

Enterprise VLAN/DHCP Project

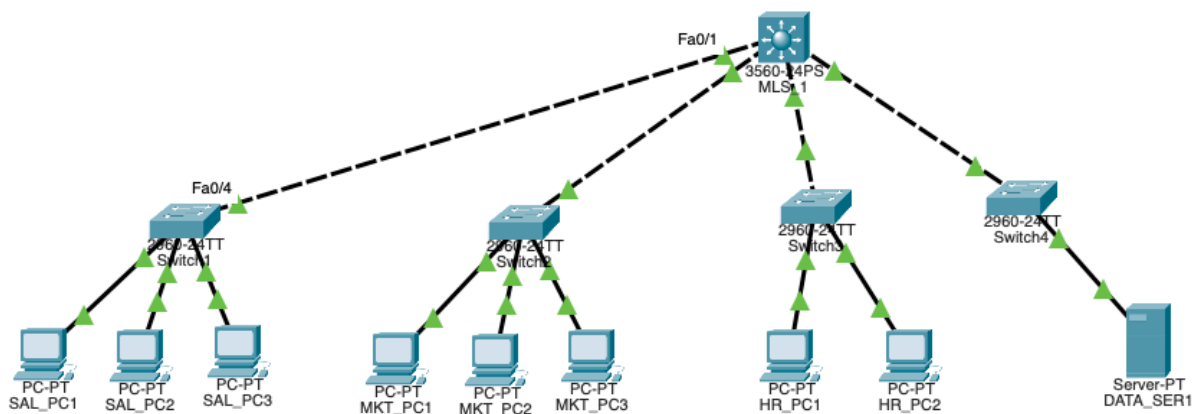
Objective:

The objective of this project is to simulate a layer 2/layer 3 enterprise network where:

- Sales, Marketing, HR, and a Data Server are separated into separate VLANs
- Each VLAN has its own dedicated access switch
- All access switches trunk to a central multilayer switch (MLS)
- The MLS facilitates inter-VLAN routing and also acts as a DHCP server
- All workstation IPs are dynamically assigned, except for the server, which is statically assigned

Network Setup:

Included below is a network diagram that showcases the logical network topology for this environment:



For this project, I will be using the following devices:

- 3 sales PCs
- 3 marketing PCs
- 2 HR PCs
- 1 data server
- 4 switches
- 1 multilayer switch (MLS)

Connect each end device to their respective access switch via copper straight-through cables. Once the end devices are connected, we will then connect the access switches to the MLS with copper crossover cables. I personally used the first numerical ports on the access switch as access ports and the next port over as the trunk port. I then connected all the access switches to the MLS on ports 1-4.

Once all the devices are physically connected, we can begin with the routing configuration.

CLI Configuration:

Step 1: Configure Access Switches -

First, we need to create the VLANs on each access switch. To do this, we open up the command line interface (CLI) and input the commands:

```
enable
conf t
vlan 10
exit
```

This creates the VLAN on the access switch.

Then, we will need to configure the switch ports that our end devices are connected to as access switches. Input the following commands on the CLI:

```
interface range fa0/1 - 3
switchport mode access
switchport access vlan 10
exit
```

This sets the interfaces Fa0/1 - Fa0/3 as access ports. These ports need to be access ports as they are connected to end devices.

The next step will be to set up the trunk port. Enter the following in the CLI:

```
interface fa0/4
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown
```

This sets the interface Fa0/4 as a trunk port and also enables 802.1Q trunking protocol on that port.

Repeat the above commands on each switch with their respective interfaces and VLANs. I personally used VLAN 20, 30, and 99 for marketing, HR, and data server, respectively. Additionally, I used the first few switch ports as access ports and the next over switch port as

the trunk port.

Step 2: Configure the MLS

First thing, we should create the VLANs on the MLS. Input the following on the MLS's CLI:

```
enable
conf t

vlan 10
exit
vlan 20
exit
vlan 30
exit
vlan 99
exit
```

Then, we need to enable inter-VLAN routing.

```
ip routing
```

Next, we need to configure each port on the MLS that connects to the access switch as trunk ports. To do this, we use the following commands:

```
interface fa0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  no shutdown
exit
```

Repeat this for the other interfaces. Just like what we did with the access switch, this command sets the selected interfaces as trunk interfaces and enables 802.1Q trunking. Once the MLS interfaces are all configured, we will need to create the switched virtual interface (SVI) for the VLANs. To do this, enter the following:

```
interface vlan 10
  ip address 192.168.10.1 255.255.255.0
  no shutdown
```

```
exit
```

What the above command does is enter the configuration mode for the SVI associated with VLAN 10, set the default gateway for all devices in that VLAN as 192.168.10.1, and enable the interface with 'no shutdown.' Repeat this command for the other VLANs. I match the VLAN number with the 3rd octet of the IP address.

Finally, we can set up the MLS as a DHCP server. First things first, let's exclude the default gateway addresses from the DHCP pool. Do this by inputting the following in the CLI:

```
ip dhcp excluded-address 192.168.10.1
```

Repeat this with the default gateway for the other VLANs. We can skip VLAN 99, because that VLAN will not be using DHCP. Instead, we will be statically assigning the IP address later.

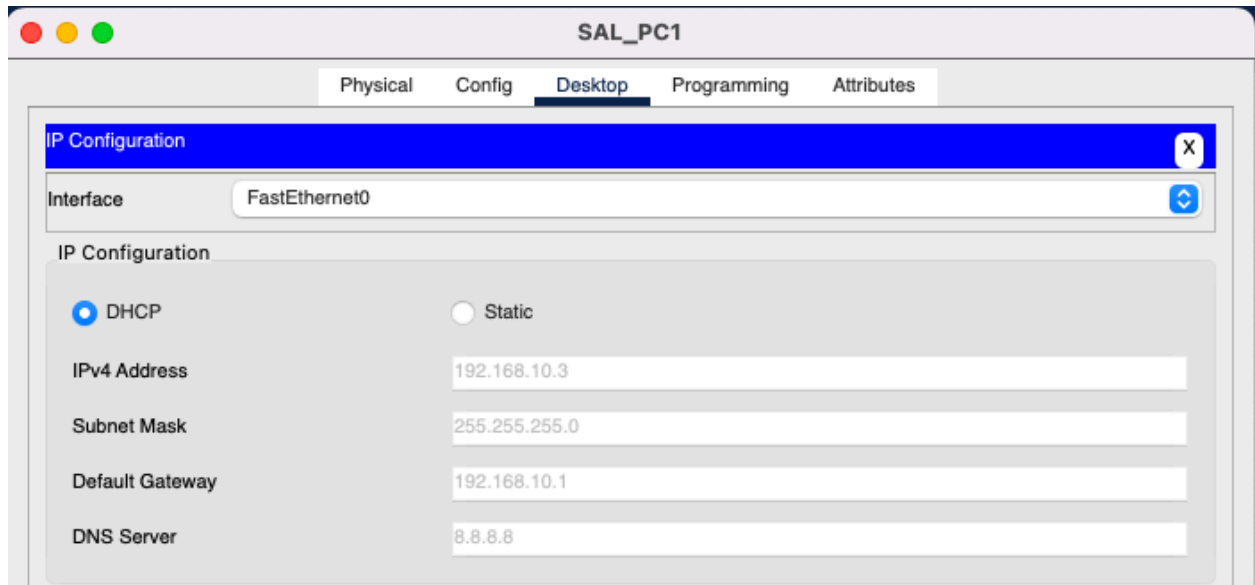
Next, we will need to define the DHCP pools for each VLAN. This will allow end devices on each VLAN to be assigned the proper IP addresses within their proper subnets. To do this, input the following command:

```
ip dhcp pool vlan10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 8.8.8.8
exit
```

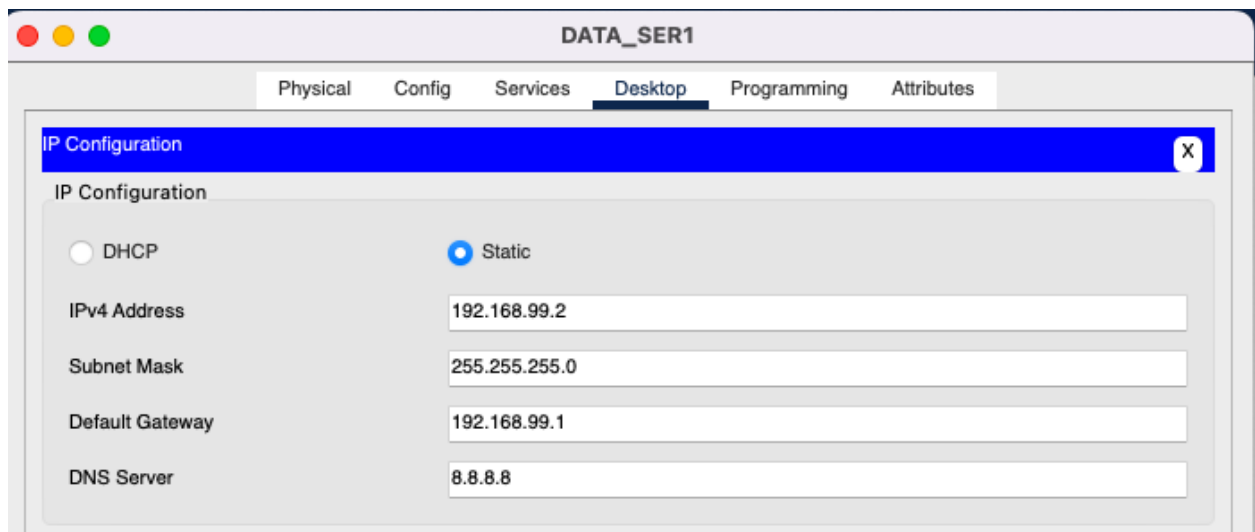
What this does is assign the subnet 192.168.10.1/24 to VLAN 10. Additionally, the default gateway will be 192.168.10.1. I personally use the first available address in each subnet as the default gateway. We also set the DNS server as 8.8.8.8, which is Google's public DNS server. Repeat this process for all the other VLANs with their respective subnets and default gateways, except for VLAN 99.

Step 3: Configure the End Devices

To configure the end devices, we will need to click on each individual PC and check that DHCP is enabled. To do this, simply click on the PC, go to desktop, then IP configuration. The output should look something like this:



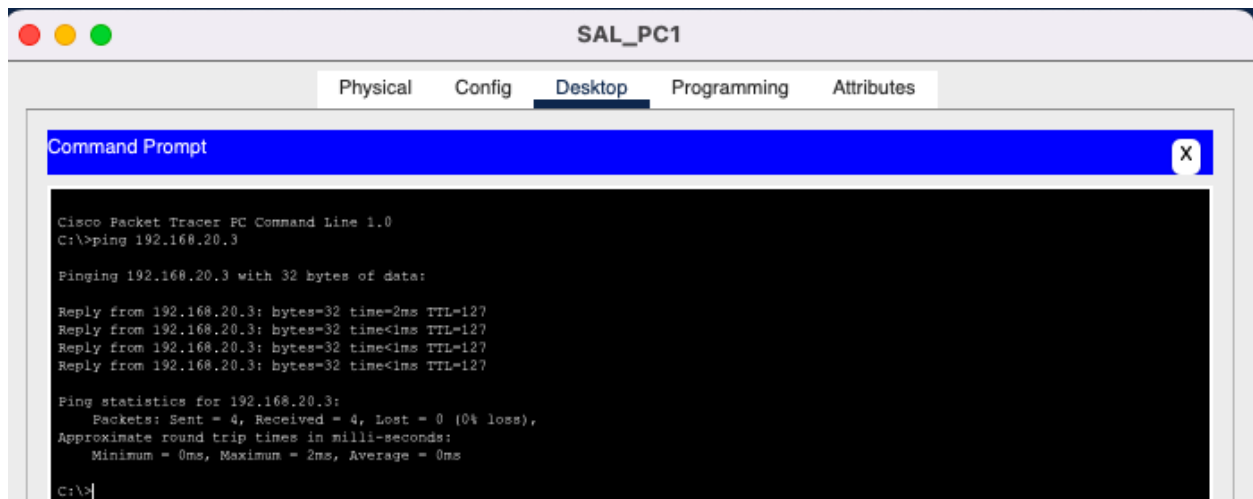
Finally, we will need to statically assign an IP address for the server. To do this, click on the server, go to desktop, then click on IP configuration and input the following:



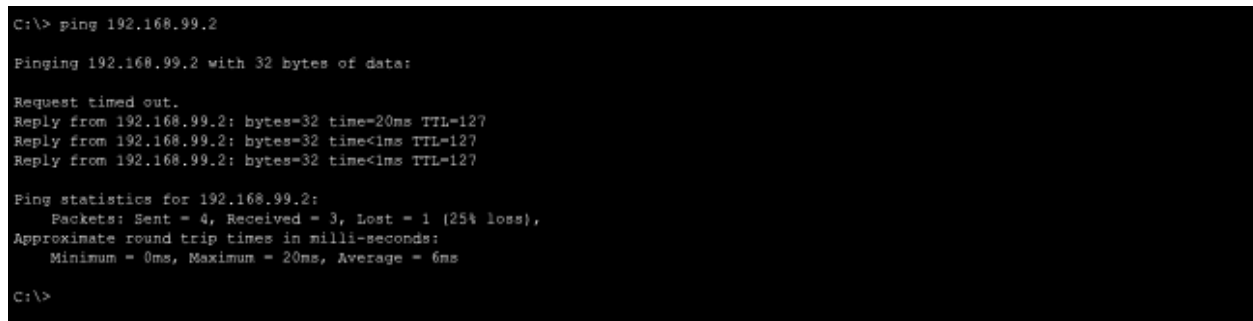
With all the end devices configured, our VLAN network should be all set!

Step 4: Verification and Troubleshooting

Now that we've finished setting up the network, we need to verify proper functionality. Let's start by pinging a PC from a different VLAN. To do this, simply ping the IP address of a PC in another VLAN from the command prompt. The output should look something like this:



Looks like we're able to communicate with PC's from different VLANs. Now let's try to ping the server, which has a statically assigned IP address. The output should look like:



We have now verified full network functionality! If there have been any issues up to this point, you can use the following commands to troubleshoot:

Task	Command
View VLANs	show vlan brief
View SVI and IP status	show ip interface brief
View trunk links	show interfaces trunk
View DHCP pools	show ip DHCP pool

You should see the following outputs for the above commands:

show vlan brief:

```
Switch>show vlan brief
```

VLAN Name	Status	Ports
1 default	active	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 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
10 VLAN0010	active	
20 VLAN0020	active	
30 VLAN0030	active	
99 VLAN0099	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
Switch>
```

show ip interface brief:

```
Switch>show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	up	up
FastEthernet0/4	unassigned	YES	unset	up	up
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	down	down
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/20	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down

```
Switch>
```

show interfaces trunk:

```
Switch>show interfaces trunk

Port      Mode      Encapsulation  Status        Native vlan
Fa0/1     on        802.1q         trunking      10
Fa0/2     on        802.1q         trunking      20
Fa0/3     on        802.1q         trunking      30
Fa0/4     on        802.1q         trunking      99

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/2     1-1005
Fa0/3     1-1005
Fa0/4     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,30,99
Fa0/2     1,10,20,30,99
Fa0/3     1,10,20,30,99
Fa0/4     1,10,20,30,99

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,20,30,99
Fa0/2     1,10,20,30,99
Fa0/3     1,10,20,30,99

Switch>
```

show ip DHCP pool:

```
Switch>show ip DHCP pool

Pool VLAN10 :
Utilization mark (high/low)    : 100 / 0
Subnet size (first/next)       : 0 / 0
Total addresses                 : 254
Leased addresses               : 3
Excluded addresses             : 0
Pending event                   : none

1 subnet is currently in the pool
Current index    IP address range    Leased/Excluded/Total
192.168.10.1    192.168.10.1 - 192.168.10.254  3 / 0 / 254

Pool VLAN20 :
Utilization mark (high/low)    : 100 / 0
Subnet size (first/next)       : 0 / 0
Total addresses                 : 254
Leased addresses               : 3
Excluded addresses             : 0
Pending event                   : none

1 subnet is currently in the pool
Current index    IP address range    Leased/Excluded/Total
192.168.20.1    192.168.20.1 - 192.168.20.254  3 / 0 / 254

Pool VLAN30 :
Utilization mark (high/low)    : 100 / 0
Subnet size (first/next)       : 0 / 0
Total addresses                 : 254
Leased addresses               : 2
Excluded addresses             : 0
Pending event                   : none

1 subnet is currently in the pool
Current index    IP address range    Leased/Excluded/Total
192.168.30.1    192.168.30.1 - 192.168.30.254  2 / 0 / 254
Switch>
```
