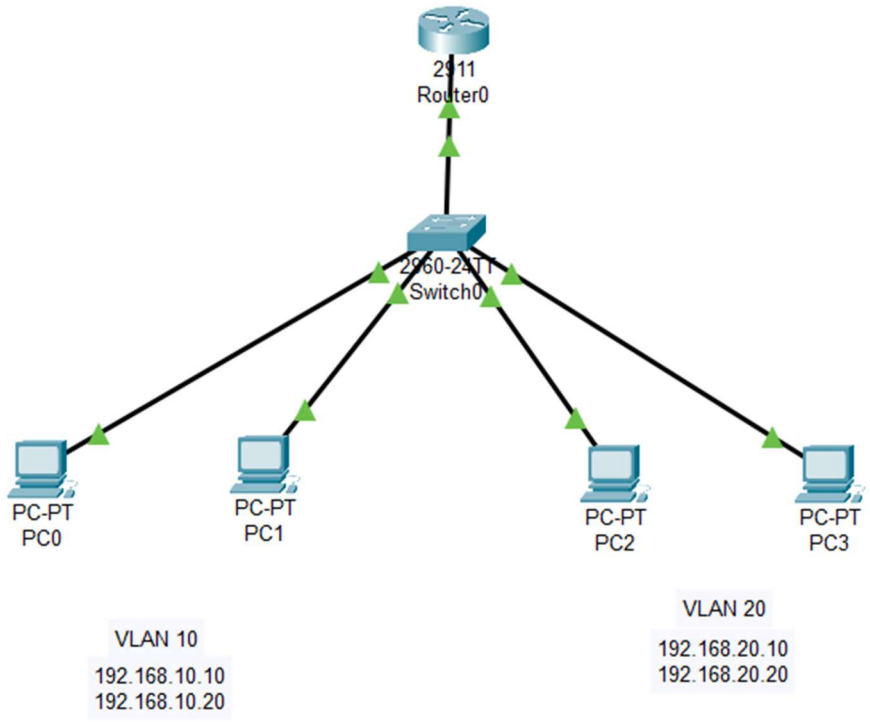
LINUX NETWORKING MODULE 7 AND 8 ASSESSMENT SOLUTION

-BY SAKTHI KUMAR S

9.Try Inter VLAN routing with Router

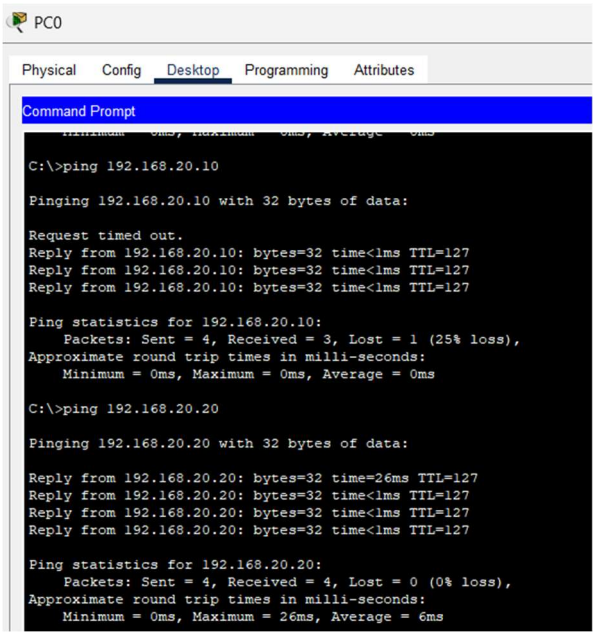
- 10.Implement ACLs to restrict traffic based on source and destination ports. Test rules by simulating legitimate and unauthorized traffic.
- 11.Configure a standard Access Control List (ACL) on a router to permit traffic from a specific IP range. Test connectivity to verify the ACL is working as intended.
- 12.Create an extended ACL to block specific applications, such as HTTP or FTP traffic. Test the ACL rules by attempting to access blocked services.

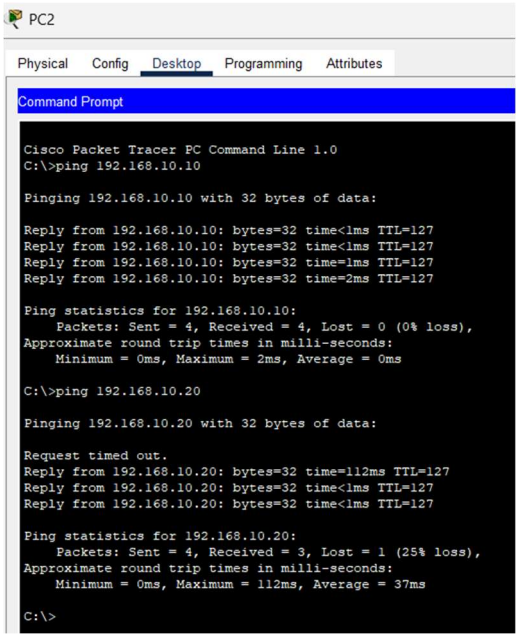
Topology:




```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/5       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/5       1-1005

Port        Vlans allowed and active in management domain
Fa0/5       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/5       1,10,20

Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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   hr                               active    Fa0/1, Fa0/2
20   fin                              active    Fa0/3, Fa0/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.10  192.168.10.1    YES manual up                    up
GigabitEthernet0/0.20  192.168.20.1    YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

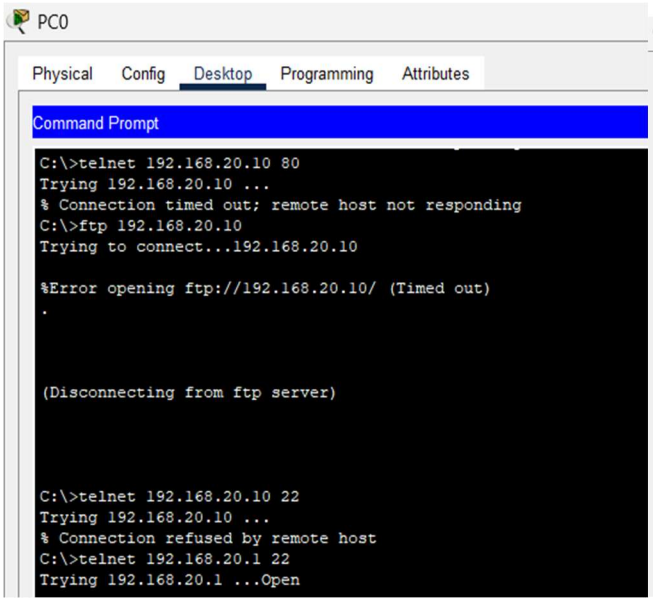


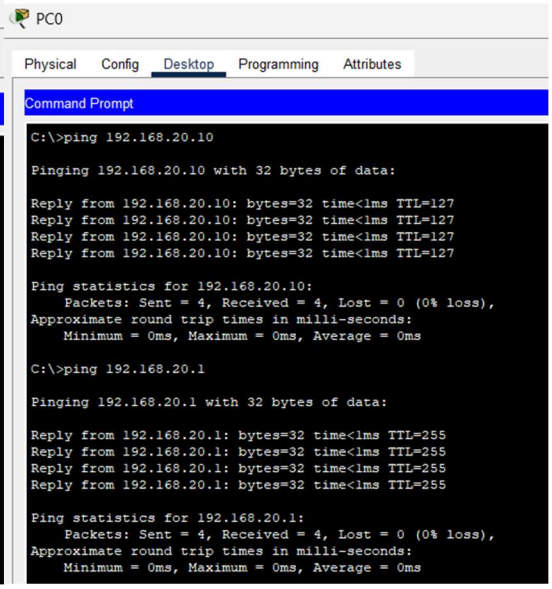


10.Implement ACLs to restrict traffic based on source and destination ports. Test rules by simulating legitimate and unauthorized traffic.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 120 deny tcp 192.168.10.0 0.0.0.255 any eq 80
Router(config)#access-list 120 deny tcp 192.168.10.0 0.0.0.255 any eq 21
Router(config)#access-list 120 permit tcp any any eq 22
Router(config)#access-list 120 deny tcp any any eq 23
Router(config)#access-list 120 permit ip any any
Router(config)#exit
```

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0.10
Router(config-subif)#ip access-group 120 in
Router(config-subif)#exit
Router(config)#
Router(config)#interface GigabitEthernet0/0.20
Router(config-subif)#ip access-group 120 in
Router(config-subif)#exit
Router(config)#
Router(config)#exit
Router#write memory
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-lists 120
Extended IP access list 120
    deny tcp 192.168.10.0 0.0.0.255 any eq www (24 match(es))
    deny tcp 192.168.10.0 0.0.0.255 any eq ftp (12 match(es))
    permit tcp any any eq 22 (6 match(es))
    deny tcp any any eq telnet
    permit ip any any (14 match(es))

Router#show running-config | include access-group
 ip access-group 120 in
 ip access-group 120 in
```





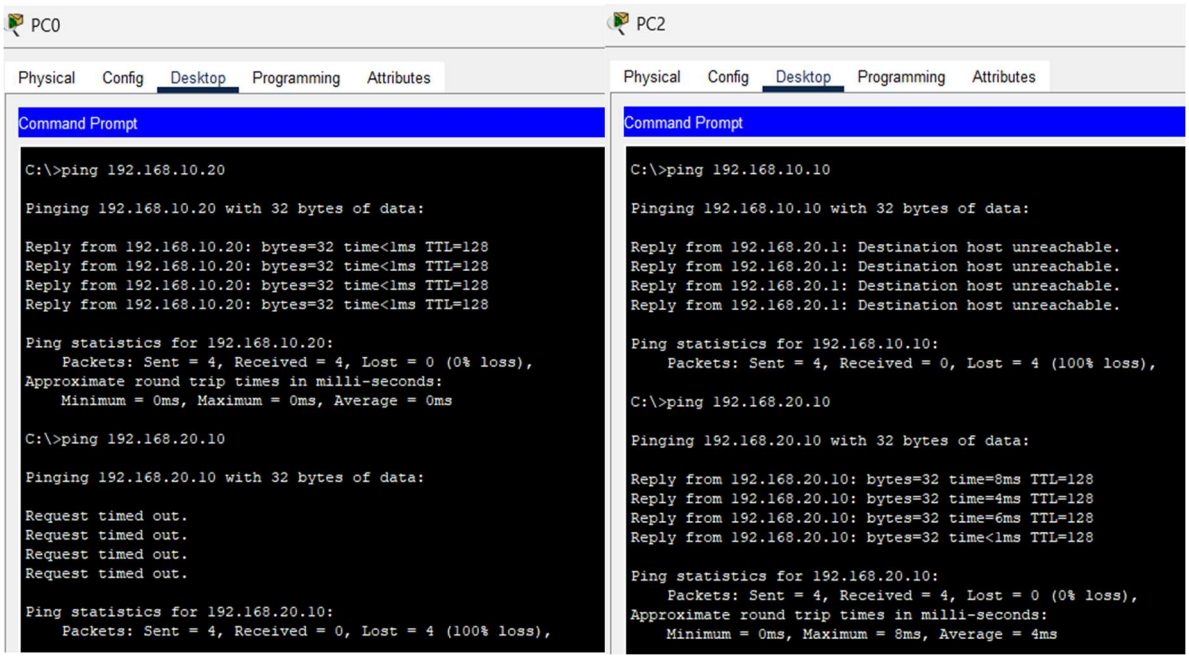
Restrict HTTPs (TCP 80) & FTP (TCP 21) from specific source IPs, Allow SSH (TCP 22), Block Telnet (TCP 23) and allows all other traffic

11.Configure a standard Access Control List (ACL) on a router to permit traffic from a specific IP range. Test connectivity to verify the ACL is working as intended.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 10 permit 192.168.10.0 0.0.0.255
Router(config)#access-list 10 deny any
Router(config)#exit
```

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0.10
Router(config-subif)#ip access-group 10 in

Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0.20
Router(config-subif)#ip access-group 10 in
Router(config-subif)#ex
Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr memory
Building configuration...
[OK]
Router#show access-lists 10
Standard IP access list 10
    permit 192.168.10.0 0.0.0.255 (8 match(es))
    deny any

Router#show running-config | include access-group
 ip access-group 10 in
 ip access-group 10 in
Router#
```

Ping Test:



The ACL permits 192.168.10.0/24 and denies all others. It is applied to the router interface where filtering is needed. Connectivity tests verify that only allowed traffic is passing.

12.Create an extended ACL to block specific applications, such as HTTP or FTP traffic. Test the ACL rules by attempting to access blocked services.

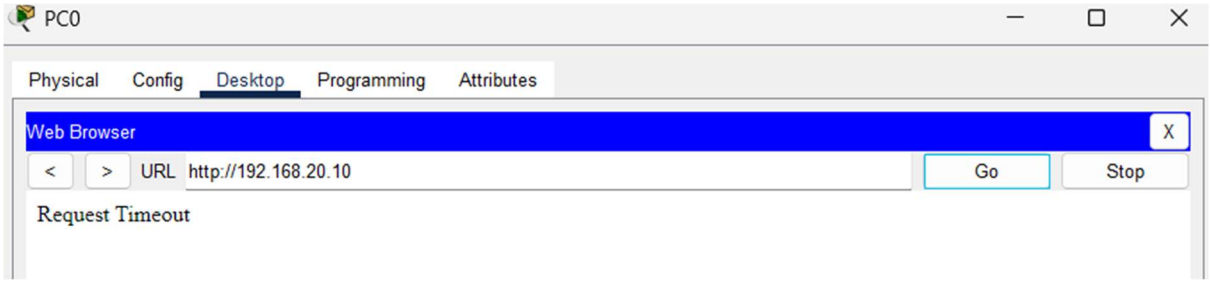
```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 110 deny tcp any any eq 80
Router(config)#access-list 110 deny tcp any any eq 20
Router(config)#access-list 110 deny tcp any any eq 21
Router(config)#access-list 110 permit ip any any
Router(config)#interface GigabitEthernet0/0.10
Router(config-subif)#ip access-group 110 in
Router(config-subif)#exit
```

```
Router#show access-lists 110
Extended IP access list 110
    deny tcp any any eq www
    deny tcp any any eq 20
    deny tcp any any eq ftp
    permit ip any any

Router#show running-config | include access-group
 ip access-group 110 in
```

Tests:

```
C:\>telnet 192.168.20.10 80
Trying 192.168.20.10 ...
% Connection timed out; remote host not responding
C:\>telnet 192.168.20.10 21
Trying 192.168.20.10 ...
% Connection timed out; remote host not responding
```

```
C:\>ftp 192.168.20.10
Trying to connect...192.168.20.10

%Error opening ftp://192.168.20.10/ (Timed out)
.


(Disconnecting from ftp server)



C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time=1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



Testing confirmed that HTTP/FTP traffic is blocked, but normal services (like ICMP and other protocols) work.