LABORATORY WORK NO. 3

VIRTUAL LOCAL-AREA NETWORKS AND TRUNKING

1. Objectives

The objective of this work is Virtual Local-Area Network definition, advantages, classification and identification and trunking knowledge.

2. Theoretical considerations

2.1 Virtual Local-Area Network definition and advantages

An important feature of Ethernet switching is the Virtual Local-Area Network (VLAN). A VLAN is a logical grouping of devices or users by function, department, or application despite the physical LAN segment location. Devices on a VLAN are restricted to only communicating with devices that are on their own VLAN. Connectivity between different VLAN-s is provided by routers. VLAN-s function by logically segmenting the network into different broadcast domains, each VLAN representing a broadcast domain. The switch maintains a separate bridging table for each VLAN. VLAN benefits are increased overall network performance, enhanced scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.

2.2 VLAN classification and identification

There are two types of VLAN membership: static, dynamic and protocol based. Static membership VLAN-s are also referred to as port-based or port-centric membership VLAN-s. In this type of VLAN membership the ports are assigned to a specific VLAN and all users of the same port are members of the VLAN to which the port was assigned. This type of VLAN membership is simple, fast and easy to manage because no complex lookup tables are required for VLAN segmentation. Static membership VLAN-s are usually implemented in networks where movement of the devices is rare and controlled. Management VLAN is VLAN 1 which is the default Ethernet

VLAN and the default VLAN for every port in the switch. This VLAN may not be deleted. Dynamic membership VLAN-s are created through network management software. In this type of VLAN membership the ports are dynamically assigned to a specific VLAN based on the MAC address of the device connected to the switch port. When a device is connected to a switch port, it queries a MAC address-to-VLAN mapping database within the switch for a VLAN membership and the switch dynamically assigns that port to the proper VLAN for that host. Multiple devices can be connected to switch port if they are all in the same VLAN. Dynamic membership VLANs are usually implemented in networks where movement of the devices is frequent and uncontrolled. Protocol based membership VLAN-s are similar to dynamic membership VLAN-s replacing MAC addresses used by these with logical or IP addresses. This membership VLAN type is no longer common because of DHCP.

The frame headers are encapsulated or modified to reflect a VLAN ID before the frame is sent over the link between switches. Before forwarding to the destination device, the frame header is changed back to the original format. The IEEE 802.1Q protocol is an IEEE standard for identifying VLAN-s by inserting a VLAN identifier into the frame header, process referred to as frame tagging or internal tagging. This is the most common method used for VLAN identification. The structure of this frame is presented in figure 10.1. Inter-Switch Link (ISL) is a Cisco proprietary encapsulation protocol that maintains VLAN information as traffic flows between switches and routers. ISL inserts a 26-byte header and a 4-byte cyclic redundancy check (CRC) to each frame. The structure of this frame is presented in figure 10.2.

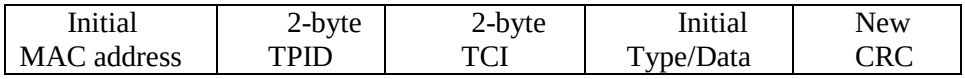

Figure 3.1 *802.1Q frame*

TPID (*Tag Protocol Identifier*) indicates that the frame carries the 802.1Q/802.1p tag information and has a fixed value of 0x8100.

TCI (*Tag Control Information*) contains the following fields: 3-bit user priority, 1-bit canonical format indicator (CFI) and 12-bit VLAN identifier (VID)-Uniquely identifies the VLAN to which the frame belongs.

26-byte header	Encapsulated frame	4-byte CRC

Figure 3.2 *ISL frame*

An important consideration in VLAN-s definition is the IP addressing scheme because a one-to-one correspondence between VLAN-s and IP subnets is strongly recommended. Each VLAN must have a unique Layer 3 network address assigned to enable routers to switch packets between VLAN-s.

2.3 Trunking

Inter-switch VLAN communication can be implemented in two ways. The first method requires one link for each VLAN shared across two switches to carry the traffic for that VLAN. This method is not scalable because it requires too many switch ports. The second method requires only one trunk link for all VLAN-s shared across two switches to carry the traffic for all VLAN-s. A trunk link is a point-to-point link that supports several VLAN-s. The trunk link does not belong to a specific VLAN. In order to identify VLAN-s, the trunk link uses IEEE 802.1Q or ISL protocols.

3. Lab activity

3.1 VLAN creation and assignation

Cable the network presented in the figure 3.3.

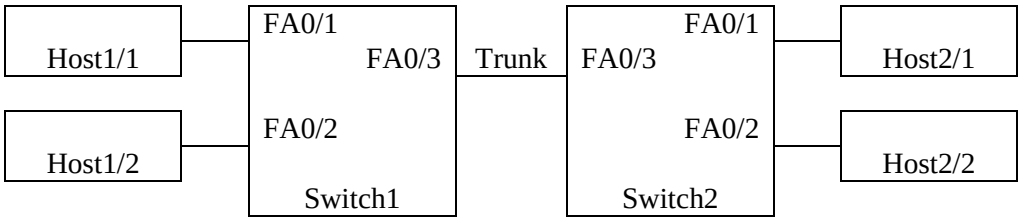

Figure 3.3 *VLAN test network*

For VLAN1 and VLAN2 consider 172.27.0.0/16 and respectively 172.28.0.0/16 as network addresses.

Assign to every host IP addresses from VLAN1.

Connect to Switch1, enter Privileged EXEC mode and completely erase the switch configuration.

Connect to Switch1, enter Privileged EXEC mode and view the vlan interface information with one of the the `show vlan` or `show vlan brief` commands.

View only the information for a certain vlan with one of the `show vlan id` *`vlan_number`* or `show vlan name` *`vlan_name`* commands.

Verify the connectivity between hosts connected to Switch1 with the `ping` command.

Connect to Switch1 and enter the global configuration mode.

Enter the config-vlan mode with the `vlan` *`vlan_number`* command. Vlan_number is 2 and is the VLAN that will be created.

Name the created VLAN with the name *`vlan_name`* command.
Exit back to the Privileged EXEC mode with the `end` command.
Issue `show vlan` command.
Verify the connectivity between hosts connected to Switch1.
Assign to Host1/2 an IP address from VLAN2.
Enter the global configuration mode.
Enter the interface mode. Choose interface 0/2.
Change a switchport to a non-default VLAN with the `switchport mode access` command.
Re-assign the port from default VLAN to VLAN2 with the `switchport access vlan` *`vlan_number`* command.
Exit to the Privileged EXEC mode with the `end` command.
Issue `show vlan` command.
Verify the connectivity between hosts connected to Switch1.

Follow the same steps for Switch2 and Host 2/2 to create VLAN2, re-assign port 0/2 to this VLAN and assign to Host2/2 an IP address from VLAN2.

3.2 Trunking implementation

Verify the connectivity between the hosts that belong to the same VLAN connected to different switches.

Connect to Switch2, enter Privileged EXEC mode and view the trunking information with the `show interfaces trunk` command.
Enter the global configuration mode.
Enter the interface mode. Trunking interface will be considered.
Set trunking mode to access with the `switchport mode access` command.
Exit to the Privileged EXEC mode and issue `show vlan` command.
Issue `show interfaces trunk` command.
Verify the connectivity between the hosts that belong to the same VLAN connected to different switches.
Enter the global configuration mode.
Enter the interface mode. The same interface will be considered.
Set trunking mode to trunk with the `switchport mode trunk` command.
Exit to the Privileged EXEC mode and issue `show vlan` command.
Issue `show interfaces trunk` command.
Verify the connectivity between the hosts that belong to the same VLAN connected to different switches.

3.3 VLAN deletion

Remove VLAN2 from one interface with the `no` form of the command.
Issue `show vlan` command.
Verify the connectivity between hosts.
Remove VLAN2 from the VLAN database with the `no` form of the command.
Issue `show vlan` command.
Verify the connectivity between hosts.
Remove any existing VLAN information by deleting the VLAN database file vlan.dat from the flash directory with the `delete flash:vlan.dat` command.
Issue `show vlan` command.
Verify the connectivity between hosts.

Notes