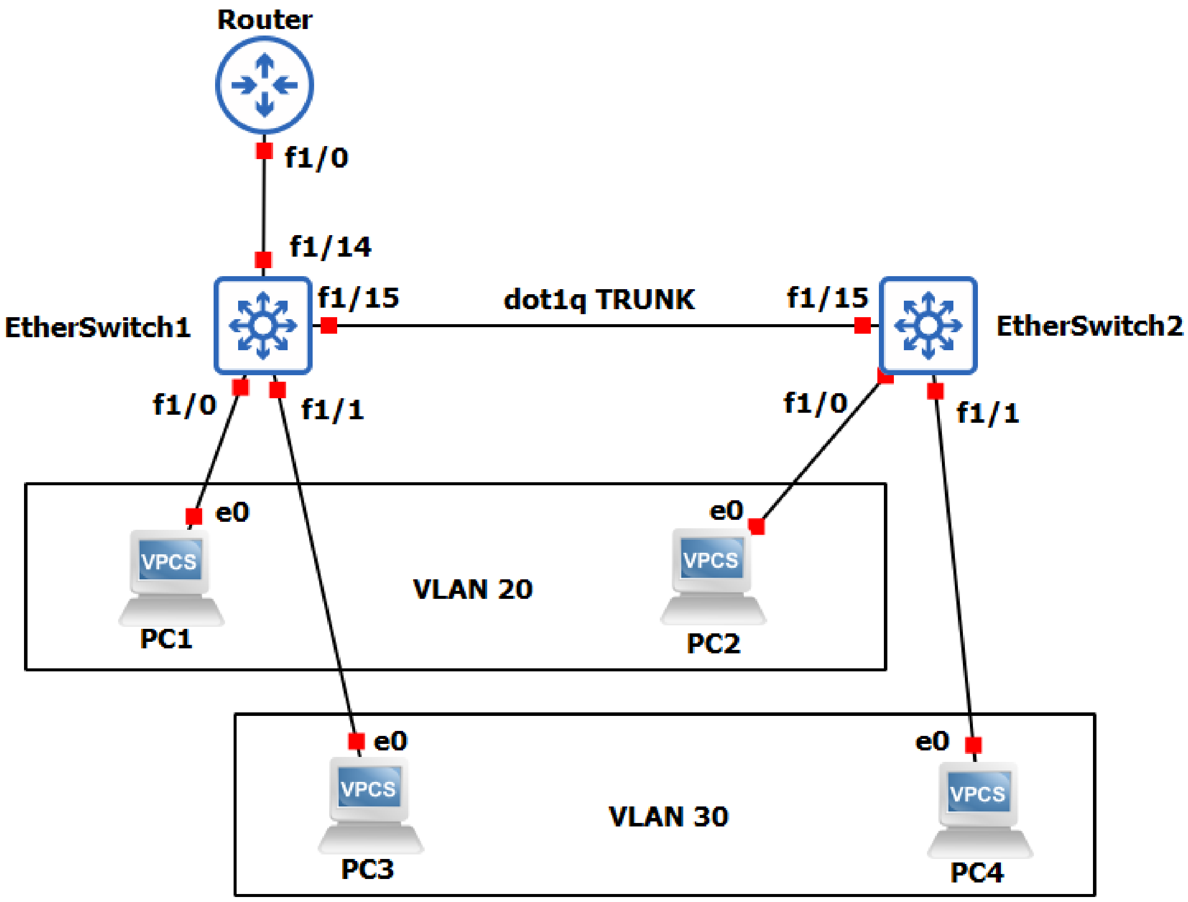
ELEC-H417: Lab 3 - VLAN

Objectives

- Layer 2 isolation via dot1q (IEE 802.1q) VLAN
- Trunks: VLAN trnasport between multiple switches
- Inter-VLAN routing

Topology



The topology for this lab will be the following:

- Guest hosts (pre-configured)

    - VPC1 (192.168.20.2/24 on VLAN 20 Gateway 192.168.20.1)
    - VPC2 (192.168.20.3/24 on VLAN 20 Gateway 192.168.20.1)
    - VPC3 (192.168.30.2/24 on VLAN 30 Gateway 192.168.30.1)
    - VPC4 (192.168.30.3/24 on VLAN 30 Gateway 192.168.30.1)
- Switches (to be configured)
    - EtherSwitch 1
        - port 1/0 : mode ACCESS on VLAN 20
        - port 1/1 : mode ACCESS on VLAN 30
        - port 1/14 : TRUNK dot1q
        - port 1/15 : TRUNK dot1q
    - EtherSwitch 2
        - port 1/0 : mode ACCESS on VLAN 20
        - port 1/1 : mode ACCESS on VLAN 30
        - port 1/15 : TRUNK dot1q
- Router (to be configured)
    - Interface VLAN 20 on 192.168.20.1
    - Interface VLAN 30 on 192.168.30.1

CISCO EtherSwitches

Many variants of L2/L3 (professional) switches exist on the market. All of them allow to implement VLANs through the IEEE 802.1q standard (also called dot1q). CISCO (like many other vendors) offers two categories of equipments: (1) Switches (Catalyst series) with a focus on L2 functionalities and (2) routers with an etherswitch. In an etherswitch, interfaces of the routers are VLANs and are then configured / manipulated as classical, real, physical interfaces.

For instance, to configure the interfaces on the EtherSwitches looks like:

1. Turn off the IP routing of the CISCO 3700 series

```
EtherSwitch1# configure terminal
EtherSwitch1(config)# no ip routing
EtherSwitch1(config)# end
```

2. declare the existence of some VLANs (here VLAN number 20 and VLAN number 30)

```
EtherSwitch1# vlan database
EtherSwitch1(vlan)# vlan 20
EtherSwitch1(vlan)# vlan 30
EtherSwitch1(vlan)# exit
```

3. configure a port (physical connector) to support VLANs. Interfaces can be either in access mode (i.e, it will tag the ethernet packet on-the-fly) or in trunk mode (it will carry all VLAN between two switches. See the lectures):

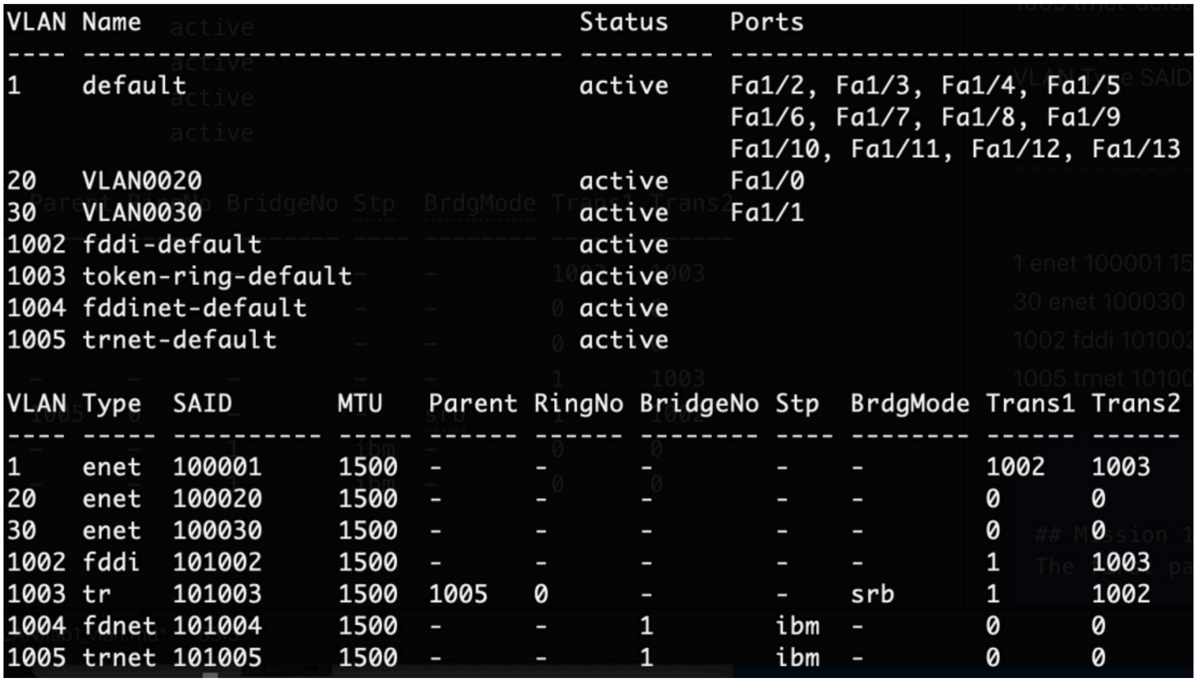
```
EtherSwitch1# configure terminal
EtherSwitch1(config)# interface fastEthernet 1/0
EtherSwitch1(config-if)# switchport mode access
EtherSwitch1(config-if)# switchport access vlan 20
EtherSwitch1(config-if)# exit
EtherSwitch1(config)# interface fastEthernet 1/1
EtherSwitch1(config-if)# switchport mode access
EtherSwitch1(config-if)# switchport access vlan 30
EtherSwitch1(config-if)# exit
```

4. Now that the VLAN have beend delcared and attached to the physical ports, they are considered as communication interfaces and can be shutdown or started.:

```
EtherSwitch1(config)# interface vlan 20
EtherSwitch1(config-if)# no shutdown
EtherSwitch1(config-if)# exit
EtherSwitch1(config)# interface vlan 30
EtherSwitch1(config-if)# no shutdown
```

5. Validate the etherswitch configuration with

```
EtherSwitch1# show vlan-switch
```



```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/2, Fa1/3, Fa1/4, Fa1/5
                                                Fa1/6, Fa1/7, Fa1/8, Fa1/9
                                                Fa1/10, Fa1/11, Fa1/12, Fa1/13
20   VLAN0020                         active    Fa1/0
30   VLAN0030                         active    Fa1/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
```

Here we can see what (physcial) ports are linked to what VLAN. Note that there always exist a VLAN1, also called management VLAN. This VLAN must never be used by the users (good practices).

Mission 1: VLAN isolation and trunking

The first part of this lab focuses on a scenario with a single switch (EtherSwitch1). Two VPCS are connected and must be relocated to VLAN 20 and VLAN 30 (layer 2 traffic separation).

Steps:

1. For this first step, PC1 and PC3 must be able to reach each other. This can be done by temporarily adjusting the netmask of PC1 and PC3 to /16 (so that they are on the same subnet).
   Note: Since we use the *VPCS* (instead of *ipterm*), the command differs slightly:

```
PC1> ip 192.168.20.2/16 192.168.20.1
```

In the beginning (no VLAN) PC1 and PC3 should be able to ping to each other. Validate this statement with a *ping* command.

2. Configure interface VLAN20 on port FastEthernet f1/0 and VLAN30 on f1/1. Now they are set apart. Validate through a ping between PC1 and PC3.

Do the same for the EtherSwitch2 with PC2 and PC4.

Note: Now do not forget to re-adjust the netmask of PC1 and PC3 to /24.

Mission 2: Trunking

VLAN are a logical separation on a single switch. It is possible to extend the L2 topology by transporting the VLANized traffic accross multiple and preserving the VLAN tag. This is called trunking. A port (or multiple ports) can be designated as a trunk between two switches. This is done via the commands:

```
EtherSwitch1(config)# configure terminal
EtherSwitch1(config)# interface fastEthernet 1/15
EtherSwitch1(config-if)# switchport mode trunk
EtherSwitch1(config-if)# switchport trunk allowed vlan all
EtherSwitch1(config-if)# no shutdown
```

And likewise on the other switch.

Note that it is possible to transport all VLANs or a limited set of VLANs (depending on the topology consideration and security needs). A good practice is to limit oneself to the minimum amount of VLANs needed.

Validate:

- By pinging (PC1 to PC2 on the same VLAN but different switches)
- Via Wireshark. Start a capture on the trunk line. Ping between PC1 and PC2. Stop the capture and analyze the traffic, look for ICMP echo ping packets and click on it. For this packet, open the 802.1Q header (between Ethernet and IP headers) and validate that the tag ID is 20.

Some final comments:

- VLAN are implemented by means of a 12-bits tag written in the Ethernet header. Therefore it is very sensitive to attacks (e.g., overwriting of the dot1q value on the trunk line). This attack is called VLAN hopping.
- Management VLAN is always active (in case you screw the configuration and cut the network in parts :-)). This is also on that VLAN that the switch has its IP address (if L3 switch).

Mission 3: Inter-VLAN routing

VLAN are disjoint LANs, one must use a router to flow the traffic between these LANs (remember that each vlan can be seen a separate interface, with its own range of IP address). Here we will connect a router to the **trunk lines** of the switches and allow inter-vlan routing . This is called a **router on a stick** topology.

1. Transform an interface to a switchport:

```
EtherSwitch1# configure terminal
EtherSwitch1(config)# interface fastEthernet 1/14
EtherSwitch1(config-if)# switchport mode trunk
EtherSwitch1(config-if)# switchport trunk allowed vlan all
EtherSwitch1(config-if)# no shutdown
EtherSwitch1(config-if)# exit
```

2. On the **router**, activate the VLANs and give an IP address to each VLAN interface on the router (do not forget that routers are L3 equipments !)

```
Router# configure terminal
Router(config)# interface fastEthernet 1/0
Router(config-subif)#no shutdown
Router(config-subif)# exit

Router(config)# interface fastEthernet 1/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface fastEthernet 1/0.30
Router(config-subif)# encapsulation dot1Q 30
Router(config-subif)# ip address 192.168.30.1 255.255.255.0
Router(config-subif)# end
```

Validate:

1. Ping between the PC1 and the router interface(s).
2. Ping between the PC1 and the PC3. Though they are on separate VLANs, this is now possible. **Why ? What is the path followed by the packets ?** What is the impact on the bandwidth ? What are the opportunities (in terms of security) offered by that inter-VLAN routing ?
3. With wireshark, monitor the ***stick line***, i.e., connection between EtherSwitch1 and the router. When pinging from PC1 to PC3 you should see packets moving PC1->router interface VLAN202 -> router interface 30 -> PC3.