Advanced Topics in Networking

Lab 4

VLAN

Patryk Figiel

January 8, 2025

Contents

1. Goal of the lab

The goal of this lab is to design and implement a network topology that demonstrates VLAN segmentation, VLAN tagging, and Inter-VLAN communication. The lab involves configuring VLANs on Layer 2 and Layer 3 switches, enabling communication between different VLANs using an L3 switch and a router. This setup highlights the role of VLANs in improving network efficiency, security, and manageability.

2. Preparations

The initial setup of the lab involved configuring Layer 2 (L2) and Layer 3 (L3) switches in GNS3 on my original operating system. However, I encountered multiple technical issues during this phase, which hindered the completion of the lab. After several attempts to resolve these problems, I switched to a Linux-based operating system (Ubuntu), where I installed GNS3 and all the necessary applications to execute the lab successfully. To ensure a clear understanding of VLAN tagging and Inter-VLAN routing, I studied provided examples and used them as a guide during the configuration process.

3. The main task

The main task of this lab involves creating and configuring a network topology with two distinct sections, each illustrating different aspects of VLAN configuration and communication. Below is the detailed breakdown of the topology.

3.1. Topology design

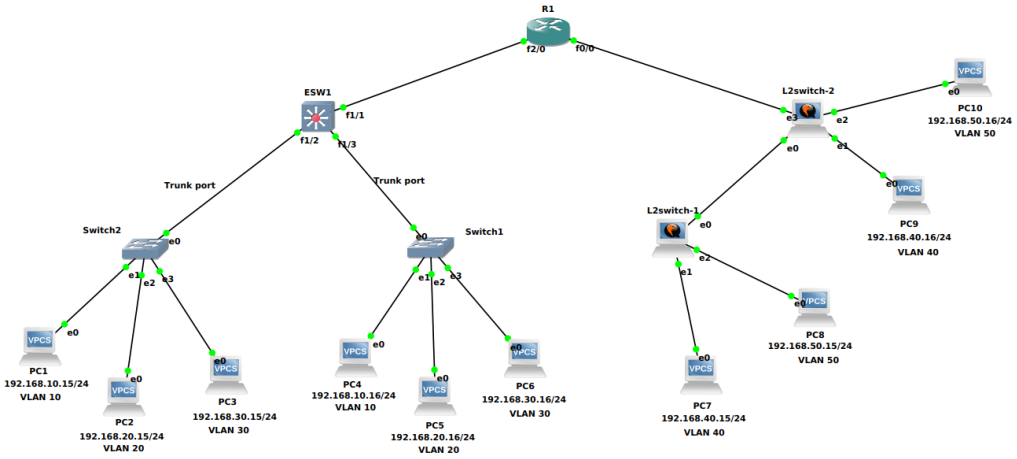

Figure 1. Network topology

Left Network

- The core of the left network is an L3 switch (ESW) configured to handle three VLANs: VLAN 10, VLAN 20, and VLAN 30
- Switches are connected to the ESW switch via trunk ports with dot1q encapsulations
- Switches were configured to have appropriate types of connections on the ports, such as:
  - Port 0 - dot1q trunk
  - Port 1 - access port assigned to VLANs
  - Port 2 - access port assigned to VLANs
  - Port 3 - access port assigned to VLANs
- All devices in this network connect to the ESW through access ports assigned to their respective VLANs
- The ESW is connected to the router through a trunk, enabling communication between VLANs and the right network
- On the router's interface `f2/0`, default gateways are set for each network in the VLANs:
  - VLAN 10: `192.168.10.1`

  - VLAN 20: `192.168.20.1`
  - VLAN 30: `192.168.30.1`
- Dot1q encapsulation is also enabled on the router's subinterfaces for VLAN communication

Right Network

- The core of the right network consists of two Layer 2 (L2) switches connected via a trunk port with dot1q encapsulation.
- These switches are configured to handle two VLANs: VLAN 40 and VLAN 50.
- Appropriate port configurations were applied, such as:
  - Trunk ports between the two switches to allow VLAN traffic.
  - Access ports assigned to VLAN 40 and VLAN 50 for connecting devices.
- One of the L2 switches is connected to the router through a trunk port, enabling inter-VLAN communication and connection to the left network.
- On the router's interface `f0/0`, subinterfaces are configured for each VLAN:
  - VLAN 40: `192.168.40.1`
  - VLAN 50: `192.168.50.1`
- Dot1q encapsulation is enabled on the router's subinterfaces to handle tagged VLAN traffic from the L2 switches.

3.2. Configuration Process

The configuration process began with setting up VLANs on the L3 switch (ESW1). VLANs were created using the `vlan` command. Trunk ports were then configured on the L3 switch to connect to the other devices, using the `switchport mode trunk` and `switchport trunk encapsulation dot1q` commands. However, no IP addresses were assigned to the ESW1 switch itself, as the router (R2) handled IP addressing.
On the router (R2), subinterfaces were configured for each VLAN to serve as gateways. The `interface` command was used to create subinterfaces, followed by `encapsulation dot1q` to enable VLAN tagging and `ip address` to assign IP addresses for each VLAN.
For the right network, VLANs were created on the L2 switches using the `vlan` command. Trunk ports between the switches and between one switch and the router were configured using `switchport mode trunk` and `switchport trunk encapsulation dot1q` commands. The router's subinterfaces were configured similarly to the left network, enabling inter-VLAN routing.
These steps ensured the proper segmentation of traffic and inter-VLAN communication across both networks, with the router acting as the gateway for each VLAN.

3.3. Verification

To verify the configuration, the following steps and commands were used:

- **VLAN Configuration:** The command `show vlan-switch` and `show vlan brief` were used to ensure VLANs were correctly created on the switches

```
ESW1#show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/4, Fa1/5, Fa1/6, Fa1/7
                                                Fa1/8, Fa1/9, Fa1/10, Fa1/11
                                                Fa1/12, Fa1/13, Fa1/14, Fa1/15
10   VLAN0010                         active    Fa1/0
20   VLAN0020                         active
30   VLAN0030                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0

ESW1#
```

Figure 2. Command on ESW1

```
vIOS-L2-01>show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
40   VLAN0040                         active    Gi0/1
50   VLAN0050                         active    Gi0/2
100  VLAN100                          active
200  VLAN0200                         active
300  VLAN0300                         active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
vIOS-L2-01>
```

Figure 3. Command on L2-2 switch

- **Trunk Ports:** The command `show interfaces trunk` verified that trunk links were active and dot1q encapsulation was in use

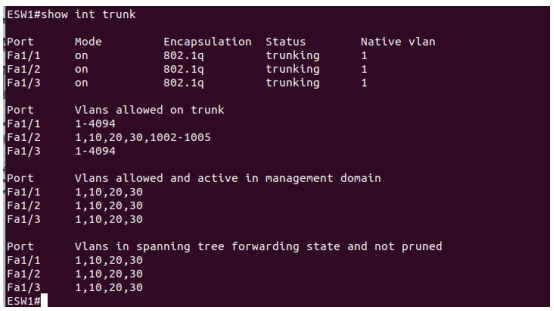

Figure 4. Command on ESW1

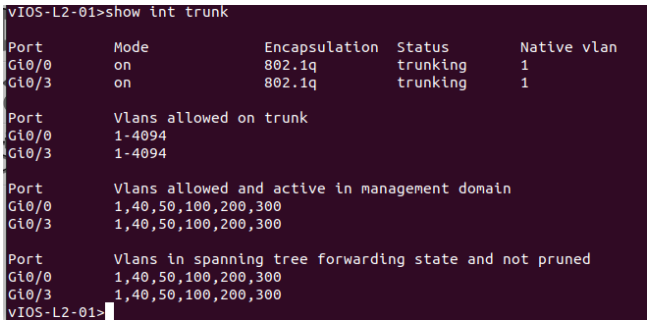

Figure 5. Command on L2-2 switch

- **Interface Status:** The command `show interfaces status` confirmed that all interfaces were up and in the correct mode (access or trunk)

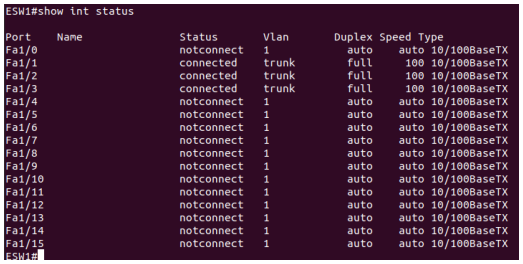

Figure 6. Command on ESW1

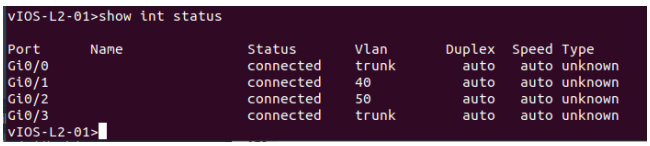

Figure 7. Command on L2-2 switch

- **Ping Tests Inside networks:** Ping tests were performed to confirm VLAN communication between different VLANs

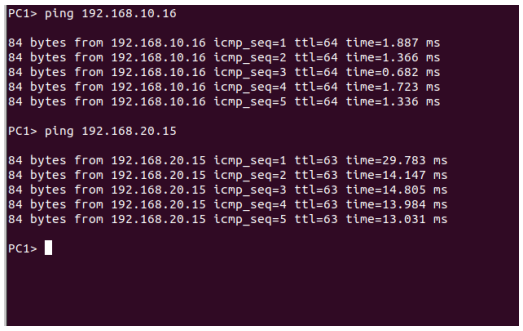

Figure 8. Command on PC1

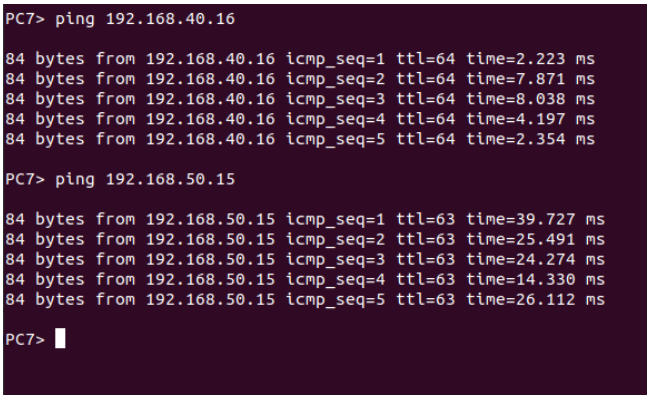

Figure 9. Command on PC7

- **Ping Tests between networks:** Ping tests were perfomed to confirm the connection between networks through the router R1

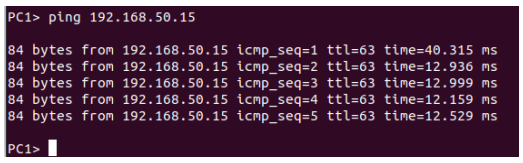

Figure 10. Command on PC1

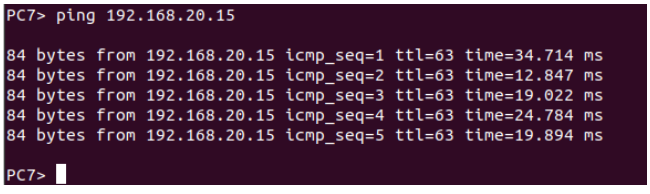

Figure 11. Command on PC7

These tests confirmed that VLANs, trunk ports, and inter-VLAN routing were properly configured and operational.

4. Theorotical part

4.1. Inter-VLAN Communication

Virtual Local Area Networks (VLANs) are logical network segments created to improve security, efficiency, and traffic management by isolating devices into separate groups. However, VLANs are isolated by default, meaning devices in one VLAN cannot directly communicate with those in another. Inter-VLAN communication is the process that enables data exchange between devices in different VLANs.

To achieve inter-VLAN communication, a Layer 3 device such as a router or a Layer 3 switch is required. Two commonly used methods include:
1. Router-on-a-Stick: This involves configuring a single router interface into multiple sub-interfaces, each associated with a unique VLAN and subnet. The router is connected to the switch via a trunk link, which carries traffic for all VLANs.
2. Layer 3 Switching: A Layer 3 switch integrates switching and routing functionalities, offering a more efficient solution for inter-VLAN communication. It uses Switched Virtual Interfaces (SVIs), which are logical interfaces configured for VLAN routing. This method is suitable for larger networks, as it enables high-speed routing directly within the switch, reducing latency and improving throughput.

By enabling devices in separate VLANs to communicate, inter-VLAN communication ensures that segmented network resources remain accessible without compromising the benefits of VLAN isolation.

4.2. VLAN Tagging

VLAN tagging is the technique used to identify the VLAN to which a data frame belongs as it traverses shared network links. The IEEE 802.1Q standard is widely employed for this purpose. It introduces a 4-byte tag into the Ethernet frame, containing a VLAN ID that specifies the frame's VLAN.

Two types of ports in VLAN tagging are crucial to understand:
1. Access Ports: These ports are used to connect end devices and carry untagged traffic for a single VLAN. When frames are sent or received on access ports, no VLAN tags are used, ensuring simplicity for endpoint devices.
2. Trunk Ports: These are used to carry traffic for multiple VLANs between switches or between switches and routers. Trunk ports append tags to frames to indicate their VLAN, allowing devices to correctly forward and segregate data for different VLANs.

The tagging mechanism ensures proper traffic segregation and facilitates the management of VLANs across shared links. On access ports, tags are stripped before delivery to end devices, ensuring compatibility.

5. Summary

This lab focused on designing and configuring a network with VLANs, trunking, and inter-VLAN routing. The left network used an L3 switch (ESW1) to segment traffic into VLANs 10, 20, and 30, with trunking between switches and the router. The right network consisted of L2 switches with VLANs 40 and 50, also utilizing trunking to ensure communication with the router. The router facilitated inter-VLAN routing using subinterfaces for each VLAN, allowing communication between different VLANs. Verification through ping tests confirmed that the VLANs were correctly configured and communication between networks was operational.