Martim Calisto Pinheiro 112938 | Diogo Coutinho 113057

DEPARTAMENTO DE ELETRÓNICA, TELECOMUNICAÇÕES E INFORMÁTICA

LICENCIATURA EM ENG. DE COMPUTADORES E INFORMÁTICA

REDES DE COMUNICAÇÕES 1

LABORATORY GUIDE NO. 3

Objectives

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

Duration

- 1 week

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).

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

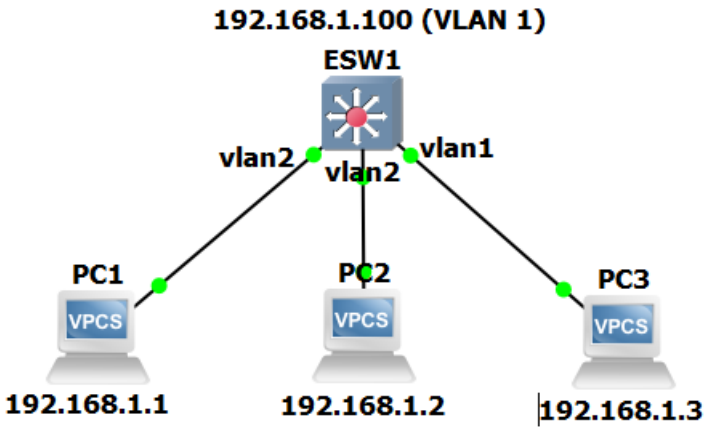


Figure 1

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):

ESW1# vlan database
ESW1(vlan)# vlan 2
ESW1(vlan)# exit
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 belonging to VLAN 1 (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

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

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

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.

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

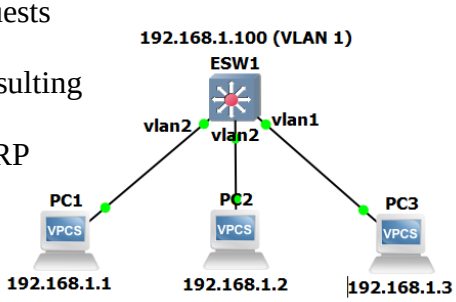
ESW1# show mac-address-table

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

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.

			(VLAN 2)	(VLAN 1)
Ping from:	**Ping to:**	**Connectivity (yes or no)**	**Packets (PC1-Switch1 link)**	**Packets (PC3-Switch1 link)**
1- PC2	Switch1	No	ARP	
2- PC2	PC3	No	ARP	
3- PC2	192.168.1.34	No	ARP	
4- PC3	Switch 1	Yes		ARP + ICMP
5- PC3	PC2	No		ARP
6- PC3	192.168.1.34	No		ARP
7- Switch1	PC3	Yes		ARP + ICMP
8- Switch1	192.168.1.34	No		ARP

1- No connectivity was made between the devices because PC2 is on vlan2 and switch1 has an ip address only at vlan1. ARP requests were made within the vlan2 but the requested ip was (predictably) not found.
2- PC's are on different vlans. Only at vlan2 (the origin of the request) ARP requests were executed.
3- IP pinged is not associated to any device on vlan. Thus, only ARP requests were made without reply.
4- PC3 and Switch1 are on the same vlan – connection was successful, resulting on the regular ARP and ICMP req. and replies.
5- PC's are on different vlans. Only at vlan1 (the origin of the request) ARP requests were executed.
6- Same occurence as in pt. 3.
7- Same occurence as in pt. 4.
8- Same reason as in pt. 3.



2. Experiments with Virtual LANs – Mode Trunk and interconnection

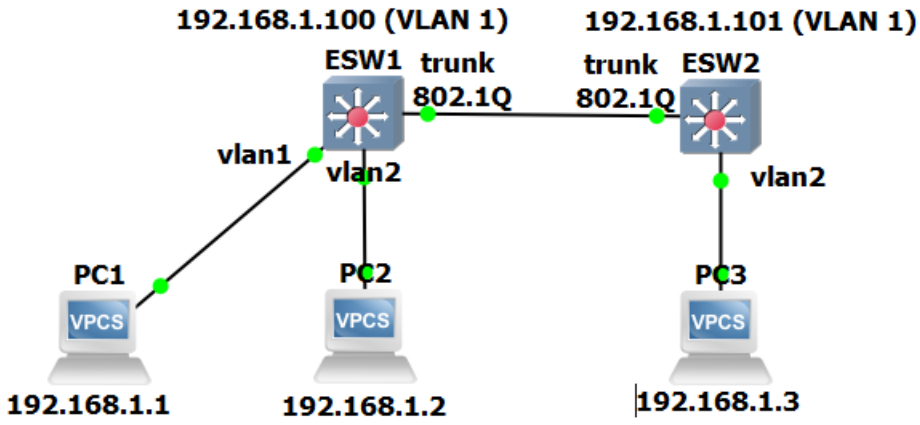


Figure 2

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

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
1- PC1	Switch 1	Yes	ARP request
2- PC1	Switch 2	Yes	ARP request and reply + ICMP request and reply
3- PC1	PC2	No	ARP request
4- PC1	PC3	No	ARP request
5- PC2	Switch 1	No	ARP request
6- PC2	Switch 2	No	ARP request
7-PC2	PC1	No	ARP request
8- PC2	PC3	Yes	ARP request and reply + ICMP request and reply

(Please check next page for justifications.)

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

1- Connection was successful, as both devices are on the same vlan. Since the analysis is happening between the Etherswitches, only the first ARP request is captured. The first ARP is broadcasted all network, in this case to ESW2, and then ESW1 answers, resulting on a successful ping.
2- PC1 and ESW2 are on the same vlan.
3- Devices are not on the same vlan.
4- Same situation as in pt. 3
5- Even though ESW1 has the interface of vlan2 defined, it does not have an ip address associated. Using the ip address registered on vlan (as expected) results on a failed ping request. Only ARP requests were passed through ESW to check if the requested ip was there. Any attempt to ping requires an ip address, and only vlan1 has an ip address defined at ESW1 and ESW2.
6- See pt. above.
7- Same situation as in pt. 3
8- Devices are on the same vlan and even though vlan2 is not yet configured as a network, the interface exists on ESW1 or ESW2, making the devices act like a “bridge” between them, allowing the ping to occur without any trouble.

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

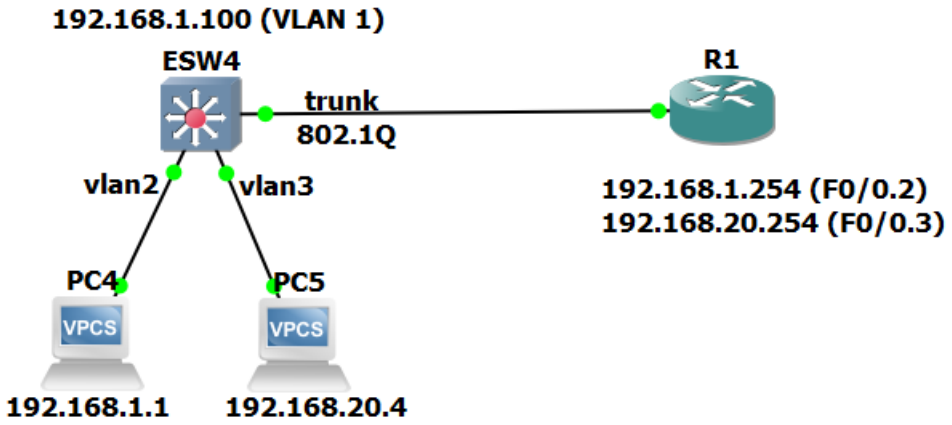


Figure 3

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)

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

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

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

C 192.168.20.0/24 is directly connected, FastEthernet0/0.3
C 192.168.1.0/24 is directly connected, FastEthernet0/0.2

The table represents both connections to the vlans using a trunk connection to ESW4.

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
1- PC4	Switch 4	No	ARP request
2- PC4	Router	Yes	ARP request and reply + ICMP request and reply
3- PC4	PC5	Yes	(ARP requests and replies + ICMP requests and replies)*
4- PC4	192.1.1.100	No	ARP request
5- PC5	Switch 4	No	ARP request
6- PC5	Router	Yes	ARP request and reply + ICMP request and reply
7- PC5	PC4	Yes	(ARP requests and replies + ICMP requests and replies)*
8- PC5	192.1.1.100	No	ARP request

1- Even though ESW4 has the interface of vlan2 defined, it is not configured, resulting on a failed ping request. Only ARP requests were passed through ESW to check if the requested ip was there. Any attempt to ping requires an ip address, and the switch has an ip address only on vlan1.
2- Connection was successful, as both devices are on the same vlan. R1 is the gateway for PC4 and answers to pings within the vlan.
3- PC4 and PC5 are not on the same vlan. Nevertheless, ping occurs due to both being related to the same router and more specifically the same interface, allowing the routing to occur. Communication between both PC's occurs as the following analysis shows:

```
125 54.298938    Private_66:68:00    Broadcast           ARP        68 Who has 192.168.1.254? Tell 192.168.1.1
126 54.325530    c2:02:5e:30:00:00   Private_66:68:00    ARP        64 192.168.1.254 is at c2:02:5e:30:00:00
127 54.326826    192.168.1.1         192.168.20.4        ICMP      102 Echo (ping) request  id=0xdc4e, seq=1/256, ttl=64 (no response found!)
128 54.356051    c2:02:5e:30:00:00   Broadcast           ARP        64 Who has 192.168.20.4? Tell 192.168.20.254
129 54.357343    Private_66:68:01    c2:02:5e:30:00:00   ARP        64 192.168.20.4 is at 00:50:79:66:68:01
134 56.328237    192.168.1.1         192.168.20.4        ICMP      102 Echo (ping) request  id=0xde4e, seq=2/512, ttl=64 (no response found!)
135 56.339928    192.168.1.1         192.168.20.4        ICMP      102 Echo (ping) request  id=0xde4e, seq=2/512, ttl=63 (reply in 136)
136 56.341063    192.168.20.4        192.168.1.1         ICMP      102 Echo (ping) reply    id=0xde4e, seq=2/512, ttl=64 (request in 135)
137 56.350160    192.168.20.4        192.168.1.1         ICMP      102 Echo (ping) reply    id=0xde4e, seq=2/512, ttl=63
```

First, an ARP request is made from PC4 to R1 (PC4's, gateway). Then, an ICMP is made within the vlan to attempt a ping request to the requested IP address on vlan2, which reports no response. Since it is not on vlan2, R1 proceeds to check if the ip address is registered to any device on vlan3, making once again an ARP request and obtains response (found PC5). After finding PC5, an ICMP request is made from PC4 to PC5, once again passing between vlans, resulting in a "duplicated" request and reply. A first ICMP request is made to R1 and R1 "forwards" it between vlans (vlan2 to vlan3), resulting on a second request. The same applies to the consequent reply.

4- The ip address specified is not a device registered on any of the vlans, thus resulting on a lack of reply.
5- Switch4 doesn't have an ip address on vlan3, making it unreachable.Only on vlan1 the switch has a configured ip address and that vlan is not specified on the router, making it unreachable.
6- Connection was successful, as both devices are on the same vlan. R1 is the gateway for PC5 and answers to pings within the vlan.
7- See pt. 3.
8- See pt. 4.

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

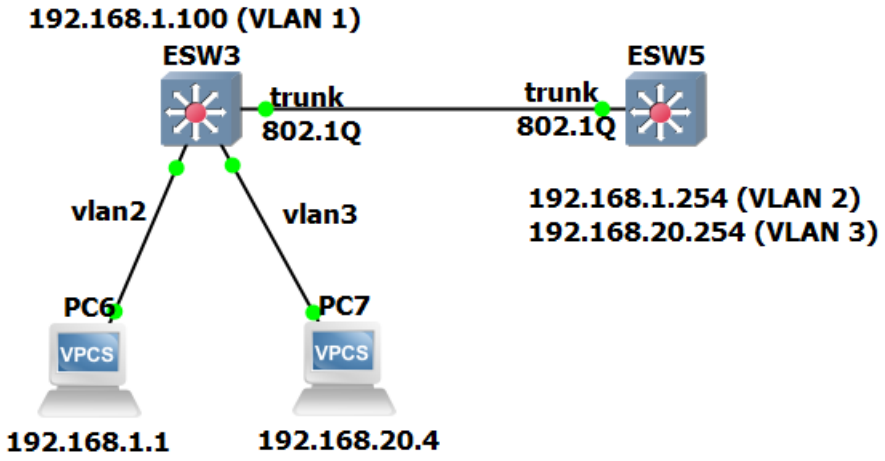


Figure 4

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.

As in the previous scenario with the router sub-interfaces, with the L3 Switch we may also support different VLANs over the same connection:

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

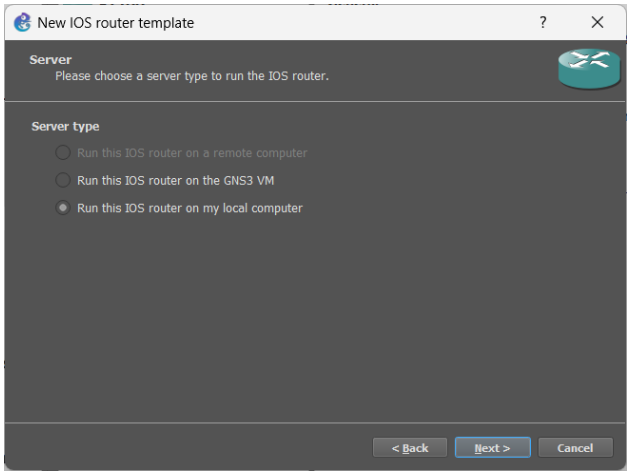
ESW5(config)# interface vlan 3
ESW5(config-if)# ip address 192.168.20.254 255.255.255.0
ESW5(config-if)# no shutdown

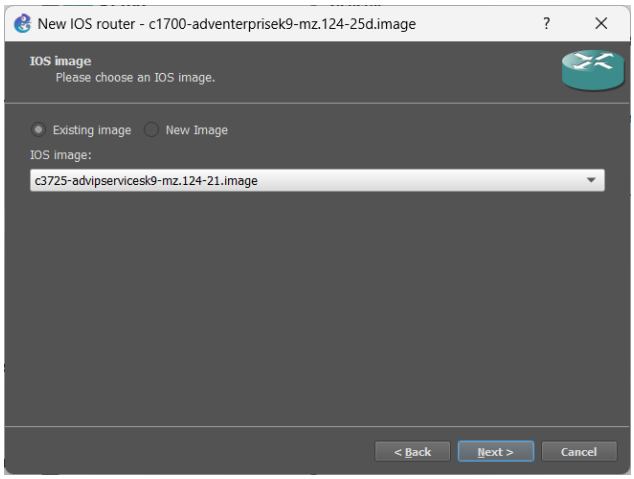
ESW5(config)# interface F1/15
ESW5(config-if)# switchport mode trunk

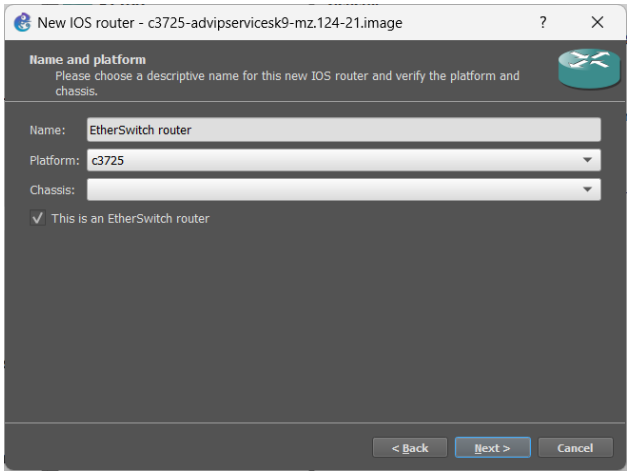
Annex A

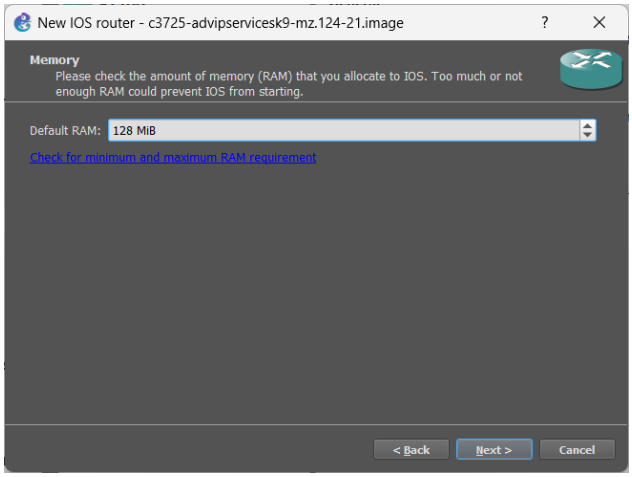
Introduction to the ESW Cisco Switch Router (L3 Switch)

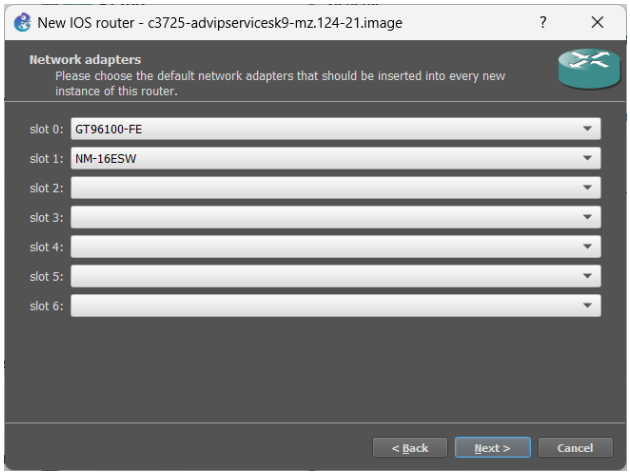
If you still do not have, you must add the ESW to your GNS installation, under Edit ➔ Preferences ➔ Dynamips ➔ IOS Routers ➔ New

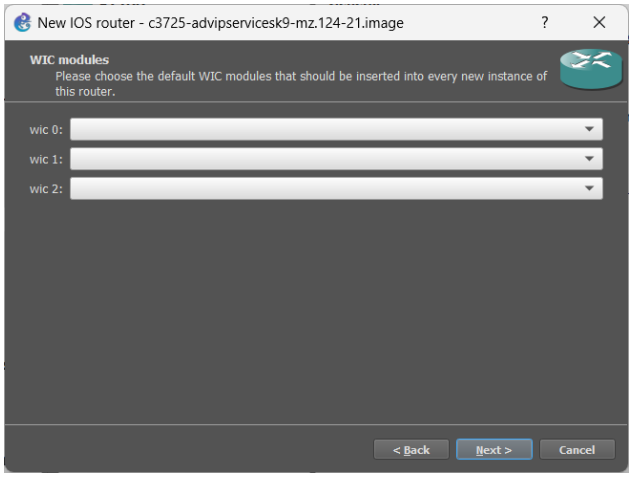


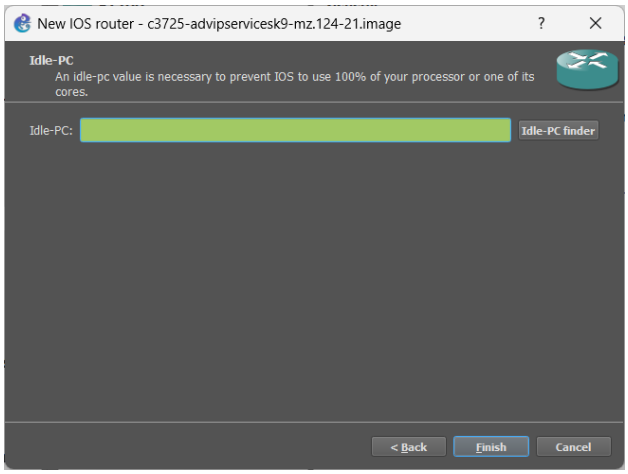


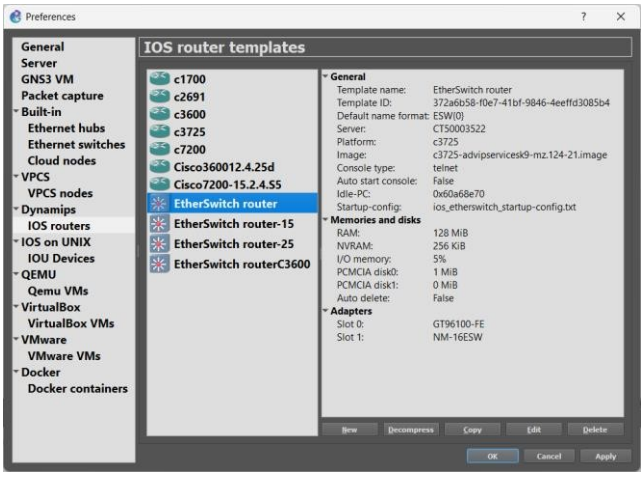




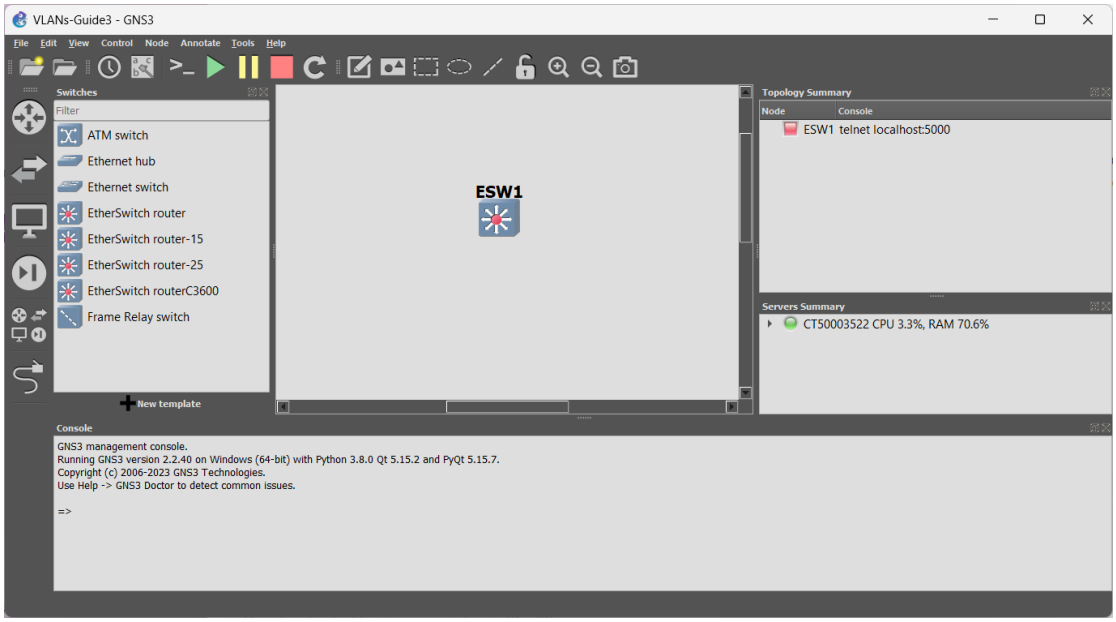




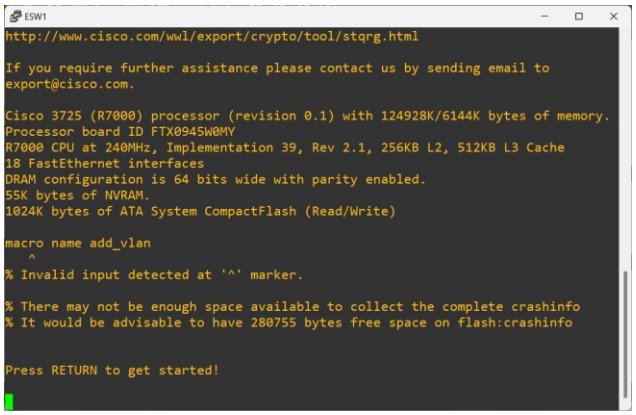


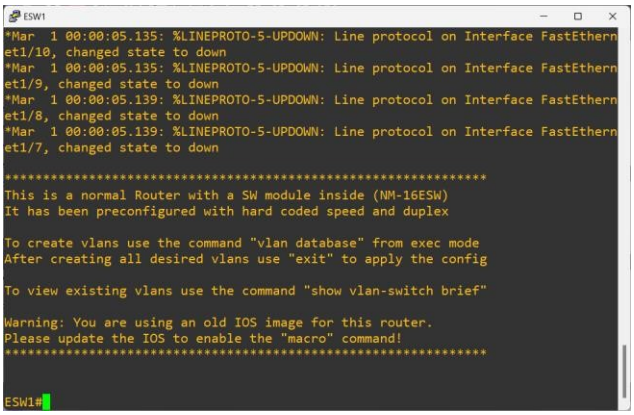


Create a new project for the VLANs Guide and add an EtherSwitch router (ESW1):

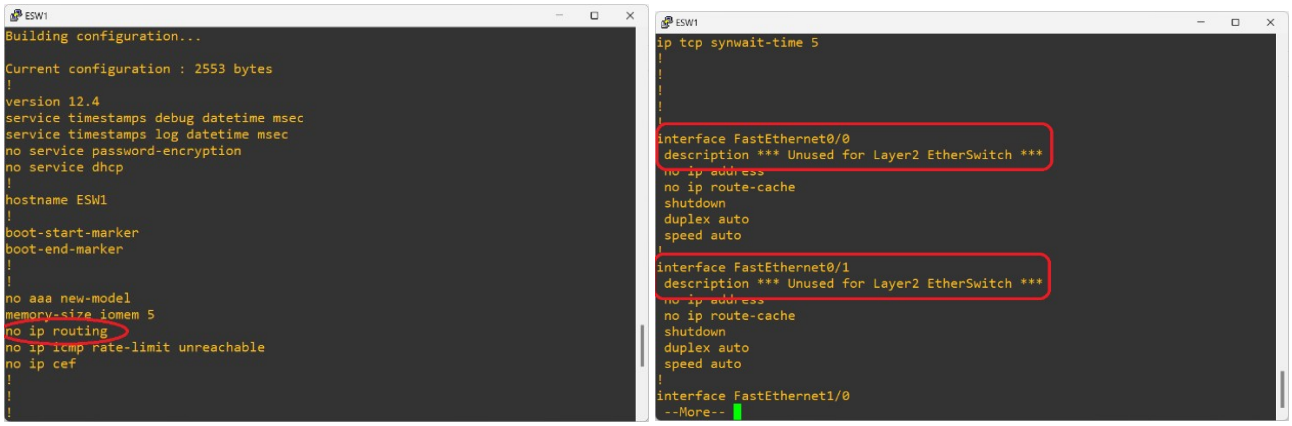


Start the device and right click over it to open the console:



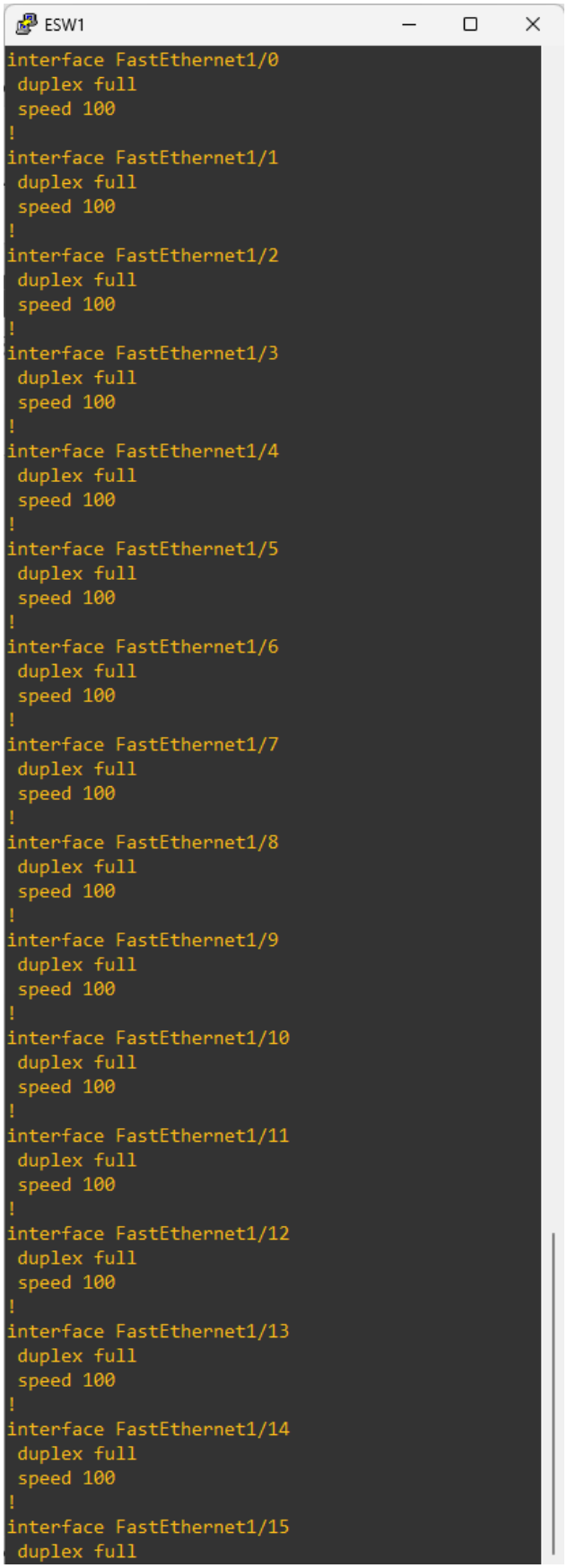


Do a show run to check its configuration, with special attention to the available interfaces.

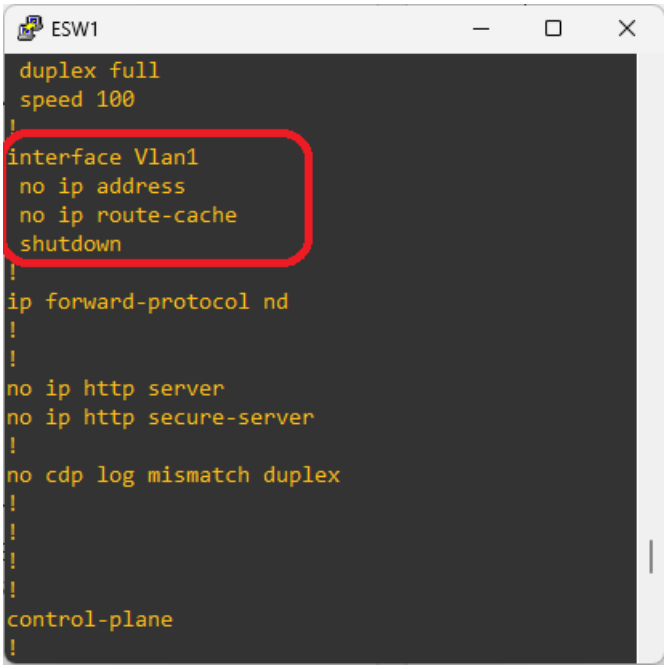


Note that:

- 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.

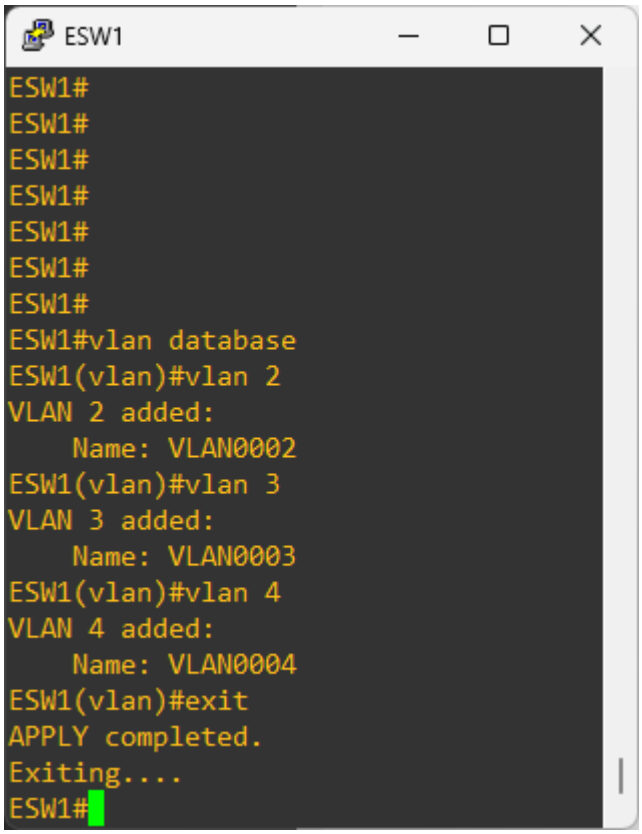


There are 16 interfaces (from F1/0 to F1/15) that "belong" to a switch card interface on the router, and these are the interfaces used for switching and VLANs.

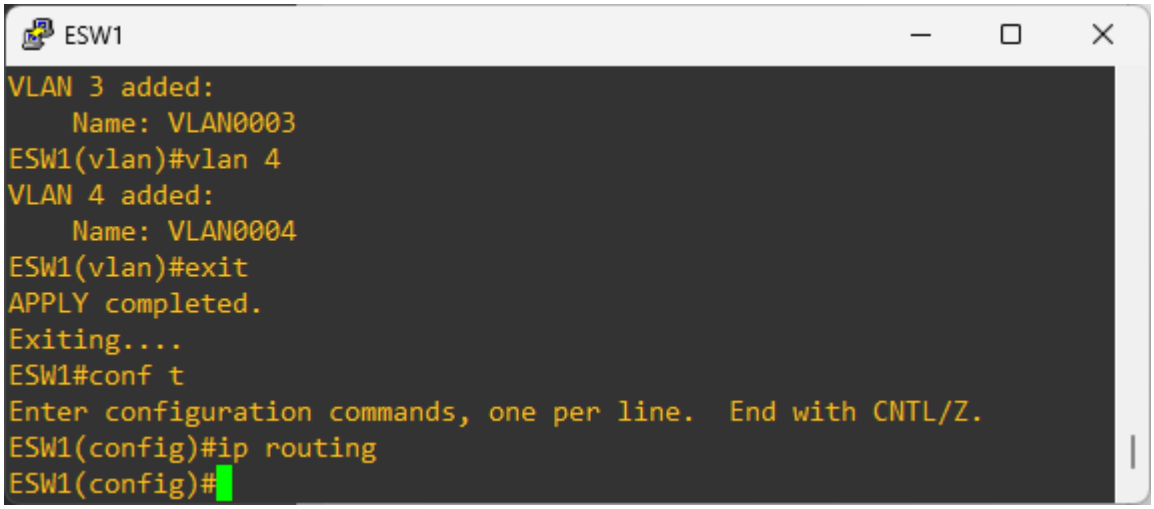


By default there is a Vlan1 interface, through which all switch ports belonging to the Vlan1 may do routing to the other routing interfaces (F0/0 and F0/1). Note that this interface is in “shutdown” by default. In order to be used, you have to do the “no shutdown” to it.

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



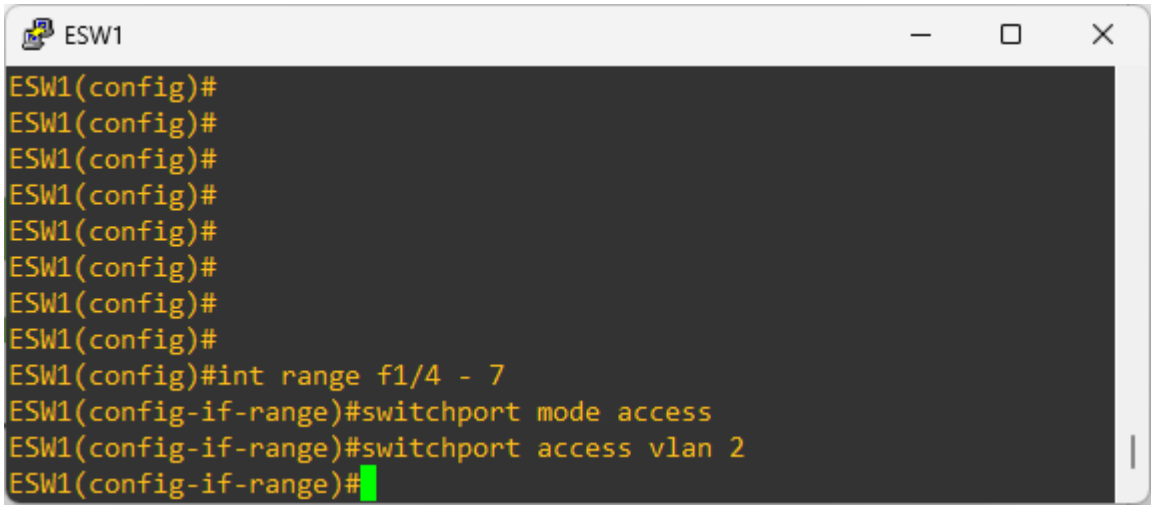
Enabling IP Routing functions on this device:



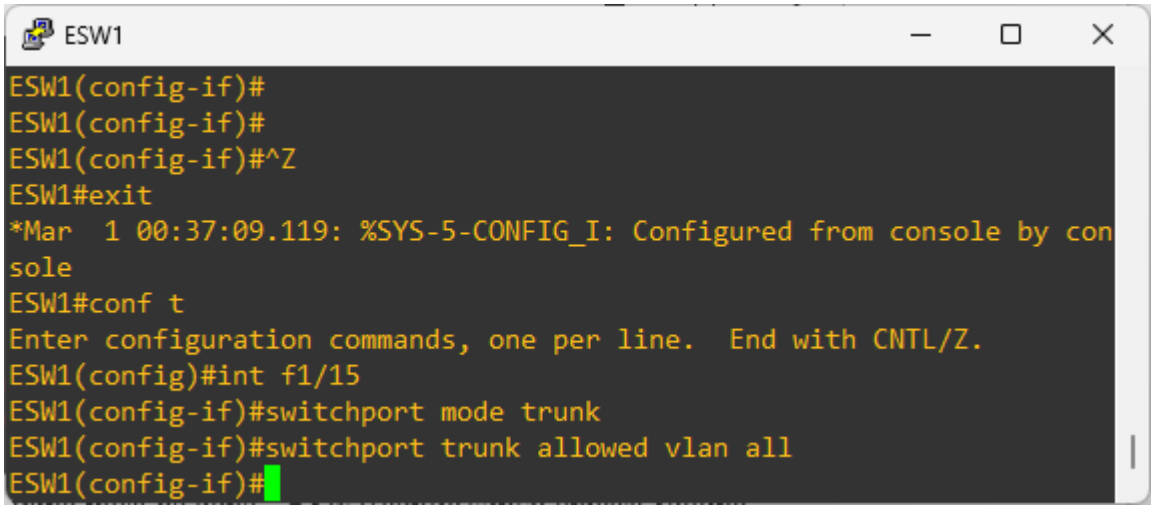
Note: for IPv6 the same thing must be done. “ESW1(config)#ipv6 unicast-routing”

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):



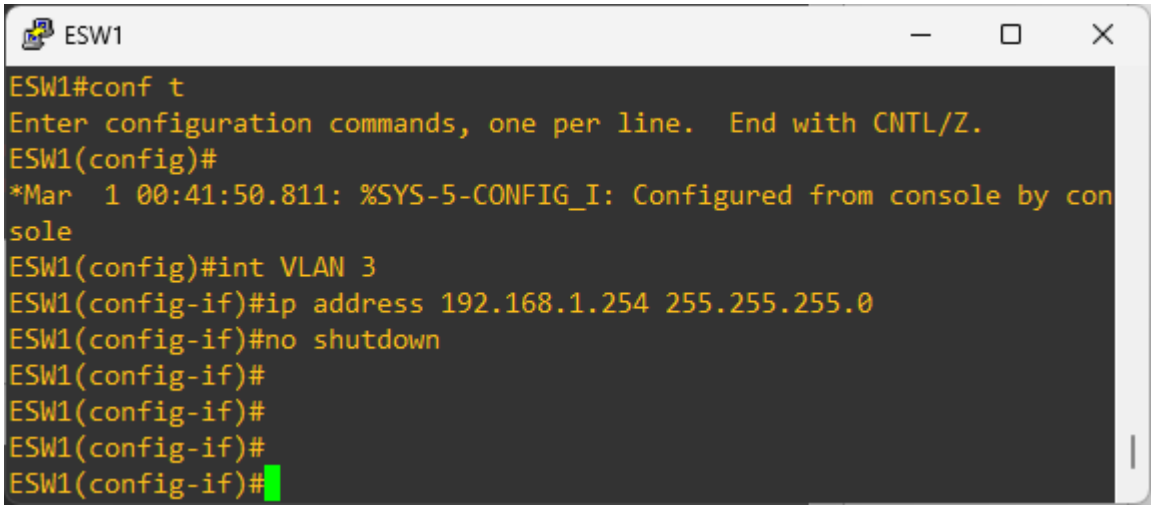
Putting a port in TUNK mode and allowing all configured VLANs to be able to come in and out of that interface (you may restrict the port to some specific interfaces, if needed):



Note:

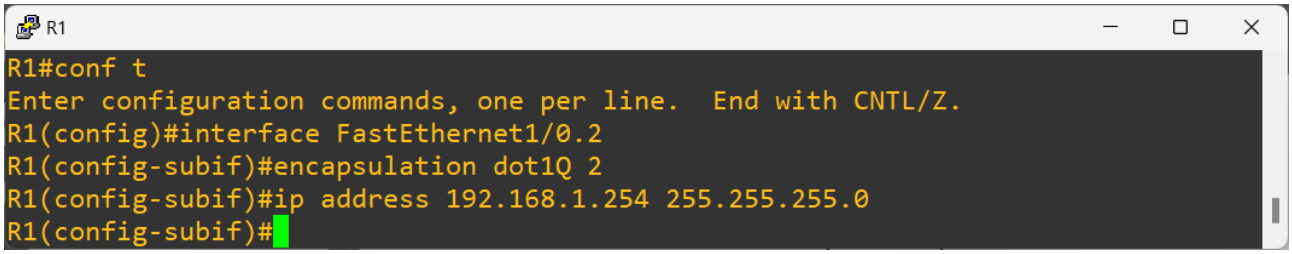
- Ports on access mode can only belong to one specific VLAN and the incoming and outgoing Ethernet frames DO NOT have VLAN TAG.
- Ports on trunk mode may input and output Ethernet frames from different VLANs and those Ethernet frames SHOULD BE TAGGED.

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.

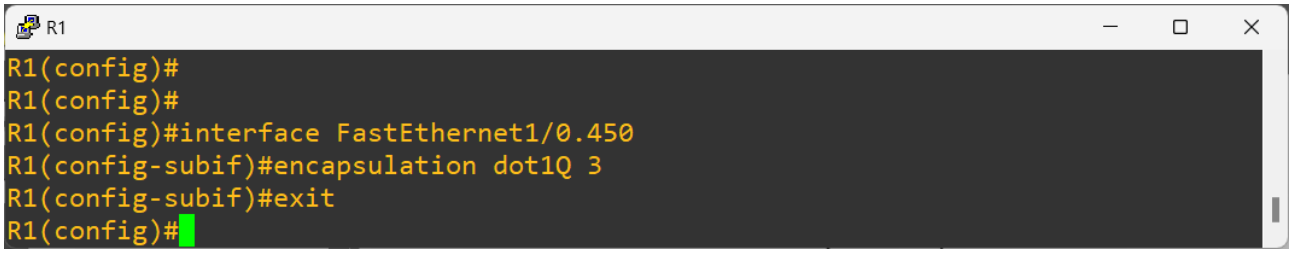
Configuring a regular router interface to send and receive Ethernet frames with VLANs



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:



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