**Riga Technical University  
Institute of Photonics, Electronics, and Electronic Communications**

**RAE475 Telecommunications and Data Networks**

**3nd Laboratory Work: VLAN LAB WITH SECURITY ENHANCEMENTS**

DITEF TI

2025

# Summary

Standards: IEEE 802.1Q, IEEE 802.1ad

Virtual Local Area Network (VLAN) is a Layer 2 method that allows multiple Virtual LANs on a single physical interface (ethernet, wireless, etc.), giving the ability to segregate LANs efficiently.

You can use MikroTik RouterOS (as well as Cisco IOS, Linux, and other router systems) to mark these packets as well as to accept and route marked ones.

As VLAN works on OSI Layer 2, it can be used just like any other network interface without any restrictions. VLAN successfully passes through regular Ethernet bridges.

You can also transport VLANs over wireless links and put multiple VLAN interfaces on a single wireless interface. Note that as VLAN is not a full tunnel protocol (i.e., it does not have additional fields to transport MAC addresses of sender and recipient), the same limitation applies to bridging over VLAN as to bridging plain wireless interfaces. In other words, while wireless clients may participate in VLANs put on wireless interfaces, it is not possible to have VLAN put on a wireless interface in station mode bridged with any other interface.

# 802.1Q

The most commonly used protocol for Virtual LANs (VLANs) is IEEE 802.1Q. It is a standardized encapsulation protocol that defines how to insert a four-byte VLAN identifier into the Ethernet header.

Each VLAN is treated as a separate subnet. It means that by default, a host in a specific VLAN cannot communicate with a host that is a member of another VLAN, although they are connected to the same switch. So if you want inter-VLAN communication you need a router. RouterOS supports up to 4094 VLAN interfaces, each with a unique VLAN ID, per interface. VLAN priorities may also be used and manipulated.

When the VLAN extends over more than one switch, the inter-switch link has to become a 'trunk', where packets are tagged to indicate which VLAN they belong to. A trunk carries the traffic of multiple VLANs; it is like a point-to-point link that carries tagged packets between switches or

### IEEE 802.1ad - VLAN Stacking (Q-in-Q)

IEEE 802.1ad, also known as Q-in-Q, is an extension of 802.1Q that allows multiple VLAN tags in a single Ethernet frame. This is often used by service providers to tunnel customer VLANs through their infrastructure.

* Outer VLAN (Provider VLAN): Used by the ISP to identify customer traffic.
* Inner VLAN (Customer VLAN): Used by the customer within their own network.
* Q-in-Q is commonly used in Metro Ethernet networks and MPLS/VPLS services.

## **Trunk vs. Access (Untagged) Ports**

VLANs can be configured on switch ports in different modes, depending on how they handle VLAN tags.

### Access Port (Untagged Port)

* Access ports are used for end devices such as computers, printers, IP phones, etc.
* These ports are assigned a single VLAN (PVID) and remove the VLAN tag before forwarding traffic to the device.
* Example: A PC connected to an access port for VLAN 10 will receive untagged traffic, and any traffic it sends will automatically be assigned to VLAN 10.

### Trunk Port (Tagged Port)

* Trunk ports carry multiple VLANs and are used between switches, routers, and access points.
* VLAN tags are preserved on trunk ports, allowing devices to identify which VLAN the packet belongs to.
* Example: A connection between a router and a switch typically requires a trunk port to transport VLANs.

### Hybrid Port

* Hybrid ports combine access and trunk modes.
* A hybrid port can carry multiple tagged VLANs while also having a default untagged VLAN (PVID).
* Often used for VoIP phones where the PC port is untagged, but the phone itself uses a tagged VLAN.

# **Lab OBJECTIVES**

* Configure VLANs on MikroTik using the single bridge method
* Set up trunk ports and access ports
* Set up vAP for clients and managment
* Implement firewall rules for VLAN isolation
* Configure VRRP for router redundancy
* Set up 802.1X authentication for secure network access

# **Lab Topology**

* Router: RB951−2HnD
* switch (L41G-2axD)
* end devices: Lab PC, mobile phone or Virtual Machine

|  |  |  |  |
| --- | --- | --- | --- |
| **VLAN** | **Name** | **Network** | **Devices (Ports)** |
| 10 | Management | 192.168.99.0/24 | Ether2 (Router1), Ether1 (Switch) |
| 100 | Servers (VM) | 10.0.0.0/24 | Ether2 (Switch) |
| 200 | Client | 172.16.0.0/28 | Ether4 (Switch) |
| Trunk | Trunk Link | Carries all VLANs | Ether5 (Router1) → Ether4 (Switch) |

Step 1: Configure VLANs on MikroTik R1 (RB951-2HnD)

1. Reset both board without configuration. For next section use the RB951-2HnD
2. Create VLANs
   1. Initial configuration

* Connect PC to ether3 (it will unused port in future)
* create the bridge: *interface/bridge add name=br-main protocol-mode=rstp*
* VLAN Filtering: Enable at the end to avoid disconnection. */interface/bridge/set br-main vlan-filtering=yes*
  1. Assign ports to bridge:
* ether2 (Management) untagged vlan: */interface/bridge/port add interface=ether2 pvid=10*
* ether5 (Trunk) tagged for all VLANs: */interface bridge port add interface=ether5 bridge=main-bridge frame-types=admit-only-vlan-tagged*
  1. Set VLANs under Bridge → VLANs
* VLAN 10 → **Tagged: Ether5**, **Untagged: Ether2: /interface/bridge/vlan/add bridge=bridge tagged=ether5,bridge untagged=ether2 vlan-ids=10**
* VLAN 100 → **Tagged: Ether5: /interface/bridge/vlan/add bridge=bridge tagged=ether5,bridge vlan-ids=100**
* VLAN 200 → **Tagged: Ether5 /interface/bridge/vlan/add bridge=bridge tagged=ether5,bridge vlan-ids=200**
* **Take the screenshot of */interface/bridge export* and put it in report with explanation of each step**

1. Create VLAN Interfaces

* vlan10-mgmt (VLAN ID 10) → **Bridge: main-bridge: */interface/vlan/add vlan-id=10 interface=main-bridge name=vlan10-mgmt comments=management***
* vlan100-servers (VLAN ID 100) → **Bridge: main-bridge: */interface/vlan/add vlan-id=100 interface=main-bridge name=vlan100-servers comments=servers***
* vlan200-servers (VLAN ID 200) → **Bridge: main-bridge: */interface/vlan/add vlan-id=200 interface=main-bridge name=vlan200-clients comments=clients***
* **Take the screenshot of */interface/vlan export* and put it in report with explanation difference from previous step**

1. Assign IP Addresses

Go to **IP → Addresses**:

* 192.168.99.1/29 → vlan10-mgmt
  + ***/ip/address/add interface=vlan10-mgmt address=192.168.99.1/29***
* 10.0.0.1/28 → vlan100-servers
* 172.16.0.1/24 → vlan200-clients

1. Configure DHCP Servers

Go to **IP → DHCP Server**:

* Enable **DHCP** for VLANs 10, 100, and 200.
* Ensure correct **IP Pools** are assigned.
* Example: ip/dhcp-server/setup → choose the e.g., vlan10-mgmt → Next till end → server done
* Repeat with another interfaces
* **Take the screenshot of */ip dhcp-server export* and put it in report**

1. Enable VLAN Filtering

* **Bridge → Enable VLAN filtering**, this will activate VLAN rules (check 2.1)
* connect PC to ether2, toggle the interface for PC side.
* **Take the screenshot of *ifconfig* (PC terminal), observe the IPand put it in report (explain why you got exactly this IP)**

Step 2: Configure VLANs on MikroTik SW1 (L41G-2axD)

**L41G-2axD** will be configurated as L3 switch with wifi AP

1. Connect L41G ether4 to ether4 RB951
2. Create a **Bridge**: switch-bridge: interface/bridge/add name=switch-bridge protocol-mode=rstp (!!!VLAN Filtering: Enable at the end to avoid disconnection)
3. Assign all available ports to bridge: ether1…ether4+wifi1, example:

* interface/bridge/port/add bridge=switch-bridge interface=ether1 pvid=10
* interface/bridge/port/add bridge=switch-bridge interface=ether2 pvid=100
* interface/bridge/port/add bridge=switch-bridge interface=ether3 pvid=200

1. in classical variation last port of switch used for trunk to next switch or hop (e.g. ether4)

* /interface bridge port add interface=ether4 bridge=switch-bridge frame-types=admit-only-vlan-tagged

1. Define VLANs under **Bridge → VLANs**:

* VLAN 10 → **Tagged: Ether4**, **Untagged: Ether1: /interface/bridge/vlan/add bridge=bridge tagged=ether4,bridge untagged=ether1 vlan-ids=10**
* VLAN 100 → **Tagged: Ether4, Untagged Ether2: /interface/bridge/vlan/add bridge=bridge tagged=ether4,bridge untagged=ether2 vlan-ids=100**
* VLAN 200 → **Tagged: Ether4, Untagged Ether3 /interface/bridge/vlan/add bridge=bridge tagged=ether4,bridge untagged=ether3 vlan-ids=200**
* **Take the screenshot of */interface/bridge export* and put it in report with explanation if there are some differences from 2.3. part**

1. Configure Management VLAN

* vlan10-mgmt (VLAN ID 10) → **Bridge: switch-bridge: */interface/vlan/add vlan-id=10 interface=switch-bridge name=vlan10-mgmt comments=management***
* **set static IP: *ip address add interface=vlan10-mgmt && ip route/add dst-address=192.168.99.0/29 gateway=192.168.99.1***
* **or dhcp-client: *ip dhcp-client add interface=vlan10-mgmt***
* **check IP address if it from mgmt pool: *ip address print* (drop result in report)**

Step 3: Verification of the setup to ensure the setup operates as expected

1. L14G Ether1 connect to PC port1 (or 2 port)
2. L14G Ether2 connect to PC port2 (or 1 port – check previous step)
3. Change in previously created VM Network type to bridged adapter and choose the PC port2 (or that port what is connected to L14G ETH2)
4. Open the **PC terminal** and check the network configuration:

* ifconfig,
* **Take a screenshot of the ifconfig output and include it in the report.**

1. Verify the assigned IP address on the VM terminal

* Open the **VM terminal** and release the current IP: *dhclient -r eno1* (Ensure the network interface name is correct.))
* Check the current IP configuration: *ifconfig;* **Take a** s**creenshot of the ifconfig output and include it in the report.**
* **Analyse and explain** whether the IP address was assigned from the DHCP server pool.
* ★ **If a different IP is assigned**, correct the configuration and **document all steps taken.**

Step 4: Configure vAP with VLAN on MikroTik SW1 (L41G-2axD)

