SDN journal

Index

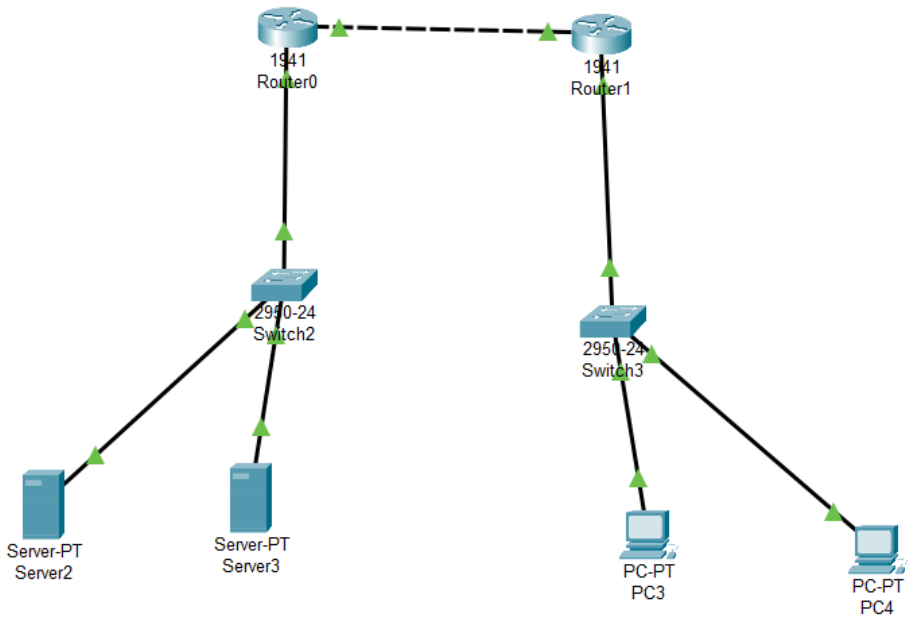
Sr no	Title	sign
1	Implement Standard Access Control list.	
2	Implement VLAN Trunking Protocol.	
3	Implement Inter-VLAN Routing.	
4	Observe STP Topology Changes and Implement RSTP	
5	OSPF Implementation 1.Implement Single Area OSPFv2 2.Implement Multi Area OSPFv2	
6	Implement BGP communities: 1.Implement EBGP 2.Implement IBGP	
7	Implement SPAN Technologies (Switch Port Analyzer)	
8	Implement IPsec Site-to-Site VPNs connection using cisco packettracer.	

Practical -1

Aim: Access control list

Requirement: 2 switches, 2 routers, 2 servers, 2pc

Topology:



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended abc
Router(config-ext-nacl)#permit tcp host 192.168.3.2 host
192.168.1.3 eq www
Router(config-ext-nacl)#permit tcp host 192.168.3.2 host
192.168.1.3 eq www
Router(config-ext-nacl)#deny tcp host 192.168.3.3 host
192.168.1.3 eq www
Router(config-ext-nacl)#exit
Router(config)#
```

Ctrl+F6 to exit CLI focus Copy Paste

Top

```
Router(config-ext-nacl)#exit
Router(config)#int gig0/1
Router(config-if)#ip access-group abc
% Incomplete command.
Router(config-if)#ip access-group abc out
Router(config-if)#
```

Ctrl+F6 to exit CLI focus Copy Paste

```
Router(config-if)#do sh access-lists
Extended IP access list abc
    10 permit tcp host 192.168.3.2 host 192.168.1.3 eq www
    20 deny tcp host 192.168.3.3 host 192.168.1.3 eq www

Router(config-if)#
```

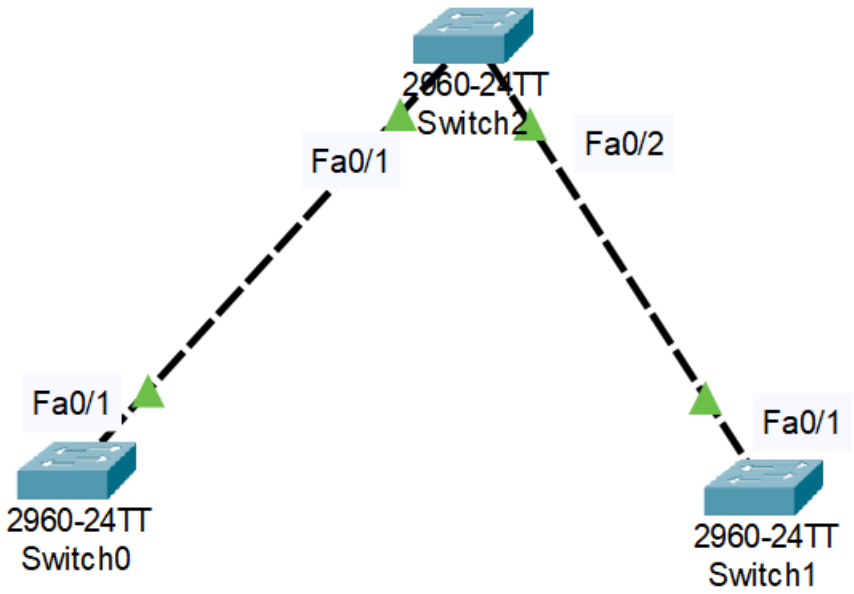
Ctrl+F6 to exit CLI focus Copy Paste

Practical- 2

Aim: Implement VTP

Requirement: 3 switches

Topology:



Steps:

Configure Switch0

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name compsci
Switch(config-vlan)#vlan 3
Switch(config-vlan)#name IT
Switch(config-vlan)#vlan 4
Switch(config-vlan)#name Biotech
Switch(config-vlan)#vlan 5
Switch(config-vlan)#name electronics
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan brief

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
Gig0/1, Gig0/2
2 compsci active
3 IT active
4 Biotech active
5 electronics active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Switch#
```

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vtp domain msc.com
Changing VTP domain name from NULL to msc.com
Switch(config)#vtp mode SERVER
Device mode already VTP SERVER.
Switch(config)#vtp password abc123
Setting device VLAN database password to abc123
Switch(config)#vtp version 2
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastEthernet0?
/
Switch(config)#interface fastEthernet0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
```

Configure Switch2

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan brief

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/5
```

Fa0/6, Fa0/7, Fa0/8, Fa0/9
Fa0/10, Fa0/11, Fa0/12, Fa0/13
Fa0/14, Fa0/15, Fa0/16, Fa0/17
Fa0/18, Fa0/19, Fa0/20, Fa0/21
Fa0/22, Fa0/23, Fa0/24, Gig0/1
Gig0/2
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Switch#show vlan brief

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/5
Fa0/6, Fa0/7, Fa0/8, Fa0/9
Fa0/10, Fa0/11, Fa0/12, Fa0/13
Fa0/14, Fa0/15, Fa0/16, Fa0/17
Fa0/18, Fa0/19, Fa0/20, Fa0/21
Fa0/22, Fa0/23, Fa0/24, Gig0/1
Gig0/2
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Switch#en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vtp domain msc.com
Domain name already set to msc.com.
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#vtp password abc123
Setting device VLAN database password to abc123
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan brief

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/5
Fa0/6, Fa0/7, Fa0/8, Fa0/9
Fa0/10, Fa0/11, Fa0/12, Fa0/13
Fa0/14, Fa0/15, Fa0/16, Fa0/17
Fa0/18, Fa0/19, Fa0/20, Fa0/21
Fa0/22, Fa0/23, Fa0/24, Gig0/1
Gig0/2
2 compsci active
3 IT active
4 Biotech active
5 electronics active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to up

Configure Switch1
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vtp domain msc.com
Changing VTP domain name from NULL to msc.com
Switch(config)#vtp password abc123
Setting device VLAN database password to abc123
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.

```
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan brief

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/5
Fa0/6, Fa0/7, Fa0/8, Fa0/9
Fa0/10, Fa0/11, Fa0/12, Fa0/13
Fa0/14, Fa0/15, Fa0/16, Fa0/17
Fa0/18, Fa0/19, Fa0/20, Fa0/21
Fa0/22, Fa0/23, Fa0/24, Gig0/1
Gig0/2
2 compsci active
3 IT active
4 Biotech active
5 electronics active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Switch#
```

Output:

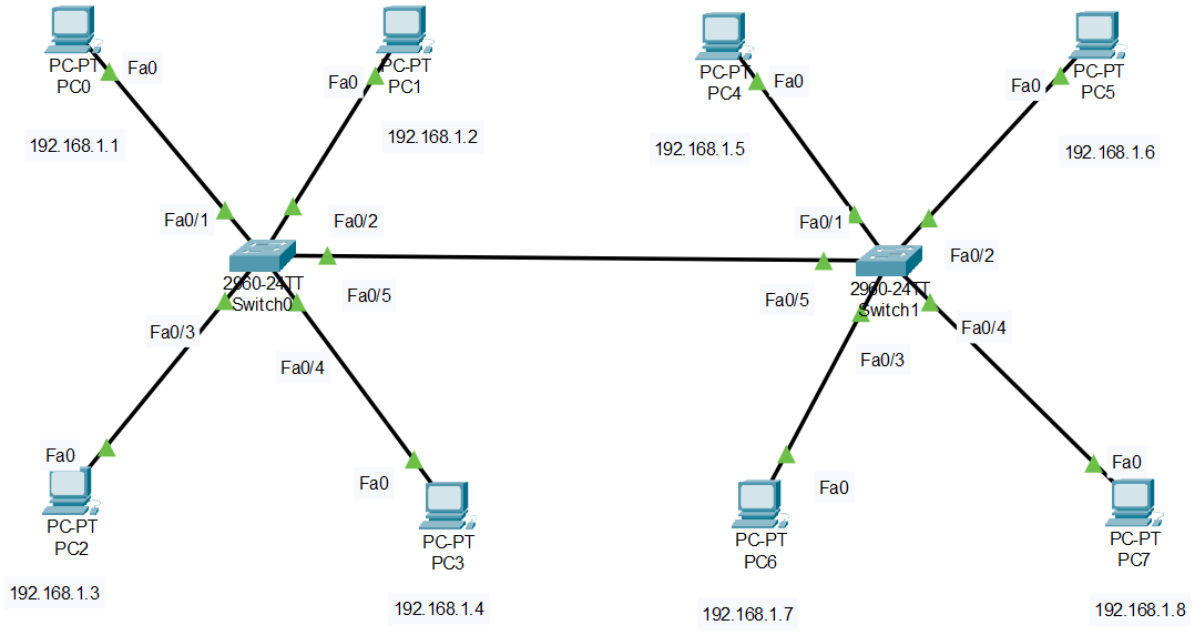
In this practical we are not sending any packets.The practical only shows how to configure VTP on switchs.

Practical – 3

Aim: Implement Inter – VLAN Routing

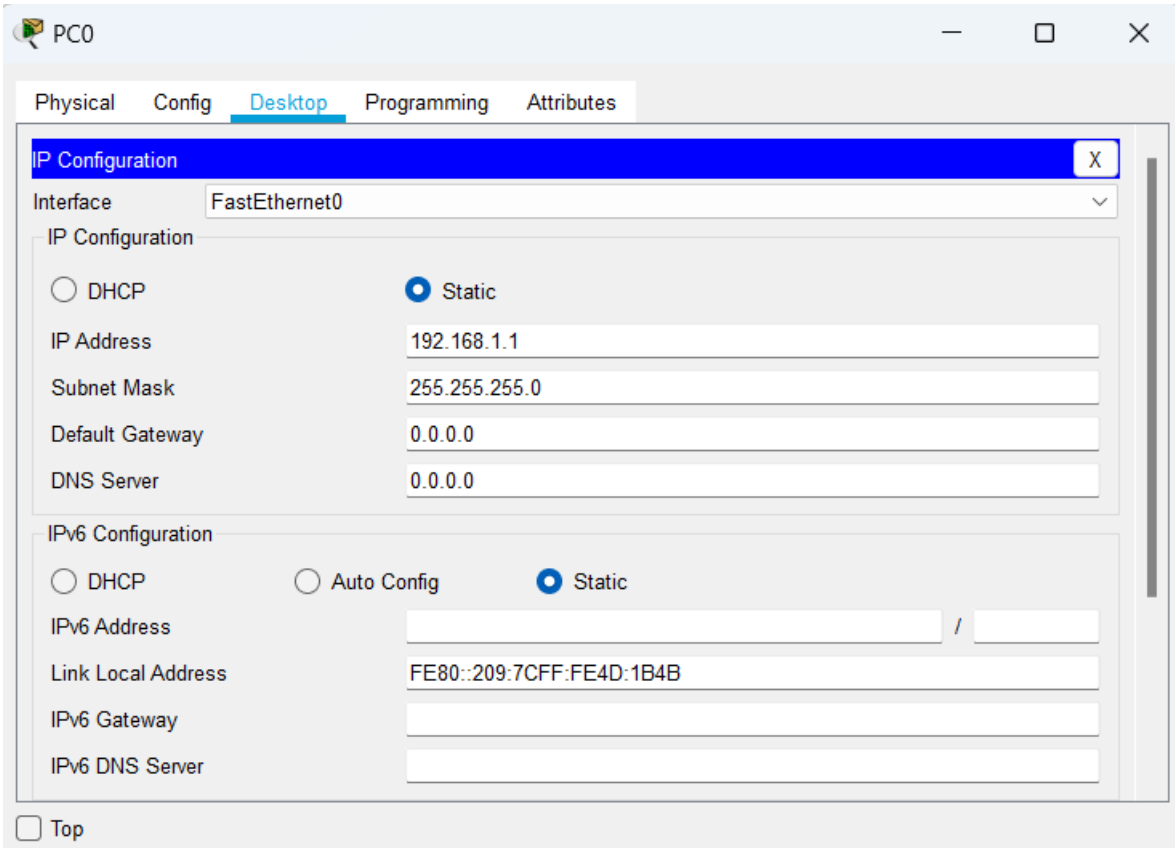
Requirement: 2 Switches and 8 End points

Topology:

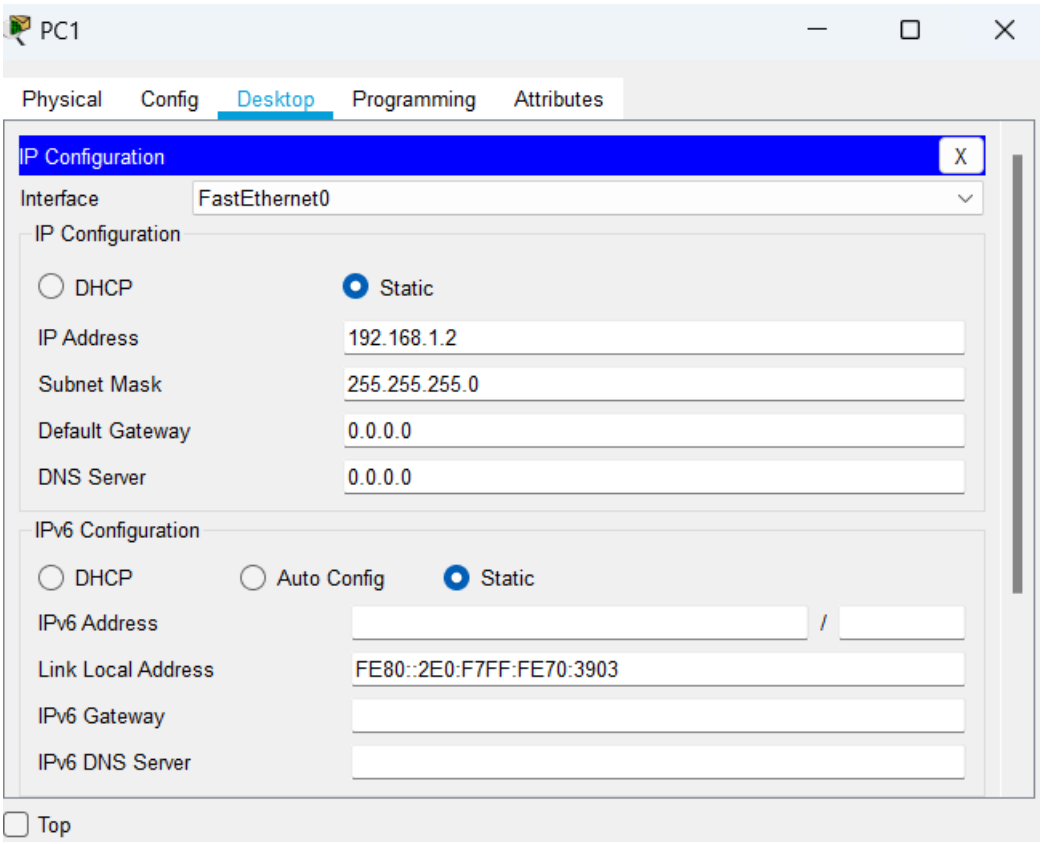


Step-1:

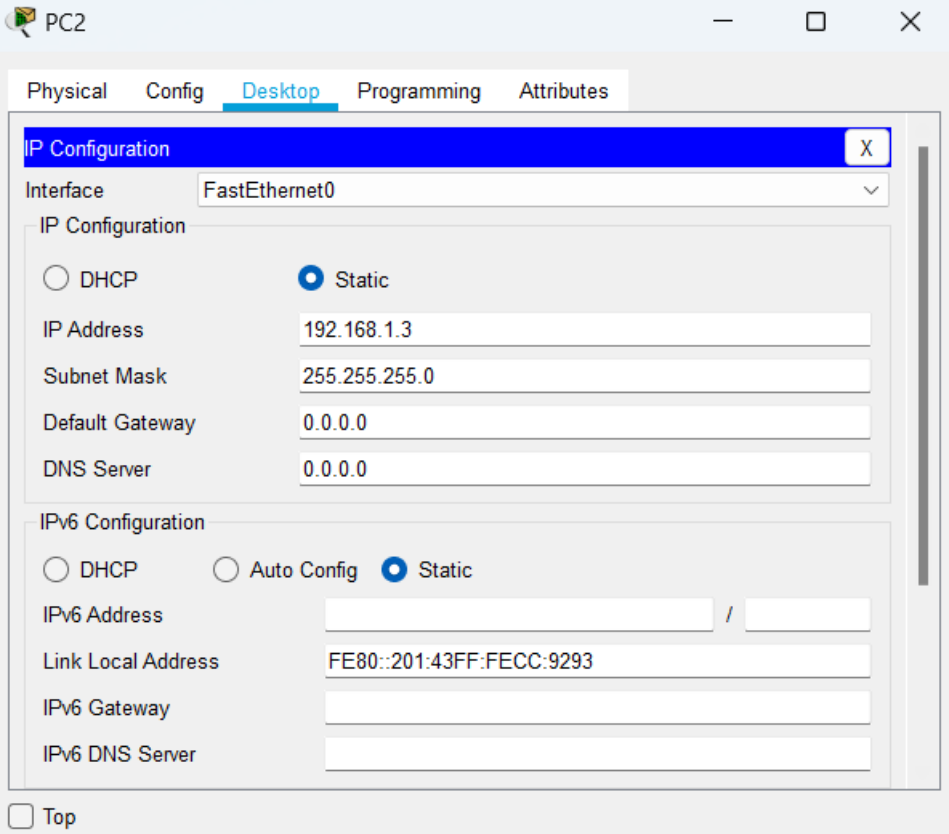
Configure PC0



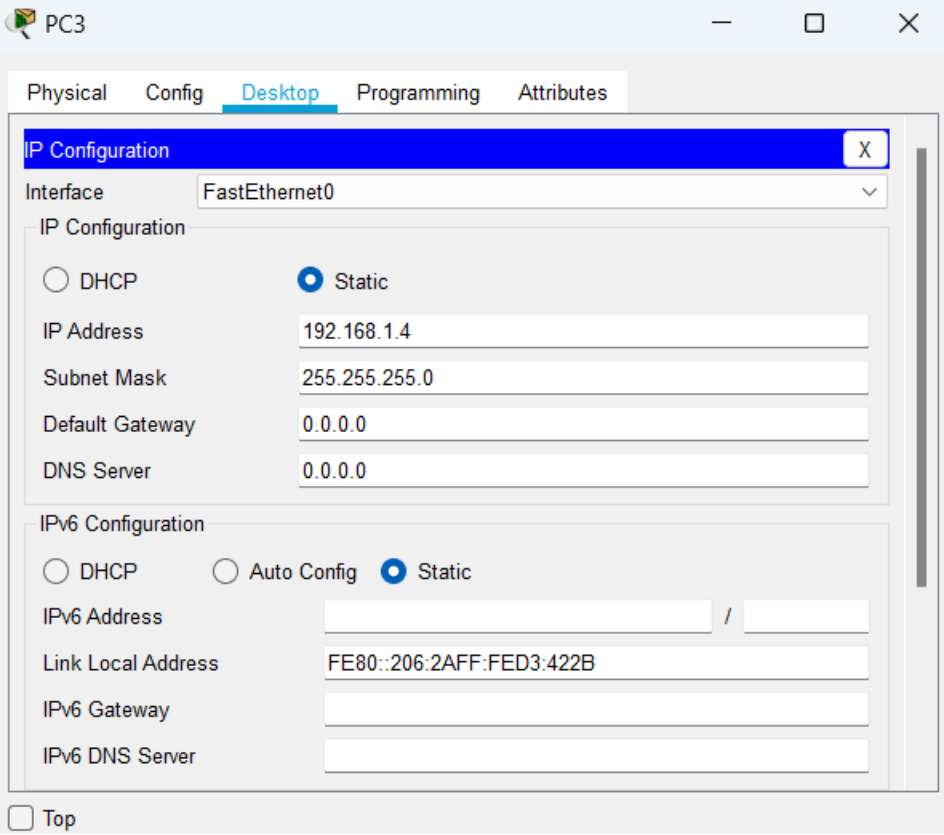
Configure PC1



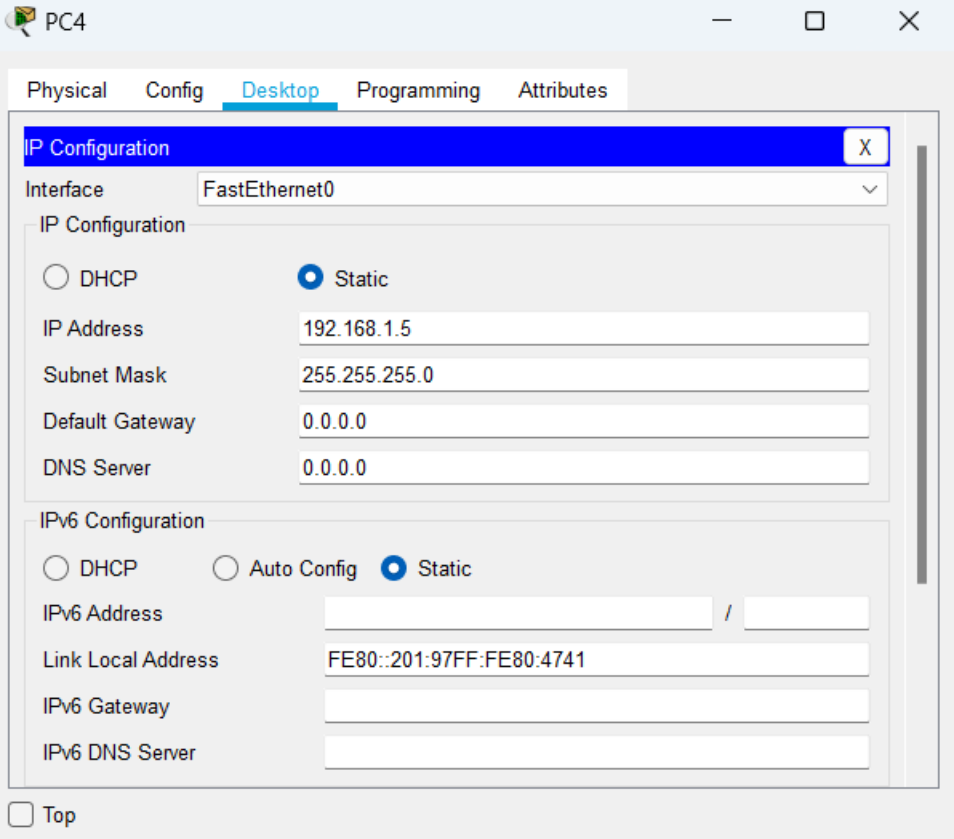
Configure PC2



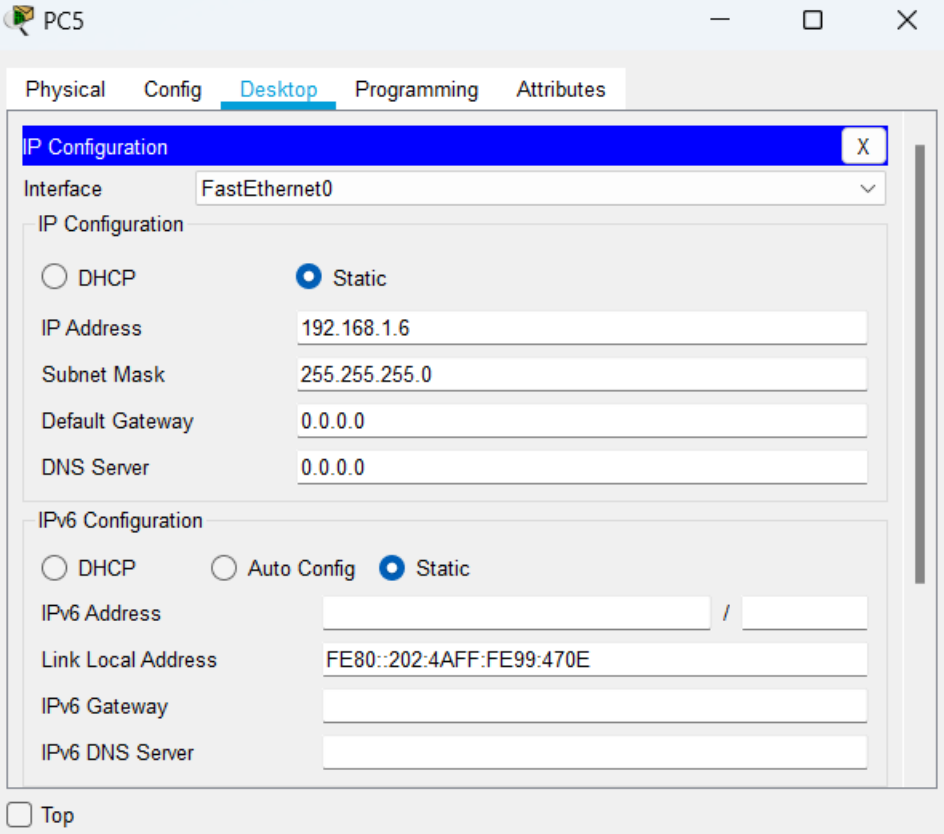
Configure PC3



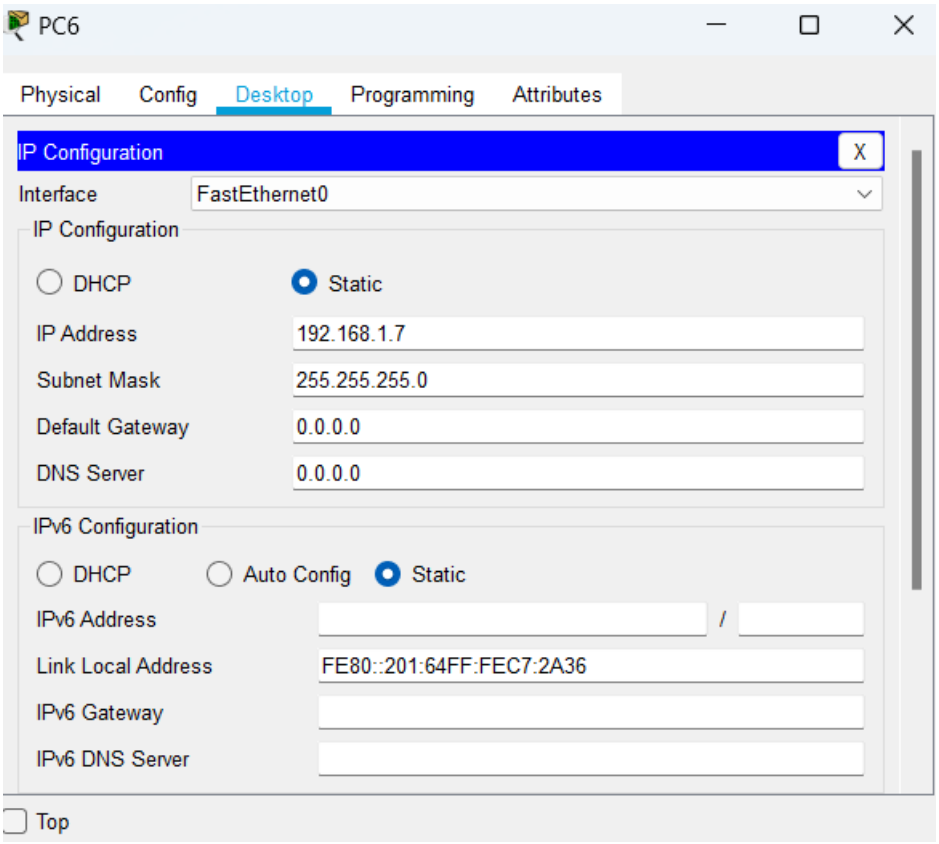
Configure PC4



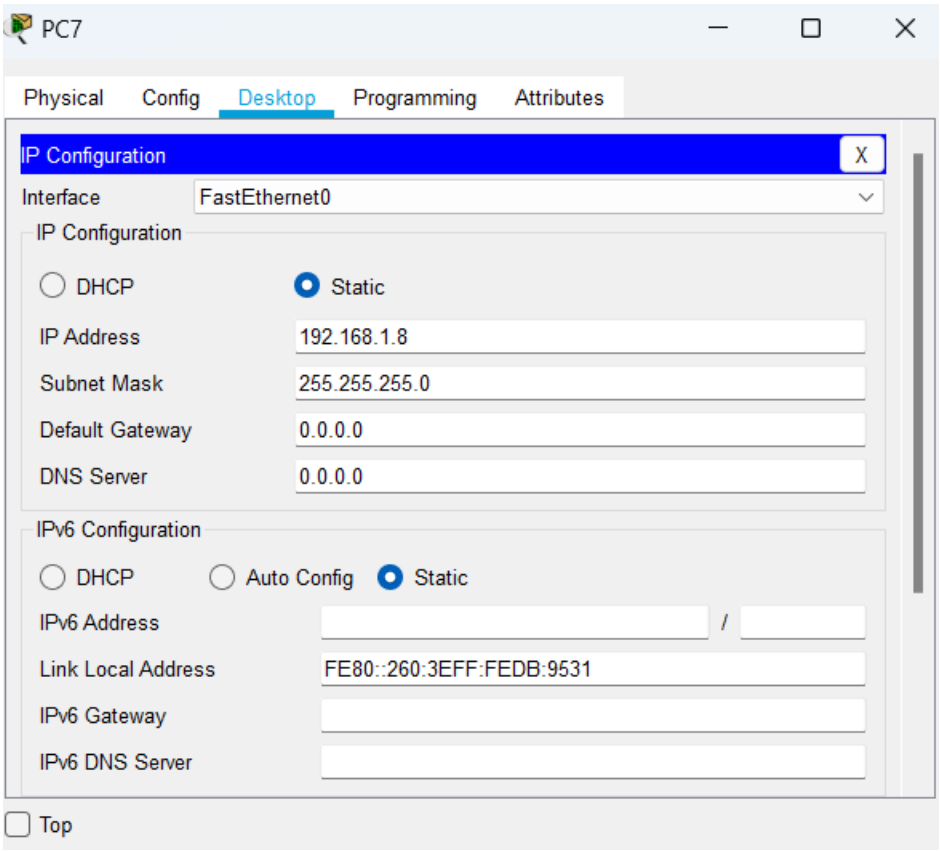
Configure PC5



Configure PC6



Configure PC7



Step-2:

Create VLAN on Switch0

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name up
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name down
Switch(config-vlan)#do sh vlan br

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24
Gig0/1, Gig0/2
10 up active
20 down active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Switch(config-vlan)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#int f0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#

Create VLAN on Switch1

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name up
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name down
Switch(config-vlan)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#int f0/4

Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#

Connecting two switches to allow data from 2 VLANs

On switch0

Switch(config-if)#int f0/5
Switch(config-if)#switchport mode trunk

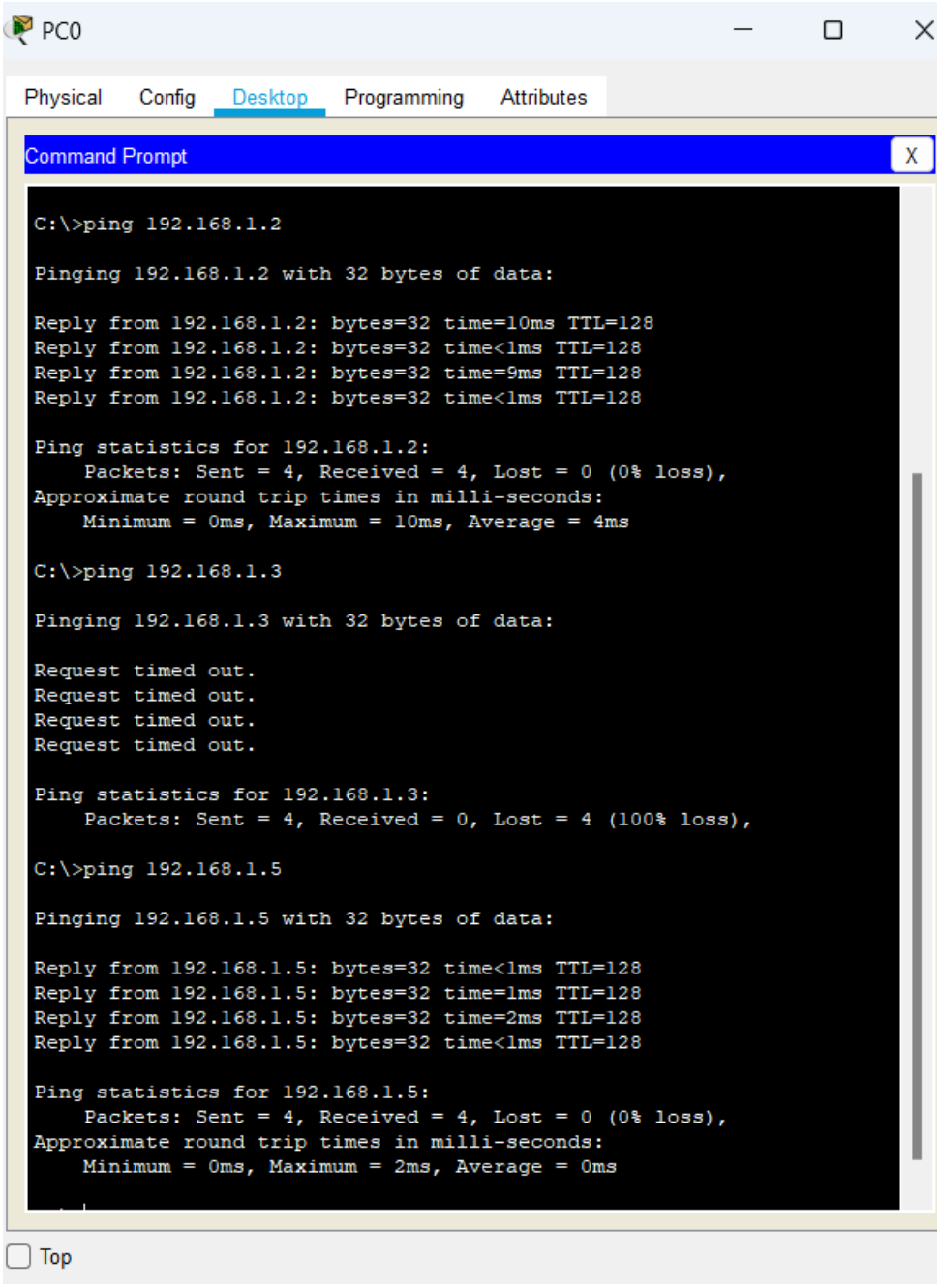
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

On Switch1

Switch(config-if)#int f0/5
Switch(config-if)#switchport mode trunk
Switch(config-if)#

Output:

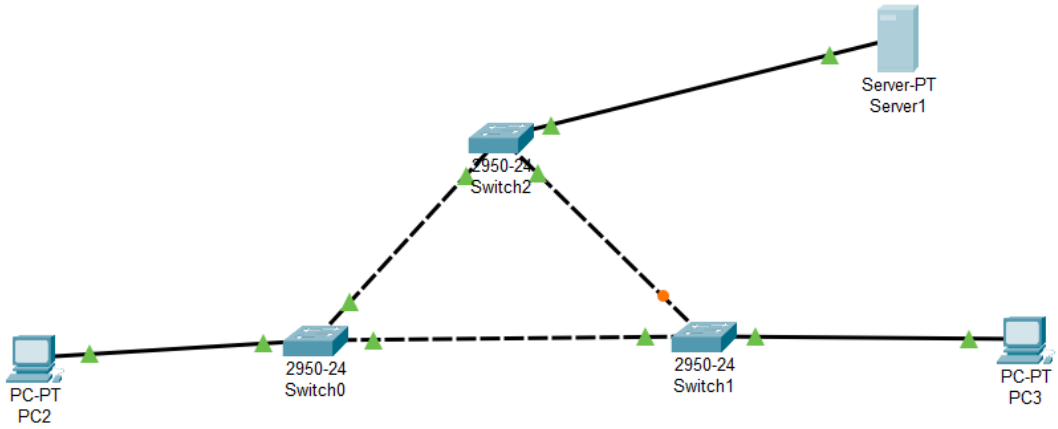

PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=10ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=9ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
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 = 10ms, Average = 4ms
C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.1.5
Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=2ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms
Top

Practical -4

Aim: - Observe STP Topology Changes and Implement RSTP

Requirements: 1 Server, 3 Switches, 2 End devices

Topology:



Steps :

1-Create topology as shown in the figure

2-Give IP address to server as 192.168.1.1

Default gateway 192.168.1.1

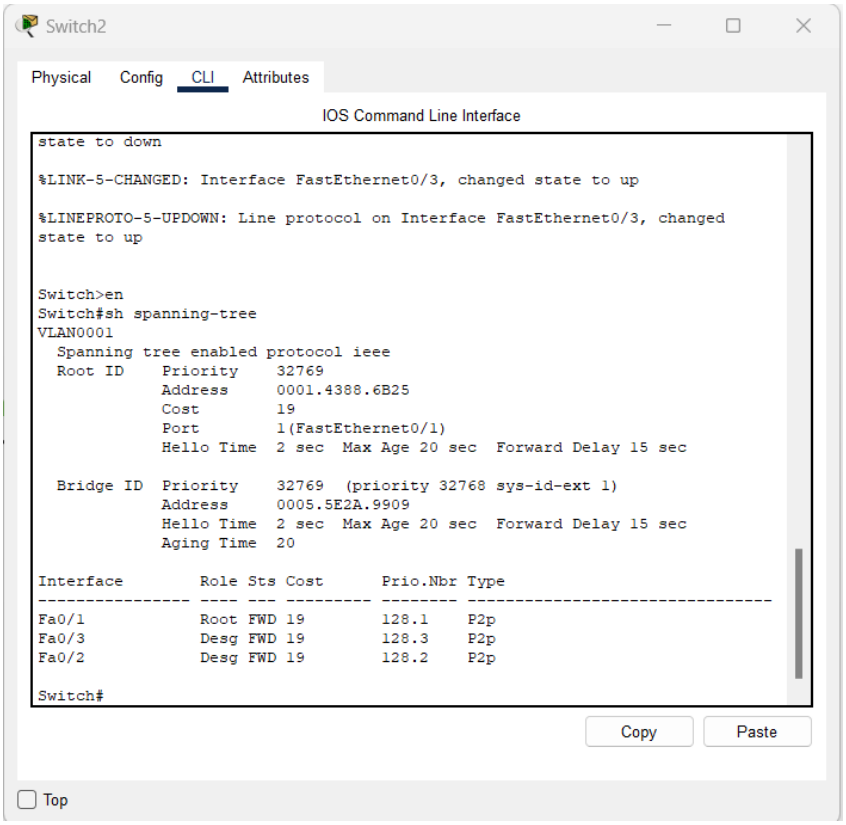
Give same series IP to other 2 end devices

3- Open CLI of switch 2 and type the following

Switch>en

Switch#sh spanning tree

We will get following result

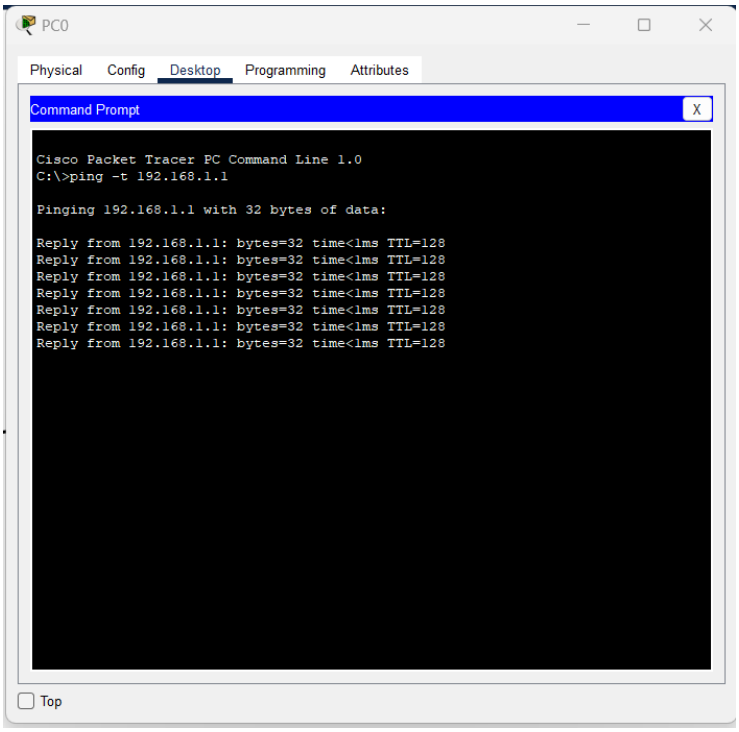


4- Do the same for other 2 switches.

5-Now go to pc0 and in command prompt type following command

C:\>ping -t 192.168.1.1

We will be able to see the data packets are reaching the server



6- configuration in Switch0

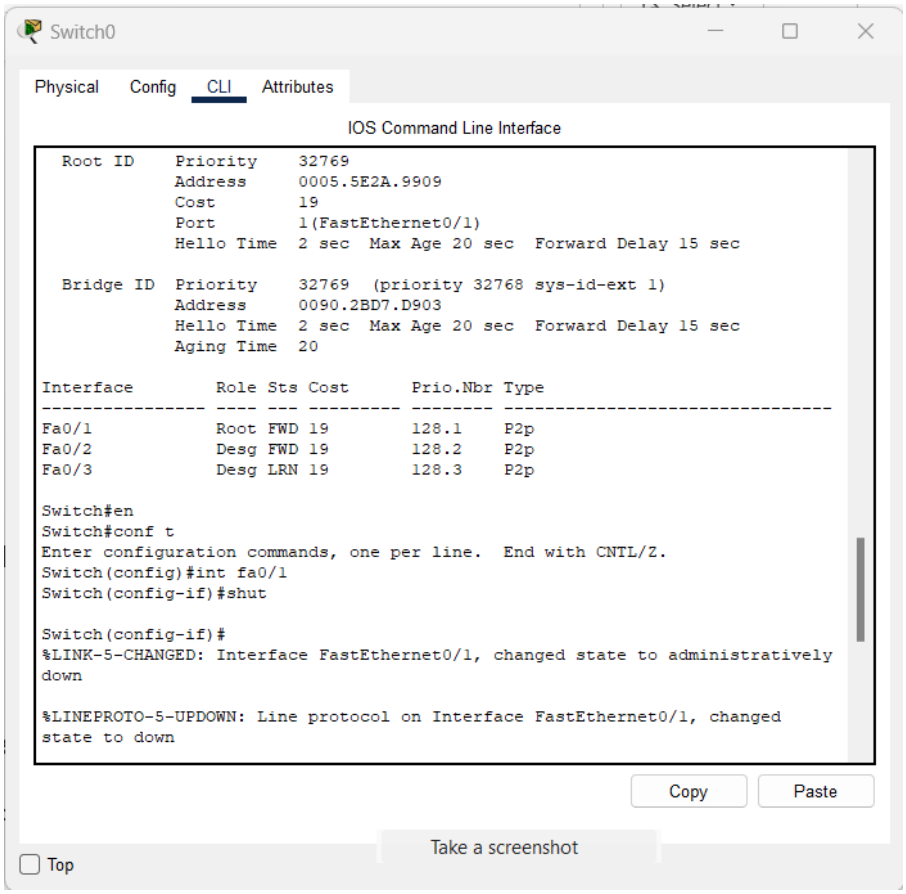
Now again in switch0 type following commands

Switch>en

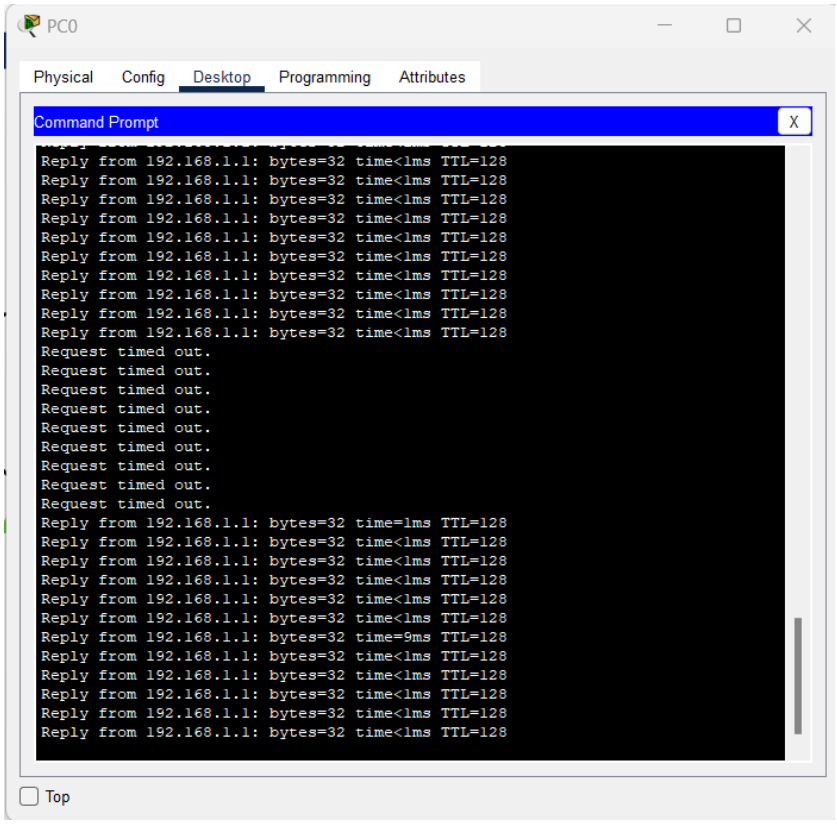
Switch#conf t

Switch(config)#int fa0/1

Switch(config-if)#shut



In following figure you can observe that at the beginning package was deliver successfully but as soon as we pass shutdown command in CLI of switch0. After some time, the switch will search for other available path and start sending the data packets. This is the demonstration of Spanning tree



2-Implementation of RSTP

For that we need to change our all switches to the RSTP

1-congifuration in switches
Open CLI of switch2

And type following commands

switch#en

switch#conf t

You will enter into Global conf

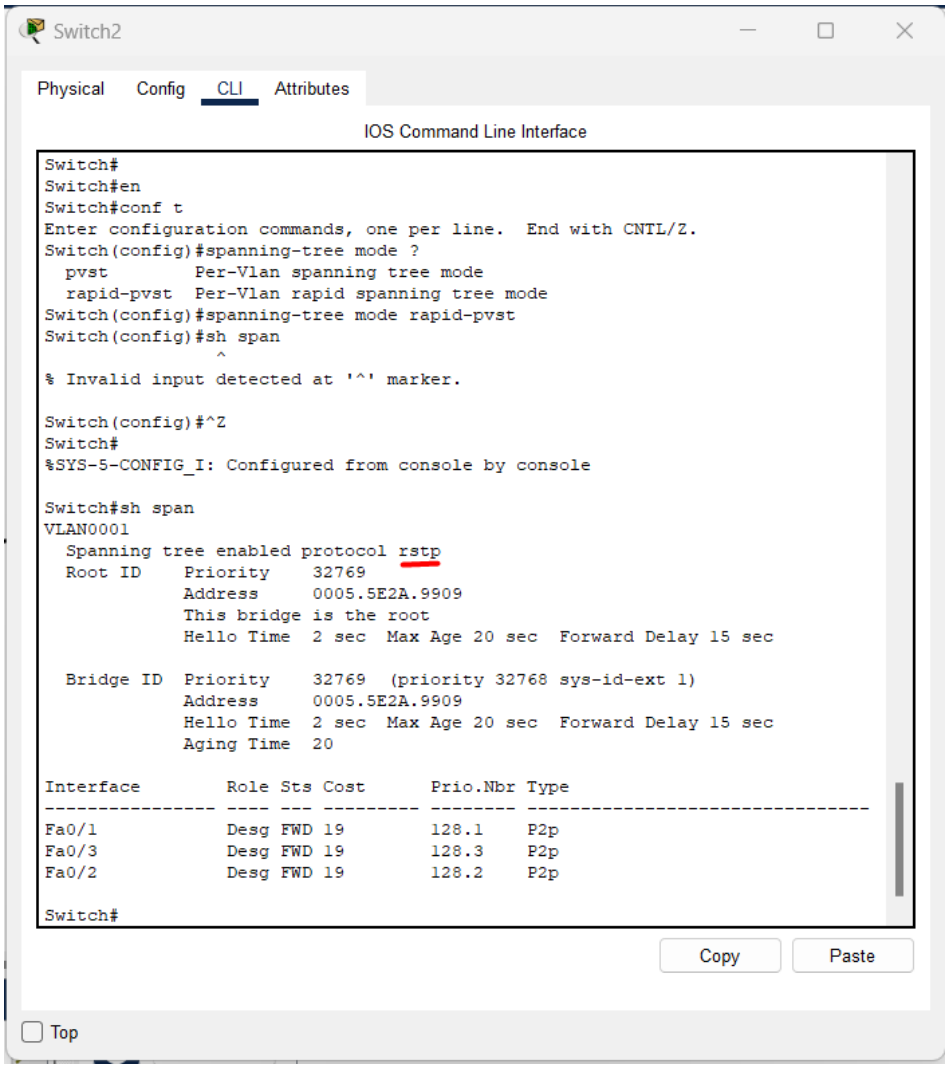
Switch(config)#spanning-tree mode ?

Switch(config)#spanning-tree mode rapid-pvst

Switch(config)# ^z **(Note: press ctrl + z)**

Switch(config)#sh span

You can see that in figure the mode of spanning tree is change to RSTP

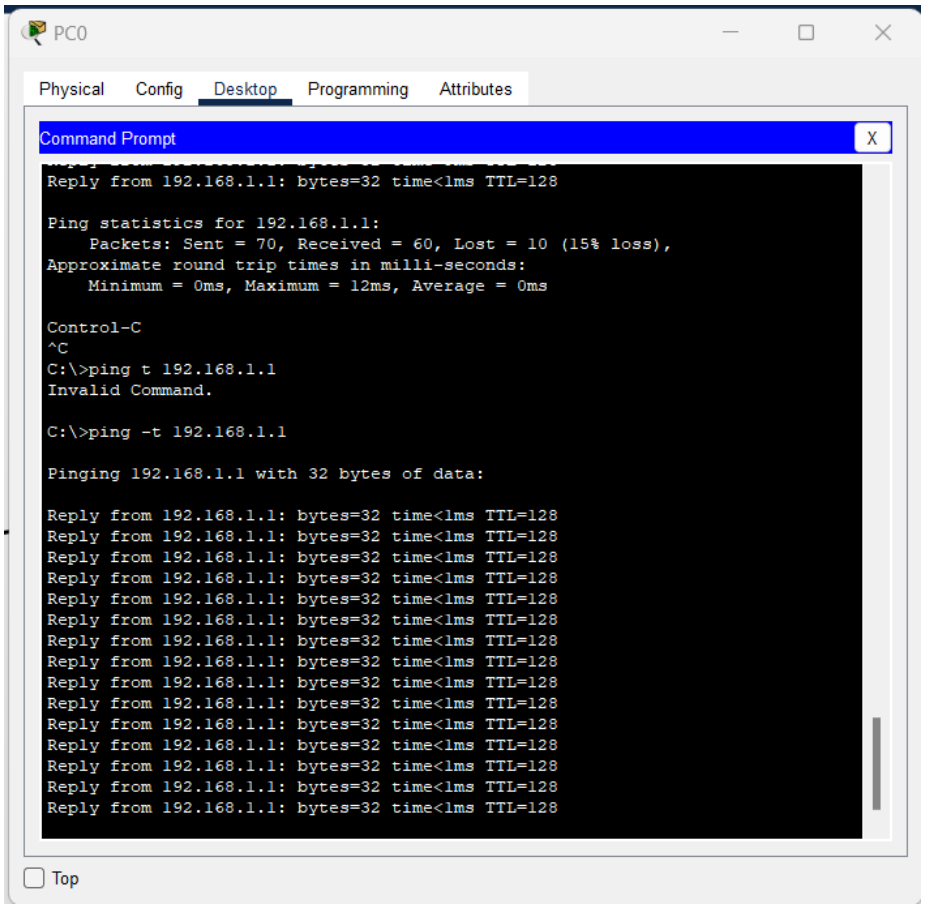


Apply this same process to all other switches

2-Once RSTP is set. From PC0

ping –t 192.168.1.1

When the reply is positive



on switch 0 do

switch#en

switch#conf t

Switch(config)#int fa0/1

Switch(config-if)#shutdown

After giving command shutdown package get stopped.

Practical -5

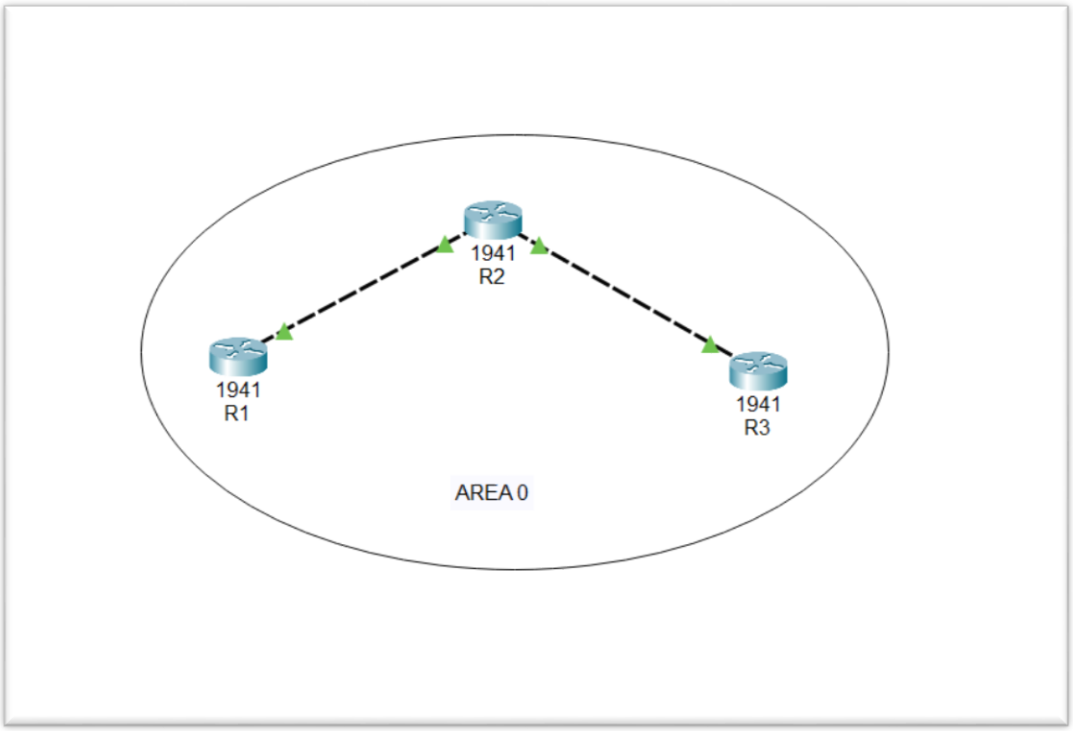
Aim: OSPF Implementation

1. Implement Single Area OSPFv2
2. Implement Multi Area OSPFv2

SOLUTION:

1. Implement Single Area OSPFv2

TOPOLOGY 1:



Steps:

Configuration table:

Devices	Interface	IP-address	Subnet mask
R1	Gig0/0	10.10.10.1	255.255.255.0
R2	Gig0/0	10.10.10.2	255.255.255.0
	Gig0/1	20.20.20.2	255.255.255.0
R3	Gig0/0	20.20.20.1	255.255.255.0

On router R1 perform the following commands

Router#en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#router ospf 1

Router(config-router)#network 10.10.10.0 0.0.0.255 area 0

Router(config-router)#

00:11:39: %OSPF-5-ADJCHG: Process 1, Nbr 20.20.20.2 on GigabitEthernet0/0 from LOADING to FULL, Loading Done

On router R2 perform the following commands

Router(config-router)#network 10.10.10.0 0.0.0.255 area 0

Router(config-router)#network 20.20.20.0 0.0.0.255 area 0

Router(config-router)#

00:12:57: %OSPF-5-ADJCHG: Process 1, Nbr 20.20.20.1 on GigabitEthernet0/1 from LOADING to FULL, Loading Done

On router R3 perform the following commands

ospf 1

Router(config-router)#network 20.20.20.0 0.0.0.255 area 0

Router(config-router)#

00:12:54: %OSPF-5-ADJCHG: Process 1, Nbr 20.20.20.2 on GigabitEthernet0/0 from LOADING to FULL, Loading Done

Now let's ping from router R1 to R2 and R3

Router(config)#do ping 10.10.10.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Router(config)#do ping 20.20.20.1

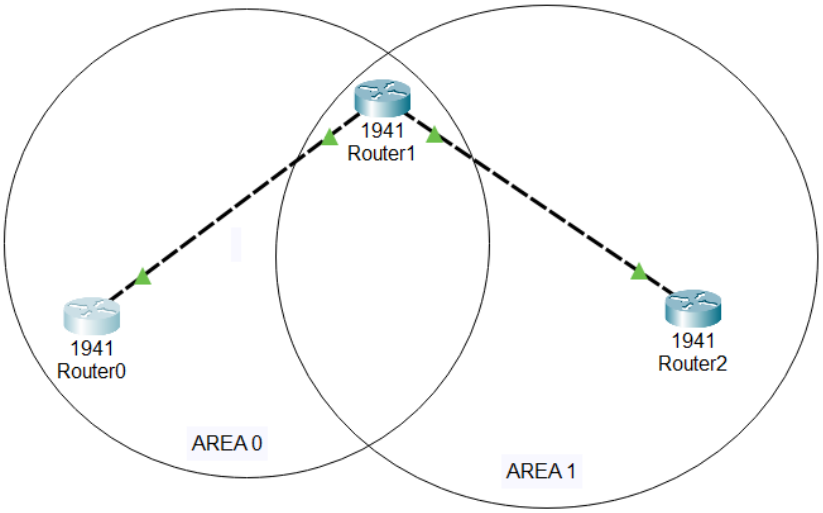
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 20.20.20.1, timeout is 2 seconds:

!!!!!

Implement Multi Area OSPFv2

TOPOLOGY 2:



Steps:

Configuration table:

Devices	Interface	IP-address	Subnet mask
R1	Gig0/0	10.10.10.1	255.255.255.0
R2	Gig0/0	10.10.10.2	255.255.255.0

	Gig0/1	20.20.20.2	255.255.255.0
R3	Gig0/0	20.20.20.1	255.255.255.0

On router R1 perform the following commands:

Router#en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#router ospf 1

Router(config-router)#network 10.10.10.0 0.0.0.255 area 0

Router(config-router)#

00:09:44: %OSPF-5-ADJCHG: Process 1, Nbr 20.20.20.2 on GigabitEthernet0/0 from LOADING to FULL, Loading Done

On router R2 perform the following commands:

Router(config)#router ospf 1

Router(config-router)#network 10.10.10.0 0.0.0.255 area 0

Router(config-router)#

00:09:42: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.1 on GigabitEthernet0/0 from LOADING to FULL, Loading Done

Router(config-router)#network 20.20.20.0 0.0.0.255 area 1

Router(config-router)#

00:11:20: %OSPF-5-ADJCHG: Process 1, Nbr 20.20.20.1 on GigabitEthernet0/1 from LOADING to FULL, Loading Done

On router R3 perform the following commands:

Router(config)#router ospf 1

Router(config-router)#network 20.20.20.0 0.0.0.255 area 1

Router(config-router)#

00:11:17: %OSPF-5-ADJCHG: Process 1, Nbr 20.20.20.2 on GigabitEthernet0/0 from LOADING to FULL, Loading Done

Now let's ping from router R1 to R2 and R3

Router(config)#do ping 10.10.10.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router(config)#do ping 20.20.20.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 20.20.20.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

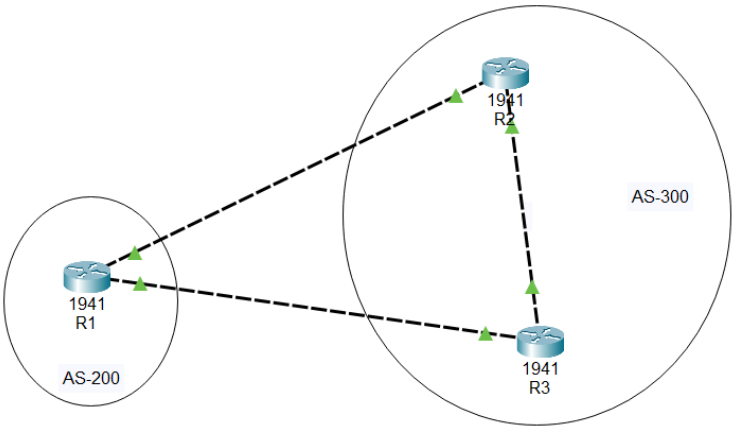
Practical -6

AIM: Implement BGP communities:

1.Implement EBGP

2.Implement IBGP

TOPOLOGY 1 :



Steps:

Configuration Table:

Devices	Interface	Ip-address	Subnet mask
R1	Gig0/0	192.168.1.1	255.255.255.0
	Gig0/1	192.168.2.1	255.255.255.0
R2	Gig0/0	192.168.1.2	255.255.255.0
	Gig0/1	192.168.3.2	255.255.255.0
R3	Gig0/0	192.168.3.1	255.255.255.0
	Gig0/0	192.168.2.2	255.255.255.0

On router R2 perform following commands:

Router(config)#router eigrp 1

Router(config-router)#network 192.168.3.0

Router(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.3.1 (GigabitEthernet0/1) is up: new adjacency

On router R3 perform the following commands:

Router(config)#router eigrp 1

Router(config-router)#network 192.168.3.0

Router(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.3.2 (GigabitEthernet0/0) is up: new adjacency

On router R1 perform the following the command:

Router(config)#router bgp 200

Router(config-router)#network 10.10.10.0

Router(config-router)#neighbor 192.168.1.2 remote-as 300

Router(config-router)#neighbor 192.168.2.2 remote-as 300

Router(config-router)#do show ip bgp summary

BGP router identifier 10.10.10.10, local AS number 200

BGP table version is 1, main routing table version 6

0 network entries using 0 bytes of memory

0 path entries using 0 bytes of memory

0/0 BGP path/bestpath attribute entries using 0 bytes of memory

0 BGP AS-PATH entries using 0 bytes of memory

0 BGP route-map cache entries using 0 bytes of memory

0 BGP filter-list cache entries using 0 bytes of memory

Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory

BGP using 32 total bytes of memory

BGP activity 0/0 prefixes, 0/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd

192.168.1.2 4 300 0 0 1 0 0 00:22:07 4

192.168.2.2 4 300 0 0 1 0 0 00:22:07 4

On router R2 perform the following commands:

Router(config)#router bgp 300

Router(config-router)#network 20.20.20.0

Router(config-router)#neighbor 192.168.1.1 remote-as 200

Router(config-router)#%BGP-5-ADJCHANGE: neighbor 192.168.1.1 Up

Router(config-router)#network 192.168.3.0

Router(config-router)#exit

On router R3 perform the following commands:

Router(config)#router bgp 300

Router(config-router)#network 30.30.30.0

Router(config-router)#network 192.168.3.0

Router(config-router)#neighbor 192.168.2.1 remote-as 200

Router(config-router)#%BGP-5-ADJCHANGE: neighbor 192.168.2.1 Up

Router(config-router)#do show ip bgp summary

BGP router identifier 30.30.30.30, local AS number 300

BGP table version is 2, main routing table version 6

1 network entries using 132 bytes of memory

1 path entries using 52 bytes of memory

0/0 BGP path/bestpath attribute entries using 0 bytes of memory

1 BGP AS-PATH entries using 24 bytes of memory

0 BGP route-map cache entries using 0 bytes of memory

0 BGP filter-list cache entries using 0 bytes of memory

Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory

BGP using 240 total bytes of memory

BGP activity 1/0 prefixes, 1/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd

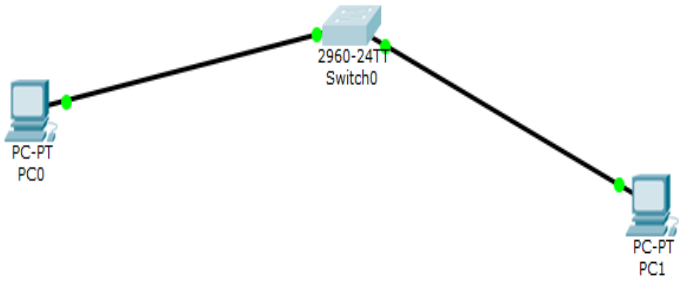
192.168.2.1 4 200 2 2 2 0 0 00:00:20 4

Practical -7

Aim: Implement SPAN Technologies (Switch Port Analyzer)

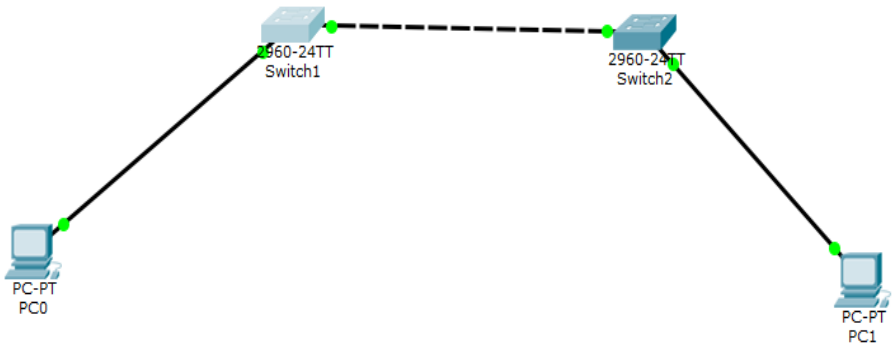
Topology:

Topology 1



Topology 2:

-Implement Remote SPAN configuration



Steps:

For topology 1:

Open CLI

Switch>en
Switch#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#monitor session ?
<1-66>

Switch(config)#monitor session 1 source interface fastEthernet 0/1

Switch(config)#monitor session 1 destination interface fastEthernet 1/1

Switch(config)#^Z

Switch#

%SYS-5-CONFIG_I: Configured from console by console

Switch#show monitor ?
detail
session
| Output Modifiers
<cr>

```
Switch#show monitor session 1
Session 1
---------
Type : Local Session
Description : -
Source Ports :
Both : Fa0/1
Destination Ports : Fa0/2
Encapsulation : Native
Ingress : Disabled
```

```
Switch#show monitor
Session 1
---------
Type : Local Session
Description : -
Source Ports :
Both : Fa0/1
Destination Ports : Fa0/2
Encapsulation : Native
Ingress : Disabled
```

```
Switch#show monitor session 1 detail
Session 1
---------
Type : Local Session
Description : -
Source Ports :
RX Only : None
TX Only : None
Both : Fa0/1
Source VLANs :
RX Only : None
TX Only : None
Both : None
Source RSPAN VLAN : None
Destination Ports : Fa0/2
Encapsulation : Native
```

Ingress : Disabled
Filter VLANs : None
Dest RSPAN VLAN : None

For topology 2:

Open CLI of Switch1

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 8
Switch(config-vlan)#remote-span
Switch(config-vlan)#

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#monitor session 1 source interface fastEthernet0/2

Switch(config)#monitor session 1 destination remote vlan 8 reflector-port fastEthernet 0/5

Switch#en
Switch#show monitor session 1
Session 1

Type : Remote Destination Session
Description : -
Source Ports :
Both : Fa0/2
Dest RSPAN VLAN : 8

Switch#show monitor session 1 detail

```
Session 1
---------
Type : Remote Destination Session
Description : -
Source Ports :
RX Only : None
TX Only : None
Both : Fa0/2
Source VLANs :
RX Only : None
TX Only : None
Both : None
Source RSPAN VLAN : None
Destination Ports : None
Encapsulation : Native
Ingress : Disabled
Filter VLANs : None
Dest RSPAN VLAN : 8


Switch#
```

Switch 2

Open CLI of Switch2

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 8
Switch(config-vlan)#remote-span
Switch(config-vlan)#


Switch>en

Switch#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#monitor session 1 source remote vlan 8
Switch(config)#monitor session 1 destination interface fastEthernet 0/2
Switch(config)#

Switch#en
Switch#show monitor session 1
Session 1
Type : Remote Source Session
Description : -
Source RSPAN VLAN : 8
Destination Ports : Fa0/2
Encapsulation : Native
Ingress : Disabled
Switch#show monitor session 1 detail
Session 1

Type : Remote Source Session
Description : -
Source Ports :
RX Only : None
TX Only : None
Both : None
Source VLANs :

RX Only : None

TX Only : None

Both : None

Source RSPAN VLAN : 8

Destination Ports : Fa0/2

Encapsulation : Native

Ingress : Disabled

Filter VLANs : None

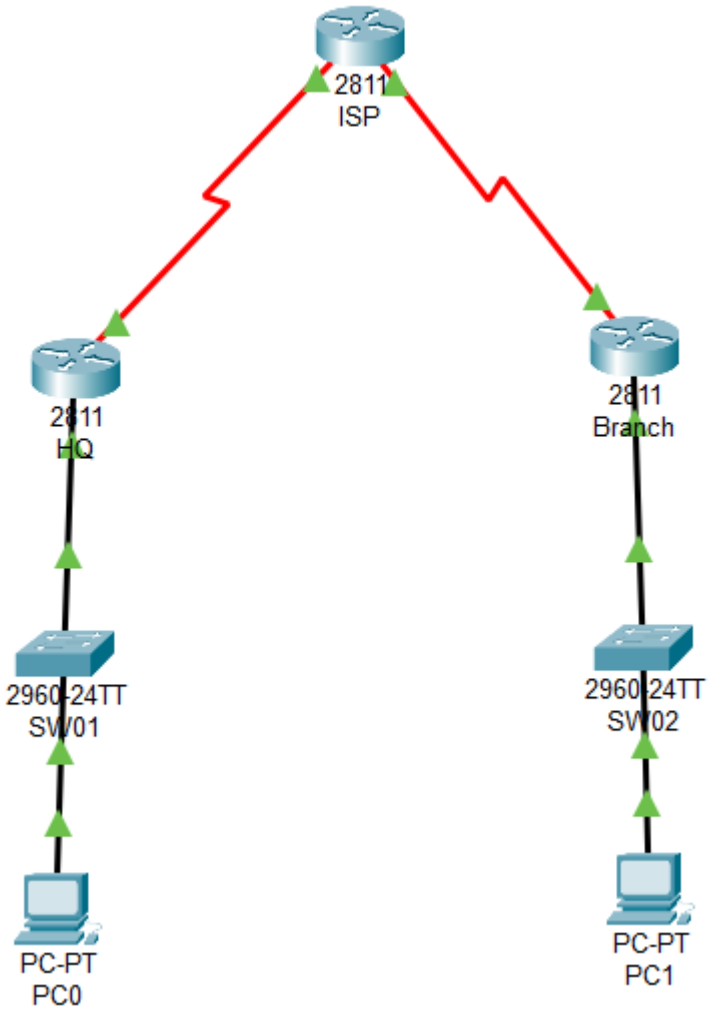
Dest RSPAN VLAN : None

Practical-8

Aim: Implement IPsec Site-to-Site VPNs connection using Cisco Packet Tracer.

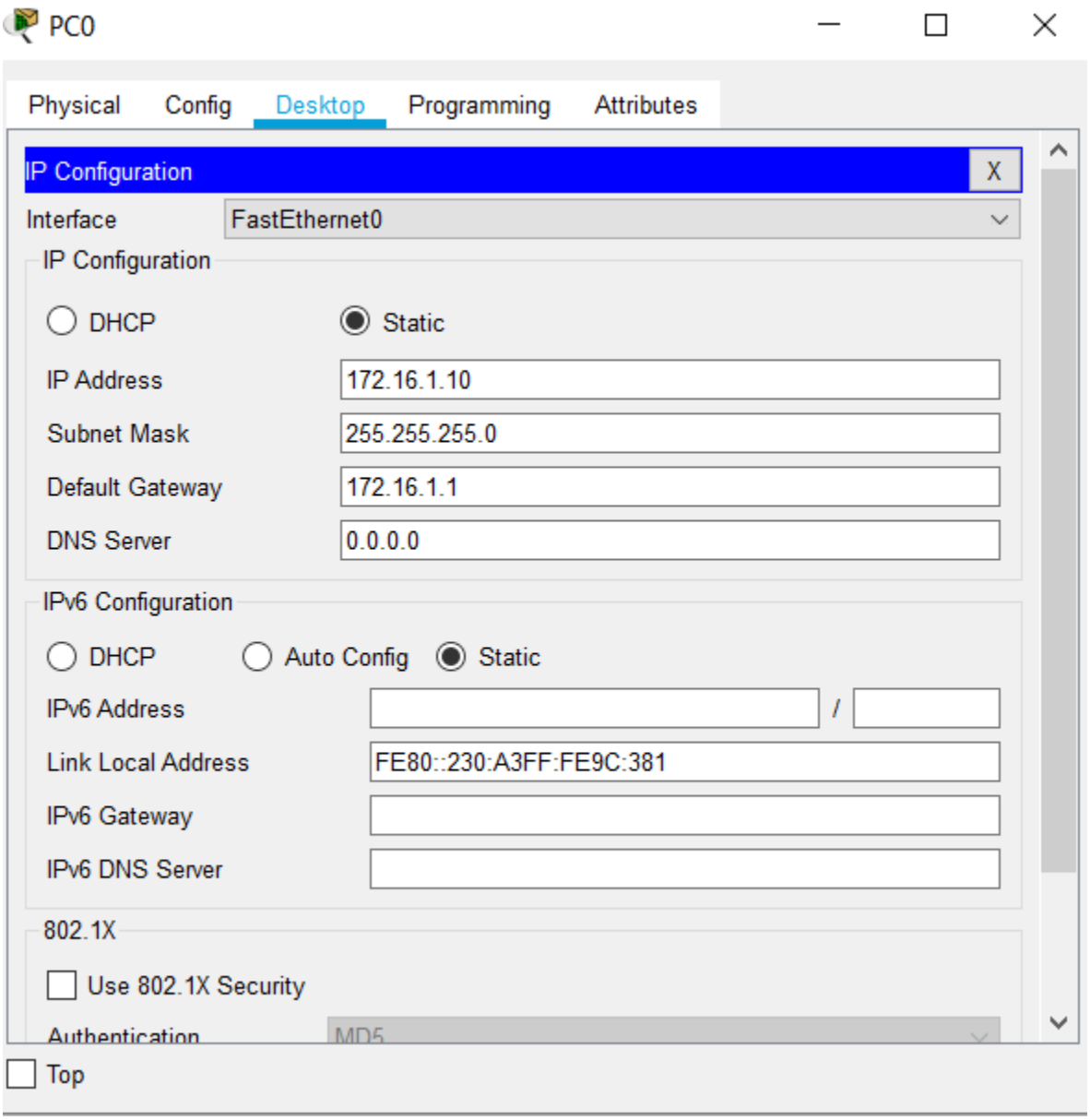
Requirement: 3 routers, 2 switches, PCs

Topology:

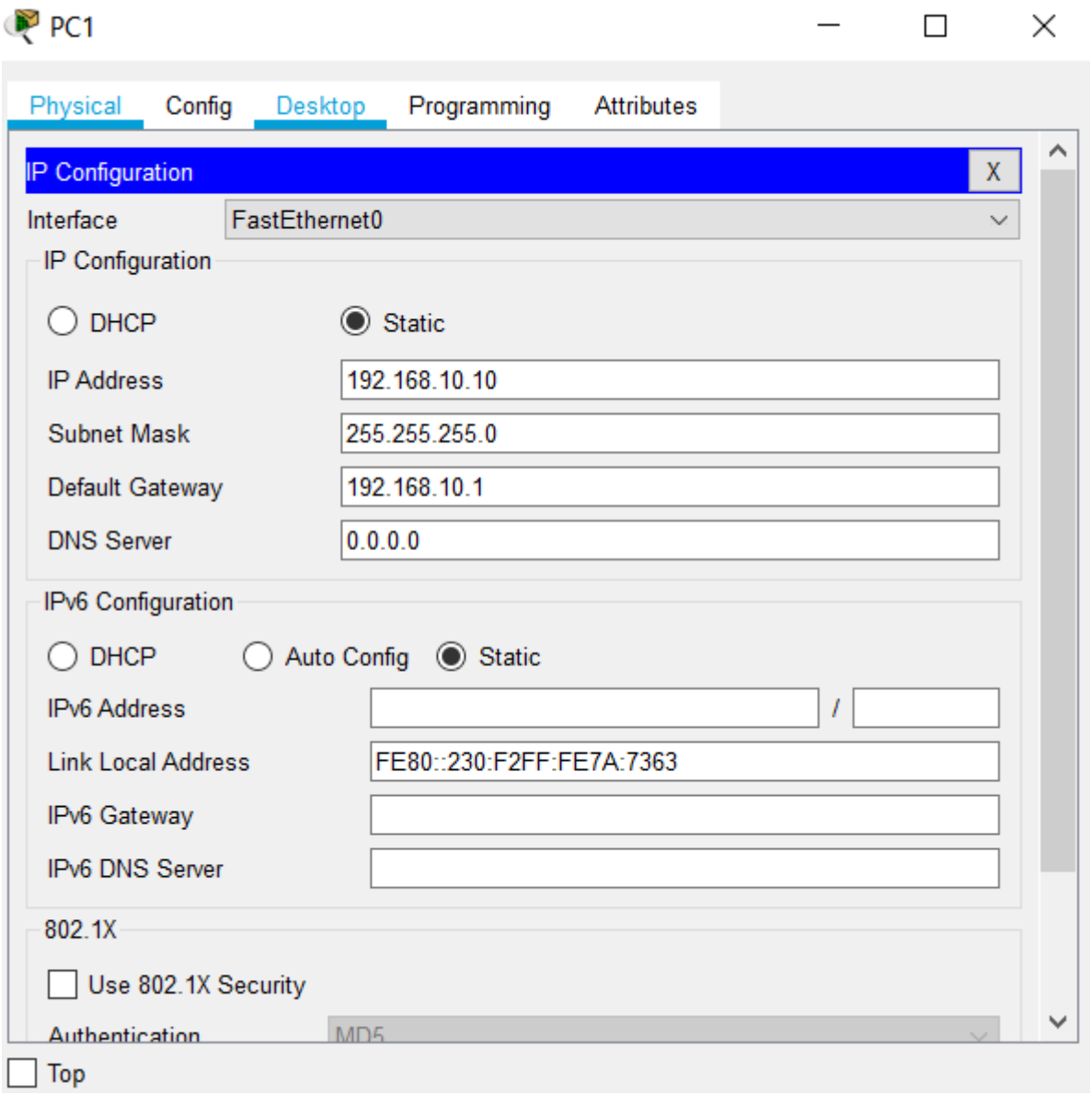


Steps:

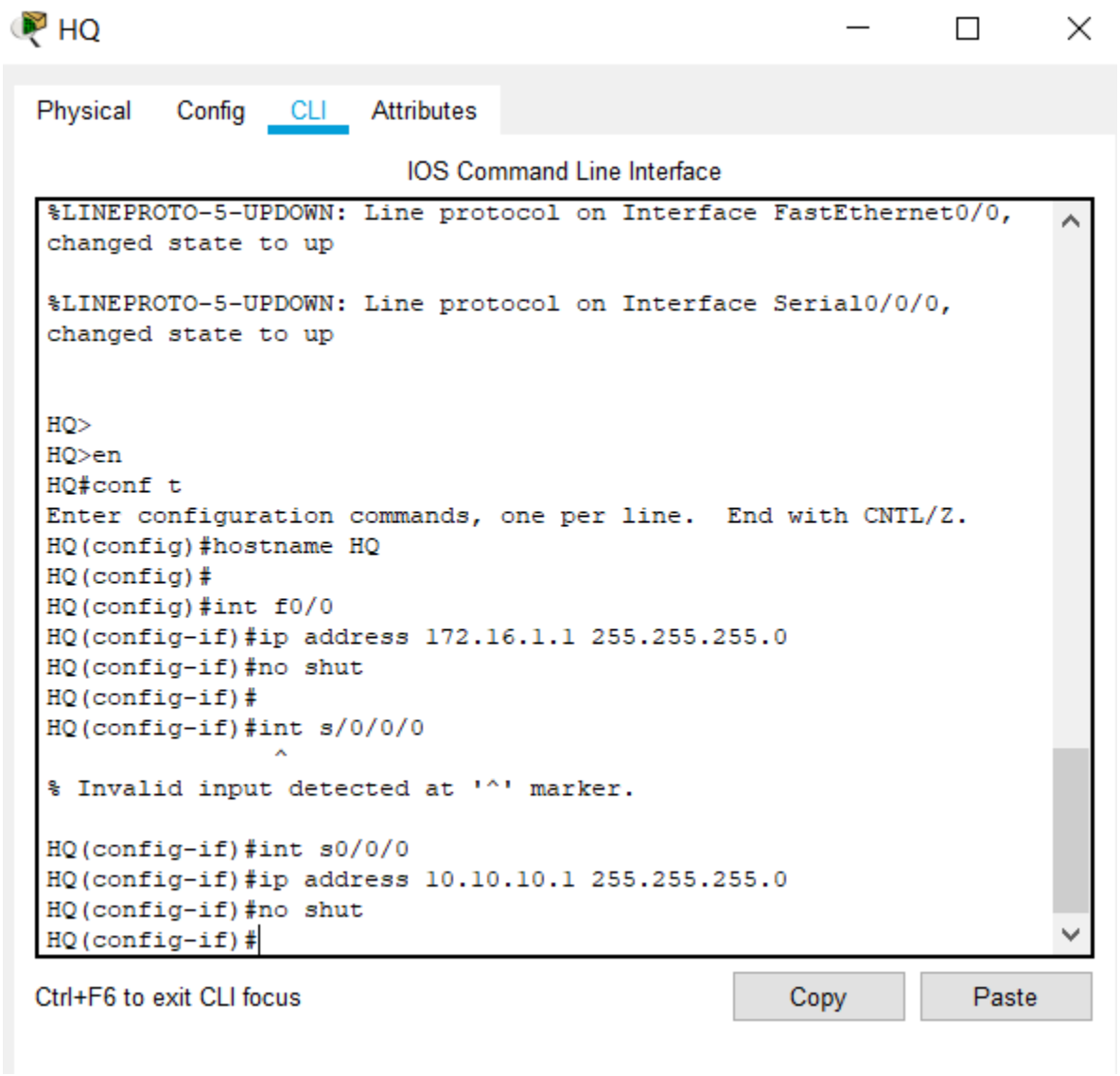
Configure PC0



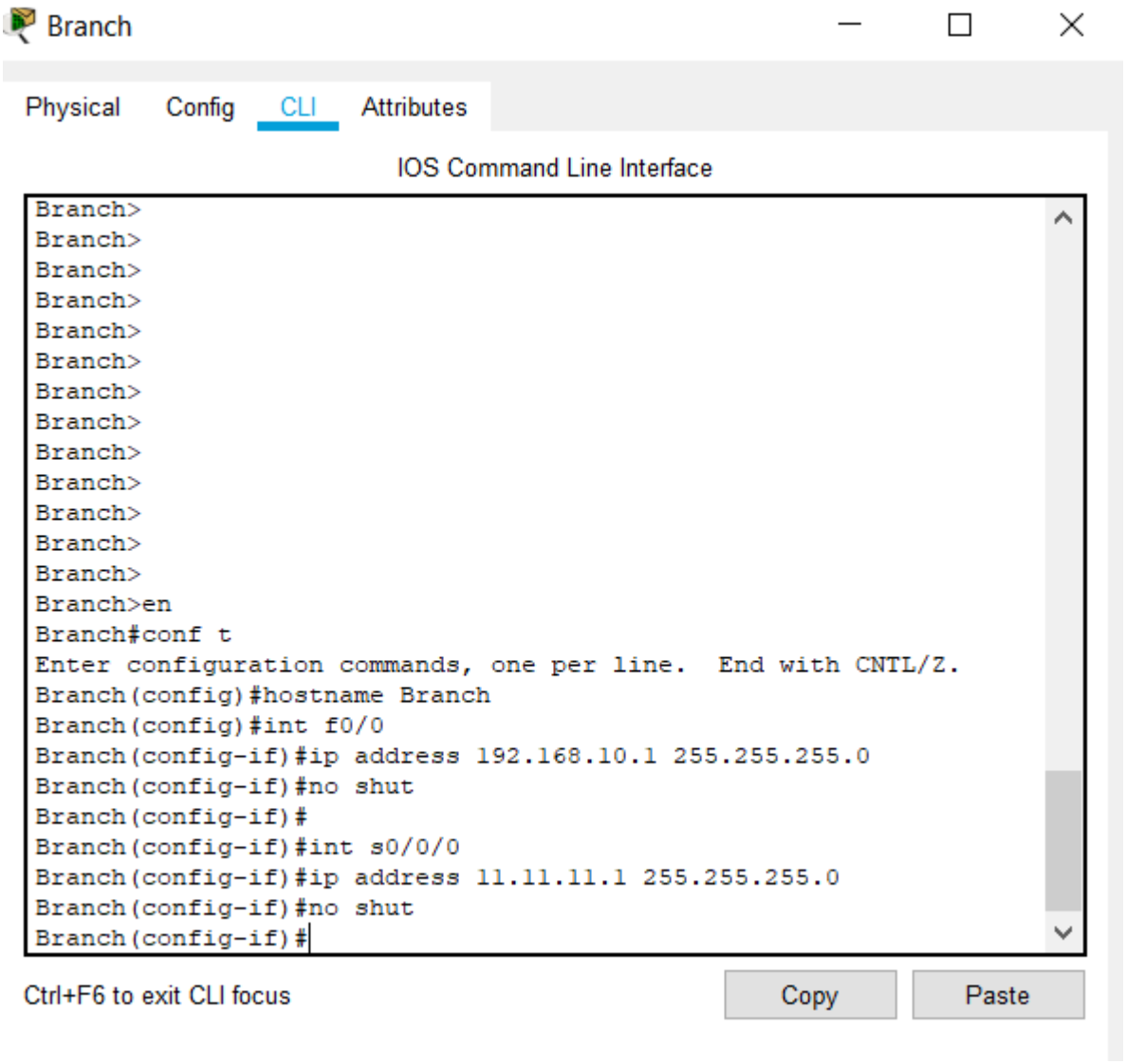
Configure PC1



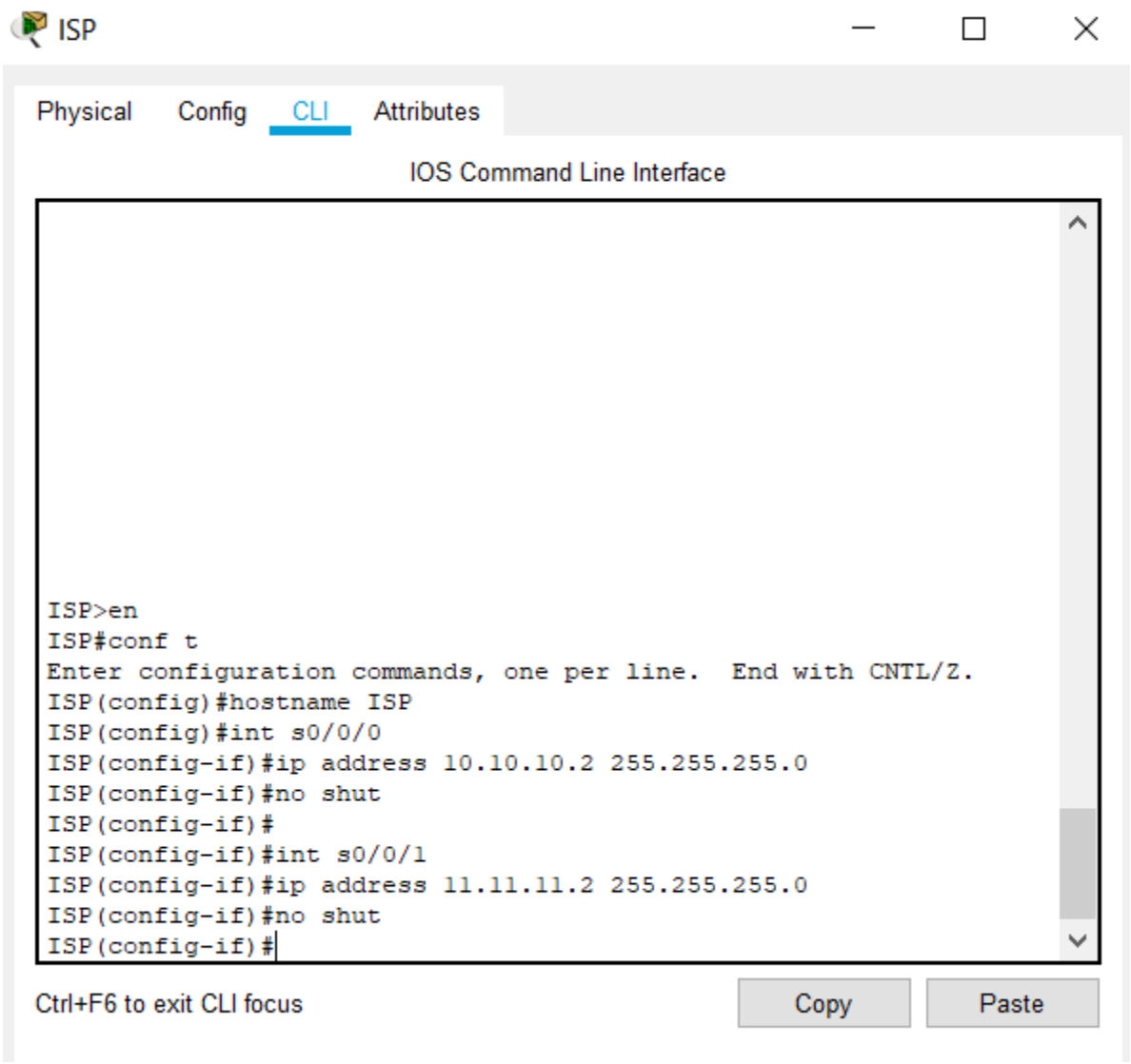
Configure Router HQ



Configure Router Branch



Configure Router ISP



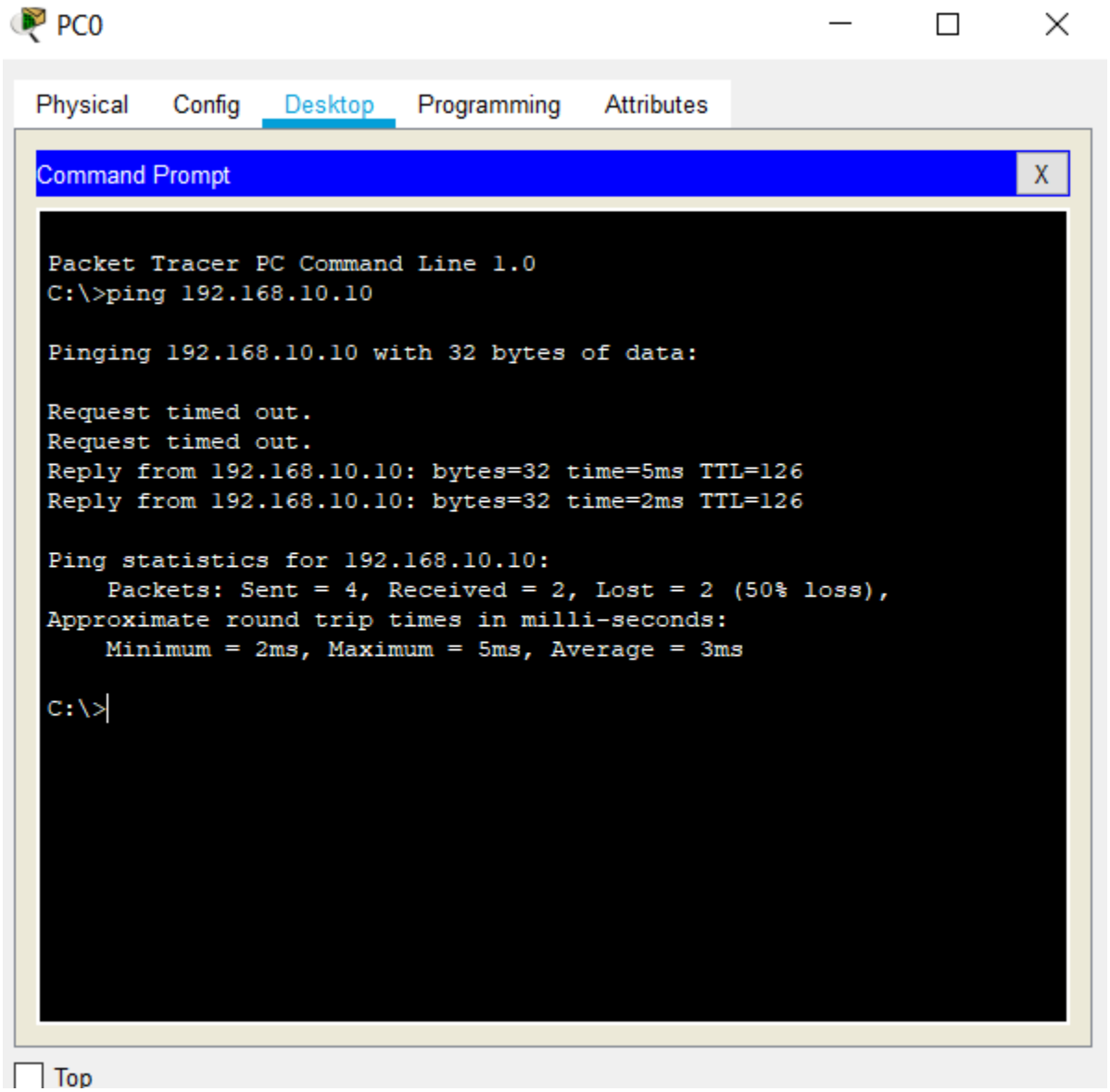
Configure Default Router on HQ, Branch, and Static Router from ISP

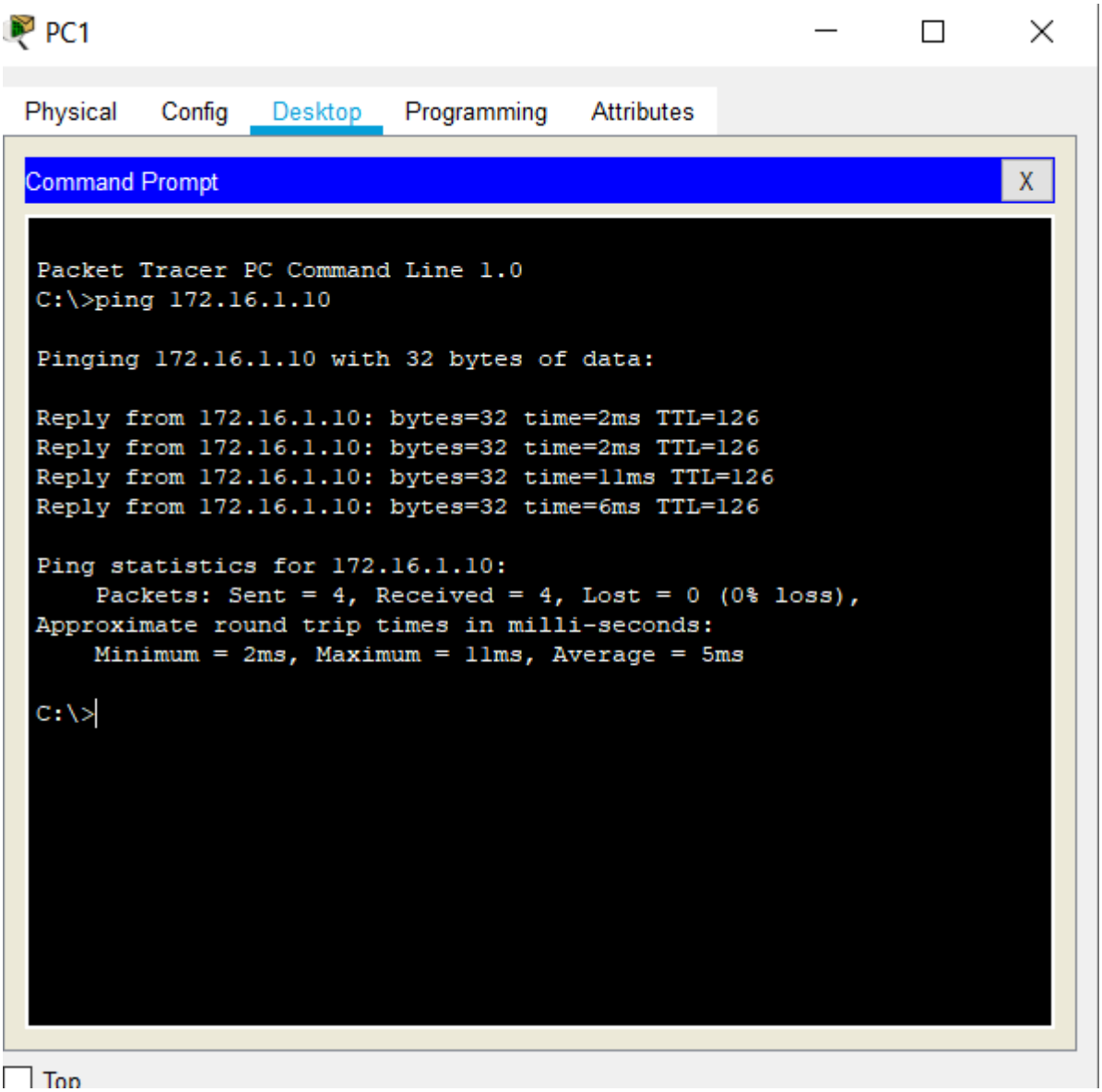
```
HQ(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
HQ(config)#
```

```
Branch(config)#ip route 0.0.0.0 0.0.0.0 11.11.11.2
Branch(config)#
```

```
ISP(config)#ip route 172.16.1.0 255.255.255.0 10.10.10.1
ISP(config)#ip route 192.168.10.0 255.255.255.0 11.11.11.1
ISP(config)#
```

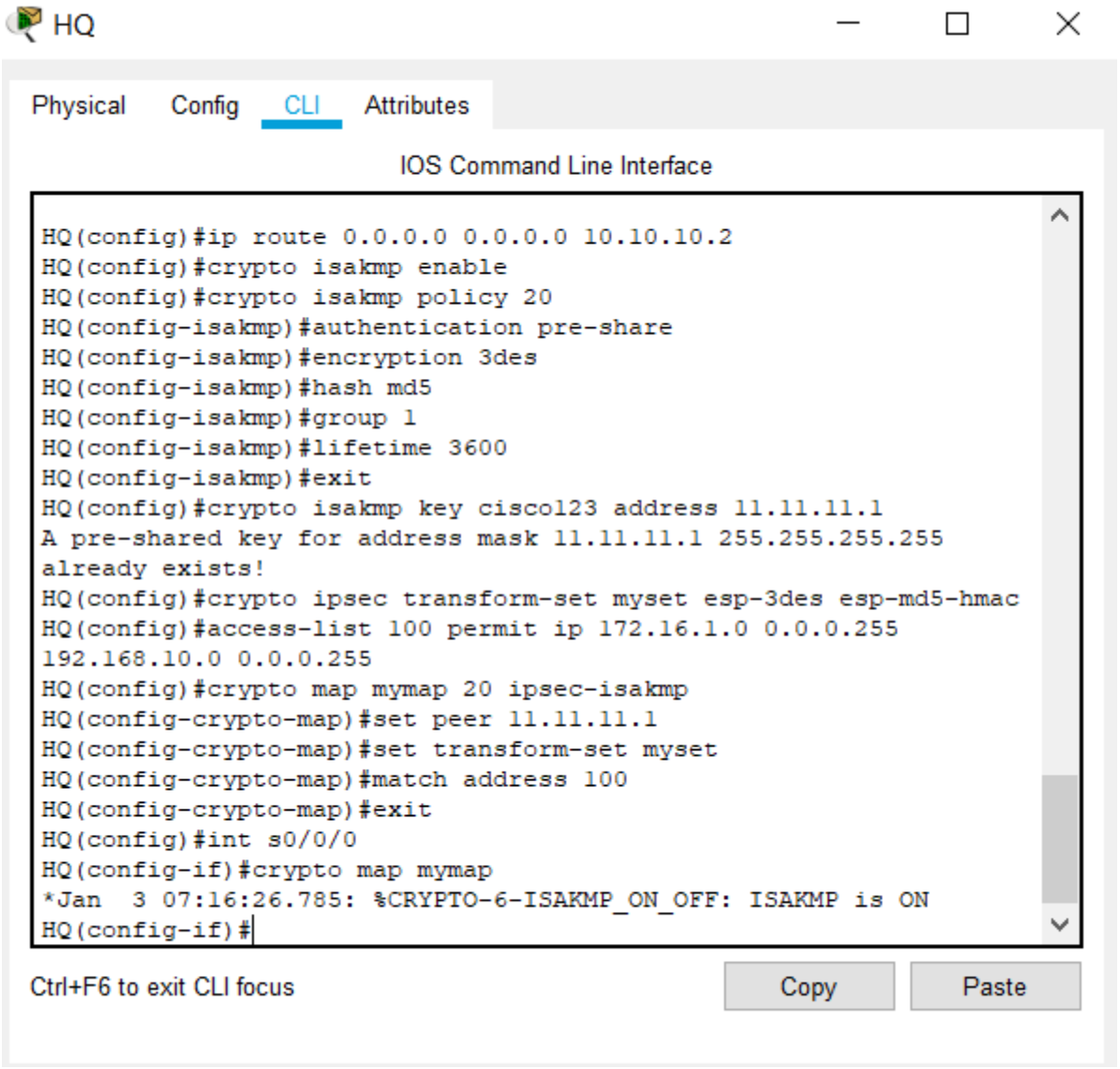
Ping both PCs





Configure VPN site-to-site

HQ

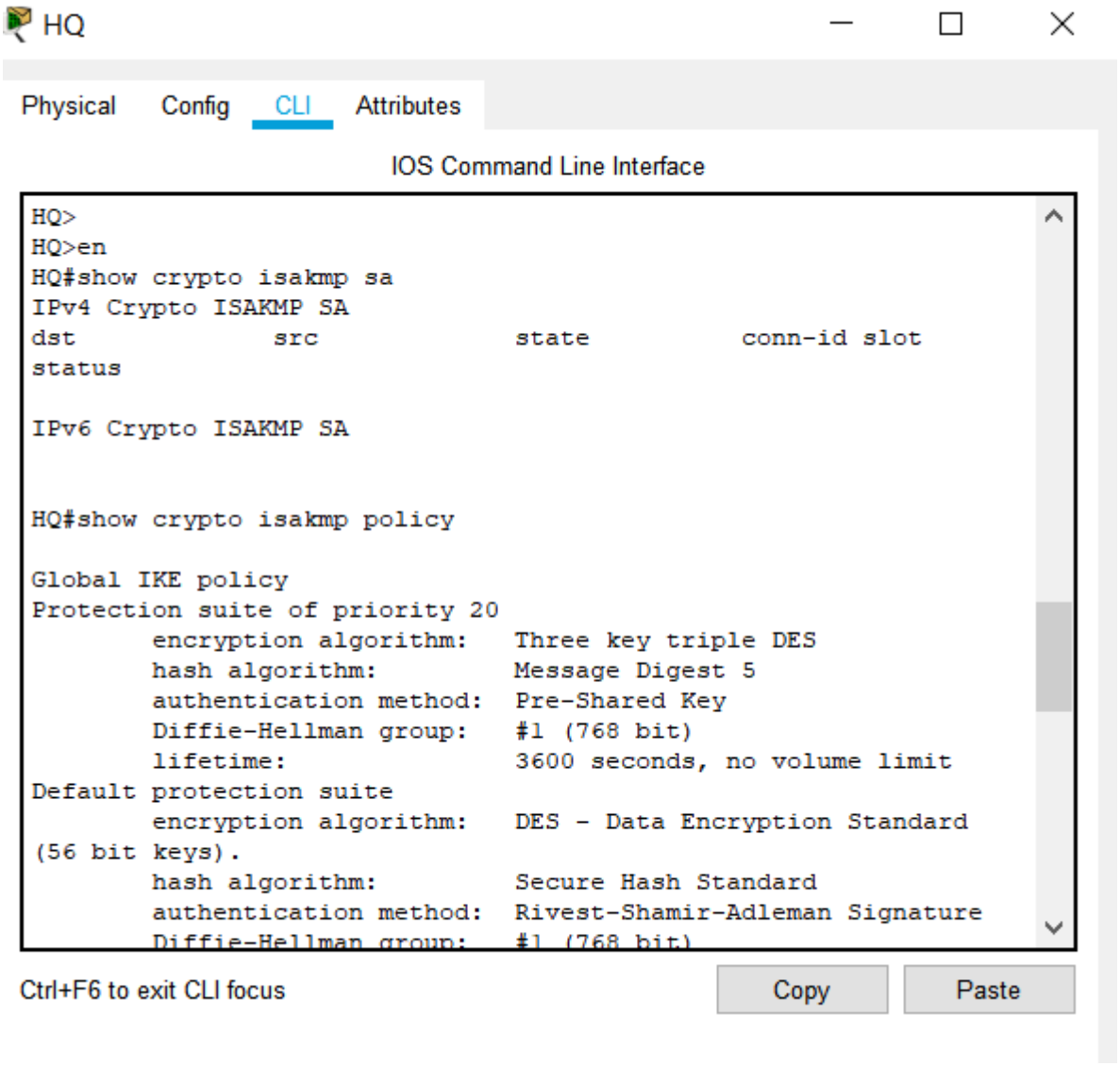


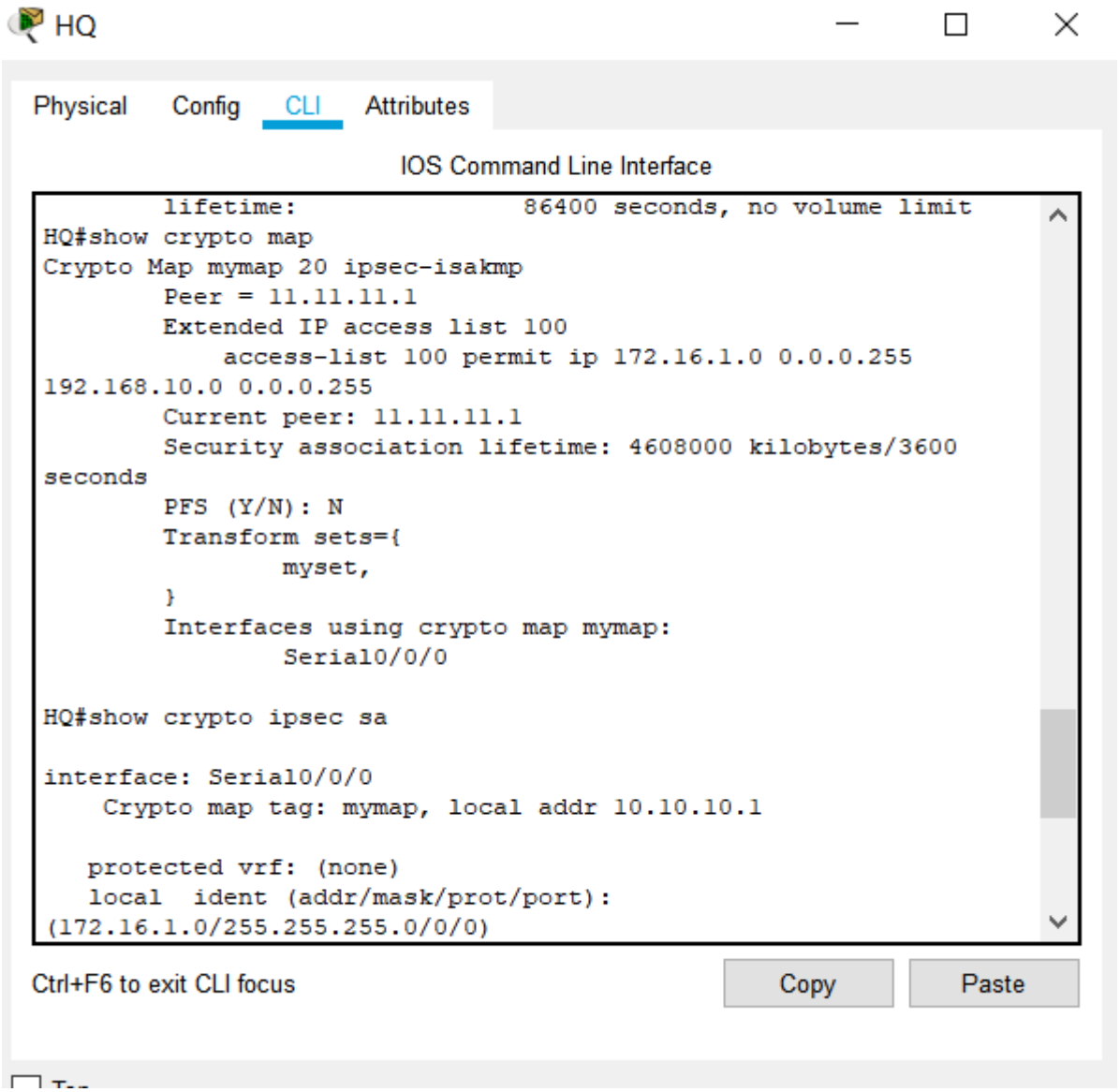
Branch

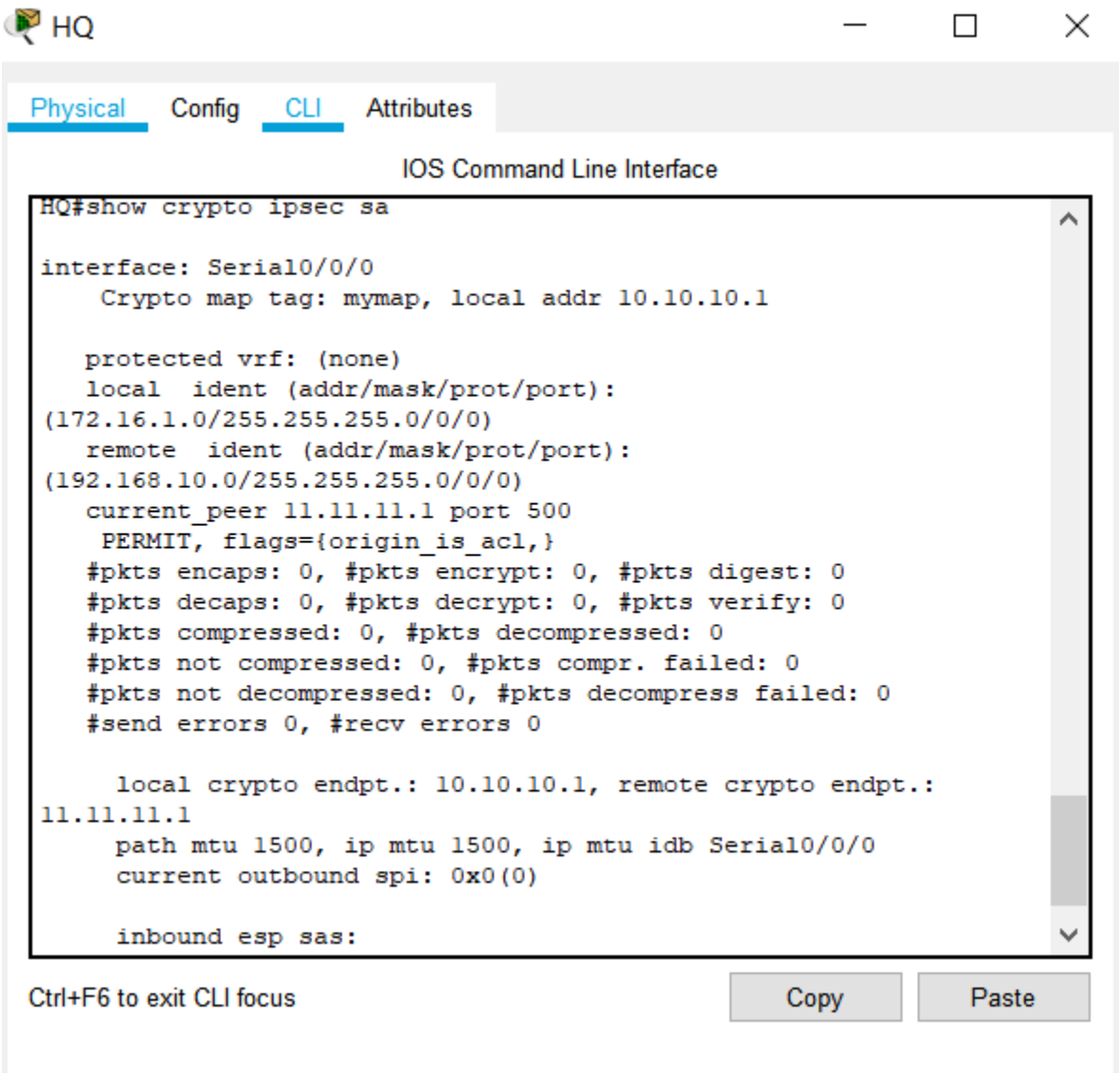
```
Branch(config)#crypto isakmp enable
Branch(config)#crypto isakmp policy 20
Branch(config-isakmp)#authentication pre-share
Branch(config-isakmp)#encryption 3des
Branch(config-isakmp)#hash md5
Branch(config-isakmp)#group 1
Branch(config-isakmp)#lifetime 3600
Branch(config-isakmp)#exit
```

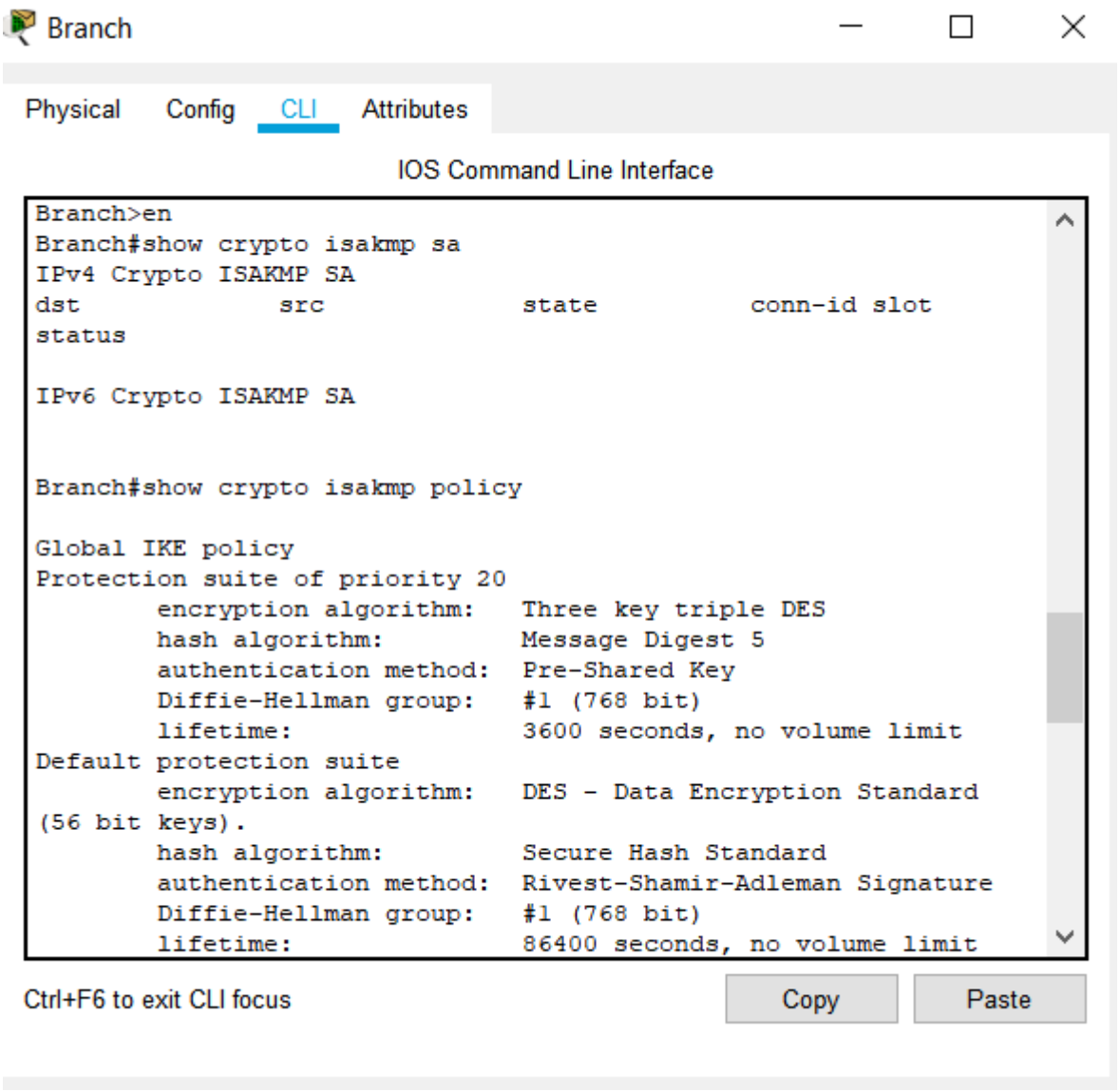
```
Branch(config)#crypto isakmp key cisco123 address 10.10.10.1
A pre-shared key for address mask 10.10.10.1 255.255.255.255
already exists!
Branch(config)#crypto ipsec transform-set myset esp-3des esp-md5-
hmac
Branch(config)#access-list 100 permit ip 192.168.10.0 0.0.0.255
172.16.1.0
% Incomplete command.
Branch(config)#access-list 100 permit ip 192.168.10.0 0.0.0.255
172.16.1.0 0.0.0.255
Branch(config)#crypto map mymap 20 ipsec-isakmp
Branch(config-crypto-map)#set peer 10.10.10.1
Branch(config-crypto-map)#set transform-set myset
Branch(config-crypto-map)#match address 100
Branch(config-crypto-map)#exit
Branch(config)#int s0/0/0
Branch(config-if)#crypto map mymap
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Branch(config-if)#
```

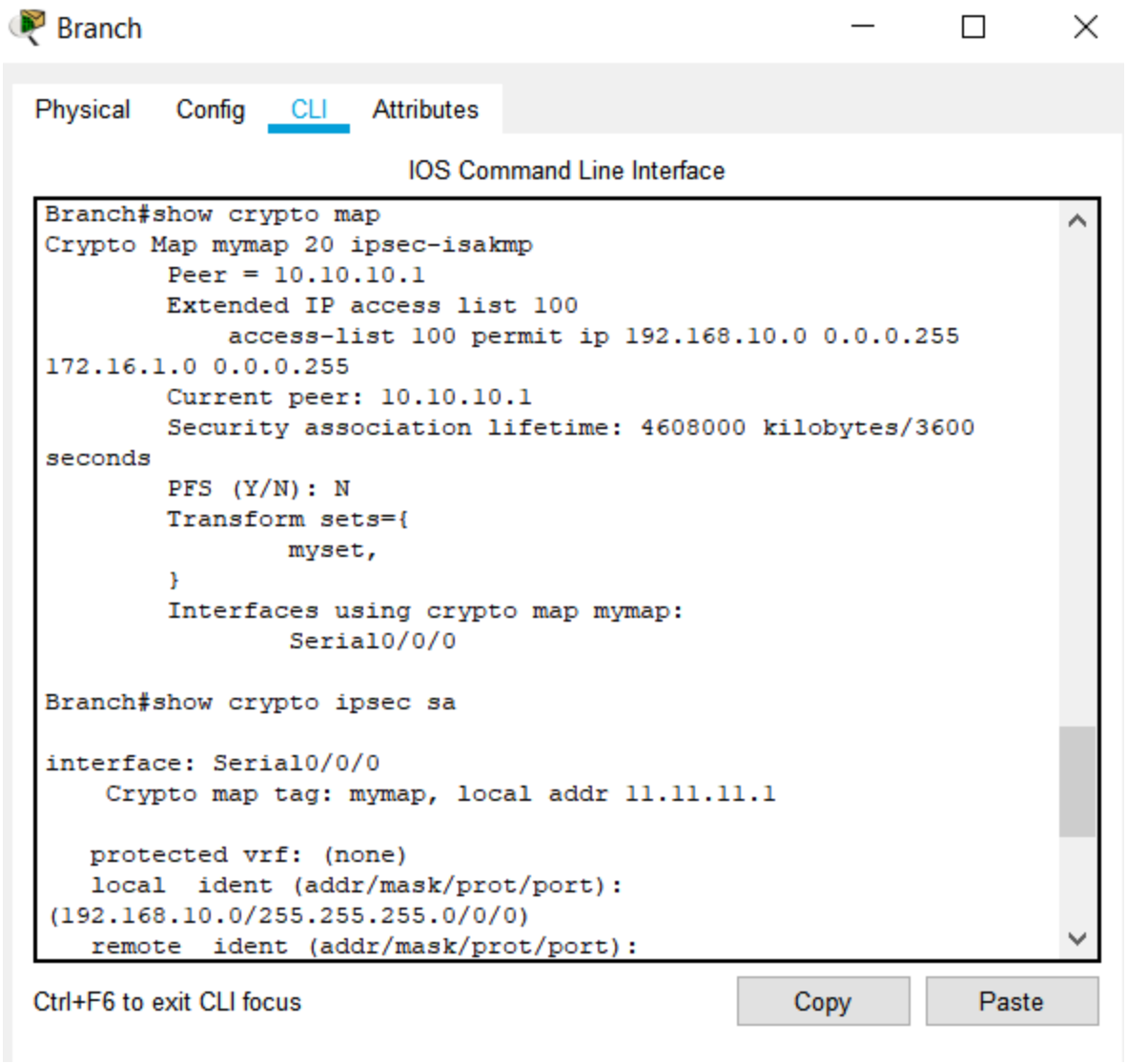
Verify Command

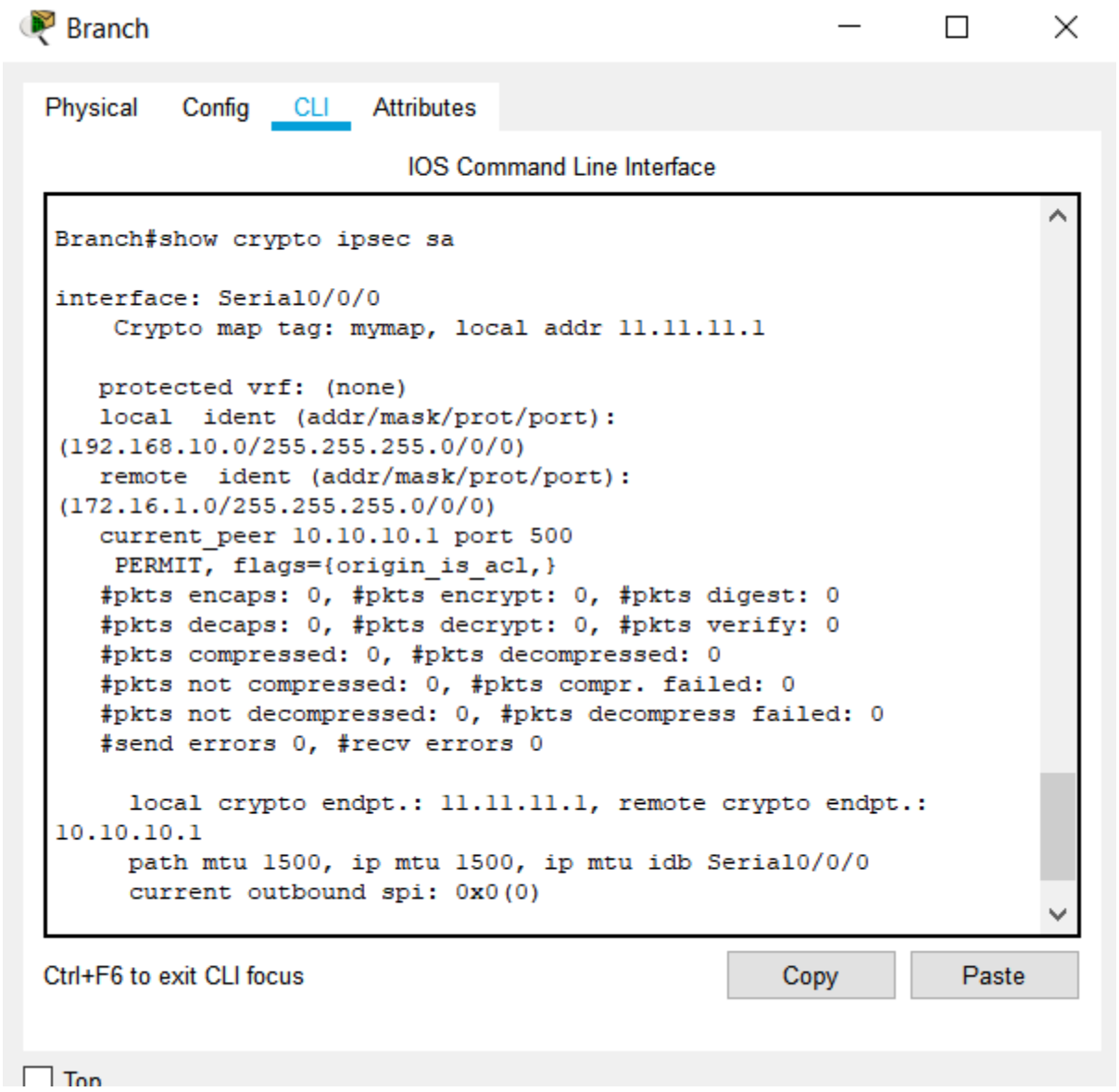

HQ
Physical
Config
CLI
Attributes
IOS Command Line Interface
HQ>
HQ>en
HQ#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id slot
status
IPv6 Crypto ISAKMP SA
HQ#show crypto isakmp policy
Global IKE policy
Protection suite of priority 20
encryption algorithm: Three key triple DES
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
lifetime: 3600 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard
(56 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit)
Ctrl+F6 to exit CLI focus
Copy
Paste


HQ
Physical
Config
CLI
Attributes
IOS Command Line Interface
lifetime: 86400 seconds, no volume limit
HQ#show crypto map
Crypto Map mymap 20 ipsec-isakmp
Peer = 11.11.11.1
Extended IP access list 100
access-list 100 permit ip 172.16.1.0 0.0.0.255
192.168.10.0 0.0.0.255
Current peer: 11.11.11.1
Security association lifetime: 4608000 kilobytes/3600
seconds
PFS (Y/N): N
Transform sets={
myset,
}
Interfaces using crypto map mymap:
Serial0/0/0
HQ#show crypto ipsec sa
interface: Serial0/0/0
Crypto map tag: mymap, local addr 10.10.10.1
protected vrf: (none)
local ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0)
Ctrl+F6 to exit CLI focus
Copy
Paste


HQ
Physical
Config
CLI
Attributes
IOS Command Line Interface
HQ#show crypto ipsec sa
interface: Serial0/0/0
Crypto map tag: mymap, local addr 10.10.10.1
protected vrf: (none)
local ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.10.0/255.255.255.0/0/0)
current_peer 11.11.11.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 10.10.10.1, remote crypto endpt.:
11.11.11.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x0(0)
inbound esp sas:
Ctrl+F6 to exit CLI focus
Copy
Paste


Branch
Physical
Config
CLI
Attributes
IOS Command Line Interface
Branch>en
Branch#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id slot
status
IPv6 Crypto ISAKMP SA
Branch#show crypto isakmp policy
Global IKE policy
Protection suite of priority 20
encryption algorithm: Three key triple DES
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
lifetime: 3600 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard
(56 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit
Ctrl+F6 to exit CLI focus
Copy
Paste


Branch
Physical
Config
CLI
Attributes
IOS Command Line Interface
Branch#show crypto map
Crypto Map mymap 20 ipsec-isakmp
Peer = 10.10.10.1
Extended IP access list 100
access-list 100 permit ip 192.168.10.0 0.0.0.255
172.16.1.0 0.0.0.255
Current peer: 10.10.10.1
Security association lifetime: 4608000 kilobytes/3600
seconds
PFS (Y/N): N
Transform sets={
myset,
}
Interfaces using crypto map mymap:
Serial0/0/0
Branch#show crypto ipsec sa
interface: Serial0/0/0
Crypto map tag: mymap, local addr 11.11.11.1
protected vrf: (none)
local ident (addr/mask/prot/port):
(192.168.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
Ctrl+F6 to exit CLI focus
Copy
Paste



Ping Both PCs and Check Packets Encapsulated using show crypto ipsec sa command