Daniel MacCarthy

CMPT_420N_111

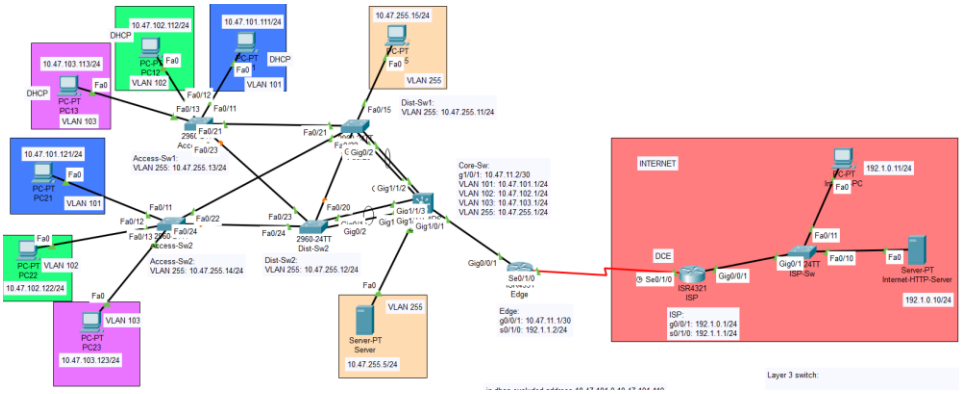
Prof. Cannistra

May 5, 2022

A) Description:

This lab included the use of multiple VLANs, as well as the switching of the administrative VLAN from the usual Vlan1 to Vlan255. This felt like a very realistic topology with the inclusion of DHCP as well as Access Switches and Distribution Switches. Using port-security and making the mac address sticky was an extremely cool concept to implement to ensure that only the one desired device can have access. Overall, this was a very fun and interesting lab.

B) Topology:



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
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
copy running-config startup-config	Copies the running configuration to the startup configuration	Privileged mode
spanning-tree portfast bpduguard default	Enables BPDU guard on spanning-tree ports	Global Configuration Mode
spanning-tree guard root	Enables Guard Root	Global Configuration Mode
switchport trunk native vlan 255	Sets the native vlan	Interface Configuration Mode
banner motd	Sets a Banner message	Global Configuration Mode
ip dhcp pool	Creates a DHCP pool	Global Configuration Mode
switchport port-security maximum 1	Sets the maximum number of Mac addresses a port can take	Global Configuration Mode
switchport port-security mac-address sticky	Makes the port learn the first MAC address it sees and stick with that	Global Configuration Mode

D) Verification:

vlans

```
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15,
Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19,
Fa0/20
                                                Fa0/22, Fa0/24, Gig0/1,
Gig0/2
101  Blue                             active
102  Green                            active
103  Purple                           active
255  Admin                            active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

making vlan 255 the admin vlan

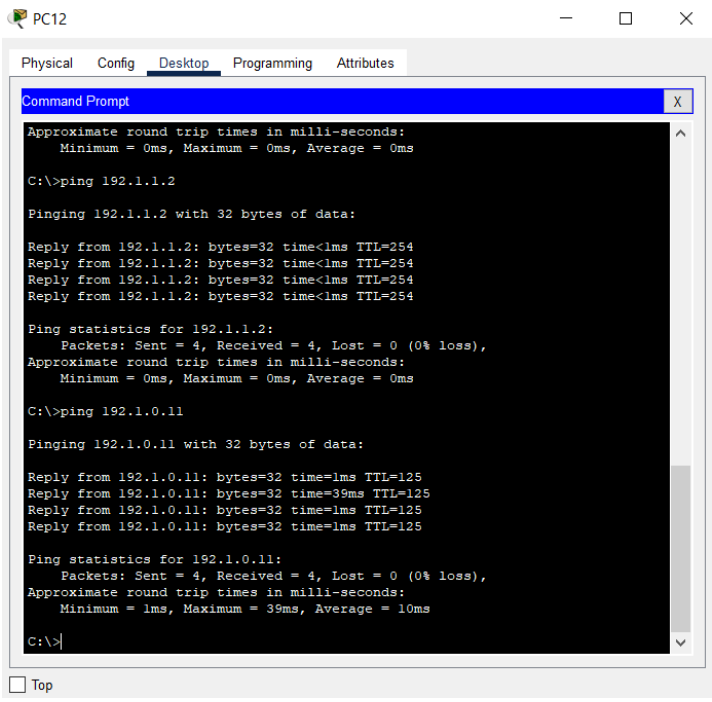
```
Switch(config)#hostname Access-Sw1
Access-Sw1(config)#!
Access-Sw1(config)#int vlan 1
Access-Sw1(config-if)# no ip add
Access-Sw1(config-if)# shut
Access-Sw1(config-if)#!
Access-Sw1(config-if)#vtp mode client
Setting device to VTP CLIENT mode.
Access-Sw1(config)#vtp domain INETSEC
Changing VTP domain name from NULL to INETSEC
Access-Sw1(config)#vtp password cisco
Setting device VLAN database password to cisco
Access-Sw1(config)#!
Access-Sw1(config)#int vlan255
Access-Sw1(config-if)# ip add 10.47.255.13 255.255.255.0
Access-Sw1(config-if)# no shut
Access-Sw1(config-if)#!
Access-Sw1(config-if)#int f0/21
Access-Sw1(config-if)# switchport mode trunk

Access-Sw1(config-if)# switchport trunk native vlan 255
Access-Sw1(config-if)# switchport nonegotiate
Access-Sw1(config-if)#int f0/23
Access-Sw1(config-if)# switchport mode trunk

Access-Sw1(config-if)# switchport trunk native vlan 255
Access-Sw1(config-if)# switchport nonegotiate
```

Edge routing table

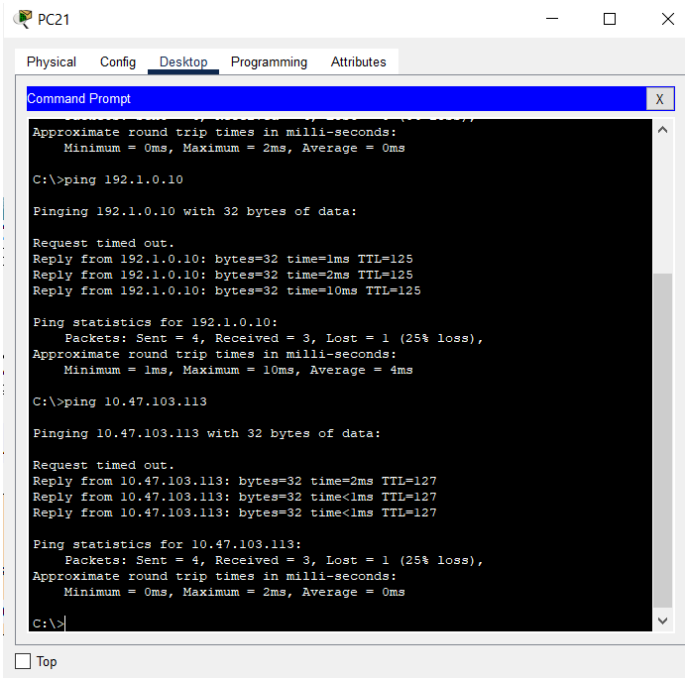
```
Gateway of last resort is 192.1.1.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
C       10.47.11.0/30 is directly connected, GigabitEthernet0/0/1
L       10.47.11.1/32 is directly connected, GigabitEthernet0/0/1
O       10.47.101.0/24 [110/2] via 10.47.11.2, 00:23:41, GigabitEthernet0/0/1
O       10.47.102.0/24 [110/2] via 10.47.11.2, 00:23:41, GigabitEthernet0/0/1
O       10.47.103.0/24 [110/2] via 10.47.11.2, 00:23:41, GigabitEthernet0/0/1
O       10.47.255.0/24 [110/2] via 10.47.11.2, 00:23:41, GigabitEthernet0/0/1
     192.1.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.1.0/24 is directly connected, Serial0/1/0
L       192.1.1.2/32 is directly connected, Serial0/1/0
S*   0.0.0.0/0 [1/0] via 192.1.1.1
```

Testing connectivity:

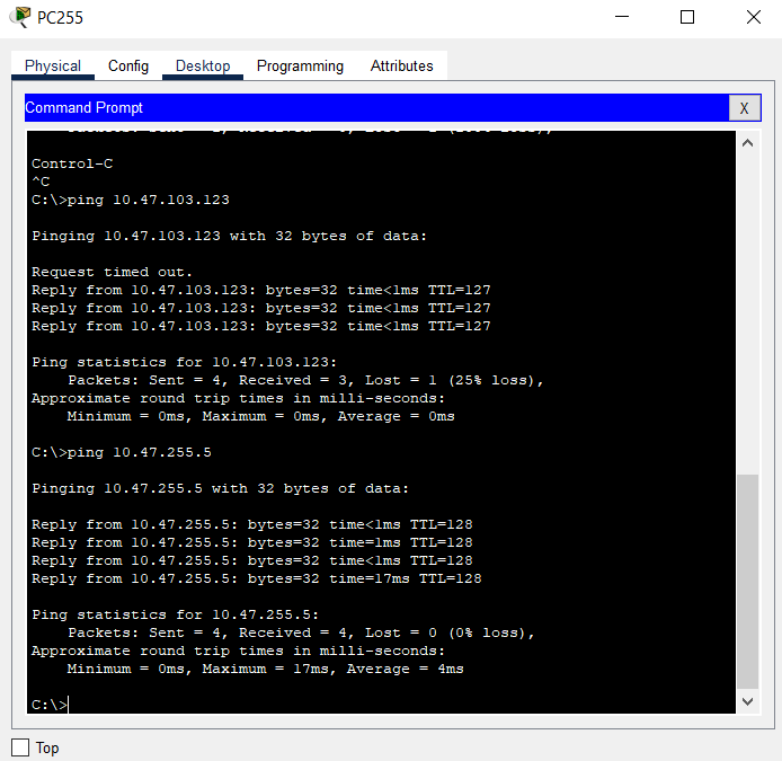
PC12 pinging outfacing Edge interface and Internet PC



PC21 pinging Internet-HTTP-Server and PC13



PC255 pinging PC23 and Server



NAT and PAT

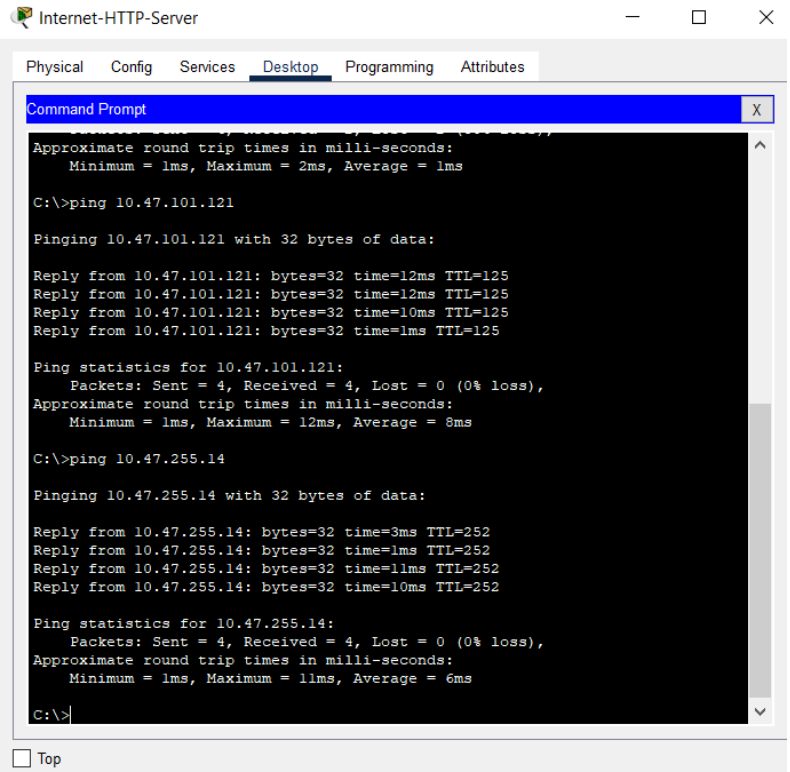
```
ip nat pool GLOBAL 197.197.197.1 197.197.197.20 netmask 255.255.255.224
ip nat inside source list 90 pool GLOBAL overload
```

NAT statistics

```
Edge#sh ip nat st
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/1/0
Inside Interfaces: GigabitEthernet0/0/1
Hits: 0  Misses: 104
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
```

Still have full connectivity after NAT and PAT

Internet-HTTP-Server pinging PC21 and Access-Sw2



11)

A) Preventing the use of DTP

```
Core-Sw(config-if)#do sh int gl/1/1 switchport
Name: Gigl/1/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dotlq
Operational Trunking Encapsulation: dotlq
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 255 (Admin)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dotlq
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

```
Access-Sw2(config-if)#do sh int f0/13 switch
Name: Fa0/13
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 103 (Purple)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

B) Spanning-tree portfast

```
Access-Sw1(config-if)#int f0/11
Access-Sw1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/11 but will only
have effect when the interface is in a non-trunking mode.
Access-Sw1(config-if)#int f0/12
Access-Sw1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/12 but will only
have effect when the interface is in a non-trunking mode.
Access-Sw1(config-if)#int f0/13
Access-Sw1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/13 but will only
have effect when the interface is in a non-trunking mode.
Access-Sw1(config-if)#
```

```
Core-Sw(config-if)#int gl/0/5
Core-Sw(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on GigabitEthernet1/0/5 but will only
have effect when the interface is in a non-trunking mode.
```

```
Dist-Sw1(config)#int f0/15
Dist-Sw1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/15 but will only
have effect when the interface is in a non-trunking mode.
```

C) Enable BPDU GUARD

```
Access-Sw1(config)#spanning-tree portfast bpduguard default
Access-Sw1(config)#
```

```
Access-Sw2(config-if)#spanning-tree bpduguard enable
Access-Sw2(config-if)#int f0/12
Access-Sw2(config-if)#spanning-tree bpduguard enable
Access-Sw2(config-if)#int f0/11
Access-Sw2(config-if)#spanning-tree bpduguard enable
Access-Sw2(config-if)#end
```

D) Show BPDU Guard

```
Access-Sw2#sh spanning-tree summary
Switch is in pvst mode
Root bridge for:
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is enabled
```

```
Port 12 (FastEthernet0/12) of VLAN0102 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.12
  Designated root has priority 32870, address 0001.63ED.4CE4
  Designated bridge has priority 32870, address 0030.F250.510C
  Designated port id is 128.12, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port is in the portfast mode
  Link type is point-to-point by default
```

```
Access-Sw2#sh spanning-tree int f0/11 detail
```

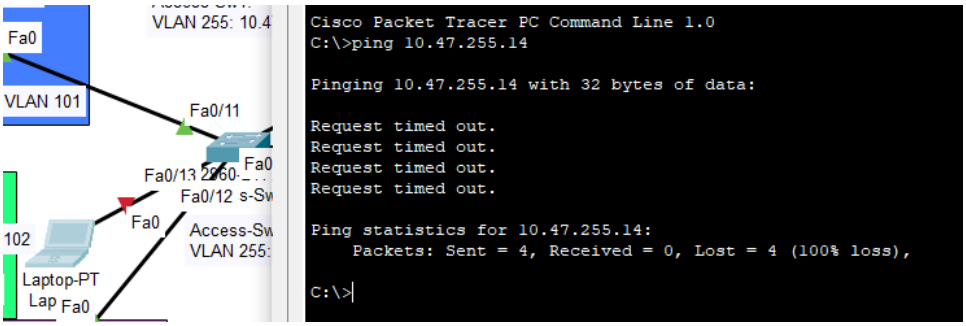
```
Port 11 (FastEthernet0/11) of VLAN0101 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.11
  Designated root has priority 32869, address 0001.63ED.4CE4
  Designated bridge has priority 32869, address 0030.F250.510C
  Designated port id is 128.11, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port is in the portfast mode
  Link type is point-to-point by default
```

G) Port Security: mac address sticky

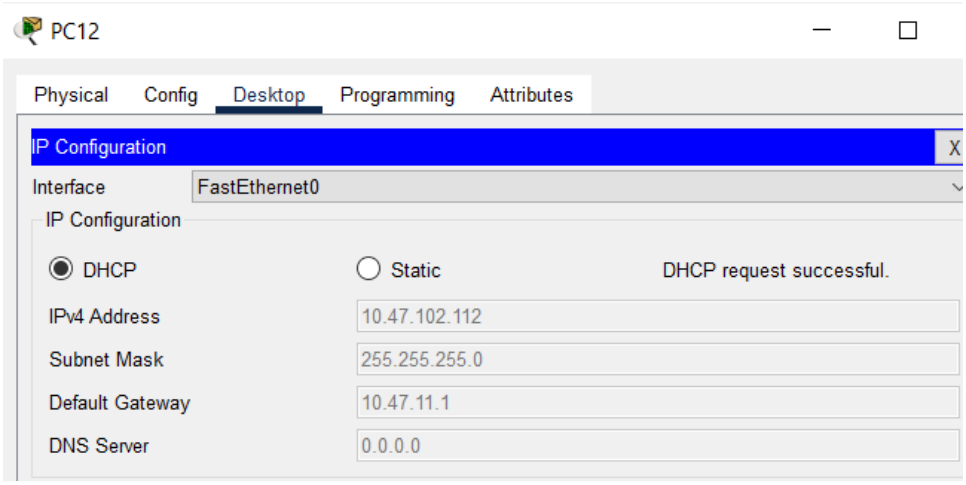
PC22 on f0/12

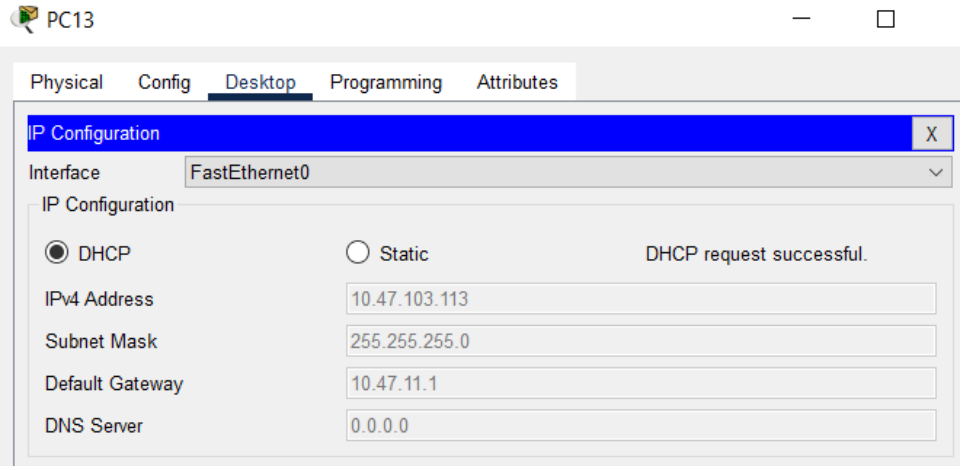
```
Access-Sw2(config-if)#do sh port-security int f0/12
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0090.2B6D.ED3D:102
Security Violation Count   : 0
```

Random laptop plugged into f0/12 (packets dropped even with same ip address)



H) DHCP implementation

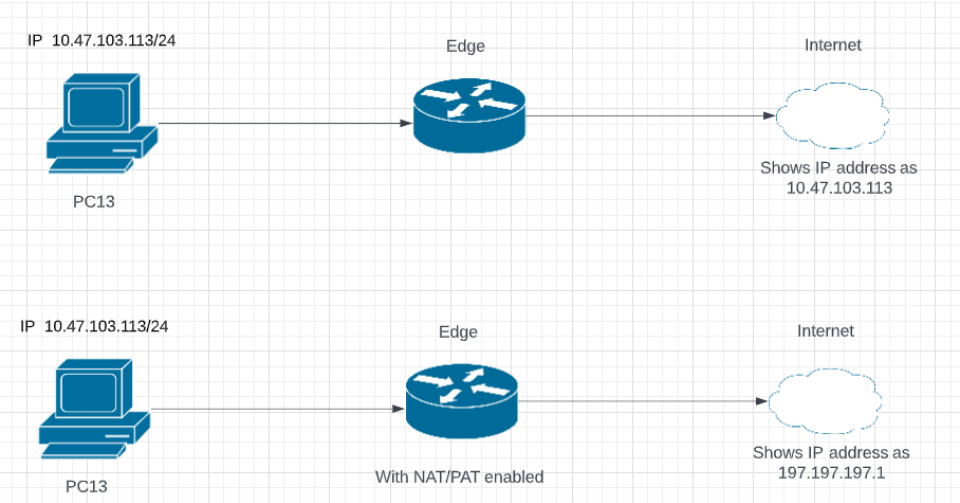





```
Dist-Sw2(config)#ip dhcp snooping
Dist-Sw2(config)#
```

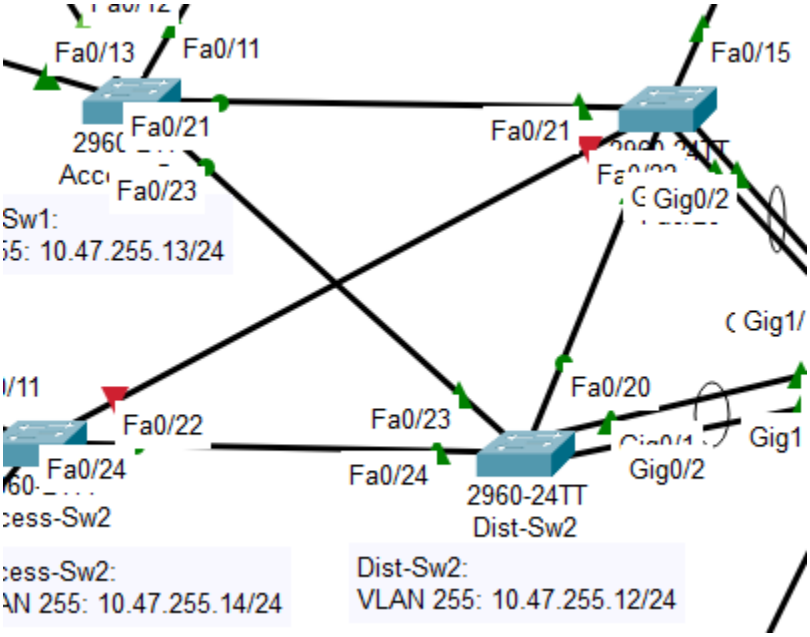
E) Test Cases

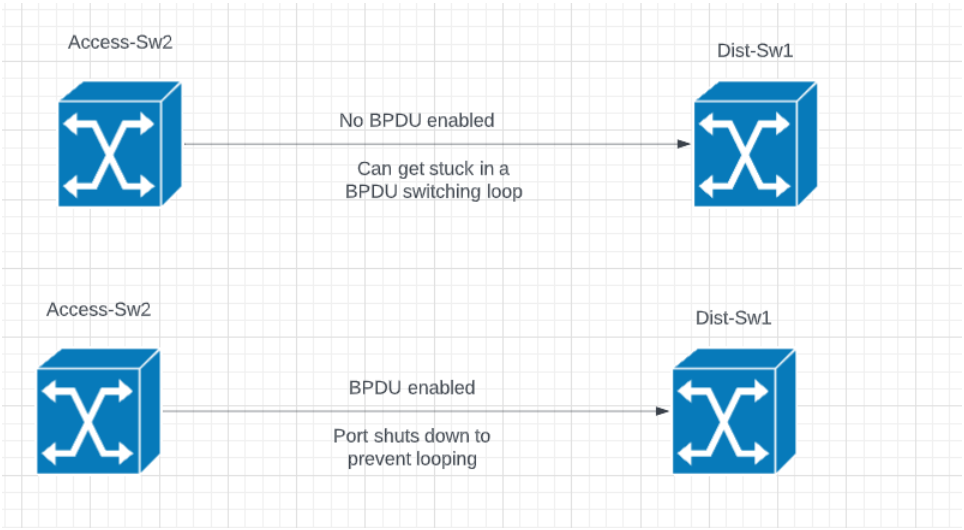
1) Implementation of NAT/PAT test case



2) BPDU

Ports shutting because of BPDU



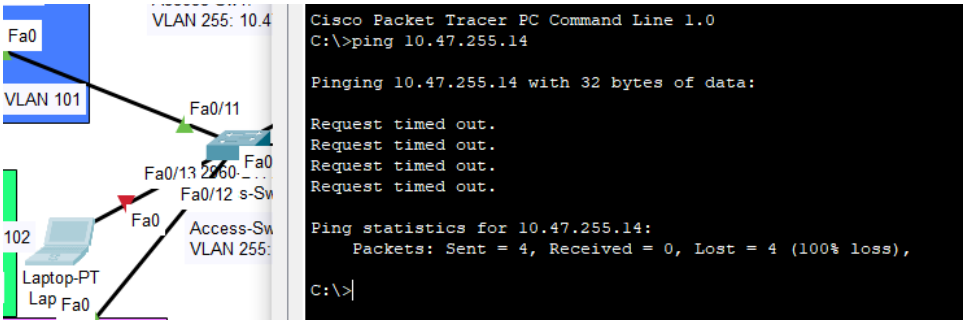


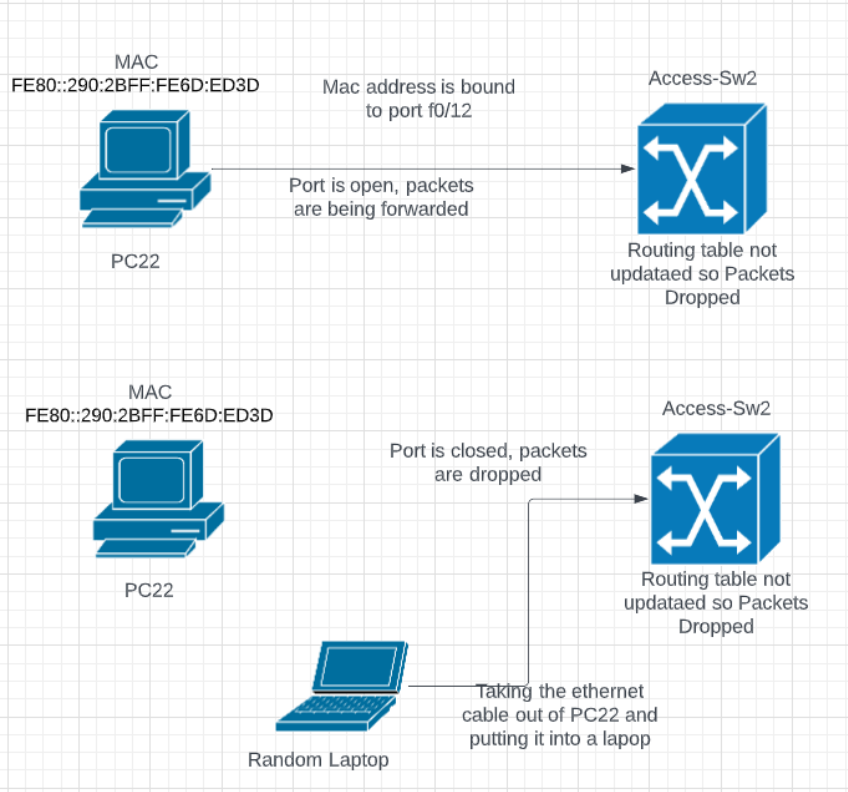
3) MAC-address change

PC22 on f0/12

```
Access-Sw2(config-if)#do sh port-security int f0/12
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0090.2B6D.ED3D:102
Security Violation Count   : 0
```

Random laptop plugged into f0/12 (packets dropped even with same ip address)





F) Conclusion:

The lab went almost exactly as planned with almost everything we implemented working as expected. The only problem I had was implementing root guard. When I tried to implement this it seemed to break the entire topology and caused all ports to go crazy. I tried implementing it in different orders as well as googling the error messages it was giving me to see what I was doing wrong. I was able to finally implement it on Access-Sw2 fine, but then when I continued it broke again. I have 2 versions, the broken one is the one with root guard enabled, while the normal one does not have that implemented.

G) Things Googled/Sites used:

How to configure Etherchannel:

https://www.cisco.com/c/en/us/td/docs/routers/access/1900/software/configuration/guide/Software_Configuration/etherchannel.pdf

How to configure DHCP snooping:

https://www.computernetworkingnotes.com/ccna-study-guide/configure-dhcp-snooping-on-cisco-switches.html