universidade de aveiro
theoria poiesis praxis

REDES DE COMUNICAÇÕES 2

Note: **I**n GNS3, a Layer 2 switch may me implement (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).

Virtual LAN

1.1. Set up the network shown in the following figure and configure all IP addresses with netmask 255.255.255.0. ip 192.168.1.1/24 na consola do PC1 + save

In Switch 1, configure two VLANs in the following way:

a) Create VLAN 2 (VLAN 1 already exists by default):

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

b) Ports numbered F1/5 to F1/8 belonging to VLAN 2:

```
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
```

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

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

```
ESW1# show vlan-switch
```

Configure VLAN 1 IPv4 address of Switch1:

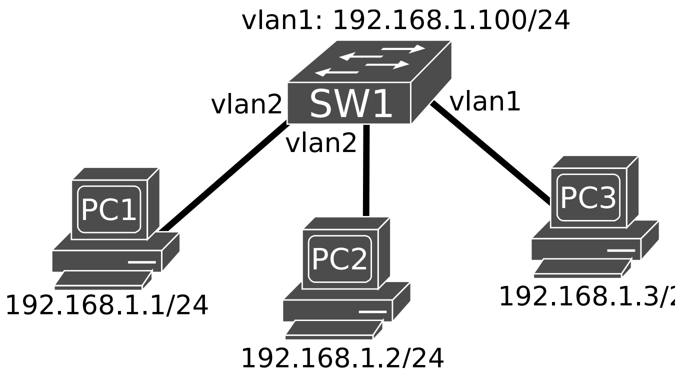
```
ESW1(config)# interface vlan 1
ESW1(config-if)# ip address 192.168.1.100 255.255.255.0
ESW1(config-if)# no shutdown
ESW1(config-if-range)# end
ESW1# write
```

In all PCs, configure the appropriate the IPv4 address.

For PC1:

```
PC-1> ip 192.168.1.1/24
```

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



Troubleshooting 1: When creating the VLAN, if a flash memory space error occurs, run the command

```
ESW1# erase flash:
```

to erase the flash, and after, create the missing VLAN. Also verify on your EtherSwitch router that you have at least 1MB in the PCMCIA disk 0 (configure→ Memories and Disks).

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

>> Verify that the status of the switch's interfaces is "up/up" for the ones in use. Use the command:

```
ESW1# show ip interface brief
```

>> Analyze the Switch's Forwarding table.

Fiz um ping primeiro entre o PC1 e o PC2 para a vlan2 aparecer na tabela

```
ESW1# show mac-address-table
```

>> Verify that the MAC addresses of the PC appear on the correct port and VLAN.

Troubleshooting 2: If the status of a switch port in use is administratively down, perform a "`no shutdown`" on the respective interface. If the protocol status is down (no cable detected), perform a "`shutdown`" followed by a "`no shutdown`" on the respective interface (the cable detection mechanism will be run for all ports).

1.3. 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.

Ping from:	**Ping to:**	**Connectivity (yes or no)**	**Packets (PC1-Switch1 link)**	**Packets (PC3-Switch1 link)**
PC2	Switch1 (vlan 1)	NO	ARP	NONE
PC2	PC3	NO	ARP	NONE
PC2	192.168.1.34	NO	ARP	NONE
PC3	Switch 1 (vlan 1)	YES	NONE	ICMP E ARP
PC3	PC2	NO	NONE	ARP
PC3	192.168.1.34	NO	NONE	ARP
Switch1	PC3	YES	NONE	ICMP
Switch1	192.168.1.34	NO	NONE	ARP

Dispositivos em VLANs diferentes não se conseguem comunicar. O flooding feito através de broadcasts está restringido à VLAN em que este acontece

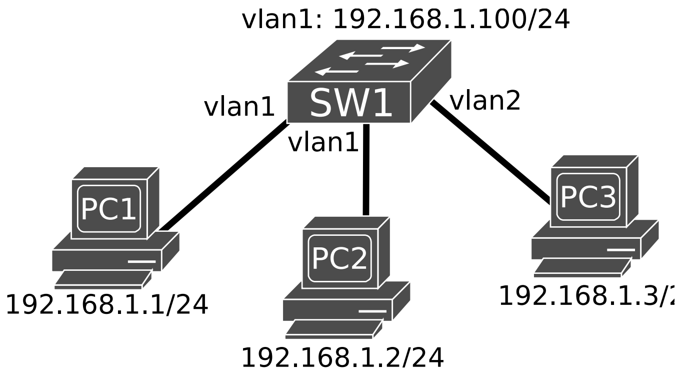
>> What do you conclude from the connectivity tests based on the VLAN of the devices?

>> What do you conclude about the way a broadcast packet is propagated?

Note: Different switches OS may allow to define (i) just an IP address for one VLAN (administration) or (ii) different IP addresses in multiple VLAN.

2.1. In Switch 1, change the connections in order to connect PC1 and PC2 to VLAN 1 ports and PC3 to a VLAN 2 port (as specified in the next figure). Once again, verify that the status of the switch's connected interfaces is "up/up" for the ones in use.

Codigo do 1.1 b) para trocar as vlans



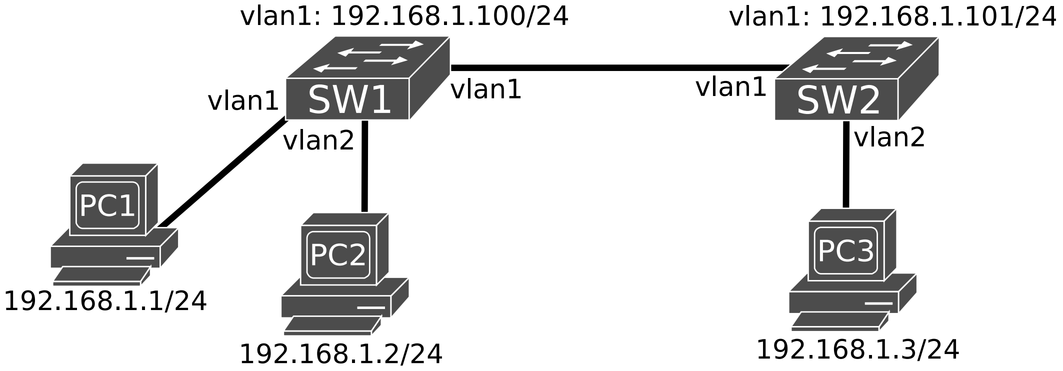
2.2. Start new captures on the links PC1-Switch1 and PC3-Switch1 and set an appropriate filter to display ARP and ICMP packets. Run the ping commands specified in the following table. For each run, register the connectivity and the filtered packets.

Ping from:	Ping to:	Connectivity (yes or no)	Packets (PC1-Switch1 link)	Packets (PC3-Switch1 link)
PC2	Switch1 (vlan 1)	YES	ARP	NONE
PC2	PC3	NO	ARP	NONE
PC2	192.168.1.34	NO	ARP	NONE
PC3	Switch1 (vlan 1)	NO	NONE	ARP
PC3	PC2	NO	NONE	ARP
PC3	192.168.1.34	NO	NONE	ARP
Switch1	PC3	NO	ARP	NONE
Switch1	192.168.1.34	NO	ARP	NONE

>> Confirm the previous conclusion about device connectivity between different VLAN.
>> Confirm the previous conclusion about the broadcast domains of each VLAN. Confirmo sim senhora

Trunk Ports/Links

3. Reconfigure the network as specified in the following figure. In the new inserted Switch 2, configure VLANs 1 and 2 in the same way as specified to Switch 1 in the previous experiments.



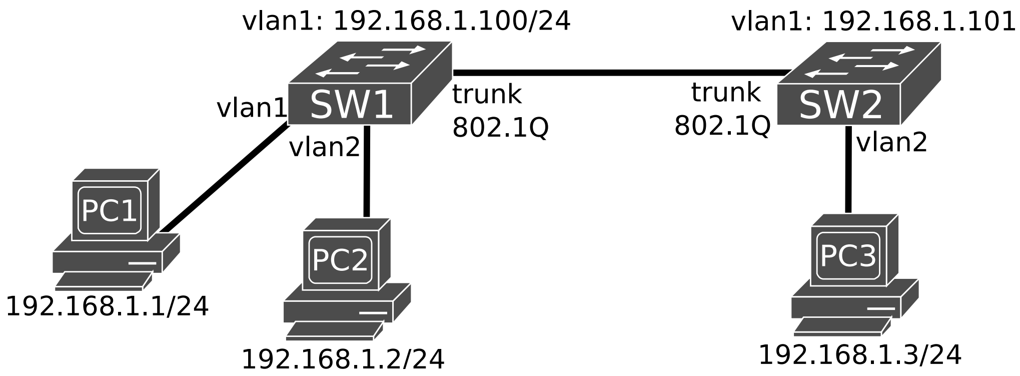
3.1. Start new capture on the link Swicth1-Switch2 and set an appropriate filter to display ARP and ICMP packets. Run the ping commands specified in the following table. For each run, register the connectivity and the filtered packets.

Ping from:	Ping to:	Connectivity(yes or no)	Filtered packets
PC1	Switch 1	YES	ARP
PC1	Switch 2	YES	ARP & ICMP
PC1	PC3	NO	ARP
PC2	Switch 1	NO	NONE
PC2	Switch 2	NO	NONE
PC2	PC3	NO	NONE
PC3	PC1	NO	NONE
PC3	PC2	NO	NONE

>> What do you conclude from the connectivity tests between devices on different switches?
>> What do you conclude about the way a broadcast packet is propagated?

3.2. 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 following figure.

```
ESW3(config)# interface F1/15
ESW3(config-if)# switchport mode trunk
```



4.1. 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.

Ping from:	Ping to:	Connectivity(yes or no)	Filtered packets
PC1	Switch 1	YES	ARP
PC1	Switch 2	YES	ARP & ICMP
PC1	PC3	NO	ARP
PC2	Switch 1	NO	ARP
PC2	Switch 2	NO	ARP
PC2	PC3	YES	ARP & ICMP
PC3	PC1	NO	ARP
PC3	PC2	YES	ICMP

>> Identify the purpose of the VLAN ID field in each Ethernet frame. VLAN ID = 2 aparece no wireshark, o 1 é default

>> What do you conclude about the importance of trunk links/ports?

Note: Different switches OS may not tag Ethernet frames from the default/native VLAN. In Cisco devices, VLAN 1 (native VLAN) ate not tagged. Any not tagged packet is assumed to belong to VLAN 1.

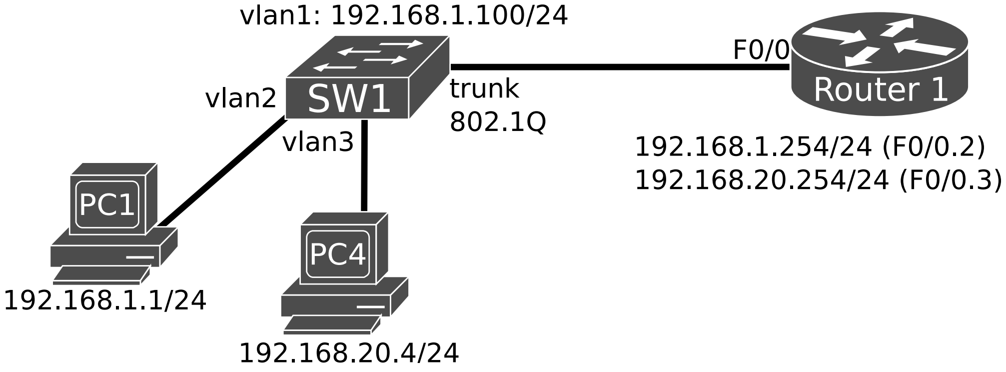
Format of the Ethernet frames with and without 802.1Q tags

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



5.1. Reconfigure the network as specified in the previous figure where Router 1 routes packets between VLAN 2 and VLAN 3 (each one with its own network IP address).

In Switch 1, 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) configure the SW1 default gateway for VLAN 1:
ESW1(config)# ip default-gateway 192.168.1.254

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

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

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-subif)# interface F0/0.3
Router (config-subif)# encapsulation dot1Q 3
Router (config-subif)# ip address 192.168.20.254 255.255.255.0
```

Router (config)# interface F0/0
Router (config-if)# no shutdown
Router (config-if)# interface F0/0.1
Router (config-subif)# encapsulation dot1Q 1
Router (config-subif)# ip address 192.168.1.254 255.255.255.0
Router (config-if)# interface F0/0.2
Router (config-subif)# encapsulation dot1Q 2
Router (config-subif)# ip address 192.168.2.254 255.255.255.0
Router (config-subif)# interface F0/0.3
Router (config-subif)# encapsulation dot1Q 3
Router (config-subif)# ip address 192.168.3.254 255.255.255.0

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

```
PC1> ip 192.168.1.1/24 192.168.1.254
PC4> ip 192.168.20.4/24 192.168.20.254
```

5.2. In order to verify the correctness of the configurations, check the IP connectivity between PC1 and PC4 with the ping command.

Use the following command to view the IPv4 routing table:

```
Router# show ip route
```

>> Register and justify the IP routing table of the Router.

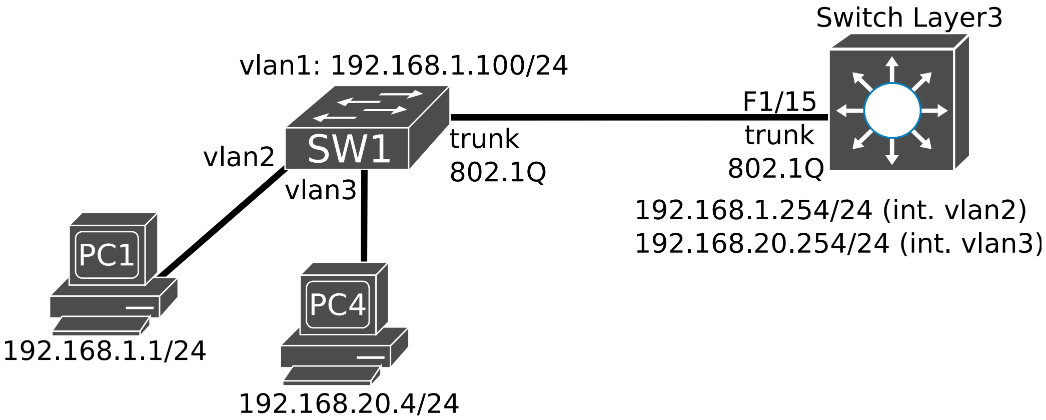
5.3. Start new capture on the link Swicth1-Router and set an appropriate filter to display ARP and ICMP packets. Run the ping commands specified in the following table. For each run, register the filtered packets and their VLAN ID value.

Ping from:	Ping to:	Connectivity (yes or no)	Filtered packets
PC1	Switch 1	YES	ARP & ICMP
PC1	Router	YES	IMCP
PC1	PC4	YES	ARP & ICMP
PC1	192.1.1.100	NO	ICMP
PC4	Switch 1	YES	ICMP
PC4	Router	YES	ICMP
PC4	PC1	YES	ARP & ICMP
PC4	192.1.1.100	YES	ICMP

>> Identify “the same” IPv4 packets that appear twice in different Ethernet frames with different 802.1Q tagging.

>> Identify the purpose of the VLAN ID field in each Ethernet frame. Identifica em que vlan estamos

>> What do you conclude how packets are routed between different VLAN?



5.4. Reconfigure the network as specified in the previous figure where the inter-VLAN routing is performed by a Layer 3 switch (GNS3 *EtherSwitch Router*).

Create VLANs 2 and 3 at the L3 Switch (VLAN2 and 3):

```
ESW1# vlan database
ESW1(vlan)# vlan 2
ESW1(vlan)# vlan 3
ESW1(vlan)# exit
```

Activate IPv4 routing (most times is active by default):

```
ESW1(config)# ip routing
```

Configure the ports that connects to Switch1 as trunk (802.1Q):

```
ESW1(config)# interface F1/15
ESW1(config-if)# switchport mode trunk
```

Configure the Switch L3 virtual (Vlan) interfaces:

```
ESW1(config)# interface Vlan 2
ESW1(config-if)# ip address 192.168.1.254 255.255.255.0
ESW1(config-if)# no autostate                        !forces the port to be always up
ESW1(config)# interface Vlan 3
ESW1(config-if)# ip address 192.168.20.254 255.255.255.0
ESW1(config-if)# no autostate                        !forces the port to be always up
```

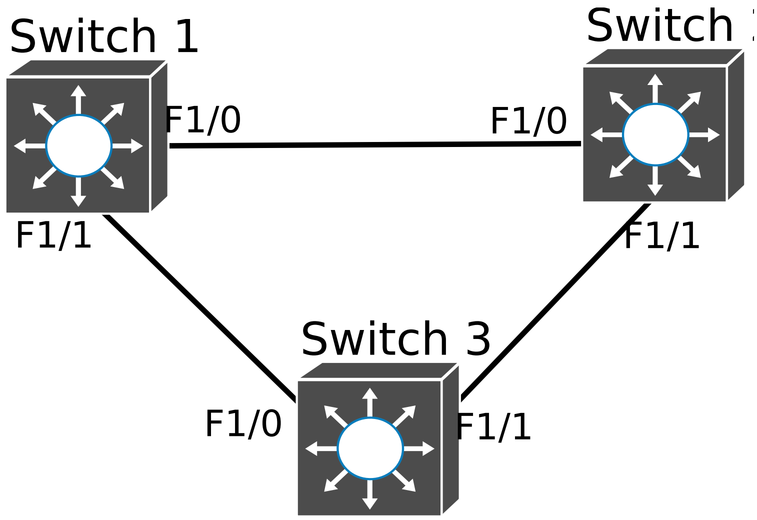
Check the IP connectivity between PC1 and PC4 with the ping command.

>> Register and justify the IP routing table of the Layer 3 switch.
>> What do you conclude how packets are routed between different VLAN using a Layer3 switch? Is any difference from routing with a router with sub-interfaces?
>> Do you identify advantages on using Layer3 switches versus Routers? Assume a network with multiple access zones.

O procedimento na troca de informação é exatamente igual quando comparado com a utilização de um Router.

- Com o Switch L3 conseguimos criar uma rede única para uma VLAN independemente da interface usada, e há mais simplicidade porque vários pontos de acesso podem usar a mesma configuração usando portas trunk (fica mais escalável).

***Spanning Tree Protocol* (STP)**



6. In GNS3 configure a network as specified in the following figure, using the connections of the switching module (ports F1/0 to F1/15) of the *"EtherSwitch Routers"*. Verify that all used ports belong to VLAN 1:

```
ESW1# show vlan-switch
```

Based on the result of commands

```
ESW1# show spanning-tree bridge
ESW1# show spanning-tree interface f1/0 brief
ESW1# show spanning-tree interface f1/1 brief
```

ESW1 - Bridge ID: 32768
Address: c201.0c34.0000
Port ID f1/0: 128.41
Port ID f1/1: 128.42

ESW2 - Bridge ID: 32768 Address:

ESW3 - Bridge ID: 32768
Address: c203.2a74.0000
Port ID f1/0: 128.42
Port ID f1/1: 128.42

>> Identify and register the following information: (base) MAC address of each bridge, priority of each bridge, *bridge IDs and ports' IDs and costs.*

>> *Predict which switch will be the root and which port(s) will be blocked?*

root bridge : SW1

SW2:
designated ports: f1/0 e f1/1
custo: 19

6.1. Based on the result of commands

```
ESW1# show spanning-tree brief
ESW1# show spanning-tree summary
ESW1# show spanning-tree vlan 1
```

SW1:
designated ports: f1/0 e f1/1
custo: 19

SW3:
designated ports: f1/0
blocked ports: f1/1
custo: 19

>> Identify and register the STP algorithm result: root bridge, designated bridges for each LAN, root port for each bridge, designated ports for each bridge, the root path cost of each bridge and the cost of all ports.

>> Confirm your previous predicted results.

6.2. Start a capture in each LAN (SW1-SW2, SW1-SW3 e SW2-SW3). Analyse the BPDU/STP captured packets, register its contents and confirm their coherence with the results obtained in the previous experiments.

>> Identify the relevant fields of each BPDU.

>> Which *bridge* is responsible for sending BPDUs in each local network (designated bridge)?

Format of the configuration BPDU packets

#octets			
2	Protocol Identifier		
1	Version		
1	Message Type		
1	TCA	Reserved	TC
8	Root ID		
4	Cost of Path to Root		
8	Bridge ID		
2	Port ID		
2	Message Age		
2	Max Age		
2	Hello Time		
2	Forward Delay		

6.2. Pause the two *switches* with the lowest bridge IDs. Start a capture in the Ethernet network that interconnects the two switches with the higher IDs. Execute the following sequence of actions:

(i) Wait two minutes and analyse the sequence of captured BPDU/STP packets;

(ii) Restart the *switch* with the second lowest *Bridge* ID, wait two minutes and analyse the sequence of captured BPDU/STP packets;

(iii) Restart the *switch* with the lowest *Bridge* ID, wait two minutes and analyse the sequence of captured BPDU/STP packets.

>> Identify how the bridge root change upon each action.

>> Explain the root election process.

6.3. Start a capture in all LANs (SW1-SW2, SW1-SW3 and SW2-SW3). Change the priority of one *bridge* in such a way that it becomes the *root bridge*.

```
ESW1# configure terminal
ESW1(config)# spanning-tree vlan 1 priority <value>
```

>> Analyse the captured BPDU/STP packets and explain the re-election process of the root *bridge*.

6.4. Start a capture in all LANs (SW1-SW2, SW1-SW3 and SW2-SW3). Change in the designated bridge of the network that is not connected to the root bridge the cost of its root port in such a way that it stops being the designated bridge, using the following commands:

```
ESW1# configure terminal
ESW1(config)# interface <interface>
ESW1(config-if)# spanning-tree cost <value>
```

Since there was a change in the *Spanning Tree* protocol parameters, the topology change notification mechanism is triggered. Let the capture last for a period of at least 1 minute after changing the port cost.

>> Analyse the sequence of captured packets and verify if BPDU packets of the TCN type were sent.

>> Identify any changes on the TC and TCA *flags* of the *Configuration BPDU* packets.

>> Explain how changes on topology are notified and and how period of change are managed by the STP.

Format of the TCN (*Topology Change Notification*) packets

#octets	
2	Protocol Identifier
1	Version
1	Message Type

6.5. Start a capture on the Ethernet network that is not directly connected to the *root bridge*.

The bridge *Hello Time* parameter can be changed with the following commands

```
ESW# configure terminal
ESW1(config)# spanning-tree vlan 1 hello-time <value>
```

Execute the following sequence of actions:

(i) change the *Hello time* parameter of the *bridge* with the second lowest bridge ID to 6 seconds and, using Wireshark, verify the periodicity of the generated BPDU packets;

(ii) change the *Hello time* parameter of the *root bridge* to 6 seconds and, using Wireshark, verify the periodicity of the generated BPDU packets;

>> What do you conclude about the effect of configuring the *Hello Time* parameter in different *switches* on the general interval between BPDU packets in all networks?

Só afeta o comportamento da rede quando o Hello Time da root bridge altera