

DHCP, ARP a switching

Správa síťových zařízení MikroTik

2. přednáška

verze 2024.2

Obsah přednášky

- DHCP
- ARP
- VRRP
- Bridging (switching)
- VLAN
- EtherChannel
- 802.1x

DHCP

DHCP

- Dynamic Host Configuration Protocol
- Used for automatic IP address distribution over a local network
- Use DHCP only in trusted networks
- Works within a broadcast domain
- RouterOS supports both DHCP client and server

DHCP Client

- Used for automatic acquiring of:
 - IP address
 - subnet mask
 - default gateway
 - DNS server address
 - additional settings (Options)
 - DNS suffix (Option 15/119)
 - WLC address (Option 43)
 - Static route (Option 33/121)
 - NTP server (Option 42)
 - TFTP server (Option 66)
 - Boot file (Option 67)
- MikroTik SOHO routers by default have DHCP client configured on ether1(WAN) interface

DHCP Client

DHCP Client

DHCP Client Options

+ - ✓ ✗ 📁 🔍 Release Renew

Interface	Use P...	Add D...	IP Address	Expires After	Status
ether10	yes	yes	83.240.64.205/26	05:55:02	bound

DHCP Client <ether10>

DHCP Advanced Status

Interface: ether10

☒ Use Peer DNS

☒ Use Peer NTP

Add Default Route: yes

OK Cancel Apply Disable Comment Copy Remove Release Renew

enabled Status: bound

DHCP Client <ether10>

DHCP Advanced Status

DHCP Options: hostname clientid

Default Route Distance: 1

Script

OK Cancel Apply Disable Comment Copy Remove Release Renew

enabled Status: bound

DHCP Client <ether10>

DHCP Advanced Status

IP Address: 83.240.64.205/26

Gateway: 83.240.64.193

DHCP Server: 192.168.1.196

Expires After: 05:54:18

Primary DNS: 83.240.64.215

Secondary DNS: 83.240.64.136

Primary NTP: 83.240.64.14

Secondary NTP: 83.240.64.215

CAPS Managers:

OK Cancel Apply Disable Comment Copy Remove Release Renew

enabled Status: bound

IP → DHCP Client

DNS

- By default DHCP client asks for a DNS server IP address
- It can also be entered manually if other DNS server is needed or DHCP is not used

The screenshot shows the 'DNS Settings' window with the following configuration:

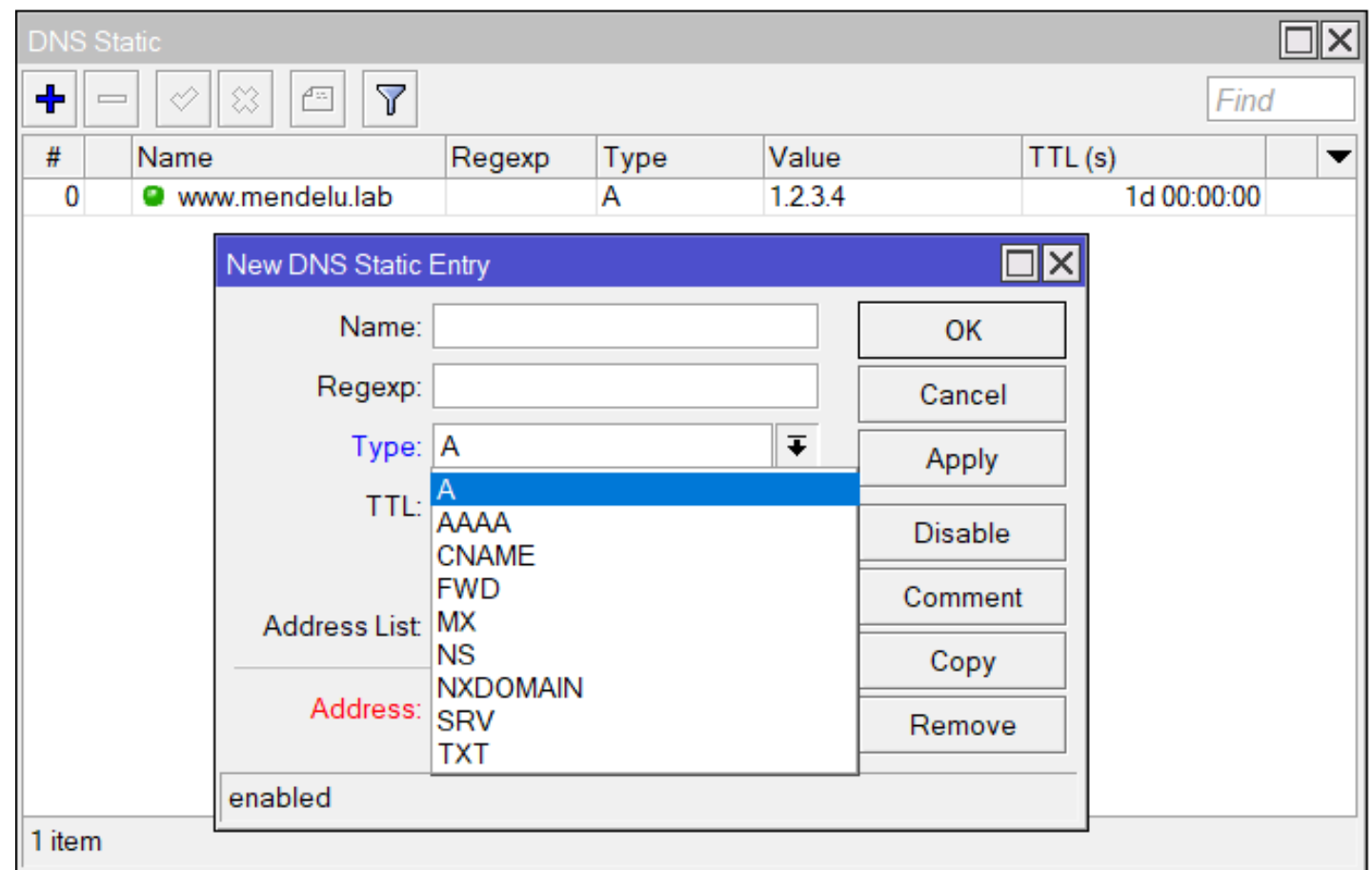
- Servers:** 1.1.1.1, 8.8.8.8, 2001:500:1, 2001:500:6:0:1
- Dynamic Servers:** 83.215, 83.136
- Use DoH Server:** (empty dropdown)
- Allow Remote Requests:** ☒
- Max UDP Packet Size:** 4096
- Query Server Timeout:** 2.000 s
- Query Total Timeout:** 10.000 s
- Max. Concurrent Queries:** 100
- Max. Concurrent TCP Sessions:** 20
- Cache Size:** 2048 KiB
- Cache Max TTL:** 7d 00:00:00
- Cache Used:** 89 KiB

Buttons on the right: OK, Cancel, Apply, Static, Cache.

IP → DNS

DNS

- RouterOS supports static DNS entries
- By default there's a static DNS A record named router which points to 192.168.88.1
- That means you can access the router by using DNS name instead of IP
- <http://router>



IP → DNS → Static

DHCP Server – Setup

- Automatically assigns IP addresses to requesting hosts
- IP address should be configured on the interface which DHCP Server will use
- To enable use 'DHCP Setup' command

DHCP Server – Setup

The image displays six sequential screenshots of the DHCP Setup wizard, arranged in a 3x2 grid. Each window has a blue title bar with 'DHCP Setup' and standard window controls. Step 1: 'Select interface to run DHCP server on'. The 'DHCP Server Interface' dropdown is set to 'bridge-local'. Step 2: 'Select network for DHCP addresses'. The 'DHCP Address Space' text box contains '192.168.199.0/24'. Step 3: 'Select gateway for given network'. The 'Gateway for DHCP Network' text box contains '192.168.199.1'. Step 4: 'Select pool of ip addresses given out by DHCP server'. The 'Addresses to Give Out' dropdown shows '192.168.199.2-192.168.199.254'. Step 5: 'Select DNS servers'. The 'DNS Servers' text box contains '10.5.120.1'. Step 6: 'Select lease time'. The 'Lease Time' text box contains '00:10:00'. Each step includes 'Back', 'Next', and 'Cancel' buttons at the bottom.

DHCP Setup

Select interface to run DHCP server on

DHCP Server Interface: bridge-local

1 Back Next Cancel

DHCP Setup

Select network for DHCP addresses

DHCP Address Space: 192.168.199.0/24

2 Back Next Cancel

DHCP Setup

Select gateway for given network

Gateway for DHCP Network: 192.168.199.1

3 Back Next Cancel

DHCP Setup

Select pool of ip addresses given out by DHCP server

Addresses to Give Out: 192.168.199.2-192.168.199.254

4 Back Next Cancel

DHCP Setup

Select DNS servers

DNS Servers: 10.5.120.1

5 Back Next Cancel

DHCP Setup

Select lease time

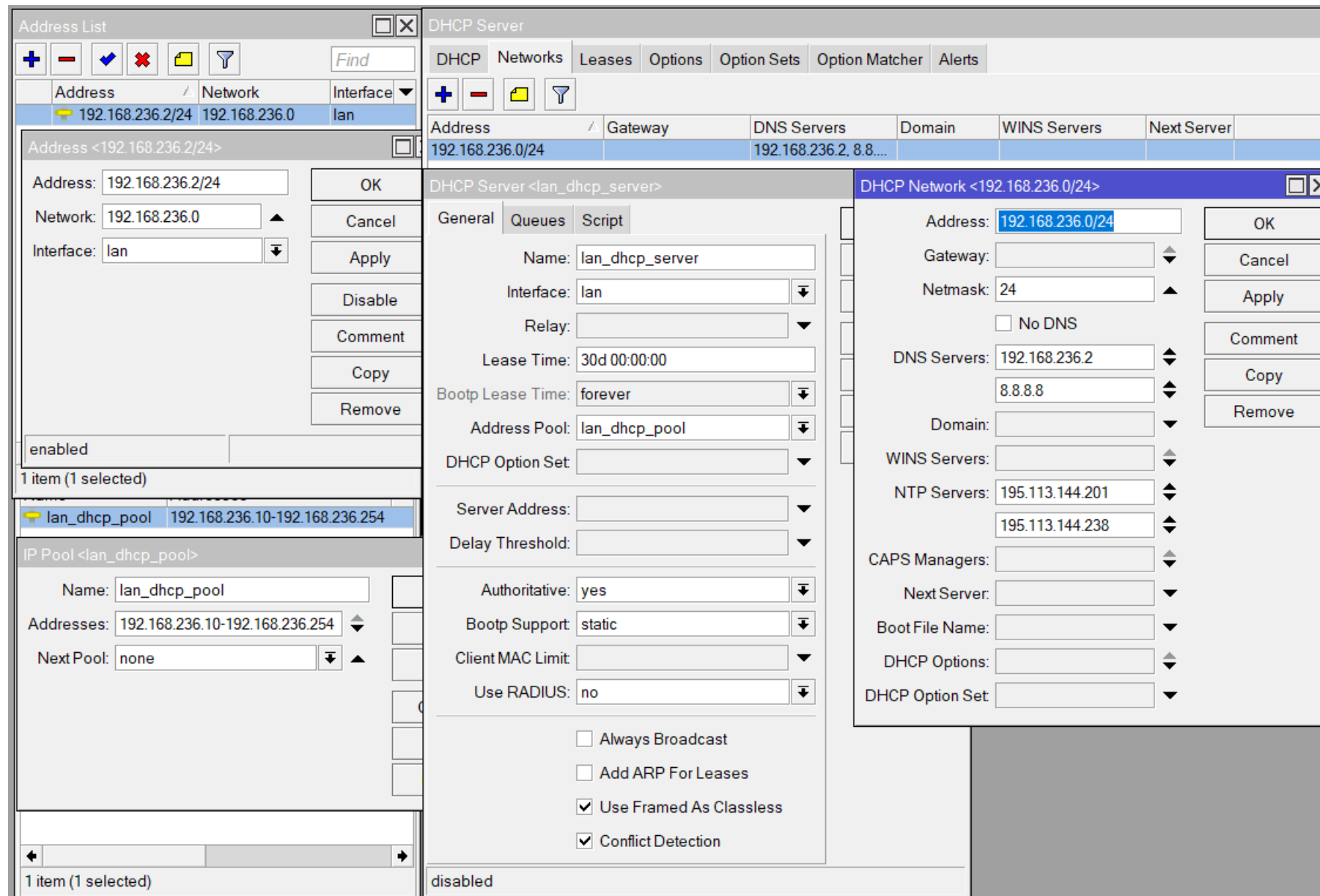
Lease Time: 00:10:00

6 Back Next Cancel

IP → DHCP Server → DHCP Setup

DHCP Server

- DHCP Server Setup wizard has created a new IP pool and DHCP Server



DHCP Static Leases

- It is possible to always assign the same IP address to the same device (identified by MAC address)
- DHCP Server could even be used without dynamic IP pool and assign only preconfigured addresses

DHCP Static Leases

The screenshot shows the Mikrotik WinBox DHCP Server interface. The 'Leases' tab is selected, displaying a table of active leases. A specific lease for IP 192.168.199.254 is highlighted. A secondary window, 'DHCP Lease <192.168.199.254, 192.168.199.254>', is open, showing details for this lease. A red arrow points to the 'Make Static' button in this window, with the text 'Convert dynamic lease to static' next to it.

DHCP Server Interface:

- Tab: Leases
- Buttons: +, -, ✓, ✗, [icon], [icon], Check Status, Find
- Table:

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Host Name	Expires After	Status
D					192.168.199.254	00:1E:C2:FB:F8:36	Kk	00:06:47	bound

DHCP Lease <192.168.199.254, 192.168.199.254> Window:

- Active
- Buttons: OK, Copy, Remove, Make Static, Check Status
- Fields:

Active Address:	192.168.199.254
Active MAC Address:	00:1E:C2:FB:F8:36
Active Client ID:	1:0:1e:c2:fb:f8:36
Active Host Name:	Kk
Active Server:	dhcp1
Expires After:	00:06:47
Last Seen:	00:03:13
Agent Circuit Id:	
Agent Remote Id:	

dynamic enabled radius blocked bound

Convert dynamic lease to static

IP → DHCP Server → Leases

DHCP Relay

- DHCP relay act as a proxy between DHCP clients and the DHCP server
- Necessary where the DHCP server is not on the same broadcast domain as the DHCP client.

The screenshot shows the 'New DHCP Relay' configuration window. The 'General' tab is active. The 'Name' field is set to 'DHCP-relay', the 'Interface' is 'lan', and the 'DHCP Server' is '192.168.0.1'. The 'Status' tab shows the relay is 'enabled'. Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Copy', 'Remove', and 'Reset Counters' are visible on the right.

The screenshot shows the 'New DHCP Server' configuration window. The 'General' tab is active. The 'Name' is 'DHCP-server', the 'Interface' is 'ether1', and the 'Relay' is '192.168.236.1'. The 'Lease Time' is '00:30:00' and the 'Bootp Lease Time' is 'forever'. The 'Address Pool' is 'lan_dhcp_pool'. On the right, there are fields for 'Address' (192.168.236.0/24), 'Mask' (24), 'DNS Servers' (192.168.236.2, 8.8.8.8), and 'Domain' (8.8.8.8). Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove' are visible.

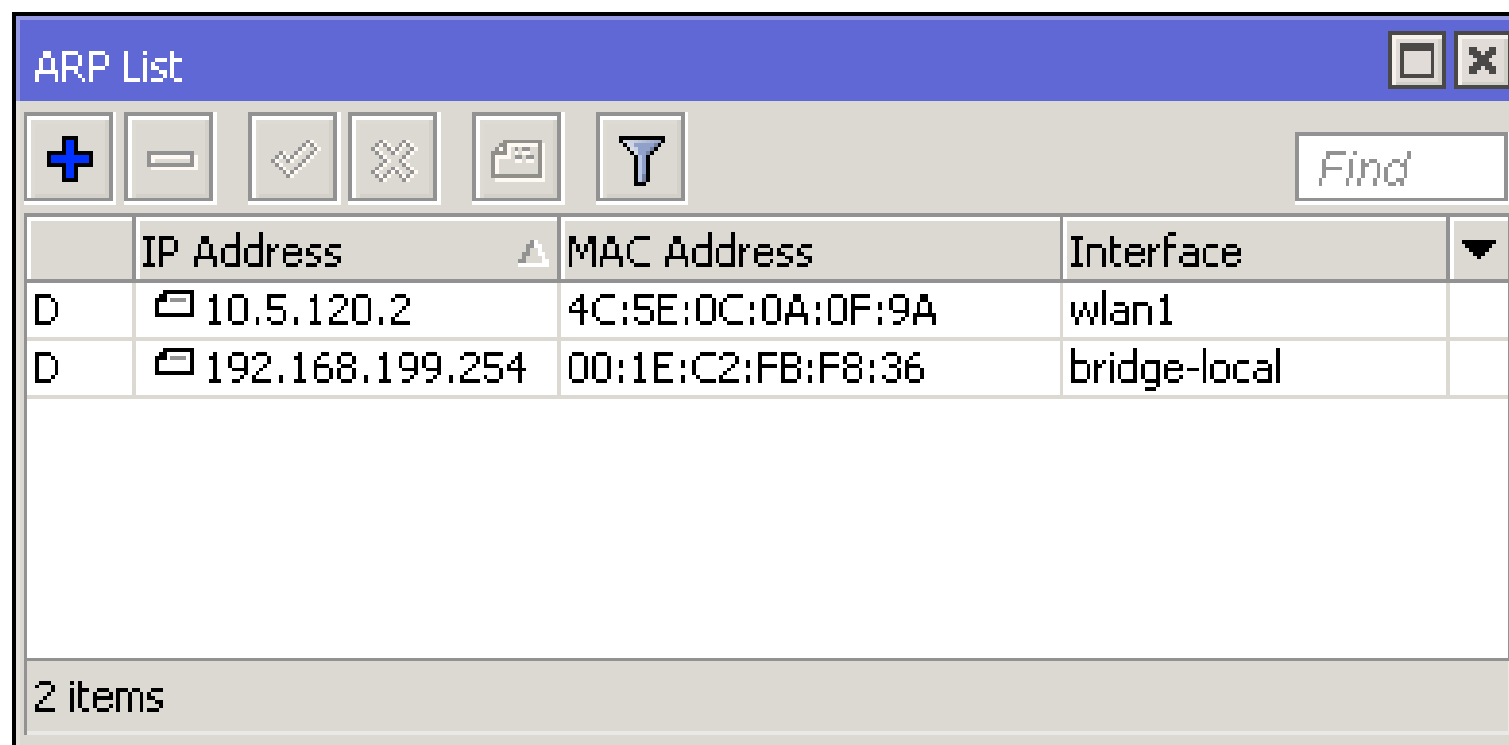
ARP

ARP

- Address Resolution Protocol
- ARP joins together client's IP address (Layer3) with MAC address (Layer2)
- ARP operates dynamically
- Can also be configured manually

ARP Table

- Provides information about IP address, MAC address and the interface to which the device is connected



	IP Address	MAC Address	Interface
D	10.5.120.2	4C:5E:0C:0A:0F:9A	wlan1
D	192.168.199.254	00:1E:C2:FB:F8:36	bridge-local

2 items

IP → ARP

Static ARP

- For increased security ARP entries can be added manually
- Network interface can be configured to reply-only to known ARP entries
- Router's client will not be able to access the Internet using a different IP address

Static ARP

The image shows two windows from the Mikrotik WinBox interface. The 'ARP List' window on the left displays a table of ARP entries. The third entry, with IP 192.168.199.199, is selected. The 'ARP <192.168.199.199>' window on the right shows the configuration for this entry. The 'Published' checkbox is checked, and a red arrow points to it with the text 'Static ARP entry'.

	IP Address	MAC Address	Interface
D	10.5.120.1	4C:5E:0C:0A:0F:9A	wlan1
D	10.5.120.2	4C:5E:0C:0A:0F:9A	wlan1
D	192.168.199.199	00:1E:C2:FB:F8:36	bridge-local

3 items (1 selected)

ARP <192.168.199.199>

IP Address: 192.168.199.199

MAC Address: 00:1E:C2:FB:F8:36

Interface: bridge-local

☒ Published

Static ARP entry

Buttons: OK, Copy, Remove, Make Static, Ping, MAC Ping, Telnet, MAC Telnet, Torch

dynamic enabled published

IP → ARP

ARP mode

**Interface will
reply only to
known ARP
entries**

Interface <bridge-local>

General STP Status Traffic

Name: bridge-local

Type: Bridge

MTU:

Actual MTU: 1500

L2 MTU: 1598

MAC Address: D4:CA:6D:E2:65:90

ARP: reply-only

Admin. MAC Address: D4:CA:6D:E2:65:90

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave

Interfaces → bridge-local

DHCP and ARP

- DHCP Server can add ARP entries automatically
- Combined with static leases and reply-only ARP can increase network security while retaining the ease of use for users

DHCP and ARP

The screenshot shows the Mikrotik WinBox DHCP Server configuration window for a server named 'dhcp1'. The window is divided into several sections. On the left, a sidebar shows a list of DHCP servers with 'dhcp1' selected. The main area contains the following fields and options:

- Name:** dhcp1
- Interface:** bridge-local
- Relay:** (empty dropdown)
- Lease Time:** 00:10:00
- Bootp Lease Time:** forever
- Address Pool:** dhcp_pool1
- Src. Address:** (empty dropdown)
- Delay Threshold:** (empty dropdown)
- Authoritative:** after 2s delay
- Bootp Support:** static
- Lease Script:** (empty text area)
- Options:**
 - ☐ Add ARP For Leases
 - ☐ Always Broadcast
 - ☐ Use RADIUS
- Status:** enabled

On the right side of the window, there is a table with the following data:

Address Pool	Add ARP For Leases
dhcp_pool1	no

Buttons for OK, Cancel, Apply, Disable, Copy, and Remove are located on the right side of the main configuration area.

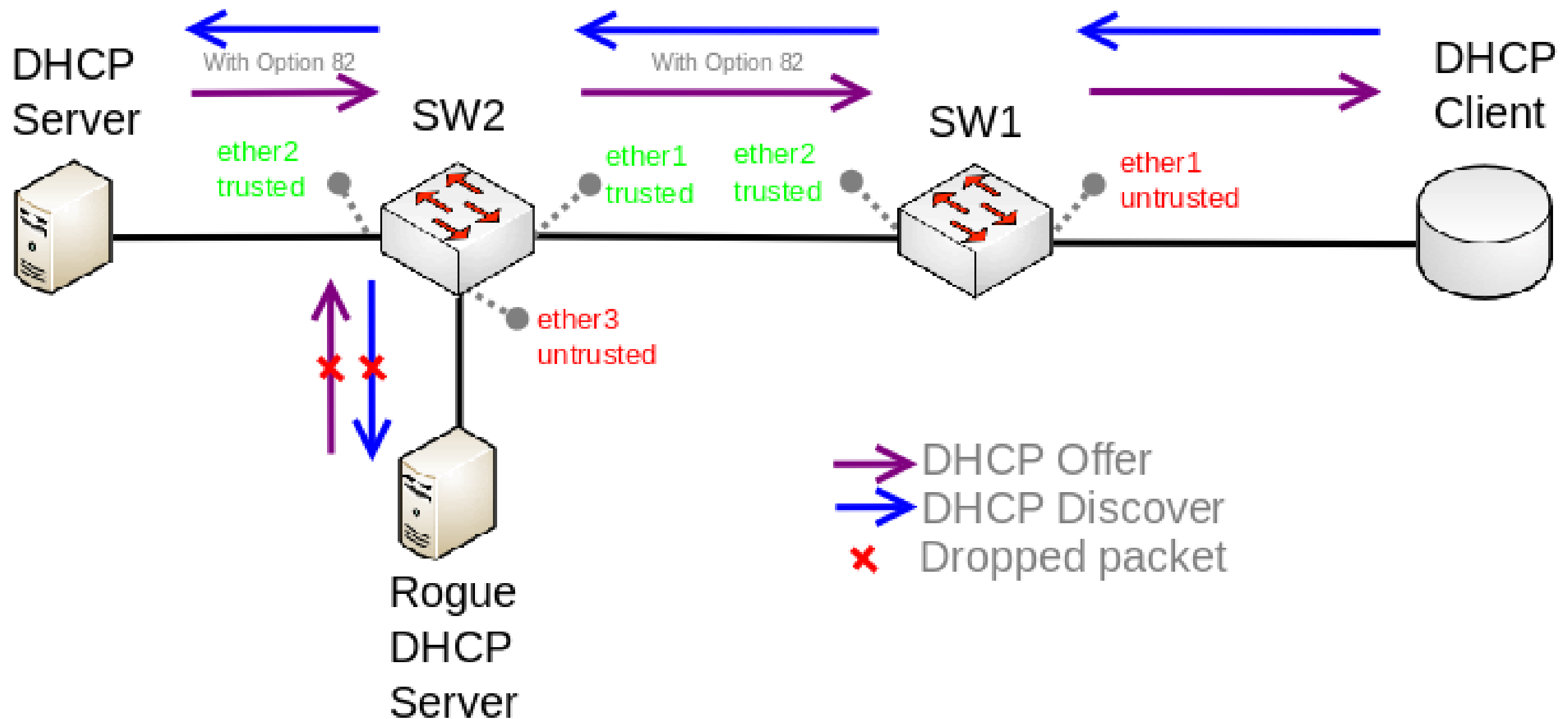
IP → DHCP Server

**Add ARP entries
for DHCP leases**

DHCP Snooping

- Limits unauthorized DHCP servers from providing a malicious information to users
 - Trusted ports – connection to DHCP server and all DHCP messages should be forwarded
 - Untrusted ports – do not forward DHCP Offer and DHCP ACK messages
- DHCP Option 82 is an additional information allowing to identify port and connecting device (switch)
 - Agent Circuit ID and Agent Remote ID

DHCP Snooping

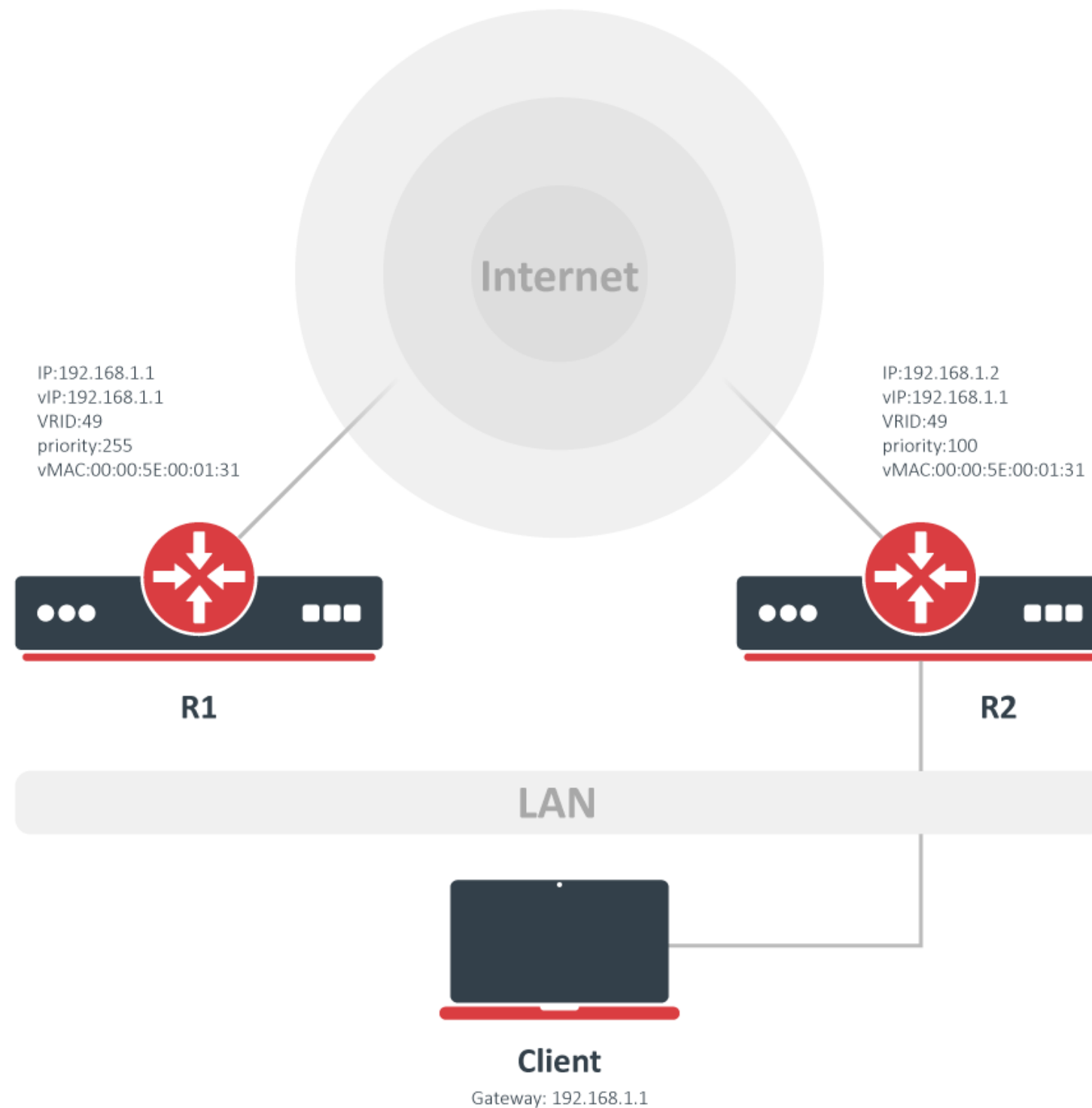


VRRP

VRRP (Virtual Router Redundancy Protocol)

- Provides router (gateway) redundancy
- Gateways communicate via multicast
 - 224.0.0.18
 - ff02::12
- VR (Virtual Router) group is identified using VRID
 - Each VR has unique MAC address
 - VR group share gateway MAC address 00:00:5E:00:01:VRID for virtual IP (VIP)
- Operation modes – Master/Backup
 - Decided by Priority (default value 100)
 - The highest priority VR becomes Master

VRRP – example topology



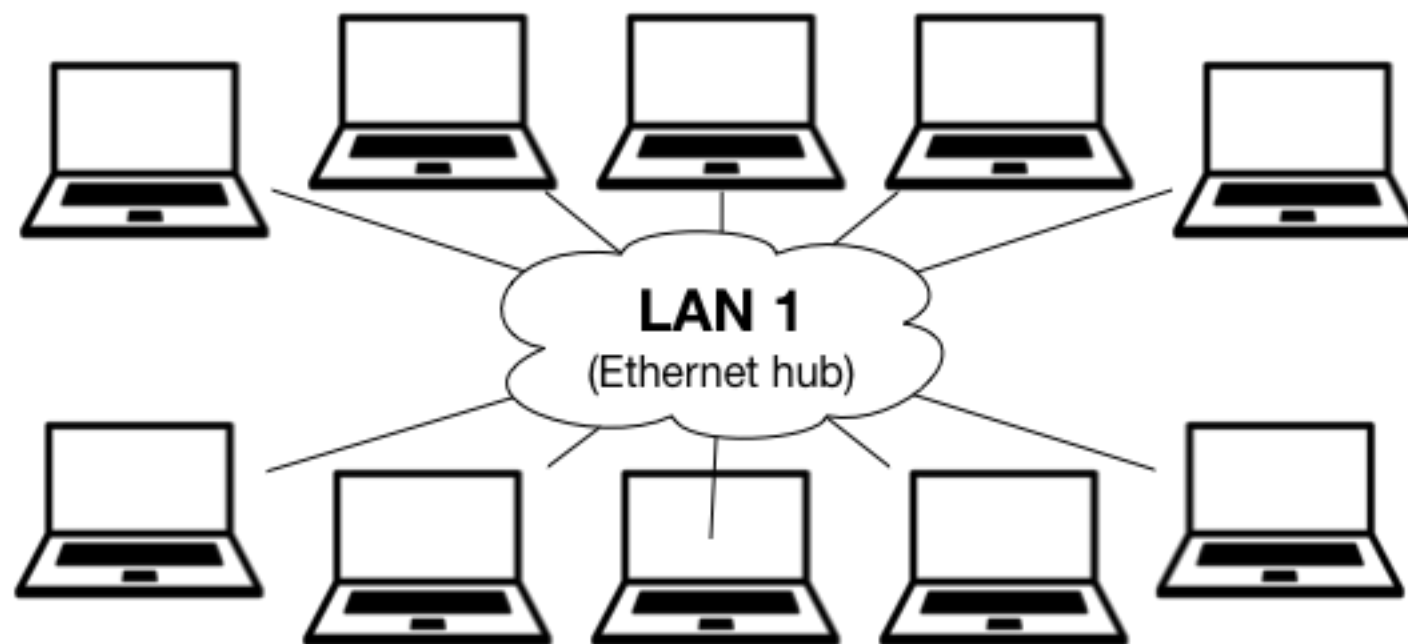
Switching

Bridge

- Bridges are OSI layer 2 devices
- Bridge is a transparent device
- Traditionally used to join two network segments
- Bridge splits collision domain in two parts
- Network switch is multi-port bridge – each port is a collision domain of one device

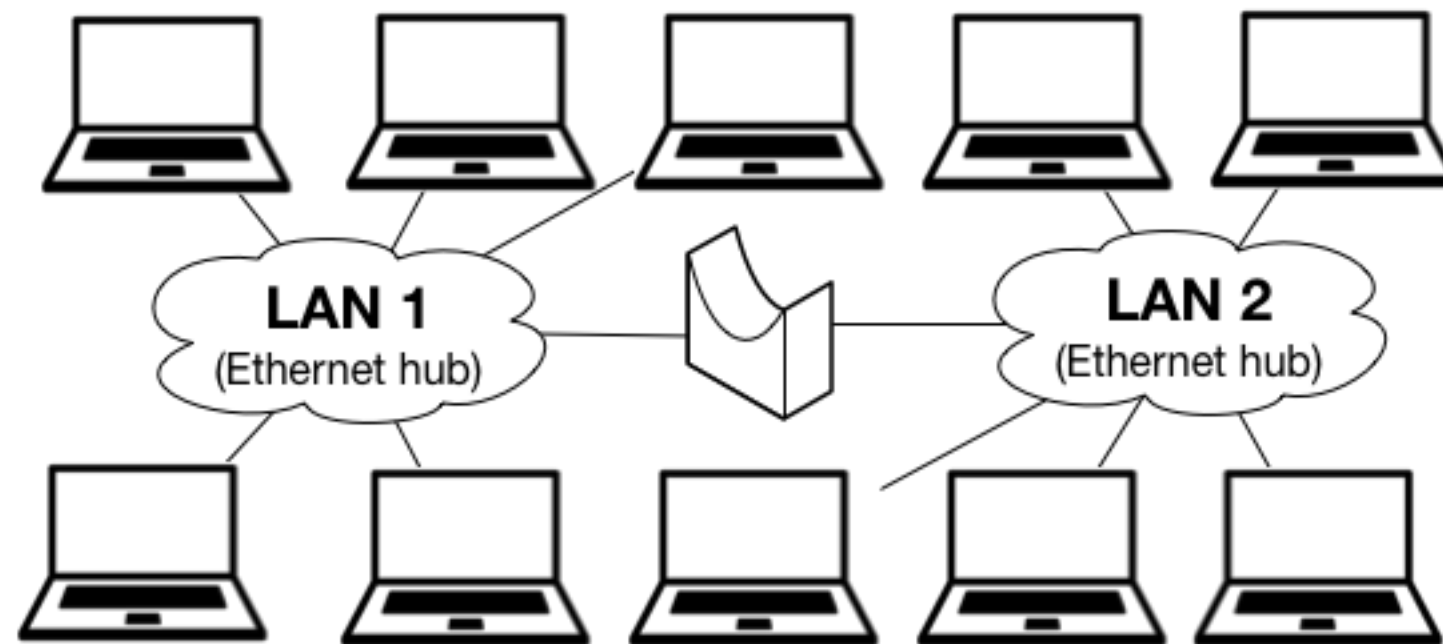
Hub – historic principle

- All hosts can communicate with each other
- All share the same collision domain



Bridge (switch)

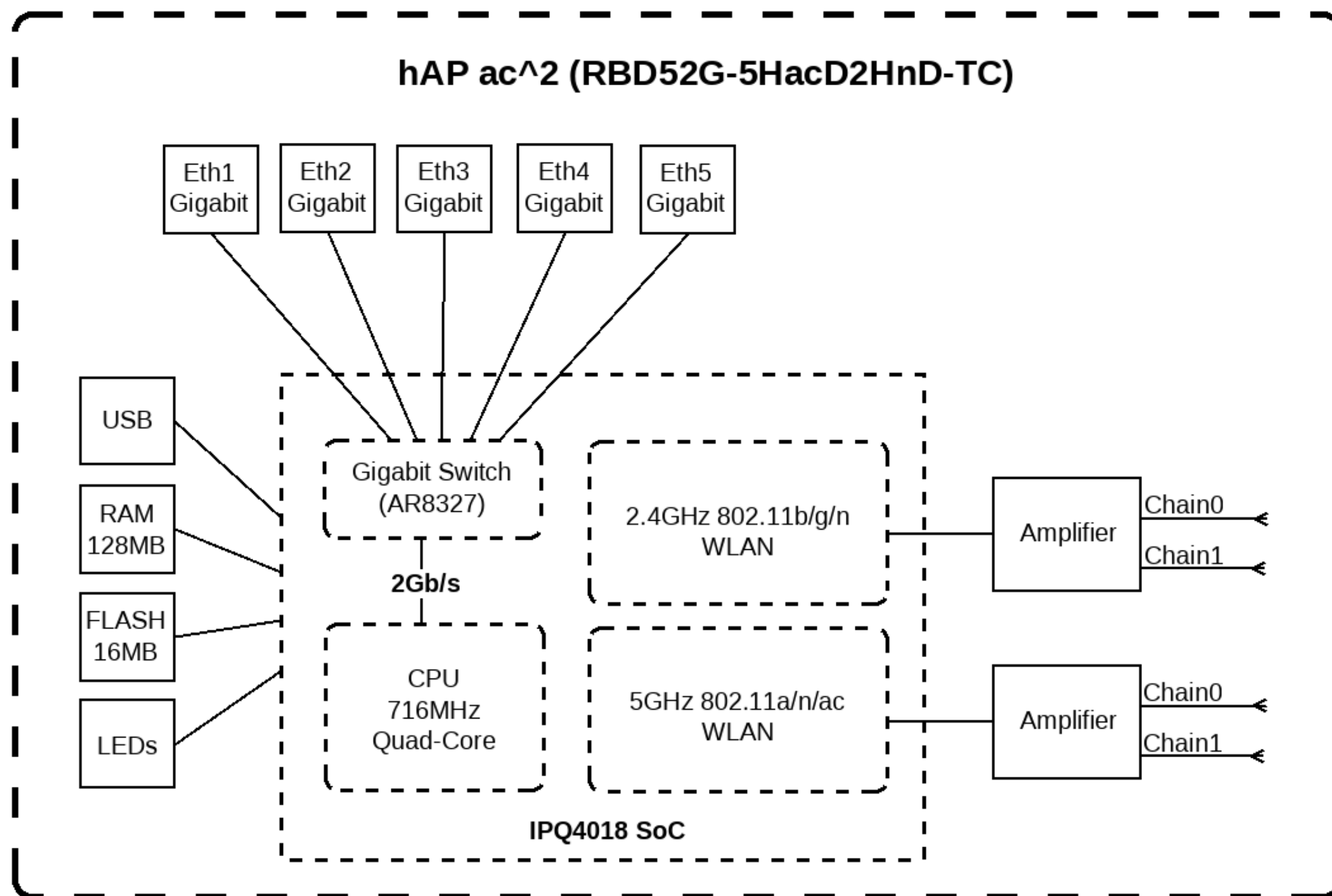
- All hosts still can communicate with each other
- Now there are 2 collision domains



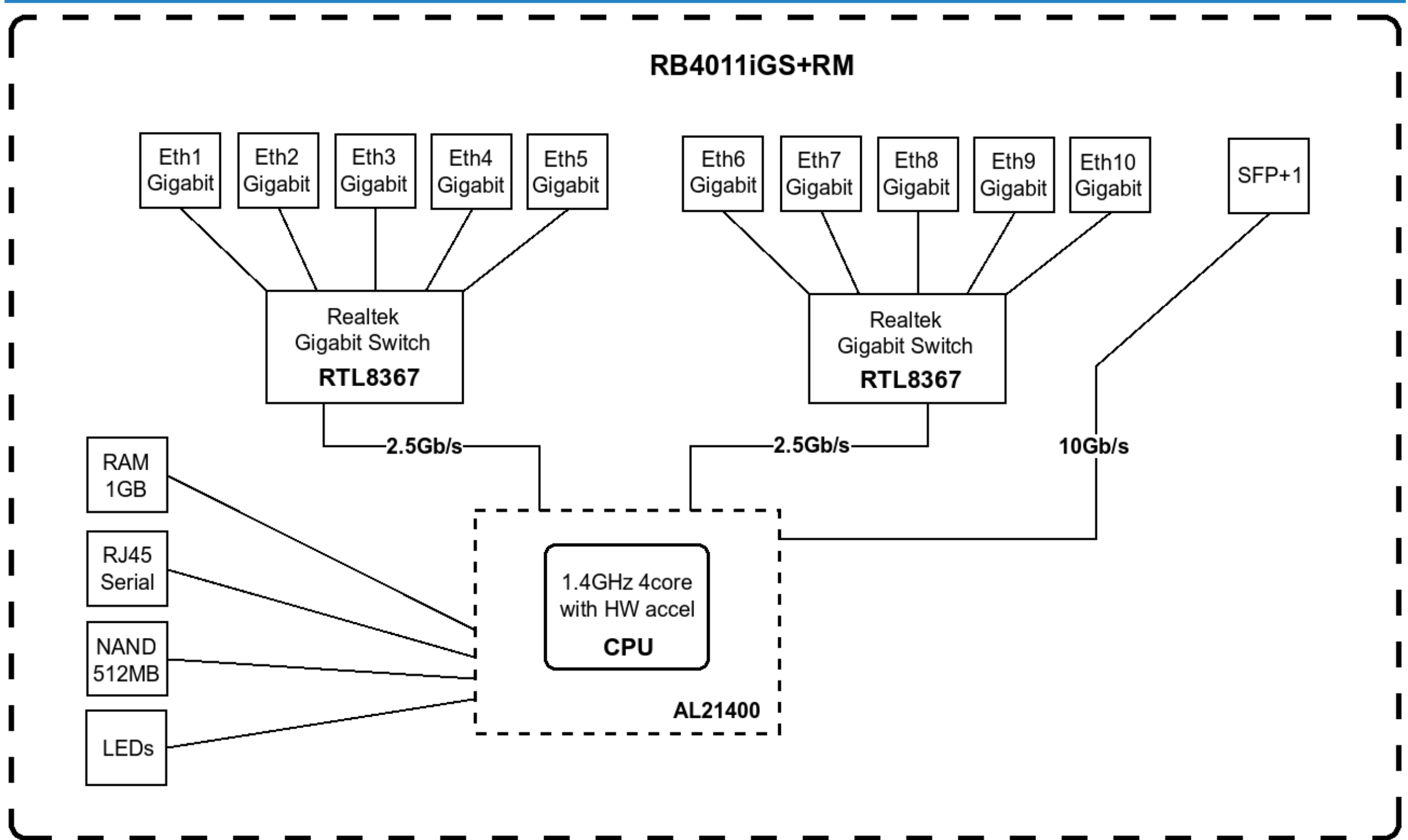
Bridge

- RouterOS implements software bridge
- Ethernet, wireless, SFP and tunnel interfaces can be added to a bridge
- Default configuration on SOHO routers bridge wireless with ether2 port
- Ether2-5 are combined together in hardware switch. Wire speed switching using switch chip
- If switch chip is not be used (ether+wireless), it will generate higher CPU usage

Internal HW scheme of hAP (in lab)



Internal HW scheme of RB4011 (in lab)



Switch Chip Features

- Port switching
- CAM table
- Port mirroring
- Tx/Rx limit
- Host table (ARP)
- VLAN table, VLAN header check
- Port isolation, Private VLAN

Bridge

- Due to limitations of 802.11 standard, wireless clients (mode: station) do not support bridging
- RouterOS implements several modes to overcome this limitation

Bridge

Set mode to station bridge

Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme Advanced Status Status Traffic

Mode: station bridge

Band: 2GHz-only-N

Channel Width: 20MHz

Frequency: auto MHz

SSID: ClassAP

Scan List: default

Wireless Protocol: 802.11

Security Profile: class

OK Cancel Apply Disable Comment Advanced Mode Torch WPS Accept

Wireless → wlan1

Disable DHCP Server

DHCP Server

DHCP Networks Leases Options Option Sets Alerts

+ - ✓ ✗ Filter DHCP Config DHCP Setup Find

Name	Interface	Relay	Lease Time	Address Pool	Add ARP For Leases
default	bridge-local		00:10:00	unknown	no

1 item (1 selected)

IP → DHCP Server

Bridge

Bridge

Bridge Ports Filters NAT Hosts

+ - ✓ ✗ 📄 🔍 Find

Interface	Bridge	Priority (...)	Path Cost	Horizon	Role	Root Path Cost	Comment
ether2-master-local	bridge-local	80	10		designated port		

New Bridge Port

General Status

Interface: wlan1

Bridge: bridge-local

Priority: 80 hex

Path Cost: 10

Horizon:

Edge: auto

Point To Point: auto

External FDB: auto

☐ Auto Isolate

OK Cancel Apply Disable Comment Copy Remove

enabled inactive

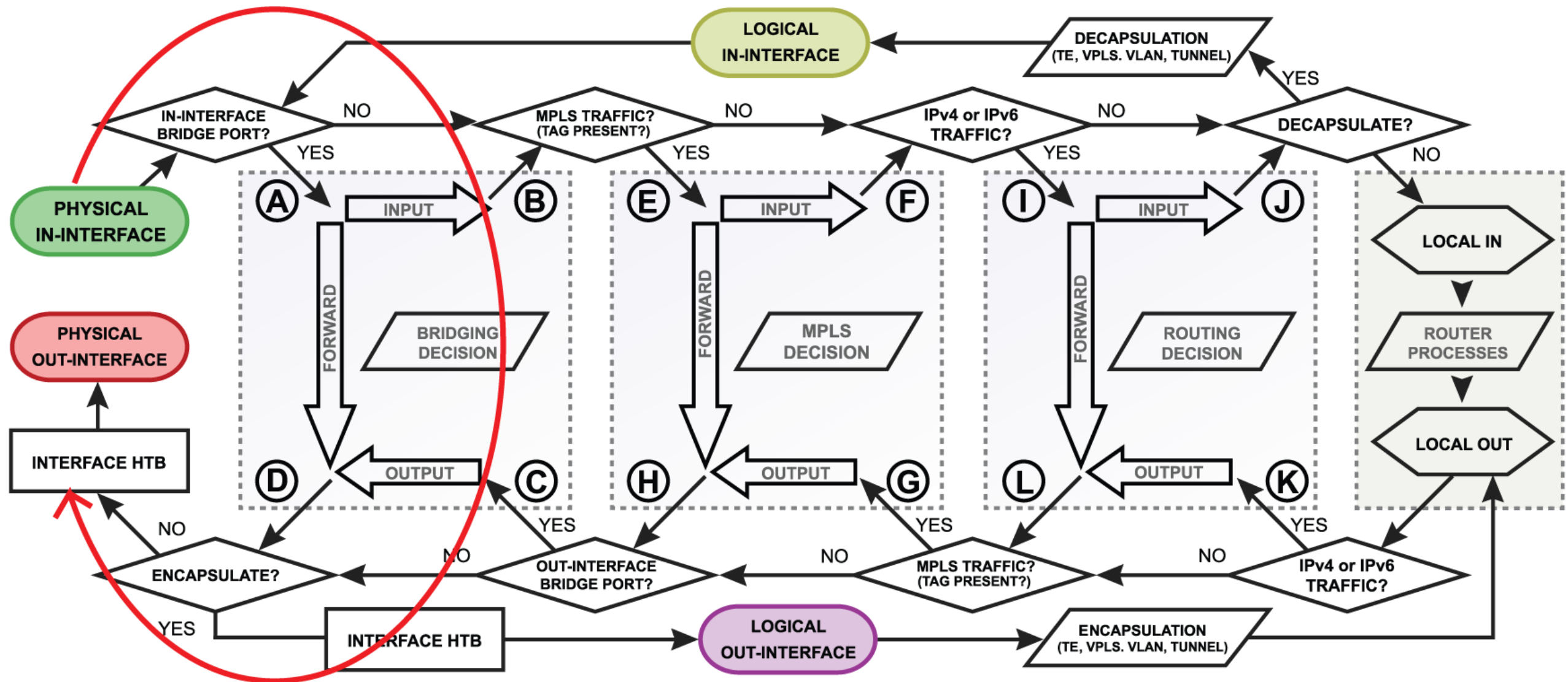
Add wireless interface to the bridge

Bridge → Ports

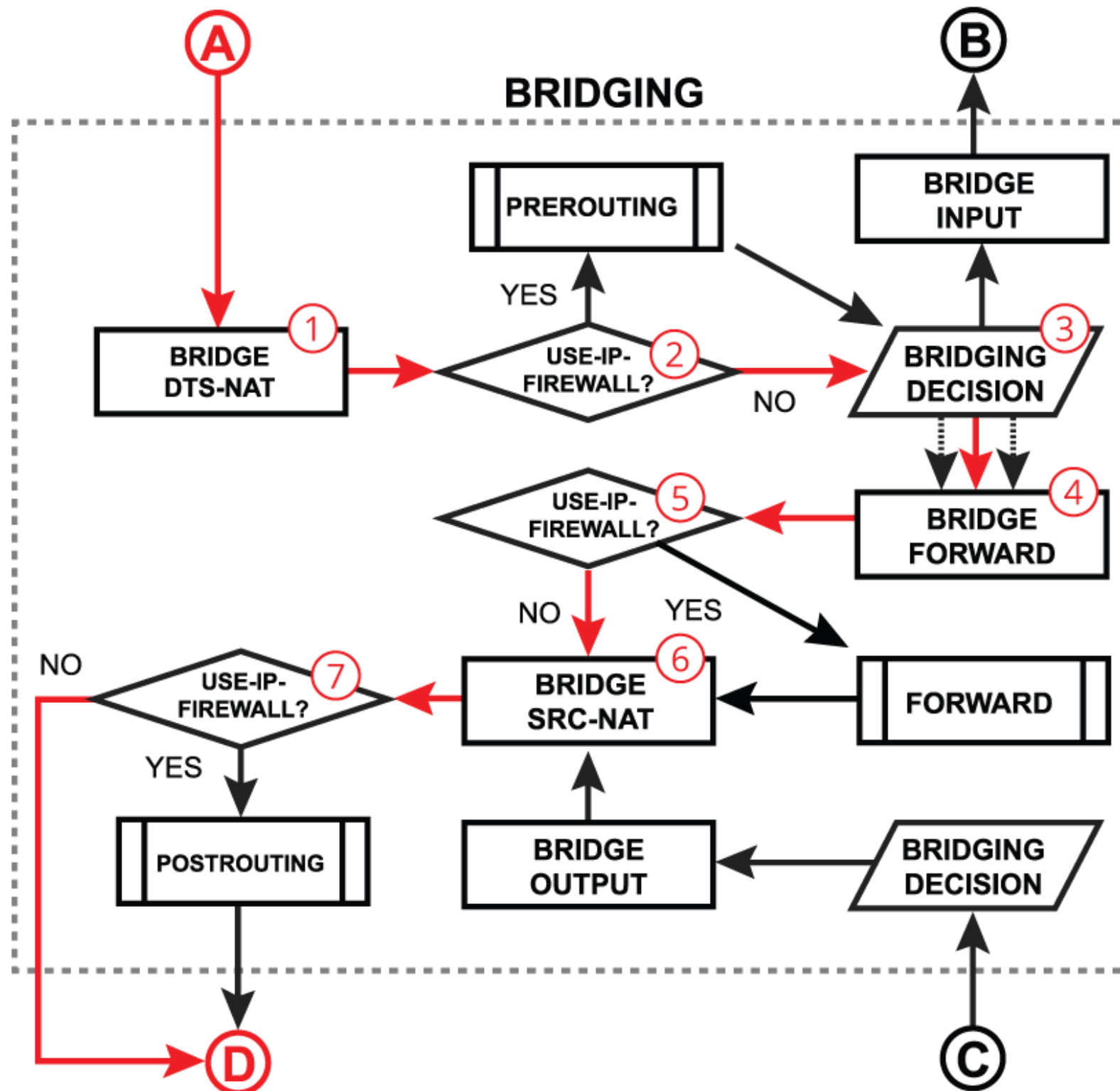
Bridge Firewall

- RouterOS bridge interface supports firewall
- Traffic which flows through the bridge can be processed by the firewall
- To enable: Bridge → Settings → Use IP Firewall

Bridge Firewall



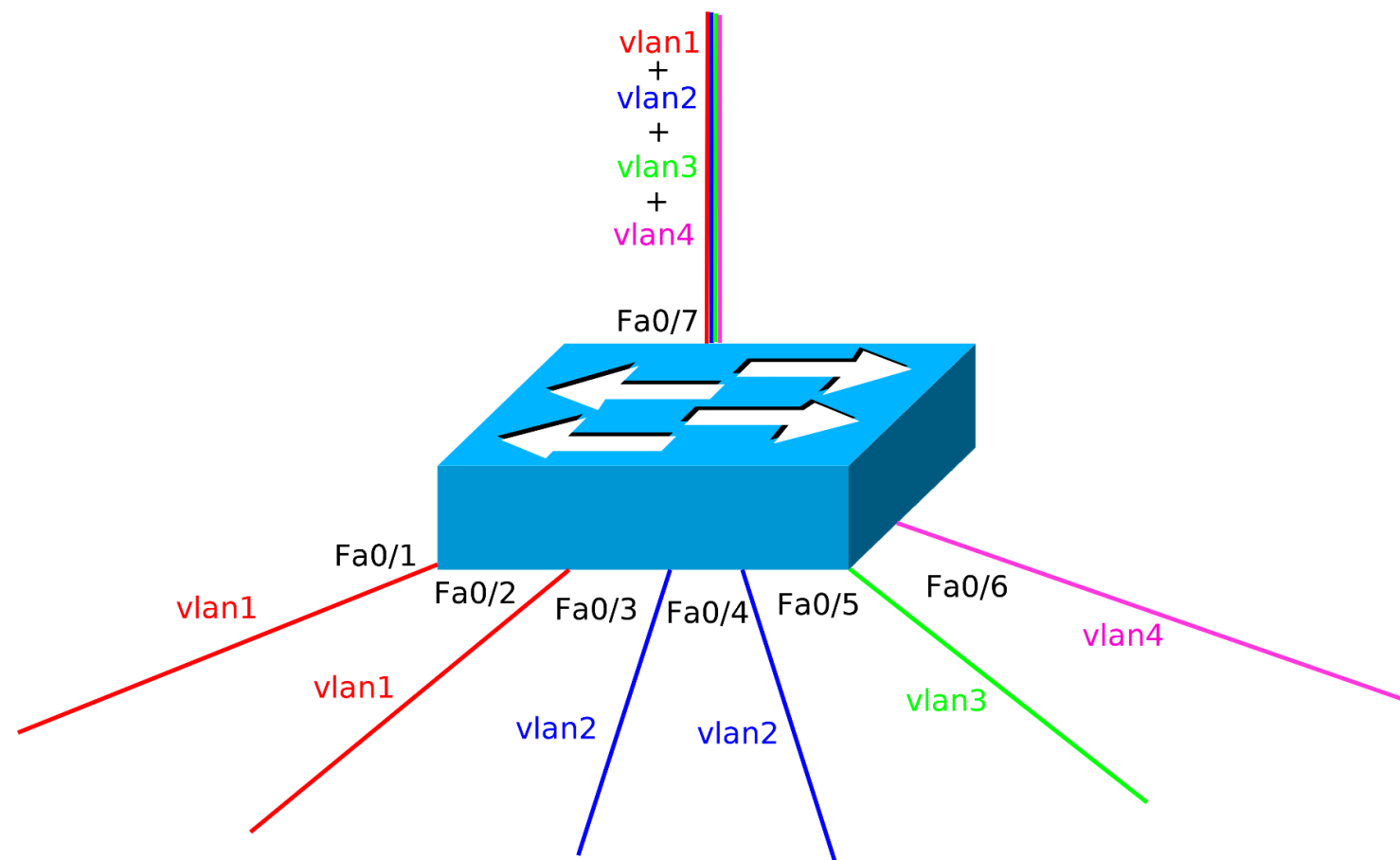
Bridge Firewall



VLAN

VLAN – Virtual Local Area Network

- Multiple different (virtual) networks on one physical infrastructure
- L2 – different networks on switch
- VLAN is identified by number, potentially by name
- Switch forwards frames by destination MAC only in same VLAN



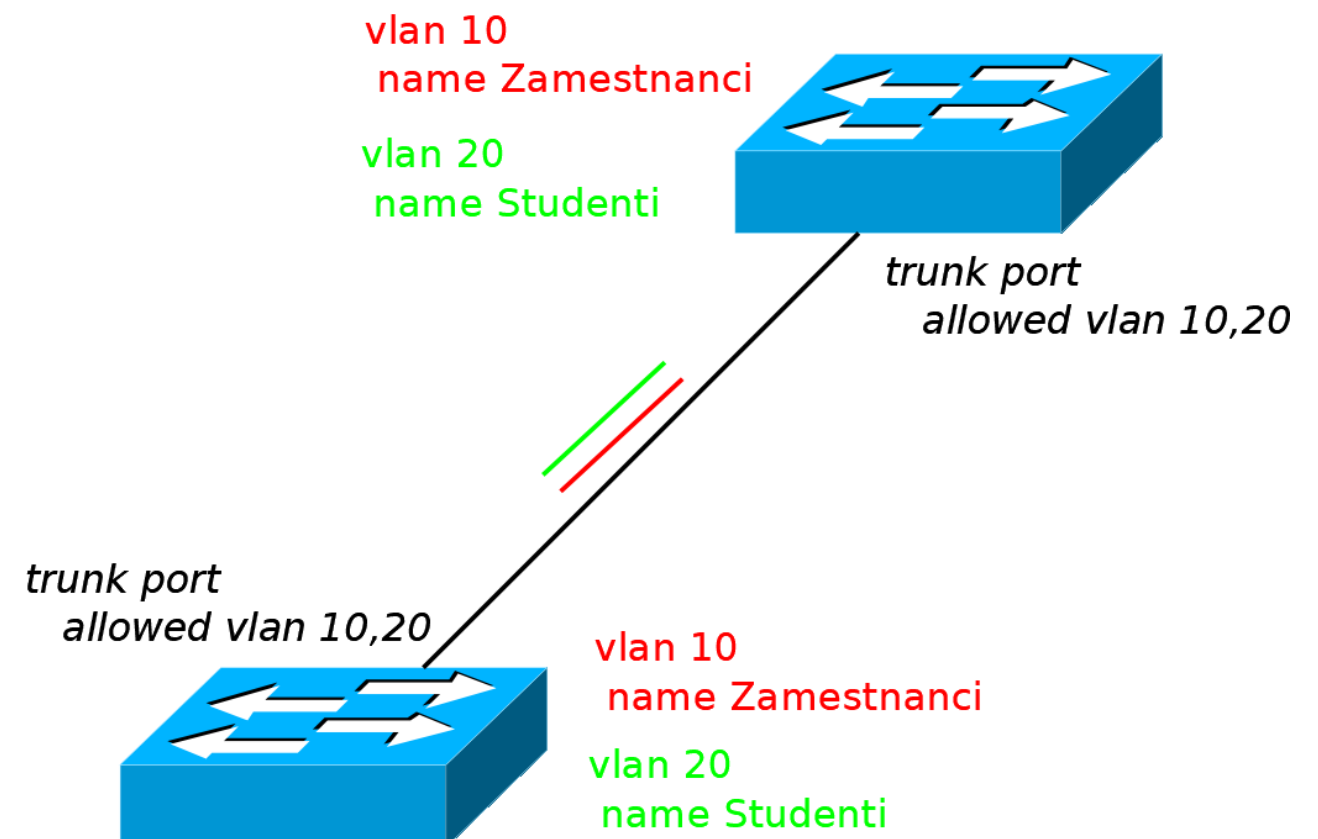
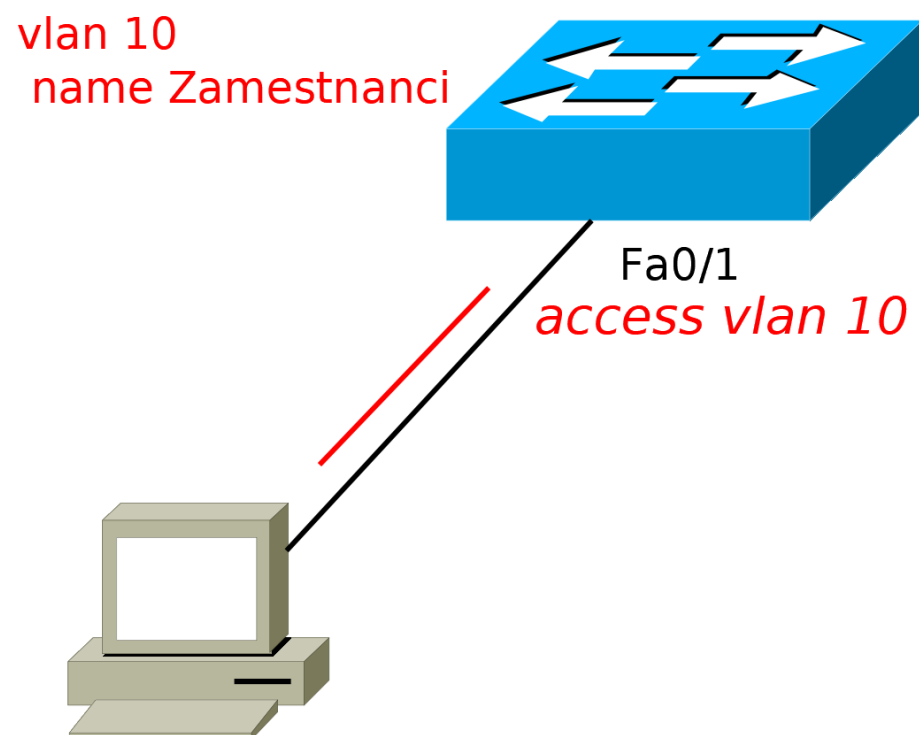
Access port vs. trunk port

- Usually for end device connection (PC, server,...)
- Interface and all traffic is in one VLAN

Usually for connection between switches (routers) or virtualization host

Port carry multiple VLANs

Output from trunk port is tagged - VID is added to frame and on opposite side of link is removed and frame is put in VLAN



VLAN ID (VID)

- VLAN ID – 12 bits (0–4095)
- 0 and 4095 – reserved for system usage
- 1 – default VLAN
 - in default it contains all ports
 - cannot be deleted
- 2 to 1001 – basic range for Ethernet VLAN
- 1002 to 1005 – special VLAN (on Cisco), cannot be used
- 1006 to 4094 – Extended VLAN
 - other range of VLANs for Ethernet

IEEE 802.1q VLAN tag

- Ethernet frame without tag:

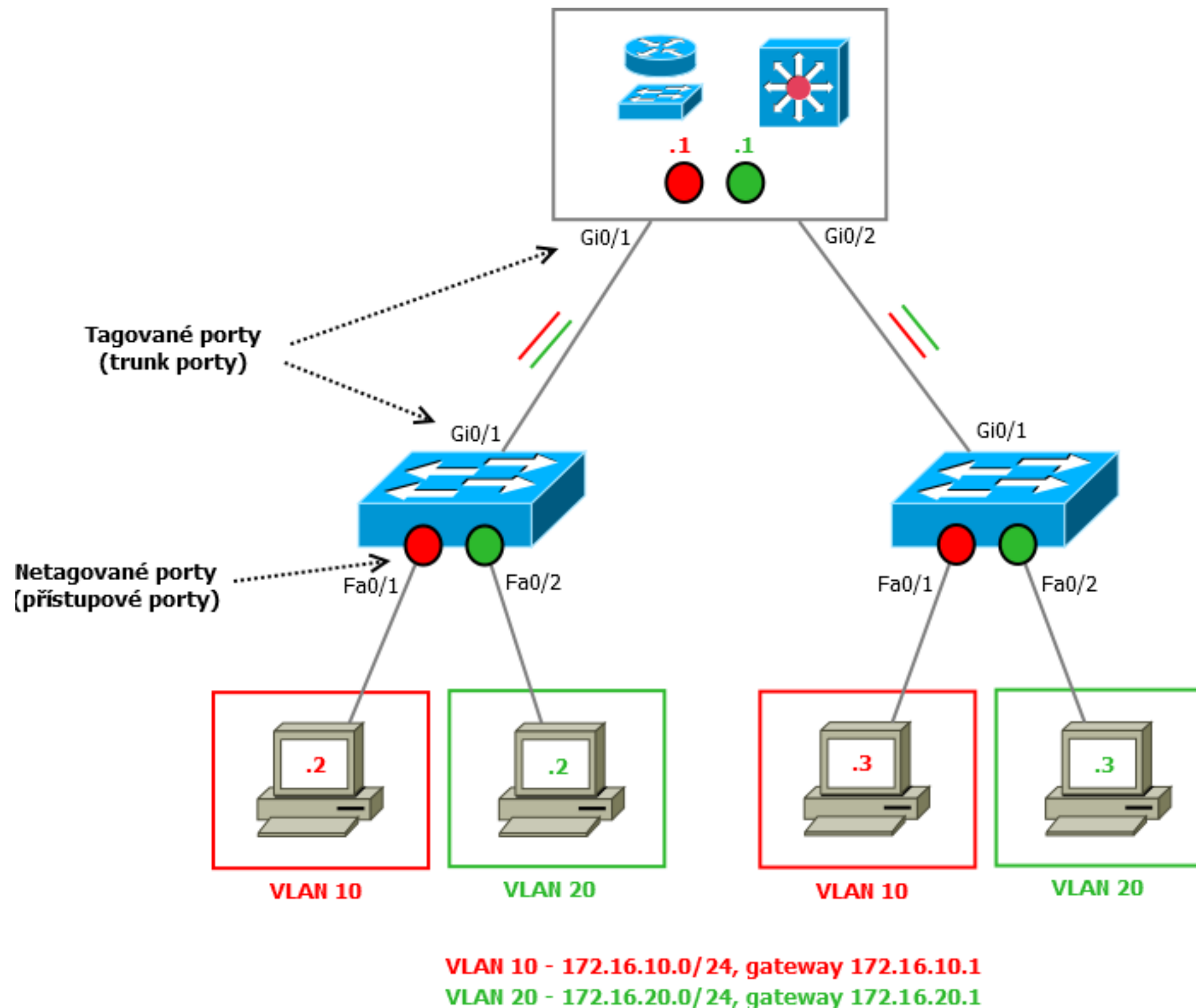
| dst MAC | src MAC | EtherType | Data | FCS |

- Ethernet frame with VLAN tag (802.1q):

| dst MAC | src MAC | **VLAN tag** | EtherType | Data | FCS |

- VLAN tag = 4 B
 - 2 B – type of inserted field type (802.1q = 0x8100)
 - 3 bits – CoS priority by 802.1p for QoS (PCP – Priority Code Point)
 - 1 bit – information if frame can be dropped in congestion (DEI – Drop Eligible Indicator)
 - 12 bits – VLAN ID
- Because the content of frame is changed, the FCS has to be recalculated
- Native VLAN – VLAN on trunk without tag (usually only one on trunk)

Tagged vs. Untagged interface



EtherChannel

Bonding

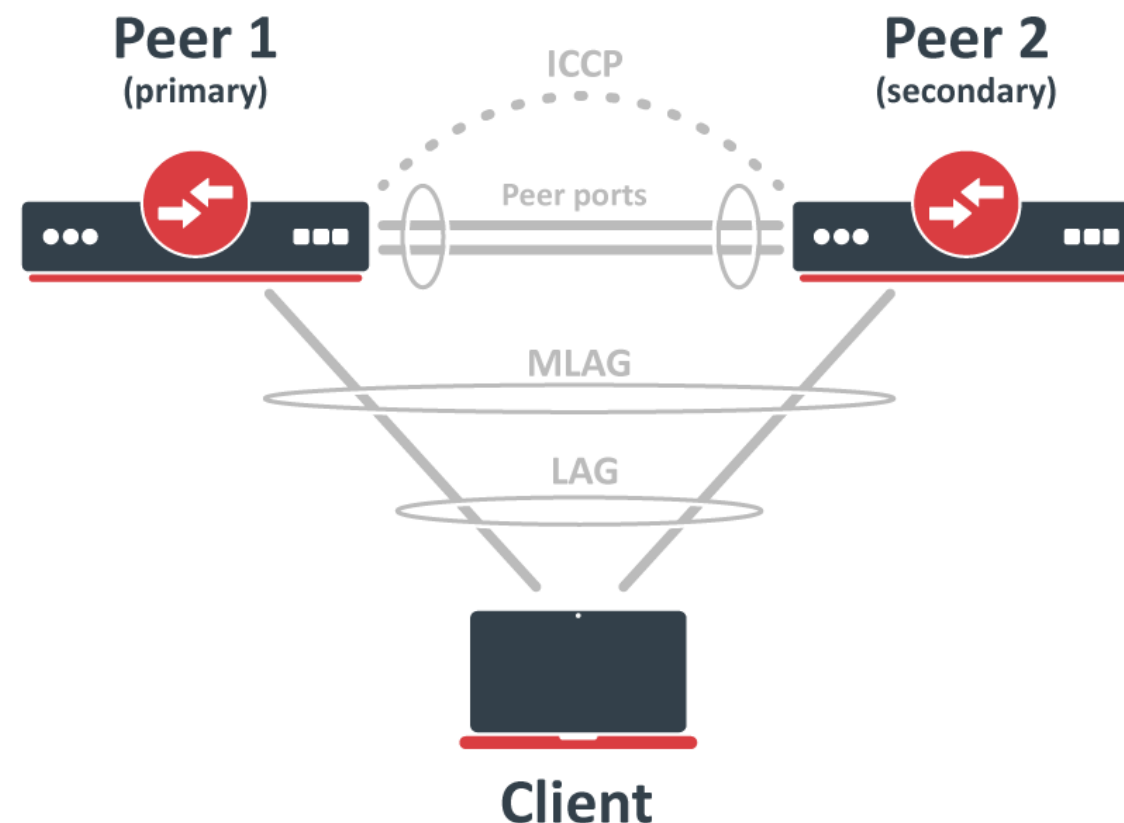
- Bonding – MikroTik term for:
 - Link Aggregation
 - EtherChannel
 - PortChannel
 - Channel Group
- All ports in bonding share same settings
- Preferred even number of links, max. 8 active

Bonding modes and balancing

- Modes:
 - 802.3ad (LACP) – standard IEEE
 - balancing based on – src MAC, dst MAC, VLAN tag, src IP, dst IP
 - balance-xor (proprietary mode)
 - balancing based on – src IP, dst IP, src port, dst port
 - balance-rr (round robin)
 - active-backup (one active, other backup)
 - broadcast (all links send same data)
 - balance-tlb (allows bonding with different speed interfaces)
 - balance-alb (same as tlb but balances by IPv4)

MLAG

- Multi-chassis Link Aggregation Group
- EtherChannel is ended on multiple different switches
 - LACP protocol to switch
 - ICGP (Inter Chassis Control Protocol) between switches
- STP setting must be same on both switches

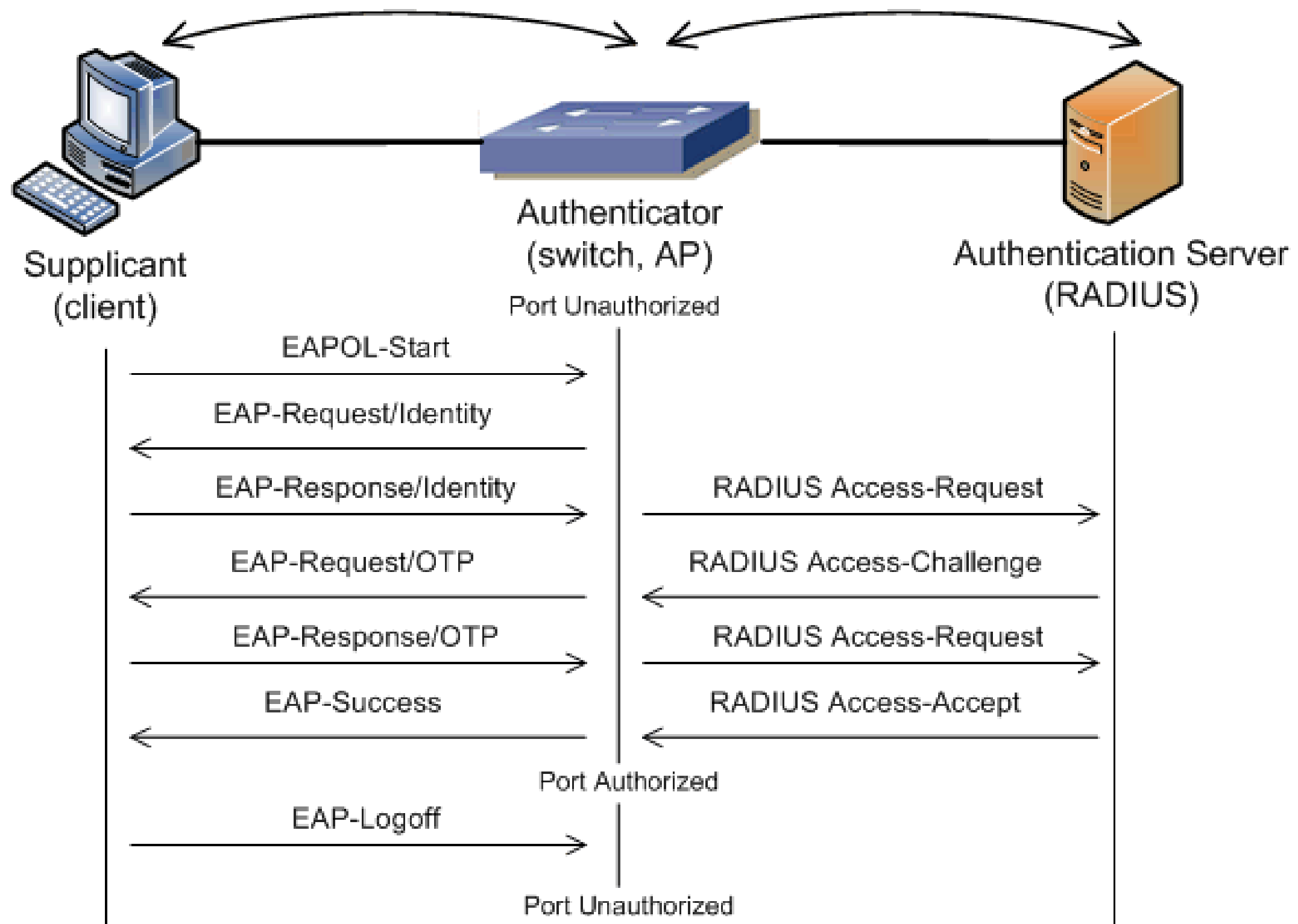


dot1x (802.1x)

802.1X

- IEEE 802.1x – Network Access Control (NAC)
 - Authentication protocol for control access of device or user to the network
 - Part AAA framework
 - Uses these protocols:
 - EAP (EAP-MD5, PEAP, EAP-TLS)
 - RADIUS/TACACS+
- Important roles:
 - Supplicant
 - Authenticator
 - Authentication Server

802.1x using EAP-MD5/RADIUS



Otázky

