Michael D’Elia

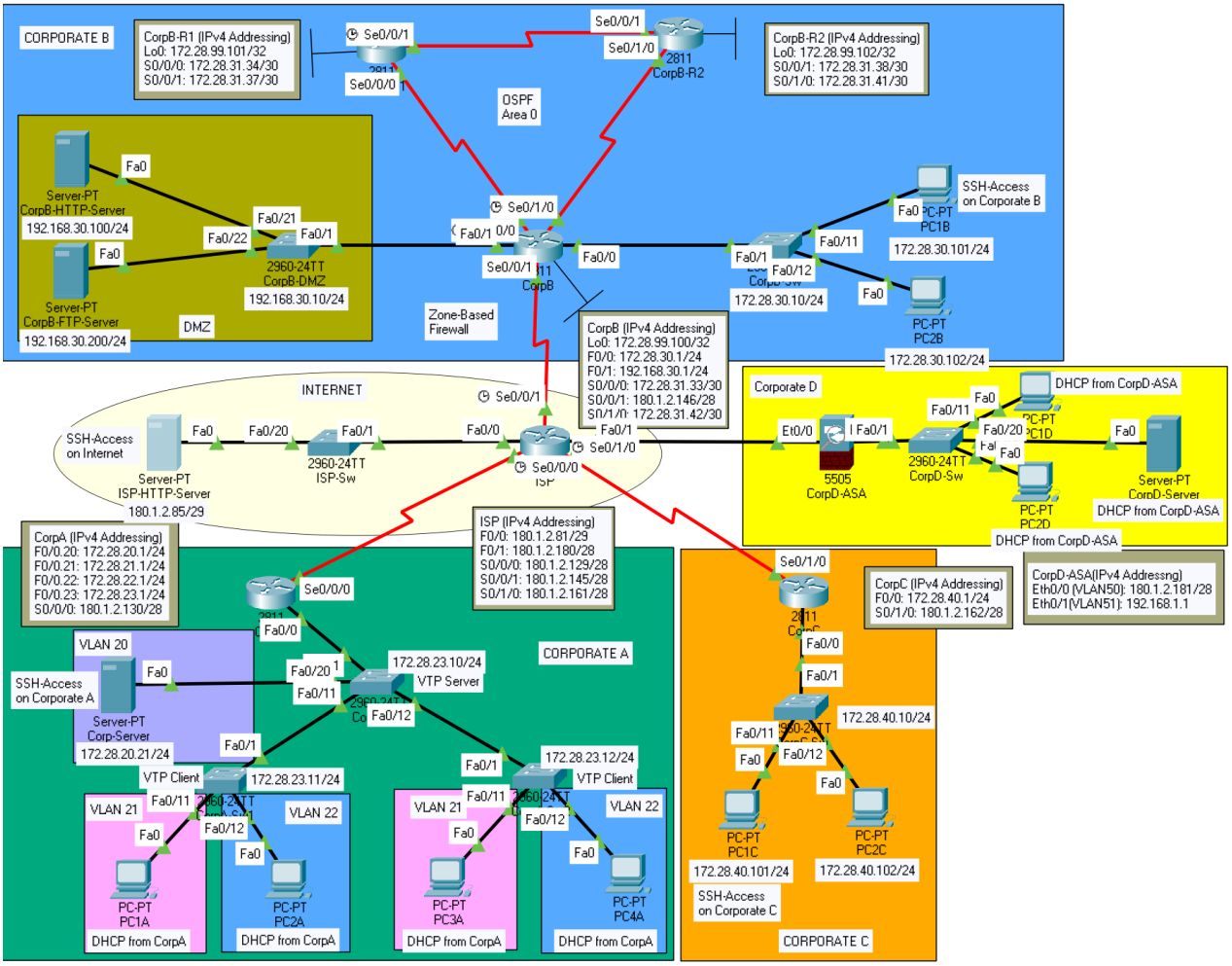
Professor Cannistra

CMPT 420N 620

27 May 2021

Challenge Lab

Topology



1. Hosts (PCs and Servers)

In a network, all hosts must be configured with an IP address, Subnet Mask, and Default Gateway in order for them to be network connectivity. This connectivity allows for layer 2 communication between hosts. Connectivity among devices can be tested through the use of pings, the ICMP protocol. IP addresses can be assigned to a host statically or dynamically. Subnet Masks define how an IP address can be divided and determine how many usable addresses there are in a network. The default gateway is the gateway that is used by the router to route traffic.

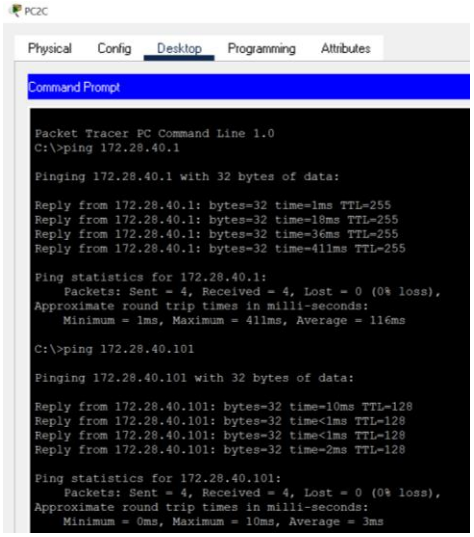


Figure 1: This screenshot displays that PC2C can successfully ping PC1C and CorpC Router. It shows that there is connectivity among the Corporate C network.

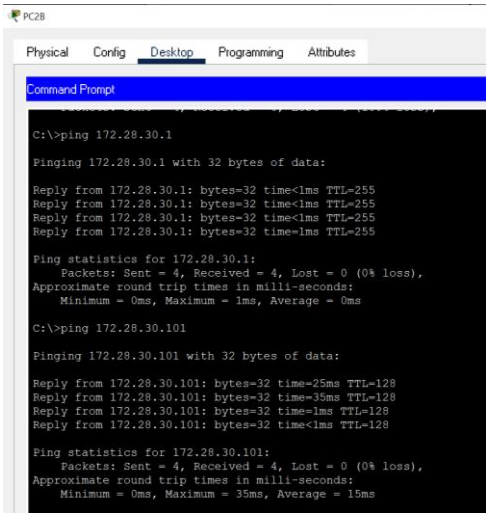


Figure 2: This screenshot displays that PC2B can successfully ping PC1B and CorpB Router. It shows that there is connectivity among the Corporate B network.

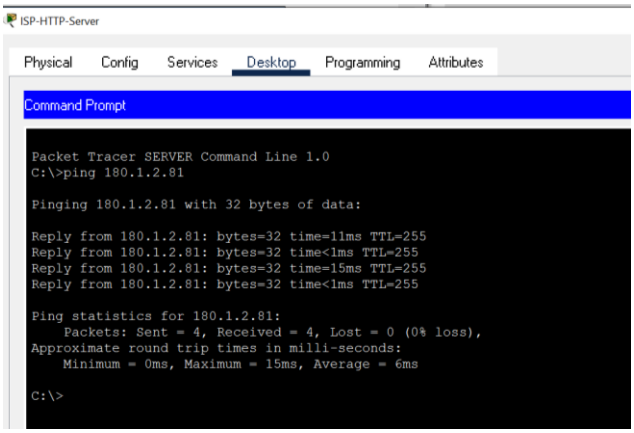


Figure 3: This screenshot displays that the ISP-HTTP-Server can successfully ping the ISP Router. This shows that there is connectivity among the Internet Network.

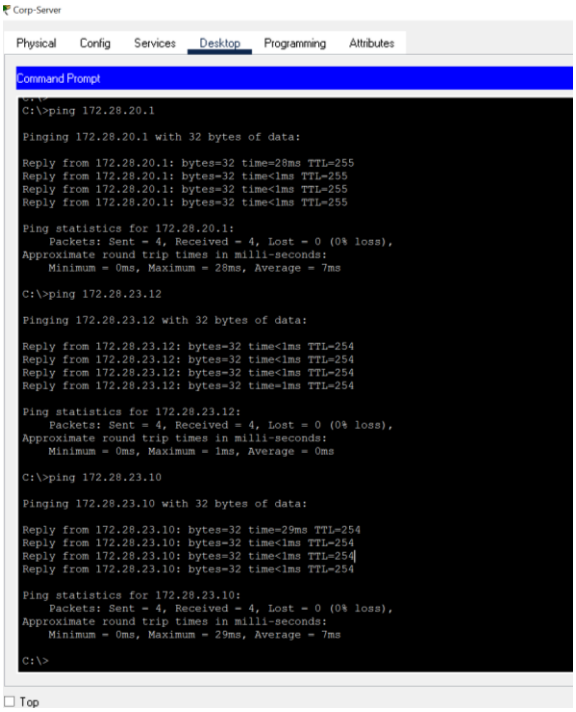


Figure 4: This screenshot displays that the Corp-Server can successfully ping the default gateway on CorpA router. It also can ping CorpA-Sw and CorpA-Sw2. This demonstrates that there is connectivity among the Corporate A network.

2. VLANs

A VLAN is a virtual local area network. VLANs are used for security on a network and to improve network performance. VLANs are very useful to network administrators for limiting access. VLAN's work over access or trunk lines. A native VLAN is used for untagged traffic and management purposed. By default all interfaces are assigned to the default VLAN of 1 to act as the broadcast VLAN. It is not secure to leave unused interfaces assigned to this default VLAN of 1. In the Challenge lab, VLANs 20, 21, 22, and 23 are configured. VLAN 20 is named CorpServer, VLAN 21 is named CorpPC1&3, VLAN 22 is named CorpPC2&4, and VLAN 23 is named NetMgmt and is configured as the native VLAN/administrative VLAN. VLAN 222 is configured to be the NEW-DEFAULT vlan which has all unused interfaces assigned to it.

Commands Used:

Vlan #	Creates a VLAN
Name [name]	Used to assign a name to a VLAN
Switchport mode access	Used to enable a port to be an access port
Switchport access vlan [number]	Assigns a VLAN to an access port
Switchport trunk native vlan [number]	Assigns a VLAN to be the native VLAN
Interface VLAN [number]	Enables a layer 3 VLAN interface

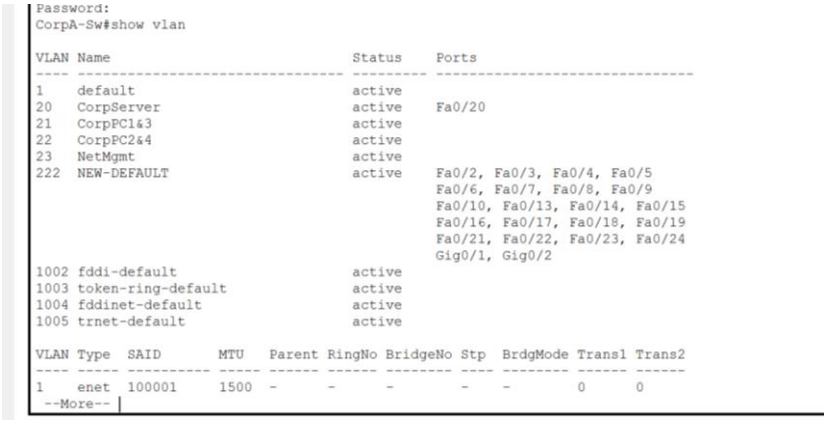


Figure 5: This screenshot displays the *show vlan* command on CorpA-Sw. It displays that VLAN 20, 21, 22, & 23 have been created and named. It also displays that VLAN 1 is not being used and VLAN 222 has been configured as the new default VLAN with all unused ports assigned to it.

```
CorpC-Sw#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
23   NetMgmt                          active    Fa0/1, Fa0/11, Fa0/12
222  NEW-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
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figure 6: This screenshot displays the *show vlan* command on CorpC Switch. It displays that VLAN 23 has been created and named NetMgmt for administrative access. It also shows that VLAN 1 is not being used on the Corporate C network and VLAN 222 has been created as the new default and all unused interfaces have been assigned.

```
CorpA-Sw2#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
20   CorpServer                       active
21   CorpPC1&3                        active    Fa0/11
22   CorpPC2&4                        active    Fa0/12
23   NetMgmt                          active
222  NEW-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
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
```

Figure 7: This screenshot displays the *show vlan* command on CorpA-Sw2. It displays that VLAN 20, 21, 22, & 23 have been created and named. It also displays that VLAN 1 is not being used and VLAN 222 has been configured as the new default VLAN with all unused ports assigned to it.

```
CorpB-Sw#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
23   NetMgmt                          active    Fa0/1, Fa0/11, Fa0/12
222  NEW-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
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figure 8: This screenshot displays the *show vlan* command on CorpB-Sw. It displays that VLAN 23 has been created and named. It also displays that VLAN 1 is not being used and VLAN 222 has been configured as the new default VLAN with all unused ports assigned to it.

3. STP

STP is short for Spanning Tree Protocol. STP is used to prevent loops in a network. When STP is configured on a network, one device is elected or set to be the root bridge. The root bridge becomes the reference point for all other switches in a network for defining the shortest path. The bridge with the lowest priority value/bridge ID is set as the root bridge. In the challenge lab, CorpA-Sw on the Corporate A network is set as the root bridge.

Commands Used

Spanning-tree vlan 20-23 priority 24576	This is the command that was issued on CorpA-Sw to set it to be the root bridge.

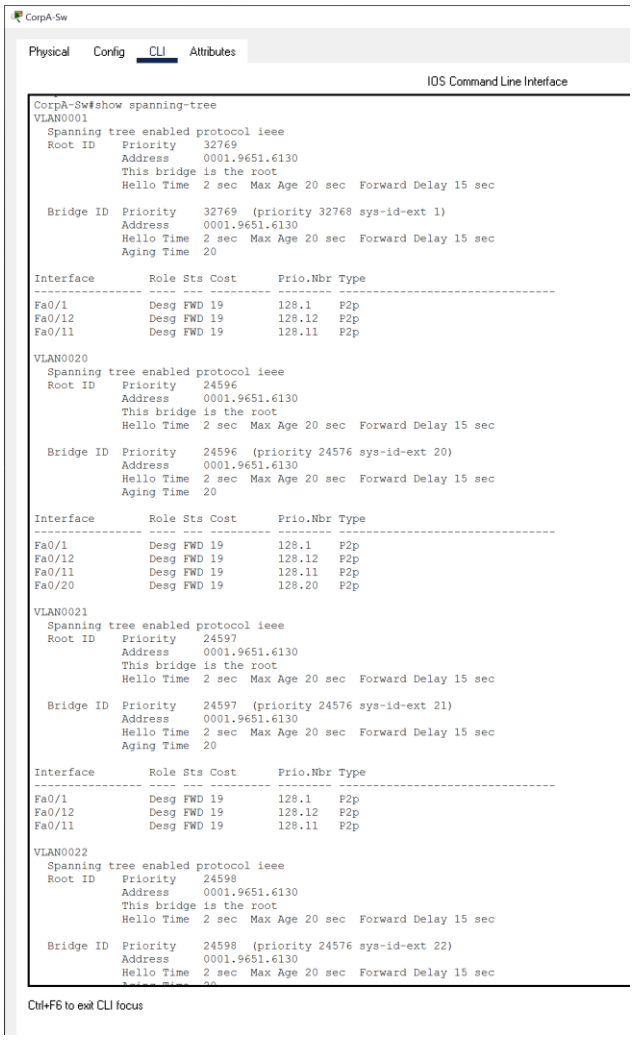


Figure 9: This screenshot displays the *show spanning-tree* command on CorpA-Sw. It displays that this switch is the root bridge. VLANs 20-23 hves been configured on CorpA-Sw as root bridges. The have been set with the priority value of 24597.

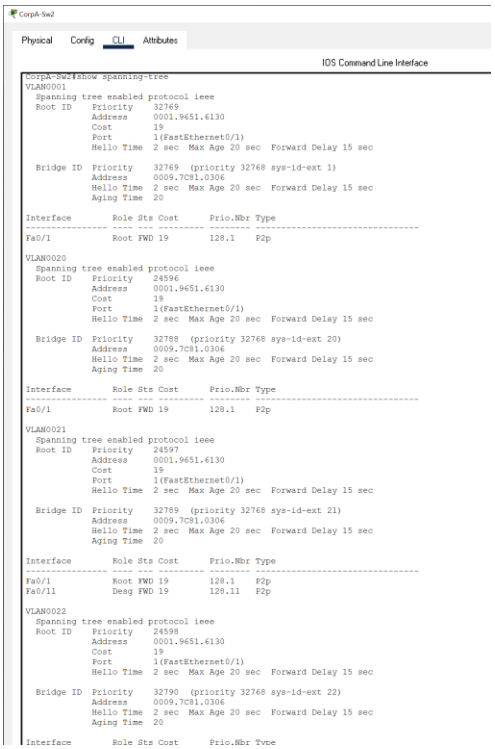


Figure 10: This screenshot displays the *show spanning-tree* command on CorpA-Sw2. It displays that STP is enabled, and that this device is not the root bridge.

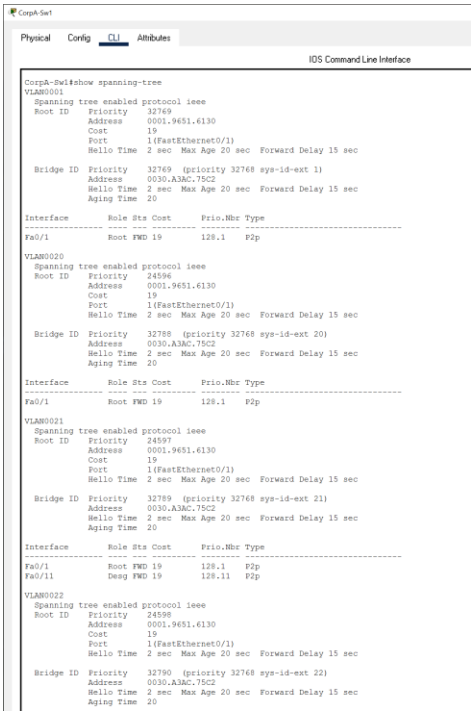


Figure 11: This screenshot displays the *show spanning-tree* command on CorpA-Sw1. It displays that STP is enabled, and that this device is not the root bridge.

4. IEEE 802.1Q Trunking

IEEE 802.1Q trunking is used by virtual LAN's (VLAN's) to allow for network interfaces to be shared. It is referred to as DOT1Q when configuring on devices. IEEE is the Institute of Electrical and Electronic Engineers that developed the standard. When configuring trunking lines, the lines can be restricted to specific VLAN's. In the challenge lab, trunking encapsulation is configured on trunk lines. Only the VLANs that are in use in the topology are allowed to traverse the trunk interfaces. Additional Layer2 security is applied to protect root ports.

Commands Used

Switchport mode trunk	Configures a port to be a trunk port
Encapsulation dot1q [number]	Enables 802.1Q Trunking on the CorpA Router
Spanning-tree portfast default	Configures PortFast globally on all non-trunking ports
Switchport nonegotiate	Disables DTP to prevent auto trunking
Switchport trunk native vlan [number]	Assigns a VLAN to be the native vlan
Switchport trunk allowed vlan [number]	Assigns allowed VLANs on a trunk
Spanning-tree bpduguard enable	Enables BPDU guard on a portfast interface

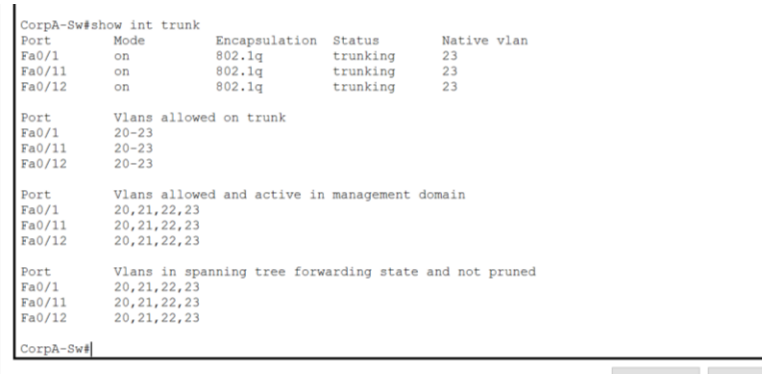


Figure 12: This screenshot displays the *show int trunk* command on CorpA-Sw of the Corporate A network. It displays that encapsulation dot1q is configured. It also shows the trunking ports that are configured. It also displays that VLAN 23 has been set as the native VLAN. Furthermore, this shows that VLANs that are allowed to traverse over trunking interfaces.

```
CorpA-Sw#
CorpA-Sw#show spanning-tree summary
Switch is in pvst mode
Root bridge for: default CorpServer CorpPC1&3 CorpPC2&4 NetMgmt NEW-DEFAULT
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                      0         0        0          3          3
VLAN0020                      0         0        0          4          4
VLAN0021                      0         0        0          3          3
VLAN0022                      0         0        0          3          3
VLAN0023                      0         0        0          3          3
VLAN0222                      0         0        0          3          3

---------------------- -------- --------- -------- ---------- ----------
6 vlans                       0         0        0         19         19

CorpA-Sw#
```

Figure 13: This screenshot displays the *show spanning-tree summary* command on CorpA-Sw on the Corporate A network. It displays that Layer2 Security has been added to protect the root ports. It displays that Portfast has been enabled to get a trunk port to enter forwarding state immediately. BPDU Guard has also been enabled which protects a switch from BPDU attacks.

```
CorpA-Sw1#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      23

Port        Vlans allowed on trunk
Fa0/1       20-23

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

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

CorpA-Sw1#
```

Figure 14: This screenshot displays the *show int trunk* command on CorpA-Sw1 on the Corporate Network. It displays that F0/1 has been configured has a trunk line with encapsulation configured and VLAN 23 set as the Native VLAN. It also displays all the VLANs that are allowed over the trunk line.

```
CorpA-Sw2#
CorpA-Sw2#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      23

Port        Vlans allowed on trunk
Fa0/1       20-23

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

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

Figure 15: This screenshot displays the *show int trunk* command on CorpA-Sw2 on the Corporate Network. It displays that F0/1 has been configured has a trunk line with encapsulation configured and VLAN 23 set as the Native VLAN. It also displays all the VLANs that are allowed over the trunk line.

5. Default Static Routing

A static route is a manually configured route in a routing table. Many routes are learned dynamically by a router. A default static route defines traffic that is to be routed to a certain address. Static routes are for paths between two routers. In the challenge lab, default static routes are set on all network edge routers pointing to the ISP router.

Commands Used

Ip route 0.0.0.0 0.0.0.0 [destination IP address]	This command sets a static route in a routing tell and tells the router to forward all traffic to the defined IP address

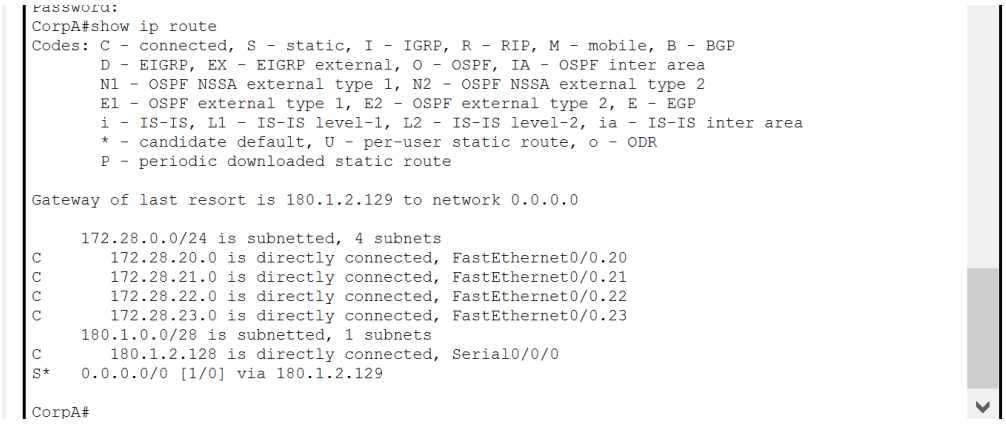


Figure 16: This screenshot displays the routing table of the CorpA router on the Corporate A network using the *show ip route* command. The last entry displays that a static route has been entered to forward all traffic to the IP address 180.1.2.129.

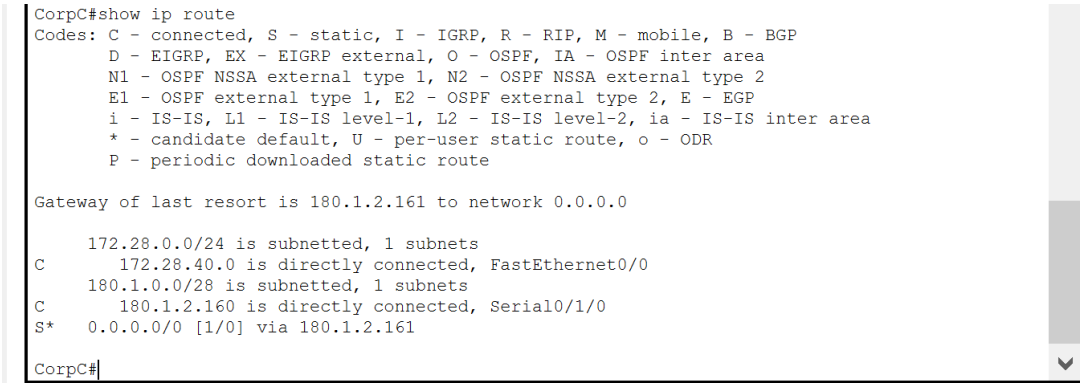
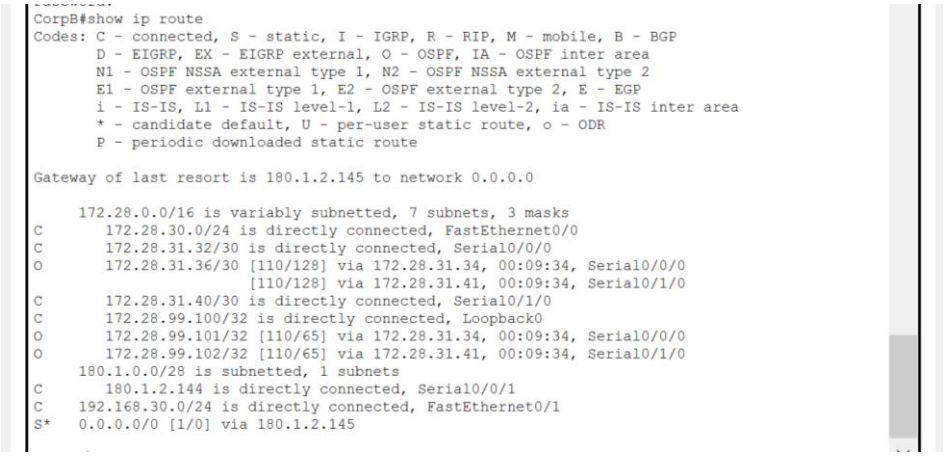


Figure 17: This screenshot displays the routing table of the CorpC router on the Corporate C network using the *show ip route* command. The last entry displays that a static route has been entered to forward all traffic to the IP address 180.1.2.161.



```
CorpB#show ip route
Codes: C - connected, S - static, I - IGRP, 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, 7 subnets, 3 masks
C       172.28.30.0/24 is directly connected, FastEthernet0/0
C       172.28.31.32/30 is directly connected, Serial0/0/0
O       172.28.31.36/30 [110/128] via 172.28.31.34, 00:09:34, Serial0/0/0
                        [110/128] via 172.28.31.41, 00:09:34, Serial0/1/0
C       172.28.31.40/30 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, 00:09:34, Serial0/0/0
O       172.28.99.102/32 [110/65] via 172.28.31.41, 00:09:34, Serial0/1/0
     180.1.0.0/28 is subnetted, 1 subnets
C       180.1.2.144 is directly connected, Serial0/0/1
C    192.168.30.0/24 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 180.1.2.145
```

Figure 18: This screenshot displays the routing table of the CorpB router on the Corporate B network using the *show ip route* command. The last entry displays that a static route has been entered to forward all traffic to the IP address 180.1.2.145.

6. Dynamic Routing

Dynamic routing allows a network routing to update and change routes in a network. The Open Shortest Path First (OSPF) protocol is routing protocol that is used to distribute IP routing information throughout a defined area on a network. OSPF passes information along to its neighbors. OSPF authentication can be enabled on interfaces to prevent rogue devices from participating in routing updates and advertisements. In the challenge lab, OSPF Area 0 is created among the routers in the Corporate B Network. The interface that connects to the outside ISP Router should not have OSPF enabled. The ISP router also should not have any routing protocols configured. Lastly, routing protocol authentication is configured to prevent rogue routers from participating in updates and advertisements.

Commands Used

Router ospf 1	Enables OSPF on a device
Network [address] [mask] area [number]	Adds a network and the number of usable addresses to an OSPF area
Router-id [ip address]	Provides a unique identity for an OSPF device
IP ospf message-digest-key [number] md5 [password]	Enables md5 encryption on an OSPF configuration password
IP ospf authentication message-digest	Enables OSPF Authentication

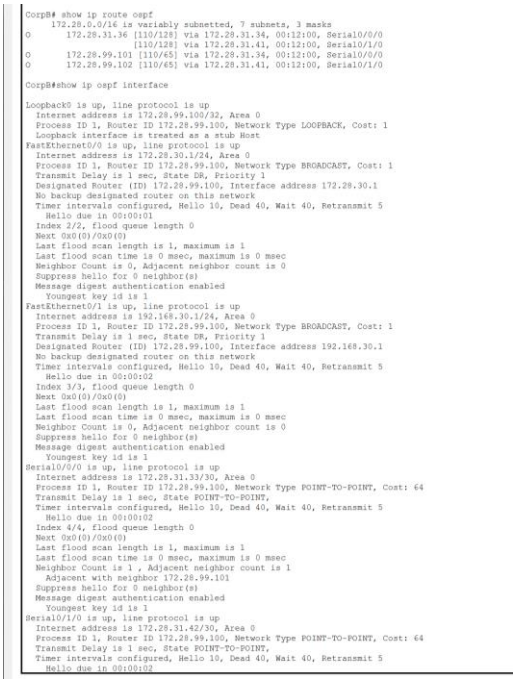
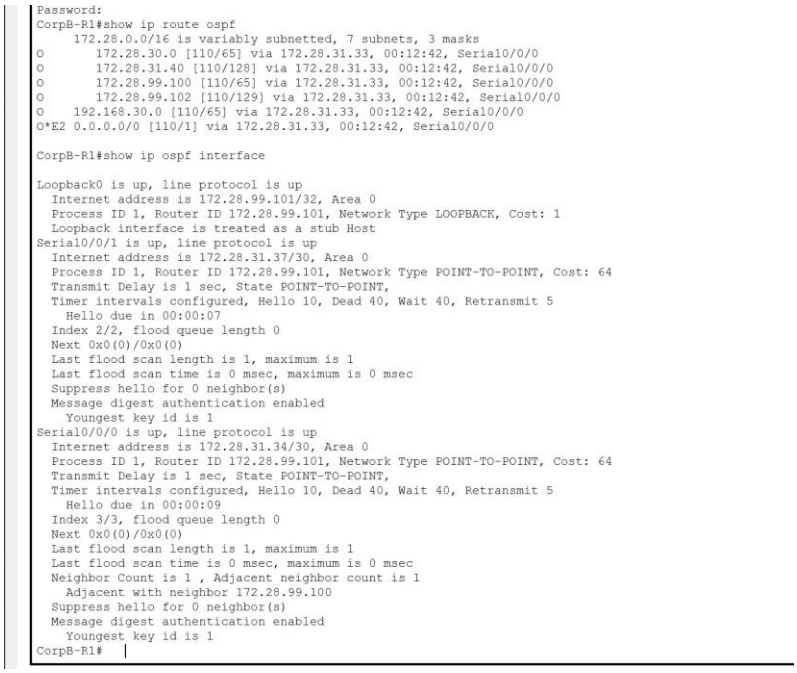


Figure 19: This screenshot displays the *show ip route ospf* command and *show ip ospf interface* command on CorpB of the Corporate B Network. The show ip route ospf command displays all the networks configured to use OSPF. The show ip ospf interface command displays all the interfaces that have OSPF configured. It also shows that MD5 authentication has been enabled on the interfaces. The interface S0/0/1 does not have OSPF configured since it connects the ISP router.

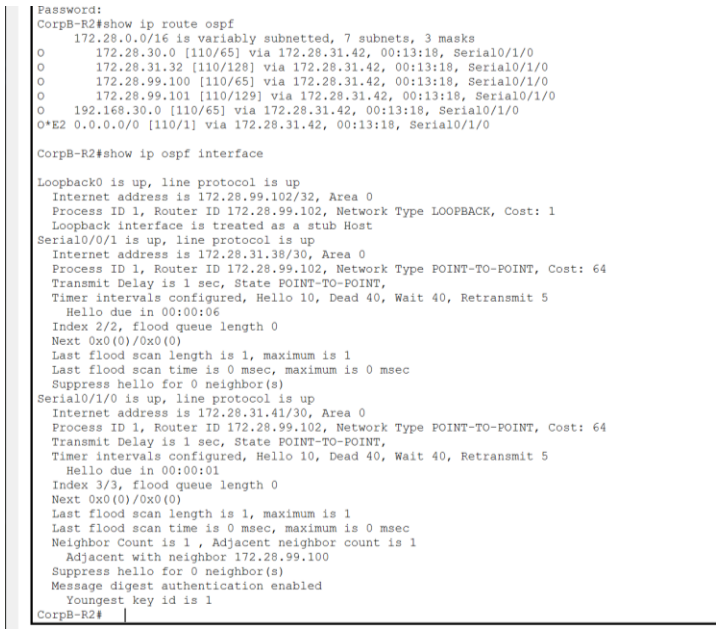


```
Password:
CorpB-R1#show ip route ospf
     172.28.0.0/16 is variably subnetted, 7 subnets, 3 masks
O       172.28.30.0 [110/65] via 172.28.31.33, 00:12:42, Serial0/0/0
O       172.28.31.40 [110/128] via 172.28.31.33, 00:12:42, Serial0/0/0
O       172.28.99.100 [110/65] via 172.28.31.33, 00:12:42, Serial0/0/0
O       172.28.99.102 [110/129] via 172.28.31.33, 00:12:42, Serial0/0/0
O    192.168.30.0 [110/65] via 172.28.31.33, 00:12:42, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.28.31.33, 00:12:42, Serial0/0/0

CorpB-R1#show ip ospf interface

Loopback0 is up, line protocol is up
  Internet address is 172.28.99.101/32, Area 0
  Process ID 1, Router ID 172.28.99.101, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Serial0/0/1 is up, line protocol is up
  Internet address is 172.28.31.37/30, Area 0
  Process ID 1, Router ID 172.28.99.101, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  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
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
Serial0/0/0 is up, line protocol is up
  Internet address is 172.28.31.34/30, Area 0
  Process ID 1, Router ID 172.28.99.101, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  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
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 172.28.99.100
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
CorpB-R1#
```

Figure 20: This screenshot displays the *show ip route ospf* command and *show ip ospf interface* command on CorpB-R1 of the Corporate B Network. The show ip route ospf command displays all the networks configured to use OSPF. The show ip ospf interface command displays all the interfaces that have OSPF configured. It also displays that MD5 authentication has been enabled on the interfaces.



```
Password:
CorpB-R2#show ip route ospf
     172.28.0.0/16 is variably subnetted, 7 subnets, 3 masks
O       172.28.30.0 [110/65] via 172.28.31.42, 00:13:18, Serial0/1/0
O       172.28.31.32 [110/128] via 172.28.31.42, 00:13:18, Serial0/1/0
O       172.28.99.100 [110/65] via 172.28.31.42, 00:13:18, Serial0/1/0
O       172.28.99.101 [110/129] via 172.28.31.42, 00:13:18, Serial0/1/0
O    192.168.30.0 [110/65] via 172.28.31.42, 00:13:18, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.28.31.42, 00:13:18, Serial0/1/0

CorpB-R2#show ip ospf interface

Loopback0 is up, line protocol is up
  Internet address is 172.28.99.102/32, Area 0
  Process ID 1, Router ID 172.28.99.102, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Serial0/0/1 is up, line protocol is up
  Internet address is 172.28.31.38/30, Area 0
  Process ID 1, Router ID 172.28.99.102, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
Serial0/1/0 is up, line protocol is up
  Internet address is 172.28.31.41/30, Area 0
  Process ID 1, Router ID 172.28.99.102, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  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
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 172.28.99.100
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
CorpB-R2#
```

Figure 21: This screenshot displays the *show ip route ospf* command and *show ip ospf interface* command on CorpB-R2 of the Corporate B Network. The show ip route ospf command displays all the networks configured to use OSPF. The show ip ospf interface command displays all the interfaces that have OSPF configured. It also displays that MD5 authentication has been enabled on the interfaces.

7. Default Route Injection

When a route to a specific network in a routing table does not exist, route injection can be used to learn the default static route automatically. Route injection is used by the OSPF routing protocol. Routes will not be advertised to any routers without a default route entered in the table.

Commands Used

Default-information originate	Generates a default route

```
CorpB#show ip ospf database
            OSPF Router with ID (172.28.99.100) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.28.99.101   172.28.99.101   970         0x80000015 0x0023ce 4
172.28.99.100   172.28.99.100   969         0x80000018 0x005c0e 7
172.28.99.102   172.28.99.102   969         0x80000015 0x009946 4

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         172.28.99.100   1265        0x80000006 0x000e2f 1
CorpB#
```

Figure 22: This screenshot displays the *show ip ospf database* command on CorpB on the Corporate B network. The Type-5 AS External Link status indicates the default-information originate command is active.

```
CorpB-R1#show ip ospf database
            OSPF Router with ID (172.28.99.101) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.28.99.101   172.28.99.101   974         0x80000015 0x0023ce 4
172.28.99.102   172.28.99.102   973         0x80000015 0x009946 4
172.28.99.100   172.28.99.100   974         0x80000018 0x005c0e 7

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         172.28.99.100   1269        0x80000006 0x000e2f 1
CorpB-R1#
```

Figure 23: This screenshot displays the *show ip ospf database* command on CorpB-R1 on the Corporate B network. The Type-5 AS External Link status indicates the default-information originate command is active.

```
CorpB-R2#show ip ospf database
            OSPF Router with ID (172.28.99.102) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.28.99.101   172.28.99.101   2778        0x80000010 0x002dc9 4
172.28.99.102   172.28.99.102   1043        0x80000015 0x009946 4
172.28.99.100   172.28.99.100   1043        0x80000018 0x005c0e 7

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         172.28.99.100   1334        0x80000006 0x000e2f 1
CorpB-R2#
```

Figure 24: This screenshot displays the *show ip ospf database* command on CorpB-R2 on the Corporate B network. The Type-5 AS External Link status indicates the default-information originate command is active.

8. DMZ Access Control Lists

A demilitarized zone (DMZ) is a firewall technology used to protect an internal network. A DMZ allows for outside traffic to enter the DMZ but not the main network. In the challenge lab, the DMZ is on the Corporate B network. The DMZ is used to allow the Internet to reach internal HTTP and FTP servers on the DMZ. DMZ traffic into the Corporate B network is then denied preventing unauthorized access into the Corporate B LAN. Traffic within the Corporate B LAN can be established and inspected to enter the DMZ.

Commands Used

Ip access-list extended [name]	Creates a named Extended ACL
Permit|deny [protocol] [source ip] [source mask] [destination ip] [destination mask]	Used to create an ACE for an ACL
Ip access-group [name] in | out	Applies and ACL inbound or outbound on an interface

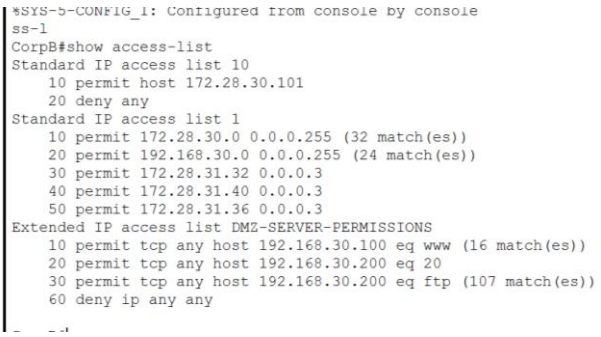


Figure 25: This screenshot displays the *show access-list* command on the CorpB router on the Corporate B network. It displays that the access-list for the DMZ has been created and called DMZ-SERVER-PERMISSIONS. This access list does not allow the servers in the DMZ to initiate traffic to the LAN. Permitted traffic to the DMZ from the internet and Corp B LAN are allowed into the DMZ. The only traffic that is permitted into the DMZ is HTTP and FTP traffic.

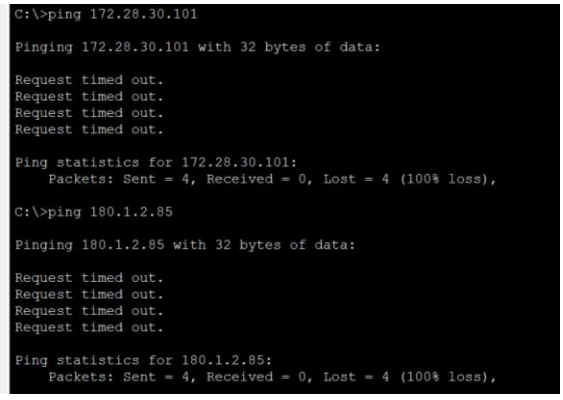


Figure 26: This screenshot displays the CorpB-HTTP-Server on the DMZ on Corporate B is unable to initiate traffic to the LAN. This also applies for the CorpB-FTP-Server on the DMZ.

```
CorpB#show ip int f0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is DMZ-SERVER-PERMISSIONS
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled

CorpB#
```

Figure 27: This screenshot displays the *show ip int f0/1* command on the CorpB router on the Corporate B network. It displays the DMZ ACL is applied to the outbound interface of F0/1 on the CorpB router.

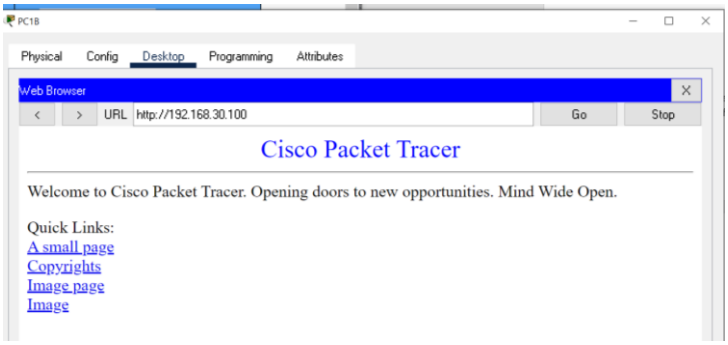


Figure 28: This screenshot displays the permitted traffic from the CorpB LAN is allowed to enter the DMZ. The permitted traffic from the LAN and the Internet is HTTP and FTP traffic. All other traffic into the DMZ is not permitted.

```
C:\>
C:\>ftp 180.1.2.158
Trying to connect...180.1.2.158
Connected to 180.1.2.158
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Figure 29: This screenshot displays the permitted traffic from the Internet is allowed to enter the DMZ. The permitted traffic from the LAN and the Internet is HTTP and FTP traffic. All other traffic into the DMZ is not permitted.

9. SSH

Secure Shell Protocol (SSH) is a secure form of data transfer between devices. SSH is commonly used for remote management of network devices from a host. It allows for authentication of the remote user and provides security to the data that is being transferred to and from the device. In the challenge lab, SSH is configured on the routers and switches. Within each network, SSH is restricted so that only one device can use SSH to access it. Telnet is an unsecure form or remote device access that is disabled from being used on all the devices. In Corporate A network, the Corp-Server is given SSH access to all the devices. In the Corporate B network, PC1B is given SSH access to all the devices on the Corporate B network. In Corporate C, PC1C is given SSH access to the devices on Corporate C, however it is restricted to only allowing those two. On the Internet, ISP-HTTP-Server is given SSH access to the ISP devices.

Commands Used

Ip domain-name [name]	Used to set the device domain name
Crypto key generate rsa	Used to generate RSA key pairs
Ip ssh version	Used to enable SSH version 2 on a device
Transpot input ssh	Used to restrict access on VTY line to SSH
Access-list [number] permit host [ip address]	Used to created an ACL to allow a device SSH access
Access-class [number] in	Used to apply an ACL to the VTY lines

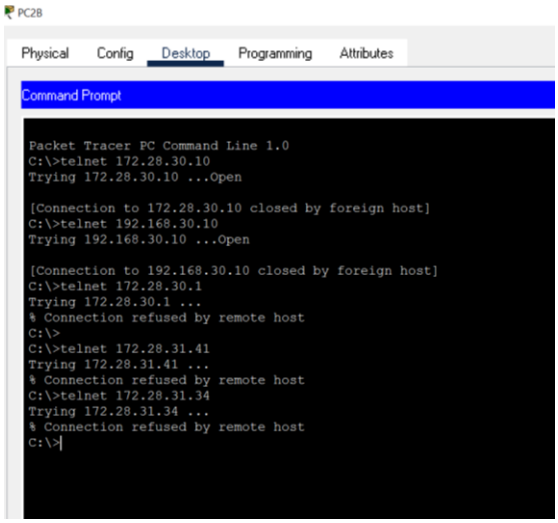


Figure 30: This screenshot displays the command prompt on PC2B on the Corporate B network which displays that telnet is not being allowed by any of the devices on the network. This demonstrates the use of the transport input ssh command on the VTY lines of network devices to restrict access to only SSH. This is true to the devices on the Internet, Corporate A, and Corporate C network also.

Figure 31: This screenshot displays the command prompt on PC2C on the Corporate C network which displays that SSH is not being allowed by any of the devices on the network. This demonstrates that SSH access on the network has been limited to only one PC on the network. This is true to the devices on the Internet, Corporate A, and Corporate C network also.

Figure 32: This screenshot displays the command prompt on PC1C on the Corporate C network which displays that SSH is working for all the devices on the network. This demonstrates that SSH access on the network has been limited to only one PC on the network. This is true to the devices on the Internet, Corporate A, and Corporate C network also.

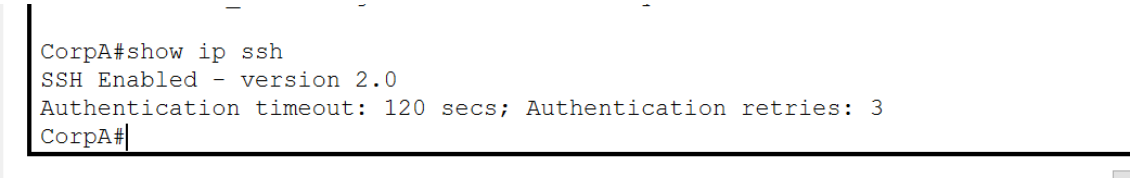


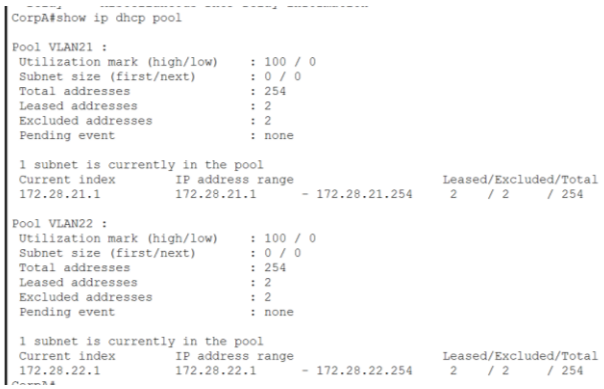
Figure 33: This screenshot displays the *show ip ssh* command on CorpA Router on the Corporate A network. This displays that SSH is enable and is using SSH version 2. This is true to all the devices on the Internet, Corporate B, and Corporate C networks also.

10. DHCP

Dynamic Host Configuration Protocol (DHCP) is used to automatically assign an IP address to a host. It assigns the host IP address and default gateway based on defined parameters of the DHCP server. A DHCP server can operate on an actual server or a router/ASA can also be configured as DHCP servers. In the challenge lab, a DHCP server is configured on CorpA. DHCP addresses are assigned to the PCs in VLAN 21 & 22 on the Corporate A network.

Commands Used

Ip dhcp excluded-address [start ip address] [end ip address range]	Specifies the range of usable addresses of a DHCP server for a specific network
Ip dhcp pool [name]	Assigns a name to a DHCP pool
Network [ip address] [subnet mask]	Defines the network to be used in a DHCP pool
Default-router [ip address]	Assigns the IP address of the default gateway of a DHCP pool
Domain-name [name]	Assigns the domain-name for a DHCP pool
Dns-server [ip address]	Assigns the IP address of the DNS Server for a DHCP pool



```
CorpA#show ip dhcp pool

Pool VLAN21 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 2
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                  Leased/Excluded/Total
 172.28.21.1          172.28.21.1      - 172.28.21.254     2    / 2     / 254

Pool VLAN22 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 2
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                  Leased/Excluded/Total
 172.28.22.1          172.28.22.1      - 172.28.22.254     2    / 2     / 254
```

Figure 34: This screenshot displays the *show ip dhcp pool* command on CorpA Router in the Corporate A network. The CorpA Router is configured as the DHCP Server. This shows the two DHCP pools that have been created and the names that have been assigned. It also displays the lease information of how many addresses have been assigned to hosts in each pool.

```
CorpA#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
172.28.21.11     0090.21C1.E791           --                     Automatic
172.28.21.12     0090.0C13.B305           --                     Automatic
172.28.22.11     0000.0C5B.02EE           --                     Automatic
172.28.22.12     00E0.B00E.D578           --                     Automatic
CorpA#
```

Figure 35: This screenshot displays the *show ip dhcp binding* command on CorpA Router. It displays the list of IP addresses that have been assigned to hosts and list the MAC address of the host that the address is assigned.

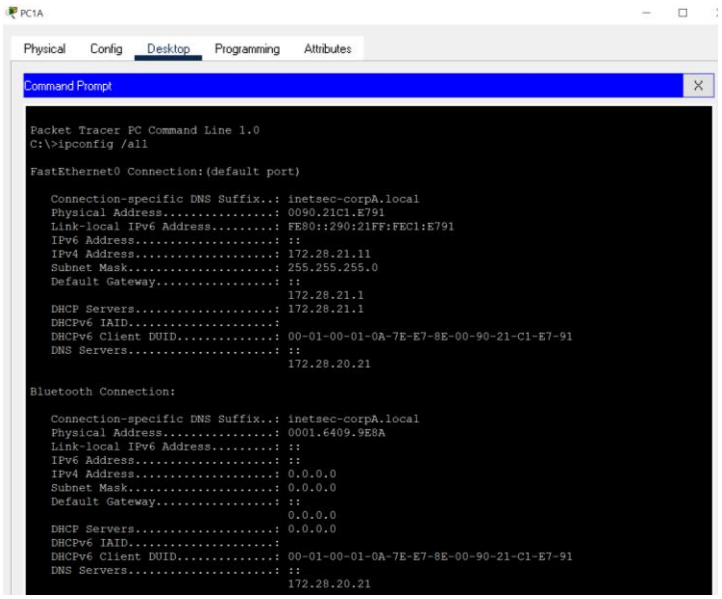


Figure 36: This screenshot displays the *ipconfig /all* command in the command prompt of PC1A in VLAN 21 of Corporate A network. This screenshot displays the DHCP assigned IP address, the address of the DHCP server, the address of the default-gateway, the address of the DNS server, and also the DNS Suffix. This displays that the DHCP server is assigned addresses to hosts within VLAN 21 using DHCP on Corporate A Network.

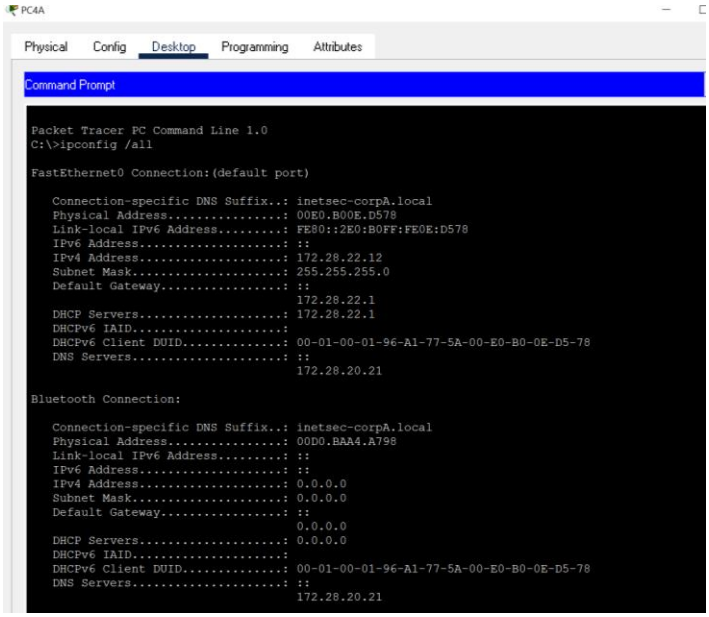


Figure 37: This screenshot displays the *ipconfig /all* command in the command prompt of PC4A in VLAN 22 of Corporate A network. This screenshot displays the DHCP assigned IP address, the address of the DHCP server, the address of the default-gateway, the address of the DNS server, and also the DNS Suffix. This displays that the DHCP server is assigned addresses to hosts within VLAN 22 using DHCP on Corporate A Network.

11. DNS

Domain Name System (DNS) is the naming service for IP addresses. DNS is referred to as the phonebook of the internet. DNS takes domain names and translates them into IP addresses. For example, with the use of DNS, a name can be typed when issuing a ping rather than an IP address. In the challenge lab, Corp-Server is configured to be a DNS server. The inetsec zone is used. An address record is configured for the devices in the topology and CNAMES have been created for devices in the Corporate A network.

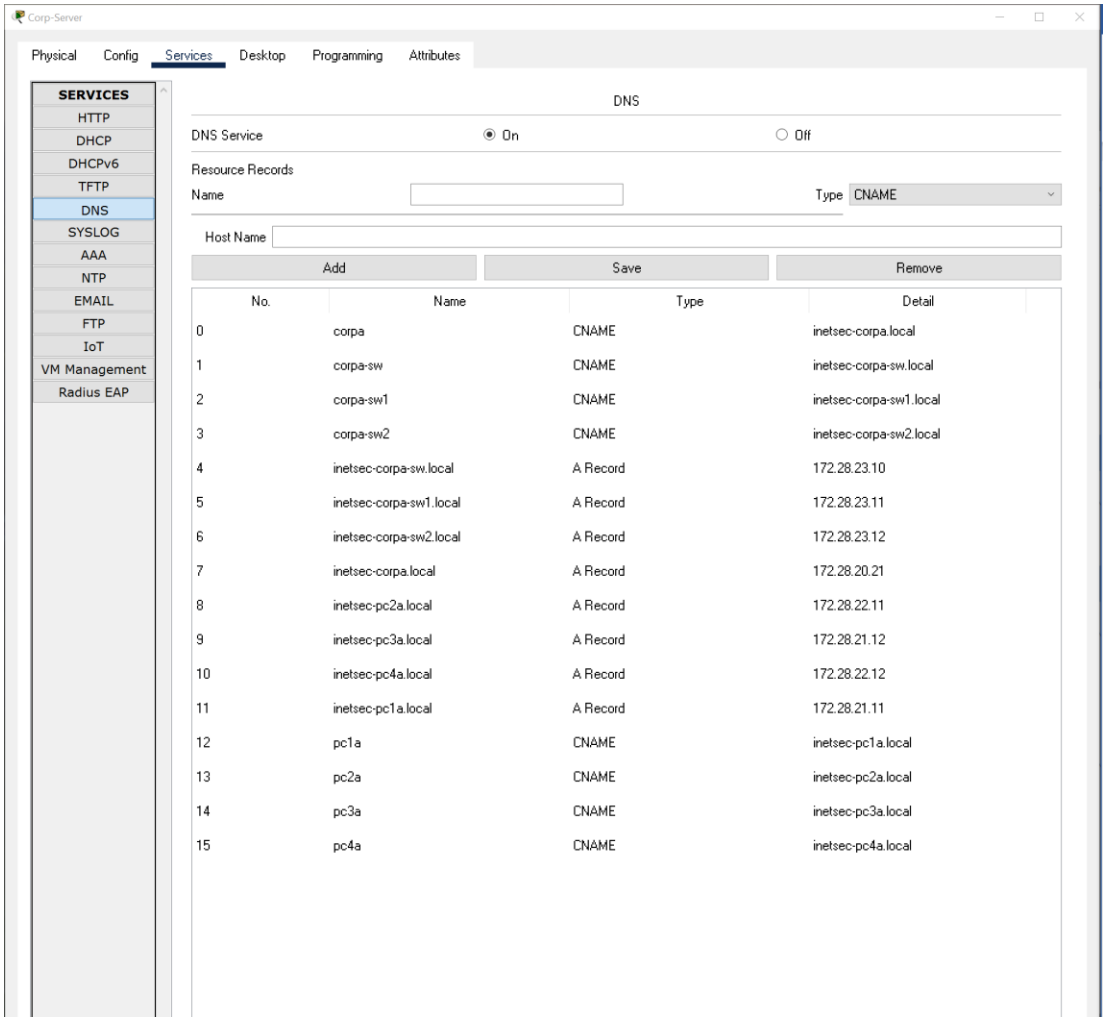


Figure 38: This screenshot displays the DNS tab on the services section of Corp-Server. DNS services have been enabled. All devices in the Corporate A network have an address record. Each device also has a CNAME record.

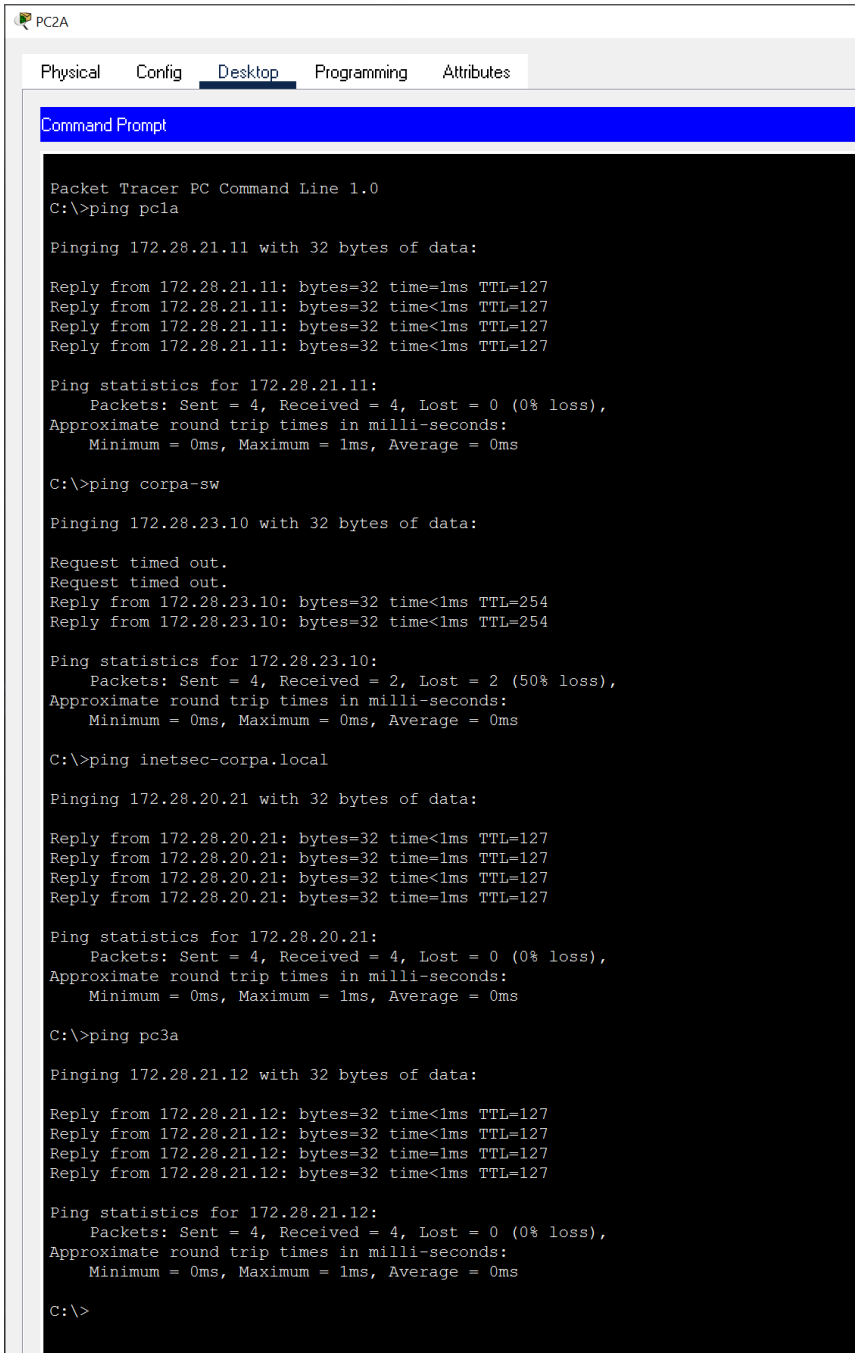


Figure 39: This screenshot displays the command prompt on PC2A in the Corporate A network. It displays that pings can successfully ping a device by using the configured DNS name. Pings are also successful by pinging the DNS Zone. The ping to PC1A is successful, the ping to CorpA-Sw is successful, the ping to the DNS server (inetsec-CorpA.local) is successful. The ping to PC3A is successful. This verifies that the DNS server is working properly.

12. PAT

Port Address Translation (PAT) works along with Network Address Translation (NAT). It allows for private IP addresses to be mapped to one or more public IP addresses. PAT allows for a private IP address to be translated to a public IP address by port numbers. NAT allows for private IP addresses to be translated to public IP addresses. These protocols often work hand-in-hand. PAT allows for a minimal number of IP addresses to be used. In the challenge lab, PAT is configured on the Corporate A, B, and C network. On the Corporate A router, the interface IP address is used. On the Corporate B router, a pool of ten addresses is used. On the Corporate C router, dynamic NAR with PAT is used using the interface IP address.

Commands Used

Ip nat inside source list [number] interface [interface]	Specifies the interface that PAT is operating on and maps the access list of addresses on the network to be translation
Ip nat inside	Configured on interface that are inside the network
Ip nat outside	Configured on interfaces that are outside the network
Ip nat inside source list [number] interface [interface] overload	Specifies the interface that PAT is operating on and maps the access list of addresses on the network to be translation. Configuration for dynamic NAT and PAT
Ip nat pool [pool name] [start ip address] [end ip address] netmask [mask of ip address range]	Configures a PAT/NAT pool of addresses to be used for translation and names the pool
Ip nat inside source list [number] pool [name]	Defines the inside IP addresses by the ACL and links the addresses to use NAT to the configured NAT pool

```
CorpA#show ip nat statistics
Total translations: 8 (0 static, 8 dynamic, 8 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: FastEthernet0/0 , FastEthernet0/0.20 , FastEthernet0/0.21 ,
FastEthernet0/0.22 , FastEthernet0/0.23
Hits: 23  Misses: 25
Expired translations: 16
Dynamic mappings:
CorpA#
CorpA#show ip nat trans
Pro  Inside global     Inside local       Outside local      Outside global
icmp 180.1.2.130:13    172.28.20.21:13    180.1.2.85:13      180.1.2.85:13
icmp 180.1.2.130:14    172.28.20.21:14    180.1.2.85:14      180.1.2.85:14
icmp 180.1.2.130:15    172.28.20.21:15    180.1.2.85:15      180.1.2.85:15
icmp 180.1.2.130:16    172.28.20.21:16    180.1.2.85:16      180.1.2.85:16
icmp 180.1.2.130:1     172.28.22.12:1     180.1.2.85:1       180.1.2.85:1
icmp 180.1.2.130:2     172.28.22.12:2     180.1.2.85:2       180.1.2.85:2
icmp 180.1.2.130:3     172.28.22.12:3     180.1.2.85:3       180.1.2.85:3
icmp 180.1.2.130:4     172.28.22.12:4     180.1.2.85:4       180.1.2.85:4

CorpA#
```

Figure 40: This screenshot displays the *show ip nat statistics* command on CorpA router on the Corporate A network. This command displays which interfaces are configured to be the nat inside and outside interfaces for CorpA. It also displays the number of translations. The *show ip nat translation* command displays the NAT translation table that maps the private IP address to the NAT assigned public IP address. This verifies that NAT is configured on the Corporate A network.

```
CorpC#show ip nat statistics
Total translations: 13 (0 static, 13 dynamic, 13 extended)
Outside Interfaces: Serial0/1/0
Inside Interfaces: FastEthernet0/0
Hits: 29  Misses: 22
Expired translations: 9
Dynamic mappings:
CorpC#
CorpC#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 180.1.2.162:13    172.28.40.102:13   172.28.20.21:13    172.28.20.21:13
icmp 180.1.2.162:14    172.28.40.102:14   172.28.20.21:14    172.28.20.21:14
icmp 180.1.2.162:15    172.28.40.102:15   172.28.20.21:15    172.28.20.21:15
icmp 180.1.2.162:16    172.28.40.102:16   172.28.20.21:16    172.28.20.21:16
icmp 180.1.2.162:17    172.28.40.102:17   180.1.2.85:17      180.1.2.85:17
icmp 180.1.2.162:18    172.28.40.102:18   180.1.2.85:18      180.1.2.85:18
icmp 180.1.2.162:19    172.28.40.102:19   180.1.2.85:19      180.1.2.85:19
icmp 180.1.2.162:1     172.28.40.101:1    180.1.2.85:1       180.1.2.85:1
icmp 180.1.2.162:20    172.28.40.102:20   180.1.2.85:20      180.1.2.85:20
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
tcp 180.1.2.162:1026   172.28.40.102:1026 180.1.2.85:80      180.1.2.85:80
```

Figure 41: This screenshot displays the *show ip nat statistics* command on CorpC router on the Corporate C network. This command displays which interfaces are configured to be the nat inside and outside interfaces for CorpC. It also displays the number of translations. The *show ip nat translation* command displays the NAT translation table that maps the private IP address to the NAT assigned public IP address. This verifies that dynamic NAT with PAT is configured on the Corporate C network.

```
CorpB#
CorpB#show ip nat stat
CorpB#show ip nat statistics
Total translations: 12 (0 static, 12 dynamic, 12 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: FastEthernet0/0 , FastEthernet0/1 , Serial0/0/0 , Serial0/1/0
Hits: 24  Misses: 28
Expired translations: 8
Dynamic mappings:
-- Inside Source
access-list 1 pool CORP_B refCount 12
 pool CORP_B: netmask 255.255.255.240
       start 180.1.2.146 end 180.1.2.156
       type generic, total addresses 11 , allocated 3 (27%), misses 0
CorpB#
CorpB#show ip nat trans
Pro  Inside global     Inside local       Outside local      Outside global
icmp 180.1.2.146:13    172.28.30.101:13   180.1.2.85:13      180.1.2.85:13
icmp 180.1.2.146:14    172.28.30.101:14   180.1.2.85:14      180.1.2.85:14
icmp 180.1.2.146:15    172.28.30.101:15   180.1.2.85:15      180.1.2.85:15
icmp 180.1.2.146:16    172.28.30.101:16   180.1.2.85:16      180.1.2.85:16
icmp 180.1.2.147:5     192.168.30.100:5   180.1.2.85:5       180.1.2.85:5
icmp 180.1.2.147:6     192.168.30.100:6   180.1.2.85:6       180.1.2.85:6
icmp 180.1.2.147:7     192.168.30.100:7   180.1.2.85:7       180.1.2.85:7
icmp 180.1.2.147:8     192.168.30.100:8   180.1.2.85:8       180.1.2.85:8
icmp 180.1.2.148:1     192.168.30.200:1   180.1.2.85:1       180.1.2.85:1
icmp 180.1.2.148:2     192.168.30.200:2   180.1.2.85:2       180.1.2.85:2
icmp 180.1.2.148:3     192.168.30.200:3   180.1.2.85:3       180.1.2.85:3
icmp 180.1.2.148:4     192.168.30.200:4   180.1.2.85:4       180.1.2.85:4

CorpB#
```

Figure 42: This screenshot displays the *show ip nat statistics* command on CorpB router on the Corporate B network. This command displays which interfaces are configured to be the nat inside and outside interfaces for CorpB. It also displays the number of translations. Additionally, it displays the pool that has been created and the number of usable addresses. The *show ip nat translation* command displays the NAT translation table that maps the private IP addresses to the NAT assigned public IP address. This verifies that a pool of at least ten addresses has been configured and is working properly on Corporate B network.

13. HTTP Server Static NAT

Static NAT is when a public IP address is assigned to be private IP address on a network. This uses a one-to-one mapping. Static NAT is useful to use when a device on a network needs to be accessed from the Internet or outside the network. In the challenge lab, the CorpB-HTTP-Server is configured with a static NAT IP address of 180.1.2.157. All the traffic to the CorpB-HTTP-Server via HTTP is permitted. All other traffic to this server is denied

Commands Used

Ip nat inside source static [host IP address] [public IP address to be assigned]	Used to assign the static NAT public IP address to a specific host on a network

```
CorpB#show ip nat trans
Pro  Inside global     Inside local       Outside local      Outside global
---  180.1.2.157       192.168.30.100     ---                ---

CorpB#
```

Figure 43: This screenshot displays the *show ip nat translation* command on CorpB router on the Corporate B network. It displays that a static NAT address of 180.1.2.157 has been assigned to 192.168.30.100 (CorpB-HTTP-Server).

```
CorpB#show access-lists
Standard IP access list 10
    10 permit host 172.28.30.101
    20 deny any
Standard IP access list 1
    10 permit 172.28.30.0 0.0.0.255 (32 match(es))
    20 permit 192.168.30.0 0.0.0.255 (24 match(es))
    30 permit 172.28.31.32 0.0.0.3
    40 permit 172.28.31.40 0.0.0.3
    50 permit 172.28.31.36 0.0.0.3
Extended IP access list DMZ-SERVER-PERMISSIONS
    10 permit tcp any host 192.168.30.100 eq www

CorpB#
```

Figure 44: This screenshot displays the *show access-list* command on the CorpB router on the Corporate B network. It displays that the access list DMZ-SERVER-PERMISSIONS has been created. This access list allows any device on the Internet or Corporate B LAN to HTTP to the server. It denies all other traffic. This is applied outbound on F0/1 of CorpB router.

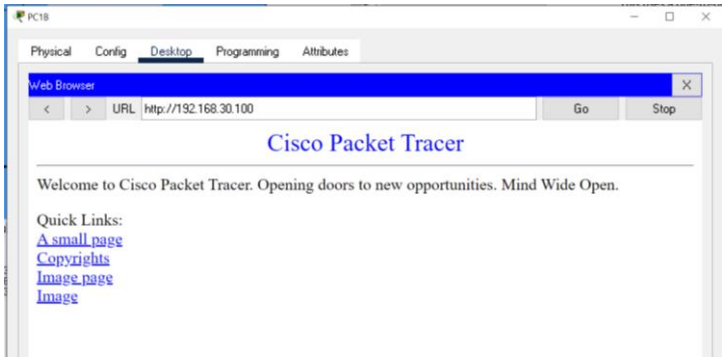


Figure 45: This screenshot displays that the PC1B PC on the Corporate B network can open a web browser and use HTTP to reach the CorpB-HTTP-Server. This is true to all the devices on the Corporate B network. It displays that HTTP traffic is being permitted.

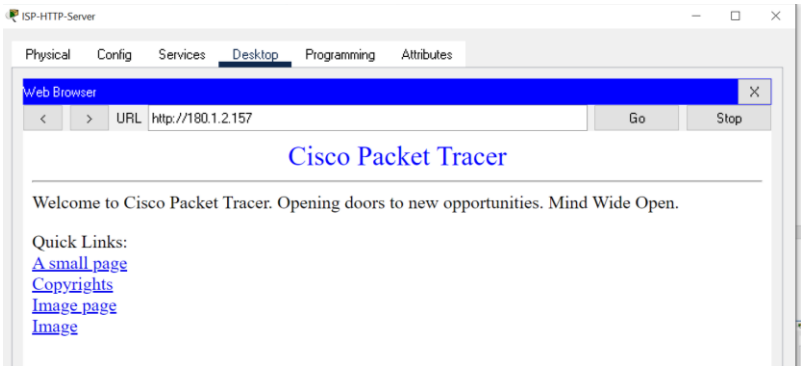


Figure 46: This screenshot displays that the ISP-HTTP-Server on the Interner can open a web browser and use HTTP to reach the CorpB-HTTP-Server via the static NAT IP address of 180.1.2.157. It displays that HTTP traffic is being permitted

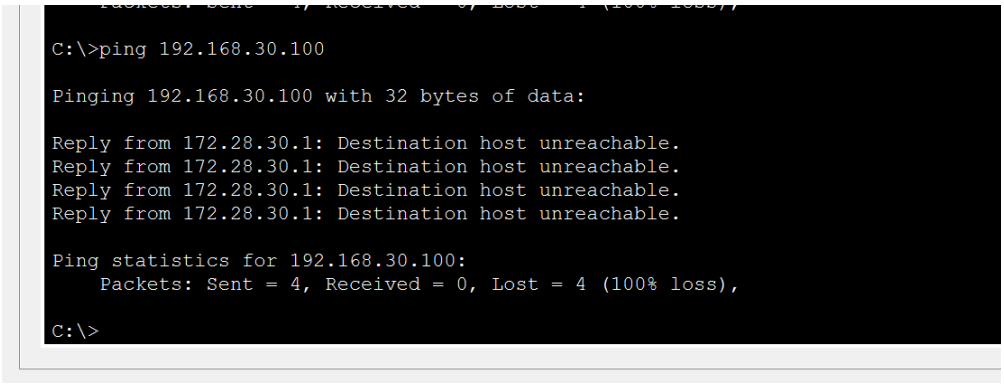


Figure 47: This screenshot displays that the PC1B PC on the Corporate B network cannot ping the CorpB-HTTP-Server. This is true to all the devices on the Corporate B network. It displays that other traffic to the CorpB-HTTP-Server is denied.

14. FTP Server Static NAT

Static NAT is when a public IP address is assigned to be private IP address on a network. This uses a one-to-one mapping. Static NAT is useful to use when a device on a network needs to be accessed from the Internet or outside the network. In the challenge lab, the CorpB-FTP-Server is configured with a static NAT IP address of 180.1.2.158. All the traffic to the CorpB-FTP-Server via FTP is permitted. All other traffic to this server is denied

Commands Used

Ip nat inside source static [host IP address] [public IP address to be assigned]	Used to assign the static NAT public IP address to a specific host on a network

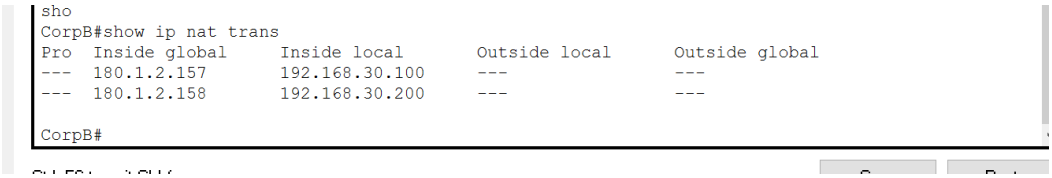


Figure 48: This screenshot displays the *show ip nat translation* command on CorpB router on the Corporate B network. It displays that a static NAT address of 180.1.2.158 has been assigned to 192.168.30.200 (CorpB-FTP-Server).

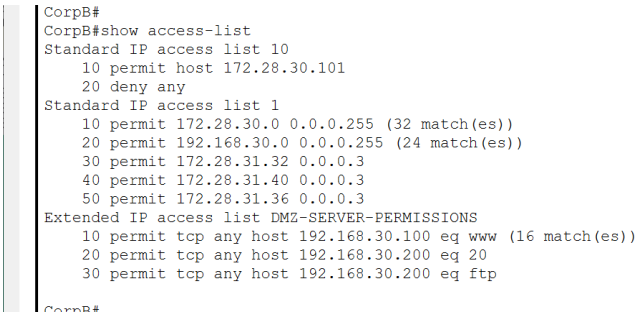


Figure 49: This screenshot displays the *show access-list* command on the CorpB router on the Corporate B network. It displays that the access list DMZ-SERVER-PERMISSIONS has been created. This access list allows any device on the Internet or Corporate B LAN to FTP to the server. It denies all other traffic. This is applied outbound on F0/1 of CorpB router.

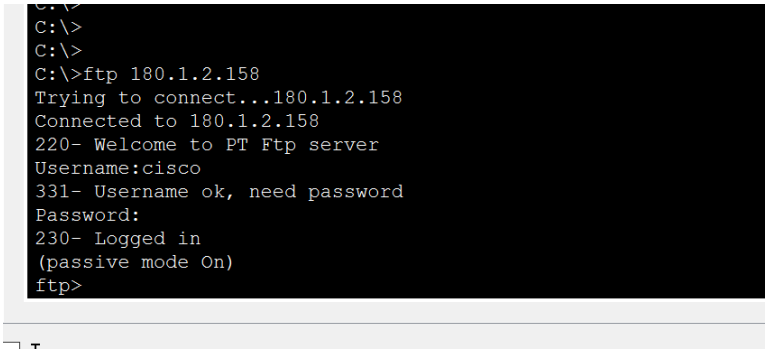


Figure 50: This screenshot displays that the ISP-HTTP-Server on the Internet can open the command prompt and ftp to 180.1.2.158 (the public IP address of the CorpB-FTP-Server). The connection is established, and the ISP-HTTP-Server can log into the CorpB-FTP-Server. This verifies that there is connectivity and FTP traffic is allowed.

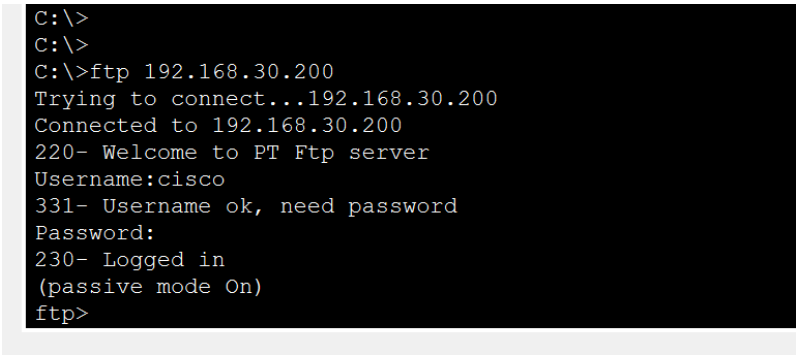


Figure 51: This screenshot displays that PC1B on the Corporate B network can open the command prompt and ftp to 192.168.30.200 (CorpB-FTP-Server). The connection is established, and PC1B can log into the CorpB-FTP-Server. This verifies that there is connectivity and FTP traffic is allowed.

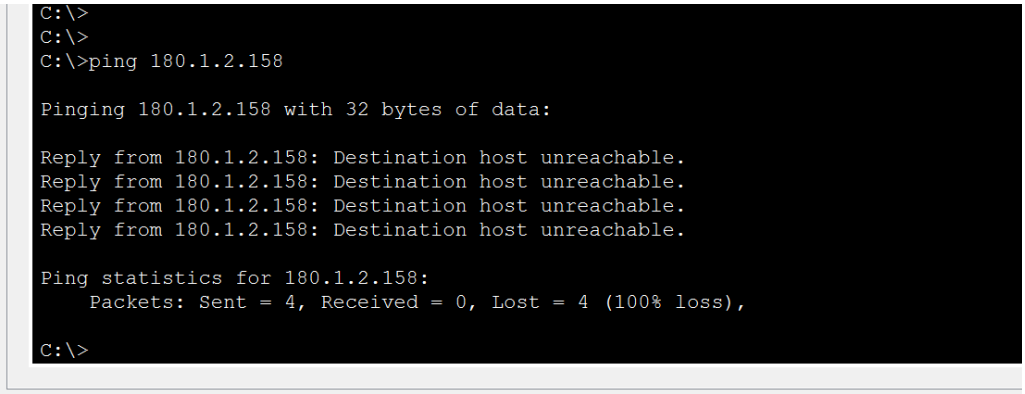


Figure 52: This screenshot displays that the ISP-HTTP-SERVER on the Internet cannot ping the CorpB-FTP-Server. This is true to all the devices on the Corporate B network and internet. It displays that other traffic to the CorpB-FTP-Server is denied.

15. Primitive Firewall

A primitive firewall is simply an access control list that is applied on an interface. ACLs are the most basic forms of firewalls. While they may not seem like a firewall, they are filtering the traffic that is allowed or not allowed through a network. Stateful firewalls are a type of primitive firewall. Stateful firewalls keep track of connections can allow certain traffic. The established keyword is added on to entries in ACE's. In the challenge lab, a primitive firewall is configured on the CorpC router of the Corporate C network. All traffic from the Corporate C network uses an established connection. All traffic from the Internet to the Corporate C network is denied. The established keyword is what allows return Internet traffic.

Commands Used

Ip access-list extended [name]	Creates a named extended ACL
Permit tcp [source ip] [source mask] [destination ip] [destination mask]	Adds a tcp permit entry an ACL
Established	Added to the end of ACE to allow for stateful firewall
Ip access-group [name] in|out	Apply and ACL to the inbound or outbound of an interface

```
CorpC#show access-list
Standard IP access list 1
    10 permit 172.28.40.0 0.0.0.255 (328 match(es))
Standard IP access list 10
    10 permit host 172.28.40.101
    20 deny any
Extended IP access list INBOUND-PRIMITIVE-FIREWALL
    10 deny ip 180.1.2.0 0.0.0.255 any
    20 deny ip host 255.255.255.255 any
    30 deny ip 127.0.0.0 0.255.255.255 any
    50 permit tcp 172.28.40.0 0.0.0.255 any (190 match(es))
    60 permit icmp 172.28.40.0 0.0.0.255 any (24 match(es))
Extended IP access list OUTBOUND-PRIMITIVE-FIREWALL
    10 permit tcp any 172.28.40.0 0.0.0.255 established (9 match(es))
    20 permit icmp any 172.28.40.0 0.0.0.255 (12 match(es))
    30 permit icmp any host 180.1.2.162 echo
    40 permit icmp any host 180.1.2.162 ttl-exceeded
    50 permit icmp any host 180.1.2.162 unreachable
    60 permit esp host 180.1.2.130 host 180.1.2.162

CorpC#
```

Figure 53: This screenshot displays the *show access-list* command on CorpC router on the Corporate C network. The access list INBOUND-PRIMITIVE-FIREWALL and OUTBOUND-PRIMITIVE-FIREWALL have been created. The established keyword is allowing traffic that originates in the Corporate C network to return from the Internet. All other traffic is blocked from entering the Corporate network.

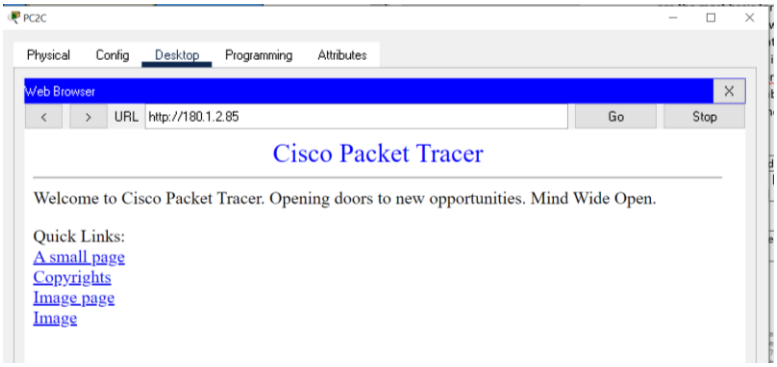


Figure 54: This screenshot displays that PC2C on the Corporate C network can open a web browser to the ISP-HTTP-Server. This occurs because of the established keyword.

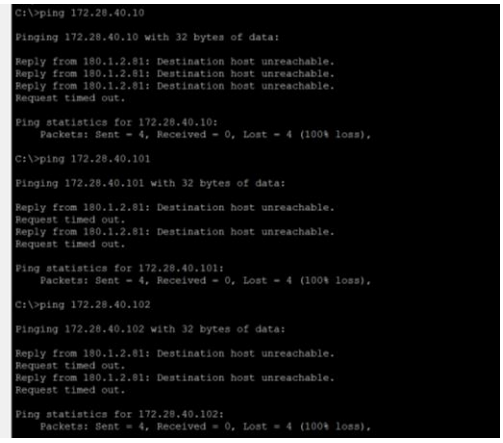


Figure 55: This screenshot displays that traffic from the Internet is not being allowed into the Corporate C network. The ISP-HTTP-Server is unable to ping to successfully ping to any of the devices on Corporate C network.

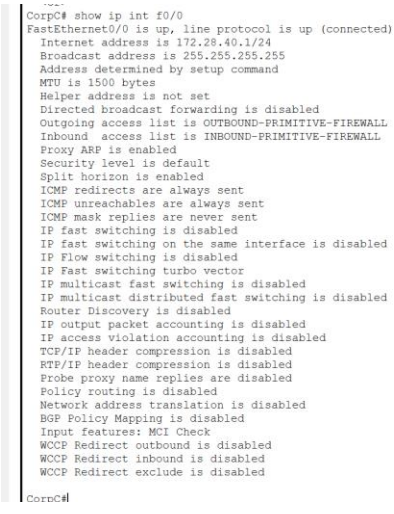


Figure 56: This screenshot displays the *show ip int f0/0* command on CorpC router on the Corporate C network. It displays that the ACL OUTBOUND-PRIMITIVE-FIREWALL is applied outbound on the interface. It also displays that the ACL INBOUND-PRIMITIVE-FIREWALL is applied inbound on the interface.

16. CBAC Firewall

Context-Based Access Control (CBAC) is a part of Cisco's firewall features. CBAC controls traffic that is allowed in and out of a network. A CBAC still uses access-list but uses IP inspection to inspect the traffic and see what traffic is to be permitted. In the challenge lab, A CBAC firewall is used on the CorpA router of the Corporate A network. All traffic destined for the Internet uses CBAC. All traffic from the Internet to the CorpA LAN should be denied by default. Additionally, all traffic that originates within the Corporate A network should be allowed back through. Configuration for this step was provided.

Commands Used

Ip inspect name [name] [protocol] timeout [timeout time]	Defines protocols that should be inspected and creates a name for the inspection group
Ip access-group [number] in|out	Used to assign an access list inbound or outbound on an interface
Ip inspect [name] in|out	Assigns the inspection group to an interface
Ip access-group [name] in|out	Apply and ACL to the inbound or outbound of an interface

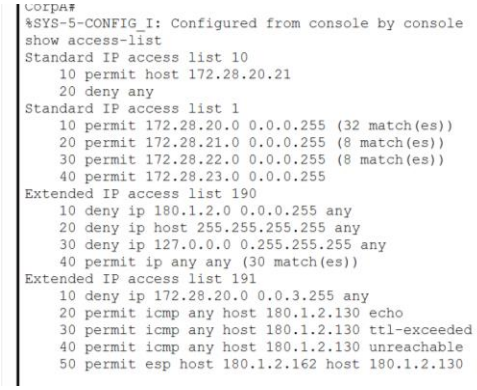


Figure 57: This screenshot displays the *show access-list* command on CorpA router on the Corporate A network. It displays access-list 190 and access-list 191 that have been created to implement the CBAC firewall.

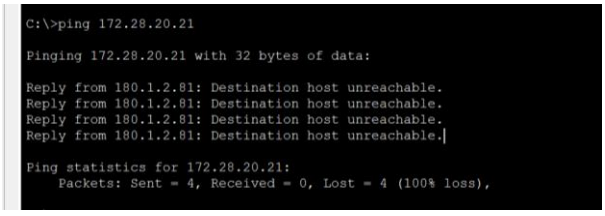


Figure 58: This screenshot displays the command prompt on ISP-HTTP-SERVER on the internet showing a ping to Corp-Server on Corporate A. It displays that the Internet traffic is denied from going to the Corporate A network.

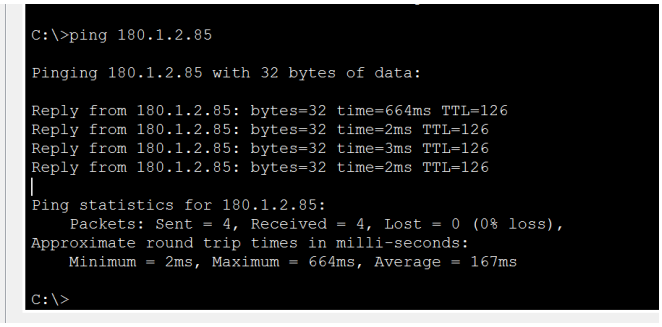


Figure 59: This screenshot displays the command prompt on Corp-Server on the Corporate A network showing a ping to ISP-HTTP-Server on the Internet. It displays that traffic initiated from within the LAN and destined for the internet is permitted.

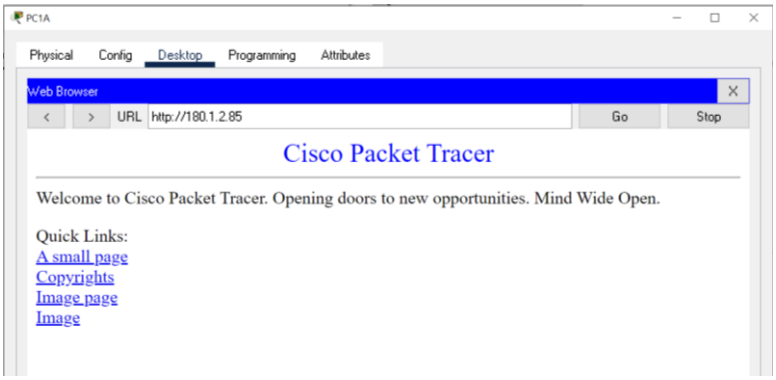


Figure 60: This screenshot displays that PC1C can open a web browser to the ISP-HTTP-Server. This is true to all PCs on the Corporate A network. It is demonstrating that traffic in the LAN can go to the internet and return. This TCP session can be inspected to demonstrate the CBAC is operating properly.

```
CorpA#show ip inspect sessions
Established Sessions
 Session 1013051856 (180.1.2.130:1025)=>(180.1.2.85:80) tcp SIS_OPEN
CorpA#show ip inspect session detail
Established Sessions
 Session 1013051856 (180.1.2.130:1025)=>(180.1.2.85:80) tcp SIS_OPEN
  Created 00:00:02, Last heard  00:00:02
  Bytes sent (initiator:responder) [360:360]
  In  SID 180.1.2.85[80:80]=>180.1.2.130[1025:1025] on ACL 191 (3 matches)
CorpA#
```

Figure 61: This screenshot displays the *show ip inspect sessions* command on CorpA router of the Corporate A network. It displays that a TCP session has been established. The source IP address is the public IP address being used by Corporate A and the destination address is the IP address of the ISP-HTTP-Server on the Internet. The *show ip inspect session detail* command is also displayed which shows the details of the session and the ACL that is being used.

17. Zone-Based Firewall

A zone-based policy firewall (ZPF) is a stateful firewall that uses zones to apply a firewall. Traffic between the zones is then monitored and inspected based on whatever policies and conditions are set. In the challenge lab, a ZPF is configured on the Corporate B network. Traffic from the Internet to the Corporate B network is denied. Traffic initiated in the LAN in permitted to return. The ZPF should track and inspect session info.

Commands Used

Zone-security [name]	Creates a new named zone
Class-map type inspect [match-any | match-all] name	Creates a class map and defines how traffic should be identified
Match protocol [protocol]	Defines a protocol in a class-map
Policy-map type inspect [name]	Creates a policy map and names it
Inspect	Tells the policy map to inspect traffic based on the class-map
Zone-pair security [name] source [source zone] destination [destination zone]	Creates a zone-pairing by defining two zones: one as the source and one as the destination
Service-policy type inspect [name]	Defines the policy map that the zone-pair applies to
Zone-member security [zone name]	Used to assign a interface to a zone

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


zone IN-ZONE
  Member Interfaces:
    FastEthernet0/0
    FastEthernet0/1


zone OUT-ZONE
  Member Interfaces:
    Serial0/0/1
```

Figure 62: This screenshot displays the *show zone security* command on the CorpB router on Corporate B network. This displays the zones that have been configured and interfaces that the zones have been assigned.

```
CorpB#show zone-pair security
Zone-pair name IN-2-OUT-ZPAIR
    Source-Zone IN-ZONE  Destination-Zone OUT-ZONE
    service-policy IN-2-OUT-PMAP
```

Figure 63: This screenshot shows the appropriate zone-pairs that have been configured on CorpB. The Corporate B network (IN-ZONE) is configured as the source zone and the Internet(OUT-ZONE) is configured as the destination.

```
CorpB#show policy-map type inspect zone-pair sessions
 Zone-pair: IN-2-OUT-ZPAIR

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

    Class-map: TRAFFIC (match-any)
      Match: protocol http
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol ftp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol icmp
        4 packets, 512 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 (default action)
        0 packets, 0 bytes
CorpB#
```

Figure 64: This screenshot shows the class map that has been created and that it is matching HTTP, TCP, ICMP, and FTP protocols. It also shows that we are using the match-any to inspect the traffic. At this point there has been no traffic/open sessions which is why there are no sessions logged.

```
CorpB#show policy-map type inspect zone-pair sessions
 Zone-pair: IN-2-OUT-ZPAIR

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

    Class-map: TRAFFIC (match-any)
      Match: protocol http
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol ftp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol icmp
        5 packets, 640 bytes
        30 second rate 0 bps
      Match: protocol tcp
        0 packets, 0 bytes
        30 second rate 0 bps
      Inspect
        Half-open Sessions
         Session 1230676144 (180.1.2.148:69)=>(180.1.2.85:0) icmp SIS_OPENING
          Created 00:00:03, Last heard 00:00:03
           ECHO request
          Bytes sent (initiator:responder) [128:0]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
CorpB#
```

Figure 65: This screenshot displays that the ZPF firewall is operating. When a ping is issued from PC1B on the Corporate B network to the ISP-HTTP-SERVER on the internet, the packets appear, and a half-session is established to show how the traffic is inspected. This displays that the ZPF is configured and operating correctly.

18. Local AAA

Authentication, Authorization, and Accounting (AAA) is used for network control. Authentication is controlling who is permitted to access. Authorization is controlling what someone can do. Accounting is keeping track what is done and by who. Local AAA uses a local database on the device and is useful on small networks. In the challenge lab, Local AAA is configured on the Corporate C network. User1 is configured with a password of cisco and is given a privilege level of 1 for user mode access. User2 is configured with a password of cisco and is given a privilege level of 15 for privilege mode access. Both users are able to remotely manage the devices locally.

Commands Used

Username [username] privilege [privilege level number] password [password]	Creates a username and password and defines a privilege level for the user.
Aaa new-model	Enables AAA on the device
Aaa authentication login default local-case	Enables authentication on the console, vty, and aux lines that uses default method list and is case sensitive
Login authentication default	Enables the lines to use login authentication
Login local	Enables lines to use local database for login

Figure 66: This screenshot displays that PC1C on the Corporate C network can successfully use local AAA to remotely manage CorpC router and CorpC-Sw. User1 with the password of cisco is used to login to each device. This demonstrates that local AAA is configured properly on the router and the switch.

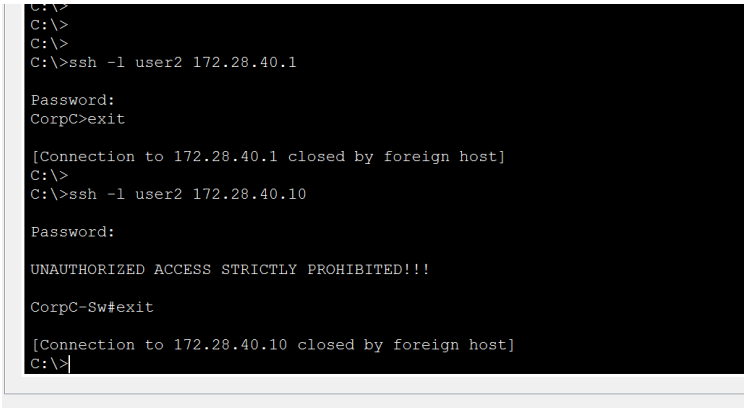


Figure 67: This screenshot displays that PC1C on the Corporate C network can successfully use local AAA to remotely manage CorpC router and CorpC-Sw. User2 with the password of cisco is used to login to each device. This demonstrates that local AAA is configured properly on the router and the switch.

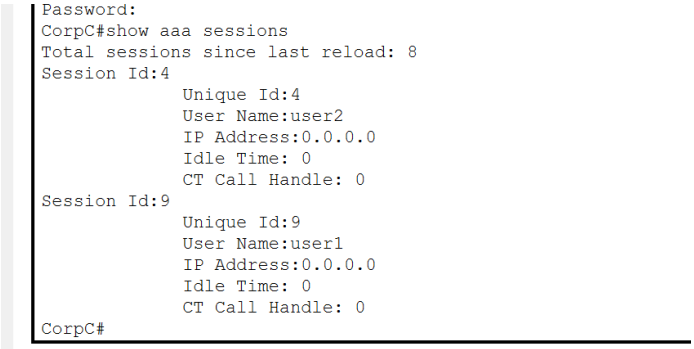


Figure 68: This screenshot displays the *show aaa sessions* command on CorpC router on the Corporate C network. This displays users that have opened a session and the ID assigned. User1 and User2 each have a session, displaying that local AAA is operating on CorpC router.

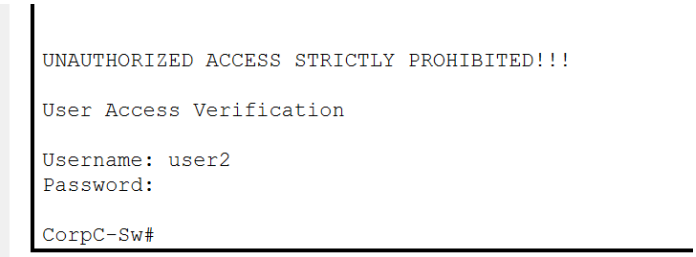


Figure 69: This screenshot displays that user2 has a privilege level of 15 and opens to the privilege mode.

19. Server-based AAA

Server-based AAA uses a configured AAA server to manage usernames and passwords. Network devices can connect to the AAA server and use the database of usernames and passwords on the server. Radius is a type of server-based AAA. Radius is the protocol that is used to communicate between the AAA server and the device. Radius is a combination of authentication and authorization. It uses UDP port 1645 or 1812 for authentication and port 1646 or 1813 for accounting. Radius hides passwords during transmission. In the challenge lab, the Corp-Server is configured as the AAA server. The username User1 is created with the password cisco. The username User2 is created with the password security. Locally on CorpA, the username admin with the password local is created.

Commands Used

Radius-server host [ip address]	Sets the IP address of the radius server for AAA
Radius-server key [key]	Sets the key being used by the radius server
Aaa new-model	Enables AAA on the device
Aaa authentication login default group radius local	Enables authentication on the console, vty, and aux lines that uses radius first then the local database as a backup
Login authentication default	Enables the lines to use login authentication

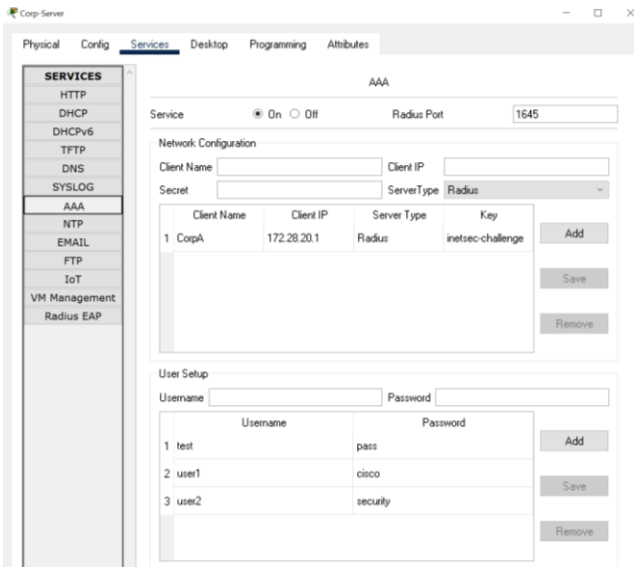


Figure 70: This screenshot displays that the Corp-Server on Corporate A network has AAA enabled. The only configured host client is CorpA router because that is the only router on the Corporate A network and the switches in packet tracer do not support AAA. The switches in the Corporate A network have local AAA enabled. Username user1 with the password cisco and username user2 with the password security have been configured on the AAA server to use for login. For some reason, user2 is not working. I configured a third username test and password pass and that one is working. I am not sure why user2 will not work.

```
UNAUTHORIZED ACCESS STRICTLY PROHIBITED!!!

User Access Verification

Username: user1
Password:
CorpA>
```

Figure 71: This screenshot displays that Server-based AAA is operating correctly on CorpA router on the Corporate A network. The username User1 and password cisco configured on AAA server can successfully be used to login into the CorpA router.

```
C:\>
C:\>
C:\>
C:\>
C:\>ssh -l user1 172.28.20.1

Password:
CorpA>
CorpA>
CorpA>exit

[Connection to 172.28.20.1 closed by foreign host]
C:\>
C:\>ssh -l test 172.28.20.1

Password:
CorpA>
CorpA>exit

[Connection to 172.28.20.1 closed by foreign host]
C:\>
C:\>ssh -l user2 172.28.20.1

Password:
% Login invalid


Password:

Password:

[Connection to 172.28.20.1 closed by foreign host]
C:\>
```

Figure 72: This screenshot displays that Corp-Server is able to use the logins created on Corp-Server to remotely access the CorpA router. Username User1 and Username test are successfully able to establish a remote connection demonstrating that the AAA server is working. However, there must be something wrong in packet tracer because User2 with password security does not work.

20. Syslog

Syslog is the network protocol for accessing system messages. It is an important aspect of security to log everything that occurs. System logging allows for information regarding when, where, what, and who was changed. System logging can occur internally or be logged externally. The logged messages can have different severity levels. Network administrators can set what alert levels they want. In the challenge lab, Syslog is enabled on CorpA router on the Corporate A network. The logs are sent to the Corp-Server on the Corporate A network.

Commands Used

Logging host [ip-address]	Set the IP address of the syslog server
Logging on	Enable system logging to log messages

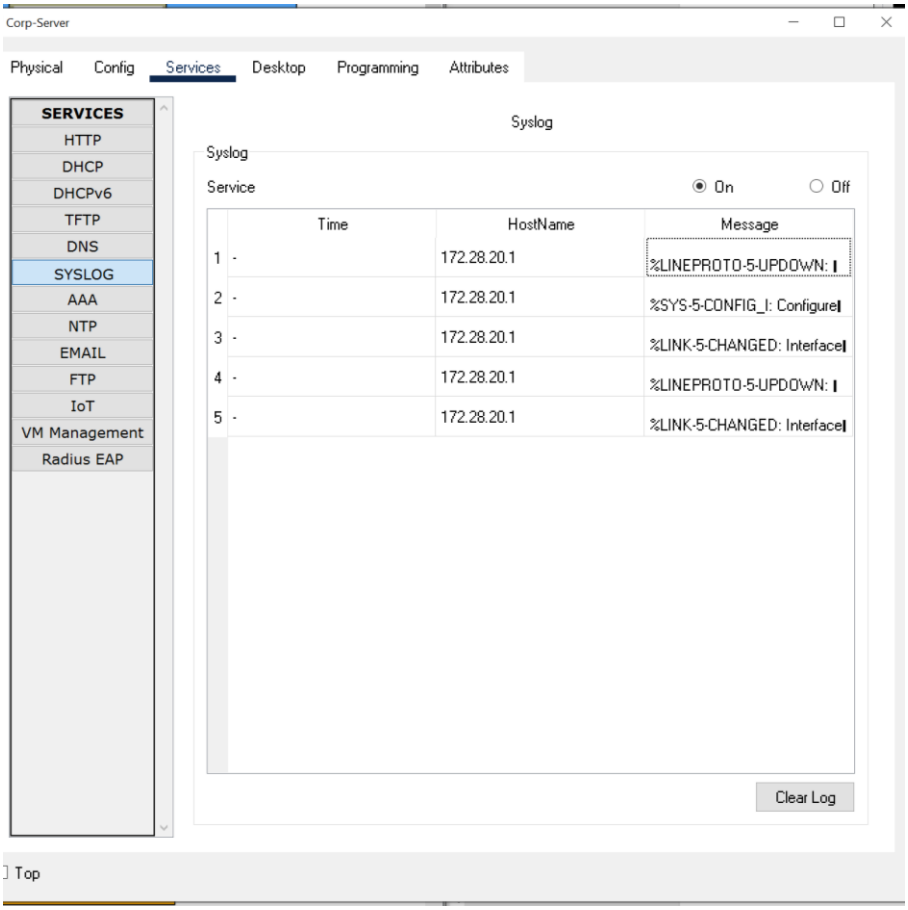


Figure 73: This screenshot displays that Syslog has been enabled on Corp-Server on the Corporate A network. This also displays that it is operational and logging messages from 172.28.20.1 (Corp A Router).

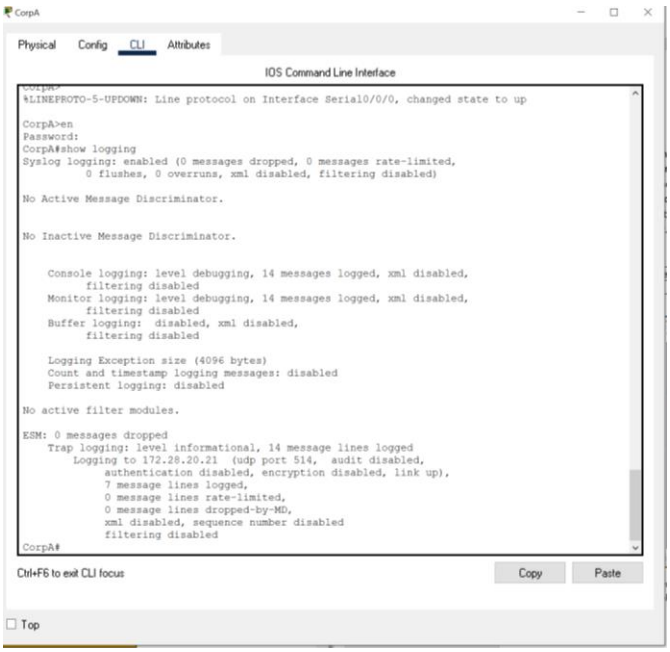


Figure 74: This screenshot displays the *show logging* command on the CorpA router on the Corporate A network. It displays that syslog logging is enabled on the device. It also displays that it is logging to 172.28.20.21 (Corp-Server) and indicates the number of messages that already have been logged.

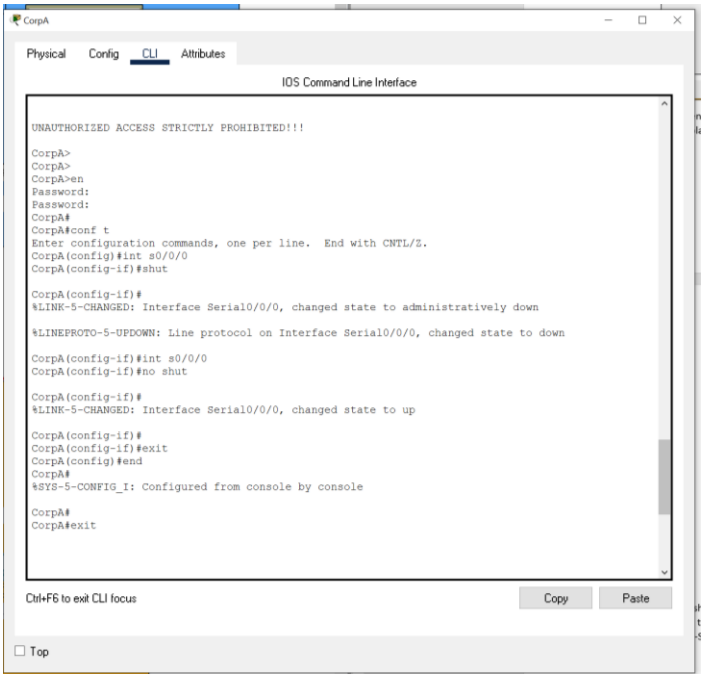


Figure 75: This screenshot displays logging messages on CorpA router. This displays the messages that appear when entering the different configuration modes and when an interface is turned on and off. This is showing that logging is occurring on the device. All these messages are then sent to the Syslog Server.

21. NTP

Network Time Protocol (NTP) is used to standardized device times across a network. Accurate date and timestamps are especially important for security. The timestamps can be useful in identifying malicious activity and changes that occurred at the same time on a network. NTP allows for clock synchronization. One device is configured as the NTP server which allows the clock to be set. From there, devices are configured as NTP clients to obtain date and time information. In the challenge lab, Corp-Server on the Corporate A network is configured to be an NTP server. CorpA router and all the other devices on the Corporate A network then utilize the NTP server for date and timestamps.

Commands Used

Ntp server [ip address]	Specifies the ip address of the NTP server
Ntp authenticate	Enables NTP authentication
Ntp authentication-key [key number] md5 [key]	Used to define the authentication keys
Ntp trusted-key [key number]	Used to identify with the system to synchronize with

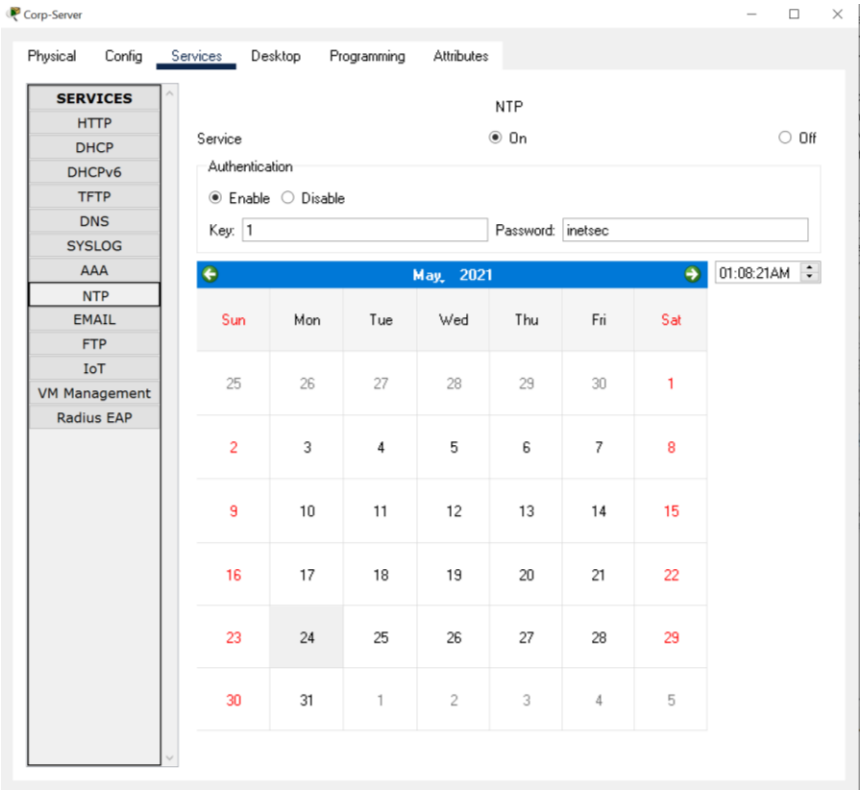


Figure 76: This screenshot displays that NTP has been enabled on Corp-Server on the Corporate A network. Additionally, NTP authentication has been enabled to enhance network security. The authentication key that has been specified is 1 and the password is inetsec. Authentication is then used by all the NTP clients to connect to the NTP server.

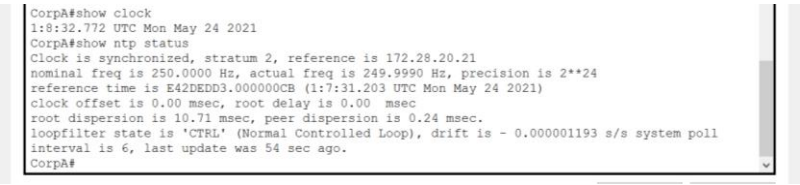


Figure 77: This screenshot displays the *show clock* command on CorpA router on the Corporate A network to display the time set on the device. Additionally the *show ntp status* command is also displayed which indicates that the clock is synchronized with the NTP server and indicates the NTP server address is 172.28.20.21 (Corp-Server).

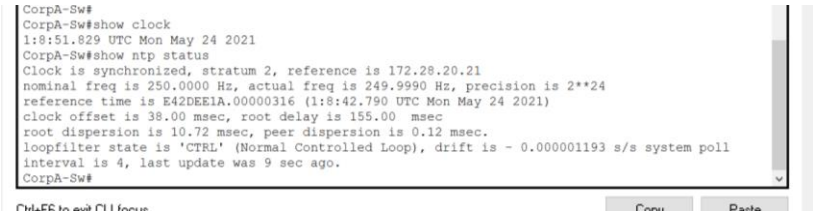


Figure 78: This screenshot displays the *show clock* command on CorpA-Sw switch on the Corporate A network to display the time set on the device. Additionally the *show ntp status* command is also displayed which indicates that the clock is synchronized with the NTP server and indicates the NTP server address is 172.28.20.21 (Corp-Server).

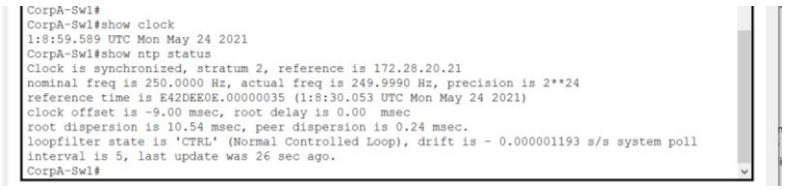


Figure 79: This screenshot displays the *show clock* command on CorpA-Sw1 switch on the Corporate A network to display the time set on the device. Additionally the *show ntp status* command is also displayed which indicates that the clock is synchronized with the NTP server and indicates the NTP server address is 172.28.20.21 (Corp-Server).

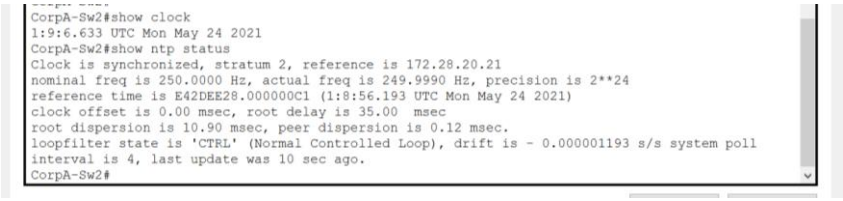


Figure 80: This screenshot displays the *show clock* command on CorpA-Sw2 switch on the Corporate A network to display the time set on the device. Additionally the *show ntp status* command is also displayed which indicates that the clock is synchronized with the NTP server and indicates the NTP server address is 172.28.20.21 (Corp-Server).

22. InterVLAN Routing

InterVLAN routing simply is allowing the traffic from one VLAN to be forwarded to another VLAN. InterVLAN routing enables communication among multiple VLANs. There are different kinds of InterVLAN routing that can be configured. In the Challenge lab we use Router-On-A-Stick interVLAN routing to configure interVLAN routing on CorpA on the Corporate A network. VLAN23 is configured as the administrative VLAN and named NetMgmt.

Commands Used

Interface f0/0.[number]	Enables sub-interfaces on one interface
Vlan [number]	Creates a VLAN
Name [name]	Names a VLAN
Switchport trunk native vlan [number]	Used to assign a VLAN to be the native/administrative VLAN

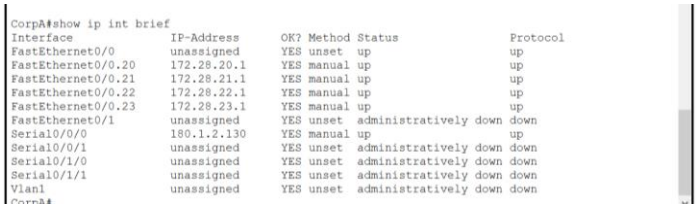


Figure 81: This screenshot displays the *show ip int brief* command on CorpA router on the Corporate A network. It displays that four sub-interfaces have been created on F0/0. F0/0.20 is configured with an IP address and is for VLAN20. F0/0.21 is configured with an IP address and is for VLAN21. F0/0.22 is configured with an IP address and is for VLAN22. F0/0.23 is configured with an IP address and is for VLAN23.

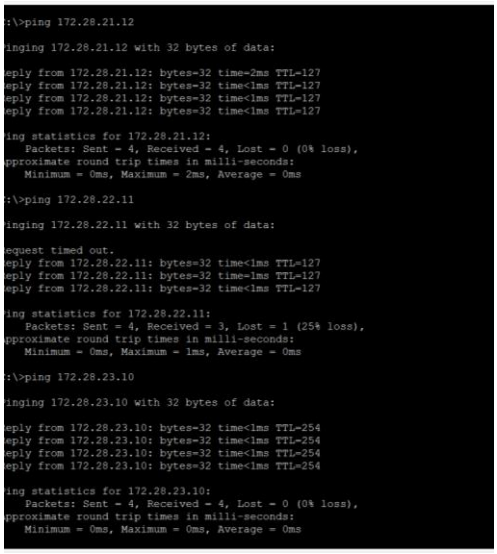


Figure 82: This screenshot displays that Corp-Server on VLAN20 can ping to VLAN 21, VLAN22, and VLAN23. This demonstrates InterVLAN connectivity and configuration.

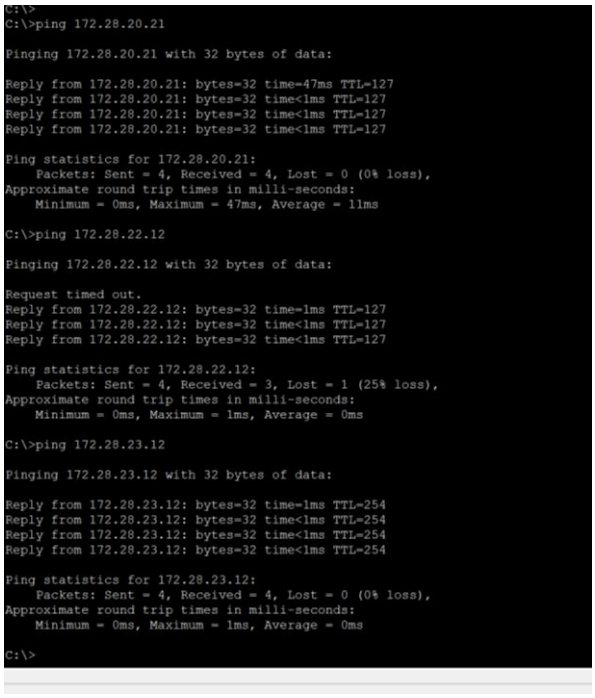


Figure 83: This screenshot displays that PC1A on VLAN21 can ping to VLAN 20, VLAN22, and VLAN23. This demonstrates InterVLAN connectivity and configuration.

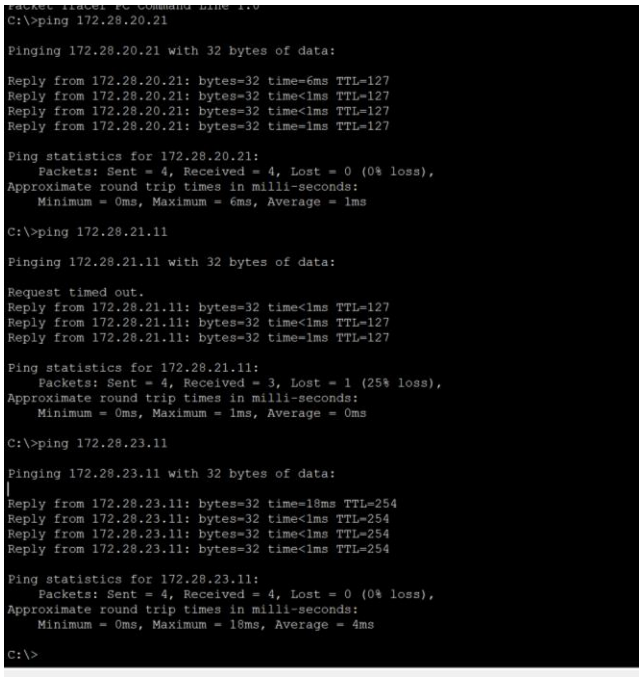


Figure 84: This screenshot displays that PC4A on VLAN22 can ping to VLAN 20, VLAN21, and VLAN23. This demonstrates InterVLAN connectivity and configuration.

23. IPSec VPN

IPSec is a standard that is used for defining how a VPN is secured. It is used to protect and authenticate IP packets between a source and a destination. A Site-to-Site VPN establishes a VPN tunnel over the internet to transmit traffic between two networks. For a Site-to-Site IPSec VPN to work properly, both sites must be configured with ISAKMP security associations. A VPN tunnel is created when defined interesting traffic is generated. In the challenge lab, an IPSec Site-to-Site VPN is configured between CorpA router on Corporate A network to CorpC router on Corporate C network.

Commands Used

Crypto isakmp policy [number]	Creates a new ISAKMP policy and assigns it a number
Encryption aes 256	Sets the encryption of the isakmp policy to use AES 256 – Configures the HASH
Authentication pre-share	Authentication information is pre-shared. This configures the authentication
Group [number]	Sets the Diffie-Hellman group
Crypto isakmp key [key] address [ip address]	Used to configure the pre-shared keys
Crypto ipsec transform-set [name] esp-aes esp-sha-hmac	Creates and names a transform set that used esp-aes for encryption and esp-sha-hmac for hashing
Crypto map [map-name] [map-sequence number] [ipsec-isakmp | ipsec-manual]	Creates a crypto map
Set peer [ip address]	Specific the peer ip address for a crypto map
Set transform-set [transform-set name]	Sets the transform set on the crypto map
Match address [number]	Binds an ACL to the crypto map
Crypto map [name]	Used to bind a crypto map to an interface

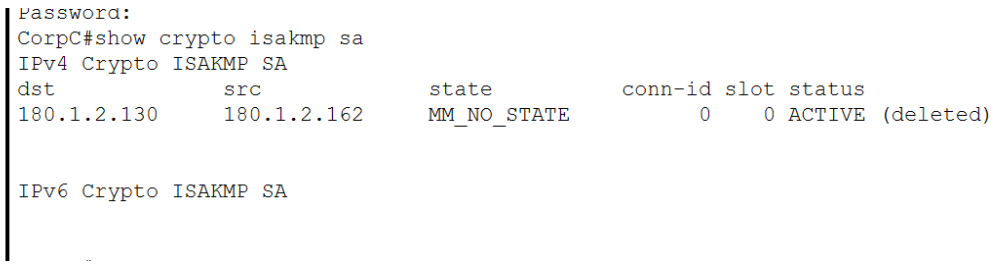
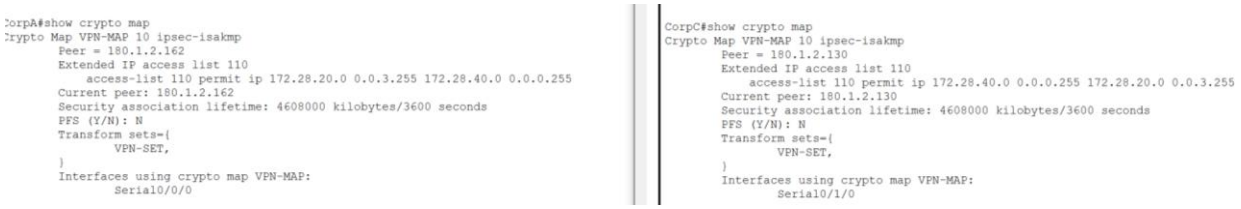


Figure 85: This screenshot displays the *show crypto isakmp sa* command on CorpC router on the Corporate C network. It displays that a VPN tunned from the CorpC network to the CorpA network is configured. For some reason, the tunnel is not connected properly to CorpA network.



```
CorpA#show crypto map
Crypto Map VPN-MAP 10 ipsec-isakmp
        Peer = 180.1.2.162
        Extended IP access list 110
            access-list 110 permit ip 172.28.20.0 0.0.3.255 172.28.40.0 0.0.0.255
        Current peer: 180.1.2.162
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                VPN-SET,
        }
        Interfaces using crypto map VPN-MAP:
                Serial0/0/0
```

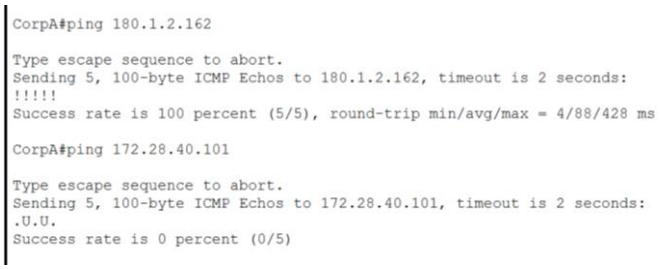
```
CorpC#show crypto map
Crypto Map VPN-MAP 10 ipsec-isakmp
        Peer = 180.1.2.130
        Extended IP access list 110
            access-list 110 permit ip 172.28.40.0 0.0.0.255 172.28.20.0 0.0.3.255
        Current peer: 180.1.2.130
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                VPN-SET,
        }
        Interfaces using crypto map VPN-MAP:
                Serial0/1/0
```

Figure 86: This screenshot displays the *show crypto map* command on the CorpA router and the Corp C router. It displays that both the devices have the crypto map configured properly. The peer address of each device is correct, and the access list is correct for each device and applied. The transform set is applied to each and each crypto map is applied to the correct interface.

```
CorpA#show crypto ipsec transform-set
Transform set VPN-SET: {    { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

```
CorpC#show crypto ipsec transform-set
Transform set VPN-SET: {    { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

Figure 87: This screenshot displays the *show crypto ipsec transform-set* command on the CorpA router and the Corp C router. It displays that both have the transform set configured to be VPN-SET using esp-aes and esp-sha-hmac.



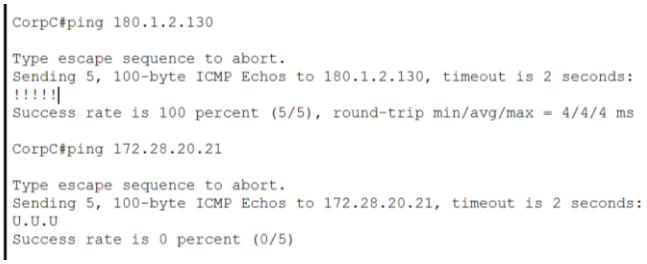
```
CorpA#ping 180.1.2.162

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 180.1.2.162, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/88/428 ms

CorpA#ping 172.28.40.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.28.40.101, timeout is 2 seconds:
.U.U.
Success rate is 0 percent (0/5)
```

Figure 88: This screenshot displays the CorpA router can ping the public IP address of CorpC router. However, it is unable to ping into the CorpC network.



```
CorpC#ping 180.1.2.130

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 180.1.2.130, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

CorpC#ping 172.28.20.21

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.28.20.21, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

Figure 89: This screenshot displays the CorpC router can ping the public IP address of CorpA router. However, it is unable to ping into the CorpA network.

I cannot figure out why the IPSec Site-to-Site VPN is not working. Everything to me looks to be configured correctly and matches. I followed a configuration that working within a past lab however it is not working here. I have even removed the ACLs on both networks and the configurations still did not work. Even after all my troubleshooting, I cannot understand what the issue is with the VPN.

24. VTP

VLAN Trunking Protocol (VTP) is a protocol used to define VLAN's for a network. From configuring a device to be a VTP server, all VLAN information that is created on the VTP server is then advertised to all devices configured as VTP clients. This is useful for managing VLAN's on a network. This allows all devices to have the VLAN's and changes can be made centrally on one device instead of all the devices in the network. VTP is used on Cisco switches. In the challenge lab, CorpA-Sw is configured as the VTP server. CorpA-Sw1 and CorpA-Sw2 are configured as VTP clients. The VTP password that has been configured is security.

Commands Used

Vtp domain [domain name]	Assigns the VTP domain name
Vtp password [password]	Assigns the VTP password
Vtp mode server	Assigns the device to be a VTP server
Vtp mode client	Assigns the device to be a VTP client

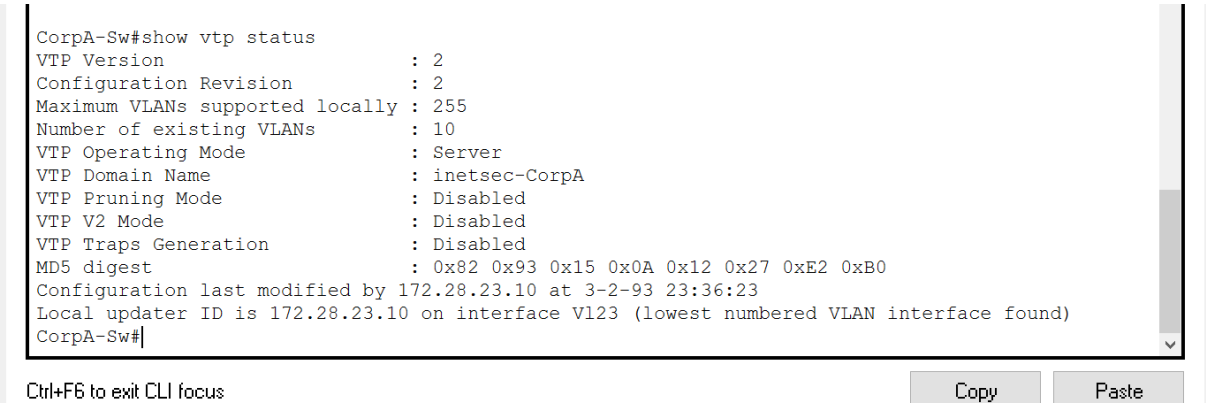


Figure 90: This screenshot displays the *show vtp status* command on CorpA-Sw on the Corporate A network. This displays that CorpA-Sw has been configured as the VTP server. It shows that the domain name is configured to be inetsec-CorpA. This displays that CorpA-Sw has been configured as the VTP server and all the VLANs are being propagated to the VTP clients.

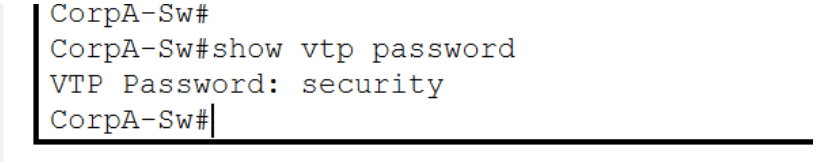


Figure 91: This screenshot displays the *show vtp password* command on CorpA-Sw on the Corporate A network. It displays that the configured VTP password is security.

```
CorpA-Sw1# show vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : inetsec-CorpA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x82 0x93 0x15 0x0A 0x12 0x27 0xE2 0xB0
Configuration last modified by 172.28.23.10 at 3-2-93 23:36:23
CorpA-Sw1#show vtp password
VTP Password: security
CorpA-Sw1#
```

Figure 92: This screenshot displays the *show vtp status* command on CorpA-Sw1 on the Corporate A network. This displays that CorpA-Sw1 has been configured as the VTP client. It shows that the domain name is configured to be inetsec-CorpA. It also shows the *show vtp password* command which displays that the password being used is security.

```
Password:
CorpA-Sw2#show vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : inetsec-CorpA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x82 0x93 0x15 0x0A 0x12 0x27 0xE2 0xB0
Configuration last modified by 172.28.23.10 at 3-2-93 23:36:23
CorpA-Sw2#show vtp password
VTP Password: security
CorpA-Sw2#
```

Figure 93: This screenshot displays the *show vtp status* command on CorpA-Sw2 on the Corporate A network. This displays that CorpA-Sw2 has been configured as the VTP client. It shows that the domain name is configured to be inetsec-CorpA. It also shows the *show vtp password* command which displays that the password being used is security.

25. Layer2 Interface Security Mitigation Techniques

Networks often protect from layer 3 and up. It is important to implement security techniques on layer 2 switches because any compromise on layer 2 will affect all the other layers. There are a variety of different switch attacks that layer 2 security can protect against. In the challenge lab, the switches on the Corporate A network have layer 2 security mitigation techniques in place. Switches automatically detect the mac address of the PC connected to an interface. The interfaces are configured to only allow a maximum number of mac-addresses to be 3. If the number of permitted MAC-Addresses is exceeded, the interfaces are configured to automatically restrict all traffic.

Commands Used

Switchport port-security	Enables port-security on an interface
Switchport port-security maximum [number]	Sets the maximum number of MAC addresses allowed to an interface
Switchport port-security violation [violation]	Sets the violation that will occur if the number of allowed MAC addresses is exceeded for an interface
Switchport port-security mac-address stick	Automatically sets the mac address on an interface to the first mac address identified
Switchport nonegotiate	Used to disable DTP
Ip dhcp snooping	Enables DHCP snooping
Ip dhcp snooping trust	Enables a port to be a trusted DHCP port
Ip dhcp snooping vlan [number]	Enables DHCP snooping on VLAN
Ip dhcp snooping limit rate [number]	Enables the limit of MAC-Addresses allowed for DHCP

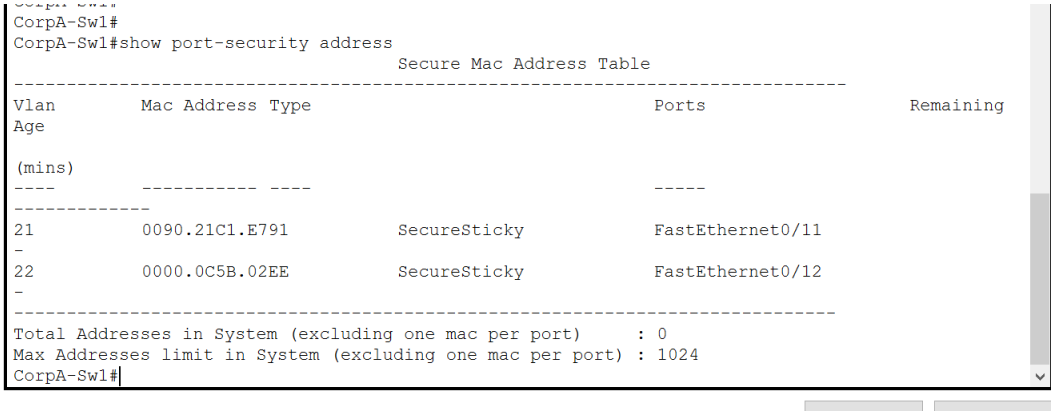


Figure 94: This screenshot displays the *show port-security address* command on CorpA-Sw1 on the Corporate A network. It displays that MAC-Addresses that have been learned for the interfaces and the VLANs that each device is on. It displays that the MAC-addresses have been learned automatically by SecureSticky. This is applied to all the switches in the Corporate A network that have hosts connected to an interface.

```
CorpA-Sw1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
-----------------------------------------------------------------------
       Fa0/11        3          1                0         Restrict
       Fa0/12        3          1                0         Restrict
-----------------------------------------------------------------------
CorpA-Sw1#
```

Figure 95: This screenshot displays the *show port-security* command on CorpA-Sw1 on the Corporate A network. It displays that the interfaces that have port-security enabled, the number of allowed Mac-addresses on an interface, the number of addresses already configured, the number of security violations that have occurred, and the action that takes place when there is a security violation on that interface.

```
  <cr>
CorpA-Sw#show dtp
Global DTP information
    Sending DTP Hello packets every 30 seconds
    Dynamic Trunk timeout is 300 seconds
    0 interfaces using DTP
CorpA-Sw#
```

Ctrl+F6 to exit CLI focus

Figure 96: This screenshot displays the *show dtp* command on CorpA-Sw on the Corporate A network. It displays that Dynamic Trunking Protocol (DTP) has been disabled. This prevents DTP negotiation and only limits a switch access or trunk access to the configured VLAN.

```
CorpA-Sw#
CorpA-Sw#
CorpA-Sw#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
20-23
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/20           yes        unlimited
CorpA-Sw#
```

Figure 97: This screenshot displays the *show ip dhcp snooping* command on CorpA-Sw on the Corporate A network. It displays that DHCP snooping has been enabled which is used to prevent rogue DHCP servers and any malicious DHCP traffic.

26. Other Protocols

All network devices come with different configurations. Many times, there are protocols and service enabled on devices that are not needed. Unused protocols should be disabled for security purposes. Additionally, all unused interfaces on a device should be shutdown to ensure those interfaces stay down and no rogue device can connect. In the challenge lab, unused enabled protocols enabled on the router are disabled. All interfaces that are not used on switches and routers are disabled.

Commands Used

No service dhcp	A DHCP server is being used, therefore the router does not need any DHCP service configured
No ip domain-lookup	Disables the Domain Name System resolution services on the router
No lldp run	Disables LLDP globally on the router.
Service password-encryption	Used to encrypt passwords
shutdown	Used to administratively shutdown interfaces

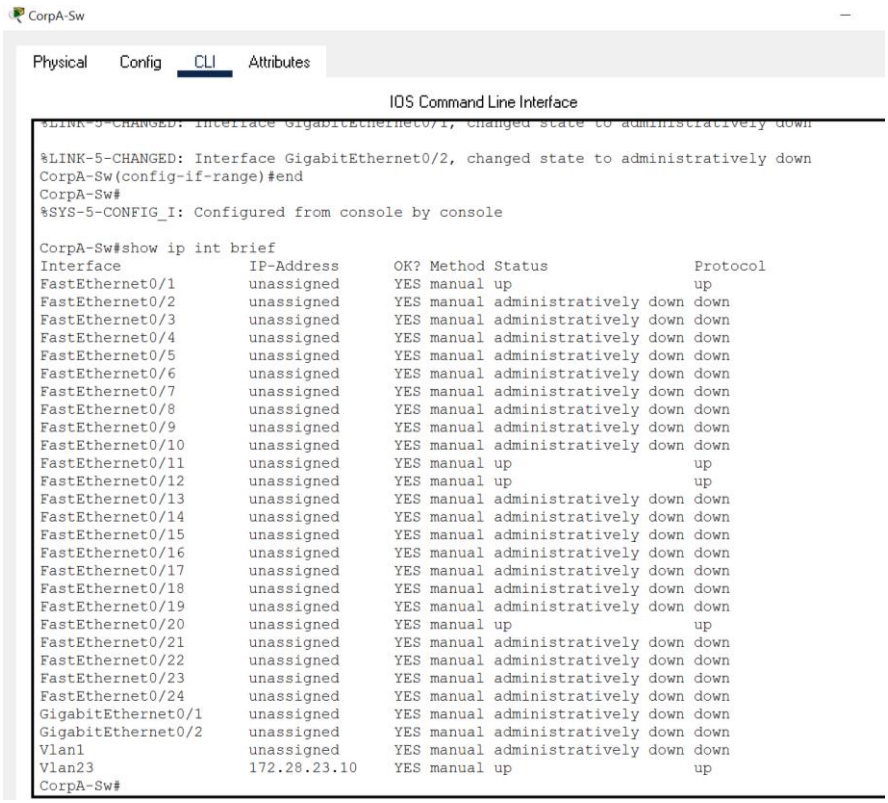


Figure 98: This screenshot displays the *show Ip int brief* command on the CorpA-Sw on the Corporate A network. This displays that all unused switch interfaces have been disabled. The administratively disabled command indicates that the interfaces have been shutdown. This is true to all the unused interfaces on any switch or router within the Corporate A, B, C or Internet.

```
CorpC#show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 172.28.40.1/24
FastEthernet0/1 is administratively down, line protocol is down
Serial0/0/0 is administratively down, line protocol is down
Serial0/0/1 is administratively down, line protocol is down
Serial0/1/0 is up, line protocol is up
  Internet address is 180.1.2.162/28
Serial0/1/1 is administratively down, line protocol is down
Vlan1 is administratively down, line protocol is down
CorpC#
```

Figure 99: This screenshot displays the *show protocols* command on the CorpC router on the Corporate C network. It displays the protocols that are enabled and the interface configurations for the device.

```
CorpB#
CorpB#
CorpB#show lldp neighbors
% LLDP is not enabled
CorpB#
```

Figure 100: This screenshot displays the *show lldp neighbors* command on the CorpB router on the Corporate B network. It displays the protocols that lldp is not enabled on the device. This feature is disabled on all the switches and routers within in the topology.

```
UNAUTHORIZED ACCESS STRICTLY PROHIBITED!!!

User Access Verification

Username: user1
Password:
CorpA>en
Password:
CorpA#
```

Figure 101: This screenshot displays how the CorpA router access is locked. Login is required to access the device and a banner message is displayed. This type of login in true to all the routers and switches within the topology. This prevents outsiders from logging in and warns the people before of any violations.

27. ASA

A Cisco Adaptive Security Appliance (ASA) is a security device that combines many features into one device. There are different models of ASA that support different capabilities and functions. In the challenge lab, a new network Corporate D is created. It is a cisco ASA5505 that is connected to the ISP router. On the CorpD network, there is one switch that has two PC's and one server connected to it. An IP addressing scheme on 192.168.1.0/24 is configured on the CorpD network. The address 180.1.2.180 is configured on ISP F0/1 and the address 180.1.2.181 is configured on the CorpD-ASA E0/0. DHCP is enabled on CorpD to assign addresses to all the devices on the network. NAT and PAT are implemented to translate private IP addresses to public IP addresses. Access control to the network is also configured.

```
CorpD-ASA(config)#exit
CorpD-ASA#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic inside-net interface
    translate_hits = 4, untranslate_hits = 3

CorpD-ASA#
```

Figure 102: This screenshot displays the *show nat* command on the CorpD-ASA. This displays that NAT and PAT have been configured to translate addresses from the inside network to the outside network. The entry in the table is from a Ping sent from the PC1D on the CorpD network to the ISP-HTTP-SERVER on the Internet.

```
CorpD-ASA#show ip address
System IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Vlan1                                      unassigned      unassigned      CONFIG
Vlan2                                      unassigned      unassigned      DHCP
Vlan50                 outside             180.1.2.181     255.255.255.240 manual
Vlan51                 inside              192.168.1.1     255.255.255.0   manual

Current IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Vlan1                                      unassigned      unassigned      CONFIG
Vlan2                                      unassigned      unassigned      DHCP
Vlan50                 outside             180.1.2.181     255.255.255.240 manual
Vlan51                 inside              192.168.1.1     255.255.255.0   manual

CorpD-ASA#show switch vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1                                     down      Et0/2, Et0/3, Et0/4, Et0/5
                                                Et0/6, Et0/7
2                                     down
50   outside                          up        Et0/0
51   inside                           up        Et0/1
CorpD-ASA#
```

Figure 103: This screenshot displays the *show ip address* command which displays the IP address and subnet mask that have been assigned to each VLAN. It also displays the *show switch vlan* command which displays which VLANs have been created and the interfaces they are assigned. The inside and outside networks are defined.

```
  all  Show all dhcpd bindings
CorpD-ASA#show dhcpd binding all
IP address       Client Identifier        Lease expiration        Type
192.168.1.10     0001.C7C7.2D2E           --                      Automatic
192.168.1.11     000B.BECD.7A54           --                      Automatic
192.168.1.12     000C.8587.2401           --                      Automatic
CorpD-ASA#
```

Figure 104: This screenshot displays the *show dhcpd binding all* command on the CorpD-ASA. This command displays the DHCP has been enabled on the CorpD-ASA and displays the IP addresses that have been assigned to the two PC's and server on the Corporate D network.

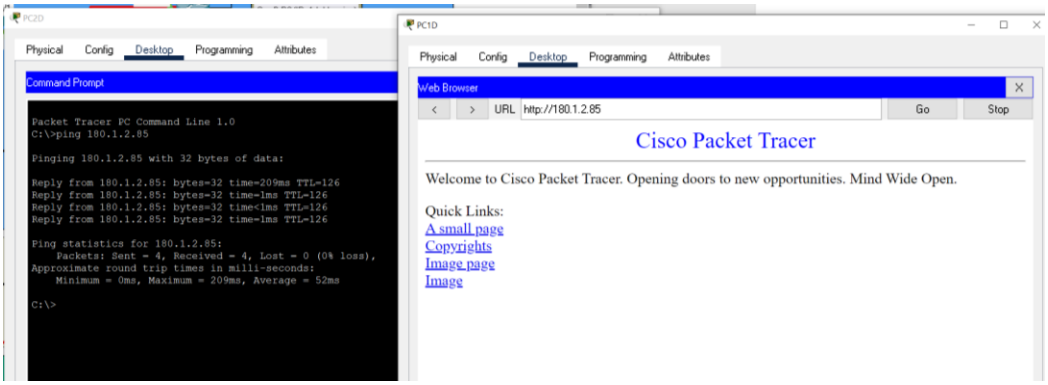


Figure 105: This screenshot displays that PC1D and PC2D on the Corporate D network can initiate traffic to the Internet and successfully get a response.

Figure 106: This screenshot displays that ISP-HTTP-SERVER on the Internet is unable to initiate traffic into the CorpD network. This displays that Internet traffic to Corporate D is denied and that the ACLs and security levels are operating correctly on CorpD-ASA.