universidade de aveiro
theoria poiesis praxis

DEPARTAMENTO DE ELECTRÓNICA, TELECOMUNICAÇÕES E INFORMÁTICA
LICENCIATURA EM ENG. DE COMPUTADORES E INFORMÁTICA

REDES DE COMUNICAÇÃO I

LAB GUIDE 03

SWITCHING AND VLANS

Objectives

- Ethernet technology (Switching)
- The Virtual LAN (VLAN) concept
- Analysis of the IEEE802.1Q VLAN protocol
- Interconnection of VLANs

Duration

2 weeks

In the end of the class, send your report to your Professor.

Part 1

1. Lab Equipment for this guide

Figure 1: Cisco Routers 2500 series (two different hardware versions, same functionality)

Figure 2: Switch D-LINK DES-3010G

Figure 3: Cisco Console Cable with RJ45 and DB9F

Figure 4: USB to RS232 Serial DB9 Cable adapter

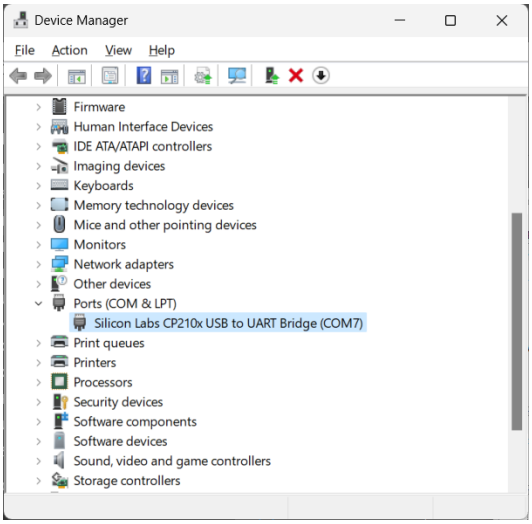
Figura 5: Ethernet Cable

To access the Cisco routers console (via putty or equivalent) you must use the cables from figure 3 and figure 4.
To access the D-LINK switch console (via putty or equivalent), you must use the cable from figure 4.

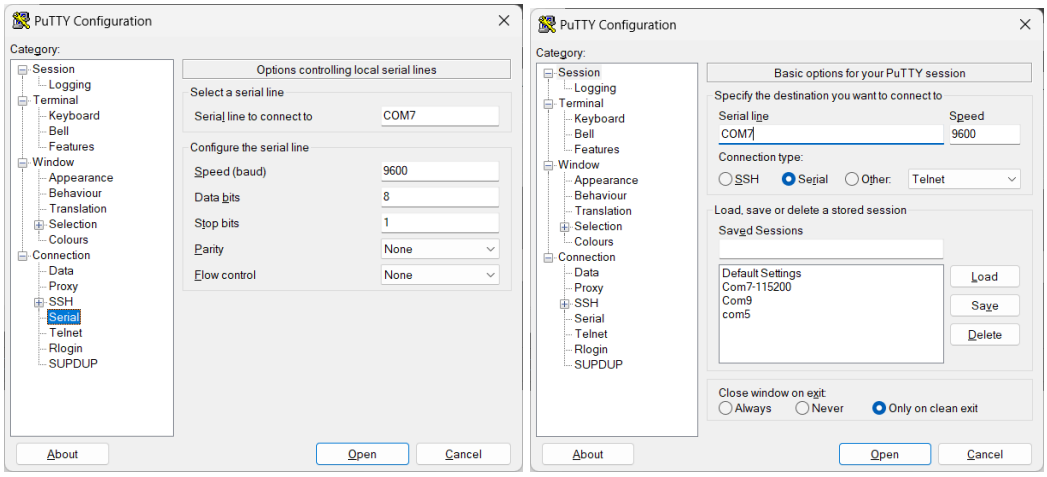
2. Using a terminal application (e.g putty) to access the console of equipment

In order to access the routers and switches console ports you will need to use a USB serial adapter (Figure 4).

On windows, depending on the adapter you are using, you will need to find it on the device manager, under "Ports" (COM & LPT) to identify the right COM port:



To access the routers and switches console, you need to configure it as shown below:



For Linux, use **picocom or PuTTY**:

```
sudo apt install picocom
sudo picocom -b 9600 /dev/ttyUSB0
```

(check under /dev which is the ttyUSB**x** you have)

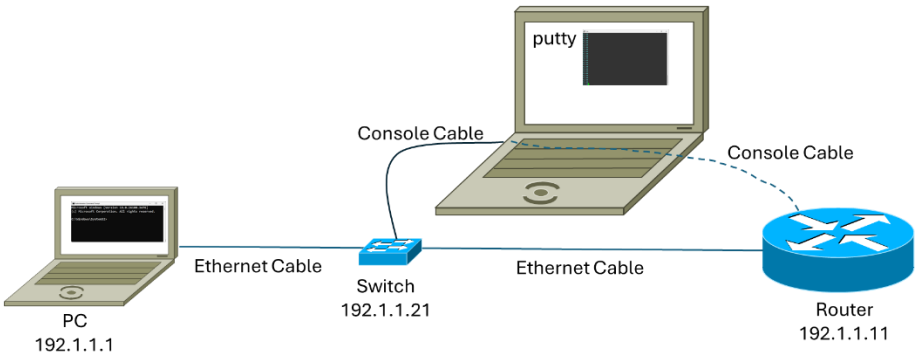
Putty is also available for Linux, if you desire:

```
sudo apt update
sudo apt install putty
```

For macOS:

PuTTY is not natively available for macOS, but you can use alternatives like Terminal or iTerm2 for SSH connections. If you prefer, you may install PuTTY as well.

3. Experiments with Switches



1. Build and configure the network above with the equipment in the la
2. b (you can use your own PC). Run the command ping –t (pings without stopping) for the router. (All configurations' examples are in the "Commands Guide"):

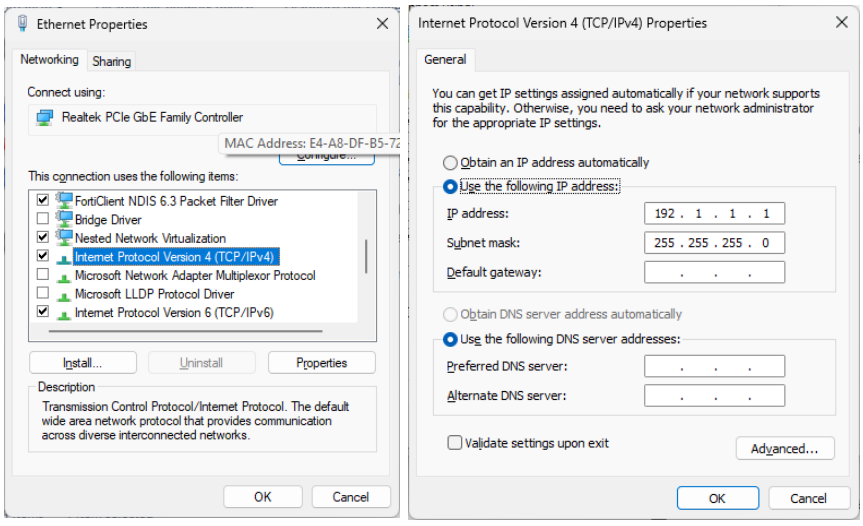
a) **D-LINK Switch**: **# config ipif System ipaddress 192.1.1.21/24**

b) **Cisco**:

Router> **enable**
Router# **configure terminal** // conf t
Router(config)# **interface FastEthernet0/0** // Enter interface configuration mode
Router(config-if)# **ip address 192.1.1.11 255.255.255.0** // Assign IPv4 address
Router(config-if)# **no shutdown** // Enable the interface
Router(config-if)# **exit** // ^Z
Router# show run // View the current router configuration

c) **PC (windows)**:

On the search bar type and open "view network connections" (ver ligações de rede) Identify the Ethernet network adapter, right click it, open properties, choose IPv4 and click on properties:



d) **PC (linux)**: **sudo ifconfig eth0 192.1.1.1 netmask 255.255.255.0**
(you must check which interface you have: #sudo ifconfig //to see all available interfaces)

3.1. Aging

1. After configuring the network, test the connectivity between all equipment using the ping command.

2. Execute again the *ping* command between PC and Router. Access the management console of the Switch using the *Web Browser (http://192.1.1.21)*. Analyse the *MAC Address Table* of the Switch and register its contents (MAC address and Ethernet address are equivalent terms). Observe that the Switch has learned on each port the MAC addresses of the equipment connected to the same port.
   ➔ Confirm on the PC and on the Router that their MAC address are the ones learned by the Switch.

3. Each entry of the *MAC Address Table* has a lifetime value that is set to zero whenever the Switch receives an incoming packet on the same input port with the same origin MAC address. During time, if an entry lifetime reaches the *Aging Time* value, the entry is eliminated (the *Aging Time* value can be configured on the Switch).
   ➔ Using the *Web Browser* access, check the default *Aging Time* value of the Switch.

4. Using the *Web Browser* access, configure an *Aging Time* value of 10 seconds. Then, wait for about 20 seconds and check if the PC MAC address entry has disappeared from the *MAC Address Table*.
   ➔ Observe that, apparently, this entry does not disappear.

NOTE: The Router MAC address does not disappear from the MAC Address Table due to the fact that routers send periodically (from 10 to 10 sec.) a LOOPBACK packet to check for physical connectivity; these packets are continuously validating the Router MAC address on the Switch.

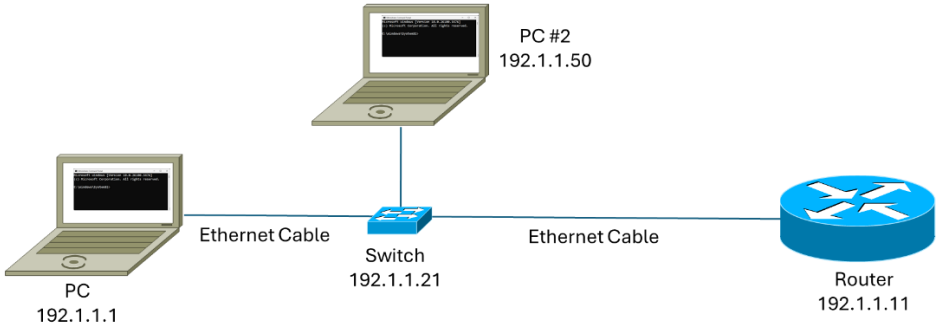
5. Close the Web Browser and connect to the management console of the Switch through its console (using the serial interface – "putty"). Examine again the MAC Address Table (command: "**show fdb**"). Check that, in this experiment, the PC MAC address disappears from the table.
   ➔ Justify the different behaviour observed in these two experiments (4 and 5).

3.2. Flooding and Forwarding

Remember from the theoretical classes that, when a Switch receives a packet on an incoming port, it searches for an entry with the packet destination MAC address on its MAC Address Table. Then, the behaviour of the Switch is one of two possibilities:

- Flooding process: no such entry exists and the Switch sends the packet to all its ports, except the incoming port.
- Forwarding process: the entry exists and the Switch sends the packet only for the port specified on the MAC Address Table entry, if it is not the incoming port.

The aim of the 2 next experiments is to verify the Switch basic flooding and forwarding processes.



1. Add to your network a connection to 2nd PC (lab PC or PC of your colleague) connected to the switch.
   ➔ Test the connectivity by executing a ping command from the Router to the PC#2.

2. Check if the entry of PC #2 is no longer on the switch fdb. If by any chance, PC #2 is sending any packets on the ethernet interface, its entry will not disappear (the switch keeps learning it with every received packet).

3. With WireShark, start a capture on both PCs, with a display filter for ICMP packets. Execute once again the ping command from the Router to PC#2.
   ➔ Register the captured packets.

   Note that the ping command has generated the exchange of 5 ICMP Echo Request and 5 ICMP Echo Reply packets between the Router and the PC#2. Nevertheless, the capture run on the PC has only one ICMP Echo Request packet.
   ➔ Explain these observations based on the Switch flooding and forwarding processes

4. VLAN Switching

Note: In GNS3, a Layer 2 switch can be implemented (i) with a basic device (Ethernet switch device) that does not have console and does not support the Spanning Tree Protocol, or (ii) with a switching module in a router (EtherSwitch router device). This guide will use the latter, EtherSwitch router as Layer 2 switch using only the switching module ports (e.g., F1/0 to F1/15).

Please refer to the annex for more information on how to configure VLANs on the ESW and on a regular Cisco Router

4.1. Experiments with Virtual LANs – Mode Access and interfaces VLAN

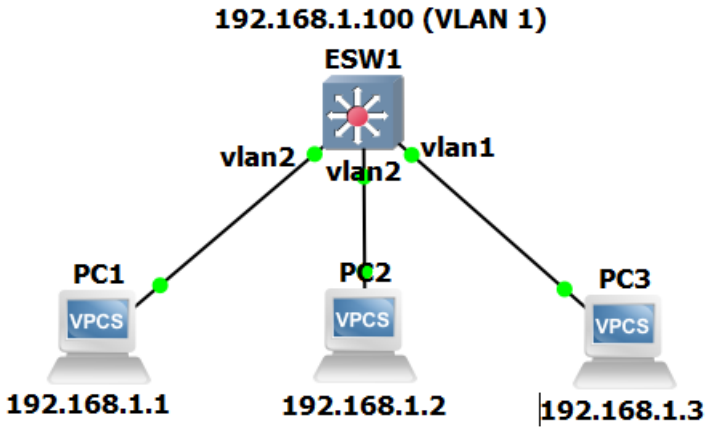


Figure 1

4.1.1. Set up the network shown in the figure above and configure all IP addresses with netmask 255.255.255.0. In Switch 1, check that the Spanning Tree protocol is disabled and configure two VLANs in the following way:

a) Ports numbered F1/5 to F1/8 belonging to VLAN 2 (must be created):

i - Create VLAN2:

ESW1# vlan database
ESW1(vlan)# vlan 2
ESW1(vlan)# exit

ii - Configure Switch ports (in this case, a range, but you can configure only one) to belong to VLAN2, in access mode:

ESW1# configure terminal
ESW1(config)# interface range F1/5 - 8
ESW1(config-if-range)# switchport access vlan 2
ESW1(config-if-range)# end
ESW1# write

b) all other ports belong to VLAN 1 (that is the default/native VLAN)

c) Configure an IP address for VLAN 1 and enable the VLAN

ESW1# configure terminal
ESW1(config)# interface vlan 1
ESW1(config-if)# ip address 192.168.1.100 255.255.255.0
ESW1(config-if)# no shutdown
ESW1(config-if)# end
ESW1# write

IMPORTANT: AFTER THE VLANS AND INTERFACES ARE CONFIGURED, IT IS NECESSARY TO WRITE THE CONFIGURATION (ESW#write) AND AFTER THAT, STOP AND START AGAIN THE L3 SWITCH.

Do this every time you add VLANs to the database and/or you modify the configuration of the switchports

To verify the VLAN associated with each interface, use the command:

ESW1# show vlan-switch

> Note: Cisco equipment have VLAN 1002 to 1005 by default (for proprietary protocols) that cannot be deleted

4.1.2. Connect the PC1 and PC2 to VLAN 2 ports and PC3 to a VLAN 1 port, as shown in the figure above

4.1.3. From each equipment run the ping command to check which pairs of equipment (including Switch 1) have IP connectivity. Verify that only equipment in the same VLAN has IP connectivity.

4.1.4. Using the switch console, verify the Forwarding Table of Switch 1:

ESW1# show mac-address-table

Check that the VLAN information is in accordance with the network setup

4.1.5. Start captures on the links PC1-Switch1 and PC3-Switch1 and set an appropriate filter to display ARP and ICMP packets. Run the ping commands specified in the following table. For each run, register the connectivity and the filtered packets. Justify the results obtained on each case.

Ping from:	**Ping to:**	**Connectivity (yes or no)**	**Packets (PC1-Switch1 link)**	**Packets (PC3-Switch1 link)**
PC2	Switch1			
PC2	PC3			
PC2	192.168.1.34			
PC3	Switch 1			
PC3	PC2			
PC3	192.168.1.34			
Switch1	PC3			
Switch1	192.168.1.34			

4.2. Experiments with Virtual LANs – Mode Trunk and interconnection

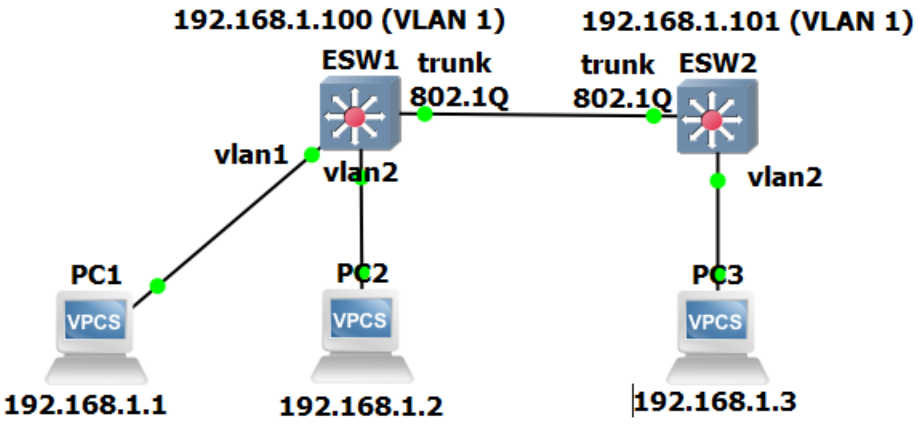


Figure 2

4.2.1. Reconfigure the network as specified in the figure above.

a) In the new inserted Switch 2, configure VLANs 1 and 2 in the same way as specified to Switch 1 in the previous experiments.

b) At both Switches 1 and 2, configure the ports connecting the switches as a trunk port (e.g., F1/15) in order to support both VLAN using the IEEE802.1Q VLAN protocol, as specified in the figure above.

ESW(config)# interface F1/15

ESW(config-if)# switchport mode trunk

4.2.2. Start new capture on the link Swicth1-Switch2 and set an appropriate filter to display ARP and ICMP packets. Run the ping commands specified in the following table. For each run, register the filtered packets and their VLAN ID value. Justify the results obtained on each case.

Ping from:	Ping to:	Connectivity (yes or no)	Filtered packets
PC1	Switch 1		
PC1	Switch 2		
PC1	PC2		
PC1	PC3		
PC2	Switch 1		
PC2	Switch 2		
PC2	PC2		
PC2	PC3		

Format of the Ethernet frames with and without 802.1Q tags

Ethernet frame without 802.1Q tag

Destination Address (6 *bytes*)
Source Address (6 *bytes*)
Type / Length (2 *bytes*)
Data Field

Ethernet frame with 802.1Q tag

Destination Address (6 *bytes*)
Source Address (6 *bytes*)
8100h (2 *bytes*)
Priority (3 *bits*)
CFI (1 *bit*)
VLAN ID (12 *bits*)
Type / Length (2 *bytes*)
Data Field

802.1Q has 4 bytes more!

4.3. Experiments with Virtual LANs – Routing between VLANs – External

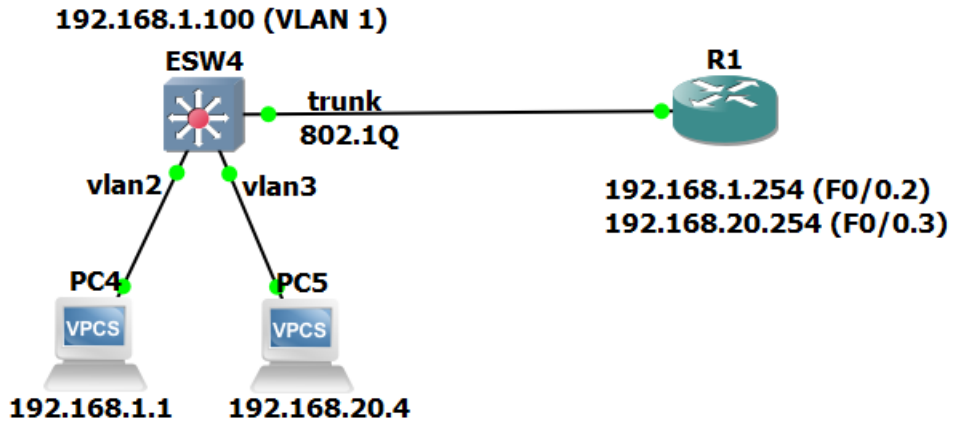


Figure 3

4.3.1. Reconfigure the network as specified in the figure above where the Router routes packets between VLAN 2 and VLAN 3 (each one with its own network IP address).

In Switch 4, configure the VLAN in the following way:

a) ports numbered F1/0 to F1/4 belonging to VLAN 3 (must be created);

ESW1# vlan database
ESW1(vlan)# vlan 3
ESW1(vlan)# exit
ESW1(config)# interface range F1/0 - 4
ESW1(config-if-range)# switchport access vlan 3

b) ports numbered F1/5 to F1/8 belonging to VLAN 2;

c) all other ports belonging to VLAN 1 (the default/native VLAN)

4.3.2. In the Router, create 2 virtual interfaces on interface F0/0, one for VLAN 2 (F0/0.2) and another for VLAN 3 (F0/0.3), with the given IP addresses:

Router (config)# interface F0/0
Router (config-if)# no shutdown
Router (config-if)# interface F0/0.2
Router (config-subif)# encapsulation dot1Q 2
Router (config-subif)# ip address 192.168.1.254 255.255.255.0
Router (config-if)# interface F0/0.3
Router (config-subif)# encapsulation dot1Q 3
Router (config-subif)# ip address 192.168.20.254 255.255.255.0

4.3.3. In both PCs, configure the appropriate the IPv4 address and Default Gateway address.

For PC4:

PC-4> ip 192.168.1.1/24 192.168.1.254

4.3.4. To verify the correctness of the configurations, check the IP connectivity between PC4 and PC5 with the ping command. Register and justify the IP routing table of the Router.

Use the command to view the IPv4 routing table:

Router# show ip route

4.3.5. Start new capture on the link Swicth1-Router and set an appropriate filter to display ARP and ICMP packets. Run the ping commands specified in the following table. For each run, register the filtered packets and their VLAN ID value. Justify the results obtained on each case.

Ping from:	**Ping to:**	**Connectivity (yes or no)**	**Filtered packets**
PC4	Switch 4		
PC4	Router		
PC4	PC5		
PC4	192.1.1.100		
PC5	Switch 4		
PC5	Router		
PC5	PC4		
PC5	192.1.1.100		

4.4. Experiments with Virtual LANs – Routing between VLANs – Internal

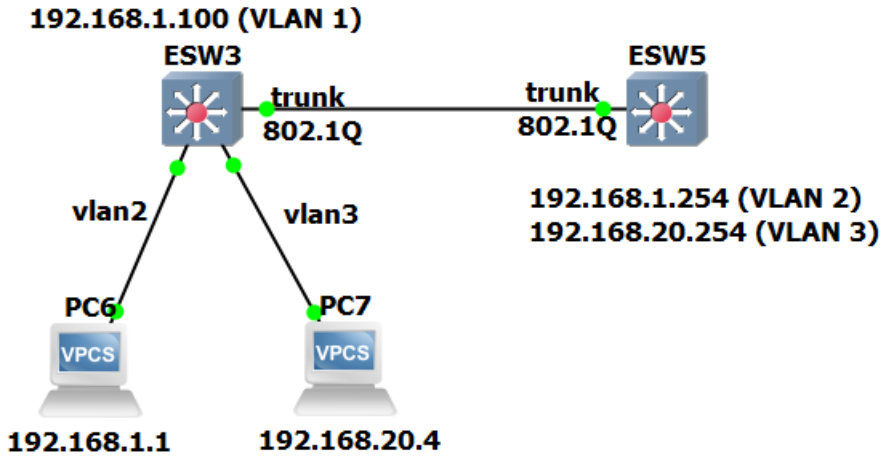


Figure 4

The previous network connectivity can be implemented using internal routing between VLANs within the L3 Switch.

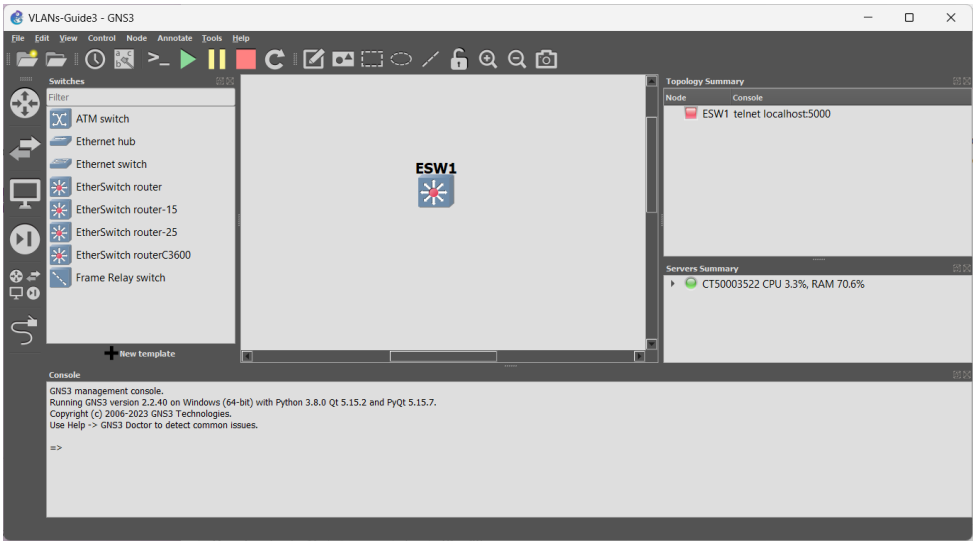
In Vlans 2 and 3, configure the right IP address which will be used as gateways. This is the way to use 1 cable of the switch in different networks, comparable to the sub-interfaces of the router:

```
ESW5# vlan database
ESW5(vlan)# vlan 2
ESW5(vlan)# vlan 3
ESW5(vlan)# exit

ESW5(config)# interface vlan 2
ESW5(config-if)# ip address 192.168.1.254 255.255.255.0
ESW5(config-if)# no shutdown

ESW5(config)# interface vlan 3
ESW5(config-if)# ip address 192.168.20.254 255.255.255.0
ESW5(config-if)# no shutdown

ESW5(config)# interface F1/15
    ESW5(config-if)# switchport mode trunk
```

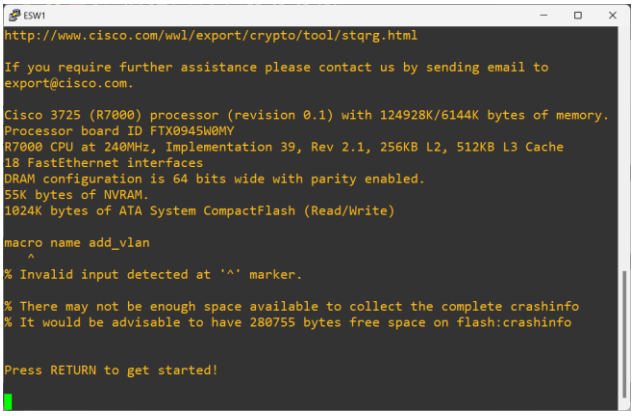
5. ANNEX – VLANs on a ESW and on a Router

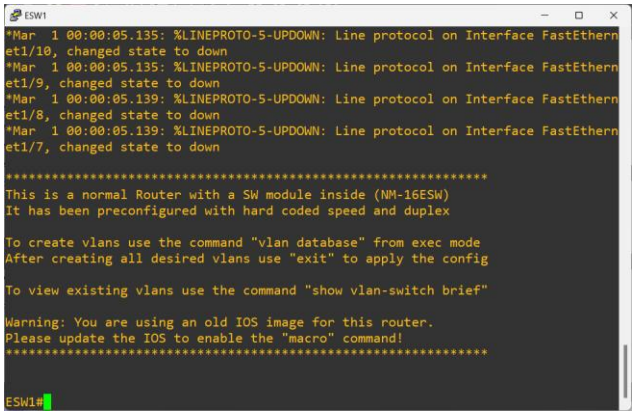
5.1. Introduction to the ESW Cisco Switch Router (L3 Switch)

Create a new project for the VLANs Guide and add an EtherSwitch router (ESW1):

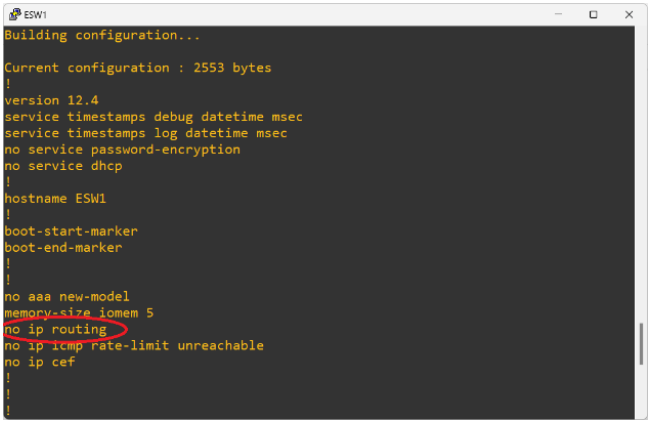


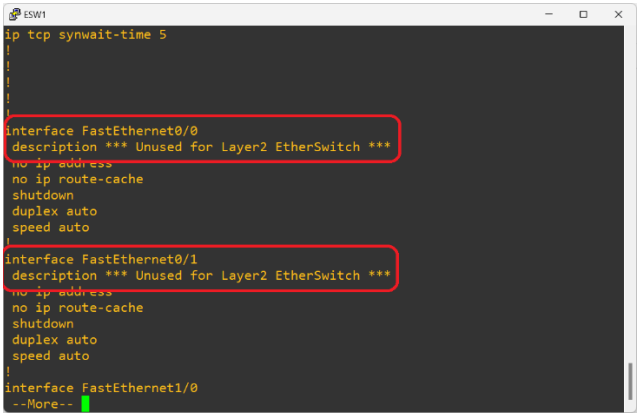
Start the device and right click over it to open the console:





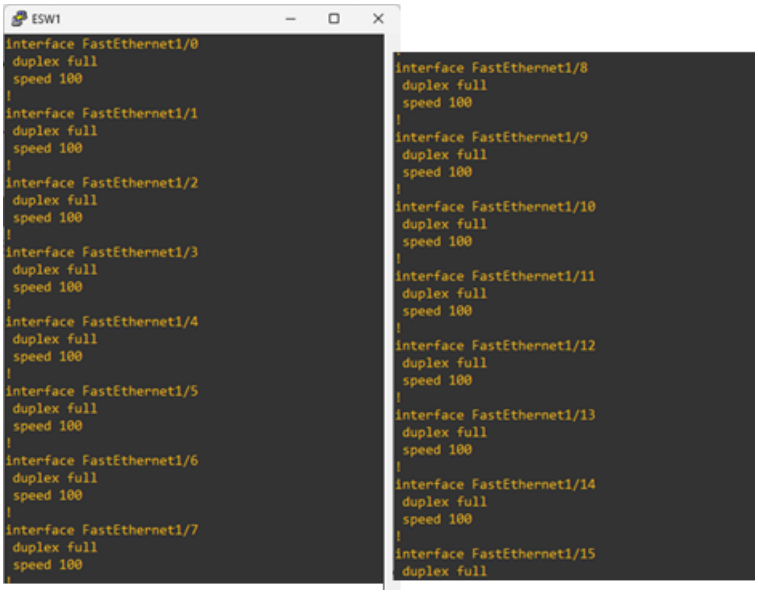
Do a show run to check its configuration, with special attention to the available interfaces.



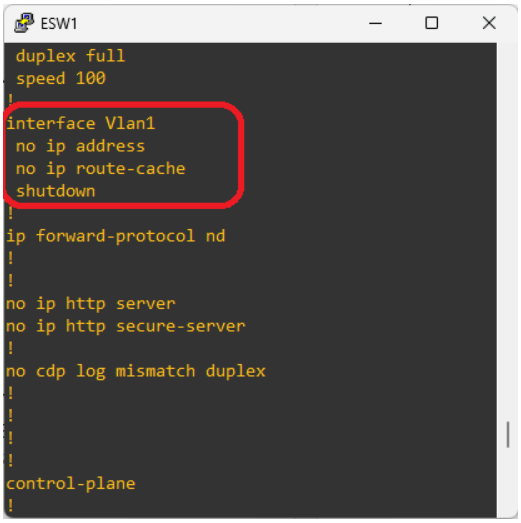


Note that:

- By default, this device will not work as a router. You will need to enable the routing engine.
- There are two interfaces (F0/0 and F0/1) that are ROUTING interfaces only. They should NOT BE USED for switching purposes.

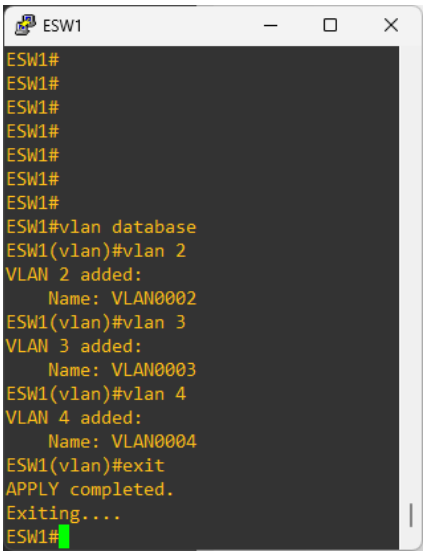


There are 16 interfaces (from F1/0 to F1/15) that "belong" to a switch card interface on the router, and these are the interfaces used for switching and VLANs.

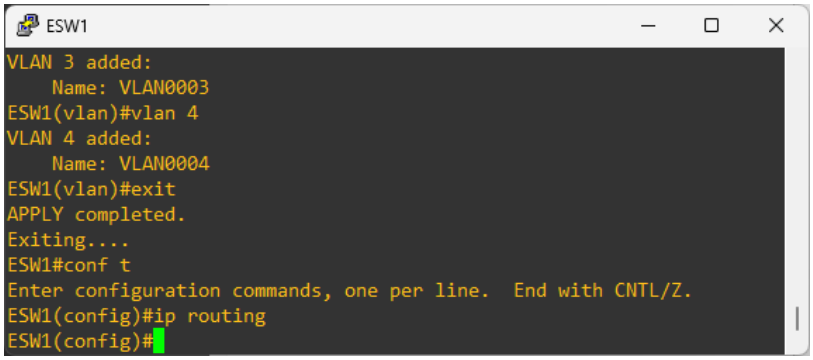


By default there is a Vlan1 interface, through which all switch ports belonging to the Vlan1 may do routing to the other routing interfaces (F0/0 and F0/1). Note that this interface is in "shutdown" by default. In order to be used, you have to do the "no shutdown" to it.

In order to have more Vlan interfaces, they must be added to the Vlan database according to the needs:



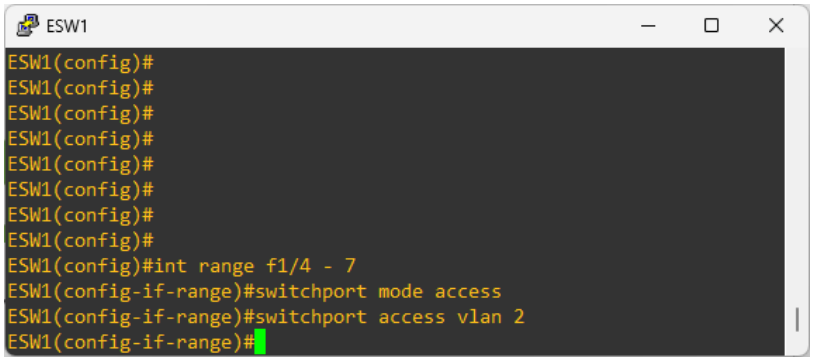
Enabling IP Routing functions on this device:



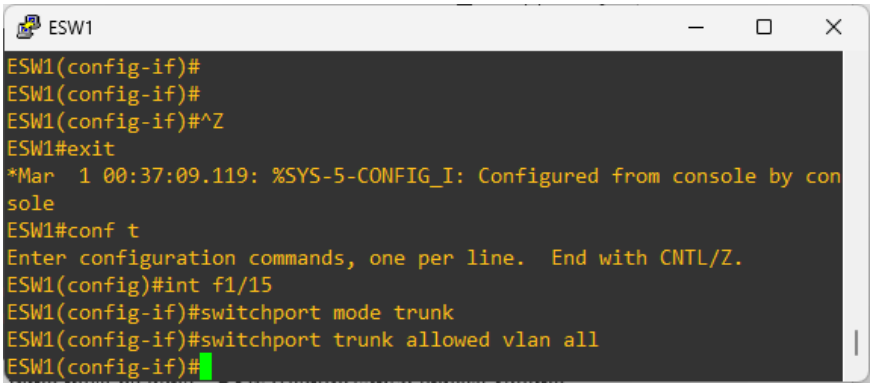
Note: for IPv6 the same thing must be done. “ESW1(config)#ipv6 unicast-routing”

Putting a switch port in access mode and associating it to a specific VLAN:

Applying the same configuration to a range of interfaces (F1/4, F1/5, F1/6 and F1/7):



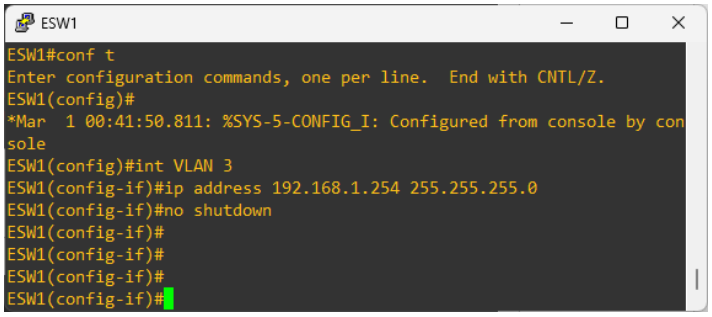
Putting a port in TUNK mode and allowing all configured VLANs to be able to come in and out of that interface (you may restrict the port to some specific interfaces, if needed):



Note:

- Ports on access mode can only belong to one specific VLAN and the incoming and outgoing Ethernet frames DO NOT have VLAN TAG.
- Ports on trunk mode may input and output Ethernet frames from different VLANs and those Ethernet frames SHOULD BE TAGGED.

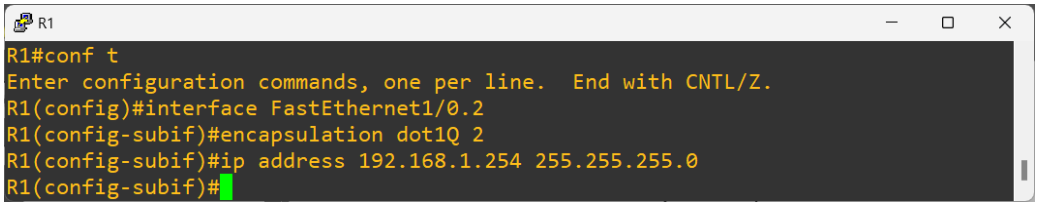
In order to have routing between VLANs, and Interface VLAN should be created and configured for each VLAN:



IMPORTANT: DUE TO A LIMITATION OF GNS3 WHEN USING THIS IOS AS A L3 SWITCH, AFTER THE VLANS AND INTERFACES ARE CONFIGURED, IT IS NECESSARY TO WRITE THE CONFIGURATION (ESW#write) AND AFTER THAT, STOP AND START AGAIN THE L3 SWITCH.

5.2. VLANs on Cisco 7200

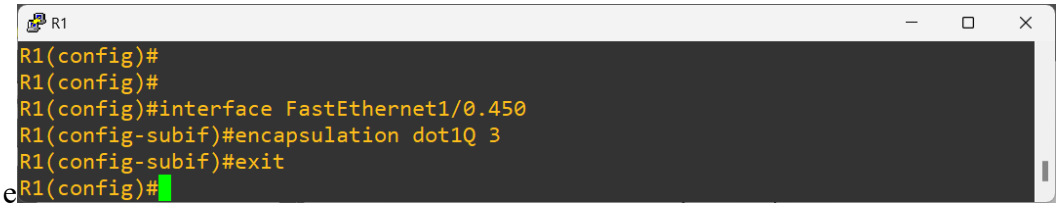
Configuring a regular router (e.g Cisco 7200) interface to send and receive Ethernet frames with VLANs



Note that a sub-interface was created (F1/0.2), belonging to the physical interface F1/0.

We then configured this sub-interface to send and receive tagged frames (with the command “encapsulation dot1Q” followed by the VLAN ID we want to use on this sub-interface)

We may add more sub-interfaces to the same physical interface (e.g. F1/0.3, F1/0.450, etc). The ID of the interface “.3”, “.450” may be different from the VLAN ID we want to use on that sub-interface:



e

To be able to use these sub-interfaces, the “mother” interface must be enabled: