ECOLE POLYTECHNIQUE DE BRUXELLES

IRELE - MA1 Electrical Engineering

ELEC-H417

Report Lab 3
Virtual Local Area Network (VLAN)

Authors :

Amaury ARICO

Alexis BOLLENGIER

Emmeran COLOT

Sefa GÖNEN

Professor :

Jean-Michel DRICOT

Assistant :

Navid LADNER

Academic year :

2024 - 2025

Contents

0 Mission 0 - Topology

0.1 Question - Routers VS Switches

Routers VS Switches

What is the difference between Routers and Switches ?

- **Routers** operate at **Layer 3 (Network Layer)** and are used for routing traffic between different networks : *routers are connecting devices from **different networks** together.*
  Routers are responsible for determining the best path for data to travel from one network to another one.

- **Switches** operate at **Layer 2 (Data Link Layer)** and are used for forwarding data within the same network : *switches are connecting multiple devices together within **one network**.*
  A switch functions by learning the MAC address of the devices connected to its ports and by forwarding frames based on these addresses. Switches **do not route traffic**[1] between different networks.
  Also, switches are **transparent** on the network (the hosts are unaware of the presence of switches) and **self-learning** (don't need to be configured).

[1] Some switches can also do routing (L3), they are known as multilayer switches

1 Mission 1 - VLAN Isolation

1.1 Question - Netmask adaptation

Netmask adaptation

What should be the netmask to achieve this and why ?

The netmask that should be used to allow PC1 (192.168.20.2) and PC3 (192.168.30.2) to communicate without changing their IP addresses is `255.255.240.0 (or /20)`.

Explanation:

We need to find a common part in the subnet portion of both PCs and set the netmask such that the new subnet is this common part.

In binary, the IP address `192.168.20.2` is represented as:

11000000.10101000.00010100.00000010

And the IP address `192.168.30.2` is represented as:

11000000.10101000.00011110.00000010

We can see that the first 20 bits of both addresses are the same. That's why the netmask is `/20 (255.255.240.0)`.

1.2 Question - Pinging across VLAN

Pinging across VLAN

Does the ping command work and why ?

The ping command does **not work** between PC1 and PC3 after configuring them to be in different VLANs.

This is because VLANs isolate traffic at Layer 2, meaning devices in different VLANs cannot communicate with each other unless there is routing in place between them (in our case, no router is configured).

2 Mission 2 - VLAN Trunking

2.1 Question - Wireshark Analysis

Wireshark Analysis

Start a Wireshark capture on the trunk line (between both switches) then analyze the ping between two PCs that are on different switches but on the same VLAN (e.g. PC1-PC2 or PC3-PC4). Stop the capture, look for ICMP echo ping packets and click on it. For this packet, open the 802.1Q header (between L2 and L3) and validate that the tag ID is 20 (or 30). Put a Wireshark screenshot with the tag ID highlighted.

The figure 2.1 shows the result of a ping command from PC1 to PC2 captured on the trunk line. These PCs are in the same VLAN (VLAN 20) but are physically connected to different switches.

As expected, the 802.1Q headers in the ICMP packets contain the tag ID of the VLAN (which is 20).

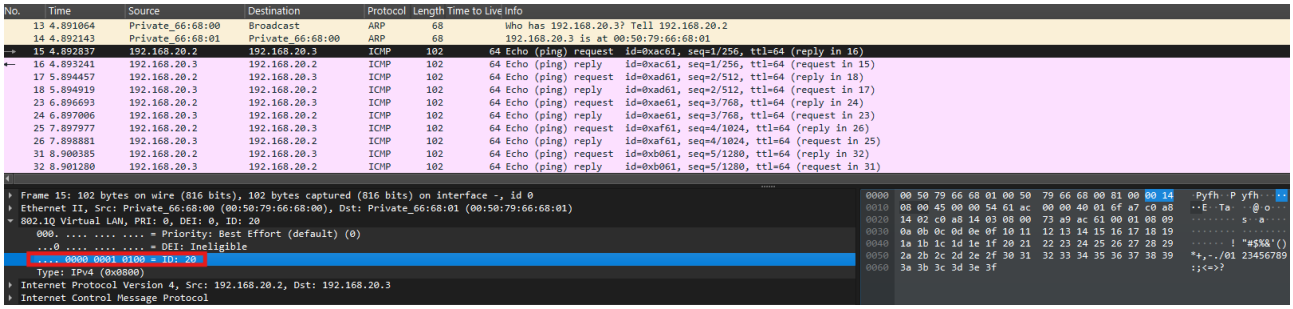

Figure 2.1: Wireshark Screenshot - Ping command from PC1 (192.168.20.2) to PC2 (192.168.20.3) in VLAN 20 - Listening to trunk link between Switch1 and Switch2. The tag ID (=20) in the 802.1Q header of an ICMP packet is shown in the red frame.

3

Mission 3 - Inter-VLAN Routing

3.1 Question - Inter-VLAN pinging

Inter-VLAN pinging

Why does the ping from PC1 to PC4 is working even if they are on different VLAN ? With wireshark, monitor the stick line (i.e. connection between Switch1 and Router) when pinging and deduce what is happening. What is the path taken by the packet and the tag (i.e. VLAN number) associated to the packet at each hop ? What is the impact on the bandwidth ?

The ping from PC1 (192.168.20.2 - VLAN 20) to PC4 (192.168.30.3 - VLAN 30) works because of inter-VLAN routing. Even though the two PCs are on different VLANs, the *router on a stick* setup assures the communication between them : the router is forwarding packets between VLAN 20 and VLAN 30, just as a router would between two different LANs.

When PC1 sends a ping request to PC4, the following happens :

1. The request reaches Switch1 where its layer 2 header is changed : an 802.1Q header is added below the ethernet header. The tag ID associated with this packet is 20 (this can be seen on the figure 3.1).
2. The request is sent from the Switch1 to the router. When it arrives there, the router changes the tag ID in the 802.1Q header to 30, as shown in the figure 3.2. Previously, the request couldn't reach PC4 because it is in VLAN 30 and the request comes from VLAN 20. The goal of the router is to forward the packets from one VLAN to another one.
3. The router returns the request to Switch1 but this time, because the tag ID is 30, Switch1 handles the request as it was part of VLAN 30. To reach PC4, Switch1 sent the request to the trunk line : Switch2 is connected to PC4. The tag ID is still 30.
4. When the request arrives at Switch2, the 802.1Q header is removed and the request is sent to PC4.
5. The reply follows the opposite path (tag ID 30 until it arrives at the router where it changes to 20)

Concerning the bandwidth : because the router changes the tag ID of the packets, there's twice the amount of packets on the line between the router and Switch1. For example, the ping command generates 5 ping requests. In the figure 3.1, we can see that there is 10 ping requests.

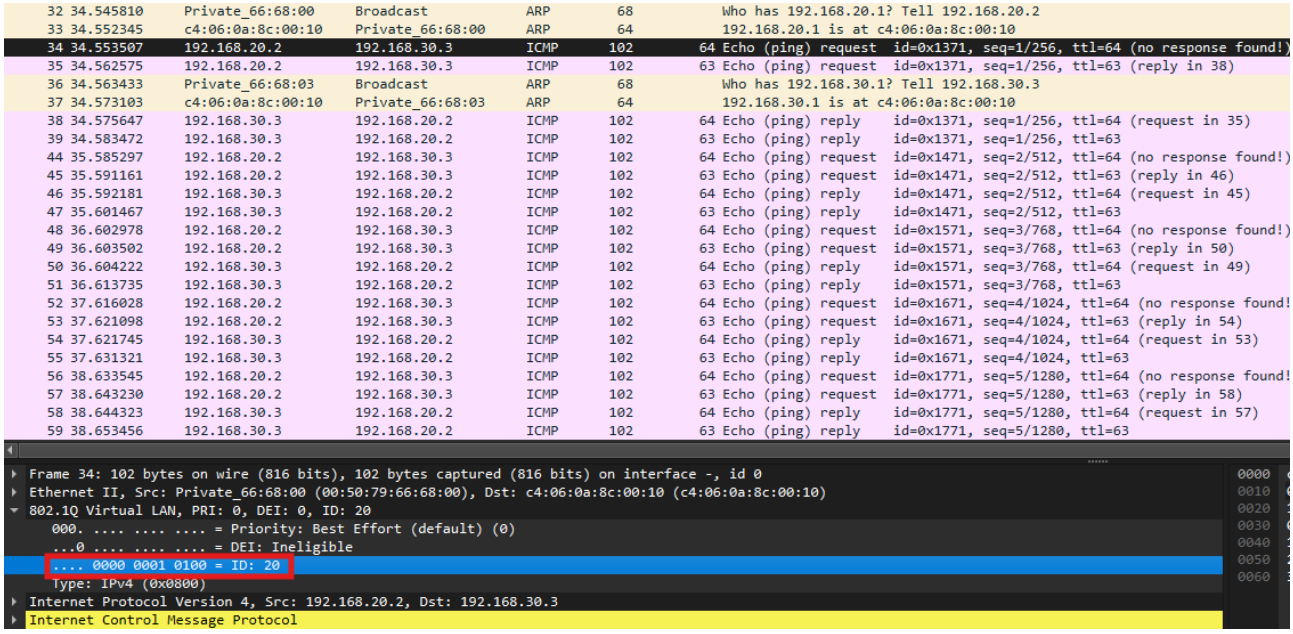

Figure 3.1: Wireshark Screenshot - Ping command from PC1 (192.168.20.2 - VLAN 20) to PC4 (192.168.30.3 - VLAN 30) - Listening to link between Switch1 and Router. The tag ID (=20) in the 802.1Q header of one **ping request** (PC1 → PC4) **before going through the router** is shown in the red frame.

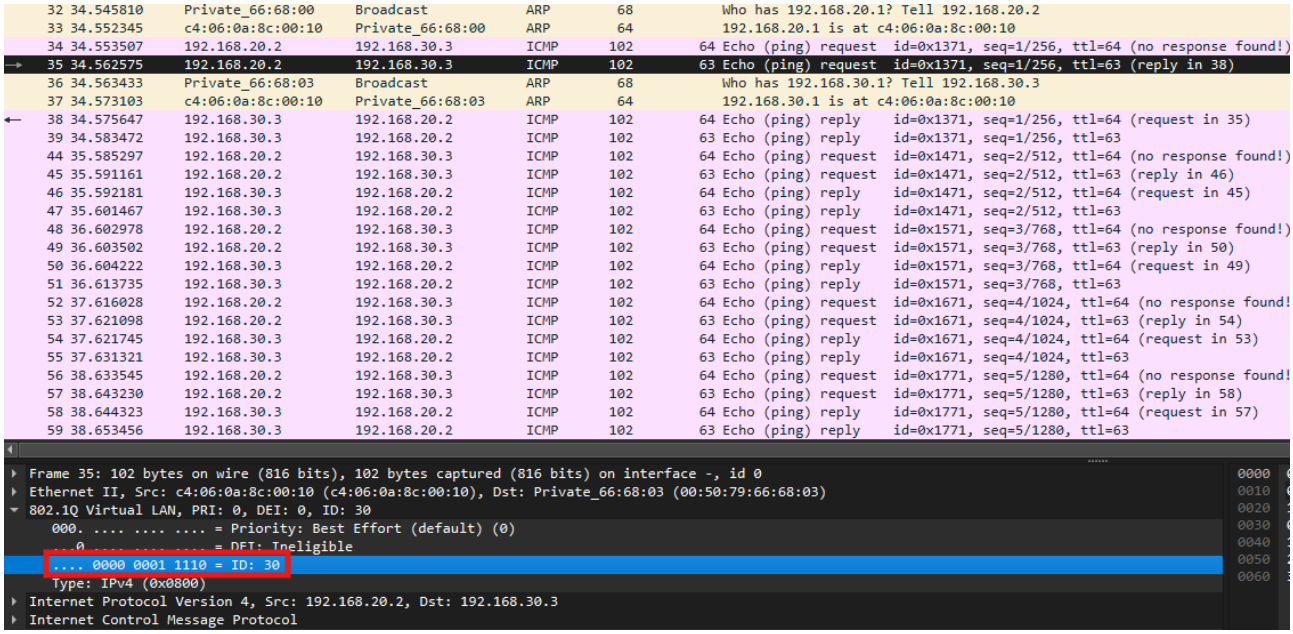

Figure 3.2: Wireshark Screenshot - Ping command from PC1 (192.168.20.2 - VLAN 20) to PC4 (192.168.30.3 - VLAN 30) - Listening to link between Switch1 and Router. The tag ID (=30) in the 802.1Q header of one **ping request** (PC1 → PC4) **after going through the router** is shown in the red frame.

3.2 Question - General conclusion

General conclusion

Explain briefly the whole lab (VLAN, isolation and trunking). To show that you have clearly understood the lab, make a schema of the physical and logical topology obtained after mission 2, and the topology after mission 3. You can use software such as draw.io or take a clean picture of a schema on paper. If you schemas are clear enough, you do not need to explain them but you can if you are unsure.

The laboratory investigation into VLANs focused on three principal areas of inquiry. The key areas of focus were **VLAN isolation**, **VLAN trunking**, and **inter-VLAN routing**.

- The demonstration of **VLAN isolation** illustrated the efficacy of establishing discrete VLANs to restrict communication between devices at *Layer 2*, enhancing security and optimizing traffic management. This demonstrated the importance of segmenting network traffic to enhance efficiency and security.
- **VLAN trunking** allows devices that are *physically apart* and connected to different switches to be *logically* connected within the same network.
- **Inter-VLAN** routing was implemented through a *router on a stick* configuration, wherein the router assured communication between devices situated within disparate VLANs by forwarding packets through its subinterfaces. This demonstrated how inter-VLAN routing enables cross-VLAN communication while maintaining the logical separation provided by VLANs.

Overall, the lab highlighted the important role of VLANs in designing scalable, efficient, and secure networks. Through VLAN isolation, trunking, and inter-VLAN routing, the lab illustrated how VLANs are used to segment, extend, and interconnect network traffic in modern network designs.

The figures 3.3 and 3.4 show the schema of the topology after mission 2 and 3.

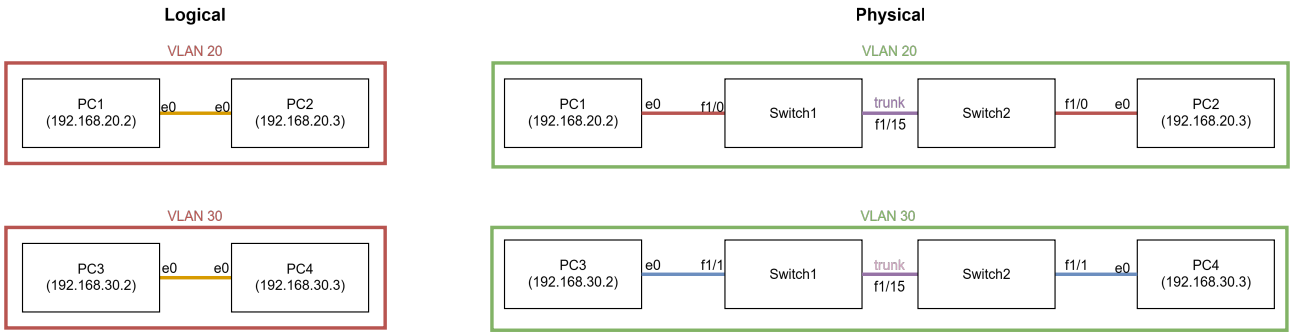

Figure 3.3: Schemas of the physical and logical topology after mission 2

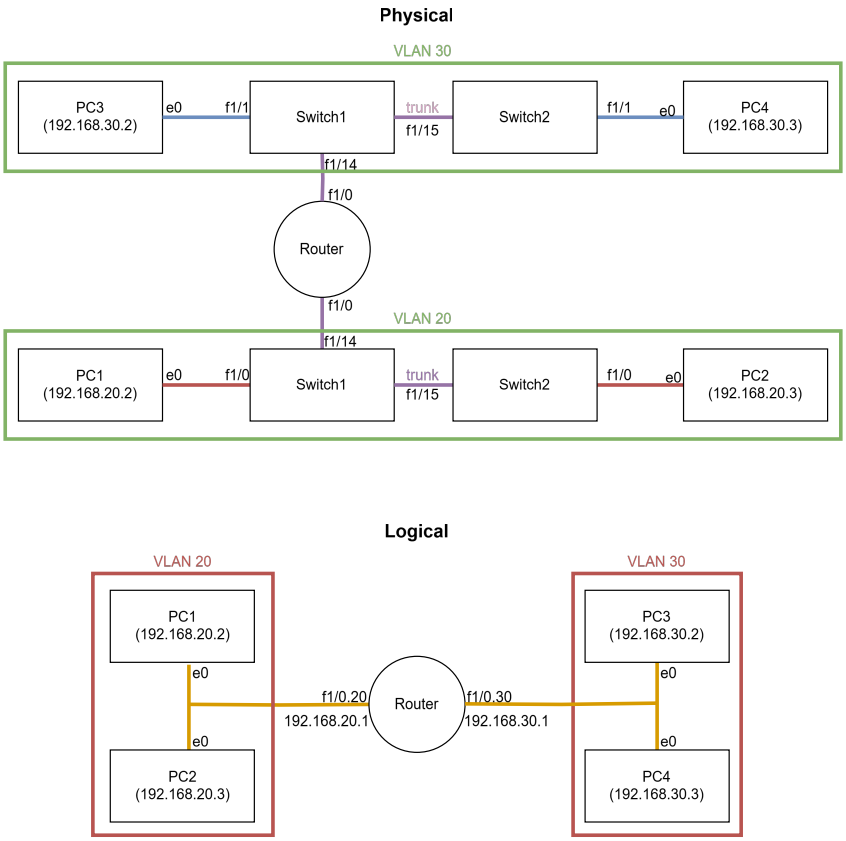

Figure 3.4: Schemas of the physical and logical topology after mission 3

3.3 Bonus question - Security

Security

What are the opportunities (in terms of security) offered by that inter-VLAN routing ?

Inter-VLAN routing provides several opportunities for enhancing security. One key benefit is **traffic segmentation**: by isolating different types of traffic into separate VLANs, you can limit access to sensitive data (like limiting the range of broadcasts from layer 2 : ARP, DHCP, MAC addresses,...) and restrict communication between devices that do not need to communicate.

Another advantage is the use of Access Control Lists. Routers can be configured with ACLs to control which devices or networks can access other VLANs, allowing for more granular security policies between VLANs.