**LABORATORY WORK NO. 9**

VLANs, Trunking and Inter-VLAN routing

1. Objectives

At the end of the practical activity, students will be able to define and classify Virtual Local Area Networks (VLANs), explain the purpose of trunking and inter-VLAN routing and configure VLAN-based networks in a multi-switched environment.

2. Theoretical considerations

The current practical work focuses on the Data Link and Network layers of the ISO/OSI stack (Figure 10.1).

Diagram

Description automatically generated

**Figure 10.1** *Network stack models and PDU naming in each level. The arrows indicate the addressed layers in the current activity*

**2.1 VLANs**

A VLAN is a partition of the set of devices connected to the local network. Grouping into VLANs can be done according to different criteria such as the role of users or the type of traffic. This grouping can be done regardless of the physical location of the devices or users (Figure 10.2). VLANs work by logically segmenting the network into broadcast domains, with each VLAN representing a different broadcast domain. The switch maintains a different bridging table for each VLAN. Devices in a VLAN are restricted to communicating only with devices in the same VLAN. Connectivity between VLANs is facilitated by routers.

The benefits of VLANs are:

* smaller broadcast domains;
* reduced cost;
* increased network performance;
* increased scalability;
* increased security;
* better management.

Common types of VLANs:

* Default VLAN – Also known as VLAN 1, cannot be deleted or renamed. All switch ports are members of VLAN 1 by default;
* Data VLAN – Data VLANs are commonly created for specific groups of users or devices. They carry user generated traffic;
* Voice VLAN – Voice VLAN is created because this type of traffic requires assured bandwidth and delay less than 150 ms from source to destination;
* Native VLAN – This is the VLAN that carries all untagged traffic. This is traffic that does not originate from a VLAN port;
* Management VLAN – This is a VLAN that is created to carry network management traffic including SSH, SNMP, Syslog, and more.

Diagram

Description automatically generated

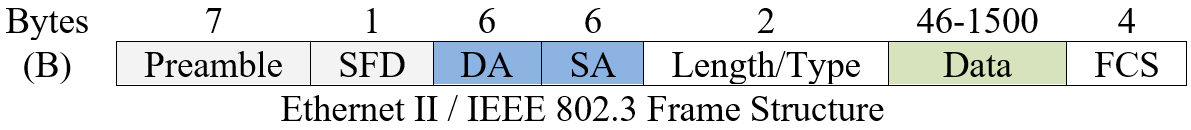
**Figure 10.2** *VLANs in a multi-switched environment*

**2.2 Trunking**

A trunk is a point-to-point link between two network devices that does not belong to a specific VLAN and carries more than one VLAN. It extends VLANs across the network and enables devices connected to different switches, but in the same VLAN, to communicate through the switched network.

The ports assigned to VLANs are configured in access mode and use standard Ethernet frame headers. This header does not contain information about the VLAN to which the frame belongs. When the frames are forwarded between switches on trunk lines, the VLAN membership information must be transmitted with the frames. Therefore, when Ethernet frames are placed on the trunk, the VLAN membership information is added, the frames using 802.1Q headers instead of Ethernet headers. Adding information about VLANs is called tagging, and 802.1Q headers also add other information to the frames beside VLAN membership.

The Figure 10.3 presents the Ethernet II/IEEE 802.3 frame structure used in ports configured in access mode and the IEEE 802.1Q frame structure used in ports configured in trunk mode. The following section describes the meaning of the Tag control information fields.



Chart

Description automatically generated

**Figure 10.3** *Ethernet II/IEEE 802.3 and IEEE 802.1Q frames*

VLAN tag control information field consists of the following fields:

* Type - Tag protocol ID (TPID) value. For Ethernet, it is set to hexadecimal 0x8100.
* User priority - Supports level or service implementation.
* Canonical Format Identifier (CFI) - Enables Token Ring frames to be carried across Ethernet links.
* VLAN ID (VID) - VLAN identification number, supports up to 4096 VLAN IDs.

In the example below (Figure 10.4), Laptop1 connected to switch S2 on access port Fa0/6 in VLAN 10 is communicating with Laptop2 connected to another switch, S3, on access port Fa0/7 in the same VLAN, VLAN 10. The ports between the switches are configured in trunk mode. Laptop 1 sends a packet to Laptop 2. When the packet enters switch S2 on access port Fa0/6, the packet is encapsulated into an Ethernet II/IEEE 802.3 frame. The S2 switch forwards the packet on the Fa0/1 trunk port encapsulating the packet into an Ethernet 802.1Q frame. The VLAN number is set to 0x00a (VLAN 10).

Diagram, application

Description automatically generated

**Figure 10.4** *Communication in the same VLAN*

**2.3 Inter-VLAN routing**

Layer 2 switches don’t forward traffic from one VLAN to another. The traffic between VLANs is forwarded using Layer 3 devices, routers or Layer 3 switches, the process being called Inter-VLAN routing. There are three options for inter-VLAN routing:

* Legacy inter-VLAN routing;
* Router-on-a-Stick;
* Layer 3 switching using SVIs.

The router-on-a-stick approach (see Figure 10.5) uses one of the router’s physical interfaces for inter-VLAN routing.

* Logical subinterfaces are created on the physical interface; one subinterface per VLAN; the subinterfaces use 802.1Q encapsulation to process VLAN tags;
* Each VLAN is assigned a different network/subnetwork address;
* Each subinterface is configured in a VLAN with an IP address from the VLAN it represents;
* VLAN hosts are assigned IP addresses from their corresponding VLANs; each host is configured to use as default gateway the subinterface representing its VLAN.
* When a host in a VLAN communicates with a host in a different VLAN, it sends the packets to its own gateway, in its own VLAN; the router internally routes between the VLANs using subinterfaces as the VLAN networks are present in the routing table as connected; the router receives the packets on the source VLAN subinterface and forwards the routed traffic as VLAN-tagged for the destination VLAN out the trunk link

A picture containing line chart

Description automatically generated

**Figure 10.5** *Router-on-a-stick option for inter-VLAN routing*

3. Practical activity

3.1 Discuss the theoretical aspects presented in this chapter.

3.2 Consider the network topology in Figure 10.6:

A picture containing diagram

Description automatically generated

**Figure 10.6** *Test network topology*

**Step 1:** Before configuring the network devices, discuss the IPv4 address assignment in the Table 10.1:

**Table 10.1** *IPv4 addresses for the test network*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Netmask** | **Gateway** |
| Laptop 0 | Fa0 | 172.16.20.2 | 255.255.255.0 | 172.16.20.1 |
| Laptop 1 | Fa0 | 172.16.10.2 | 255.255.255.0 | 172.16.10.1 |
| Laptop 2 | Fa0 | 172.16.10.3 | 255.255.255.0 | 172.16.10.1 |
| Laptop 3 | Fa0 | 172.16.20.3 | 255.255.255.0 | 172.16.20.1 |
| R1 | Fa0/0.10 | 172.16.10.1 | 255.255.255.0 | - |
| R1 | Fa0/0.20 | 172.16.20.1 | 255.255.255.0 | - |

**Step 2:** Specify the host names for the networking devices (router and switches)

General syntax:

*Switch(config)#hostname host-name*

Description: Specifies or modifies the host name

Example:

*Switch(config)#hostname S2*

**Step 3:** Create VLAN 10 and 20 on all the switches and verify vlan information

General syntax:

*Switch(config)#vlan vlan\_id*

Description: Global configuration command that creates VLAN vlan\_id

*Switch(config-vlan)#name vlan\_name*

Description: Assigns a name to the VLAN

Example:

S2(config)#vlan 10

S2(config-vlan)#name Vlan10

S2(config-vlan)#exit

S2(config)#vlan 20

S2(config-vlan)#name Vlan20

General syntax:

Switch#show vlan

Switch#show vlan brief

Description: Displays VLANs information (the contents of the vlan.dat file )

**Step 4:** Assign ports to VLANs and verify the configuration

General syntax:

*Switch(config)#interface interface\_id*

Description: Enters interface configuration mode

*Switch(config-if)#switchport mode access*

Description: Sets the port to access mode

*Switch(config-if)#switchport access vlan vlan\_id*

Description: Assigns the port to a VLAN

Example:

S2(config)#interface fastEthernet 0/6

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 10

S2(config-if)#exit

S2(config)#interface fastEthernet 0/5

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 20

General syntax:

Switch#show vlan

Switch#show vlan brief

Description: Displays VLANs information (the contents of the vlan.dat file)

**Step 5:** Set the switch ports connected to other networking devices to trunk mode and verify the configuration

General syntax:

*Switch(config)#interface interface\_id*

Description: Enters interface configuration mode

*Switch(config-if)#switchport mode trunk*

Description: Forces the link to be a trunk link

Example:

S2(config)#interface fastEthernet 0/1

S2(config-if)#switchport mode trunk

General syntax:

*Switch#show interfaces trunk*

Description: Displays trunking information for the switch

**Step 6:** Configure the hosts with the IP addressing information in the figure (IP address, netmask and gateway) and test the connectivity between them

a. ping <target IP>

b. tracert <target IP>

**Step 7:** Configure Inter-VLAN routing and test the connectivity between hosts in different VLANs

General syntax:

*Router(config)#interface interface\_id*

Description: Enters interface configuration mode

*Router(config-if)#no shutdown*

Description: Enables the interface

*Router(config-if)#exit*

Description: Returns to the global configuration mode

*Router(config)#interface interface\_id.subinterface\_id*

Description: Creates a subinterface on an interface

*Router(config-subif)#encapsulation dot1Q vlan\_id*

Description: Specifies IEEE 802.1Q as the VLAN tagging method for VLAN vlan\_id on this subinterface

*Router(config-subif)#ip address ip\_address netmask*

Description: Adds an IP address and a netmask on this subinterface

*Router(config-subif)#end*

Description: Returns to the privileged exec mode

*Router#show ip route*

Description: Displays the routing table

Example:

R1(config)#interface fastEthernet 0/0

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#interface fastEthernet 0/0.10

R1(config-subif)#encapsulation dot1Q 10

R1(config-subif)#ip address 172.16.10.1 255.255.255.0

R1(config-subif)#exit

R1(config)#interface fastEthernet 0/0.20

R1(config-subif)#encapsulation dot1Q 20

R1(config-subif)#ip address 172.16.20.1 255.255.255.0

*R1(config-subif)#end*

*R1#show ip route*

Test the connectivity using:

a. ping <target IP>

b. tracert <target IP>

**Step 8:** In the simulation mode, using *ping* command, analyze the communication between hosts in the same VLAN and between hosts in different VLANs