Daniel MacCarthy

CMPT_420N_111

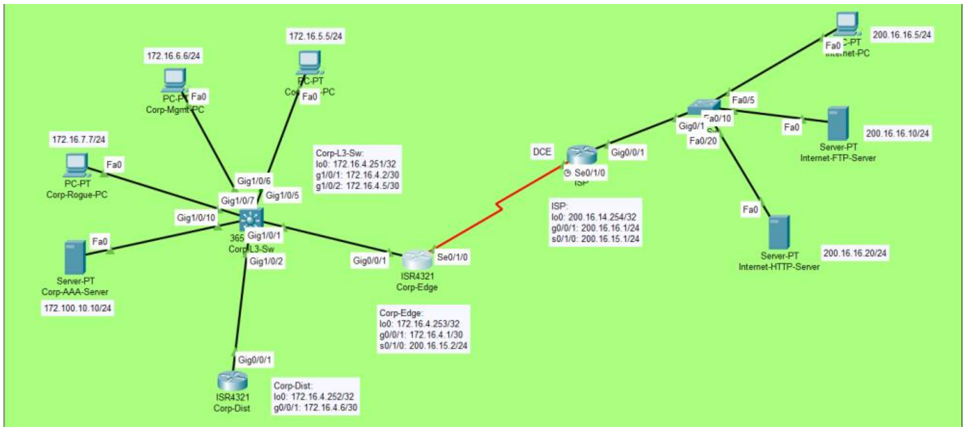
Prof. Cannistra

April 22, 2022

A) Description:

This lab included the use of InterVLAN routing, built on old topics such as ACLs and NAT/PAT, as well as including some new features like ZPF. This lab had almost the exact same topology as the last lab, with some parts not included. Working more with servers is interesting, as we had three different uses for the servers in this lab. The addition of having an internal rogue device was fun, as it shows how much access it could have if not for the security measures we had taken. Continuing to use OSPF with MD5 authentication is an amazing concept which builds on top of one of my favorite things to do in networking.

B) Topology:



Corp-L3-Sw:
lo0: 172.16.4.251/32
g1/0/1: 172.16.4.2/30
g1/0/2: 172.16.4.5/30

Corp-Edge:
lo0: 172.16.4.253/32
g0/0/1: 172.16.4.1/30
s0/1/0: 200.16.15.2/24

Corp-Dist:
lo0: 172.16.4.252/32
g0/0/1: 172.16.4.6/30

ISP:
lo0: 200.16.14.254/32
g0/0/1: 200.16.16.1/24
s0/1/0: 200.16.15.1/24

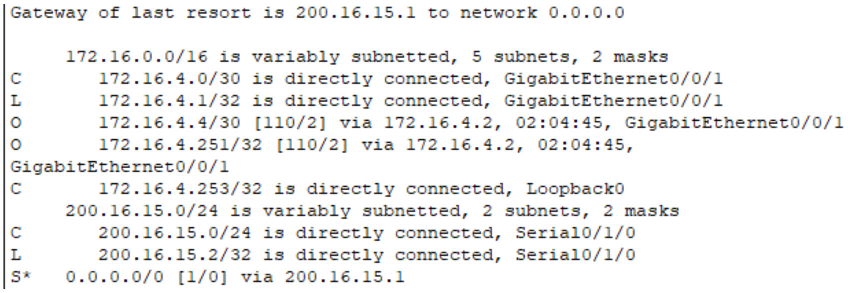
C) Key Syntax:

Command	Description	IOS Mode
hostname	Sets the name of the device	Global Configuration mode
login	Prompts the user to enter a password to gain access	Line Configuration mode
logging synchronous	Synchronizes the console line	Line Configuration modeP
int x/x	Accesses and interface	Global Configuration mode
ip config	Verifies the ip address and subnet mask of a host	CMD User mode

ping	Verify connectivity to another entity on the network through the IP address	CMD User mode
ip default-gateway	Sete the address to forward packets to on a switch	Global Configuration mode
ip route 0.0.0.0 0.0.0.0	Sets default static route to forward all packets across a connection	Global Configuration mode
ftp (ip address)	Set up an FTP connection	Command Prompt
router ospf (number)	Sets up ospf on a router	Global Configuration mode
ip nat pool	Creates a NAT pool of ip addresses	Global Configuration mode
ip access-list extended	Creates an extended access list	Global Configuration mode
Ip ospf message-digest-key (number) md5 (word)	Sets up OSPF to use an md5 key	Global Configuration mode
copy running-config startup-config	Copies the running configuration to the startup configuration	Privileged mode

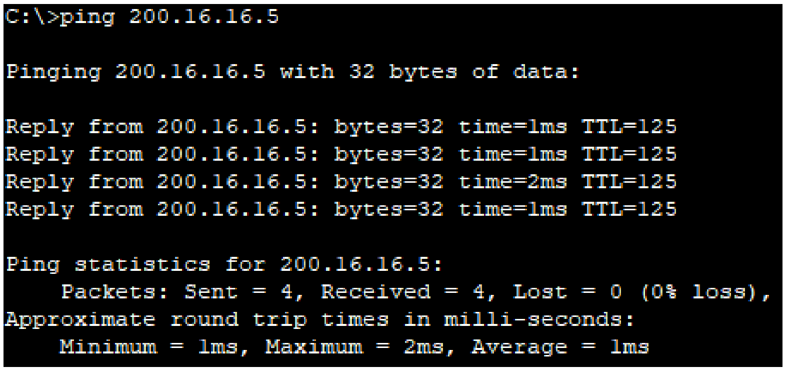
D) Verification:

Default static route and Single area ospf



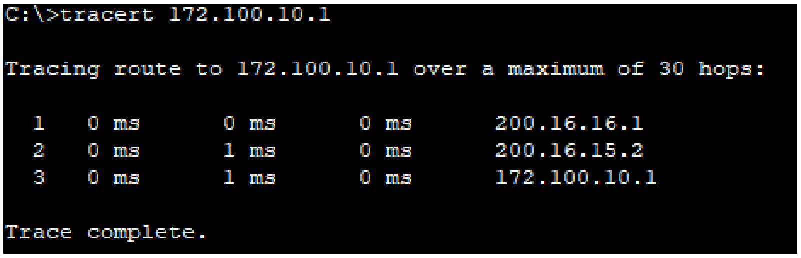
```
Gateway of last resort is 200.16.15.1 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.16.4.0/30 is directly connected, GigabitEthernet0/0/1
L       172.16.4.1/32 is directly connected, GigabitEthernet0/0/1
O       172.16.4.4/30 [110/2] via 172.16.4.2, 02:04:45, GigabitEthernet0/0/1
O       172.16.4.251/32 [110/2] via 172.16.4.2, 02:04:45,
GigabitEthernet0/0/1
C       172.16.4.253/32 is directly connected, Loopback0
     200.16.15.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.16.15.0/24 is directly connected, Serial0/1/0
L       200.16.15.2/32 is directly connected, Serial0/1/0
S*   0.0.0.0/0 [1/0] via 200.16.15.1
```

Corp-Mgmt PC pinging ISP PC



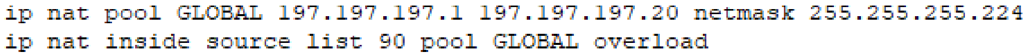
```
C:\>ping 200.16.16.5

Pinging 200.16.16.5 with 32 bytes of data:

Reply from 200.16.16.5: bytes=32 time=1ms TTL=125
Reply from 200.16.16.5: bytes=32 time=1ms TTL=125
Reply from 200.16.16.5: bytes=32 time=2ms TTL=125
Reply from 200.16.16.5: bytes=32 time=1ms TTL=125

Ping statistics for 200.16.16.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Internet-FTP-Server tracert Corp-AAA-Server



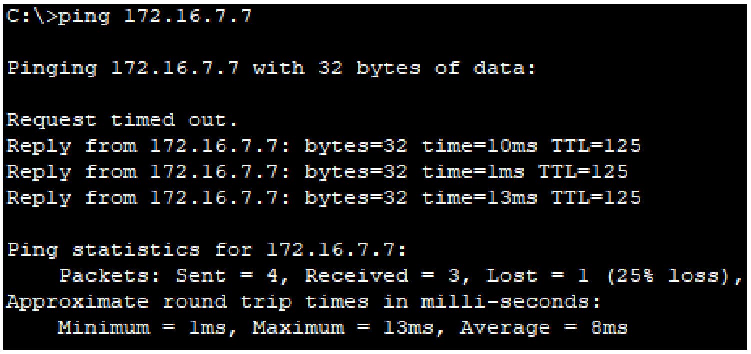
```
C:\>tracert 172.100.10.1

Tracing route to 172.100.10.1 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      200.16.16.1
  2   0 ms      1 ms      0 ms      200.16.15.2
  3   0 ms      1 ms      0 ms      172.100.10.1

Trace complete.
```

NAT and PAT



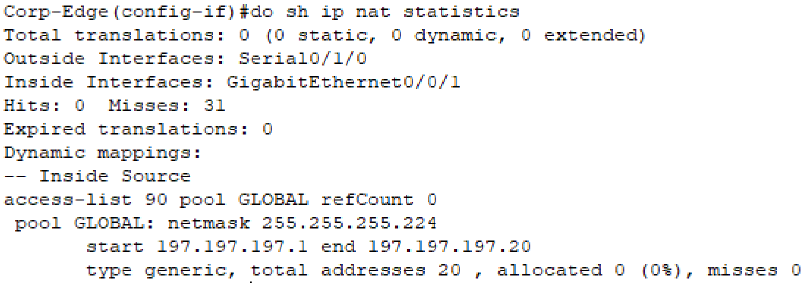
```
ip nat pool GLOBAL 197.197.197.1 197.197.197.20 netmask 255.255.255.224
ip nat inside source list 90 pool GLOBAL overload
```

Still have full connectivity after NAT and PAT



```
C:\>ping 172.16.7.7

Pinging 172.16.7.7 with 32 bytes of data:

Request timed out.
Reply from 172.16.7.7: bytes=32 time=10ms TTL=125
Reply from 172.16.7.7: bytes=32 time=1ms TTL=125
Reply from 172.16.7.7: bytes=32 time=13ms TTL=125

Ping statistics for 172.16.7.7:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 13ms, Average = 8ms
```

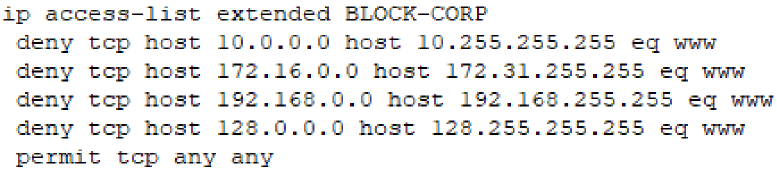
NAT statistics



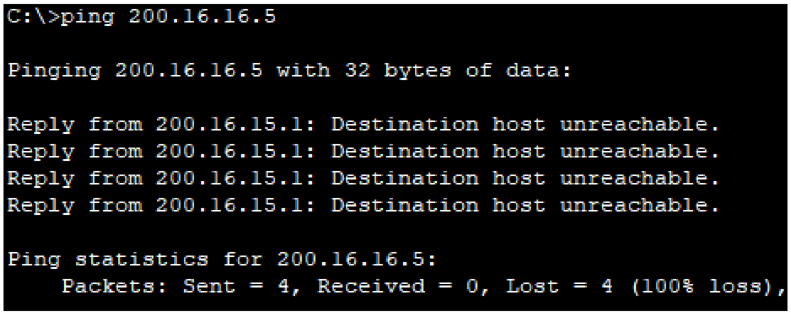
```
Corp-Edge(config-if)#do sh ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/1/0
Inside Interfaces: GigabitEthernet0/0/1
Hits: 0  Misses: 31
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 90 pool GLOBAL refCount 0
 pool GLOBAL: netmask 255.255.255.224
       start 197.197.197.1 end 197.197.197.20
       type generic, total addresses 20 , allocated 0 (0%), misses 0
```

After implementing the ACLs to block RFC1918 and 127.0.0.0/8

ISP ACL and proof of ping being denied

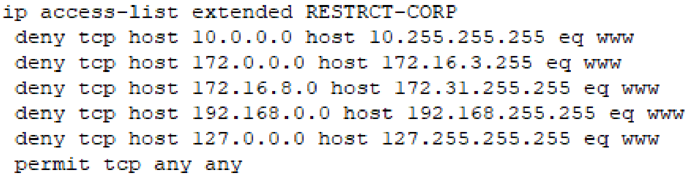


```
ip access-list extended BLOCK-CORP
 deny tcp host 10.0.0.0 host 10.255.255.255 eq www
 deny tcp host 172.16.0.0 host 172.31.255.255 eq www
 deny tcp host 192.168.0.0 host 192.168.255.255 eq www
 deny tcp host 128.0.0.0 host 128.255.255.255 eq www
 permit tcp any any
```

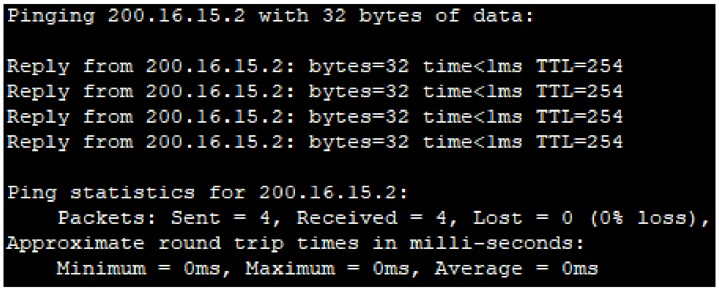


```
C:\>ping 200.16.16.5

Pinging 200.16.16.5 with 32 bytes of data:

Reply from 200.16.15.1: Destination host unreachable.
Reply from 200.16.15.1: Destination host unreachable.
Reply from 200.16.15.1: Destination host unreachable.
Reply from 200.16.15.1: Destination host unreachable.

Ping statistics for 200.16.16.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Corp-Edge ACL and proof of pings still working

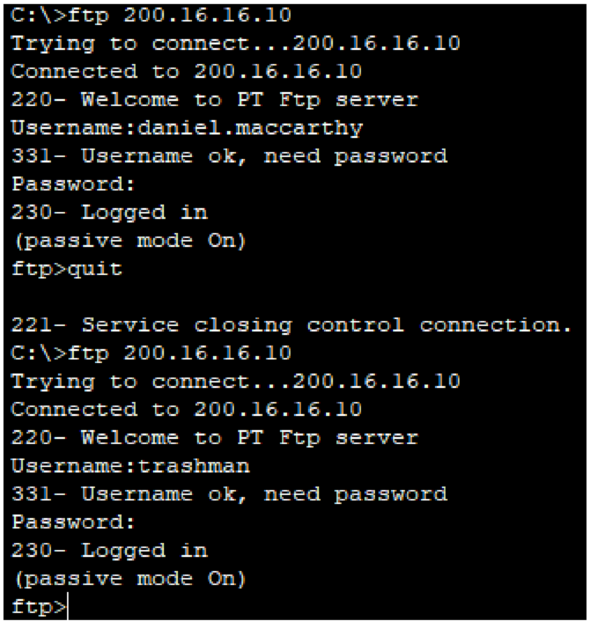


```
ip access-list extended RESTRCT-CORP
 deny tcp host 10.0.0.0 host 10.255.255.255 eq www
 deny tcp host 172.0.0.0 host 172.16.3.255 eq www
 deny tcp host 172.16.8.0 host 172.31.255.255 eq www
 deny tcp host 192.168.0.0 host 192.168.255.255 eq www
 deny tcp host 127.0.0.0 host 127.255.255.255 eq www
 permit tcp any any
```

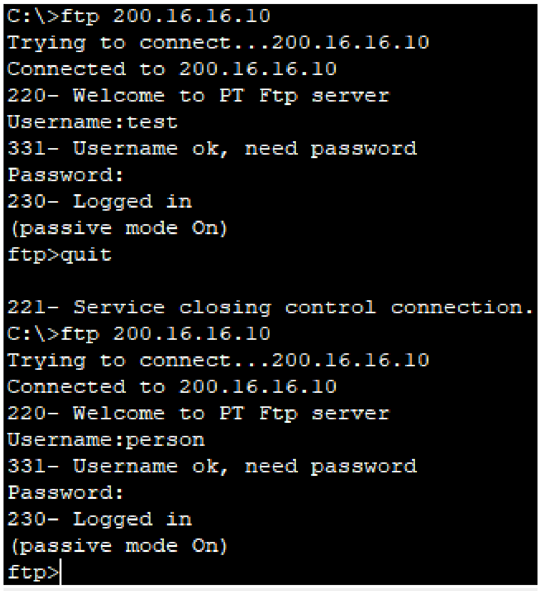


```
Pinging 200.16.15.2 with 32 bytes of data:

Reply from 200.16.15.2: bytes=32 time<1ms TTL=254
Reply from 200.16.15.2: bytes=32 time<1ms TTL=254
Reply from 200.16.15.2: bytes=32 time<1ms TTL=254
Reply from 200.16.15.2: bytes=32 time<1ms TTL=254

Ping statistics for 200.16.15.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Corp-Mgmt using FTP server

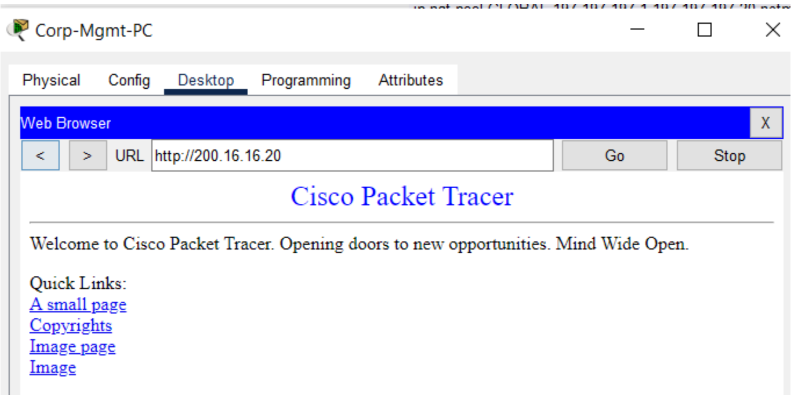


```
C:\>ftp 200.16.16.10
Trying to connect...200.16.16.10
Connected to 200.16.16.10
220- Welcome to PT Ftp server
Username:daniel.maccarthy
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>ftp 200.16.16.10
Trying to connect...200.16.16.10
Connected to 200.16.16.10
220- Welcome to PT Ftp server
Username:trashman
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```



```
C:\>ftp 200.16.16.10
Trying to connect...200.16.16.10
Connected to 200.16.16.10
220- Welcome to PT Ftp server
Username:test
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>ftp 200.16.16.10
Trying to connect...200.16.16.10
Connected to 200.16.16.10
220- Welcome to PT Ftp server
Username:person
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Corp-Mgmt and Corp-Rogue HTTP into HTTP server

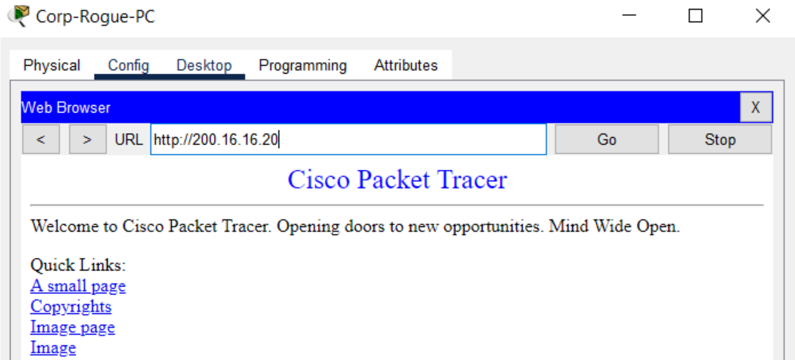


http://200.16.16.20

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image



http://200.16.16.20

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

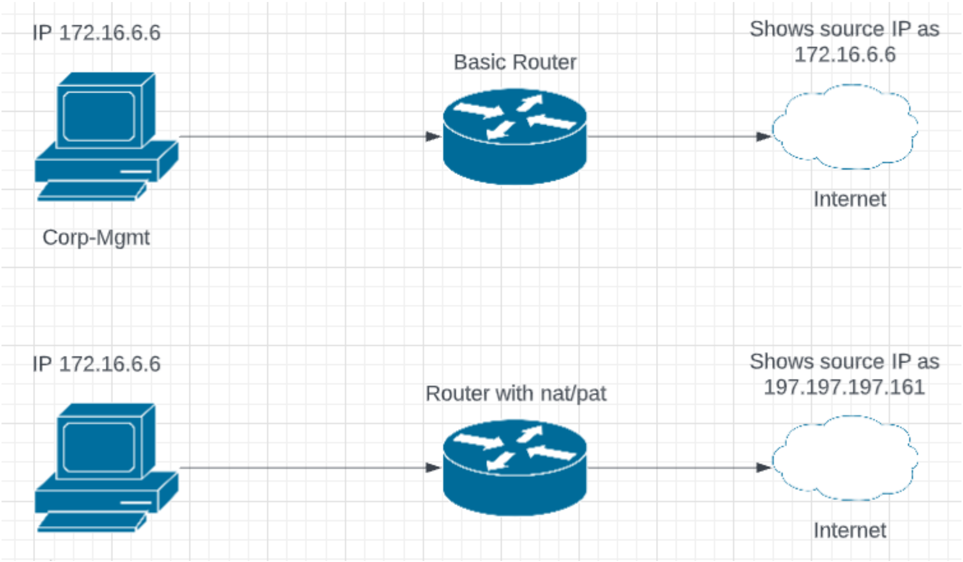
After implementing the ZPF

ZPF inspecting results

```
Corp-Edge#show policy-map type inspect zone-pair sessions

policy exists on zp INSIDE-TO-OUTSIDE
 Zone-pair: INSIDE-TO-OUTSIDE

  Service-policy inspect : HTTP-FTP

    Class-map: TRAFFIC (match-all)
      Match: access-group 101
      Inspect

        Number of Established Sessions = 3
        Established Sessions
         Session 2771957392 (172.16.5.5:1027)=>(200.16.16.10:21) tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:31, Last heard  00:00:29
          Bytes sent (initiator:responder) [308:247]
         Session 2771915232 (172.16.6.6:1033)=>(200.16.16.10:21) tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:54, Last heard  00:00:49
          Bytes sent (initiator:responder) [316:247]
         Session 2771898864 (172.16.7.7:1029)=>(200.16.16.10:21) tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:09, Last heard  00:00:02
          Bytes sent (initiator:responder) [324:247]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

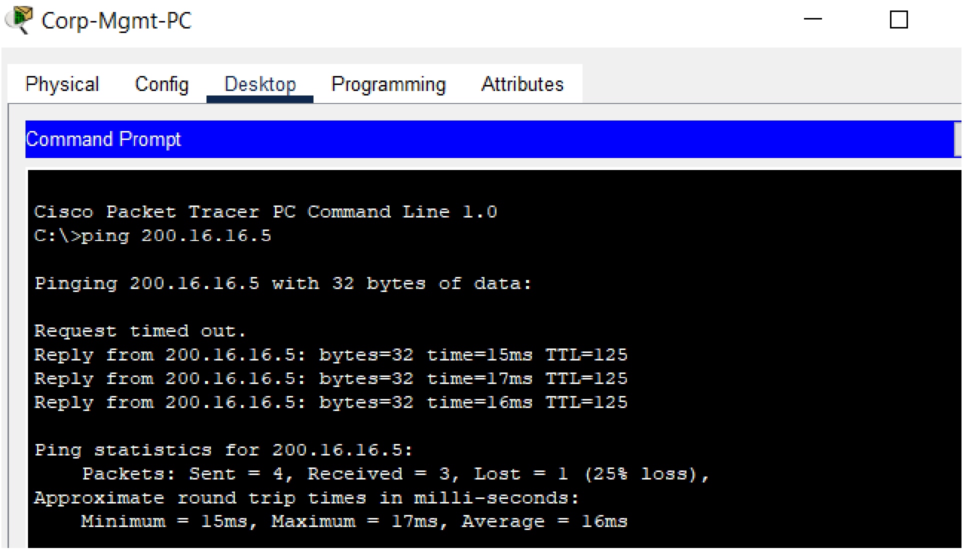
E) Test Cases

1) Implementation of NAT/PAT test case



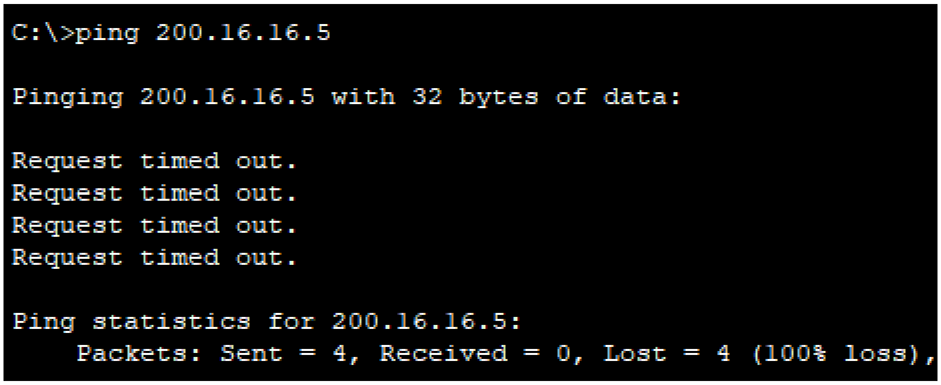
2) IP Spoofing test case

Corp-Mgmt before IP change

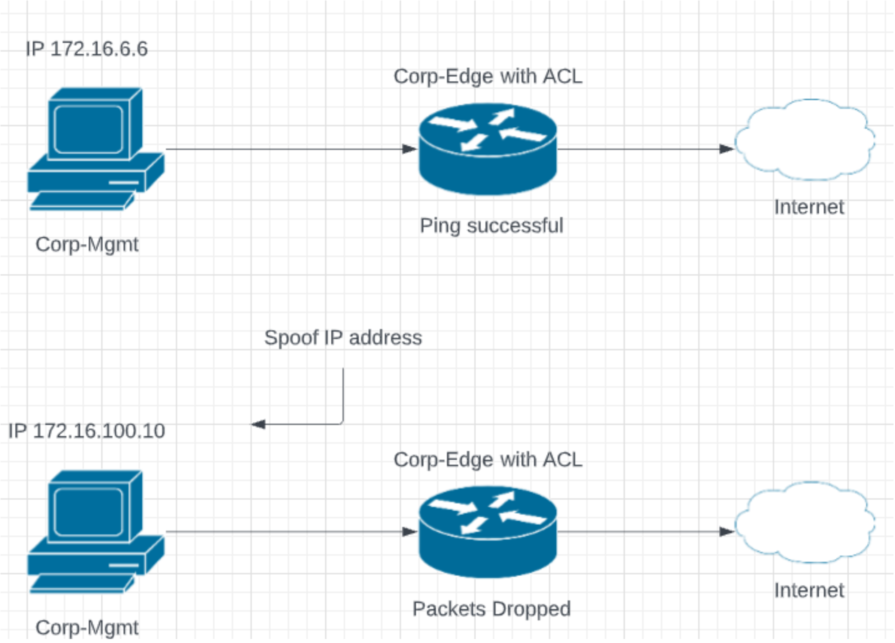


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.16.16.5

Pinging 200.16.16.5 with 32 bytes of data:

Request timed out.
Reply from 200.16.16.5: bytes=32 time=15ms TTL=125
Reply from 200.16.16.5: bytes=32 time=17ms TTL=125
Reply from 200.16.16.5: bytes=32 time=16ms TTL=125

Ping statistics for 200.16.16.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 17ms, Average = 16ms
```

Corp-Mgmt after IP address has been changed to 172.16.100.10

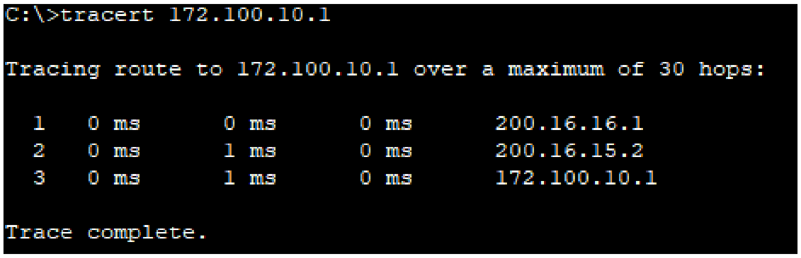


```
C:\>ping 200.16.16.5

Pinging 200.16.16.5 with 32 bytes of data:

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

Ping statistics for 200.16.16.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



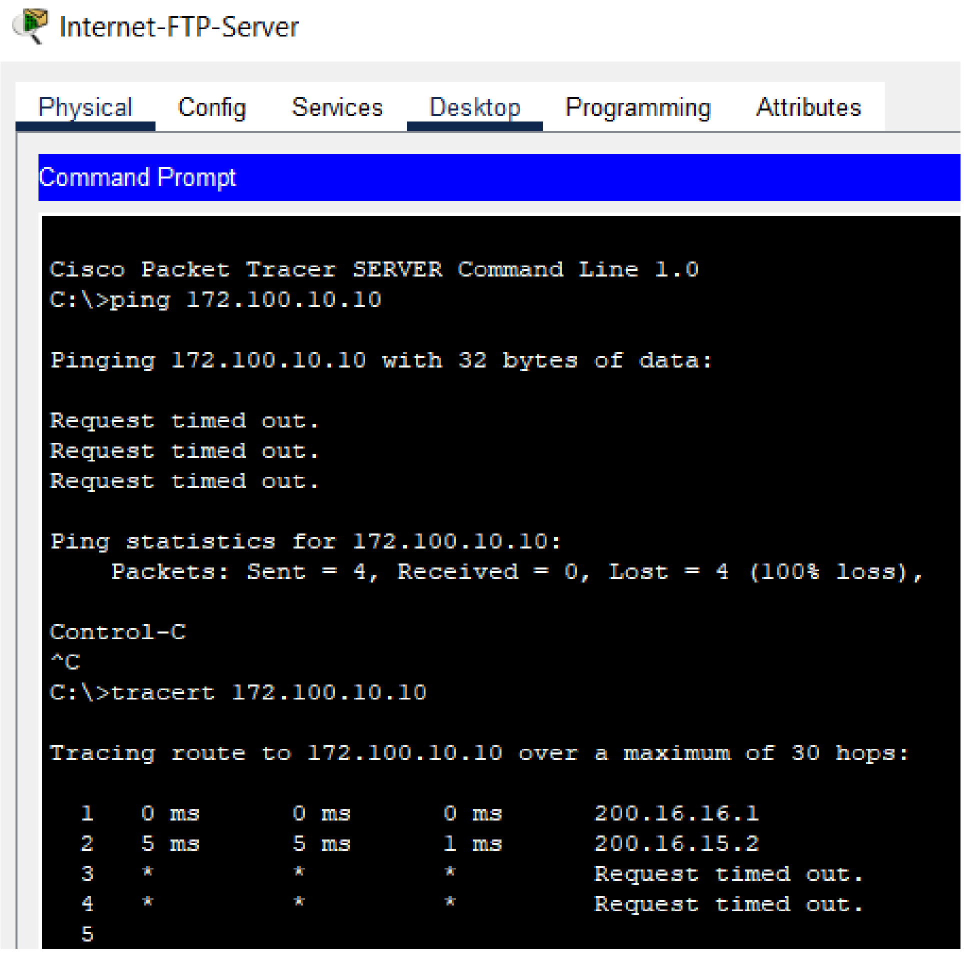
3) ZPF test case

Internet-FTP-Server tracert Corp-AAA-Server

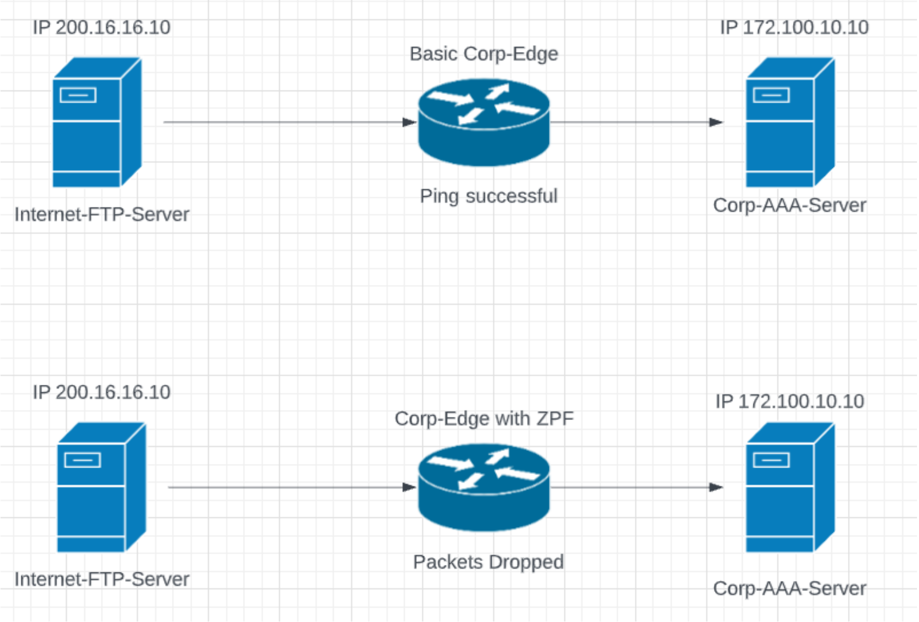


```
C:\>tracert 172.100.10.1

Tracing route to 172.100.10.1 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      200.16.16.1
  2   0 ms      1 ms      0 ms      200.16.15.2
  3   0 ms      1 ms      0 ms      172.100.10.1

Trace complete.
```

Internet-FTP-Server ping and tracert Corp-AAA-Server after ZPF

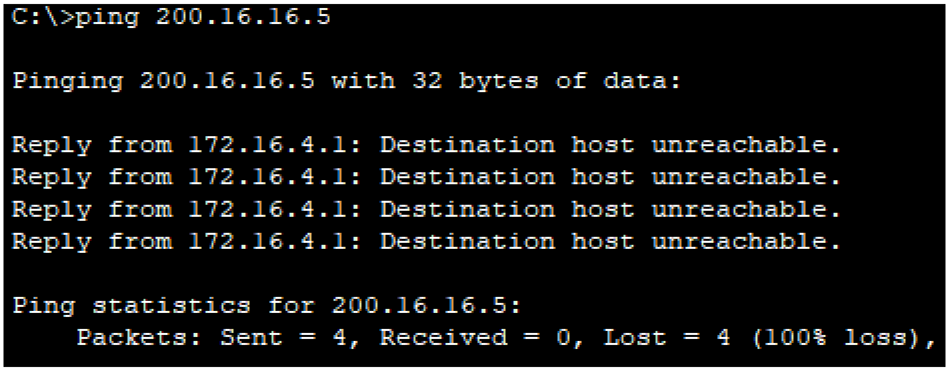


```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 172.100.10.10

Pinging 172.100.10.10 with 32 bytes of data:

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

Ping statistics for 172.100.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Control-C
^C
C:\>tracert 172.100.10.10

Tracing route to 172.100.10.10 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      200.16.16.1
  2   5 ms      5 ms      1 ms      200.16.15.2
  3   *         *         *         Request timed out.
  4   *         *         *         Request timed out.
  5
```



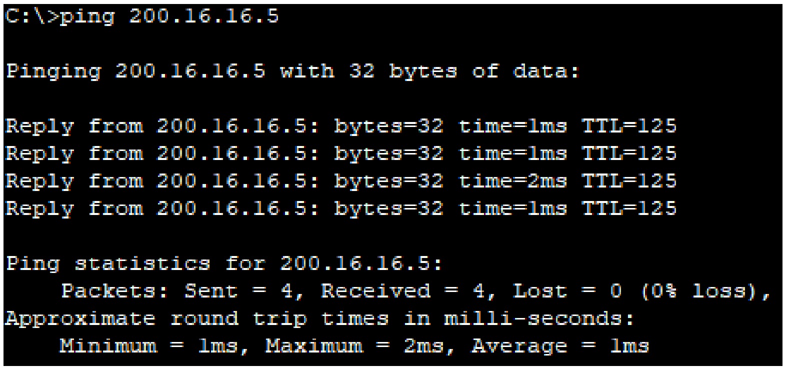
4) Default Static Route test case

Before DSR was configured

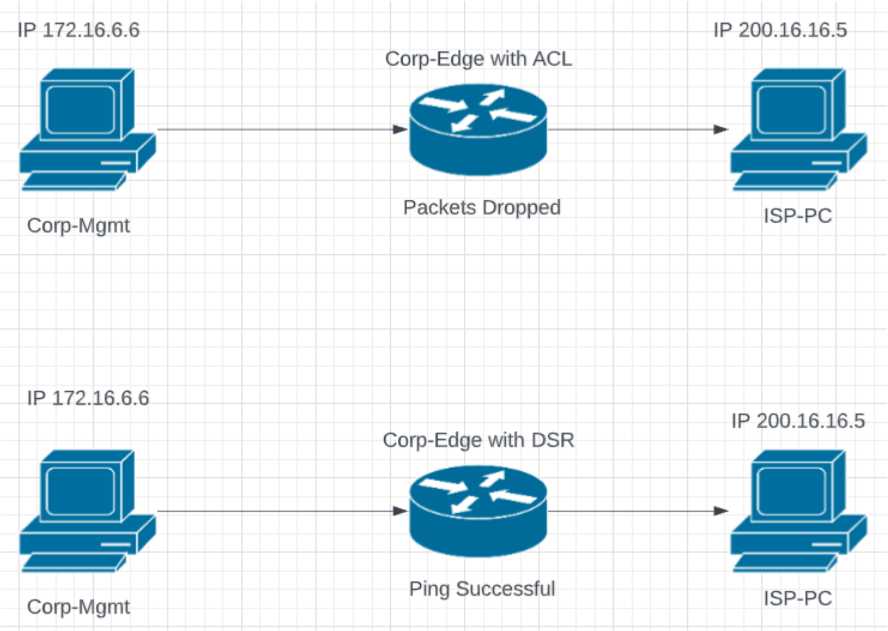


```
C:\>ping 200.16.16.5

Pinging 200.16.16.5 with 32 bytes of data:

Reply from 172.16.4.1: Destination host unreachable.
Reply from 172.16.4.1: Destination host unreachable.
Reply from 172.16.4.1: Destination host unreachable.
Reply from 172.16.4.1: Destination host unreachable.

Ping statistics for 200.16.16.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

After DSR has been configured



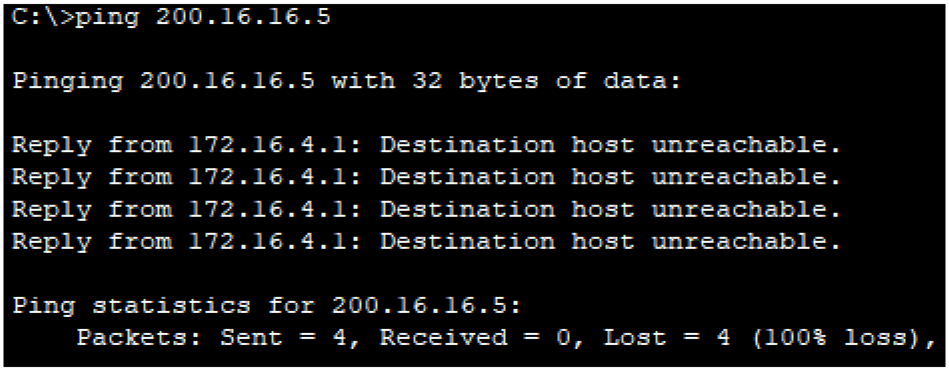
```
C:\>ping 200.16.16.5

Pinging 200.16.16.5 with 32 bytes of data:

Reply from 200.16.16.5: bytes=32 time=1ms TTL=125
Reply from 200.16.16.5: bytes=32 time=1ms TTL=125
Reply from 200.16.16.5: bytes=32 time=2ms TTL=125
Reply from 200.16.16.5: bytes=32 time=1ms TTL=125

Ping statistics for 200.16.16.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```



5) OSPF with md5 Authentication test case

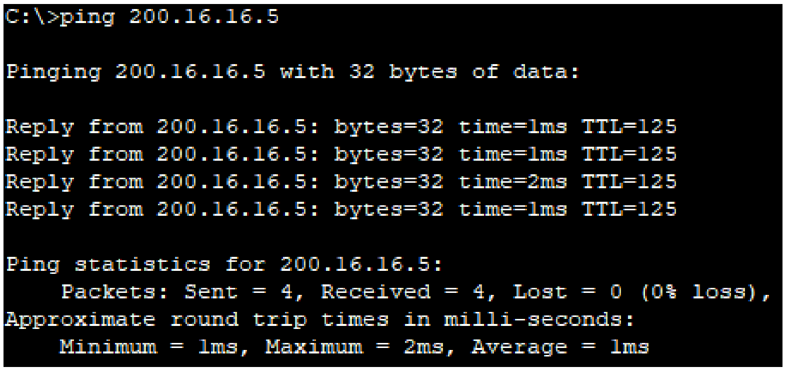
Without the md5 authentication on the specific ports, the routing tables will not be allowed to update via OSPF

Corp-Mgmt before md5 authentication was configured

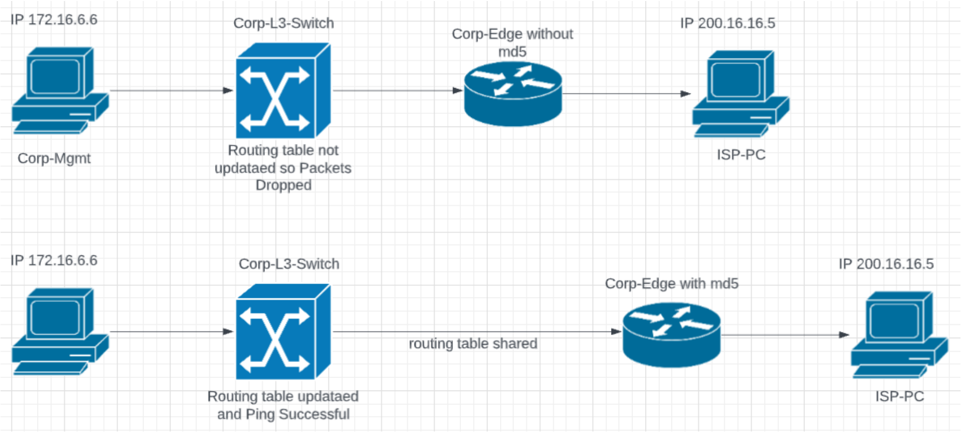


```
C:\>ping 200.16.16.5

Pinging 200.16.16.5 with 32 bytes of data:

Reply from 172.16.4.1: Destination host unreachable.
Reply from 172.16.4.1: Destination host unreachable.
Reply from 172.16.4.1: Destination host unreachable.
Reply from 172.16.4.1: Destination host unreachable.

Ping statistics for 200.16.16.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Corp-Mgmt after md5 authentication has been configured



```
C:\>ping 200.16.16.5

Pinging 200.16.16.5 with 32 bytes of data:

Reply from 200.16.16.5: bytes=32 time=1ms TTL=125
Reply from 200.16.16.5: bytes=32 time=1ms TTL=125
Reply from 200.16.16.5: bytes=32 time=2ms TTL=125
Reply from 200.16.16.5: bytes=32 time=1ms TTL=125

Ping statistics for 200.16.16.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```



F) Conclusion:

The lab went exactly as planned with everything we implemented working as expected. Simple things like OSPF all the way to the more complex like ZPF were implemented without any problems. I was a little confused about the test cases and making the diagrams, but I tried to include plenty of screenshots before and after the technologies were implemented in this lab report. I am hoping that helps to see how everything worked.

G) Things Googled/Sites used:

How to configure FTP server:

https://computernetworking747640215.wordpress.com/2019/11/22/how-to-configure-an-ftp-server-in-packet-tracer/

How to configure a ZPF packet tracer:

https://itexamanswers.net/4-4-1-1-packet-tracer-configuring-zone-based-policy-firewall-zpf-answers.html

What is RFC1918 addressing:

https://netbeez.net/blog/rfc1918/