. Implementation :

Done by students in the lab.

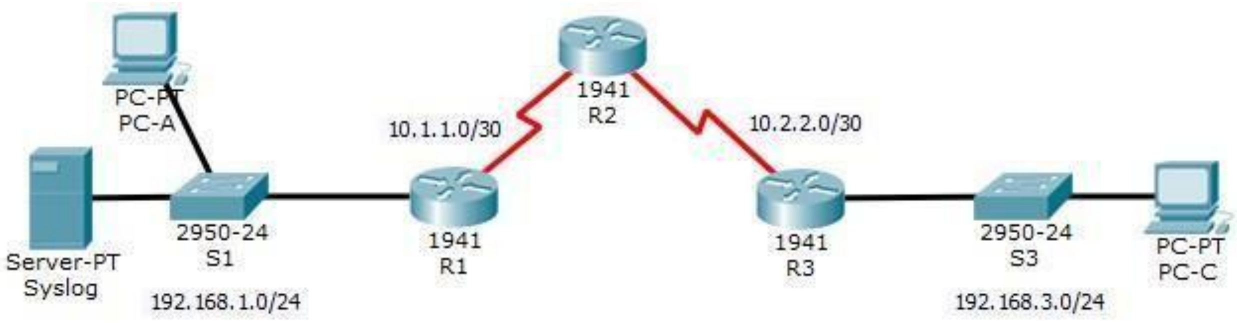
7. Results:

O/P of the program

8. Application:

Real life application in network designing

9. Questions:



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	S0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
Syslog	NIC	192.168.1.50	255.255.255.0	192.168.1.1	S1 F0/2
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1	S1 F0/3
PC-C	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/2

Part 1: Enable IOS IP-Note: Within Packet Tracer, the routers already have the signature files imported and in place. They are the default xml files in flash. For this reason, it is not necessary to configure the public crypto key and complete a manual import of the signature files.

Step 1: Enable the Security Technology package.

a. On R1, issue the show version command to view the Technology Package license information.

b. If the Security Technology package has not been enabled, use the following command to enable the package.

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

c. Accept the end user license agreement.

d. Save the running-config and reload the router to enable the security license.

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

Step 2: Verify network connectivity.

```
R1(config)#router rip

R1(config-router)#network 192.168.1.0

R1(config-router)#network 10.1.1.0

R1(config-router)#network 10.2.2.0

R1(config-router)#network 192.168.3.0

R1(config-router)#exit

R1(config)#

R2(config)#router rip

R2(config-router)#network 192.168.1.0

R2(config-router)#network 10.1.1.0

R2(config-router)#network 10.2.2.0

R2(config-router)#network 192.168.3.0

R2(config-router)#exit

R2(config)#

R3(config)#router rip

R3(config-router)#network 192.168.1.0

R3(config-router)#network 10.1.1.0

R3(config-router)#network 10.2.2.0

R3(config-router)#network 192.168.3.0

R3(config-router)#exit

R3(config)#
```

a. Ping from PC-C to PC-A. The ping should be successful. ping 192.168.1.2

b. Ping from PC-A to PC-C. The ping should be successful.

```
ping 192.168..3.2
```

Step 3: Create an IOS IPS configuration directory in flash. On R1, create a directory in flash using the mkdir command. Name the directory ipsdir.

```
R1# mkdir ipsdir
```

Create directory filename [ipsdir]? <Enter> Created dir flash:ipsdir

Step 4: Configure the IPS signature storage location. On R1, configure the IPS signature storage location to be the directory you just created.

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

Note : if there is an error then type:

R1(config)#exit

R1#copy run start

Enter

Enter

R1#reload

Enter

R1>en

R1#config t

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

Step 5: Create an IPS rule.On R1, create an IPS rule name using the ip ips name name command in global configuration mode. Name the IPS rule iosips.

R1(config)# ip ips name iosips

Step 6: Enable logging. IOS IPS supports the use of syslog to send event notification. Syslog notification is enabled by default. If logging console is enabled, IPS syslog messages display. a. Enable syslog if it is not enabled.

R1(config)# ip ips notify log

b. If necessary, use the clock set command from privileged EXEC mode to reset the clock.

R1# clock set 10:20:00 10 january 2014

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.

R1(config)# service timestamps log datetime msec

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

R1(config)# logging host 192.168.1.50

Step 7: Configure IOS IPS to use the signature categories.Retire the all signature category with the retired true command (all signatures within the signature release). Unretire the IOS_IPS Basic category with the retired false command.

```
R1(config)# ip ips signature-category

R1(config-ips-category)# 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-cateogry)# exit

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

Step 8: Apply the IPS rule to an interface.Apply the IPS rule to an interface with the ip ips name direction command in interface configuration mode.

Apply the rule outbound on the G0/1 interface of R1. After you enable IPS, some log messages will be sent to the console line indicating that the IPS engines are being initialized.

Note: The direction in means that IPS inspects only traffic going into the interface. Similarly, out means that IPS inspects only traffic going out of the interface.

```
R1(config)# interface g0/1

R1(config-if)# ip ips iosips out
```

Part 2: Modify the Signature

Step 1: Change the event-action of a signature. Un-retire the echo request signature (signature 2004, subsig ID 0), enable it, and change the signature action to alert and drop.

```
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)# eventaction 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 commands to verify IPS.Use the

R1#show ip ips all command to view the IPS configuration status summary. To which interfaces and in which direction is the iosips rule applied?

G0/1 outbound.

Step 3: Verify that IPS is working properly.

a. From PC-C, attempt to ping PC-A. Were the pings successful? Explain.

ping 192.168.1.2

The pings should fail. This is because the IPS rule for event-action of an echo request was set to “denypacket-inline”.

b. From PC-A, attempt to ping PC-C. Were the pings successful? Explain.

ping 192.168.3.2

The ping should be successful. This is because the IPS rule does not cover echo reply. When PC-A pings

PC-C, PC-C responds with an echo reply.

Step 4: View the syslog messages.

a. Click the Syslog server.

b. Select the Services tab.

c. In the left navigation menu, select SYSLOG to view the log file.

Step 5: Check results.

Your completion percentage should be 100%. Click Check Results to see feedback and verification of

which required components have been completed.

Output :

!!!Script for R1

clock set 10:20:00 10 january 2014 mkdir

ipsdir

config

```
license boot module c1900 technology-package
security k9 yes end reload config t
ip ips config location flash:ipsdir
ip ips name iosips ip ips notify log
service timestamps log datetime msec
logging host 192.168.1.50
ip ips signature-category
category all retired true exit
category ios_ips basic retired
false exit exit interface
g0/1 ip ips ios ips out exit ip
ips signature-definition
signature 2004 0 status
retired false enabled true
exit engine event-action
produce-alert event-action
deny-packet-inline exit exit
exit
```

Practical: 7

1.Title: Packet Tracer Layer 2 Security

2. Prior Concepts:

a. Assigning IP address to Router, Server, PC

b. Configure all switch devices with the following:

i. Enable password: ciscoenpa55

ii. Console password: ciscoconpa55

iii. SSH username and password: SSHadmin / ciscosshpa55

3. New Concepts:

To configure port security to limit the number of MAC addresses each switch port can learn. If the number of MAC addresses exceeds the set limit, the port should be shutdown.

4. Objectives:

a. Assign the Central switch as the root bridge.

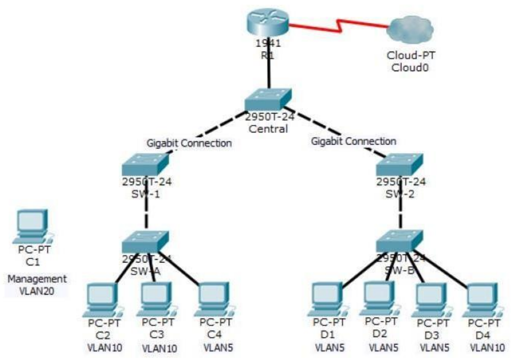
b. Secure spanning-tree parameters to prevent STP manipulation attacks.

c. Enable port security to prevent CAM table overflow attacks.

5. Procedure:

Background/Scenario To prevent spanning-tree manipulation attacks, the administrator wants to ensure that the STP parameters are secure. To prevent against CAM table overflow attacks, the network administrator has decided to configure port security to limit the number of MAC addresses each switch port can learn. If the number of MAC addresses exceeds the set limit, the administrator would like the port to be shutdown.

Topology



Part 1: Configure Root Bridge

Step 1: Determine the current root bridge. From Central, issue the show spanning-tree command to determine the current root bridge, to see the ports in use, and to see their status.

Step 2: Assign Central as the primary root bridge.

Using the spanning-tree vlan 1 root primary command, and assign Central as the root bridge.

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

Step 3: Assign SW-1 as a secondary root bridge.

Assign SW-1 as the secondary root bridge using the spanning-tree vlan 1 root secondary command.

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

Step 4: Verify the spanning-tree configuration.

Issue the show spanning-tree command to verify that Central is the root bridge.

Part 2: Protect Against STP Attacks

Secure the STP parameters to prevent STP manipulation attacks.

Step 1: Enable PortFast on all access ports.

PortFast is configured on access ports that connect to a single workstation or server to enable them to become

active more quickly. On the connected access ports of the SW-A and SW-B, use the spanning-tree portfast

command.

SW-A(config)# interface range f0/1 - 4

SW-A(config-if-range)# spanning-tree portfast

SW-B(config)# interface range f0/1 - 4

SW-B(config-if-range)# spanning-tree portfast

Step 2: Enable BPDU guard on all access ports.

BPDU guard is a feature that can help prevent rogue switches and spoofing on access ports. Enable BPDU

guard on SW-A and SW-B access ports.

SW-A(config)# interface range f0/1 - 4

SW-A(config-if-range)# spanning-tree bpduguard enable

SW-B(config)# interface range f0/1 - 4

```
SW-B(config-if-range)# spanning-tree bpduguard enable
```

Note: Spanning-tree BPDU guard can be enabled on each individual port using the spanning-tree

bpduguard enable command in interface configuration mode or the spanning-tree portfast bpduguard default

command in global configuration mode. For grading purposes in this activity, please use the spanning-tree

bpduguard enable command.

Step 3: Enable root guard.

Root guard can be enabled on all ports on a switch that are not root ports. It is best deployed on ports that connect

to other non-root switches. Use the show spanning-tree command to determine the location of the root port on

each switch.

On SW-1, enable root guard on ports F0/23 and F0/24. On SW-2, enable root guard on ports F0/23 and F0/24.

```
SW-1(config)# interface range f0/23 - 24

SW-1(config-if-range)# spanning-tree guard root

SW-2(config)# interface range f0/23 - 24

SW-2(config-if-range)# spanning-tree guard root
```

Part 3: Configure Port Security and Disable Unused Ports

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

This procedure should be performed on all access ports on SW-A and SW-B. Set the maximum number of learned

MAC addresses to 2, allow the MAC address to be learned dynamically, and set the violation to shutdown.

Note: A switch port must be configured as an access port to enable port security.

```
SW-A(config)# interface range f0/1 - 22

SW-A(config-if-range)# switchport mode access

SW-A(config-if-range)# switchport port-security

SW-A(config-if-range)# switchport port-security maximum 2

SW-A(config-if-range)# switchport port-security violation shutdown
```

```
SW-A(config-if-range)# switchport port-security mac-address sticky

SW-B(config)# interface range f0/1 - 22

SW-B(config-if-range)# switchport mode access

SW-B(config-if-range)# switchport port-security

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

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

SW-B(config-if-range)# switchport port-security mac-address sticky
```

Step 2: Verify port security.

a. On SW-A, issue the command show port-security interface f0/1 to verify that port security has been configured.

```
SW-A# show port-security interface f0/1

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 0

Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0000.0000.0000:0

Security Violation Count : 0
```

b. Ping from C1 to C2 and issue the command show port-security interface f0/1 again to verify that the switch has

learned the MAC address for C1.

Step 3: Disable unused ports.

Disable all ports that are currently unused.

```
SW-A(config)# interface range f0/5 - 22

SW-A(config-if-range)# shutdown
```

```
SW-B(config)# interface range f0/5 - 22
SW-B(config-if-range)# shutdown
```

6. Implementation:

Done by students in the lab using Cisco Packet Tracer

7. Results:

Successful port security implementation, switch has learned MAC address for C1.

8. Application:

Real world implementation in any organization network.

Practical: 8

1.Title: Packet Tracer – Layer 2 VLAN Security

2. Prior Concepts:

a. Assigning IP address to Router, Server, PC

b. Configure all switch devices with the following:

i. Enable password: ciscoenpa55

ii. Console password: ciscoconpa55

iii. SSH username and password: SSHadmin / ciscosshpa55

3. New Concepts:

Enabling the management PC to connect to all switches and the router, but other devices should not connect to the management PC or the switches. Creation of new VLAN 20 for management purposes.

4. Objectives:

a. Connect a new redundant link between SW-1 and SW-2.

b. Enable trunking and configure security on the new trunk link between SW-1 and SW-2.

c. Create a new management VLAN (VLAN 20) and attach a management PC to that VLAN.

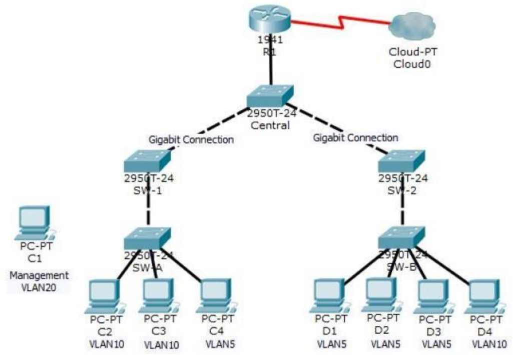
d. Implement an ACL to prevent outside users from accessing the management VLAN.

5. Procedure:

Background/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. A network administrator wants to add a redundant link between switch SW-1 and SW-2. The link must have trunking enabled and all security requirements should be in place. In addition, the network administrator wants to connect a management PC to switch SW-A. The administrator would like to enable the management PC to connect to all switches and the router, but does not want any other devices to connect to the management PC or the switches. The administrator would like to create a new VLAN 20 for management purposes.

Topology



Part 1: Verify Connectivity

Step 1: Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10).

Step 2: Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5).

Note: If using the simple PDU GUI packet, be sure to ping twice to allow for ARP.

Part 2: Create a Redundant Link Between SW-1 and SW-2

Step 1: Connect SW-1 and SW-2.

Using a crossover cable, connect port F0/23 on SW-1 to port F0/23 on SW-2.

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

Trunking has already been configured on all pre-existing trunk interfaces. The new link must be configured for

trunking, including all trunk security mechanisms. On both SW-1 and SW-2, set the port to trunk, assign native

VLAN 15 to the trunk port, and disable auto-negotiation.

```
SW-1(config)# interface f0/23

SW-1(config-if)# switchport mode trunk

SW-1(config-if)# switchport trunk native vlan 15

SW-1(config-if)# switchport nonegotiate

SW-1(config-if)# no shutdown

SW-2(config)# interface f0/23

SW-2(config-if)# switchport mode trunk

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

SW-2(config-if)# switchport nonegotiate

SW-2(config-if)# no shutdown
```

Part 3: Enable VLAN 20 as a Management VLAN

The network administrator wants to access all switch and routing devices using a management PC. For security

purposes, the administrator wants to ensure that all managed devices are on a separate VLAN.

Step 1: Enable a management VLAN (VLAN 20) on SW-A.

a. Enable VLAN 20 on SW-A.

```
SW-A(config)# vlan 20

SW-A(config-vlan)# exit
```

b. Create an interface VLAN 20 and assign an IP address within the 192.168.20.0/24 network.

```
SW-A(config)# interface vlan 20

SW-A(config-if)# ip address 192.168.20.1 255.255.255.0
```

Step 2: Enable the same management VLAN on all other switches.

a. Create the management VLAN on all switches: SW-B, SW-1, SW-2, and Central.

```
SW-B(config)# vlan 20

SW-B(config-vlan)# exit

SW-1(config)# vlan 20

SW-1(config-vlan)# exit

SW-2(config)# vlan 20

SW-2(config-vlan)# exit

Central(config)# vlan 20

Central(config-vlan)# exit
```

b. Create an interface VLAN 20 on all switches and assign an IP address within the 192.168.20.0/24

network.

```
SW-B(config)# interface vlan 20

SW-B(config-if)# ip address 192.168.20.2 255.255.255.0

SW-1(config)# interface vlan 20

SW-1(config-if)# ip address 192.168.20.3 255.255.255.0
```

```
SW-2(config)# interface vlan 20

SW-2(config-if)# ip address 192.168.20.4 255.255.255.0

Central(config)# interface 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 SW-A port F0/1 and ensure that it is assigned an available IP address within the

192.168.20.0/24 network.

Step 4: On SW-A, ensure the management PC is part of VLAN 20.

Interface F0/1 must be part of VLAN 20.

```
SW-A(config)# interface f0/1

SW-A(config-if)# switchport access vlan 20

SW-A(config-if)# no shutdown
```

Step 5: Verify connectivity of the management PC to all switches.

The management PC should be able to ping SW-A, SW-B, SW-1, SW-2, and Central.

Part 4: Enable the Management PC to Access Router R1

Step 1: Enable a new subinterface on router R1.

a. Create subinterface g0/0.3 and set encapsulation to dot1q 20 to account for VLAN 20.

```
R1(config)# interface g0/0.3

R1(config-subif)# encapsulation dot1q 20
```

b. Assign an IP address within the 192.168.20.0/24 network.

```
R1(config)# interface g0/0.3

R1(config-subif)# ip address 192.168.20.100 255.255.255.0
```

Step 2: Verify connectivity between the management PC and R1.

Be sure to configure the default gateway on the management PC to allow for connectivity.

Step 3: Enable security.

While the management PC must be able to access the router, no other PC should be able to access the management VLAN.

a. Create an ACL that allows only the Management PC to access the router.

Example: (may vary from student configuration)

```
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
```

b. Apply the ACL to the proper interface(s).

Example: (may vary from student configuration)

```
R1(config)# interface g0/0.1
R1(config-subif)# ip access-group 101 in
R1(config-subif)# interface g0/0.2
R1(config-subif)# ip access-group 101 in
R1(config-subif)# line vty 0 4
R1(config-line)# access-class 102 in
```

Note: Access list 102 is used to only allow the Management PC (192.168.20.50 in this example) to access the router. This prevents an IP address change to bypass the ACL.

Note: There are multiple ways in which an ACL can be created to accomplish the necessary security. For this reason, grading on this portion of the activity is based on the correct connectivity requirements. The management PC must be able to connect to all switches and the router. All other PCs should not be able to connect to any devices within the management VLAN.

Step 4: Verify security.

a. Verify only the Management PC can access the router. Use SSH to access R1 with username SSHadmin and

password ciscosshpa55.

PC> ssh -l SSHadmin 192.168.20.100 From the management PC, ping SW-A, SW-B, and R1. The pings should be successful because all devices within the 192.168.20.0 network should be able to ping one another. Devices within VLAN20 are not required to route through the router.From D1, ping the management PC. The ping should fail because for a device within a different VLAN to successfully ping a device within VLAN20, it must be routed. The router has an ACL that prevents all packets from accessing the 192.168.20.0 network.

6. Implementation:

Done by students in the lab using Cisco Packet Tracer

7. Results:

From the management PC, ping SW-A, SW-B, and R1. The pings should be successful because all devices within the 192.168.20.0 network should be able to ping one another.

Devices within VLAN20 are not required to route through the router.From D1, ping the management PC. The ping should fail because for a device within a different VLAN to successfully ping a device within VLAN20, it must be routed. The router has an ACL that prevents all packets from accessing the 192.168.20.0 network

8. Application:

Real world implementation in any organization network

Practical: 9

1.Title: Configure and verify a Site-to-Site IPsec VPN using CLI

2. Prior Concepts:

1. RIP
2. SSH

3. New Concepts:

The network topology shows three routers. The task is to configure R1 and R3 to support a site-to-site IPsec VPN when traffic flows between their respective LANs. The IPsec VPN tunnel is from R1 to R3 via R2. R2 acts as a pass-through and has no knowledge of the VPN. IPsec provides secure transmission of sensitive information over unprotected networks, such as the Internet. IPsec operates at the network layer and protects and authenticates IP packets between participating IPsec devices (peers), such as Cisco routers. ISAKMP Phase 1 Policy Parameters.

4.Objectives:

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

5. Procedure:

1. Configure IPsec parameters.

6. Implementation :

Done by students in the lab.

7. Results:

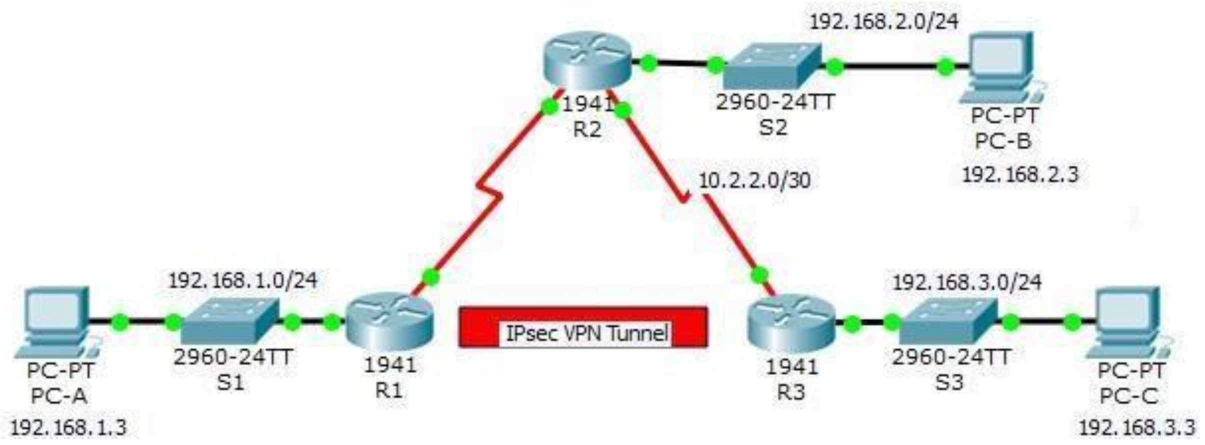
O/P of the program

8. Application:

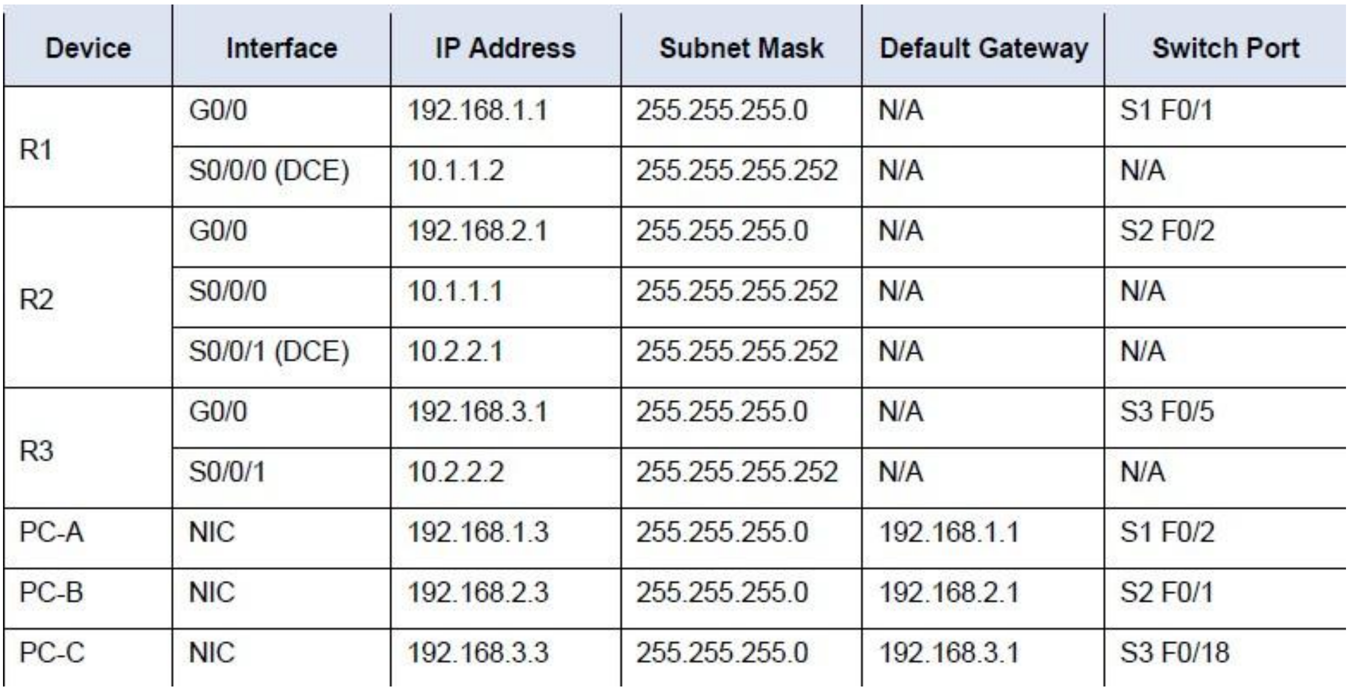
Real life application in network designing

9. Questions

Topology



Addressing Table



Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Enable RIP on all routers

```
R1(config)#router rip

R1(config-router)#network 192.168.1.0

R1(config-router)#network 10.1.1.0

R1(config-router)#network 10.2.2.0

R1(config-router)#network 192.168.3.0

R1(config-router)#exit

R1(config)#

R2(config)#router rip
```

```
R2(config-router)#network 192.168.1.0

R2(config-router)#network 10.1.1.0

R2(config-router)#network 10.2.2.0

R2(config-router)#network 192.168.3.0

R2(config-router)#exit

R2(config)#

R3(config)#router rip

R3(config-router)#network 192.168.1.0

R3(config-router)#network 10.1.1.0

R3(config-router)#network 10.2.2.0

R3(config-router)#network 192.168.3.0

R3(config-router)#exit

R3(config)#
```

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. On R1, issue the show version command to view the Security Technology package license information.

b. If the Security Technology package has not been enabled, use the following command to enable the package. R1(config)# license boot module c1900 technology-package securityk9 .

c. Accept the end-user license agreement.

d. Save the running-config (copy run start) and reload the router to enable the security license(reload).

e. 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.

```
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.

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

```
R3# show version
```

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

Configure reciprocating parameters on R3. Configure ACL 110 identifying 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.

a. 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
```

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.

```
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.

Output

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

Practical: 10

1.Title: Configuring ASA Basic Settings and Firewall Using CLI

a) Configure basic ASA settings and interface security levels using CLI

b) Configure routing, address translation, and inspection policy using CLI

c) Configure DHCP, AAA, and SSH

d) Configure a DMZ, Static NAT, and ACLs

2. Prior Concepts:

1. SSH

3. New Concepts:

A company has one location connected to an ISP. R1 represents a CPE device managed by the ISP. R2 represents an intermediate Internet router. R3 represents an ISP that connects an administrator from a network management company, who has been hired to remotely manage your network. The ASA is an edge CPE security device that connects the internal corporate network and DMZ to the ISP while providing NAT and DHCP services to inside hosts. The ASA will be configured for management by an administrator on the internal network and by the remote administrator. Layer 3 VLAN interfaces provide access to the three areas created in the activity: Inside, Outside, and DMZ. The ISP assigned the public IP address space of 209.165.200.224/29, which will be used for address translation on the ASA.

4.Objectives:

1. Verify connectivity and explore the ASA
2. Configure basic ASA settings and interface security levels using CLI
3. Configure routing, address translation, and inspection policy using CLI
4. Configure DHCP, AAA, and SSH
5. Configure a DMZ, Static NAT, and ACLs

5. Procedure:

1. Verify Connectivity and Explore the ASA
2. Configure ASA Settings and Interface Security Using the CLI
3. Configure Routing, Address Translation, and Inspection Policy Using the CLI
4. Configure DHCP, AAA, and SSH
5. Configure a DMZ, Static NAT, and ACLs

6. Implementation :

Done by students in the lab.

7. Results:

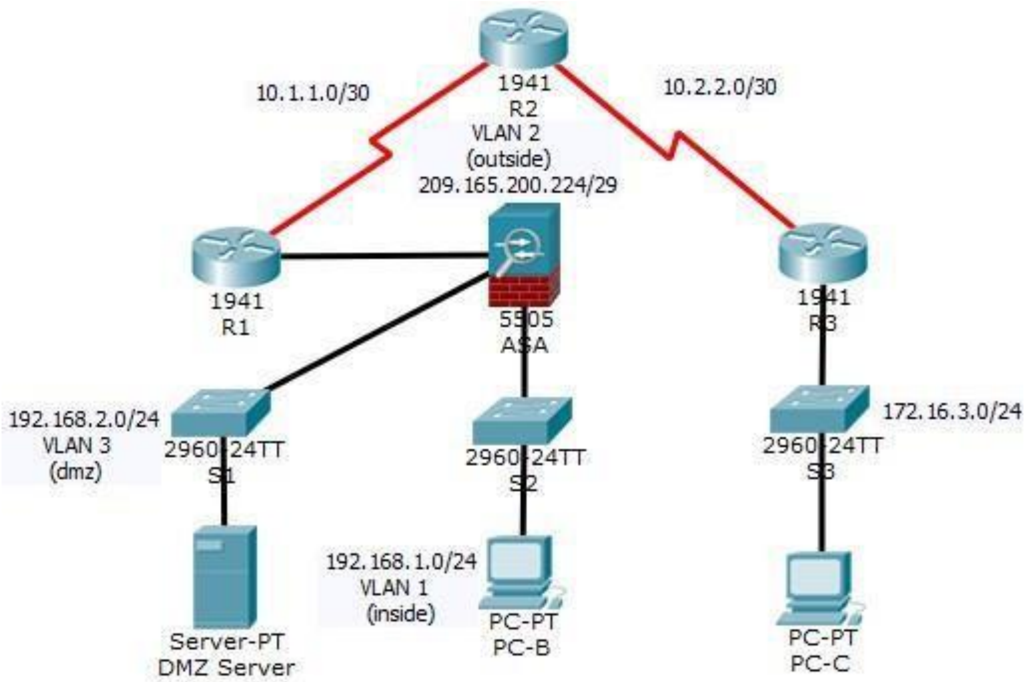
O/P of the program

8. Application:

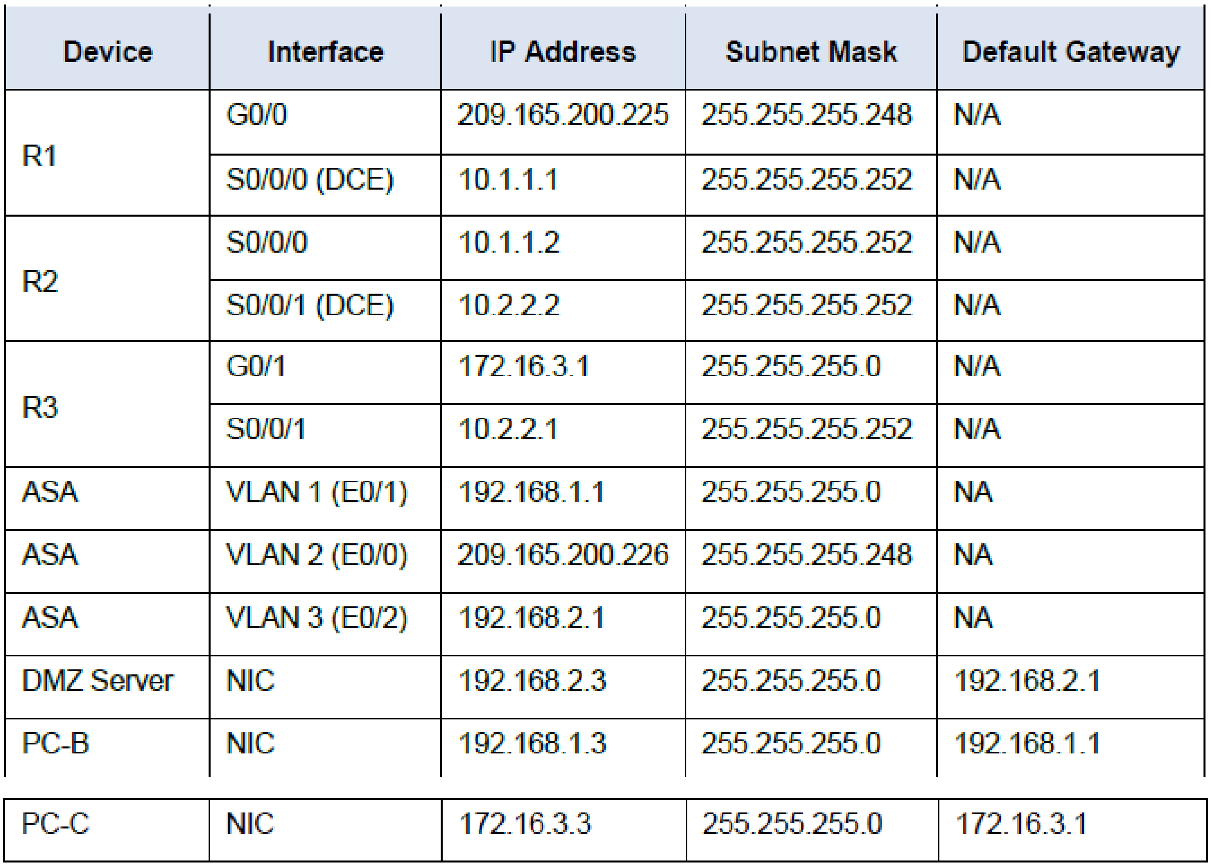
Real life application in network designing

9. Questions

Topology



Addressing Table



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	209.165.200.225	255.255.255.248	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	NA
ASA	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	NA
ASA	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	NA
DMZ Server	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1

Part 1: Verify Connectivity and Explore the ASA

Step 1: Verify connectivity.

The ASA is not currently configured. However, all routers, PCs, and the DMZ server are configured. Verify that PC-C can ping any router interface. PC-C is unable to ping the ASA, PC-B, or the DMZ server.

Step 2: Determine the ASA version, interfaces, and license.

Use the show version command to determine various aspects of this ASA device.

Step 3: Determine the file system and contents of flash memory.

a. Enter privileged EXEC mode. A password has not been set. Press Enter when prompted for a password.

b. Use the show file system command to display the ASA file system and determine which prefixes are supported.

c. Use the show flash: or show disk0: command to display the contents of flash memory.

Part 2: Configure ASA Settings and Interface Security Using the CLI

Step 1: Configure the hostname and domain name.

a. Configure the ASA hostname as CCNAS-ASA.

b. Configure the domain name as ccnasecurity.com.

Step 2: Configure the enable mode password.

Use the enable password command to change the privileged EXEC mode password to ciscoenpa55 .

Step 3: Set the date and time.

Use the clock set command to manually set the date and time

Step 4: Configure the inside and outside interfaces.

Configure the VLAN 1 (inside) and VLAN 2 (outside) interfaces at this time. The VLAN 3 (dmz) interface will be configured in Part 5 of the activity.

a. 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
```

b. Create a logical VLAN 2 interface for the outside network (209.165.200.224/29), set the security level to

the lowest setting of 0, and enable the VLAN 2 interface.

```
CCNAS-ASA(config-if)# 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
```

c. Use the following verification commands to check your configurations:

1) Use the show interface ip brief command to display the status for all ASA interfaces. Note: This command is different from the IOS command show ip interface brief. If any of the physical or logical interfaces previously configured are not up/up, troubleshoot as necessary before continuing.

2) Use the show ip address command to display the information for the Layer 3 VLAN interfaces.

3) Use the show switch vlan command to display the inside and outside VLANs configured on the ASA and to display the assigned ports.

Step 5: Test connectivity to the ASA.

a. You should be able to ping from PC-B to the ASA inside interface address (192.168.1.1). If the pings fail, troubleshoot the configuration as necessary.

b. From PC-B, ping the VLAN 2 (outside) interface at IP address 209.165.200.226. You should not be able to ping this address.

Part 3 : Configure Routing, Address Translation, and Inspection Policy Using the CLI

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

Configure a default static route on the ASA outside interface to enable the ASA to reach external networks.

a. Create a "quad zero" default route using the route command, associate it with the ASA outside interface, and point to the R1 G0/0 IP address (209.165.200.225) as the gateway of last resort.

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

b. Issue the show route command to verify the static default route is in the ASA routing table.

c. Verify that the ASA can ping the R1 S0/0/0 IP address 10.1.1.1. If the ping is unsuccessful, troubleshoot as necessary.

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

a) Create network object inside-net and assign attributes to it using the subnet and nat commands.

```
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
```

From PC-B attempt to ping the R1 G0/0 interface at IP address 209.165.200.225. The pings should fail.

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

Create the class-map, policy-map, and service-policy. Add the inspection of ICMP traffic to the policy map list using the following commands:

```
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
```

From PC-B, attempt to ping the R1 G0/0 interface at IP address 209.165.200.225. The pings should be successful this time because ICMP traffic is now being inspected and legitimate return traffic is being allowed. If the pings fail, troubleshoot your configurations.

Part 4 : Configure DHCP, AAA, and SSH

Configure the ASA as a DHCP server.

Configure a DHCP address pool and enable it on the ASA inside interface.

```
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
```

Configure AAA to use the local database for authentication.

Define a local user named admin by entering the username command. Specify a password of adminpa55.

```
CCNAS-ASA(config)# username admin password adminpa55
```

Configure AAA to use the local ASA database for SSH user authentication.

```
CCNAS-ASA(config)# aaa authentication ssh console LOCAL
CCNAS-ASA(config)# crypto key generate rsa modulus 1024
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
```

Establish an SSH session from PC-C to the ASA (209.165.200.226). Troubleshoot if it is not successful.

```
PC> ssh -l admin 209.165.200.226
```

Establish an SSH session from PC-B to the ASA (192.168.1.1). Troubleshoot if it is not successful.

```
PC> ssh -l admin 192.168.1.1
```

Part 5 : Configure DHCP, AAA, and SSH

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
```

Assign ASA physical interface E0/2 to DMZ VLAN 3 and enable the interface.

```
CCNAS-ASA(config-if)# interface Ethernet0/2

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

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
```

Configure an ACL to allow access to the DMZ server from the 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 interface outside
```

Test access to the DMZ server

At the time this Packet Tracer activity was created, the ability to successfully test outside access to the DMZ web server was not in place; therefore, successful testing is not required.

Output

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

Newly Added Experiments (To be added at the end of all practicals)

Practical 1:

1.Title: Write a program to generate asymmetric keys for RSA algorithm

2. Prior Concepts:

1. Basic Mathematics
2. Core Java Knowledge

3.New Concepts:

Asymmetric key cryptography

4.Objectives:

Learning the process of public key and private key generation.

5.Procedure:

1. Choose two distinct large prime numbers p and q.
2. Compute the product M = P*Q. This number is called the modulus.
3. Also compute the Euler totient T = (P-1)*(Q-1).
4. Choose a public key e such that 1 < E < T and greatest common divisor of (E, T) = 1; i.e., E and T are coprime.
5. Compute a private key D so that E*D leaves a remainder of 1 when divided by T i.e. (D*E) mod T = 1
6. Finish

6. Implementation :

Done by students in the lab.

7. Results:

O/P of the program

8. Application:

Real life application in network designing

The algorithm is incorporated into all of the major protocols for secure Internet communications, including S/MIME, SSL, and S/WAN.

9. Questions

Write java program to convert a plain text entered in upper case or lower case and convert it into cipher text using the keys generated.

```
import java.math.*;
import java.security.*;
public class RSA
{
BigInteger p,q,n,subtractp,subtractq,result,d,e;
SecureRandom r;
public RSA()
{
r=new SecureRandom();
p=new BigInteger(512,100,r);
q=new BigInteger(512,100,r); `
System.out.println("prime no. p is "+p.intValue());
System.out.println("prime no. q is "+q.intValue());
n=p.multiply(q);
subtractp=(p.subtract(new BigInteger("1")));
subtractq=(q.subtract(new BigInteger("1")));
result=subtractp.multiply(subtractq);
e=new BigInteger("2");
while(result.gcd(e).intValue()>1)
{
e = e.add(new BigInteger("1"));
}
d=e.modInverse(result);
System.out.println("public key is "+e.intValue());
System.out.println("pvt key is "+d.intValue());
BigInteger msg= new BigInteger("15");
System.out.println("Message is: "+msg);
BigInteger enmsg=encrypt(msg,e,n);
System.out.println("Encrypted msg is: "+enmsg.intValue());
BigInteger demsg=decrypt(enmsg,d,n);
System.out.println("Decrypted msg is: "+demsg.intValue());
}
BigInteger encrypt(BigInteger msg,BigInteger e,BigInteger n)
{
return msg.modPow(e, n);
}
BigInteger decrypt (BigInteger msg,BigInteger d,BigInteger n)
{
return msg.modPow(d, n);
}
public static void main(String[] args)
{
new RSA();
}
}
```

Result: Output

❑ Two primes: p = 7, q = 17

❑ N = pq = 7 x 17 = 119

❑ T = (p-1)(q-1) = 6 x 16 = 96

❑ E = 5

❑ D = 77

❑ Public Key = {5, 119} and Private Key = {77, 119}

Practical 2:

1.Title: Write a program in java to implement Encryption and Decryption using Caesar Cipher

2. Prior Concepts:

3. Basic Mathematics

4. Core Java Knowledge

3.New Concepts:

Substitution Cryptography

4.Objectives:

Learning the process of key generation and performing encryption and decryption.

5.Procedure:

1. Read each alphabet in the cipher text message,& search for it in the second row of the replacement table.

2. When a match is found replace that alphabet in the cipher text message with the corresponding alphabet in the same column but the first row of the table

3. Repeat the process for all alphabets in the cipher text message

B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

6. Implementation :

Done by students in the lab.

7. Results:

O/P of the program

8. Application:

Real life application in network designing and cryptography

9. Questions

Write a program in java to implement Caesar Cipher Technique

```
import java.io.*;

class CaesarCipher
```

```
{
public static void main(String []args)throws Exception
{
String plaintxt,ciphertxt="";
BufferedReader br = new BufferedReader(new InputStreamReader(System.in));
System.out.print("Enter plain text : ");
plaintxt = br.readLine();
plaintxt = plaintxt.toLowerCase();
for(int i=0;i<plaintxt.length();i++)
{
char c = plaintxt.charAt(i);
int x = c;
if(x>=97 && x<=122)
{
x += 3;
if(x > 122)
{
x -= 26;
}
}
c = (char)x;
ciphertxt += c;
}
System.out.println("Encrypted Text : "+ciphertxt);
plaintxt="";
for(int i=0;i<ciphertxt.length();i++)
{
char c = ciphertxt.charAt(i);
int x = c;
if(x>=97 && x<=122)
{
x = x-3;
if(x<97)
{
x+=26;
}
}
c = (char)x;
plaintxt += c;
}
System.out.println("Decrypted Text : "+plaintxt);
}
}
```

Output :

```
Plain Text – HELLO HOW ARE YOU
Cipher Text – KHOOR KRZ DUH BRX .
Plain Text – HELLO HOW ARE YOU
```