

Daniel MacCarthy

CMPT_420N_111

Prof. Cannistra

March 10, 2022

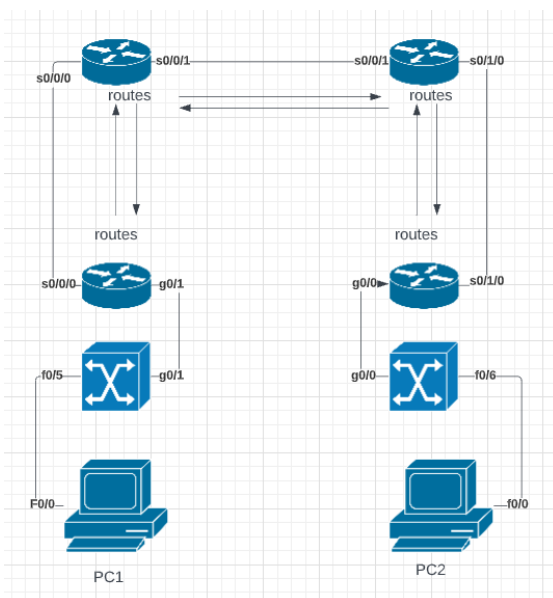
A) Description:

This lab included a few different tasks. In part one we were able to make a topology out of descriptions of where certain routers and switches went. For part two we looked at and identified OSPF and SSH more in-depth. Part three included building a network from scratch with 4 routers, three internal, one external, and a network of a switch and at least one host attached to each. We implemented OSPF with MD5 authentication and did not have full connectivity to every host across the network. Later while setting up NTP and SYSLOG on the internal server, we attempted to bring everything together

B) Task One:

OSPF:

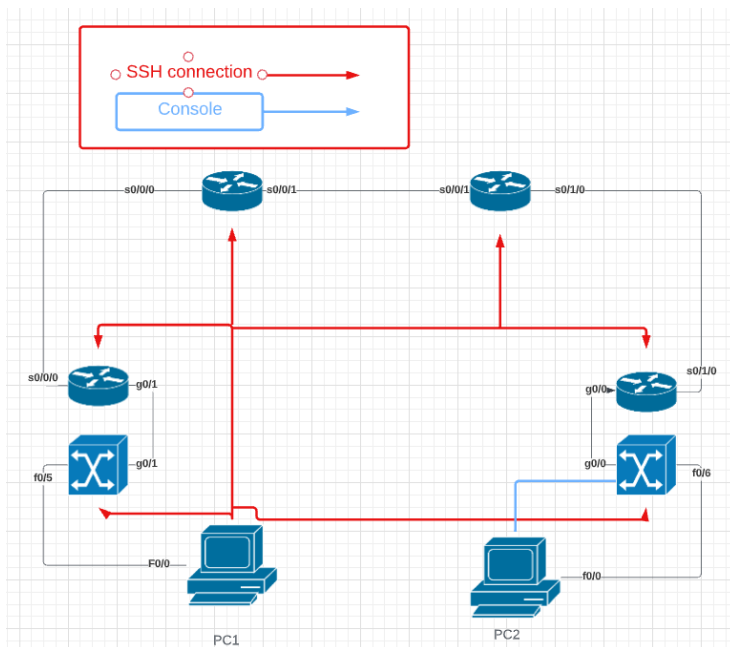
OSPF is an internal, linked state protocol used for sharing routes to neighboring routers to update routing tables. OSPF works by taking its directly connected routes and sending them to adjacent routers, who take the information, update their tables, and forward it to its adjacent routers. The purpose is for a router to know where to forward a certain packet, even if it is not directly connected to the destination. Due to it being a linked state protocol it can choose to send only updates from its routing table out to neighboring routers instead of its entire routing table, which saves time.



Here, PC1 is trying to send data to PC2, however, its default gateway has no clue how to get to PC2. When you implement OSPF the routers will share their connections, allowing the routers to know exactly where to forward the packets so that they can reach their destination host. The types of authentications for this are null authentication, simple password authentication, and cryptographic authentication.

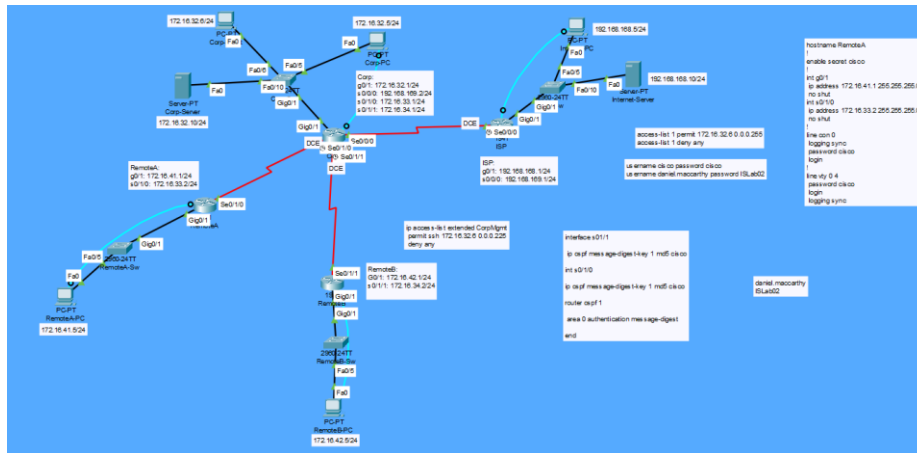
SSH:

SSH, which stands for Secure Shell, is a form of a virtual terminal, like telnet only more secure due to it being encrypted. A virtual terminal allows us to control our switches and routers without being physically consoled in, which is extremely beneficial when working with large networks. SSH is used on port 22, which means disabling that will disable the ability to establish an SSH connection.



Here, we can use SSH from the command prompt of PC1 to control any network device on our network. The red arrows symbolize the possible connections we can make. Here, PC2 cannot use SSH, and therefore can only control the switch that they are physically consoled into. If they want to control a different device, they will have to establish the same kind of physical connection to that device. The types of authentications for SSH are Public Key Authentication, Password Authentication, Host-Based Authentication, Keyboard Authentication, and Authentication of Servers.

D) Topology:



E) 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 |
| SSH -l (username)(ip address) | Set up an SSH connection | Command Prompt |
| ntp authenticate | Uses the key to authenticate the device | Global Configuration mode |
| ntp authentication-key (number)(word) | Uses the key to identify the trusted device | Global Configuration mode |
| logging (ip address) | Logs to an ip address | Global Configuration mode |
| Ip ospf message-digest-key (number) md5 (word) | Sets up OSPF to use an md5 key | Global Configuration mode |

F) Verification:

Corp

```
Corp(config)#int g0/1
Corp(config-if)# ip address 172.16.32.1 255.255.255.0
Corp(config-if)# no shut

Corp(config-if)#int s0/0/0
Corp(config-if)# ip address 192.168.169.2 255.255.255.0
Corp(config-if)# no shut

Corp(config-if)#int s0/1/0
Corp(config-if)# ip address 172.16.33.1 255.255.255.0
Corp(config-if)# no shut

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Corp(config-if)# clock rate 2000000
Corp(config-if)#int s0/1/1
Corp(config-if)# ip address 172.16.34.1 255.255.255.0
Corp(config-if)# no shut

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
Corp(config-if)# clock rate 2000000
Corp(config-if)#!
Corp(config-if)#line con 0
Corp(config-line)# logging sync
Corp(config-line)# password cisco
Corp(config-line)# login
Corp(config-line)#!
Corp(config-line)#line vty 0 4
Corp(config-line)# password cisco
Corp(config-line)# login
Corp(config-line)# logging sync
```

RemoteB-PC pinging default gateway

```
C:\>ping 172.16.42.1

Pinging 172.16.42.1 with 32 bytes of data:

Reply from 172.16.42.1: bytes=32 time<1ms TTL=255
Reply from 172.16.42.1: bytes=32 time<1ms TTL=255
Reply from 172.16.42.1: bytes=32 time<1ms TTL=255
Reply from 172.16.42.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.42.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Copr-PC pinging default gateway

```
C:\>ping 172.16.32.1

Pinging 172.16.32.1 with 32 bytes of data:

Reply from 172.16.32.1: bytes=32 time<1ms TTL=255
Reply from 172.16.32.1: bytes=32 time<1ms TTL=255
Reply from 172.16.32.1: bytes=32 time<1ms TTL=255
Reply from 172.16.32.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.32.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Corp pinging other DCE connections

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.169.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/25 ms

Corp#ping 172.16.42.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.42.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Corp#ping 172.16.34.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.34.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

Corp#ping 172.16.41.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.41.1, timeout is 2 seconds:
..
Success rate is 0 percent (0/3)

Corp#ping 172.16.33.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.33.2, timeout is 2 seconds:
```

ISP routing table

```
Gateway of last resort is not set

    192.168.168.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.168.0/24 is directly connected, GigabitEthernet0/1
L       192.168.168.1/32 is directly connected, GigabitEthernet0/1
    192.168.169.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.169.0/24 is directly connected, Serial0/0/0
L       192.168.169.1/32 is directly connected, Serial0/0/0
```

Corp routing table

```
Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C       172.16.32.0/24 is directly connected, GigabitEthernet0/1
L       172.16.32.1/32 is directly connected, GigabitEthernet0/1
C       172.16.33.0/24 is directly connected, Serial0/1/0
L       172.16.33.1/32 is directly connected, Serial0/1/0
C       172.16.34.0/24 is directly connected, Serial0/1/1
L       172.16.34.1/32 is directly connected, Serial0/1/1
    192.168.169.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.169.0/24 is directly connected, Serial0/0/0
L       192.168.169.2/32 is directly connected, Serial0/0/0
```

RemoteA routing table

```
Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.33.0/24 is directly connected, Serial0/1/0
L       172.16.33.2/32 is directly connected, Serial0/1/0
C       172.16.41.0/24 is directly connected, GigabitEthernet0/1
L       172.16.41.1/32 is directly connected, GigabitEthernet0/1
```

RemoteB routing table

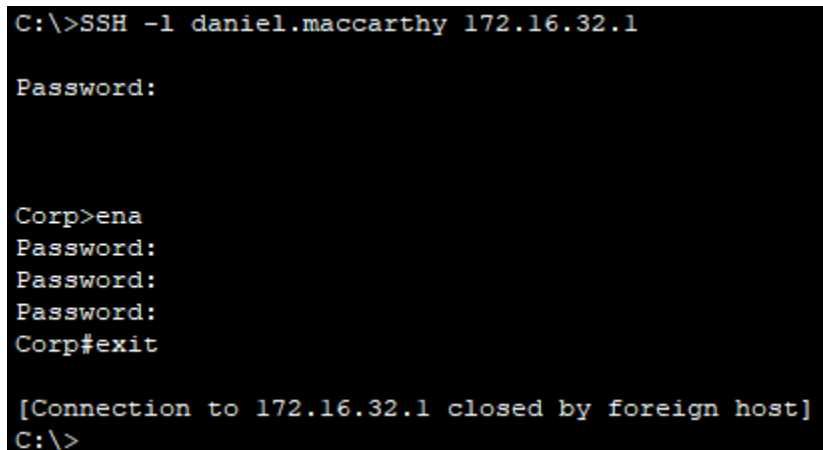
```
Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.34.0/24 is directly connected, Serial0/1/1
L       172.16.34.2/32 is directly connected, Serial0/1/1
C       172.16.42.0/24 is directly connected, GigabitEthernet0/1
L       172.16.42.1/32 is directly connected, GigabitEthernet0/1
```

There is no difference between the routing tables after configuring OSPF with Md5 authentication.

No, I am unable to ping the different PCs across the topology. However, I do not think that I should be able to because there is no key.

Corp-mgmt ssh to Corp after ACL



```
C:\>SSH -l daniel.maccarthy 172.16.32.1

Password:

Corp>ena
Password:
Password:
Password:
Corp#exit

[Connection to 172.16.32.1 closed by foreign host]
C:\>
```

G) Conclusion:

The lab went mostly as planned until the end. Every part of the lab was done properly, except for setting up the server. NTP was properly in use on Corp Router, however, it would not work across the DCE connections, even when I tried to use the md5 key. I tried re-creating the keys, changing the number on the server, reading through random commands using “?” and nothing seemed to work. I set up SYSLOG the exact way I thought was right and no matter what the table would not populate. I tried taking off the ACL, turning every service on the server off and on, and like NTP looked it up on the internet. I watched many videos on YouTube and read different websites and I was doing exactly what it said. Finally, I tried taking off the “deny any” from the ACL to see if that changed anything, which it did not.

H) References:

[How to configure ntp server cisco router](#)

[How to Configure Syslog Server in Cisco Packet Tracer | Technical Hakim
#SyslogConfiguration CCNA](#)

https://techhub.hpe.com/eginfolib/networking/docs/switches/3100-48/5998-7645r_nmm_cg/content/442451578.htm

<https://itexamanswers.net/6-3-7-packet-tracer-configure-ospf-authentication-answers.html>

<https://www.nsoftware.com/kb/articles/legacy/sbb/ssh-authentication-methods.rst>

<https://www.oreilly.com/library/view/cisco-ios-cookbook/0596527225/ch08s10.html#:~:text=RFC%202328%2C%20which%20defines%20OSPF,and%20cryptographic%20authentication.%20...>