

SUNY POLYTECHNIC INSTITUTE

NCS 450

NETWORK SECURITY

---

## Lab 6: Inter VLAN Routing with Trunking

---

*Author:*

Jess YANARELLA

Tony PEREZ

*Professor:*

Ronny BULL

April 1st 2015

# 1 Introduction:

In this lab we will learn about VLANs and trunking and how to set it up on router and switch. On the router, we must create subinterfaces and tag them with encapsulation dot1Q. Over on the switch, we will create multiple VLANS and give them each different names and an IP address. These VLANS must be assigned to different ports on the switch. VLAN 20 will be assigned to the fa0/1 interface, which will be configured as the native vlan.

## 2 Network Diagram:

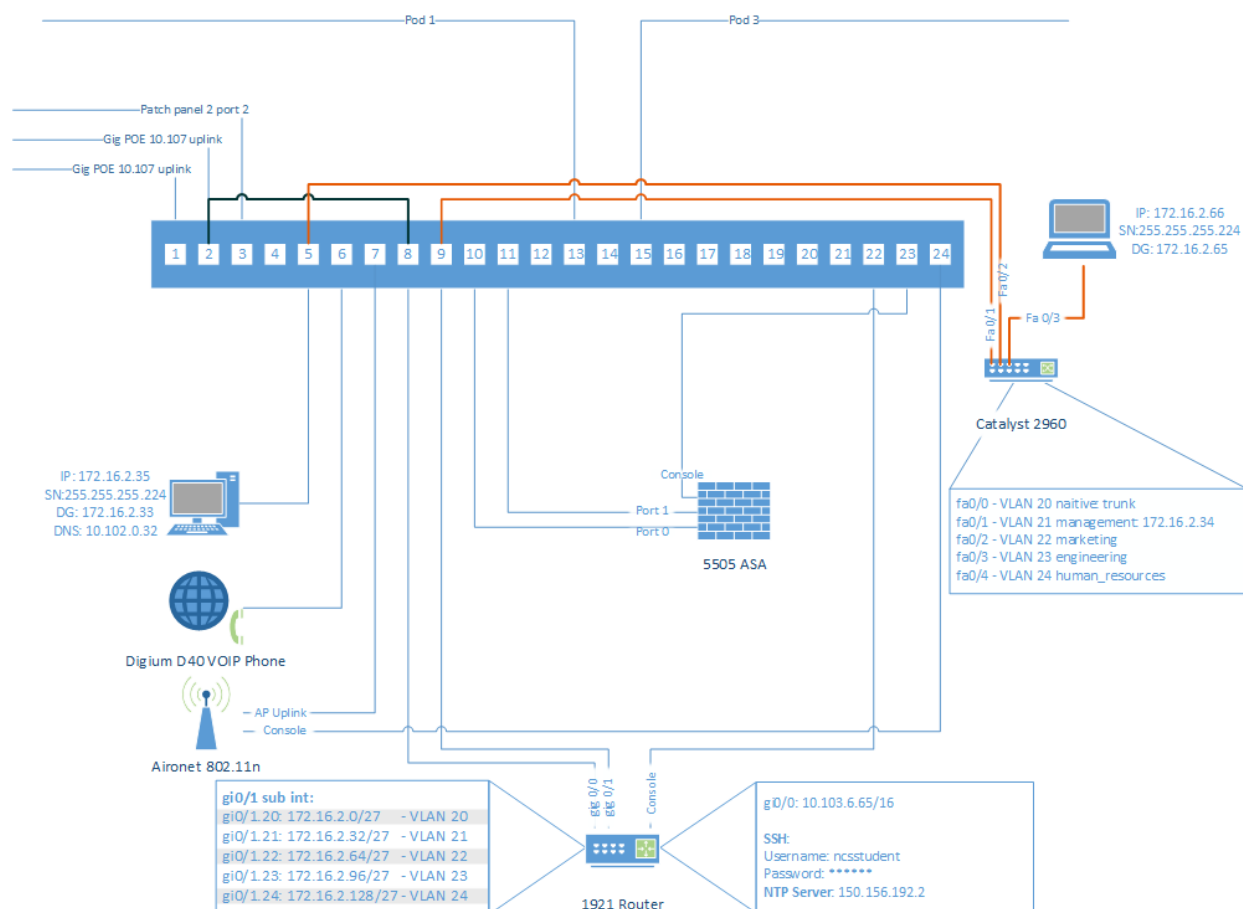


Figure 1: Added Sub-interfaces & VLANS

## 3 Disable VTP on the Router & Switch

To disable VTP, we have to put each device into transparent mode.  
(config)# vtp mode transparent

## 4 Configure Subinterfaces on the Router:

We will be creating 5 different subinterfaces on our router. The first will be on the interface gi0/1.20. Then after that, we will continue to go down the line with gi0/1.21, gi0/1.22, gi0/1.23, gi0/1.24, gi0/1.25.

```
(config)# interface gi0/1.20
```

This command will bring us to the subinterface configuration mode. We need to tell it what VLAN tagging to use and the best one is the standard 802.1q tag. On each subinterface we created, we must assign it this encapsulation.

```
(config)# encapsulation dot1Q 20
```

We should still be in the subinterface mode, so now we can assign this new interface an IP address and subnet mask. Since we are using the network 172.16.2.0/27, the first host available is 172.16.2.1, which will be used for or gi0/1.20. The netmask will be 255.255.255.224.

```
(config)# ip address 172.16.2.1 255.255.255.224
```

IP address

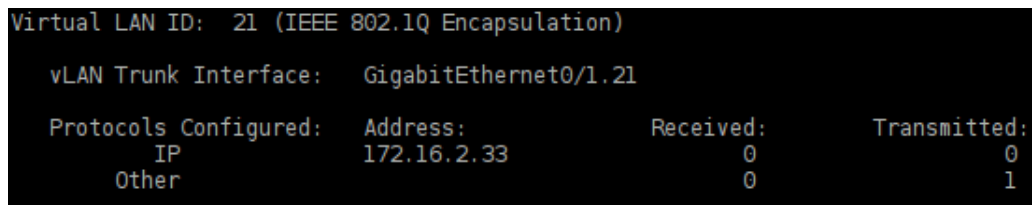
gi0/1.20 - 172.16.2.1

gi0/1.21 - 172.16.2.33

gi0/1.22 - 172.16.2.65

gi0/1.23 - 172.16.2.97

gi0/1.24 - 172.16.2.129

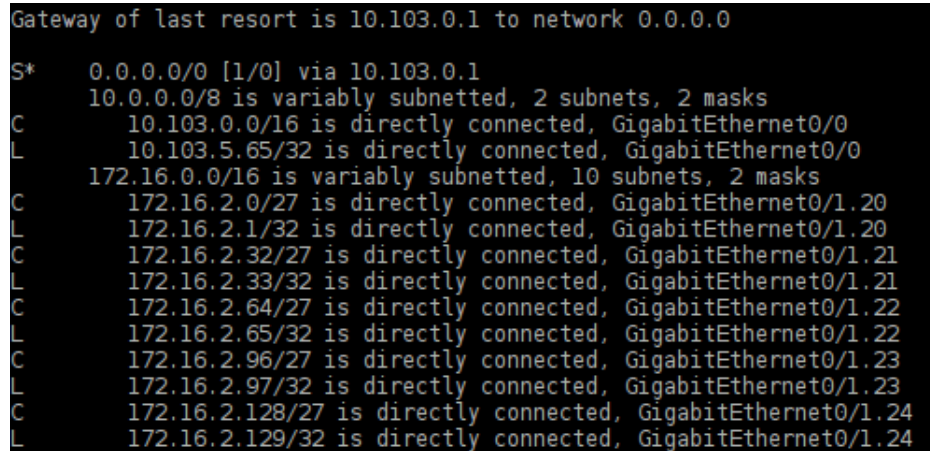


Virtual LAN ID: 21 (IEEE 802.1Q Encapsulation)			
vLAN Trunk Interface:		GigabitEthernet0/1.21	
Protocols Configured:	Address:	Received:	Transmitted:
IP	172.16.2.33	0	0
Other		0	1

Figure 2: Subinterface 21

We can see and verify that the following commands properly made changes to the configuration.

```
# show vlans
show ip route
show ip interface brief
```



```
Gateway of last resort is 10.103.0.1 to network 0.0.0.0

S*  0.0.0.0/0 [1/0] via 10.103.0.1
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.103.0.0/16 is directly connected, GigabitEthernet0/0
L    10.103.5.65/32 is directly connected, GigabitEthernet0/0
    172.16.0.0/16 is variably subnetted, 10 subnets, 2 masks
C    172.16.2.0/27 is directly connected, GigabitEthernet0/1.20
L    172.16.2.1/32 is directly connected, GigabitEthernet0/1.20
C    172.16.2.32/27 is directly connected, GigabitEthernet0/1.21
L    172.16.2.33/32 is directly connected, GigabitEthernet0/1.21
C    172.16.2.64/27 is directly connected, GigabitEthernet0/1.22
L    172.16.2.65/32 is directly connected, GigabitEthernet0/1.22
C    172.16.2.96/27 is directly connected, GigabitEthernet0/1.23
L    172.16.2.97/32 is directly connected, GigabitEthernet0/1.23
C    172.16.2.128/27 is directly connected, GigabitEthernet0/1.24
L    172.16.2.129/32 is directly connected, GigabitEthernet0/1.24
```

Figure 3: IP Route Configuration

## 5 Create VLANs on the Switch:

These configuration changes must be done in global configuration mode and we will be creating a VLAN with VLAN number 20-24 and the name of the vlan of our choice. A simple command can be used to create the vlan.

```
(config)# vlan 20
(config)# vlan 21
(config)# vlan 22
(config)# vlan 23
(config)# vlan 24
```

## 6 Configure the Management VLAN on the Switch:

Usually with any native VLAN, the default to use is VLAN 1 for the management. For better security purposes, it is recommend to use the management VLAN to another VLAN other then the native one. We are going to configure our VLANS with a static Layer 3 configuration in VLAN configuration mode. First, we need to assign it an IP address and subnet along with the default gateway.

```
(config)# ip address 172.16.2.34
(config)# ip default-gateway 172.16.2.33
```

Vlan Network Setup:

VLAN 20 - Native - 172.16.2.0/27

VLAN 21 - Management - 172.16.2.32/27

VLAN 22 - Marketing - 172.16.2.64/27

VLAN 23 - Engineering - 172.16.2.96/27

VLAN 24 - Human\_Resources - 172.16.2.128/27

```
Switch(config)#do sh vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Gi0/1
20	native	active	
21	management	active	
22	marketing	active	
23	engineering	active	
24	human_resources	active	

Figure 4: VLAN Names

## 7 Assign VLANs to Ports on the Switch:

Now that our VLAN is created, we can apply it to our switch port. We need to move to our switch and the ports configuration mode. We can tell our switch port to behave as an access port.

```
(config-if)# switchport mode access
```

Next, we must assign our created VLANs to different ports on the switch. This is done on the different interfaces of the switch.

```
(config)# int fa0/1
```

```
(config-if)# switchport mode access
```

```
(config-if)# switchport access VLAN 21
```

VLAN 20 - fa0/1

VLAN 21 - fa0/2

VLAN 22 - fa0/3

VLAN 23 - fa0/4

VLAN 24 - fa0/5

## 8 Configure a Trunk Port on the Switch:

Trunk ports on switches allow VLAN trunking between two switches or between a switch and a router. We must tell the switch port to be a trunk port using the following command.

```
(config-if)# switchport mode trunk
```

```
Switch#sh vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/6, Fa0/7, Fa0/8, Gi0/1
20	native	active	
21	management	active	Fa0/2
22	marketing	active	Fa0/3
23	engineering	active	Fa0/4
24	human resources	active	Fa0/5

Figure 5: VLANS & Associated Switch Ports

## 9 Configure the Native VLAN on a Trunk Port:

All switches have a native VLAN, which can be assigned to switch ports. It is best not to use VLAN 1 for anything and never assign it to a switch port. If we decide to use VLAN 1 as the native VLAN for a trunk, we will not need to do any extra configuration. If we wanted to assign our VLAN 20 as the native VLAN on a trunk, we must make changes.

```
(config-if)# switchport trunk native vlan 20
```

## 10 Secure a Switch Port with Port Security:

We can secure our switch port by limiting the number of MAC addresses that can be associated with it. On our switch port, we will be limiting it to at most 6 entries in the CAM table. First, we must disable "sticky MAC" switch port behavior and remove any existing MAC addresses. This will all be done our trunk port, which is fa0/1.

```
(config)# no switchport port-security mac-address sticky
```

Now we are allowed to use this port security and limit the number of MAC addresses.

```
(config)# switchport port-security maximum 6
```

After the port security is set up, we can re-enable "sticky MAC" because we want our port switch to learn new MAC addresses.

```
(config)# switch port-security mac-address sticky
```

## 11 PC Test Configuration:

On our Pod PC, we connected it to our switch and changed its' IP address and default-gateway. Once it was configured properly, we were able to ping the different IP addresses on our switch.

```

yanarej@tequila ~ $ sudo ifconfig eth0 172.16.2.35 netmask 255.255.255.224
yanarej@tequila ~ $ sudo route add default gw 172.16.2.33
SIOCADDRT: File exists
yanarej@tequila ~ $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.2.35 netmask 255.255.255.224 broadcast 172.16.2.63
    inet6 fe80::82c1:6eff:febd:28a1 prefixlen 64 scopeid 0x20<link>
    ether 80:c1:6e:fd:28:a1 txqueuelen 1000 (Ethernet)
    RX packets 43869 bytes 34141904 (32.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27135 bytes 5338350 (5.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 20 memory 0xfe700000-fe720000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 0 (Local Loopback)
    RX packets 140 bytes 21364 (20.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 140 bytes 21364 (20.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figure 6: Pod PC ifconfig

We also connected a laptop to the switch and manually set the IP address and default gateway. The IP address was on the same network and allowed us to ping the other interfaces as well.

```

Tony@TPMB:~$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=10b<RXCSUM, TXCSUM, VLAN_HWTAGGING, AV>
    ether a8:20:66:08:66:bb
    inet6 fe80::aa20:66ff:fe08:66bb%en0 prefixlen 64 scopeid 0x4
    inet 172.16.2.66 netmask 0xffffffe0 broadcast 172.16.2.95
    nd6 options=1<PERFORMNUD>
    media: autoselect (100baseTX <full-duplex>)
    status: active

```

Figure 7: Laptop ifconfig

The Pod PC is on the 172.16.2.32/27 network and the laptop is on the 172.16.2.64/27 network.

```

yanarej@tequila ~ $ ping 172.16.2.66 -c 4
PING 172.16.2.66 (172.16.2.66) 56(84) bytes of data.
64 bytes from 172.16.2.66: icmp_seq=1 ttl=63 time=0.881 ms
64 bytes from 172.16.2.66: icmp_seq=2 ttl=63 time=0.937 ms
64 bytes from 172.16.2.66: icmp_seq=3 ttl=63 time=0.906 ms
64 bytes from 172.16.2.66: icmp_seq=4 ttl=63 time=0.951 ms

--- 172.16.2.66 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.881/0.918/0.951/0.046 ms

```

Figure 8: Pod PC ping test to Laptop

```
Tony@TPMB:~$ ping -c 4 172.16.2.35
PING 172.16.2.35 (172.16.2.35): 56 data bytes
64 bytes from 172.16.2.35: icmp_seq=0 ttl=63 time=0.738 ms
64 bytes from 172.16.2.35: icmp_seq=1 ttl=63 time=1.048 ms
64 bytes from 172.16.2.35: icmp_seq=2 ttl=63 time=1.052 ms
64 bytes from 172.16.2.35: icmp_seq=3 ttl=63 time=0.947 ms

--- 172.16.2.35 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.738/0.946/1.052/0.127 ms
```

Figure 9: Laptop ping test to Pod PC