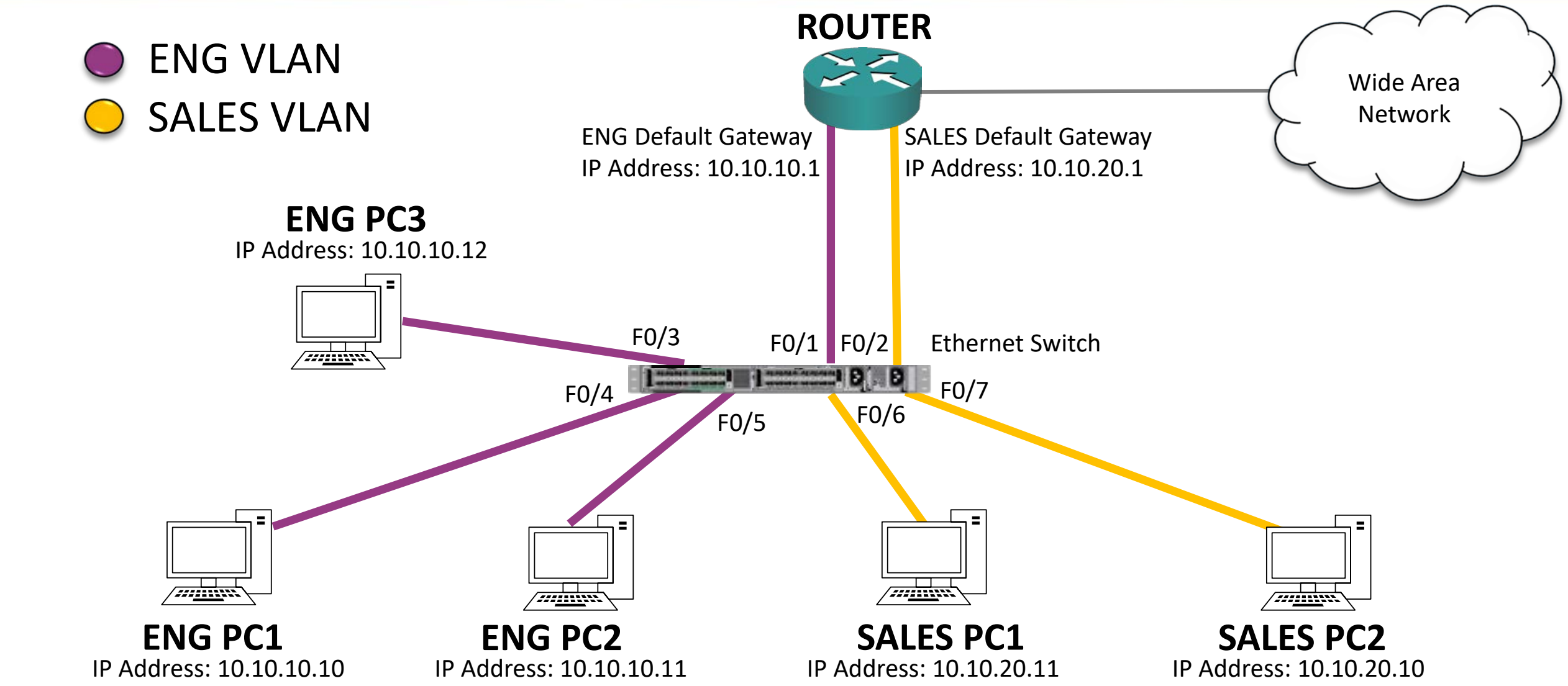
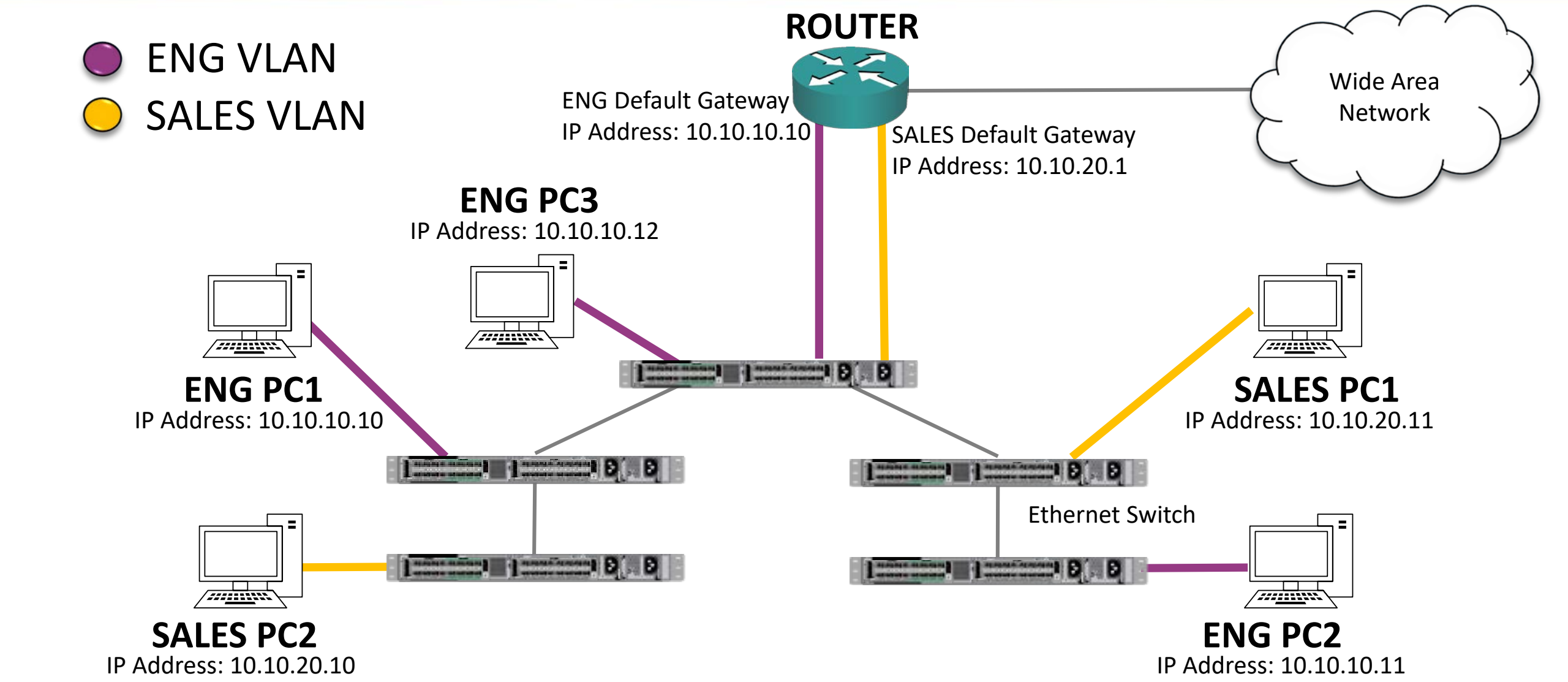
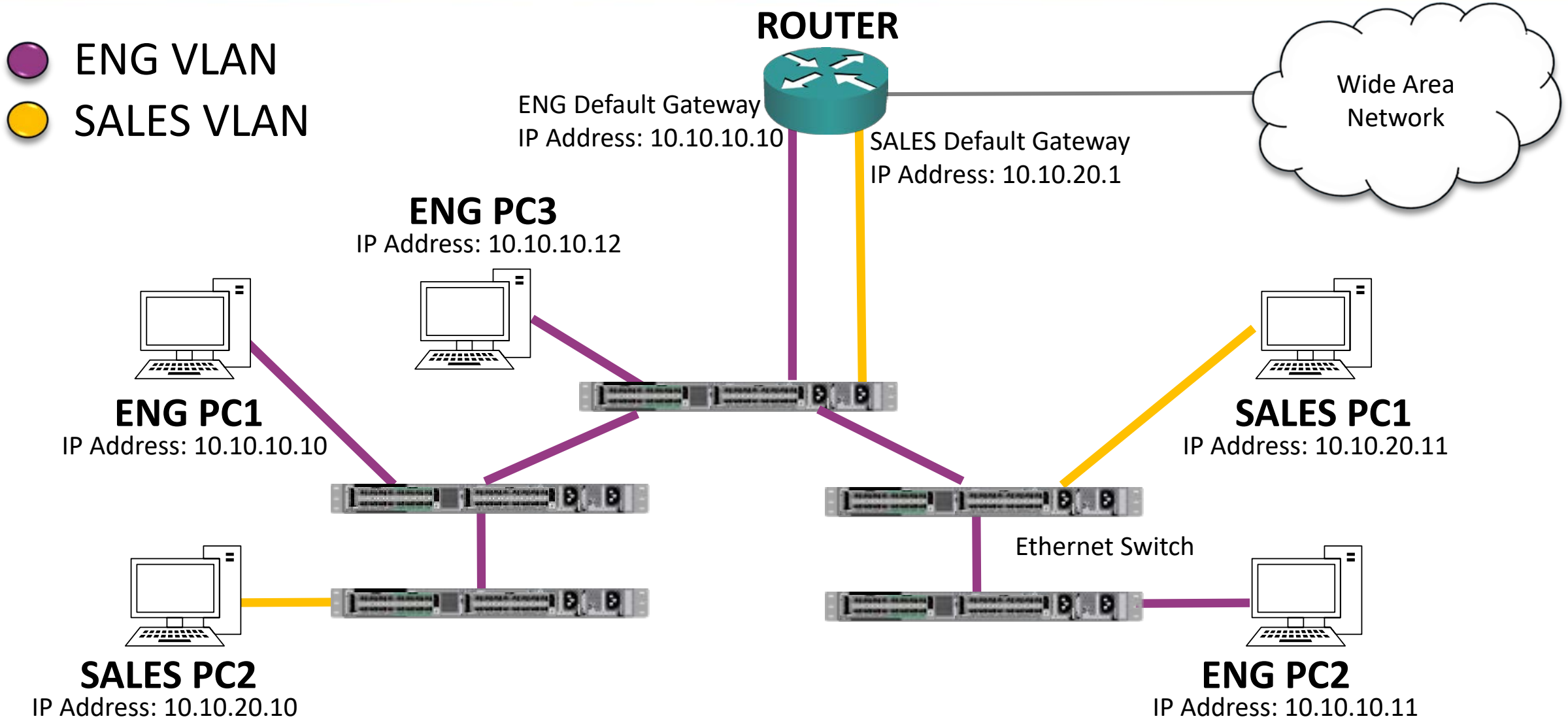
VLAN Access Ports



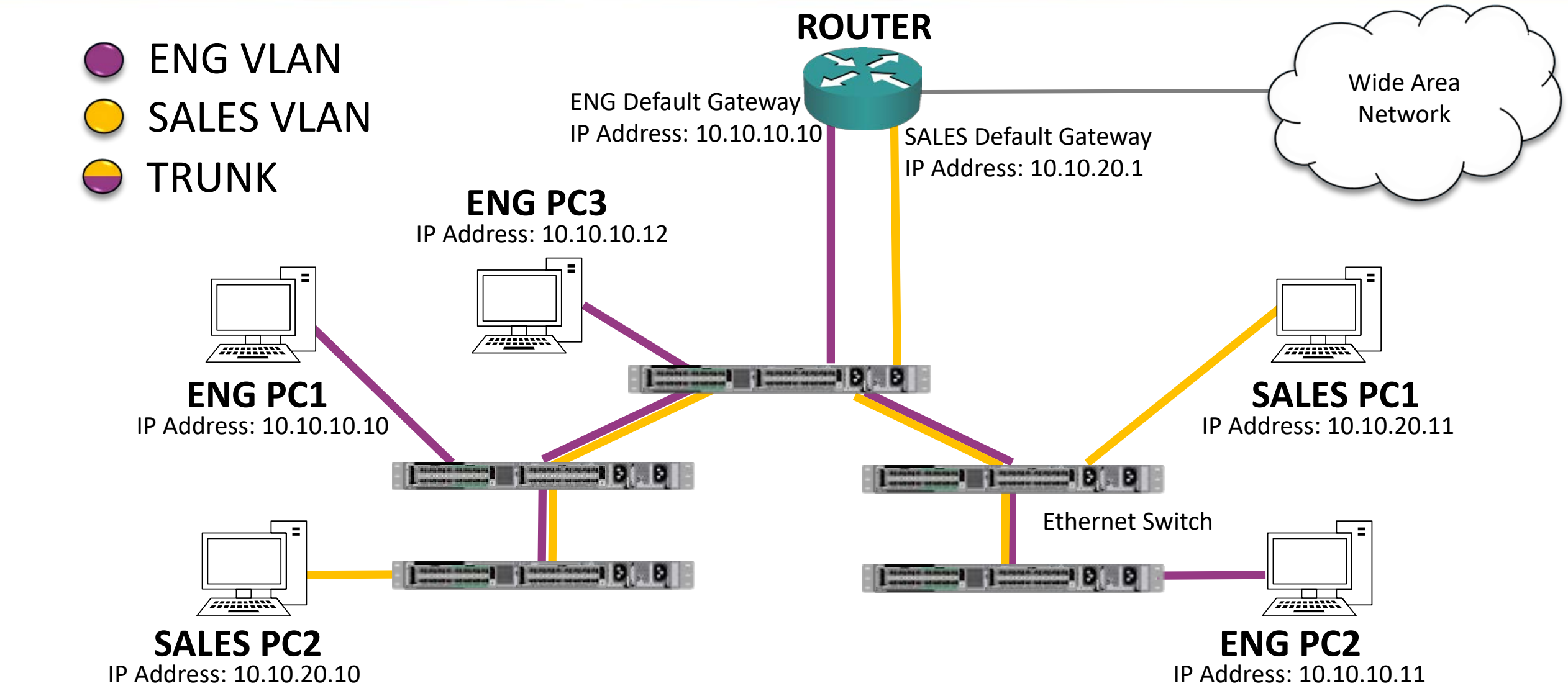
What about the links between switches?



What about the links between switches?



Dot1Q Trunks



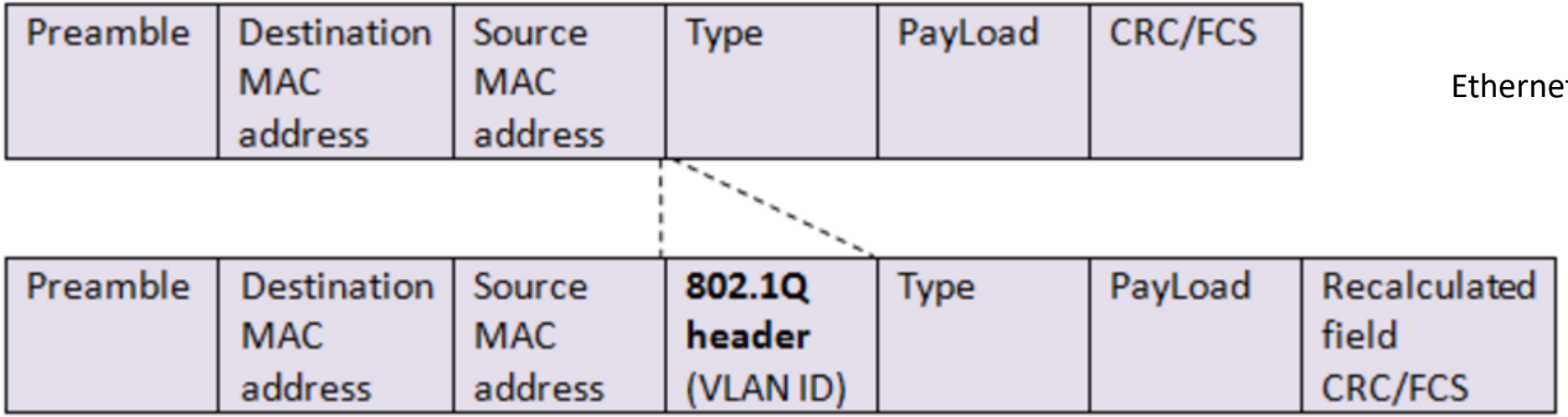
Dot1Q Trunks

- An access port carries traffic for one specific VLAN
- Dot1Q trunks are configured on the links between switches where we need to carry traffic for multiple VLANs
- ISL (Inter-Switch Link) was a Cisco proprietary trunking protocol which is now obsolete

Dot1Q Trunks

- When the switch forwards traffic to another switch, it tags the layer 2 Dot1Q header with the correct VLAN
- The receiving switch will only forward the traffic out ports that are in that VLAN
- The switch removes the Dot1Q tag from the Ethernet frame when it sends it to the end host

Dot1Q Format

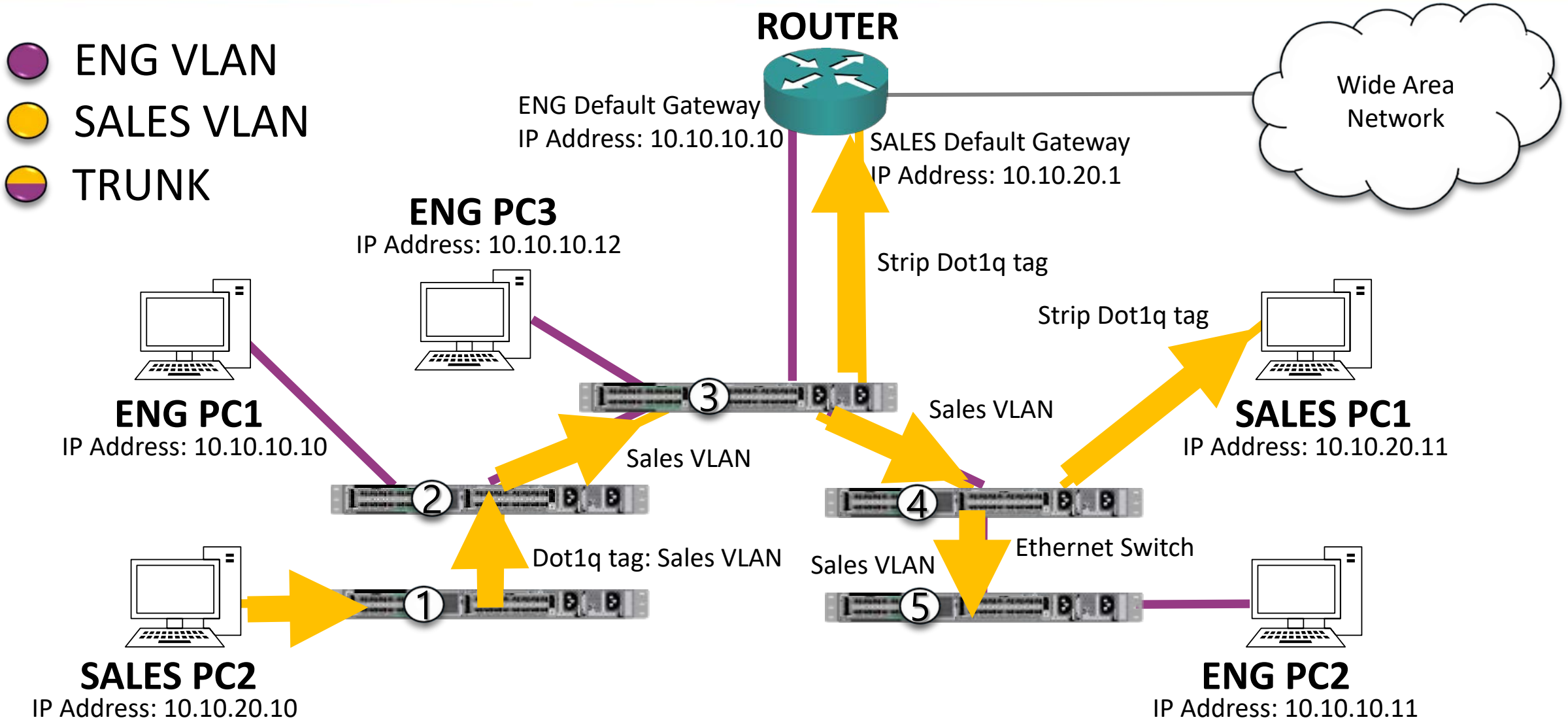


Ethernet frame received from host

Switch inserts Dot1Q tag when sending out a trunk port

A receiving switch will remove the Dot1Q tag when forwarding the frame out an access port

Dot1Q Trunks

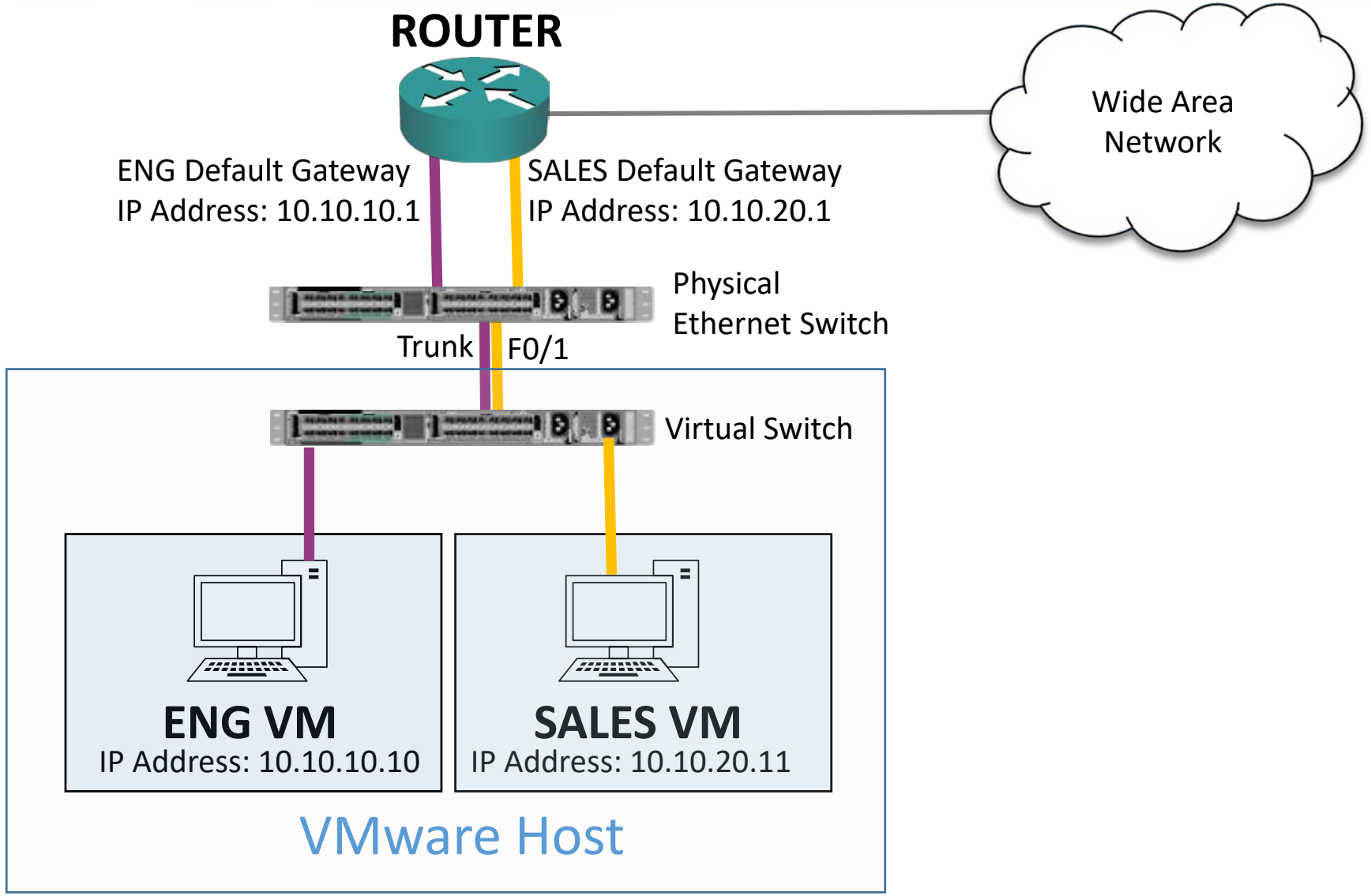


Hypervisors - VLAN Aware Hosts

- End hosts are typically members of only one VLAN and are not VLAN aware
- A special case is virtualized hosts, where there are virtual machines in different IP subnets on the host
- In this case we need to trunk the VLANs down to the host

Hypervisors - VLAN Aware Hosts

- ENG VLAN
- SALES VLAN
- TRUNK



Voice VLAN

Trunk Port Configuration

```
SW1(config)#interface FastEthernet 0/24
SW1(config-interface)#description Trunk to SW2
SW1(config-interface)#switchport trunk encapsulation dot1q
SW1(config-interface)#switchport mode trunk
```

Voice VLAN Configuration

```
SW1(config)#interface FastEthernet 0/10
SW1(config-interface)#description IP Phone
SW1(config-interface)#switchport mode access
SW1(config-interface)#switchport access vlan 10
SW1(config-interface)#switchport voice vlan 20
```

The Native VLAN

- The switch needs to know which VLAN to assign to any traffic which comes in untagged on a trunk port
- This used to be required for when a switch was connected to a hub. Hubs are Layer 1 devices so are not VLAN aware
- The Native VLAN is used for this
- The default Native VLAN is VLAN 1
- There are some security issues with using VLAN 1 as the Native VLAN so best practice is to change it to an unused VLAN
- The Native VLAN must match on both sides of a trunk for it to come up

Native VLAN Configuration

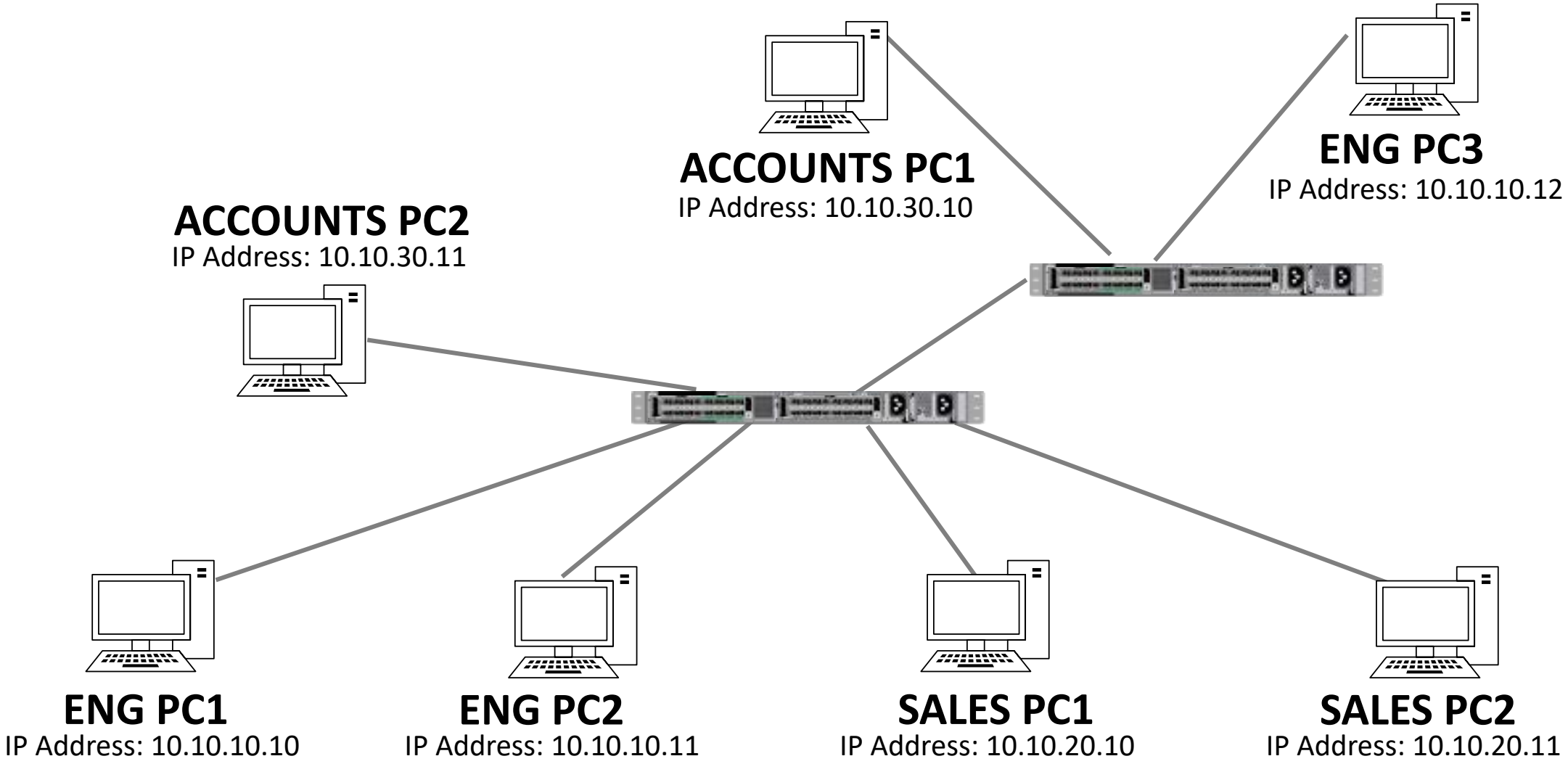
```
SW1(config)#vlan 199
SW1(config-vlan)#name Native

SW1(config)#interface GigabitEthernet 0/1
SW1(config-interface)#description Trunk to SW2
SW1(config-interface)#switchport trunk encapsulation dot1q
SW1(config-interface)#switchport mode trunk
SW1(config-interface)#switchport trunk native vlan 199
```

Verification – show interface switchport

```
SW1#show interface gig0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 199 (Inactive)
Voice VLAN: none
truncated
```

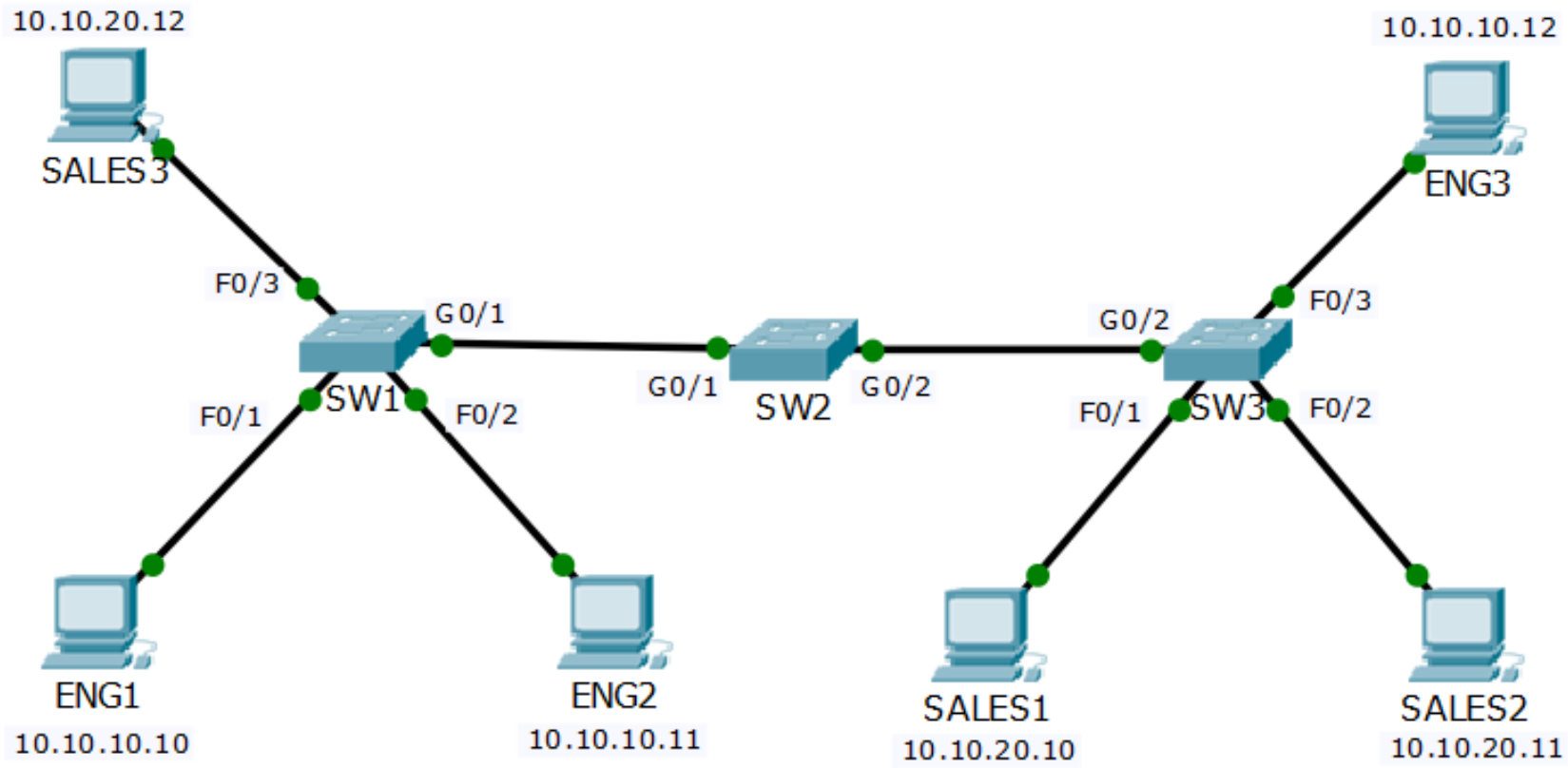
Limiting Allowed VLANs



Allowed VLAN Configuration

```
SW1(config)#interface GigabitEthernet 0/1
SW1(config-if)#switchport trunk allowed vlan 10,30
```

VLAN Lab


10.10.20.12
SALES3
F0/3
G0/1
F0/1
SW1
F0/2
ENG1
10.10.10.10
ENG2
10.10.10.11
G0/1
SW2
G0/2
10.10.10.12
ENG3
F0/3
G0/2
F0/1
SW3
F0/2
SALES1
10.10.20.10
SALES2
10.10.20.11