DOCUMENTATION

VLAN Configuration and Troubleshooting, EtherChannel configuration & OSPF configuration

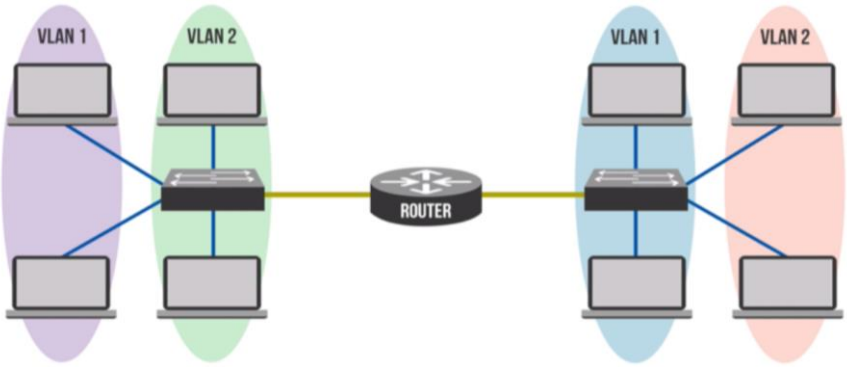
KAREEM DIAA HELAL
WE SCHOOL FOR APPLIED TECHNOLOGY
Day 3 of Telecommunications Training

Day 3: VLAN, EtherChannel, and OSPF Configurations

LAB 1: VLAN Configuration and Troubleshooting

1.1 What is VLAN and its importance?

A VLAN (Virtual Local Area Network) is a logical grouping of network devices that allows them to communicate as if they were on the same physical network, regardless of their actual location. Importance of VLANs: higher security, higher performance, increases the number of broadcasts, and more flexibility.



1.2 Configuring the initial basic switch configuration

At the beginning of every network device, we must configure the initial basic configuration, here is the basic network configuration:

Switch> enable
Switch# configure terminal
Swicth (config)# hostname SW2
SW2 (config)# line console 0
SW2 (config-line)# password comm
SW2 (config-line)# login
SW2 (config-line)# exit
SW2 (config)# Eenable secret we123
SW2 (config)# banner motd "Don't touch my switch!"

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW2
SW2(config)#
SW2(config)#
SW2(config)#
SW2(config)#
SW2(config)#
SW2(config)#line console 0
SW2(config-line)#password comm
SW2(config-line)#login
SW2(config-line)#ex
SW2(config-line)#exit
SW2(config)#enable sec
SW2(config)#enable secret we123
SW2(config)#banner motd "Kareem, Don't touch my switch!"
```

1.3 Creating VLANS and specifying them for their purpose

To create a vlan, follow the following steps:

SW2 (config)# vlan 10
SW2 (config-vlan)# name it

An the same for both vlan 20 and vlan 30:

SW2 (config)# vlan 20
SW2 (config-vlan)# name comm
SW2 (config-vlan)# exit
SW2 (config)# vlan 30
SW2 (config-vlan)# name hr

```
SW2(config)#vlan 10
SW2(config-vlan)#name it
SW2(config-vlan)#exit
```

```
SW2(config)#vlan 20
SW2(config-vlan)#name comm
SW2(config-vlan)#exit
```

```
SW2(config)#vlan 30
SW2(config-vlan)#name hr
SW2(config-vlan)#exit
```

1.4 Assign each port to its specified VLAN

There are two types of modes that exists in the switchport:

i. **Access mode:**

The access mode is used to connect end devices such as PCs that belong to a single VLAN and the port carries traffic for only one VLAN, and all frames that pass through are untagged.

ii. **Trunk mode:**

The trunk mode is used to connect switches to each other or to other network devices that need to handle multiple VLANs. The trunk mode carries traffic for multiple VLANs. VLAN tags are used to identify which VLAN each frame belongs to. The default native VLAN is VLAN 1, and traffic for the native VLAN is sent untagged.

For the switch ports that will be connected to the PCs, they will have the access mode as shown in the figure:

```
SW2(config)#int range g1/0/1-2
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 10
SW2(config-if-range)#exit
```

In this configuration, the interfaces GigabitEthernet 1/0/1 and 1/0/2 will be in vlan 10 and they are access mode.

The interfaces GigabitEthernet 1/0/3 and 1/0/4 will be also access mode but in vlan 20:

```
SW2(config)#int range g1/0/3-4
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 20
SW2(config-if-range)#exit
```

The interfaces GigabitEthernet 1/0/5 and 1/0/6 will be also access mode but in vlan 30:

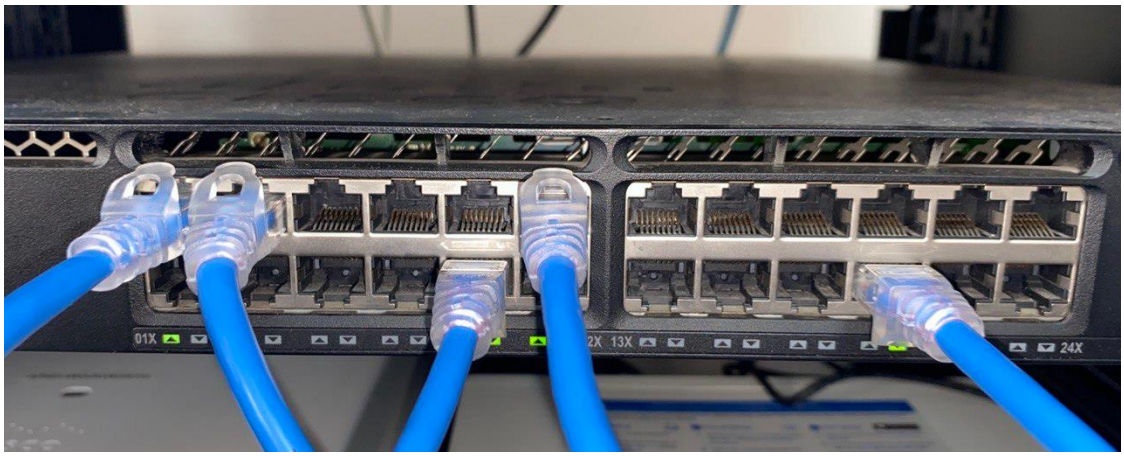
```
SW2(config)#int range g1/0/5-6
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 30
SW2(config-if-range)#exit
```

And the interfaces connected to the other switches will be trunk mode and automatically will be in vlan 1 as shown. The interfaces GigabitEthernet 1/0/10 is connected to a switch and GigabitEthernet 1/0/11 is connected to a Multilayer Switch.

```
SW2(config)#int range g1/0/10-11
SW2(config-if-range)#switchport mode trunk
SW2(config-if-range)#exit
```

The interface GigabitEthernet 1/0/20 is connected to another switch which will also be trunk:

```
SW2(config)#interface g1/0/20
SW2(config-if)#switchport mode trunk
```



For the Multilayer switch configuration, we must also configure the vlans on it and verify them but will be given an IP address and a subnet mask to make the vlans communicate with each other:

1. **Configuring vlan 10 on the L3 switch:**

```
Switch(config)#interface vlan 10
Switch(config-if)#no shut
Switch(config-if)#ip add 192.168.10.1 255.255.255.0
```

Here we gave the vlan 10 an ip address and a subnet mask and then started it to be available on the network. We will do the same for vlan 20 and vlan 30 on the L3 switch.

2. **Configuring vlan 20 on the L3 switch:**

```
Switch(config)#interface vlan 20
Switch(config-if)#ip add 192.168.20.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
```

3. **Configuring vlan 30 on the L3 switch:**

```
Switch(config)#interface vlan 30
Switch(config-if)#no shut\
*Jan  2 01:25:54.203: %LINEPROTO-5-UPDOWN: Line protocol
o shut
Switch(config-if)#ip add 192.168.30.1 255.255.255.0
Switch(config-if)#no shut
```

Alright! but there will be a simple command to write on the L3 switch to make the PCs at each vlan communicate with each other which is:

Switch (config)# ip routing

```
Switch(config)#ip routing
```

1.5 Pinging and troubleshooting

Before pinging, we have to check for the ip addresses that are assigned to each vlan. As shown in the figure, each ip address is assigned to its vlan successfully:

```
Switch(config)#do show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES unset  administratively down down
Vlan10                 192.168.10.1    YES manual up                    up
Vlan20                 192.168.20.1    YES manual up                    up
Vlan30                 192.168.30.1    YES manual up                    up
```

Here we used the command "show ip interface brief" to check each interface and its assigned ip address.

And now it’s time to ping the PCs with each other to check the connectivity:

```
C:\Windows\system32>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

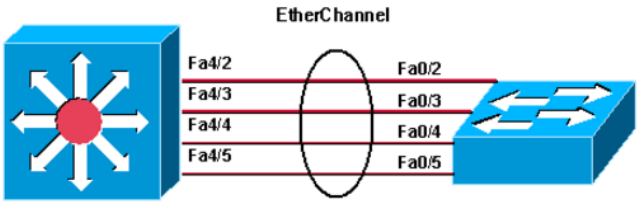
```
C:\Windows\system32>ping 192.168.20.20

Pinging 192.168.20.20 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.20: bytes=32 time<1ms TTL=127
Reply from 192.168.20.20: bytes=32 time<1ms TTL=127
Reply from 192.168.20.20: bytes=32 time<1ms TTL=127
```

As you can see that the connectivity is successful and now any device in vlan 10, 20, or 30 can communicate with any vlan in the network.

LAB 2: EtherChannel Configuration

EtherChannel is a port link aggregation technology or port-channel architecture used primarily on Cisco switches. It allows grouping of several physical Ethernet links to create one logical Ethernet link for the purpose of providing fault-tolerance and high-speed links between switches, routers and servers.



To implement an EtherChannel, you must first understand that there are two ways to use an EtherChannel link:

1. **LACP (Link Aggregation Control Protocol)**
   LACP is an IEEE standard defined in IEEE 802.3ad. LACP lets devices send Link Aggregation Control Protocol Data Units (LACPDUs) to each other to establish a link aggregation connection.
2. **PAgP (Port Aggregation Protocol)**
   PAgP is a proprietary specification designed and authored by Cisco.

The first thing to do is to combine the interfaces together to make the EtherChannel link using to following steps:

Switch (config)# interface range GigabitEthernet0/1 – 2

Switch (config-if-range)# channel-group 1 mode active

Switch (config-if-range)# interface port-channel 1

Switch (config-if-range)# switchport trunk encapsulation dot1Q

```
SW1(config-if)#interface range g3/0/1-2
SW1(config-if-range)#channel-group 2 mode desirable
SW1(config-if-range)#interface port-channel 2
SW1(config-if)#switchport trunk encapsulation dot1q
```

```
SW1(config)#interface range g3/0/3-4
SW1(config-if-range)#channel-group 1 mode active
SW1(config-if-range)#interface port-channel 1
SW1(config-if)#switchport trunk encapsulation dot1q
```

For the EtherChannel link, we have to understand that it cannot be two interfaces opposite to each other to be “Passive” in LACP or “Auto” in PAgP. It must be at least one active (or desirable) and one passive (or auto). And its better if the both interfaces are active (or desirable).

Important show command to use for ensuring the connectivity:

SW1# Show etherchannel summary

```
SW1#show etherchannel summary
```

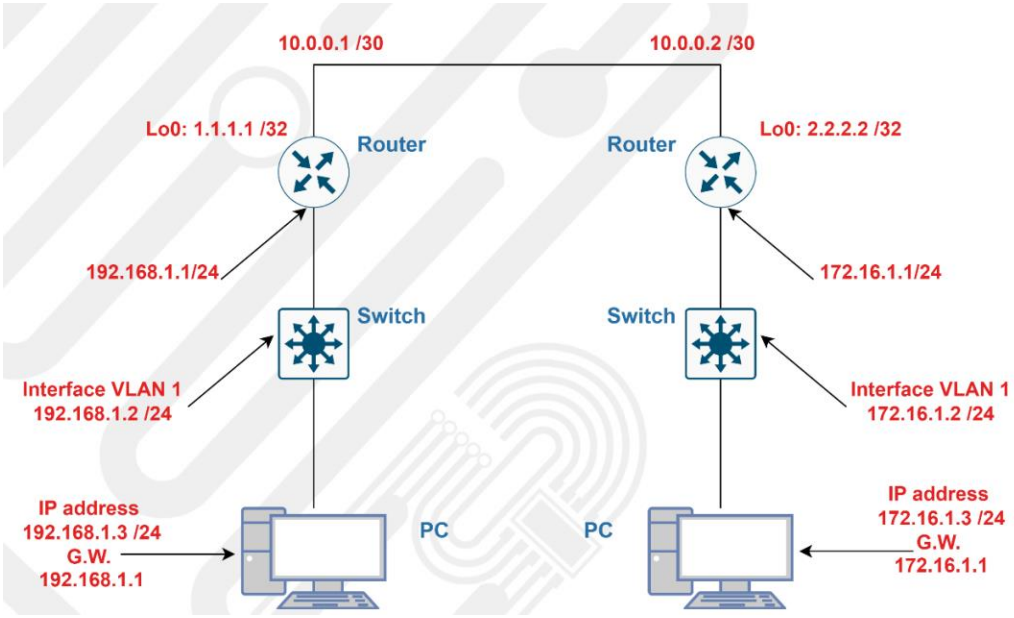
In the following output, we can see that the two ports are SU or State Up which means that our configuration was successful!

```
Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Gi3/0/3(P)  Gi3/0/4(P)
2      Po2(SU)         PAgP      Gi3/0/1(P)  Gi3/0/2(P)
```

LAB 3: OSPF Configuration

In this scenario, we will configure OSPF on the router and introduce a loopback interface to demonstrate its use and importance in OSPF:



The configuration on the PCs giving the addressing from the cmd:

```
C:\Windows\system32>netsh interface ip set address name="ethernet 2" static 192.168.30.30 255.255.255.0 192.168.30.1

C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8006:c8a5:4839:272e%10
   IPv4 Address. . . . . . . . . . . : 192.168.30.30
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.30.1
```

The configuration on the switches:

vlan 10
name IT
exit
vlan 20
name comm
exit
interface GigabitEthernet 0/1
switchport mode trunk
no ip address
no shutdown
interface GigabitEthernet 0/0
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0

Then, you should configure the loopback interface:

Interface loopback 1
Ip address 100.1.1.1 255.255.255.255

```
Router(config)#interface loopback 1
Router(config-if)#ip add 200.1.1.1 255.255.255.255
```

After that, you should implement the OSPF on each router. For short, here is the OSPF configuration for router 1 and it will be similar to the other one:

Router ospf 1
Network 200.1.1.1 0.0.0.0 area 0
Network 10.1.1.0.0 0.0.0.3 area 0
Network 11.1.1.0.0 0.0.0.3 area 0

```
Router(config)#Router ospf 1
Router(config-router)#network 11.1.1.0 0.0.0.3 area 0
Router(config-router)#network 10.1.1.0 0.0.0.3 area 0
Router(config-router)#network 200.1.1.1 0.0.0.0 area 0
```

Finally, you should configure a command to let the internal router to send the packet to the main router if the destination is not in the internal network, which is the purpose of the following command:

IP default-gateway 200.1.1.1

Pinging to ensure the connectivity:

```
Router(config)#do ping 192.168.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Router(config)#do ping 192.168.20.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Router(config)#do ping 192.168.30.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Router(config)#do ping 192.168.40.40
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.40, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router(config)#
```

And pinging the loopback interface for checking up:

```
Router(config)#do ping 200.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router(config)#
```

Question and Answer (Q&A) Section based on the previous configurations:

LAB 1 Q&A:

- What steps did you take to ensure that VLAN 30 can communicate with other VLANs?
    1. Use the multilayer switch (to act as the gateway of the network)
    2. Assign an ip address and a subnet mask for each vlan on the multilayer switch
    3. Use the command "No shutdown" to make the vlans up state
    4. And finally, use the command "ip routing" to ensure that data can be transmitted between the different vlans on the network.

```
Switch(config)#ip routing
```

- Why is it important to keep the Management VLAN isolated, and how did you verify this in your configuration?
  The management vlan is used for network administration tasks. Keeping it isolated ensures that unauthorized devices cannot access sensitive network management interfaces, which protects the network from threats.
  I verified isolation by ensuring that the management vlan was not allowed on trunk links used by other vlans and that only authorized devices had access to this VLAN.

- If a ping from the HR PC to another VLAN fails, what troubleshooting steps would you take to identify and resolve the issue?
    1. Use the multilayer switch (to act as the gateway of the network)
    2. Assign an ip address and a subnet mask for each vlan on the multilayer switch
    3. Use the command "No shutdown" to make the vlans up state
    4. And finally, use the command "ip routing" to ensure that data can be transmitted between the different vlans on the network.

```
Switch(config)#ip routing
```

LAB 2 and 3 Q&A:

- What would happen if the loopback interface was not advertised in OSPF?
  The loopback interface wouldn't be reachable by other routers in the OSPF network, which could lead to routing issues or loss of communication with the router's services.
- Why is it important for the router's loopback interface to be stable and always up in OSPF?
  The loopback interface is used as the router's ID in OSPF. It ensures consistent and stable routing, making the network more reliable.
- How can you troubleshoot if a device in one VLAN cannot reach the loopback interface?
  Check the device's IP configuration, verify VLAN and trunk configurations, ensure OSPF is correctly configured, and make sure the loopback interface is advertised in OSPF.
- What benefits does OSPF provide in a network like this, compared to static routing?
  OSPF automatically adjusts to changes in the network, finds the best paths, and scales better for larger networks, unlike static routing, which requires manual updates.