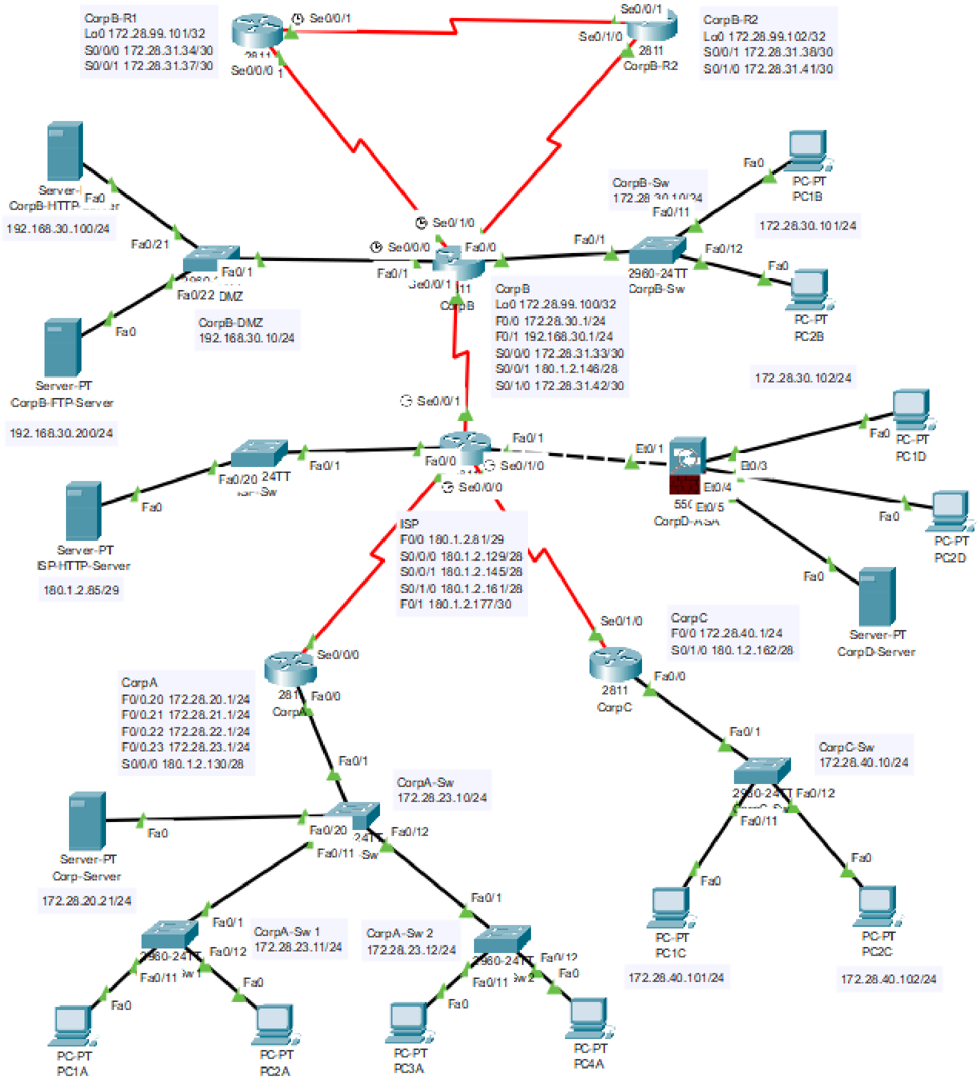
Eric Guzman 5/4/2025

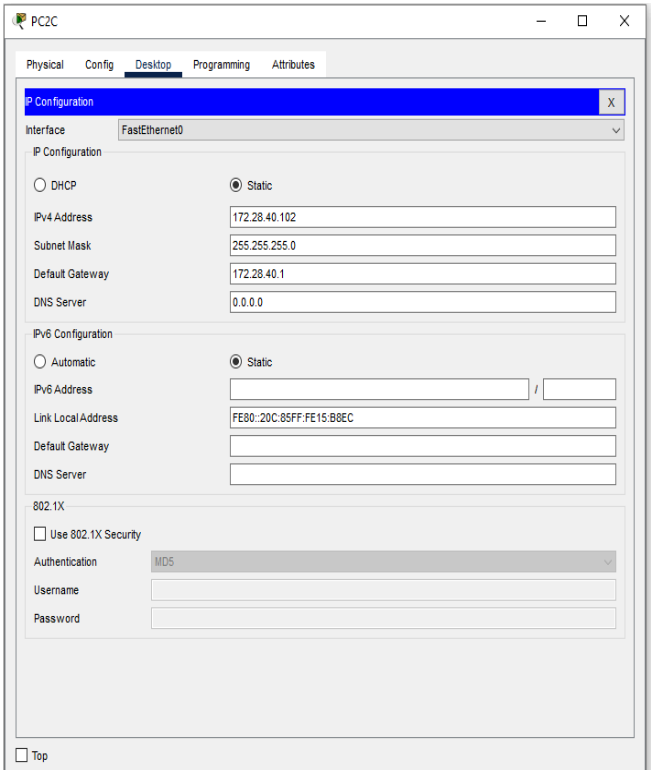
Professor Cannistra Internet Security

Challenge Lab

Topology:



1. Hosts



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	172.28.40.102
Subnet Mask	255.255.255.0
Default Gateway	172.28.40.1
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

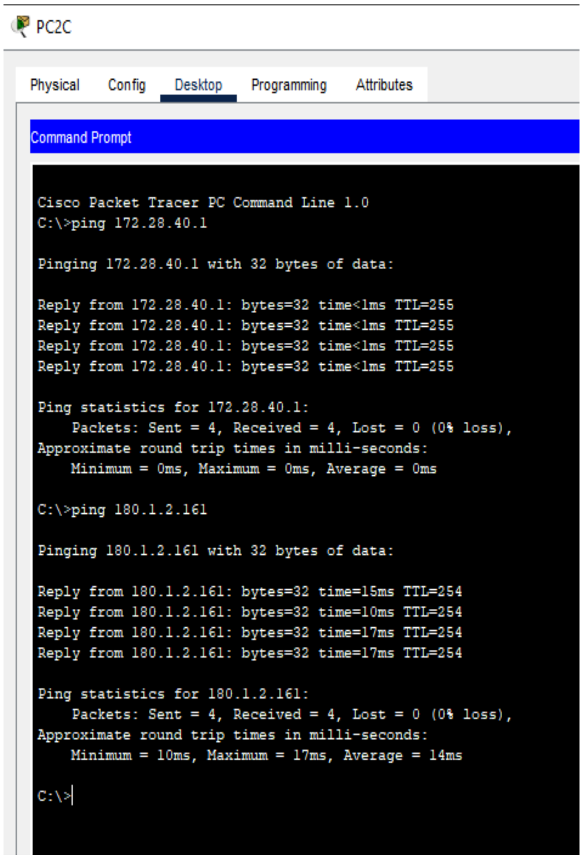
IPv6 Address	/
Link Local Address	FE80::20C:85FF:FE15:B8EC
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

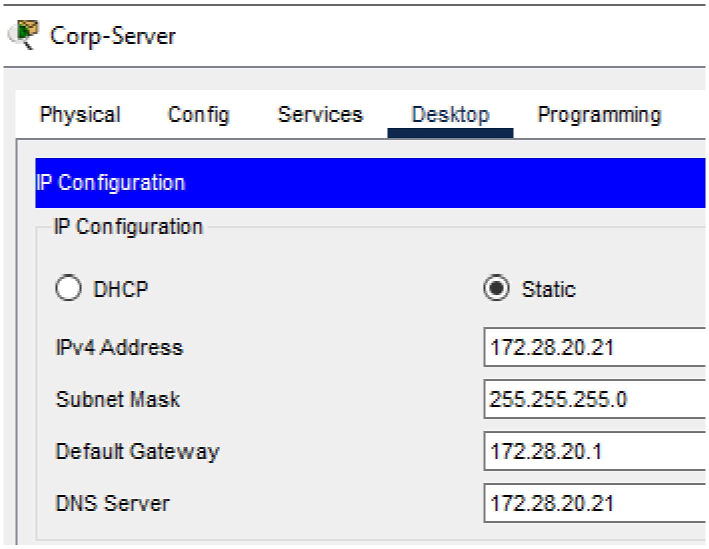
Authentication	MD5
Username	
Password	

□ Top



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.28.40.1

Pinging 172.28.40.1 with 32 bytes of data:

Reply from 172.28.40.1: bytes=32 time<1ms TTL=255
Reply from 172.28.40.1: bytes=32 time<1ms TTL=255
Reply from 172.28.40.1: bytes=32 time<1ms TTL=255
Reply from 172.28.40.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.28.40.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 180.1.2.161

Pinging 180.1.2.161 with 32 bytes of data:

Reply from 180.1.2.161: bytes=32 time=15ms TTL=254
Reply from 180.1.2.161: bytes=32 time=10ms TTL=254
Reply from 180.1.2.161: bytes=32 time=17ms TTL=254
Reply from 180.1.2.161: bytes=32 time=17ms TTL=254

Ping statistics for 180.1.2.161:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 17ms, Average = 14ms

C:\>
```

These screenshots show that PC2C is statically addressed correctly and can ping up to the ISP interface.

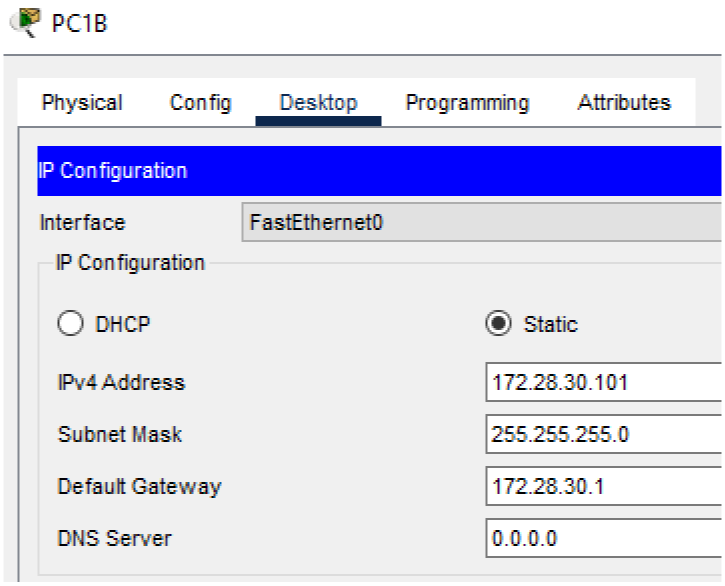


IP Configuration

○ DHCP ● Static

IPv4 Address	172.28.20.21
Subnet Mask	255.255.255.0
Default Gateway	172.28.20.1
DNS Server	172.28.20.21

This screenshot shows that Corp-Server is statically addressed correctly.



IP Configuration

Interface FastEthernet0

IP Configuration

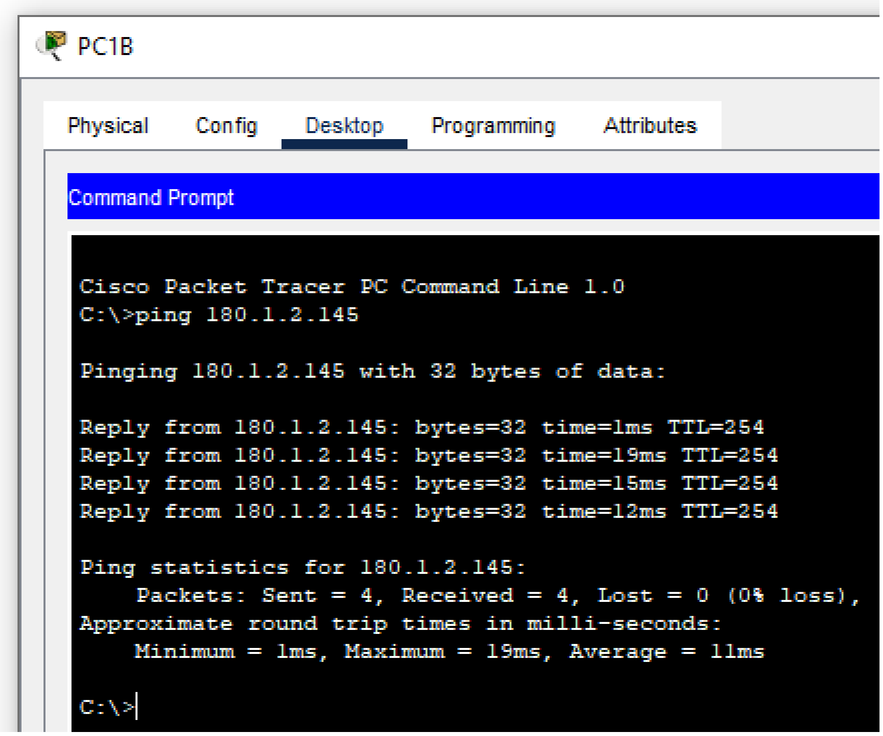
○ DHCP ● Static

IPv4 Address 172.28.30.101

Subnet Mask 255.255.255.0

Default Gateway 172.28.30.1

DNS Server 0.0.0.0

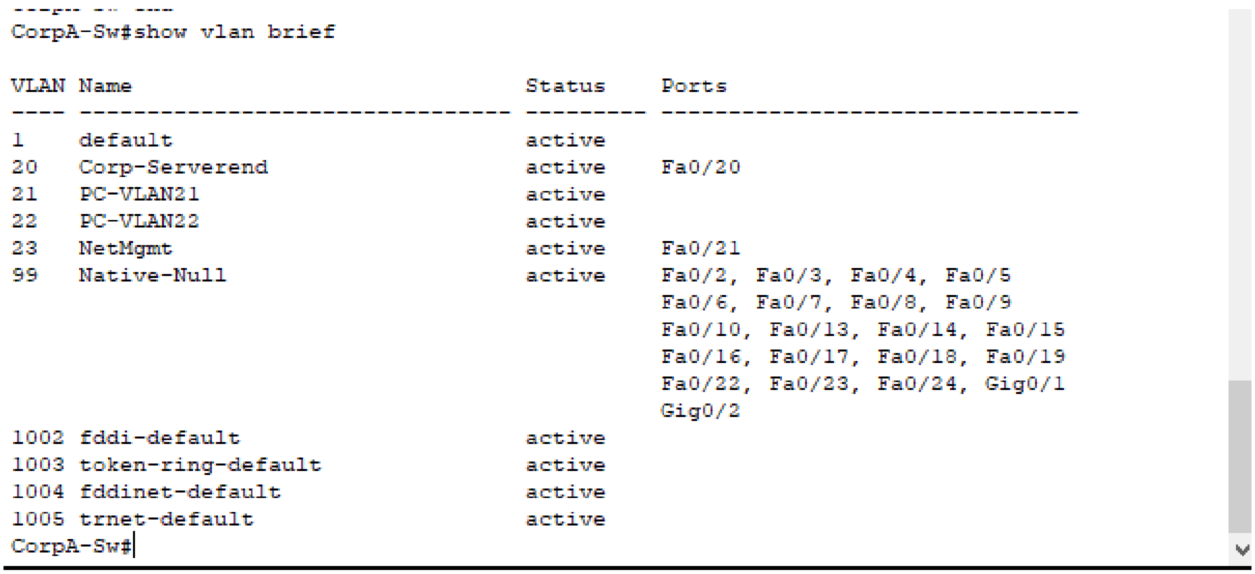


Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 180.1.2.145

Pinging 180.1.2.145 with 32 bytes of data:

Reply from 180.1.2.145: bytes=32 time=1ms TTL=254
Reply from 180.1.2.145: bytes=32 time=19ms TTL=254
Reply from 180.1.2.145: bytes=32 time=15ms TTL=254
Reply from 180.1.2.145: bytes=32 time=12ms TTL=254

Ping statistics for 180.1.2.145:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 19ms, Average = 11ms

C:\>
```

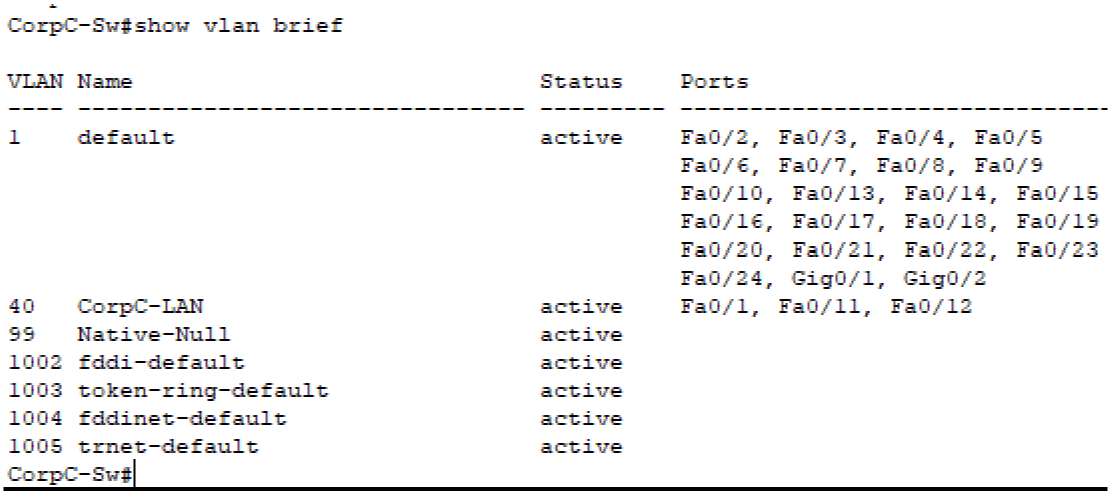
These screenshots show that PC1B is statically addressed correctly and can ping to the ISP interface.

2. VLANs



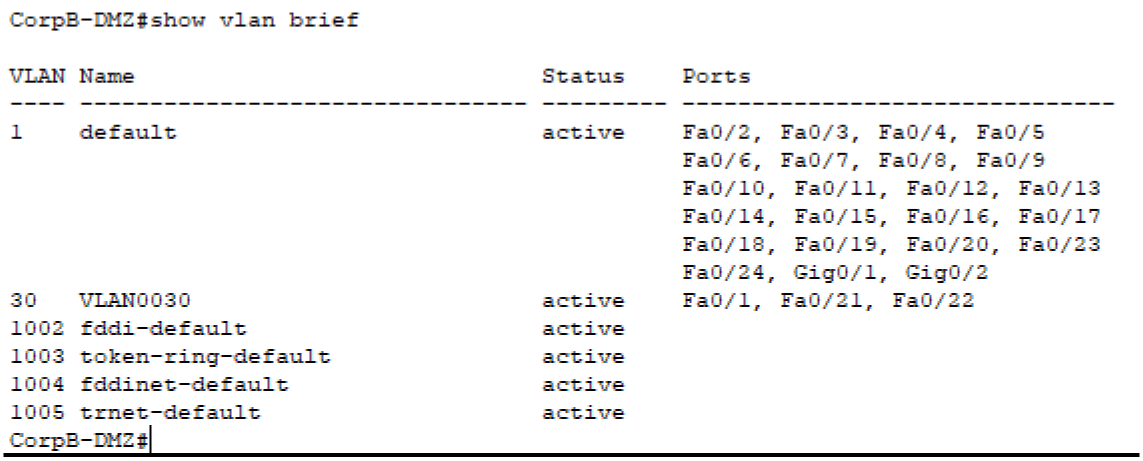
```
CorpA-Sw#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    
20   Corp-Serverend                   active    Fa0/20
21   PC-VLAN21                        active    
22   PC-VLAN22                        active    
23   NetMgmt                          active    Fa0/21
99   Native-Null                      active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                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    
CorpA-Sw#
```

This screenshot shows that VLANs 20, 21, 22 and 23 are created and assigned to the correct ports. VLAN 1 is unused.



```
CorpC-Sw#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, Fa0/13, 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
40   CorpC-LAN                        active    Fa0/1, Fa0/11, Fa0/12
99   Native-Null                      active    
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
CorpC-Sw#
```

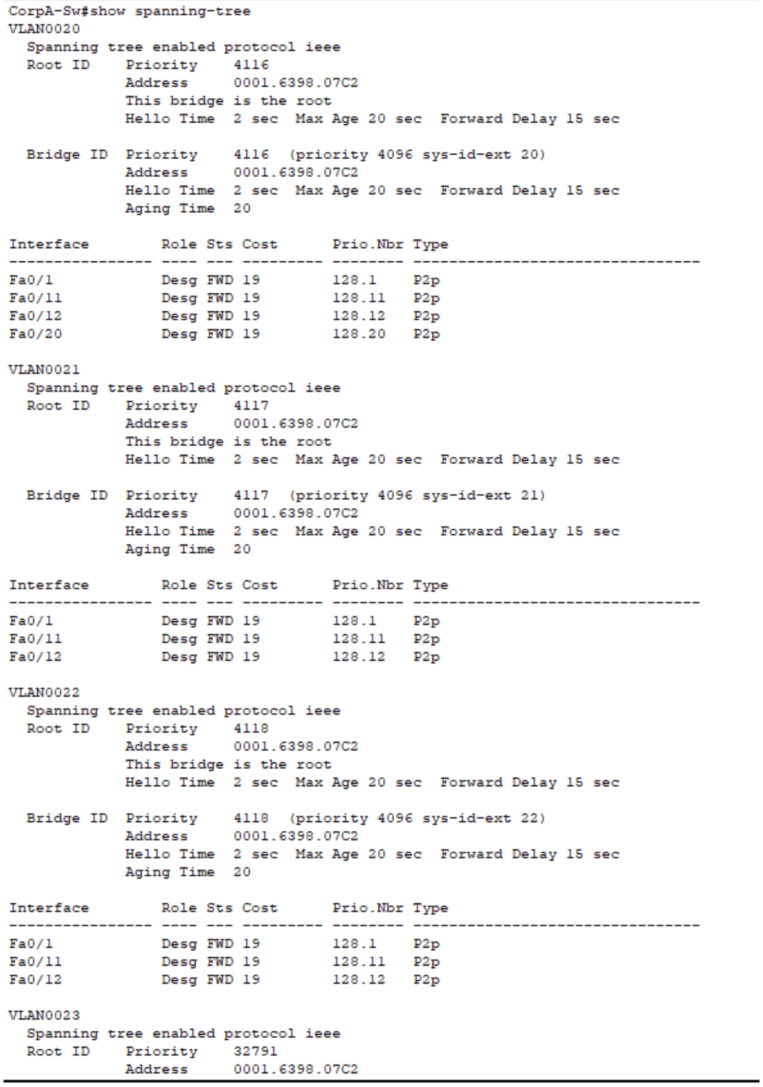
This screenshot shows that VLAN 40 is created and assigned to the correct ports. VLAN 1 is unused by any active ports but best practice is to move them to an unused VLAN like VLAN 99 to reduce unauthorized access.



```
CorpB-DMZ#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, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
30   VLAN0030                         active    Fa0/1, Fa0/21, Fa0/22
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
CorpB-DMZ#
```

This screenshot shows that VLAN 30 in the DMZ is created and assigned to the correct ports. VLAN 1 is unused by any active ports but best practice is to move them to an unused VLAN like VLAN 99 to reduce unauthorized access.

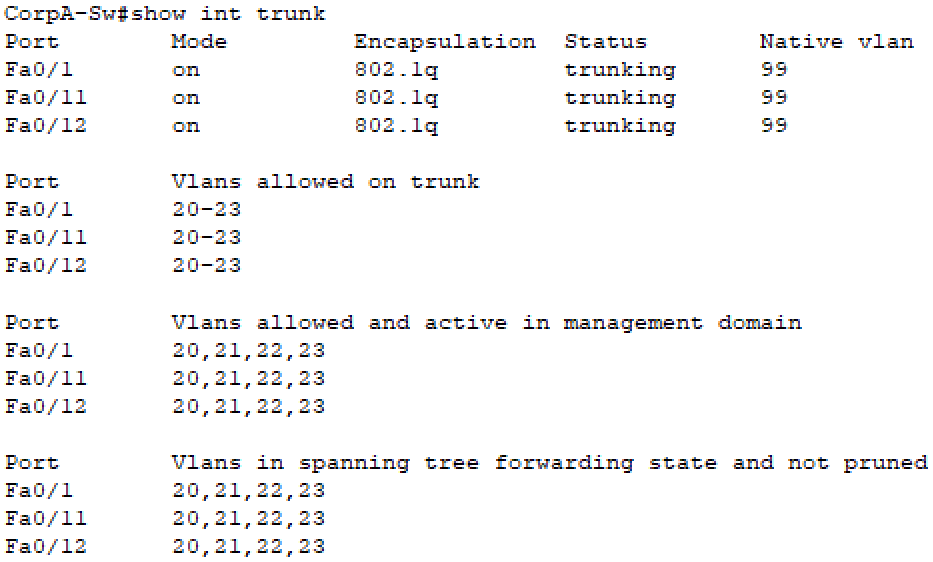
3. STP



```
CorpA-Sw#show spanning-tree
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    4116
             Address     0001.6398.07C2
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4116  (priority 4096 sys-id-ext 20)
             Address     0001.6398.07C2
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/12           Desg FWD 19        128.12   P2p
Fa0/20           Desg FWD 19        128.20   P2p

VLAN0021
  Spanning tree enabled protocol ieee
  Root ID    Priority    4117
             Address     0001.6398.07C2
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4117  (priority 4096 sys-id-ext 21)
             Address     0001.6398.07C2
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/12           Desg FWD 19        128.12   P2p

VLAN0022
  Spanning tree enabled protocol ieee
  Root ID    Priority    4118
             Address     0001.6398.07C2
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4118  (priority 4096 sys-id-ext 22)
             Address     0001.6398.07C2
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/12           Desg FWD 19        128.12   P2p

VLAN0023
  Spanning tree enabled protocol ieee
  Root ID    Priority    32791
             Address     0001.6398.07C2
```

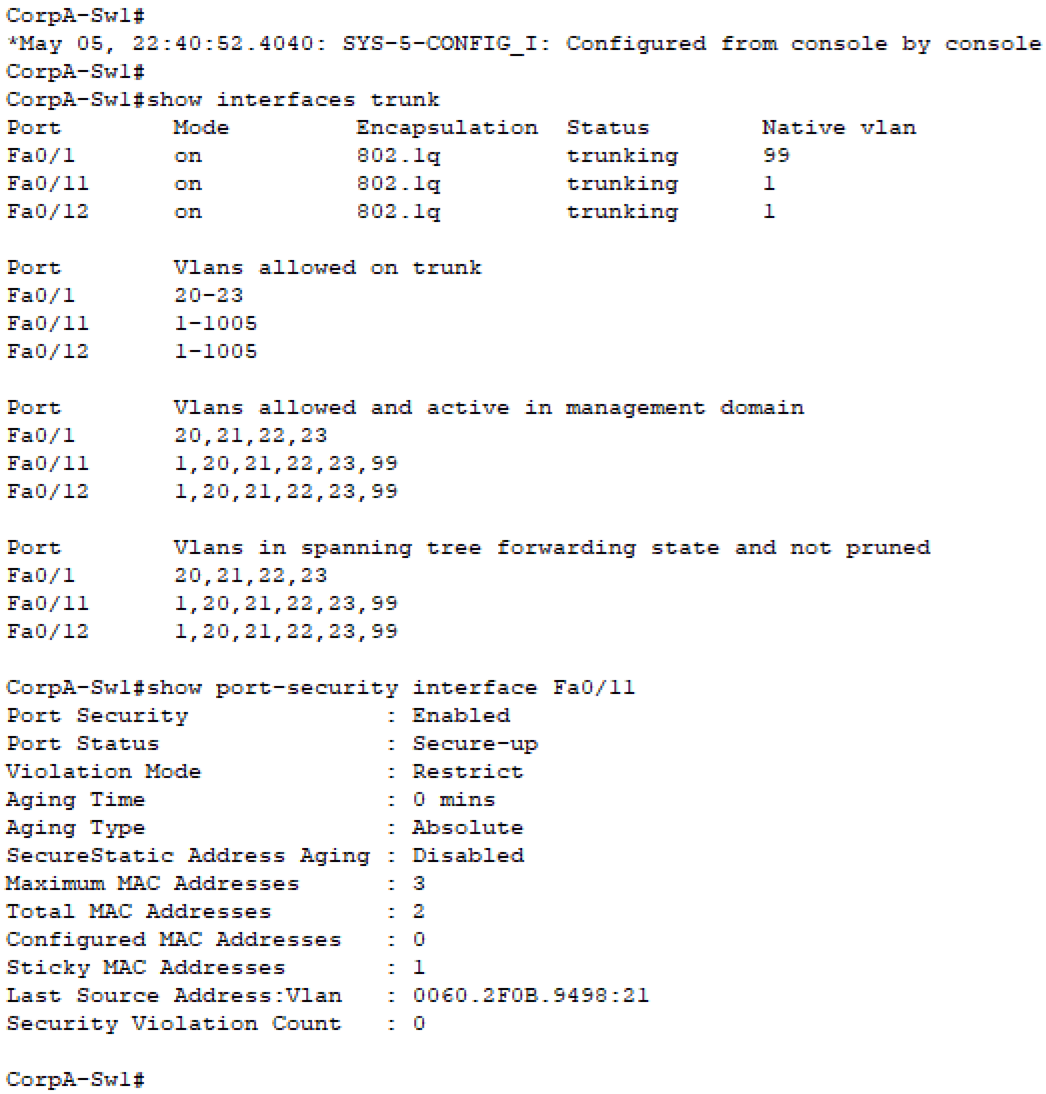
This screenshot shows output of show spanning-tree on CorpA-Sw. Each VLAN confirms that this bridge is the root, which is proof that CorpA-Sw is the STP root bridge for all of the VLANs in this network.

4. IEEE 802.1Q Trunking



```
CorpA-Sw#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/11      on           802.1q         trunking      99
Fa0/12      on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       20-23
Fa0/11      20-23
Fa0/12      20-23

Port        Vlans allowed and active in management domain
Fa0/1       20,21,22,23
Fa0/11      20,21,22,23
Fa0/12      20,21,22,23

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       20,21,22,23
Fa0/11      20,21,22,23
Fa0/12      20,21,22,23
```

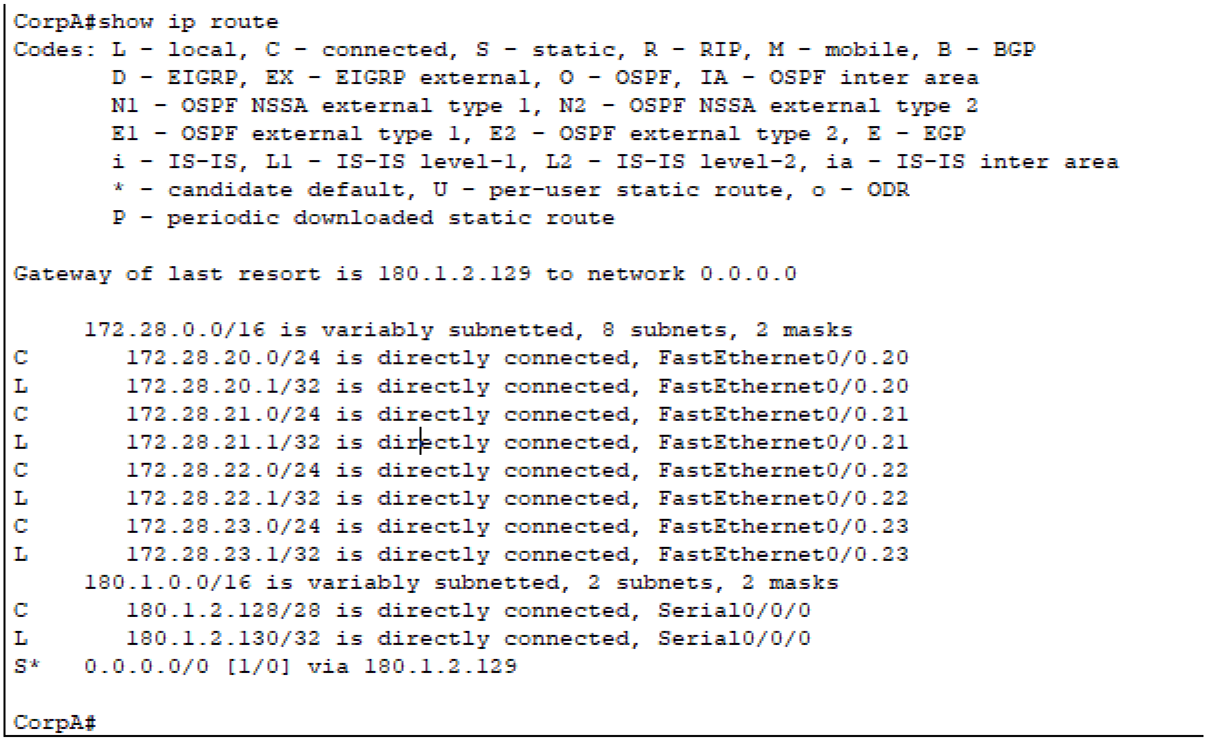
This screenshot shows that interfaces F0/1, F0/11 and F0/12 on CorpA-Sw are all configured as 802.1Q trunk ports.



```
CorpA-Sw1#
*May 05, 22:40:52.4040: SYS-5-CONFIG_I: Configured from console by console
CorpA-Sw1#
CorpA-Sw1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/11      on           802.1q         trunking      1
Fa0/12      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       20-23
Fa0/11      1-1005
Fa0/12      1-1005

Port        Vlans allowed and active in management domain
Fa0/1       20,21,22,23
Fa0/11      1,20,21,22,23,99
Fa0/12      1,20,21,22,23,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       20,21,22,23
Fa0/11      1,20,21,22,23,99
Fa0/12      1,20,21,22,23,99

CorpA-Sw1#show port-security interface Fa0/11
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 2
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0060.2F0B.9498:21
Security Violation Count   : 0

CorpA-Sw1#
```

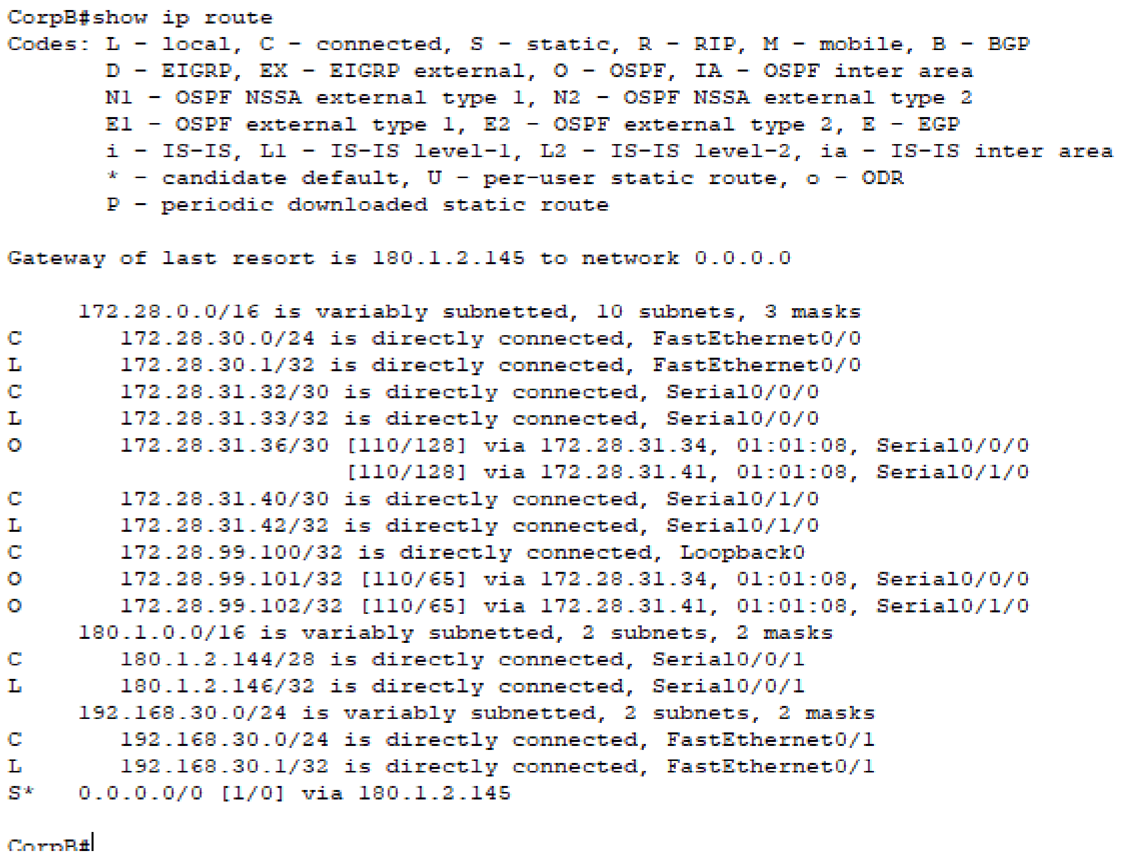
This screenshot shows that the trunk ports on CorpA-Sw1 are also configured as 802.1Q ports. We can also see that port security is enabled on F0/11 only allowing a maximum of 3 mac addresses.

5. Default Static Routing



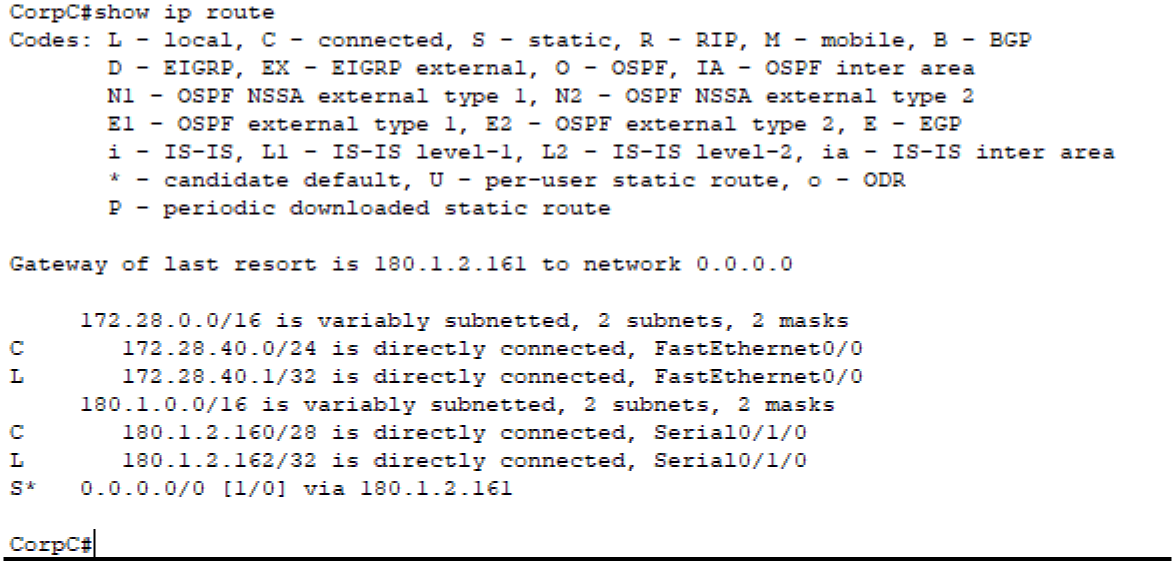
```
CorpA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 180.1.2.129 to network 0.0.0.0

     172.28.0.0/16 is variably subnetted, 8 subnets, 2 masks
C       172.28.20.0/24 is directly connected, FastEthernet0/0.20
L       172.28.20.1/32 is directly connected, FastEthernet0/0.20
C       172.28.21.0/24 is directly connected, FastEthernet0/0.21
L       172.28.21.1/32 is directly connected, FastEthernet0/0.21
C       172.28.22.0/24 is directly connected, FastEthernet0/0.22
L       172.28.22.1/32 is directly connected, FastEthernet0/0.22
C       172.28.23.0/24 is directly connected, FastEthernet0/0.23
L       172.28.23.1/32 is directly connected, FastEthernet0/0.23
     180.1.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       180.1.2.128/28 is directly connected, Serial0/0/0
L       180.1.2.130/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 180.1.2.129

CorpA#
```

This screenshot shows that CorpA router has a static default route pointing up to 180.1.2.129.



```
CorpB#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 180.1.2.145 to network 0.0.0.0

     172.28.0.0/16 is variably subnetted, 10 subnets, 3 masks
C       172.28.30.0/24 is directly connected, FastEthernet0/0
L       172.28.30.1/32 is directly connected, FastEthernet0/0
C       172.28.31.32/30 is directly connected, Serial0/0/0
L       172.28.31.33/32 is directly connected, Serial0/0/0
O       172.28.31.36/30 [110/128] via 172.28.31.34, 01:01:08, Serial0/0/0
                        [110/128] via 172.28.31.41, 01:01:08, Serial0/1/0
C       172.28.31.40/30 is directly connected, Serial0/1/0
L       172.28.31.42/32 is directly connected, Serial0/1/0
C       172.28.99.100/32 is directly connected, Loopback0
O       172.28.99.101/32 [110/65] via 172.28.31.34, 01:01:08, Serial0/0/0
O       172.28.99.102/32 [110/65] via 172.28.31.41, 01:01:08, Serial0/1/0
     180.1.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       180.1.2.144/28 is directly connected, Serial0/0/1
L       180.1.2.146/32 is directly connected, Serial0/0/1
     192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.30.0/24 is directly connected, FastEthernet0/1
L       192.168.30.1/32 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 180.1.2.145

CorpB#
```

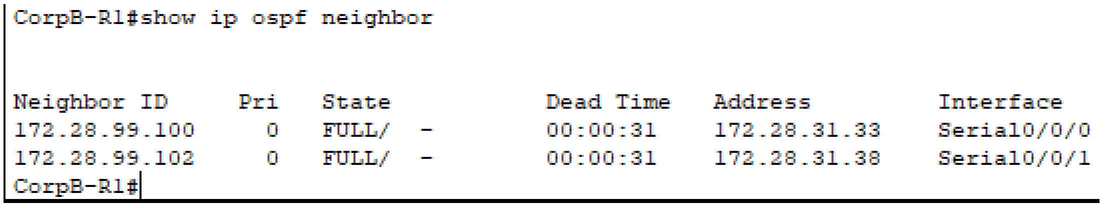
This screenshot shows that CorpB router has a static default route pointing up to 180.1.2.145.



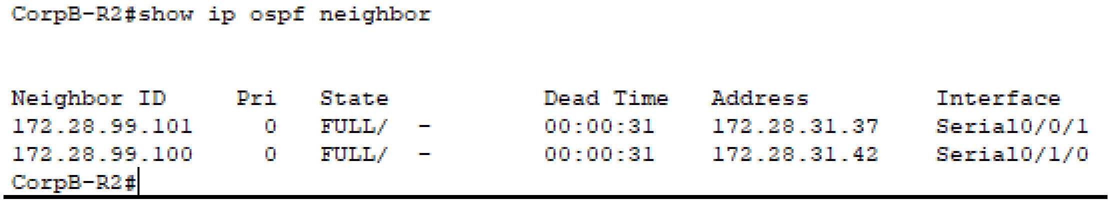
```
CorpC#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 180.1.2.161 to network 0.0.0.0

     172.28.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.28.40.0/24 is directly connected, FastEthernet0/0
L       172.28.40.1/32 is directly connected, FastEthernet0/0
     180.1.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       180.1.2.160/28 is directly connected, Serial0/1/0
L       180.1.2.162/32 is directly connected, Serial0/1/0
S*   0.0.0.0/0 [1/0] via 180.1.2.161

CorpC#
```

This screenshot shows that CorpC router has a static default route pointing up to 180.1.2.161.

6. Dynamic Routing

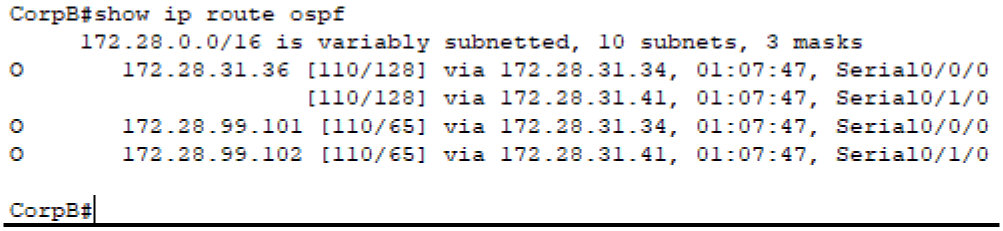


```
CorpB-R1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
172.28.99.100     0   FULL/  -        00:00:31    172.28.31.33    Serial0/0/0
172.28.99.102     0   FULL/  -        00:00:31    172.28.31.38    Serial0/0/1
CorpB-R1#
```



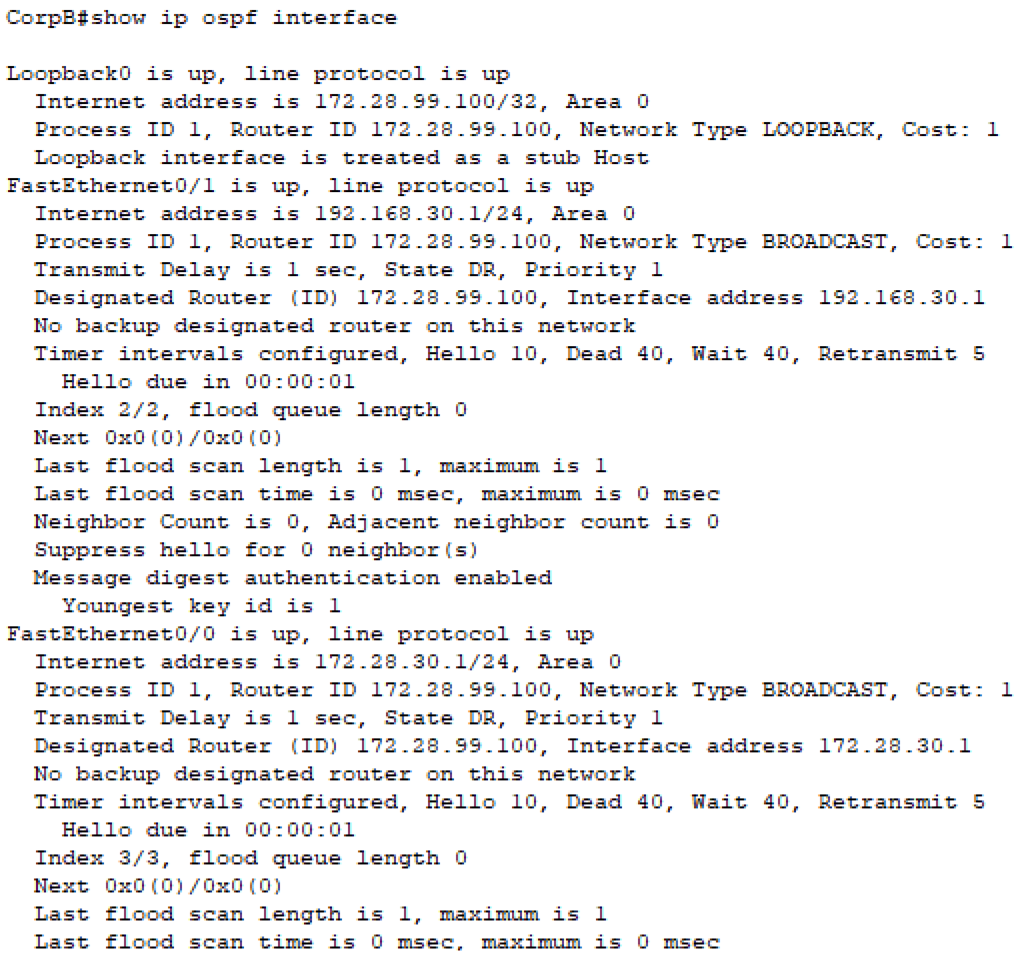
```
CorpB-R2#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
172.28.99.101     0   FULL/  -        00:00:31    172.28.31.37    Serial0/0/1
172.28.99.100     0   FULL/  -        00:00:31    172.28.31.42    Serial0/1/0
CorpB-R2#
```

These screenshots show that OSPF neighbor adjacencies have been established between CorpB, CorpB-R1 and CorpB-R2.



```
CorpB#show ip route ospf
     172.28.0.0/16 is variably subnetted, 10 subnets, 3 masks
O       172.28.31.36 [110/128] via 172.28.31.34, 01:07:47, Serial0/0/0
                     [110/128] via 172.28.31.41, 01:07:47, Serial0/1/0
O       172.28.99.101 [110/65] via 172.28.31.34, 01:07:47, Serial0/0/0
O       172.28.99.102 [110/65] via 172.28.31.41, 01:07:47, Serial0/1/0

CorpB#
```

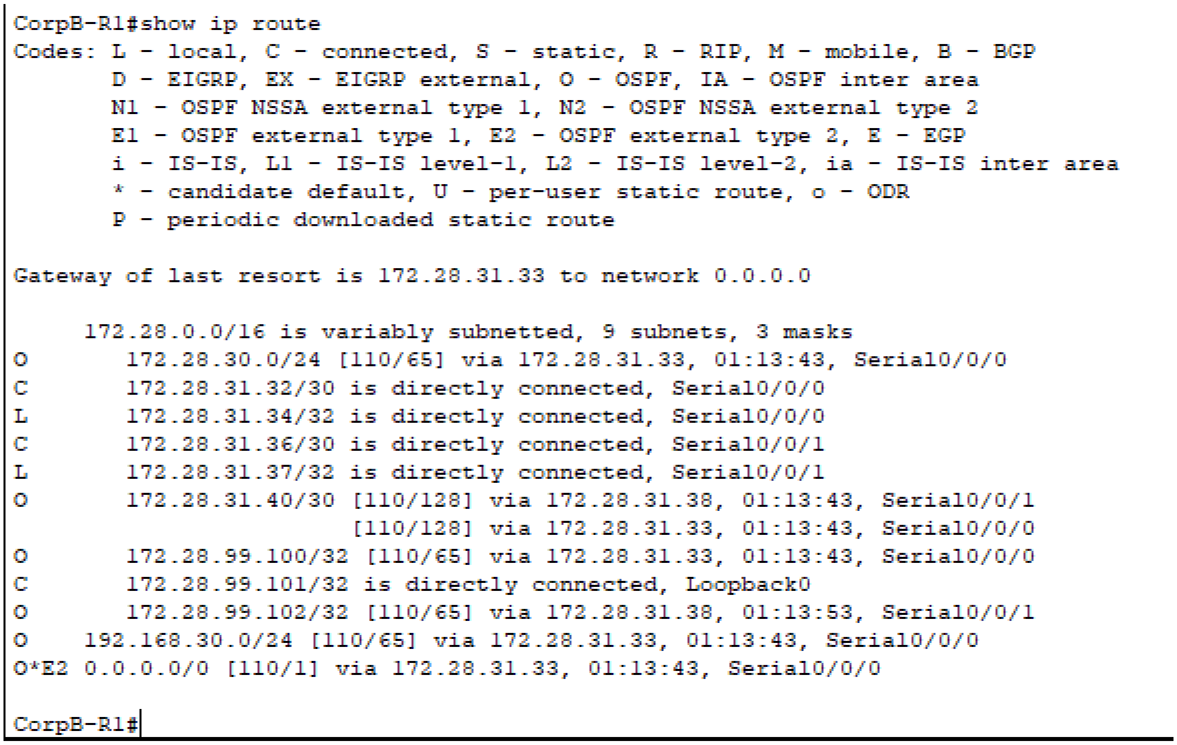
This screenshot shows that CorpB is learning OSPF routes from its peer routers. This proves that dynamic routing is functioning properly.



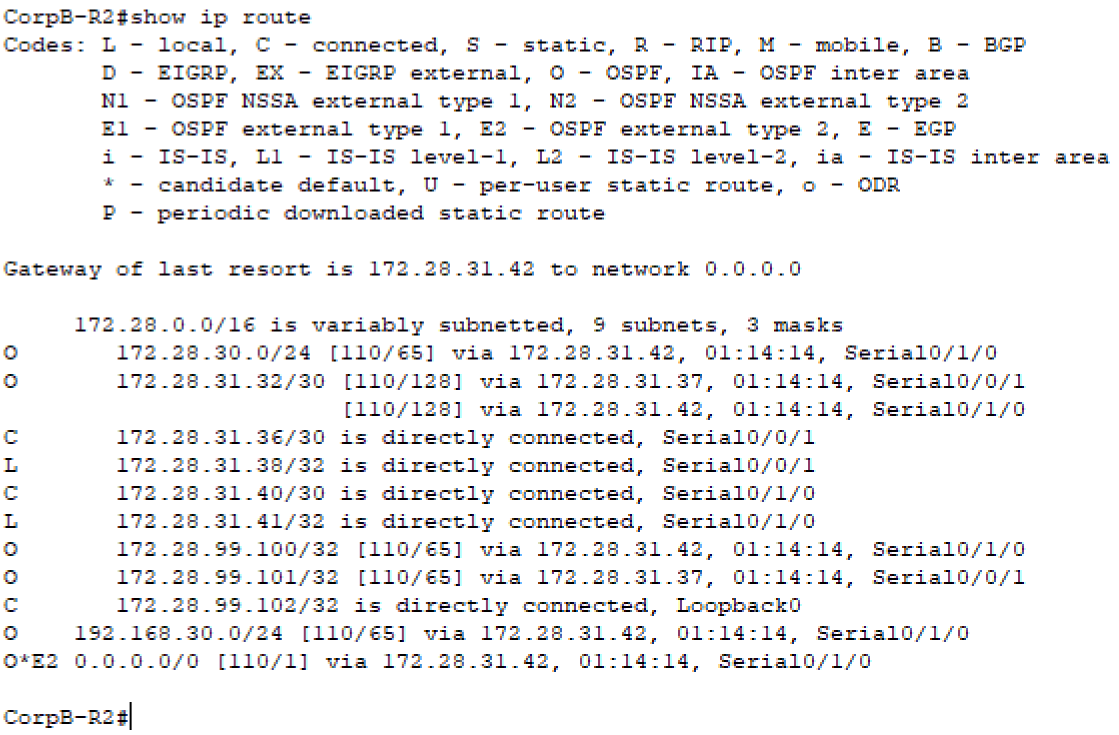
```
CorpB#show ip ospf interface

Loopback0 is up, line protocol is up
  Internet address is 172.28.99.100/32, Area 0
  Process ID 1, Router ID 172.28.99.100, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
FastEthernet0/1 is up, line protocol is up
  Internet address is 192.168.30.1/24, Area 0
  Process ID 1, Router ID 172.28.99.100, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.28.99.100, Interface address 192.168.30.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  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
FastEthernet0/0 is up, line protocol is up
  Internet address is 172.28.30.1/24, Area 0
  Process ID 1, Router ID 172.28.99.100, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.28.99.100, Interface address 172.28.30.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 3/3, 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
```

This screenshot shows that OSPF is running on CorpB’s interfaces except the one that is facing the ISP.

7. Default Route Injection

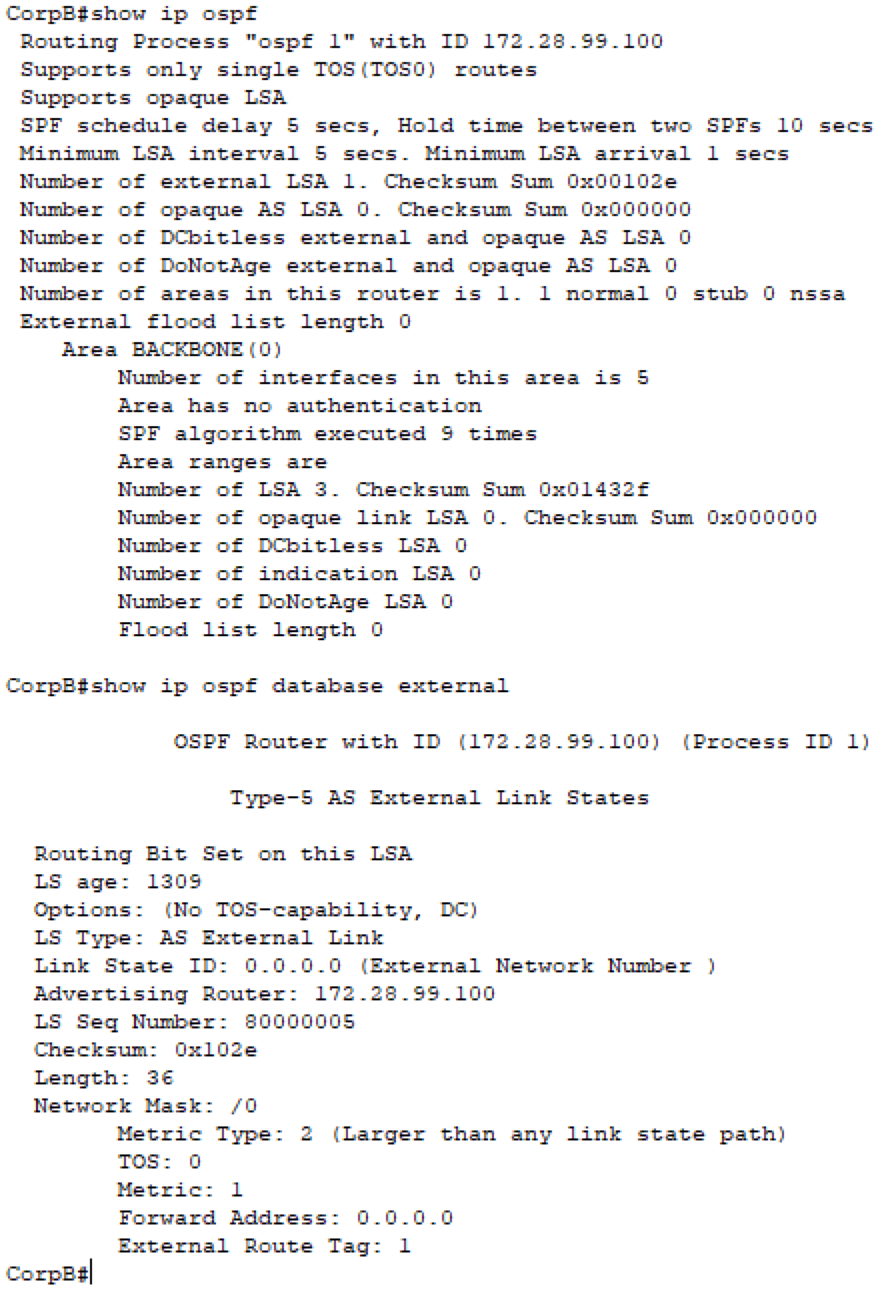


```
CorpB-R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.28.31.33 to network 0.0.0.0

     172.28.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.28.30.0/24 [110/65] via 172.28.31.33, 01:13:43, Serial0/0/0
C       172.28.31.32/30 is directly connected, Serial0/0/0
L       172.28.31.34/32 is directly connected, Serial0/0/0
C       172.28.31.36/30 is directly connected, Serial0/0/1
L       172.28.31.37/32 is directly connected, Serial0/0/1
O       172.28.31.40/30 [110/128] via 172.28.31.38, 01:13:43, Serial0/0/1
                        [110/128] via 172.28.31.33, 01:13:43, Serial0/0/0
O       172.28.99.100/32 [110/65] via 172.28.31.33, 01:13:43, Serial0/0/0
C       172.28.99.101/32 is directly connected, Loopback0
O       172.28.99.102/32 [110/65] via 172.28.31.38, 01:13:53, Serial0/0/1
O    192.168.30.0/24 [110/65] via 172.28.31.33, 01:13:43, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.28.31.33, 01:13:43, Serial0/0/0

CorpB-R1#
```



```
CorpB-R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.28.31.42 to network 0.0.0.0

     172.28.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.28.30.0/24 [110/65] via 172.28.31.42, 01:14:14, Serial0/1/0
O       172.28.31.32/30 [110/128] via 172.28.31.37, 01:14:14, Serial0/0/1
                        [110/128] via 172.28.31.42, 01:14:14, Serial0/1/0
C       172.28.31.36/30 is directly connected, Serial0/0/1
L       172.28.31.38/32 is directly connected, Serial0/0/1
C       172.28.31.40/30 is directly connected, Serial0/1/0
L       172.28.31.41/32 is directly connected, Serial0/1/0
O       172.28.99.100/32 [110/65] via 172.28.31.42, 01:14:14, Serial0/1/0
O       172.28.99.101/32 [110/65] via 172.28.31.37, 01:14:14, Serial0/0/1
C       172.28.99.102/32 is directly connected, Loopback0
O    192.168.30.0/24 [110/65] via 172.28.31.42, 01:14:14, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.28.31.42, 01:14:14, Serial0/1/0

CorpB-R2#
```

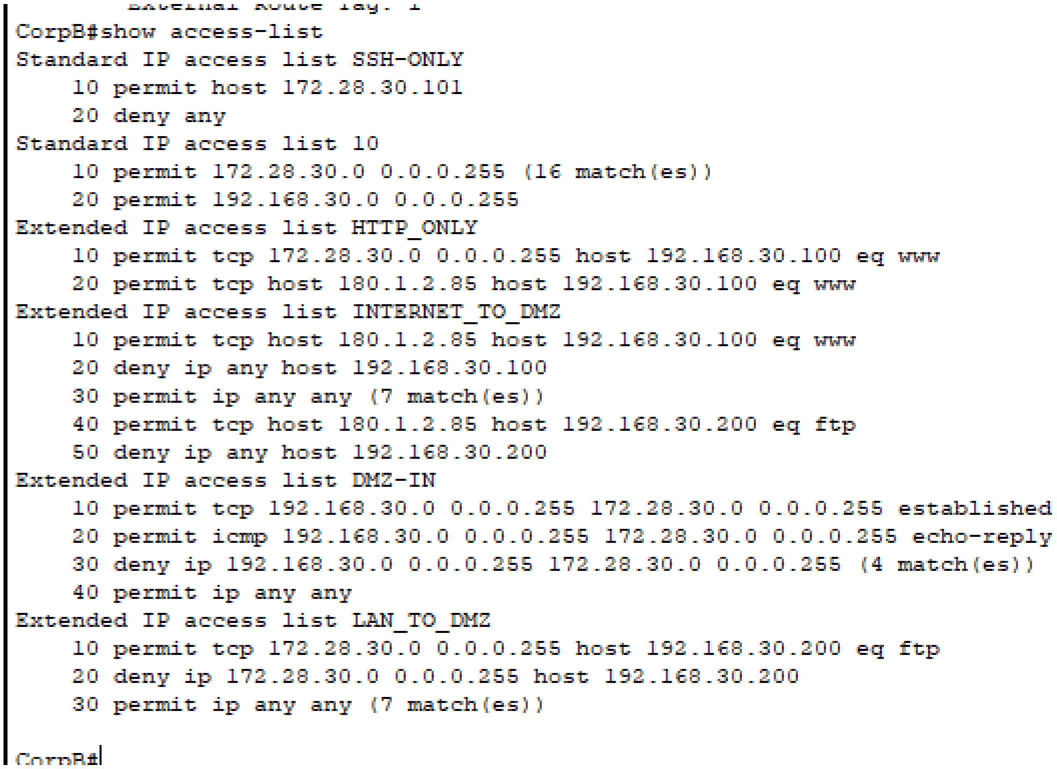
These two screenshots show that CorpB-R1 and CorpB-R2 have learned their default routes through OSPF.



```
CorpB#show ip ospf
 Routing Process "ospf 1" with ID 172.28.99.100
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 1. Checksum Sum 0x00102e
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 5
        Area has no authentication
        SPF algorithm executed 9 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x01432f
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

CorpB#show ip ospf database external

            OSPF Router with ID (172.28.99.100) (Process ID 1)

                Type-5 AS External Link States

  Routing Bit Set on this LSA
  LS age: 1309
  Options: (No TOS-capability, DC)
  LS Type: AS External Link
  Link State ID: 0.0.0.0 (External Network Number )
  Advertising Router: 172.28.99.100
  LS Seq Number: 80000005
  Checksum: 0x102e
  Length: 36
  Network Mask: /0
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 1
        Forward Address: 0.0.0.0
        External Route Tag: 1
CorpB#
```

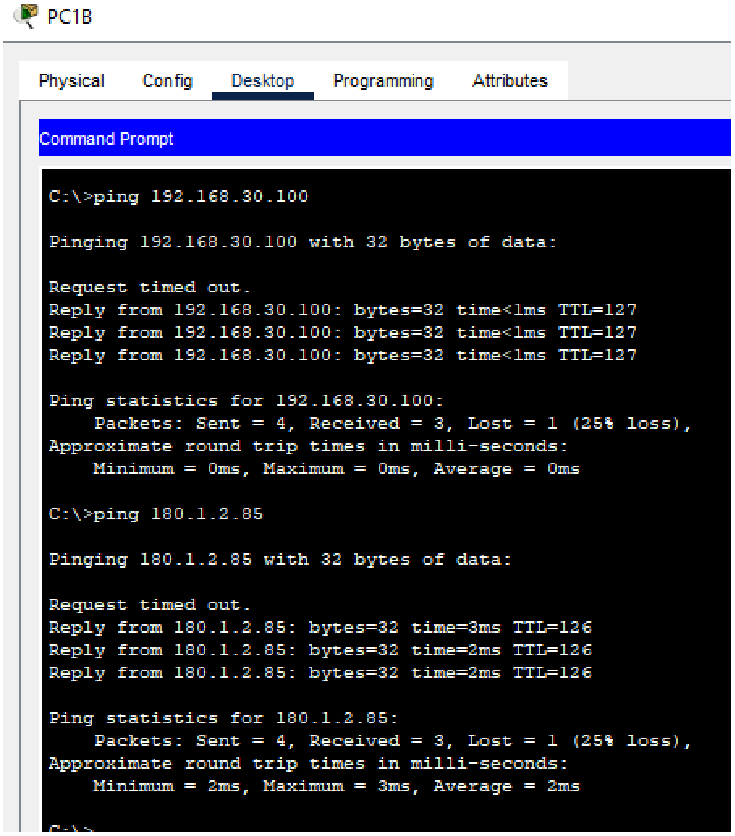
This screenshot shows output of show IP ospf and show IP ospf database external confirming that the default route is being advertised into OSPF by the edge router.

8. DMZ Access Control Lists



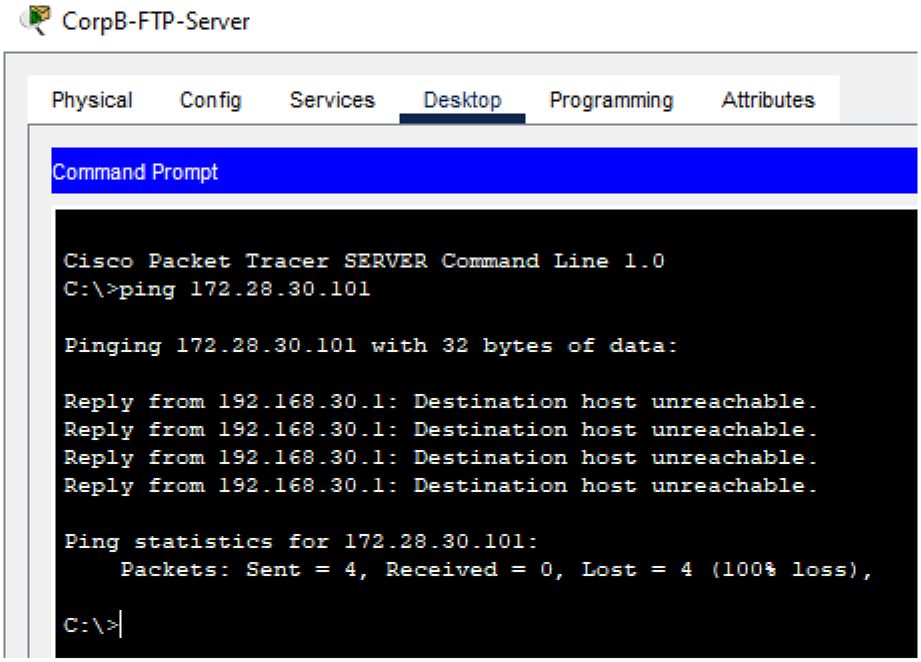
```
        External Route Tag: 1
CorpB#show access-list
Standard IP access list SSH-ONLY
    10 permit host 172.28.30.101
    20 deny any
Standard IP access list 10
    10 permit 172.28.30.0 0.0.0.255 (16 match(es))
    20 permit 192.168.30.0 0.0.0.255
Extended IP access list HTTP_ONLY
    10 permit tcp 172.28.30.0 0.0.0.255 host 192.168.30.100 eq www
    20 permit tcp host 180.1.2.85 host 192.168.30.100 eq www
Extended IP access list INTERNET_TO_DMZ
    10 permit tcp host 180.1.2.85 host 192.168.30.100 eq www
    20 deny ip any host 192.168.30.100
    30 permit ip any any (7 match(es))
    40 permit tcp host 180.1.2.85 host 192.168.30.200 eq ftp
    50 deny ip any host 192.168.30.200
Extended IP access list DMZ-IN
    10 permit tcp 192.168.30.0 0.0.0.255 172.28.30.0 0.0.0.255 established
    20 permit icmp 192.168.30.0 0.0.0.255 172.28.30.0 0.0.0.255 echo-reply
    30 deny ip 192.168.30.0 0.0.0.255 172.28.30.0 0.0.0.255 (4 match(es))
    40 permit ip any any
Extended IP access list LAN_TO_DMZ
    10 permit tcp 172.28.30.0 0.0.0.255 host 192.168.30.200 eq ftp
    20 deny ip 172.28.30.0 0.0.0.255 host 192.168.30.200
    30 permit ip any any (7 match(es))

CorpB#
```

This screenshot shows all of the ACLs on CorpB. The ACL LAN_To_DMZ allows LAN initiated traffic to the FTP server while the ACL DMZ-In denies traffic initiation from the DMZ to the LAN.



```
C:\>ping 192.168.30.100

Pinging 192.168.30.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.100: bytes=32 time<1ms TTL=127
Reply from 192.168.30.100: bytes=32 time<1ms TTL=127
Reply from 192.168.30.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 180.1.2.85

Pinging 180.1.2.85 with 32 bytes of data:

Request timed out.
Reply from 180.1.2.85: bytes=32 time=3ms TTL=126
Reply from 180.1.2.85: bytes=32 time=2ms TTL=126
Reply from 180.1.2.85: bytes=32 time=2ms TTL=126

Ping statistics for 180.1.2.85:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>
```

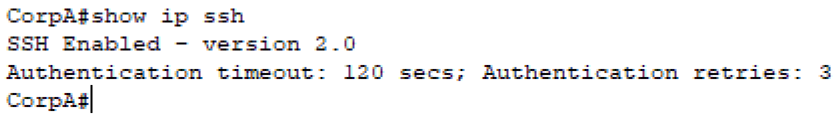
This screenshot shows that PC1B can ping the DMZ server and the ISP -HTTP-Server proving that the ACL works as intended.



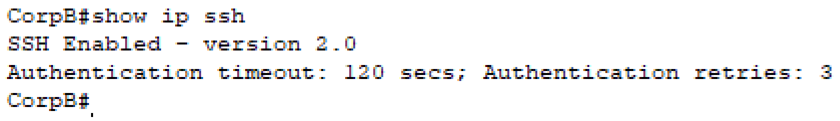
```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 172.28.30.101

Pinging 172.28.30.101 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 172.28.30.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

This screenshot shows that the DMZ is not able to ping a LAN host proving that the ACL works.

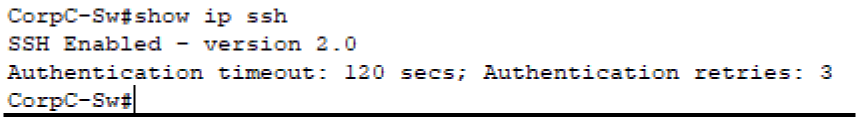
9. SSH



```
CorpA#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
CorpA#
```

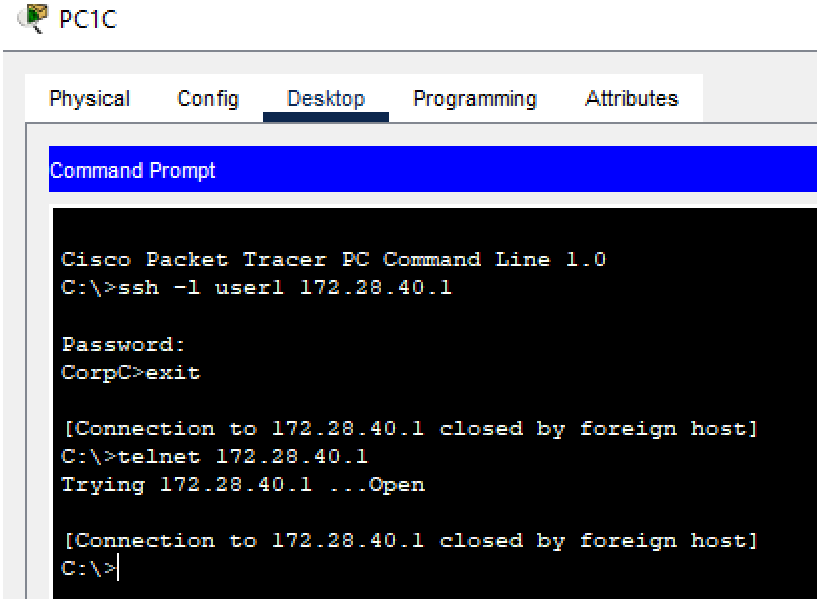


```
CorpB#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
CorpB#
```



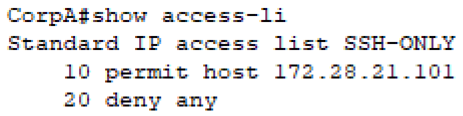
```
CorpC-Sw#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
CorpC-Sw#
```

These screenshots show that ssh is enables on all supported devices.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l user1 172.28.40.1

Password:
CorpC>exit

[Connection to 172.28.40.1 closed by foreign host]
C:\>telnet 172.28.40.1
Trying 172.28.40.1 ...Open

[Connection to 172.28.40.1 closed by foreign host]
C:\>
```

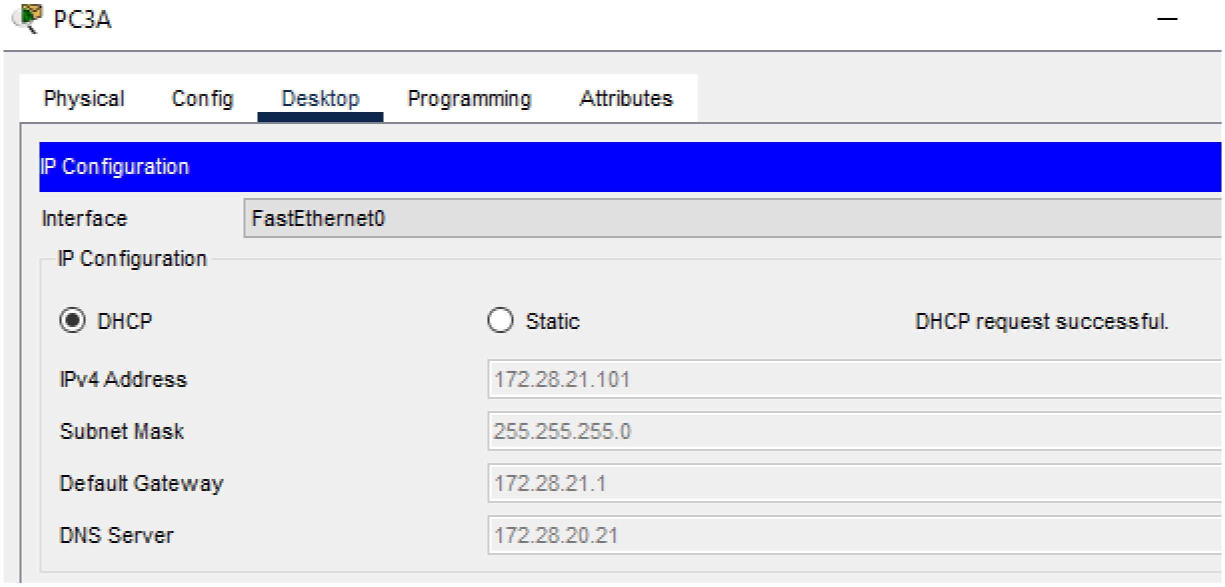
This screenshot shows that PC1C was able to ssh into CorpC but not telnet since it is not allowed.



```
CorpA#show access-li
Standard IP access list SSH-ONLY
    10 permit host 172.28.21.101
    20 deny any
```

This screenshot shows an ACL on CorpA that only allows 172.28.21.101 to be able to ssh into the devices.

10. DHCP


PC3A

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

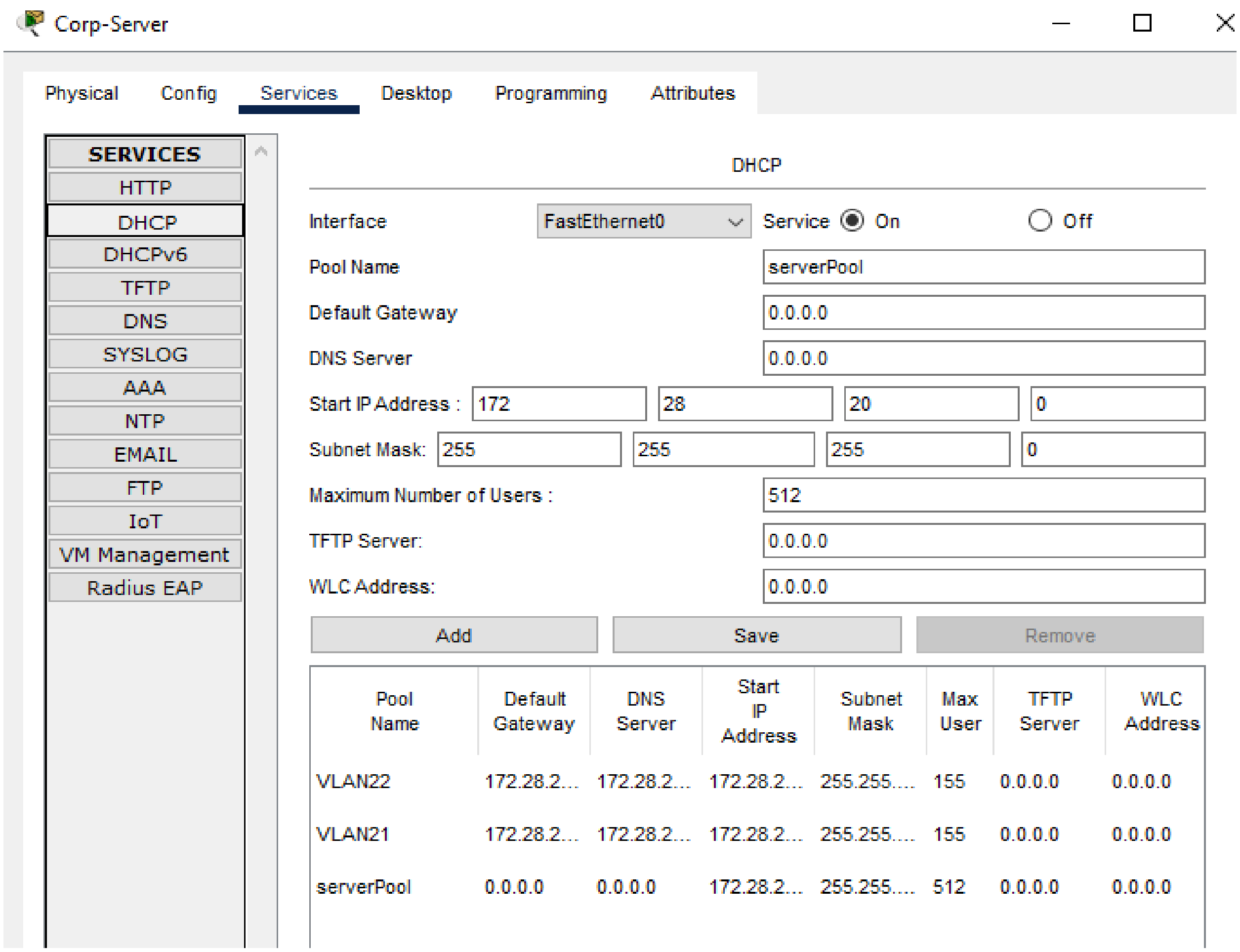
IPv4 Address: 172.28.21.101

Subnet Mask: 255.255.255.0

Default Gateway: 172.28.21.1

DNS Server: 172.28.20.21

This screenshot shows that PC3A receives an IP address, subnet mask, default gateway and DNS server via DHCP.



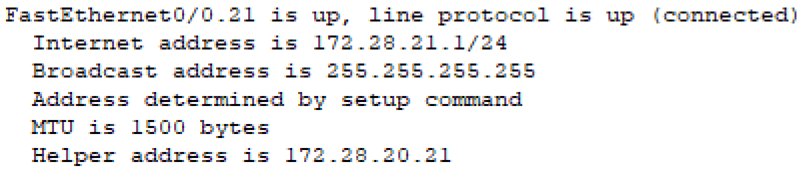
DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name	serverPool
Default Gateway	0.0.0.0
DNS Server	0.0.0.0
Start IP Address :	172 . 28 . 20 . 0
Subnet Mask:	255 . 255 . 255 . 0
Maximum Number of Users :	512
TFTP Server:	0.0.0.0
WLC Address:	0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
VLAN22	172.28.2...	172.28.2...	172.28.2...	255.255....	155	0.0.0.0	0.0.0.0
VLAN21	172.28.2...	172.28.2...	172.28.2...	255.255....	155	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	172.28.2...	255.255....	512	0.0.0.0	0.0.0.0

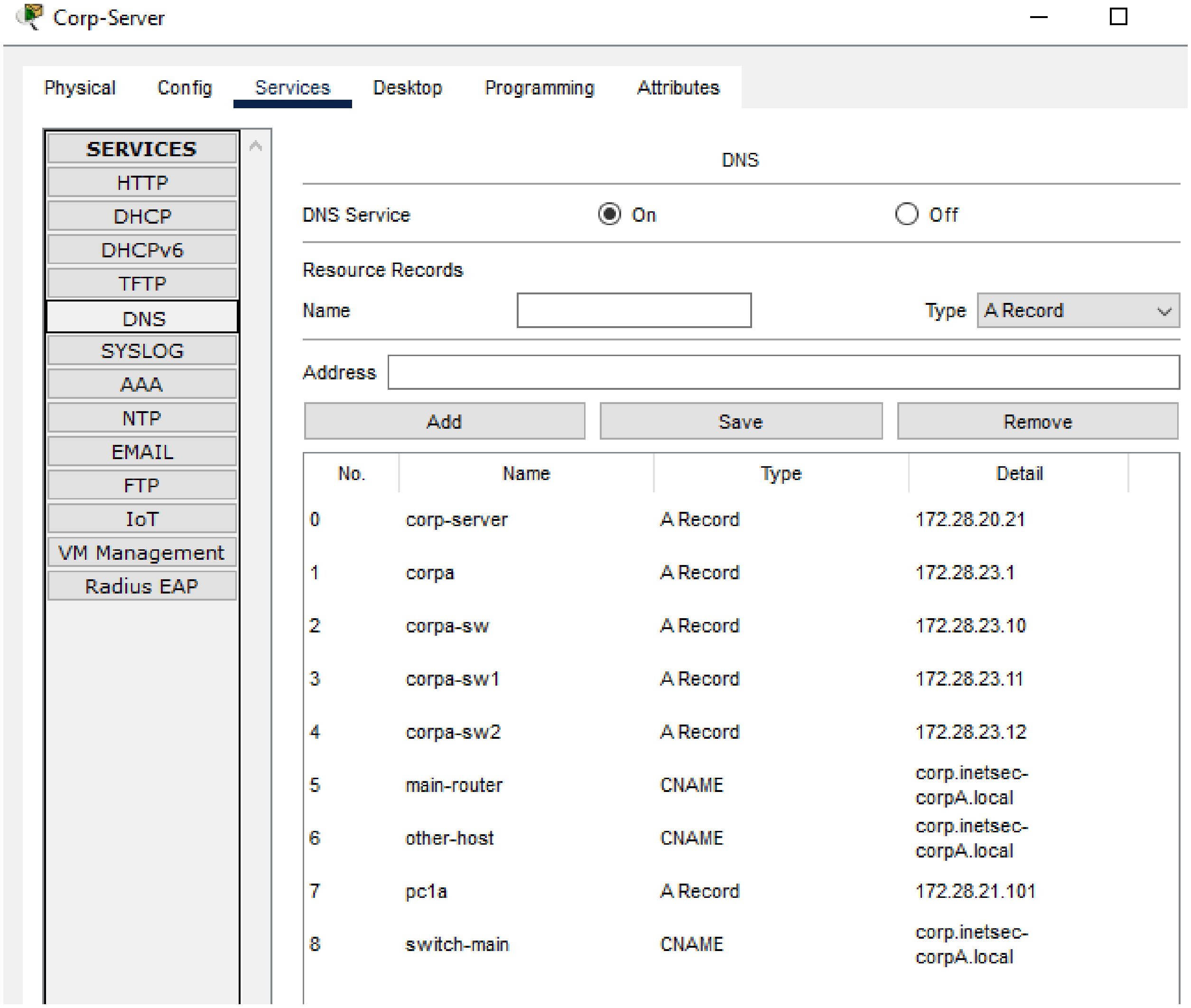
This screenshot shows the DHCP configuration on the Corp-Server with separate scopes for VLAN 21 and 22.



```
FastEthernet0/0.21 is up, line protocol is up (connected)
  Internet address is 172.28.21.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 172.28.20.21
```

This screenshot shows the DHCP helper address of 172.28.20.21.

11. DNS



DNS Service ● On ○ Off

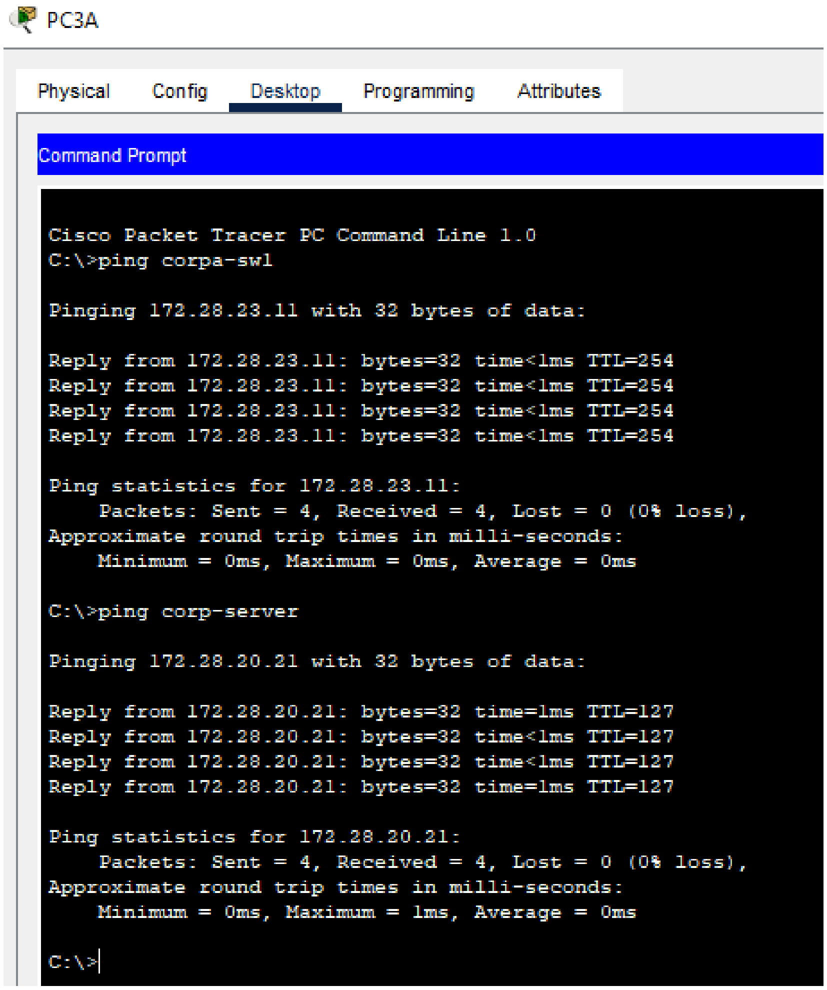
Name

Type: A Record

Address

No.	Name	Type	Detail
0	corp-server	A Record	172.28.20.21
1	corpa	A Record	172.28.23.1
2	corpa-sw	A Record	172.28.23.10
3	corpa-sw1	A Record	172.28.23.11
4	corpa-sw2	A Record	172.28.23.12
5	main-router	CNAME	corp.inetsec-corpA.local
6	other-host	CNAME	corp.inetsec-corpA.local
7	pc1a	A Record	172.28.21.101
8	switch-main	CNAME	corp.inetsec-corpA.local

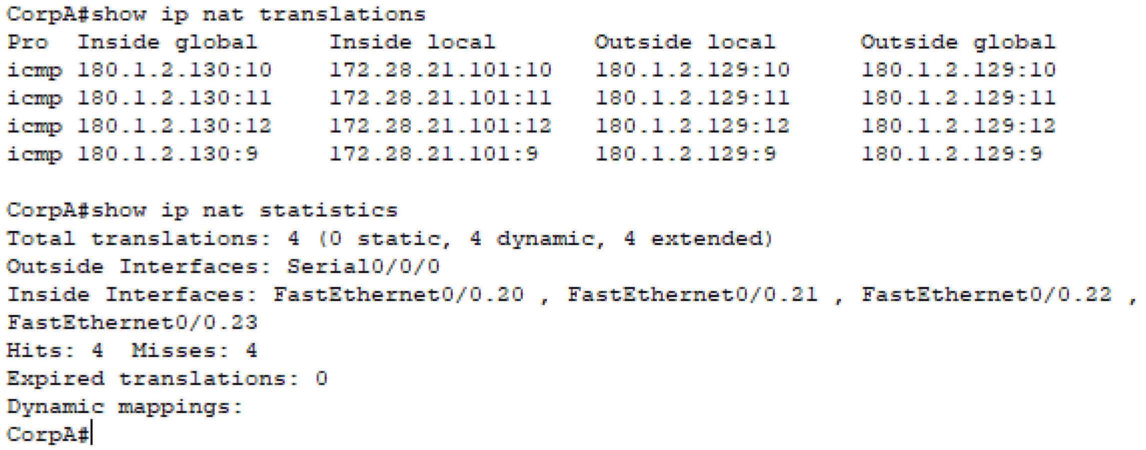
This screenshot shows the DNS server configuration that I made with everything needed being present.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping corpa-sw1

Pinging 172.28.23.11 with 32 bytes of data:

Reply from 172.28.23.11: bytes=32 time<1ms TTL=254
Reply from 172.28.23.11: bytes=32 time<1ms TTL=254
Reply from 172.28.23.11: bytes=32 time<1ms TTL=254
Reply from 172.28.23.11: bytes=32 time<1ms TTL=254

Ping statistics for 172.28.23.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping corp-server

Pinging 172.28.20.21 with 32 bytes of data:

Reply from 172.28.20.21: bytes=32 time=1ms TTL=127
Reply from 172.28.20.21: bytes=32 time<1ms TTL=127
Reply from 172.28.20.21: bytes=32 time<1ms TTL=127
Reply from 172.28.20.21: bytes=32 time=1ms TTL=127

Ping statistics for 172.28.20.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

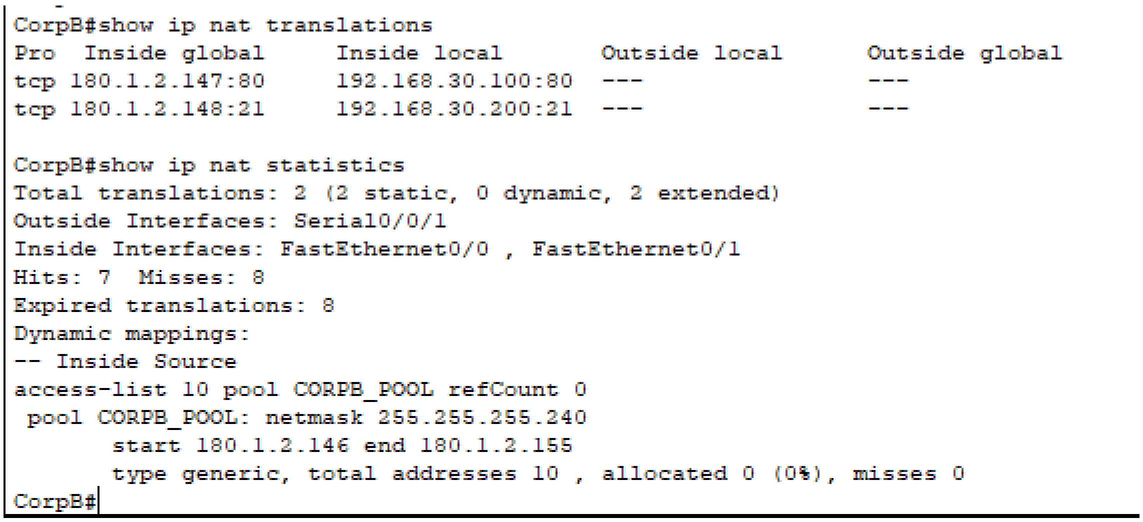
This screenshot shows that DNS resolutions are successful and can be pinged by PCs.

12. PAT



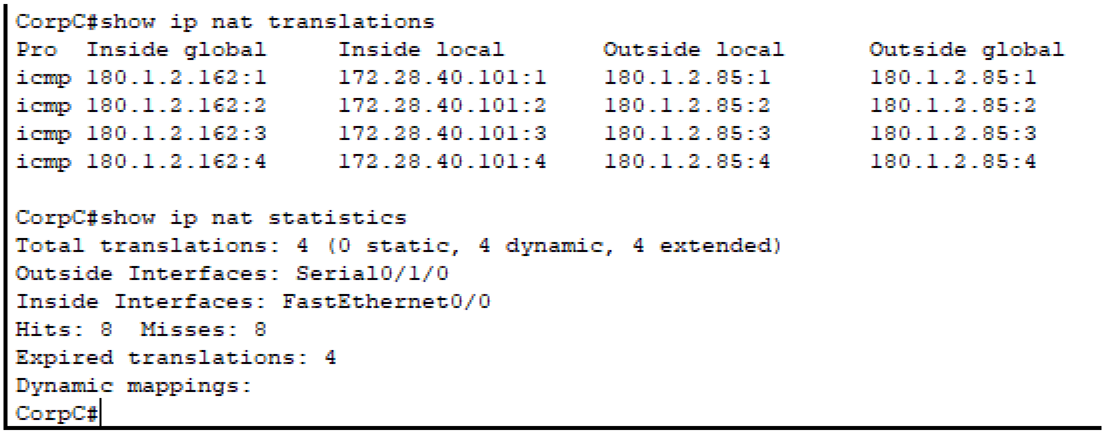
```
CorpA#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 180.1.2.130:10    172.28.21.101:10   180.1.2.129:10     180.1.2.129:10
icmp 180.1.2.130:11    172.28.21.101:11   180.1.2.129:11     180.1.2.129:11
icmp 180.1.2.130:12    172.28.21.101:12   180.1.2.129:12     180.1.2.129:12
icmp 180.1.2.130:9     172.28.21.101:9    180.1.2.129:9      180.1.2.129:9

CorpA#show ip nat statistics
Total translations: 4 (0 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: FastEthernet0/0.20 , FastEthernet0/0.21 , FastEthernet0/0.22 ,
FastEthernet0/0.23
Hits: 4  Misses: 4
Expired translations: 0
Dynamic mappings:
CorpA#
```

This screenshot shows that PAT is working, translating multiple internal addresses to the outside.



```
CorpB#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 180.1.2.147:80     192.168.30.100:80  ---                ---
tcp 180.1.2.148:21     192.168.30.200:21  ---                ---

CorpB#show ip nat statistics
Total translations: 2 (2 static, 0 dynamic, 2 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: FastEthernet0/0 , FastEthernet0/1
Hits: 7  Misses: 8
Expired translations: 8
Dynamic mappings:
-- Inside Source
access-list 10 pool CORPB_POOL refCount 0
 pool CORPB_POOL: netmask 255.255.255.240
       start 180.1.2.146 end 180.1.2.155
       type generic, total addresses 10 , allocated 0 (0%), misses 0
CorpB#
```

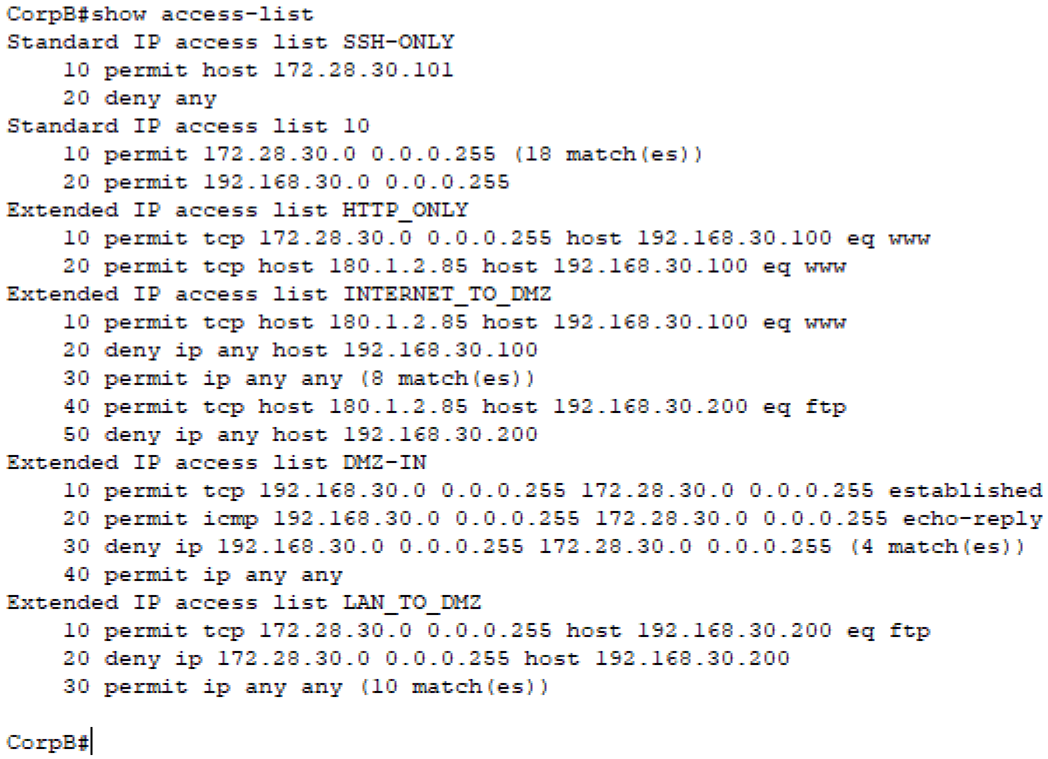
This screenshot shows a NAT pool of 10 addresses that are defined and able to be used for translations.



```
CorpC#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 180.1.2.162:1     172.28.40.101:1    180.1.2.85:1       180.1.2.85:1
icmp 180.1.2.162:2     172.28.40.101:2    180.1.2.85:2       180.1.2.85:2
icmp 180.1.2.162:3     172.28.40.101:3    180.1.2.85:3       180.1.2.85:3
icmp 180.1.2.162:4     172.28.40.101:4    180.1.2.85:4       180.1.2.85:4

CorpC#show ip nat statistics
Total translations: 4 (0 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/1/0
Inside Interfaces: FastEthernet0/0
Hits: 8  Misses: 8
Expired translations: 4
Dynamic mappings:
CorpC#
```

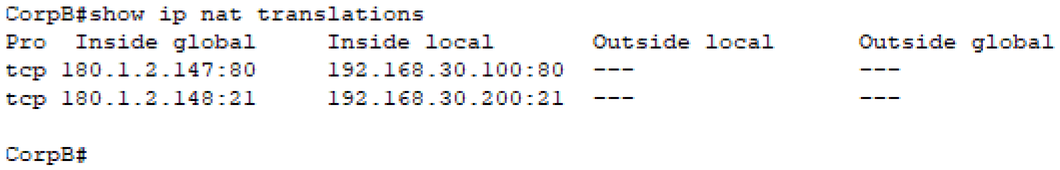
This screenshot shows show ip nat translations and show ip nat statistic commands that confirm NAT with PAT is working on CorpC.

13. HTTP Server Static NAT



```
CorpB#show access-list
Standard IP access list SSH-ONLY
    10 permit host 172.28.30.101
    20 deny any
Standard IP access list 10
    10 permit 172.28.30.0 0.0.0.255 (18 match(es))
    20 permit 192.168.30.0 0.0.0.255
Extended IP access list HTTP_ONLY
    10 permit tcp 172.28.30.0 0.0.0.255 host 192.168.30.100 eq www
    20 permit tcp host 180.1.2.85 host 192.168.30.100 eq www
Extended IP access list INTERNET_TO_DMZ
    10 permit tcp host 180.1.2.85 host 192.168.30.100 eq www
    20 deny ip any host 192.168.30.100
    30 permit ip any any (8 match(es))
    40 permit tcp host 180.1.2.85 host 192.168.30.200 eq ftp
    50 deny ip any host 192.168.30.200
Extended IP access list DMZ-IN
    10 permit tcp 192.168.30.0 0.0.0.255 172.28.30.0 0.0.0.255 established
    20 permit icmp 192.168.30.0 0.0.0.255 172.28.30.0 0.0.0.255 echo-reply
    30 deny ip 192.168.30.0 0.0.0.255 172.28.30.0 0.0.0.255 (4 match(es))
    40 permit ip any any
Extended IP access list LAN_TO_DMZ
    10 permit tcp 172.28.30.0 0.0.0.255 host 192.168.30.200 eq ftp
    20 deny ip 172.28.30.0 0.0.0.255 host 192.168.30.200
    30 permit ip any any (10 match(es))

CorpB#
```

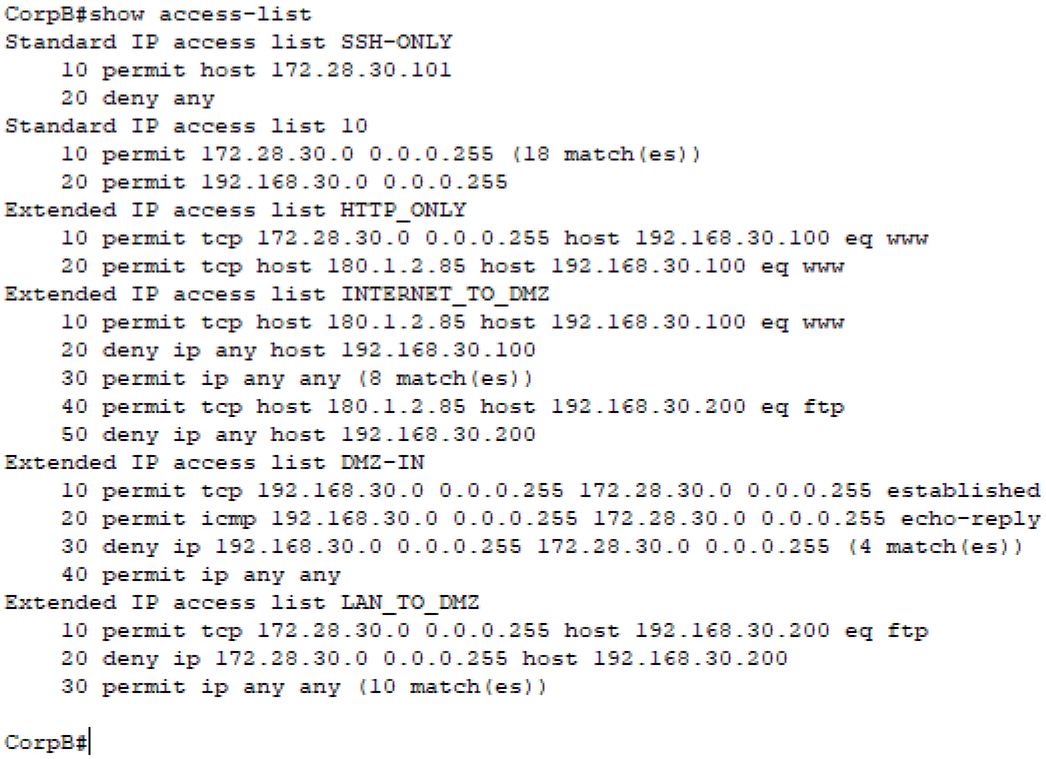
This screenshot shows the configured ACLs I have on CorpB. The HTTP_ONLY and INTERNET_TO_DMZ ACLs are used to allow HTTP traffic to the DMZ server from both internal and external sources, while explicitly denying all other types of traffic.



```
CorpB#show ip nat translations
Pro  Inside global      Inside local       Outside local      Outside global
tcp 180.1.2.147:80     192.168.30.100:80  ---                ---
tcp 180.1.2.148:21     192.168.30.200:21  ---                ---

CorpB#
```

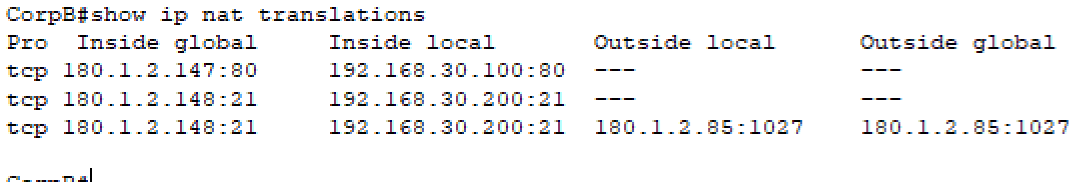
This screenshot shows that the static NAT has been configured successfully and is translating 180.1.2.147 to the internal HTTP server 192.168.30.100 proving that the HTTP traffic is being correctly redirected.

14. FTP Server Static NAT



```
CorpB#show access-list
Standard IP access list SSH-ONLY
    10 permit host 172.28.30.101
    20 deny any
Standard IP access list 10
    10 permit 172.28.30.0 0.0.0.255 (18 match(es))
    20 permit 192.168.30.0 0.0.0.255
Extended IP access list HTTP_ONLY
    10 permit tcp 172.28.30.0 0.0.0.255 host 192.168.30.100 eq www
    20 permit tcp host 180.1.2.85 host 192.168.30.100 eq www
Extended IP access list INTERNET_TO_DMZ
    10 permit tcp host 180.1.2.85 host 192.168.30.100 eq www
    20 deny ip any host 192.168.30.100
    30 permit ip any any (8 match(es))
    40 permit tcp host 180.1.2.85 host 192.168.30.200 eq ftp
    50 deny ip any host 192.168.30.200
Extended IP access list DMZ-IN
    10 permit tcp 192.168.30.0 0.0.0.255 172.28.30.0 0.0.0.255 established
    20 permit icmp 192.168.30.0 0.0.0.255 172.28.30.0 0.0.0.255 echo-reply
    30 deny ip 192.168.30.0 0.0.0.255 172.28.30.0 0.0.0.255 (4 match(es))
    40 permit ip any any
Extended IP access list LAN_TO_DMZ
    10 permit tcp 172.28.30.0 0.0.0.255 host 192.168.30.200 eq ftp
    20 deny ip 172.28.30.0 0.0.0.255 host 192.168.30.200
    30 permit ip any any (10 match(es))

CorpB#
```

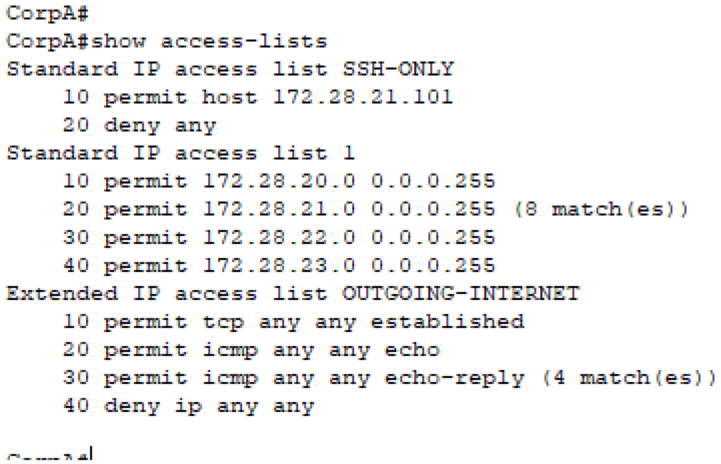
This screenshot once again shows the corpb acls, but the one we are focused on here is “permit tcp host 180.1.2.85 host 192.168.30.200 eq ftp” which allows FTP and “deny an host 192.168.30.200” that denies everything else.



```
CorpB#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 180.1.2.147:80     192.168.30.100:80  ---                ---
tcp 180.1.2.148:21     192.168.30.200:21  ---                ---
tcp 180.1.2.148:21     192.168.30.200:21  180.1.2.85:1027    180.1.2.85:1027

CorpB#
```

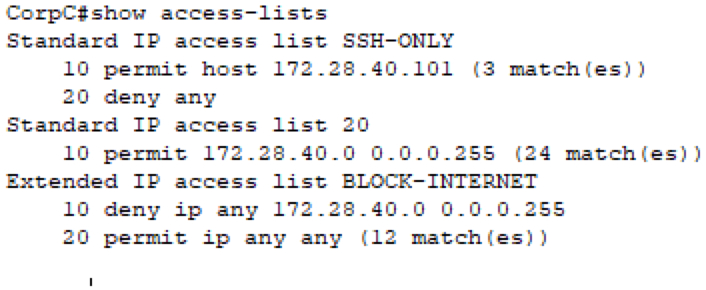
This screenshot shows an active static NAT translation for FTP, confirming that the FTP session from the internet to the FTP server is functional.

15. Primitive Firewall



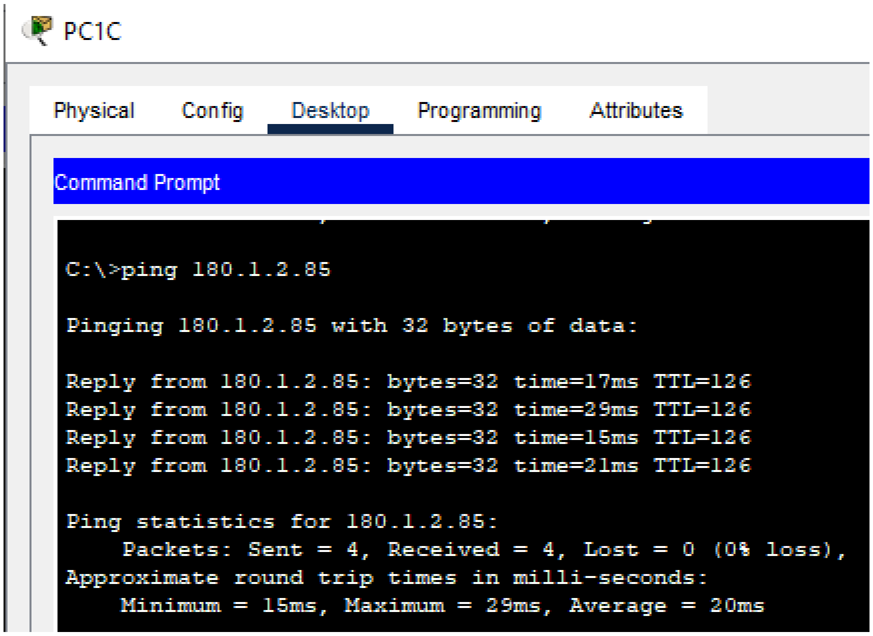
```
CorpA#
CorpA#show access-lists
Standard IP access list SSH-ONLY
    10 permit host 172.28.21.101
    20 deny any
Standard IP access list 1
    10 permit 172.28.20.0 0.0.0.255
    20 permit 172.28.21.0 0.0.0.255 (8 match(es))
    30 permit 172.28.22.0 0.0.0.255
    40 permit 172.28.23.0 0.0.0.255
Extended IP access list OUTGOING-INTERNET
    10 permit tcp any any established
    20 permit icmp any any echo
    30 permit icmp any any echo-reply (4 match(es))
    40 deny ip any any

CorpA#
```

This screenshot shows the OUTGOING-INTERNET extended ACL applied on the CorpA router to enforce a primitive firewall. It allows return traffic and ICMP echo requests/replies, while denying all other inbound traffic, effectively protecting the internal network from unsolicited connections.



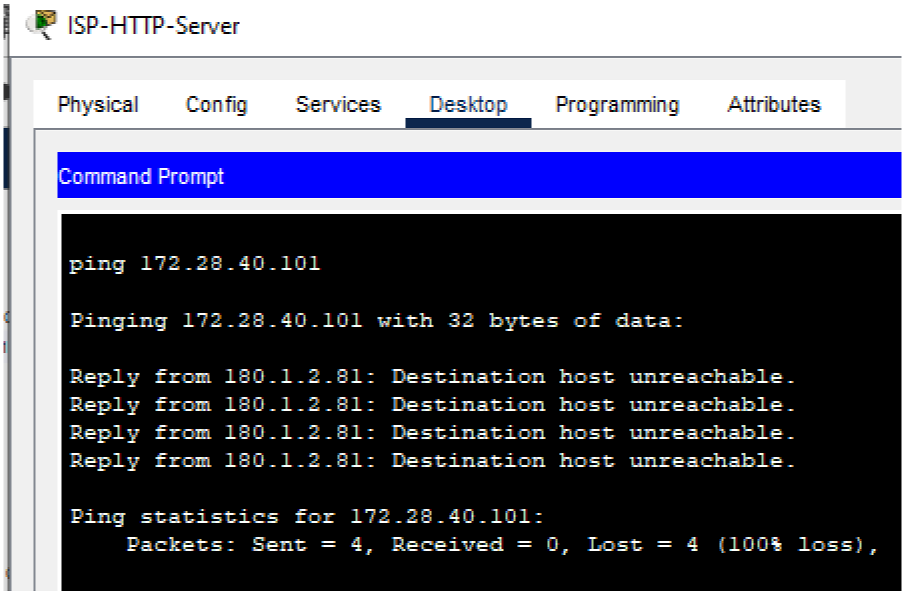
```
CorpC#show access-lists
Standard IP access list SSH-ONLY
    10 permit host 172.28.40.101 (3 match(es))
    20 deny any
Standard IP access list 20
    10 permit 172.28.40.0 0.0.0.255 (24 match(es))
Extended IP access list BLOCK-INTERNET
    10 deny ip any 172.28.40.0 0.0.0.255
    20 permit ip any any (12 match(es))
```

This screenshot shows that the BLOCK-INTERNET extended ACL is configured on CorpC to deny all inbound traffic from any source to the CorpC LAN.



```
C:\>ping 180.1.2.85

Pinging 180.1.2.85 with 32 bytes of data:

Reply from 180.1.2.85: bytes=32 time=17ms TTL=126
Reply from 180.1.2.85: bytes=32 time=29ms TTL=126
Reply from 180.1.2.85: bytes=32 time=15ms TTL=126
Reply from 180.1.2.85: bytes=32 time=21ms TTL=126

Ping statistics for 180.1.2.85:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 29ms, Average = 20ms
```

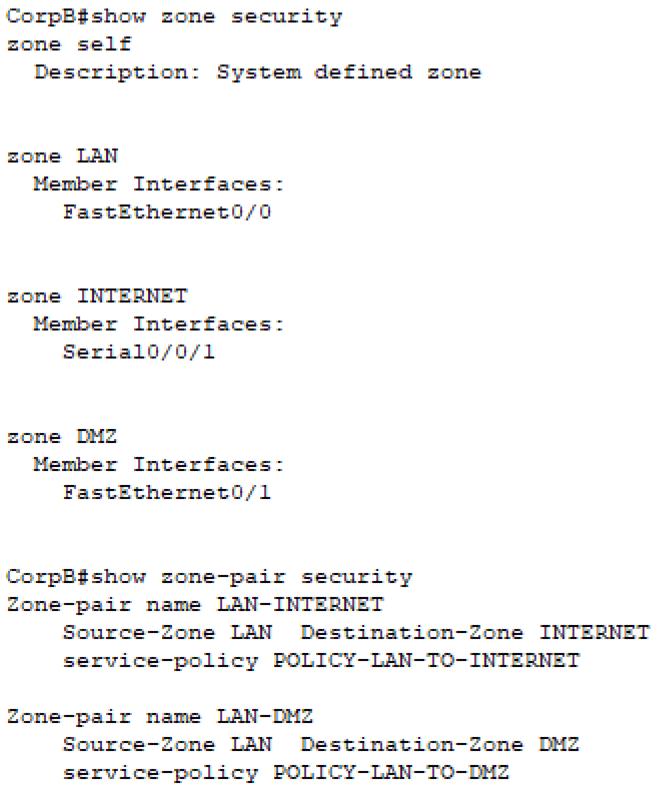
This screenshot shows a ping from inside CorpC to ISP-HTTP-Server succeeds.



```
ping 172.28.40.101

Pinging 172.28.40.101 with 32 bytes of data:

Reply from 180.1.2.81: Destination host unreachable.
Reply from 180.1.2.81: Destination host unreachable.
Reply from 180.1.2.81: Destination host unreachable.
Reply from 180.1.2.81: Destination host unreachable.

Ping statistics for 172.28.40.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

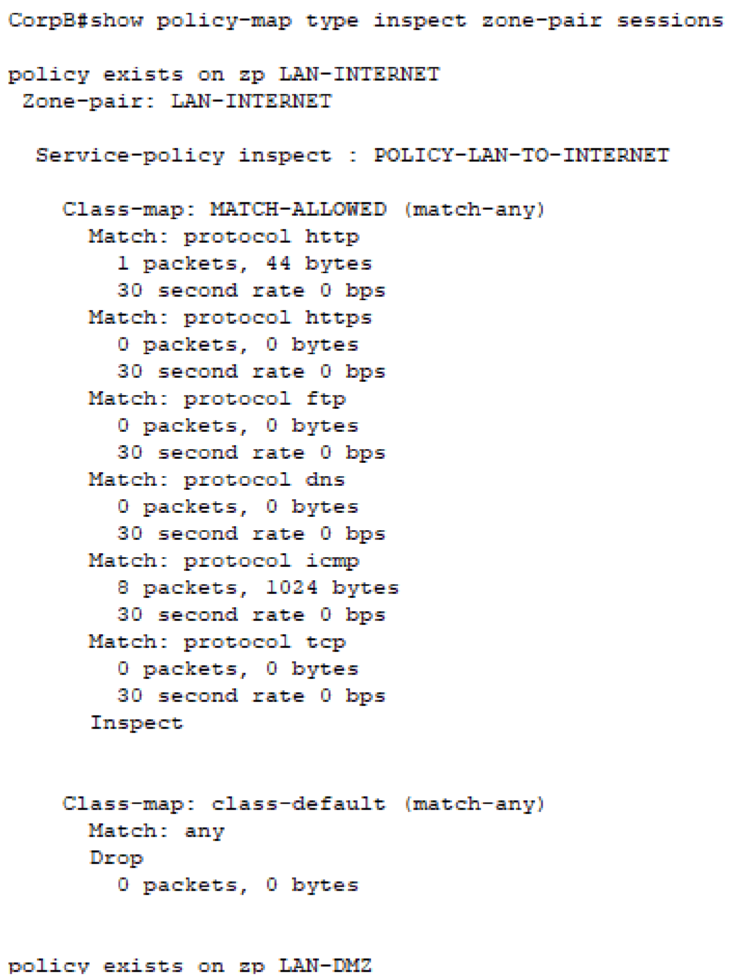
This screenshot shows a ping from ISP-HTTP-Server that fails proving that the ACL functions as intended.

16. Zone-Based Firewall



```
CorpB#show zone security
zone self
  Description: System defined zone


zone LAN
  Member Interfaces:
    FastEthernet0/0


zone INTERNET
  Member Interfaces:
    Serial0/0/1


zone DMZ
  Member Interfaces:
    FastEthernet0/1


CorpB#show zone-pair security
Zone-pair name LAN-INTERNET
    Source-Zone LAN  Destination-Zone INTERNET
    service-policy POLICY-LAN-TO-INTERNET

Zone-pair name LAN-DMZ
    Source-Zone LAN  Destination-Zone DMZ
    service-policy POLICY-LAN-TO-DMZ
```

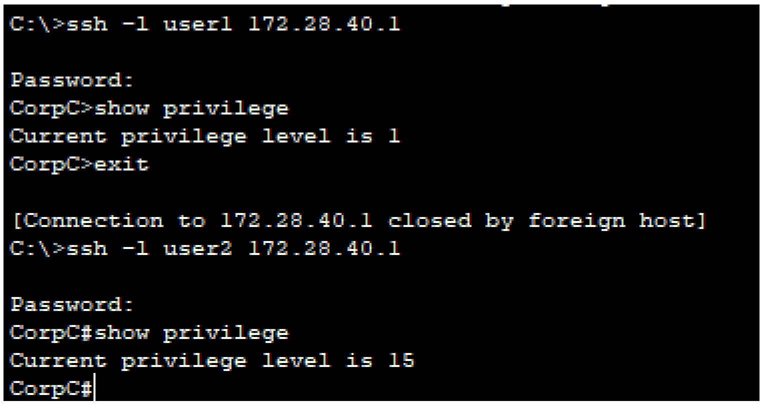
This screenshot shows the configured security zones and the interfaces associated with them. It also shows zone pairs LAN-INTERNET and LAN-DMZ which both have their own service policies which make sure that only LAN initiated traffic is allowed and inspected.



```
CorpB#show policy-map type inspect zone-pair sessions

policy exists on zp LAN-INTERNET
 Zone-pair: LAN-INTERNET

  Service-policy inspect : POLICY-LAN-TO-INTERNET

    Class-map: MATCH-ALLOWED (match-any)
      Match: protocol http
        1 packets, 44 bytes
        30 second rate 0 bps
      Match: protocol https
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol ftp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol dns
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol icmp
        8 packets, 1024 bytes
        30 second rate 0 bps
      Match: protocol tcp
        0 packets, 0 bytes
        30 second rate 0 bps
      Inspect


    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes


policy exists on zp LAN-DMZ
```

This screenshot shows the active zone pair policy LAN-TO-INTERNET on CorpB. It proves that protocols like HTTP, ICMP and others are inspected from LAN to Internet.

17. Local AAA



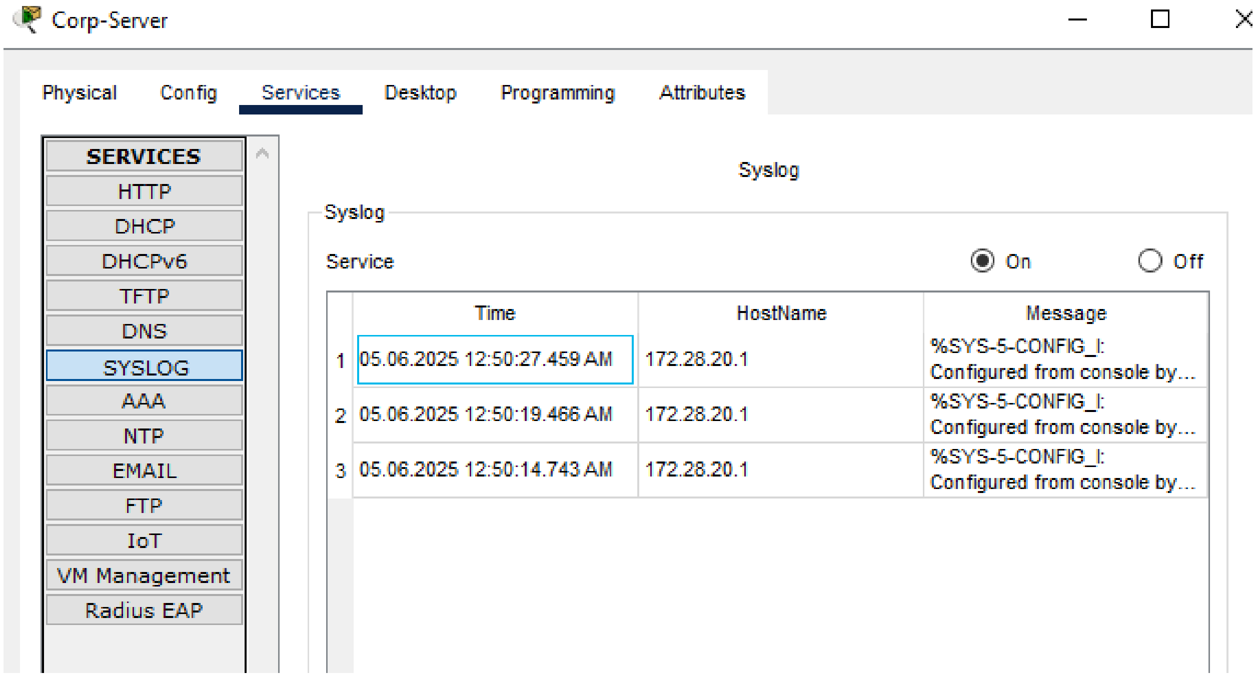
```
C:\>ssh -l user1 172.28.40.1

Password:
CorpC>show privilege
Current privilege level is 1
CorpC>exit

[Connection to 172.28.40.1 closed by foreign host]
C:\>ssh -l user2 172.28.40.1

Password:
CorpC#show privilege
Current privilege level is 15
CorpC#
```

This screenshot shows that I can log in with SSH from PC1C using local AAA. Logging in with user1 only shows that our privilege level is 1 but user2 shows a privilege level of 15.

18. Server-based AAA

I chose to exclude this technology.

19. Syslog



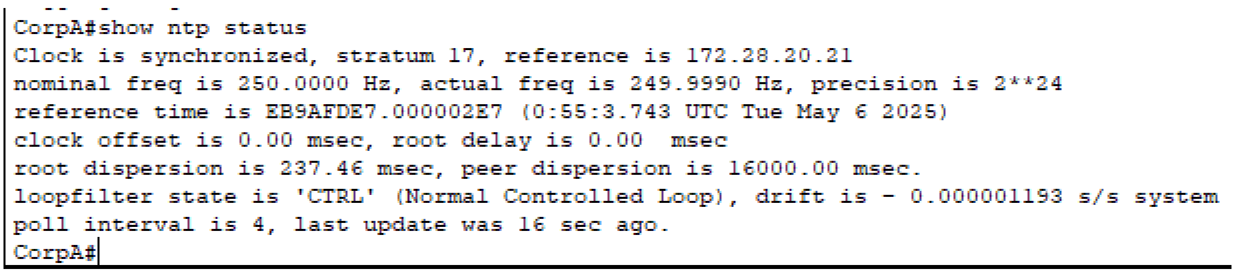
Syslog

Service ● On ○ Off

	Time	HostName	Message
1	05.06.2025 12:50:27.459 AM	172.28.20.1	%SYS-5-CONFIG_I: Configured from console by...
2	05.06.2025 12:50:19.466 AM	172.28.20.1	%SYS-5-CONFIG_I: Configured from console by...
3	05.06.2025 12:50:14.743 AM	172.28.20.1	%SYS-5-CONFIG_I: Configured from console by...

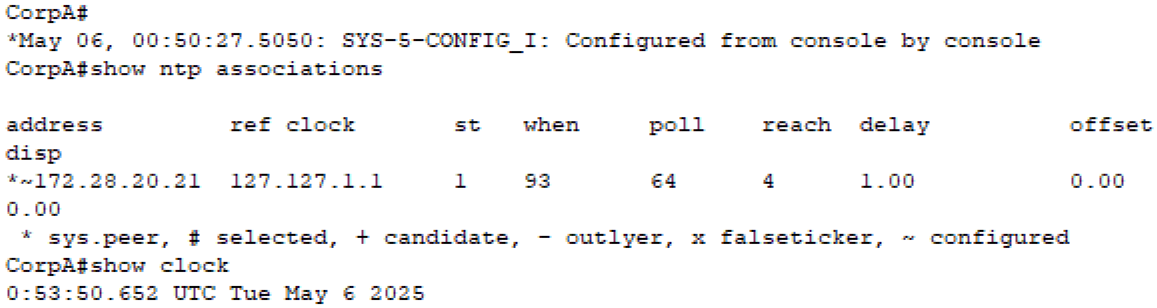
This screenshot shows three logs from exiting configuration mode on the Corp-Server Syslog feature from 172.28.20.1 (CorpA).

20. NTP



```
CorpA#show ntp status
Clock is synchronized, stratum 17, reference is 172.28.20.21
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is EB9AFDE7.000002E7 (0:55:3.743 UTC Tue May 6 2025)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 237.46 msec, peer dispersion is 16000.00 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 4, last update was 16 sec ago.
CorpA#
```

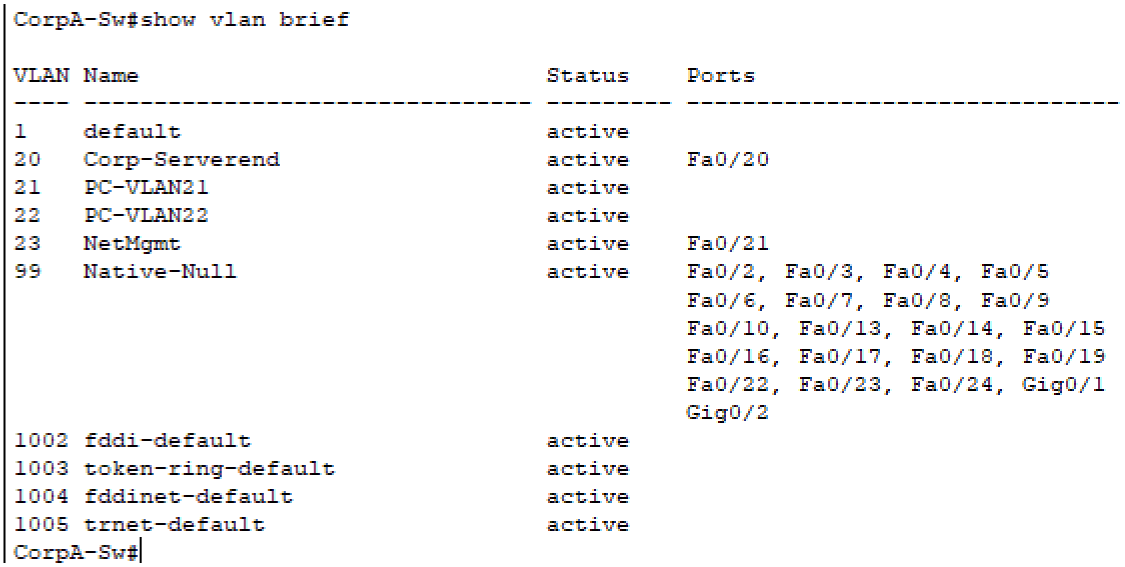
This screenshot shows the output of show ntp status and proves that the router is synchronized with the Corp-Server and is stable.



```
CorpA#
*May 06, 00:50:27.5050: SYS-5-CONFIG_I: Configured from console by console
CorpA#show ntp associations

address          ref clock        st   when     poll    reach  delay           offset
disp
*~172.28.20.21   127.127.1.1      1    93       64      4      1.00            0.00
0.00
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
CorpA#show clock
0:53:50.652 UTC Tue May 6 2025
```

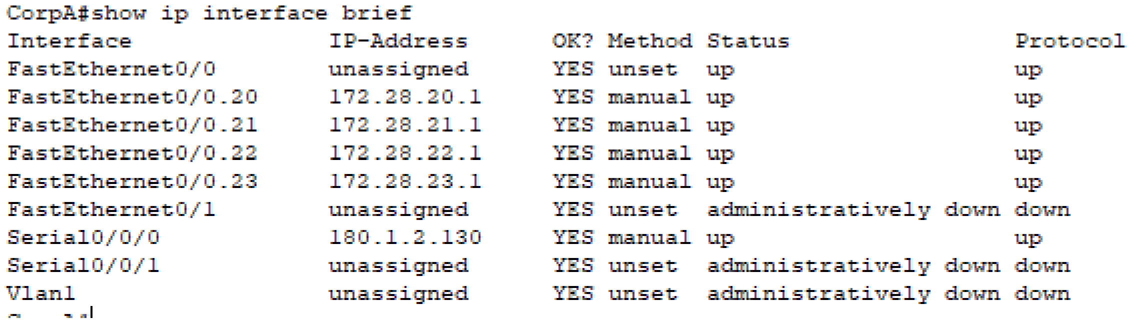
This screenshot shows more evidence that CorpA is synced with the Corp-Server.

21.   InterVLAN Routing



```
CorpA-Sw#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
20   Corp-Serverend                   active    Fa0/20
21   PC-VLAN21                        active
22   PC-VLAN22                        active
23   NetMgmt                          active    Fa0/21
99   Native-Null                      active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                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
CorpA-Sw#
```

This screenshot shows the output of show vlan brief on CorpA-Sw confirming that VLAN 23 exists and is named NetMgmt, reserved for administrative access.



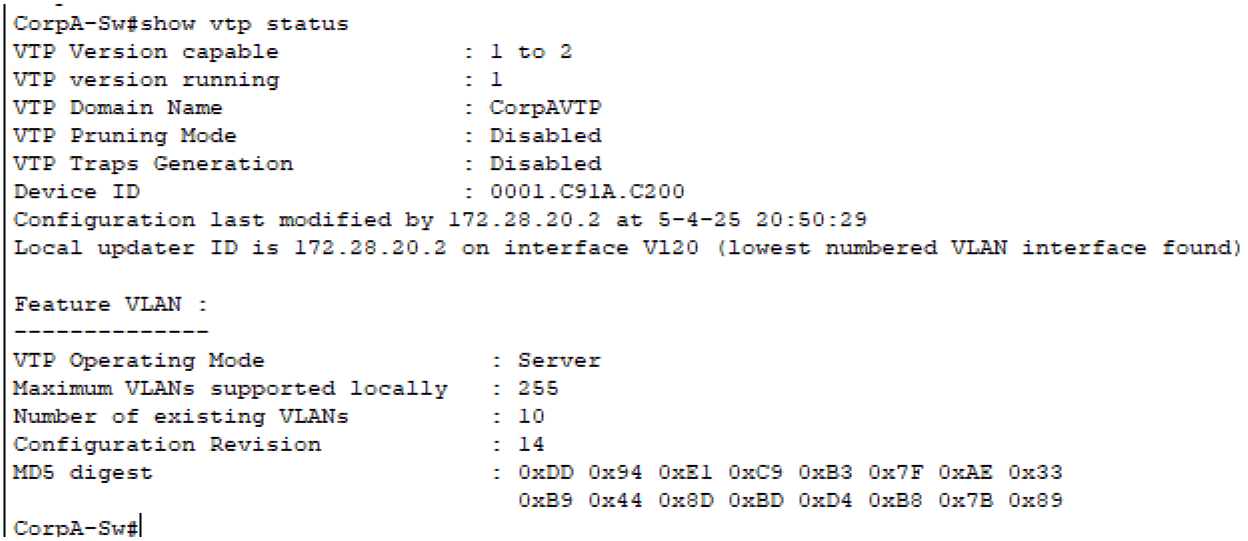
```
CorpA#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  up                    up
FastEthernet0/0.20     172.28.20.1     YES manual up                    up
FastEthernet0/0.21     172.28.21.1     YES manual up                    up
FastEthernet0/0.22     172.28.22.1     YES manual up                    up
FastEthernet0/0.23     172.28.23.1     YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/0/0            180.1.2.130     YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

This screenshot shows output of show ip interface brief on CorpA confirming that the router is performing interVLAN routing across VLANs 20-23.

22. IPSec VPN

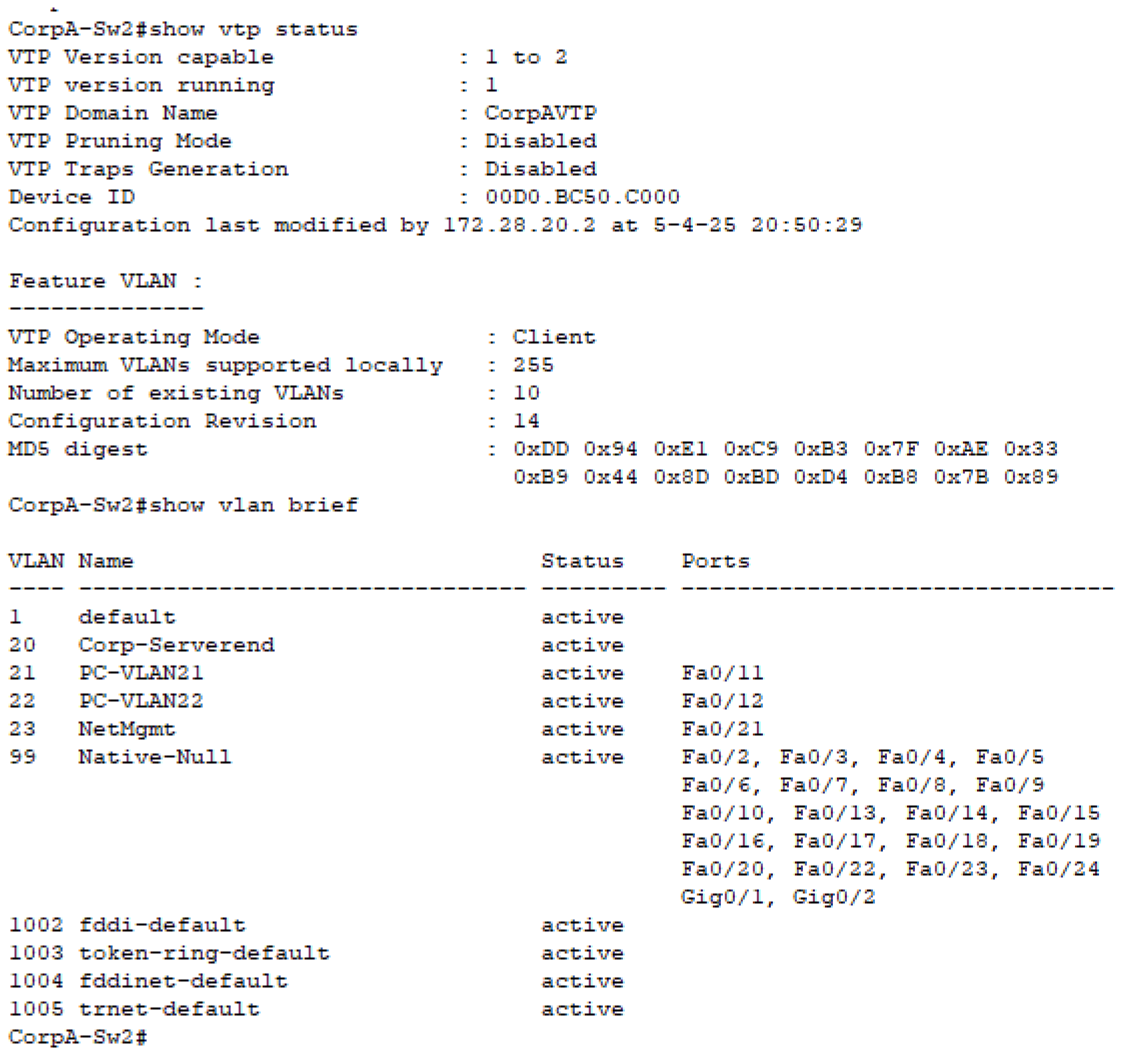
I configured the IPSec VPN between CorpA andCorpC and was able to get Phase 1 and Phase 2 seemingly working. Unfortunately the tunnel never fully opened and traffic from CorpA to CorpC did not pass through. I tried troubleshooting for a while but in the end did not get it to work.

23. VTP



```
CorpA-Sw#show vtp status
VTP Version capable              : 1 to 2
VTP version running              : 1
VTP Domain Name                  : CorpAVTP
VTP Pruning Mode                 : Disabled
VTP Traps Generation             : Disabled
Device ID                        : 0001.C91A.C200
Configuration last modified by 172.28.20.2 at 5-4-25 20:50:29
Local updater ID is 172.28.20.2 on interface Vl20 (lowest numbered VLAN interface found)

Feature VLAN :
--------------
VTP Operating Mode                 : Server
Maximum VLANs supported locally    : 255
Number of existing VLANs           : 10
Configuration Revision             : 14
MD5 digest                         : 0xDD 0x94 0xE1 0xC9 0xB3 0x7F 0xAE 0x33
                                     0xB9 0x44 0x8D 0xBD 0xD4 0xB8 0x7B 0x89

CorpA-Sw#
```

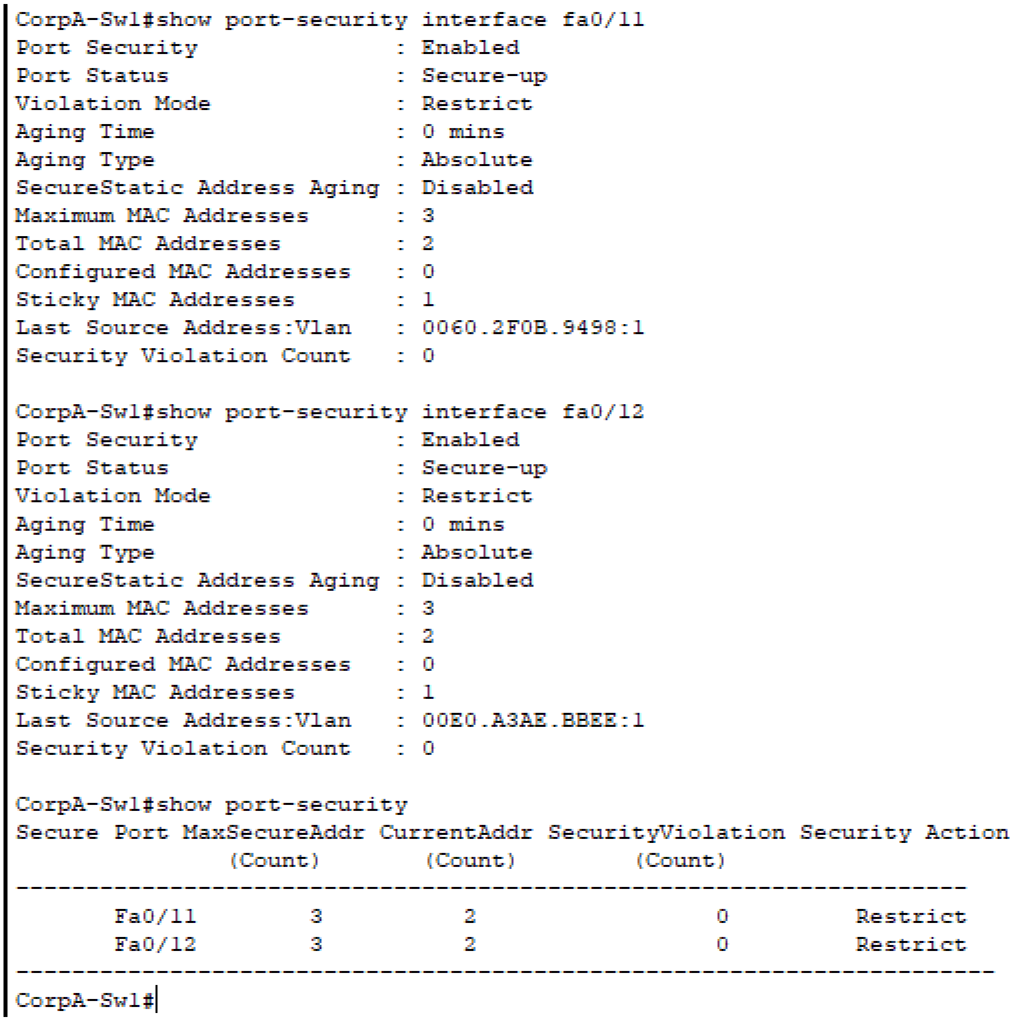
This screenshot shows output from show vtp status on CorpA-Sw confirming that it is the server.



```
CorpA-Sw2#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : CorpAVTP
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 00D0.BC50.C000
Configuration last modified by 172.28.20.2 at 5-4-25 20:50:29

Feature VLAN :
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 10
Configuration Revision            : 14
MD5 digest                        : 0xDD 0x94 0xE1 0xC9 0xB3 0x7F 0xAE 0x33
                                    0xB9 0x44 0x8D 0xBD 0xD4 0xB8 0x7B 0x89
CorpA-Sw2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    
20   Corp-Serverend                   active    
21   PC-VLAN21                        active    Fa0/11
22   PC-VLAN22                        active    Fa0/12
23   NetMgmt                          active    Fa0/21
99   Native-Null                      active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, 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    
CorpA-Sw2#
```

This screenshot shows the output of show vtp status and show vlan brief on CorpA-Sw2 confirming that it is a client and that the VLANs were received via VTP.

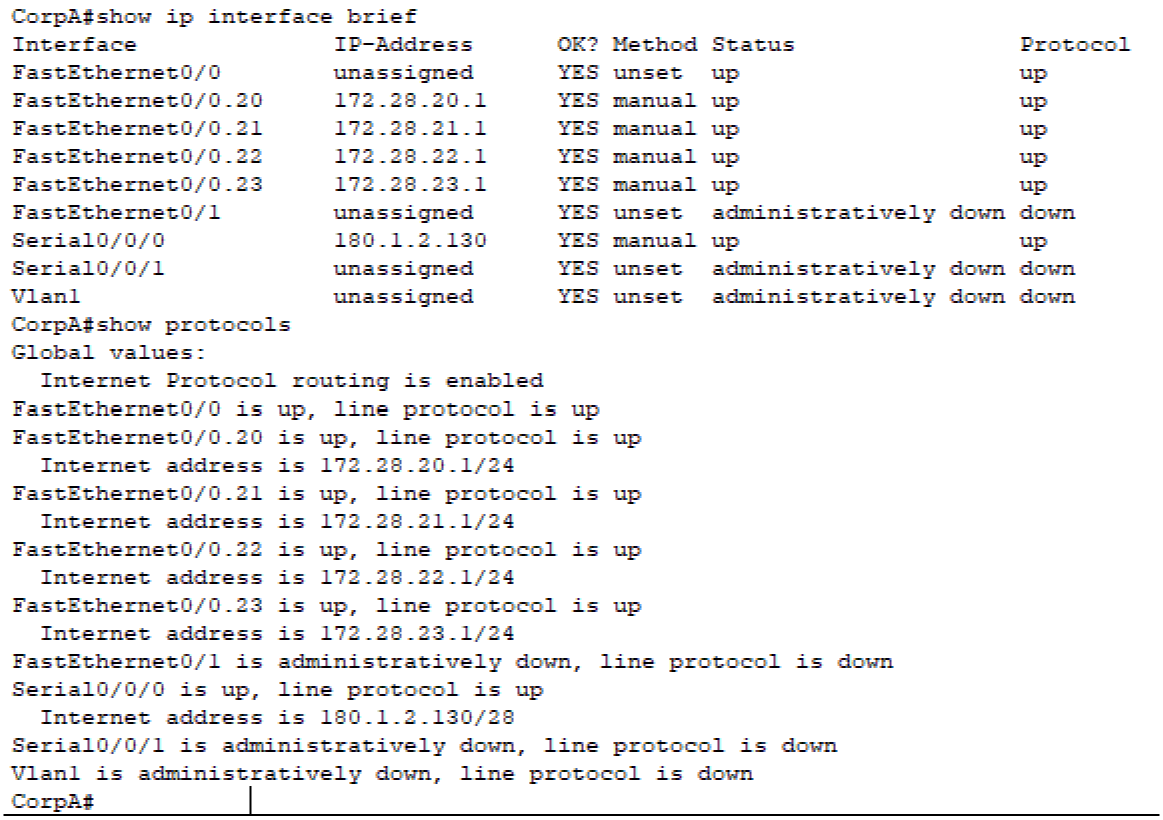
24. Layer 2 Interface Security Mitigation Techniques



```
CorpA-Sw1#show port-security interface fa0/11
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 2
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0060.2F0B.9498:1
Security Violation Count   : 0

CorpA-Sw1#show port-security interface fa0/12
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 2
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00E0.A3AE.BBEE:1
Security Violation Count   : 0

CorpA-Sw1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
--------------------------------------------------------------------
       Fa0/11        3           2                 0         Restrict
       Fa0/12        3           2                 0         Restrict
----------------------------------------------------------------------
CorpA-Sw1#
```

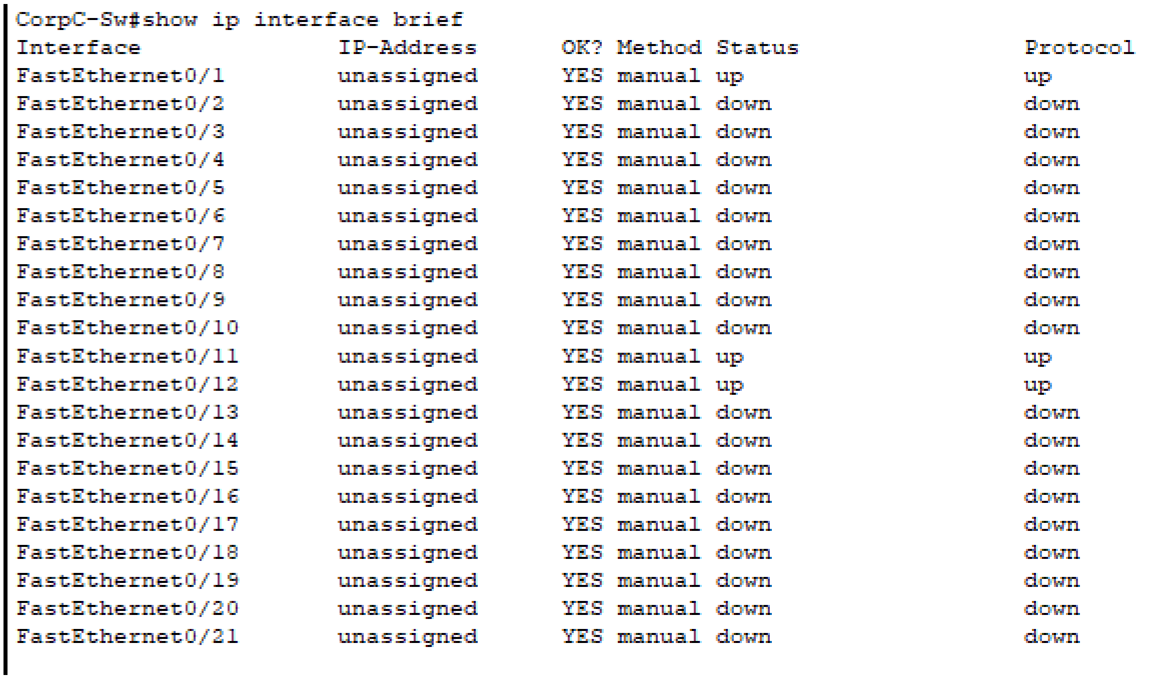
This screenshot shows layer 2 port security that is configured on CorpA-Sw interfaces F0/11 and F0/12. Both ports are only allowed 3 MAC addresses and are set to restrict violation mode.

25. Other Protocols



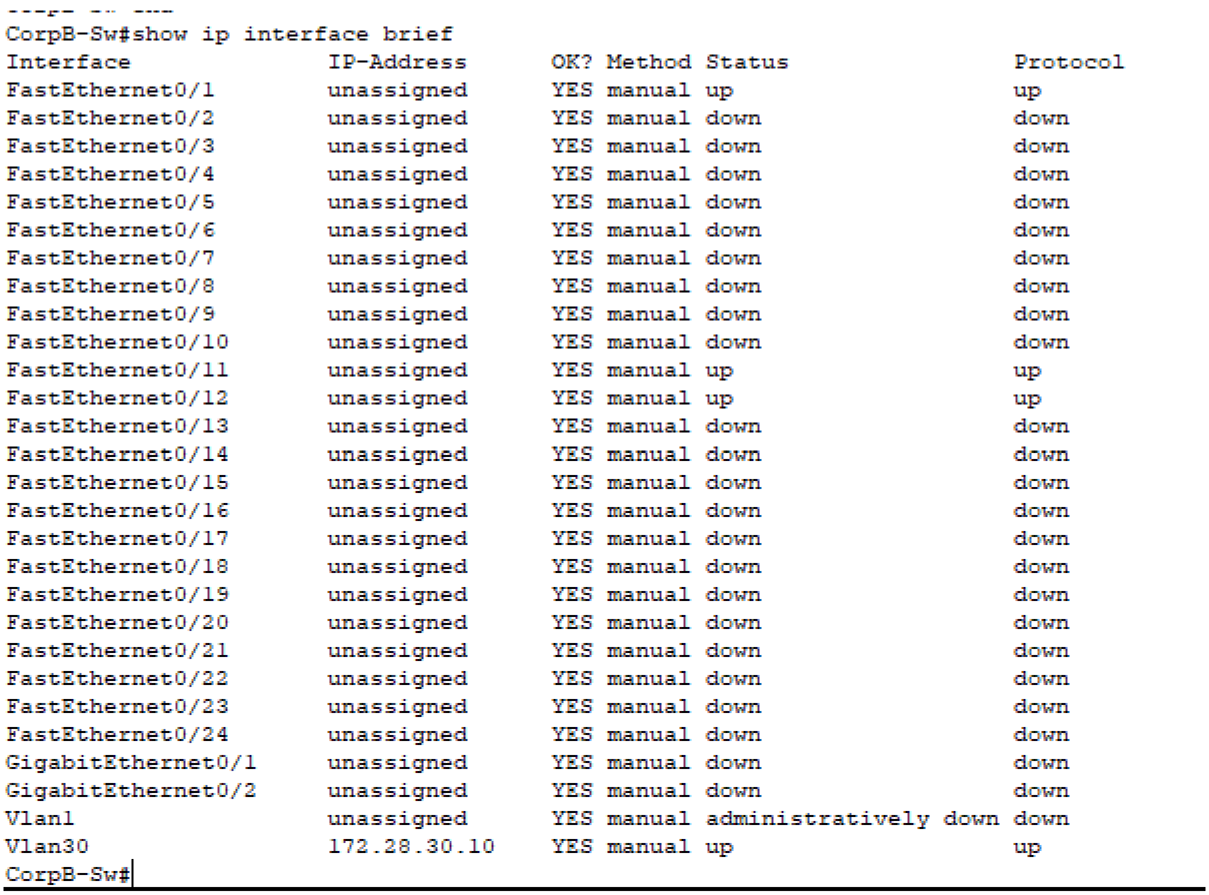
```
CorpA#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  up                    up
FastEthernet0/0.20     172.28.20.1     YES manual up                    up
FastEthernet0/0.21     172.28.21.1     YES manual up                    up
FastEthernet0/0.22     172.28.22.1     YES manual up                    up
FastEthernet0/0.23     172.28.23.1     YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/0/0            180.1.2.130     YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
CorpA#show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
FastEthernet0/0.20 is up, line protocol is up
  Internet address is 172.28.20.1/24
FastEthernet0/0.21 is up, line protocol is up
  Internet address is 172.28.21.1/24
FastEthernet0/0.22 is up, line protocol is up
  Internet address is 172.28.22.1/24
FastEthernet0/0.23 is up, line protocol is up
  Internet address is 172.28.23.1/24
FastEthernet0/1 is administratively down, line protocol is down
Serial0/0/0 is up, line protocol is up
  Internet address is 180.1.2.130/28
Serial0/0/1 is administratively down, line protocol is down
Vlan1 is administratively down, line protocol is down
CorpA#
```

This screenshot shows output from show ip interface brief and show protocols on CorpA. It confirms that only required interfaces are up, all unused interfaces are down and only necessary services are enabled.



```
CorpC-Sw#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual up                    up
FastEthernet0/12       unassigned      YES manual up                    up
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
```

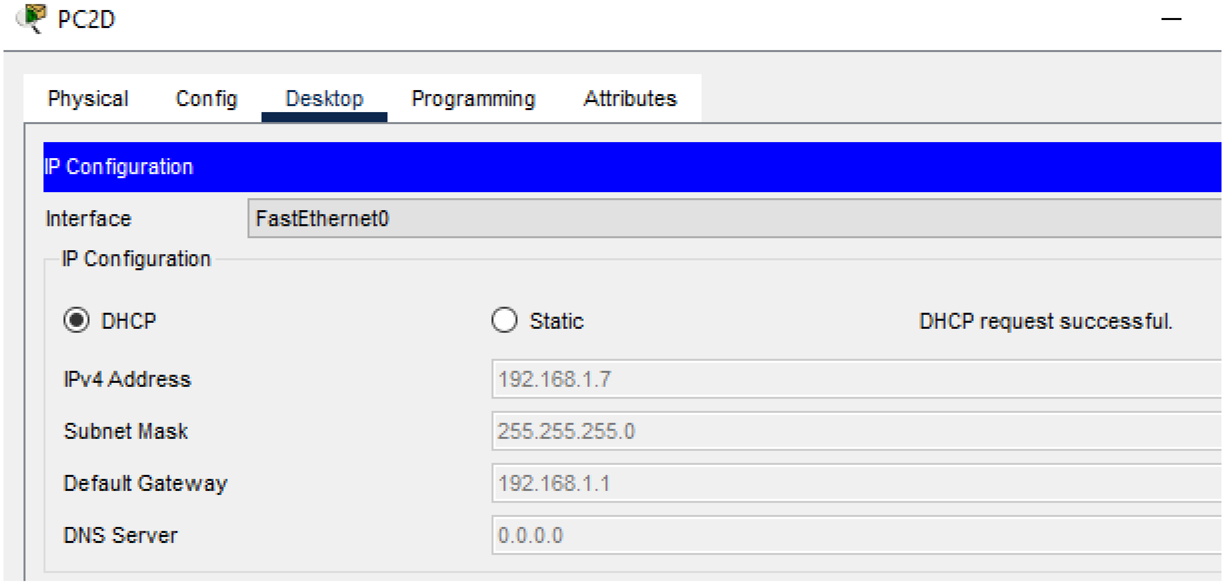
This screenshot shows show ip interface brief on CorpC-Sw confirming all unused ports are disabled.



```
CorpB-Sw#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual up                    up
FastEthernet0/12       unassigned      YES manual up                    up
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  unassigned      YES manual administratively down down
Vlan30                 172.28.30.10    YES manual up                    up
CorpB-Sw#
```

This screenshot shows show ip interface brief on CorpB-Sw confirming all unused ports are disabled.

26. ASA



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

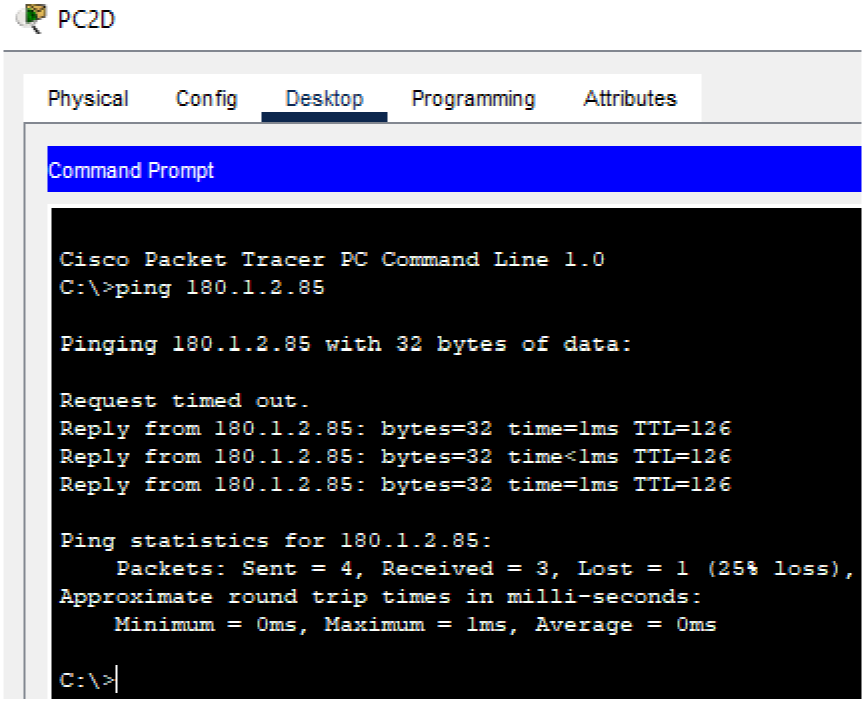
IPv4 Address: 192.168.1.7

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

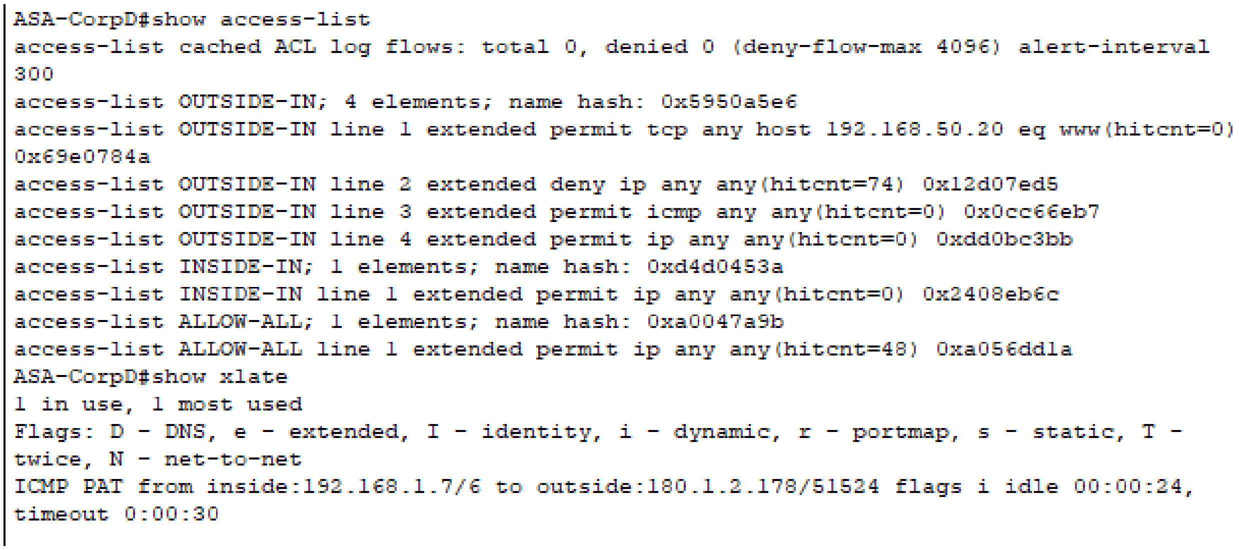
DNS Server: 0.0.0.0

This screenshot shows that PC2D can successfully obtain a DHCP address from the ASA.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 180.1.2.85

Pinging 180.1.2.85 with 32 bytes of data:

Request timed out.
Reply from 180.1.2.85: bytes=32 time=1ms TTL=126
Reply from 180.1.2.85: bytes=32 time<1ms TTL=126
Reply from 180.1.2.85: bytes=32 time=1ms TTL=126

Ping statistics for 180.1.2.85:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

This screenshot shows that PC2D can successfully ping to an internet address.



```
ASA-CorpD#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list OUTSIDE-IN; 4 elements; name hash: 0x5950a5e6
access-list OUTSIDE-IN line 1 extended permit tcp any host 192.168.50.20 eq www(hitcnt=0)
0x69e0784a
access-list OUTSIDE-IN line 2 extended deny ip any any(hitcnt=74) 0x12d07ed5
access-list OUTSIDE-IN line 3 extended permit icmp any any(hitcnt=0) 0x0cc66eb7
access-list OUTSIDE-IN line 4 extended permit ip any any(hitcnt=0) 0xdd0bc3bb
access-list INSIDE-IN; 1 elements; name hash: 0xd4d0453a
access-list INSIDE-IN line 1 extended permit ip any any(hitcnt=0) 0x2408eb6c
access-list ALLOW-ALL; 1 elements; name hash: 0xa0047a9b
access-list ALLOW-ALL line 1 extended permit ip any any(hitcnt=48) 0xa056dd1a
ASA-CorpD#show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s - static, T -
twice, N - net-to-net
ICMP PAT from inside:192.168.1.7/6 to outside:180.1.2.178/51524 flags i idle 00:00:24,
timeout 0:00:30
```

This screenshot shows that the ASA's access control list and NAT is configured. The show xlate command proves that dynamic PAT functions correctly and is translating addresses properly. The access control list is allowing traffic but definitely could be restricted more to lock down that network better.