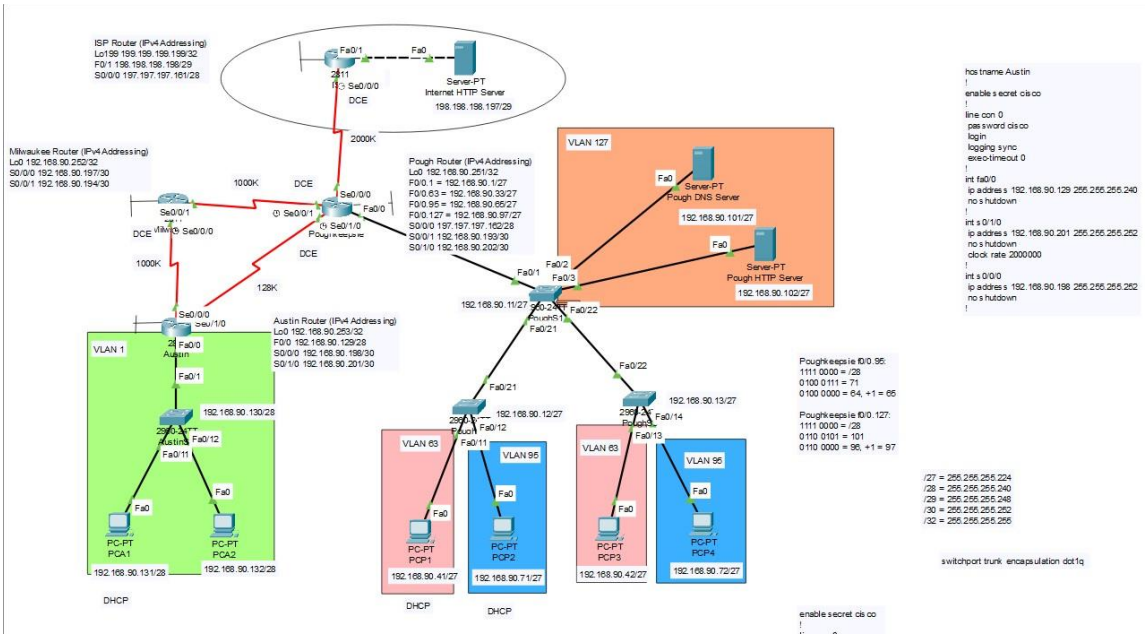
Dan MacCarthy

CMPT 420N_111

a) Description:

This lab included many topics such as DHCP, NAT/PAT, OSPF, STP, different VLANS, InterVlan routing, and many more. We worked with 4 routers, 3 as part of a WAN and one as the ISP connected to the edge router. We also used DHCP on a DNS server in a local area network to assign certain IP addresses as well as over a WAN connection.

b) Topology:



c) Syntax:

Command	Description	IOS Mode
hostname	Sets the name of the device	Global Configuration mode
enable	Enables privilege mode	User Mode
configure terminal	Enters Global Configuration mode	Privilege Mode
enable secret cisco	Encrypts the password used to access privilege mode	Global Configuration mode
password	Sets the password to get into terminal configuration mode	Line Configuration mode
login	Prompts the user to enter a password to gain access	Line Configuration mode

logging synchronous	Synchronizes the console line	Line Configuration mode
int x/x	Accesses and interface	Global Configuration mode
switchport trunk encapsulation dot1q	Puts IEEE encapsulation on a sub interface	Interface Configuration mode
show ip in brief	Shows a summary of the device's interfaces.	Privilege 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
show vlan	Displays all vlans associated with the switch	Privilege mode
show int trunk	Displays all ports designated as trunks on the switch	Privilege mode
switchport mode access	Sets the port as an access port	Global Configuration mode
switchport mode trunk	Sets the port as a trunk port	Global Configuration mode
switchport access vlan	Assigns a port to a vlan	Global Configuration mode
ip helper-address	Sete the address to forward DHCP requests to	Interface Configuration mode
ip dhcp pool	Creates a new dhcp pool	Global Configuration mode
ip excluded-address	Excludes certain ip addresses from being lent out by DHCP	Global Configuration mode

d) Verification:

Vlans

```
                                                 Gig0/2
63   RED                               active
95   BLUE                              active
127  ORANGE                            active    Fa0/2, Fa0/3
```

IEEE Trunking

```
interface FastEthernet0/21
 switchport mode trunk
!
interface FastEthernet0/22
 switchport mode trunk
```

STP

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000A.418A.B491
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000A.418A.B491
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/21           Desg FWD 19        128.21   P2p
Fa0/22           Desg FWD 19        128.22   P2p
```

IP address and Subnetting

Poughkeepsie f0/0.95:
1111 0000 = /28
0100 0111 = 71
0100 0000 = 64, +1 = 65

Poughkeepsie f0/0.127:
1111 0000 = /28
0110 0101 = 101
0110 0000 = 96, +1 = 97

Clock Rates

```
interface Serial0/0/1
 bandwidth 1000
 ip address 192.168.90.193 255.255.255.252
 ip nat inside
 clock rate 1000000
!
interface Serial0/1/0
 bandwidth 128
 ip address 192.168.90.202 255.255.255.252
 ip nat inside
 clock rate 128000
```

InterVLAN routing

```
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 192.168.90.1 255.255.255.224
 ip nat inside
!
interface FastEthernet0/0.63
 encapsulation dot1Q 63
 ip address 192.168.90.33 255.255.255.224
 ip nat inside
!
interface FastEthernet0/0.95
 encapsulation dot1Q 95
 ip address 192.168.90.65 255.255.255.224
 ip nat inside
!
interface FastEthernet0/0.127
 encapsulation dot1Q 127
 ip address 192.168.90.97 255.255.255.224
 ip nat inside
```

Default Static Routing

```
     192.168.90.0/24 is variably subnetted, 16 subnets, 3 masks
C       192.168.90.0/27 is directly connected, FastEthernet0/0.1
S       192.168.90.0/30 [1/0] via 192.168.90.201
                        [1/0] via 192.168.90.194
L       192.168.90.1/32 is directly connected, FastEthernet0/0.1
```

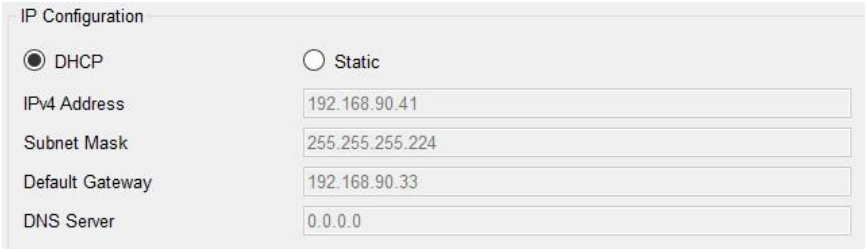
OSPF

```
L       192.168.90.202/32 is directly connected, Serial0/1/0
O       192.168.90.252/32 [110/101] via 192.168.90.194, 00:39:40, Serial0/0/1
O       192.168.90.253/32 [110/201] via 192.168.90.194, 00:39:40, Serial0/0/1
     197.197.197.0/24 is variably subnetted, 2 subnets, 2 masks
```

Default route injection

```
O*E2 0.0.0.0/0 [110/1] via 192.168.90.197, 00:20:41, Serial0/0/0
```

DHCP



NAT/PAT

```
ip nat pool PUBLIC-POUGH-POOL 197.197.197.163 197.197.197.165 netmask
255.255.255.240
ip nat inside source list 90 pool PUBLIC-POUGH-POOL overload
```

VTP

```
Feature VLAN :
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 8
Configuration Revision            : 12
MD5 digest                        : 0x22 0xC8 0x06 0x14 0xCD 0xBF 0xFB 0xD9
                                    0xF9 0x17 0xA9 0x21 0x8C 0x89 0x88 0x84
```

TASK THREE

A) We would use Access Control Lists on the edge router (Poughkeepsie) to ensure that IP addresses that are not part of our network would not be able to access our network.

B) We could use the commands “enable secret cisco” to set an encrypted password and then set up “password cisco” and “login” to secure our devices further. Which I did out of habit on half of these, I am very sorry for the inconvenience : (.

C) The firewall would go between the edge router and the ISP. This would further protect our network against any outside attackers.

D) The security is not very effective. Our most important router is also the edge router, and while I am not sure if that is necessarily bad it would be the first device accessed by an outside attacker. There are no ACLs, no firewall, and some passwords on devices, making our network very vulnerable.

e) Conclusion:

The lab went as planned, all hosts and switches were connected and able to ping each other. the network is set up, to assign ip addresses automatically via DHCP and have full DNS resolution.