VILNIUS TECH

FACULTY OF ELECTRONICS

COMPUTER ENGINEERING AND TELECOMMUNICATIONS DEPARTMENT

LABORATORY WORK #5

# VLAN

Student: Mark Mikula

Teacher: Artūras Medeišis

Vilnius, 2025

## Contents



## Objective

The primary objective of this lab work was to familiarise with VLAN networking principles and learn to configure switches and routers to manage intra- and inter-VLAN communication

This involved examining a scenario where two virtual subnets (VLANs) were created on a simulated commercial company's LAN to serve different groups of employees. The lab aimed to demonstrate how dividing a LAN into smaller subnets, using VLANs, can improve overall network efficiency by reducing broadcast traffic, and potentially allow for other optimisations like different security settings or connections to different file servers for each VLAN

## Topology Overview

The LAN scenario featured a Cisco 1941 router connected to a Cisco Catalyst 3560 switch

End devices (desktop workstations and laptops) were connected to the switch. Two virtual subnets (VLANs) were created: VLAN ID 10 for desktop workstations (intended for administrative staff) and VLAN ID 20 for work desks with laptops (potentially for travelling salesmen). Assigning a terminal device to a specific VLAN is determined by the switch port it is connected to

## Part 1: Creating VLAN Subnets

This part focused on configuring the network for inter-VLAN routing using a router connected to the switch via a single link.

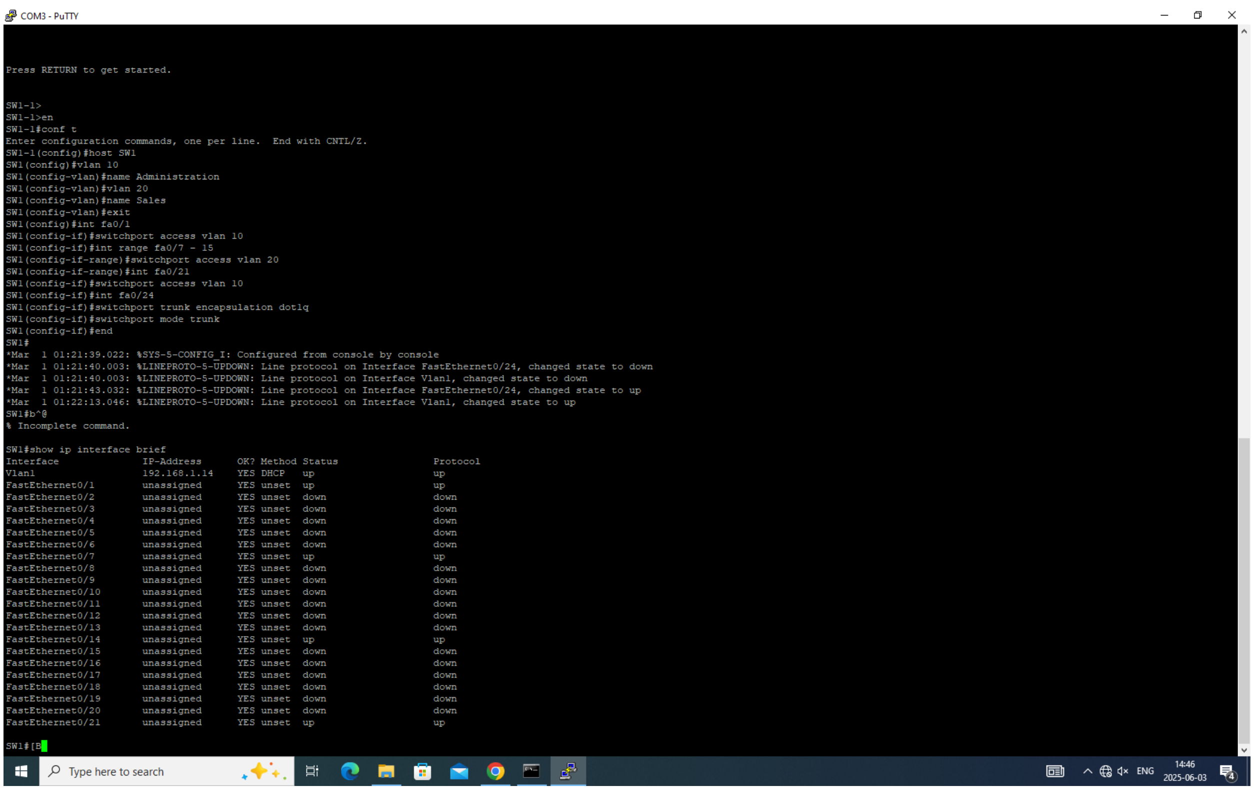
1.

Router Configuration: The Cisco 1941 router (hostname R1) was configured

This involved creating virtual subinterfaces on the GigabitEthernet0/1 port. Subinterface Gi0/1.10 was created for VLAN 10, and Gi0/1.20 for VLAN 20. Each subinterface was configured with IEEE 802.1q encapsulation specifying the corresponding VLAN ID (encapsulation dot1Q 10 for VLAN 10, encapsulation dot1Q 20 for VLAN 20). Unique IP addresses were assigned to these subinterfaces to serve as default gateways for each VLAN: 10.0.10.1/24 for VLAN 10 and 10.0.20.1/24 for VLAN 20. DHCP pools were configured on the router to service each VLAN subnet (LW5_VLAN10 for 10.0.10.0/24 with default-router 10.0.10.1, and LW5_VLAN20 for 10.0.20.0/24 with default-router 10.0.20.1). The physical interface Gi0/1 was set to an active state using the no shut command, implicitly activating its subinterfaces. The router configuration was verified using show ip interface brief

2.

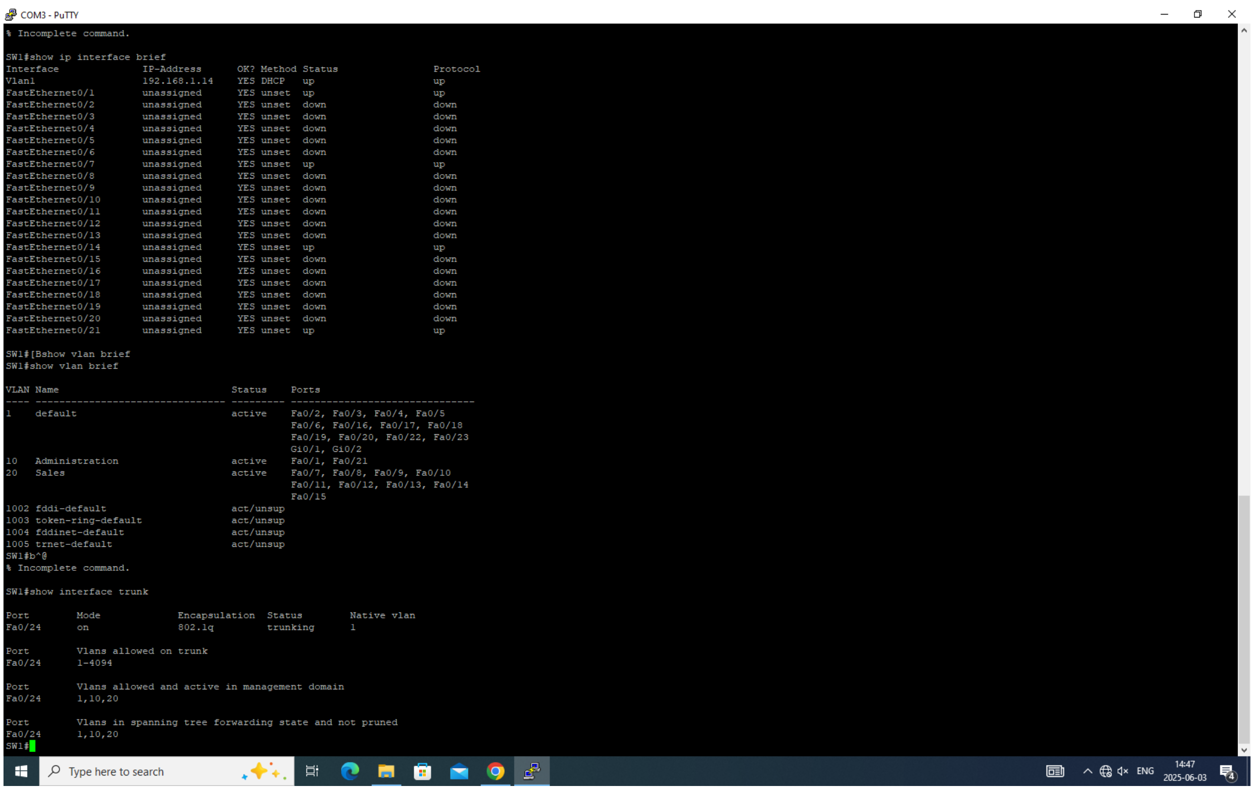
Switch Configuration: The Cisco Catalyst 3560 switch (hostname SW1) was configured




VLANs 10 and 20 were established and assigned logical names, "Administration" and "Sales" respectively. Switch ports connected to end devices were configured as access ports for specific VLANs. For example, ports like fa0/1 and fa0/21 were set as access ports for VLAN 10. A range of ports (fa0/7 - 15) was set up as access ports for VLAN 20 terminals.

The switch port connected to the router (fa0/24) was configured as a trunk port using switchport trunk encapsulation dot1q and switchport mode trunk. This trunk link allows the transfer of VLAN packets encapsulated according to the IEEE 802.1q standard, carrying traffic for multiple VLANs between the switch and the router. Switch configuration was verified using show vlan brief (to see VLANs and assigned ports) and show interface trunk (to check the active trunk status)

3.End Device Configuration: Terminal computers (desktop PCs as PC1, PC2, and laptops as Laptop1) were connected to the switch ports according to the diagram. The ipconfig /renew command was run on each computer to obtain IP configurations via DHCP from the router. Based on the configuration, devices were expected to receive IPs from the correct DHCP scopes. For example, Laptop 1 received 10.0.10.2 (VLAN 10), and PC1 and PC2 received 10.0.20.2 and 10.0.20.3 respectively (VLAN 20)




4.

Connectivity Testing: Ping commands (ping x.x.x.x) were run from each computer to check connectivity within the same VLAN and between different VLANs

Intra-VLAN communication (e.g., PC1 to PC2, both in VLAN 20) was expected to be successful. Inter-VLAN communication (e.g., Laptop 1 in VLAN 10 to PC1/PC2 in VLAN 20) involved the router for routing between the subnets.

5.

MAC Address Table Observation: The show mac address-table command was used on the switch to observe the MAC addresses learned on active ports and their association with specific VLAN subnets

. This table indicates how the switch learns the location (port and VLAN) of connected devices based on the source MAC addresses in frames it receives.

## Part 2: Configuring Switch for Autonomous VLAN Management (Layer 3 Switch)

This part explored the capability of a Layer 3 switch to perform inter-VLAN routing internally without relying on an external router

1.

Simulating Router Failure: The cable between the router and the switch was disconnected

2.

Observing Connectivity Change: Ping tests were repeated

It was observed that intra-VLAN packet transmission (e.g., between PC1 and PC2 in VLAN 20) continued to be successful. However, packet transmission between different VLAN subnets (e.g., Laptop 1 in VLAN 10 to PC1/PC2 in VLAN 20) stopped because the external router, previously handling the inter-VLAN routing at Layer 3, was disconnected

3.

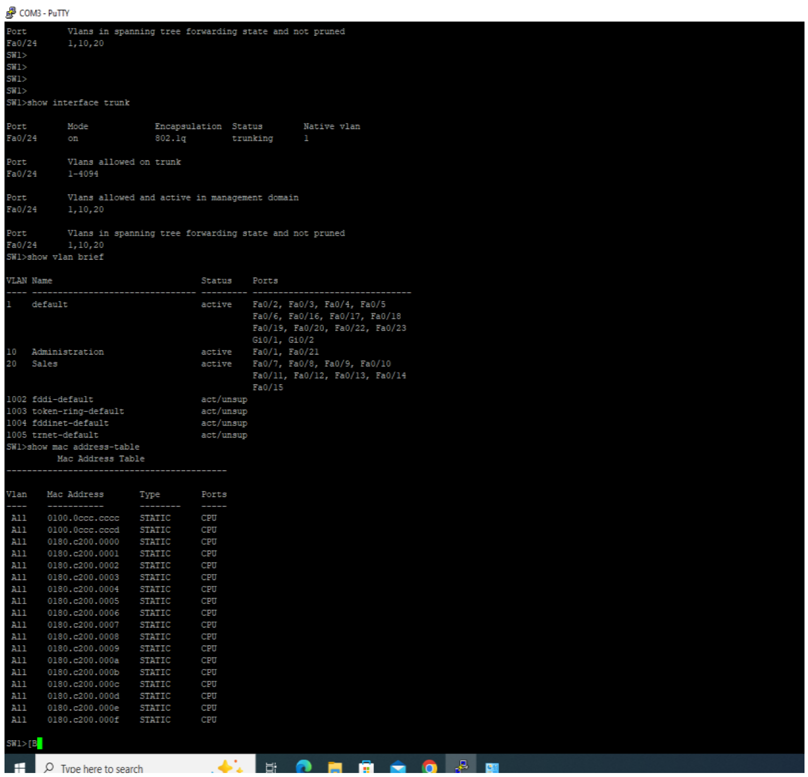
Configuring L3 Switch Functionality: The Cisco Catalyst 3560 switch, being a Layer 3 switch, has autonomous IP routing functionality

Additional configuration was performed on the switch to enable it to route traffic between its served VLAN subnets. This involved initialising configuration for virtual interfaces associated with VLANs, known as Switched Virtual Interfaces (SVIs). SVIs were created for VLAN 10 (interface vlan 10) and VLAN 20 (interface vlan 20), and assigned the respective default gateway IP addresses (10.0.10.1/24 for VLAN 10 and 10.0.20.1/24 for VLAN 20). The IP routing mode was activated on the switch using the ip routing command

4.

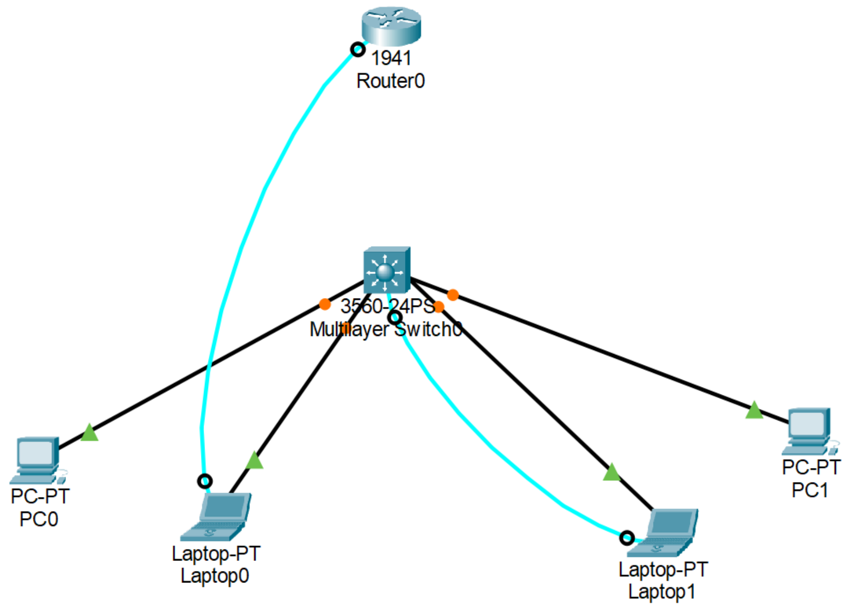
Retesting Connectivity: Ping commands were used again to check communication within and between VLANs

With the L3 switch now handling routing, both intra-VLAN and inter-VLAN connectivity were restored.




5.

Verifying L3 Switch Status: The commands show ip interface brief (to see active IP interfaces, including the SVIs) and show ip route (to view the switch's routing table) were used to verify the correct configuration and operational status of the L3 switch functionality




## Conclusion

This lab successfully provided hands-on experience in setting up and managing VLANs using both the "router-on-a-stick" model with an external router and the autonomous routing capabilities of a Layer 3 switch

Creating VLAN subnets effectively separated network traffic, demonstrating enhanced security and efficiency by reducing broadcast domains. The lab successfully validated the setup through the implementation of VLAN IDs, DHCP services via router subinterfaces/SVIs, and the configuration of access and trunk ports on the switch according to the IEEE 802.1q standard. Configuring and testing the Layer 3 switch for independent VLAN management and IP routing was a key outcome of the second part. This exercise significantly improved practical skills in network configuration and troubleshooting related to VLANs and inter-VLAN routing. The lab report included descriptions of results, illustrative screenshots, and comments on the configurations and connectivity tests.