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

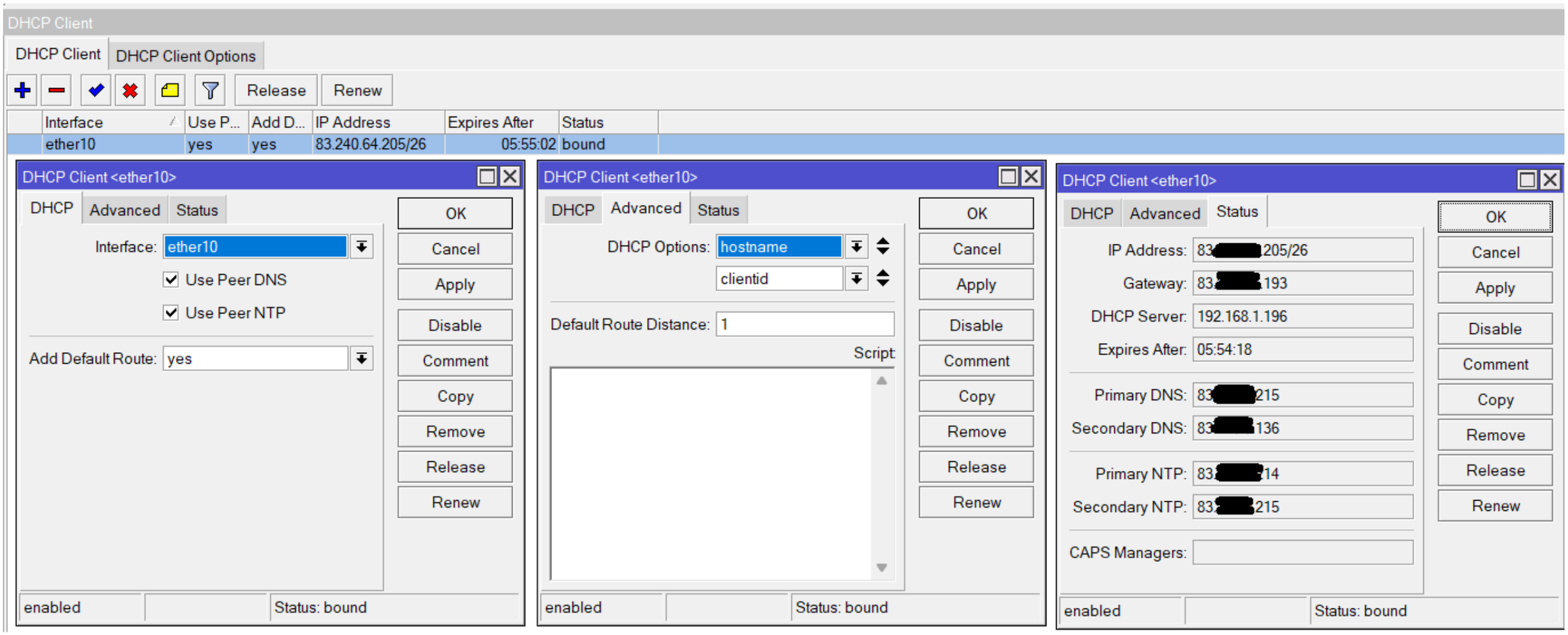
DHCP

- 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 sufix (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

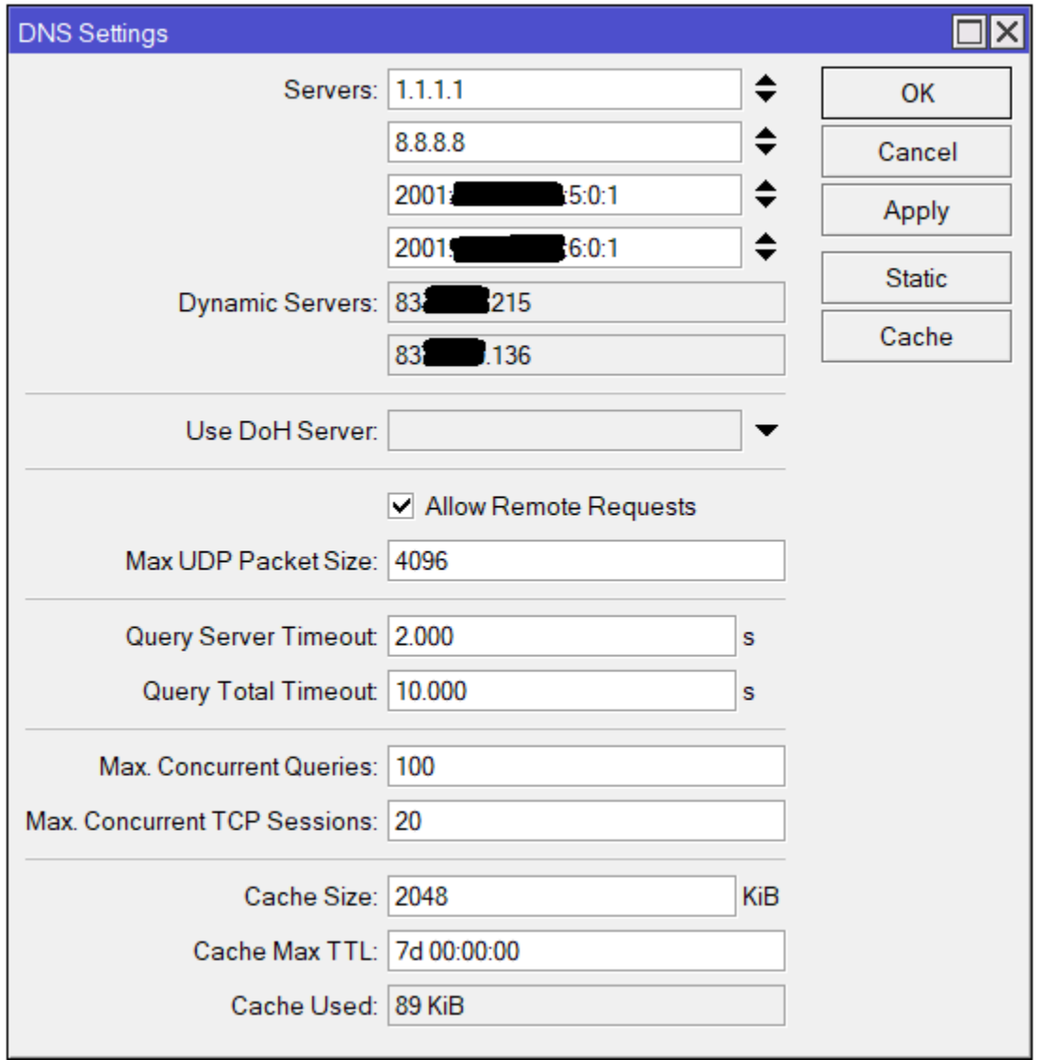
DHCP Client



IP → DHCP Client

DNS

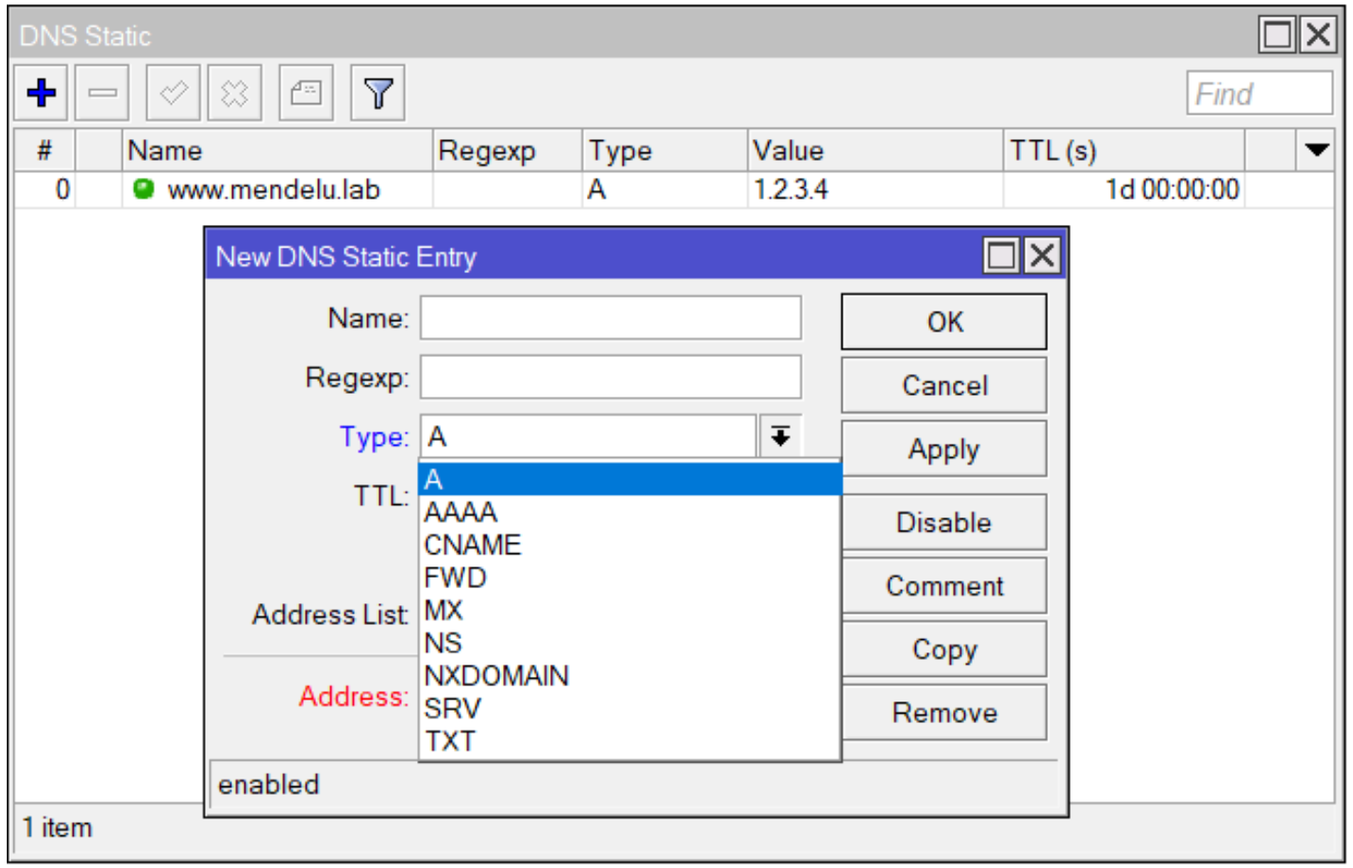
- By default DHCP client asks for a DNS server IP address
- It can also be entered manually if other DNS server is needed or DHCP is not used



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

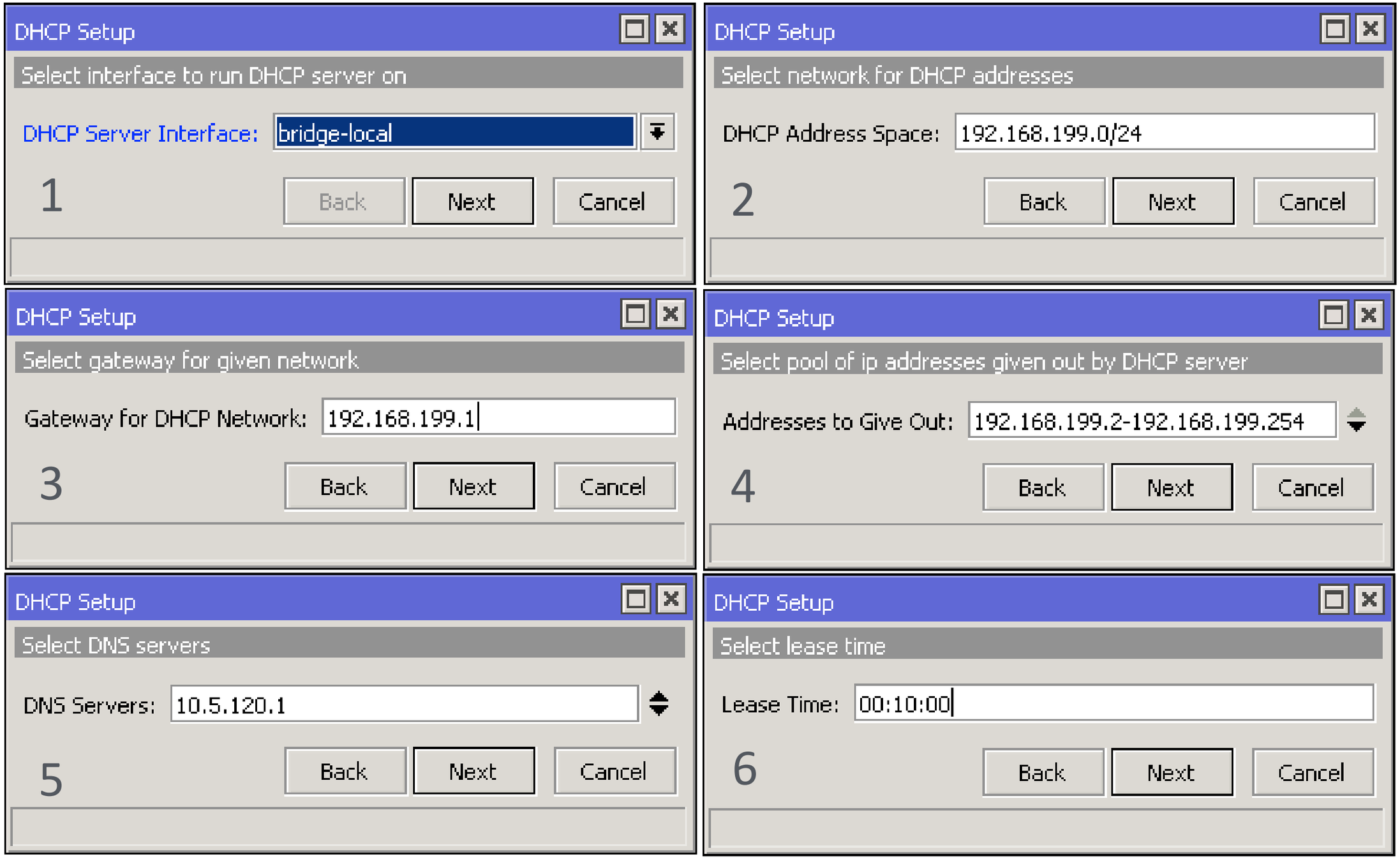


IP → DNS → Static

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

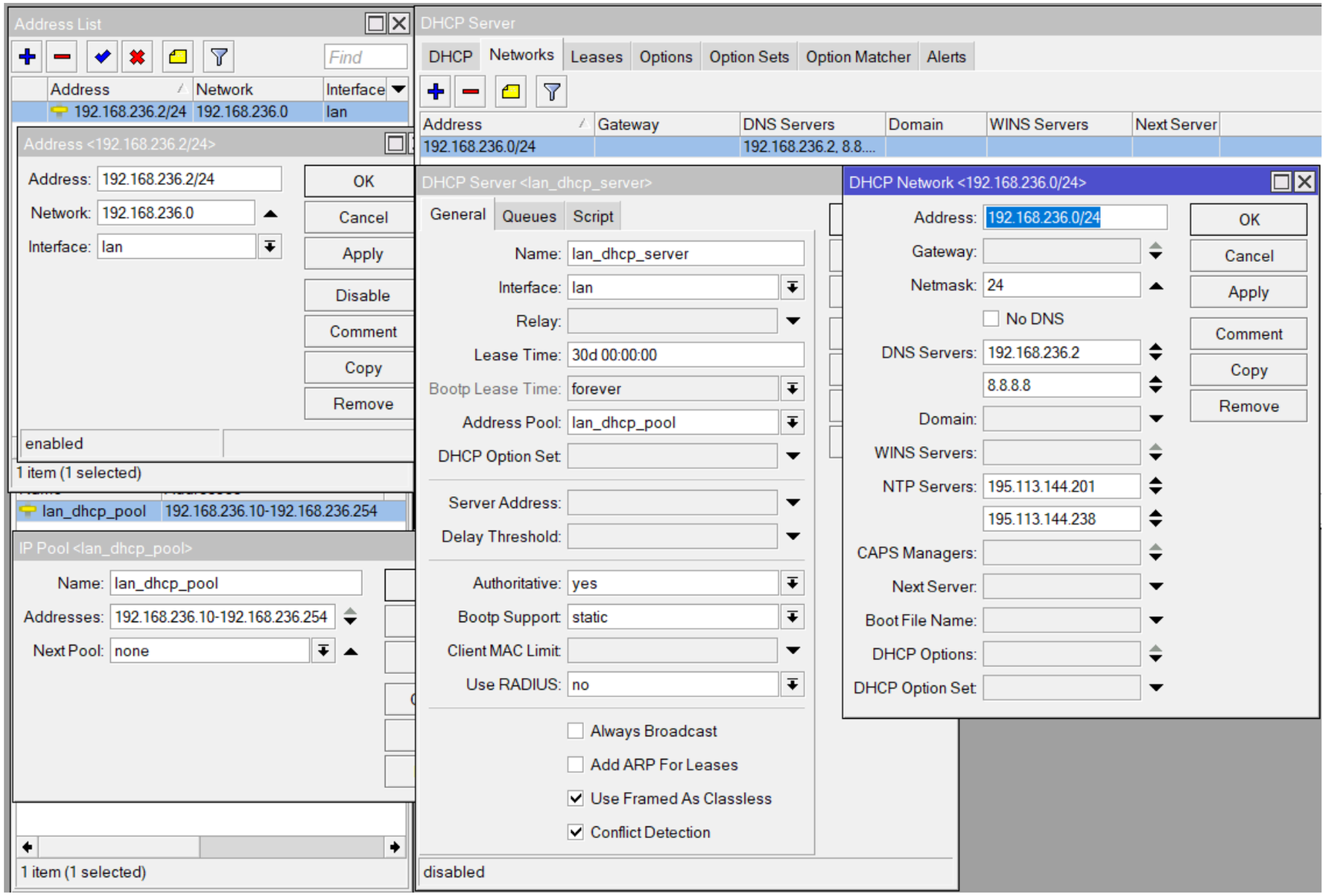
DHCP Server – Setup



IP → DHCP Server → DHCP Setup

DHCP Server

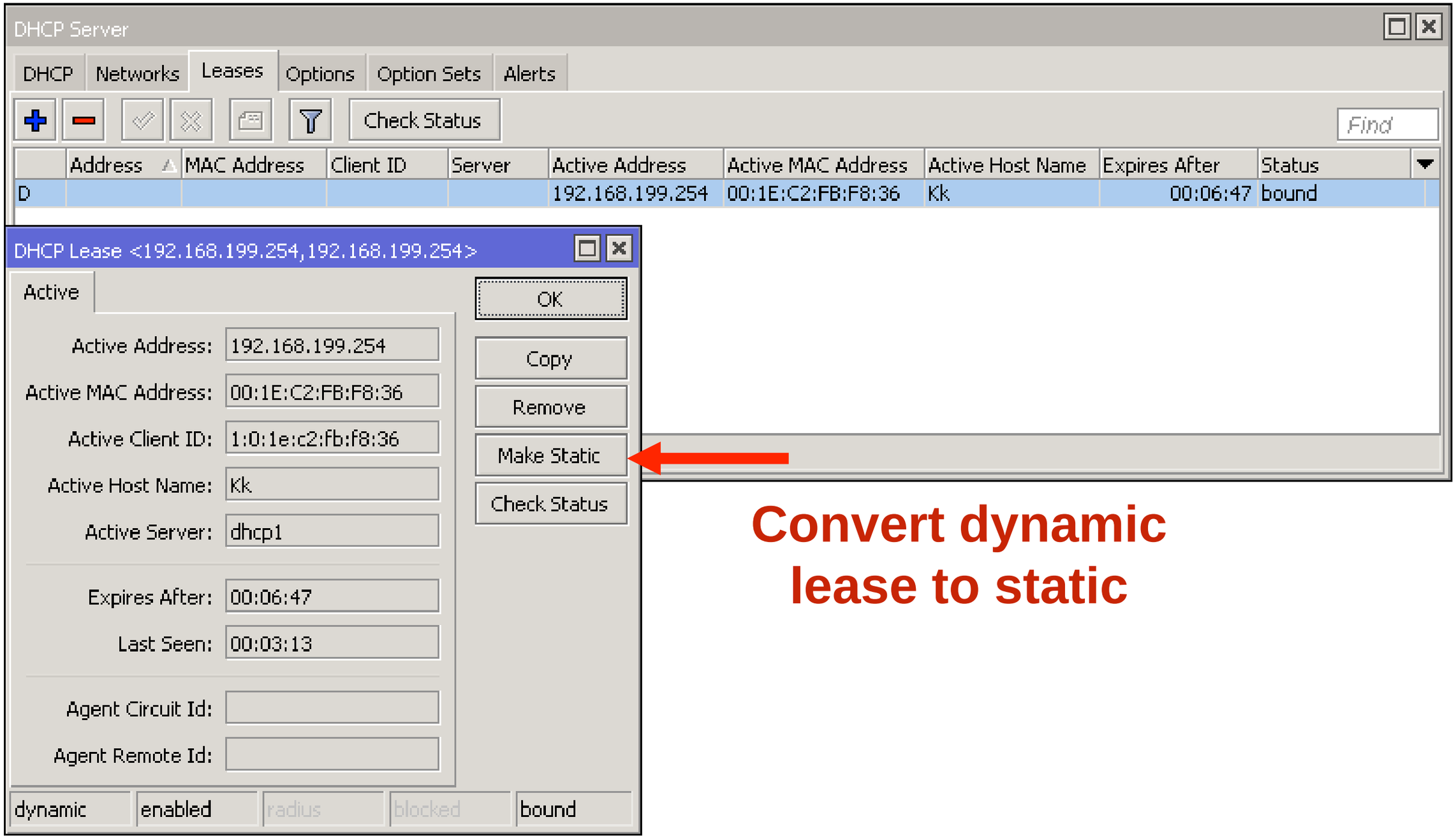
- DHCP Server Setup wizard has created a new IP pool and DHCP Server



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

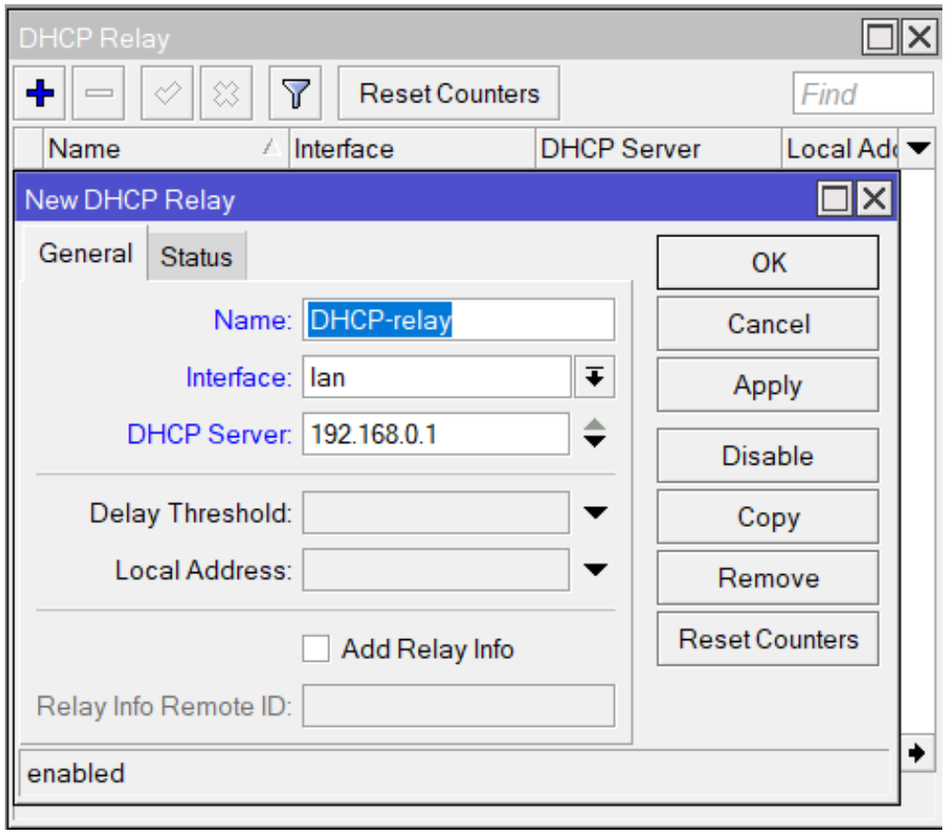


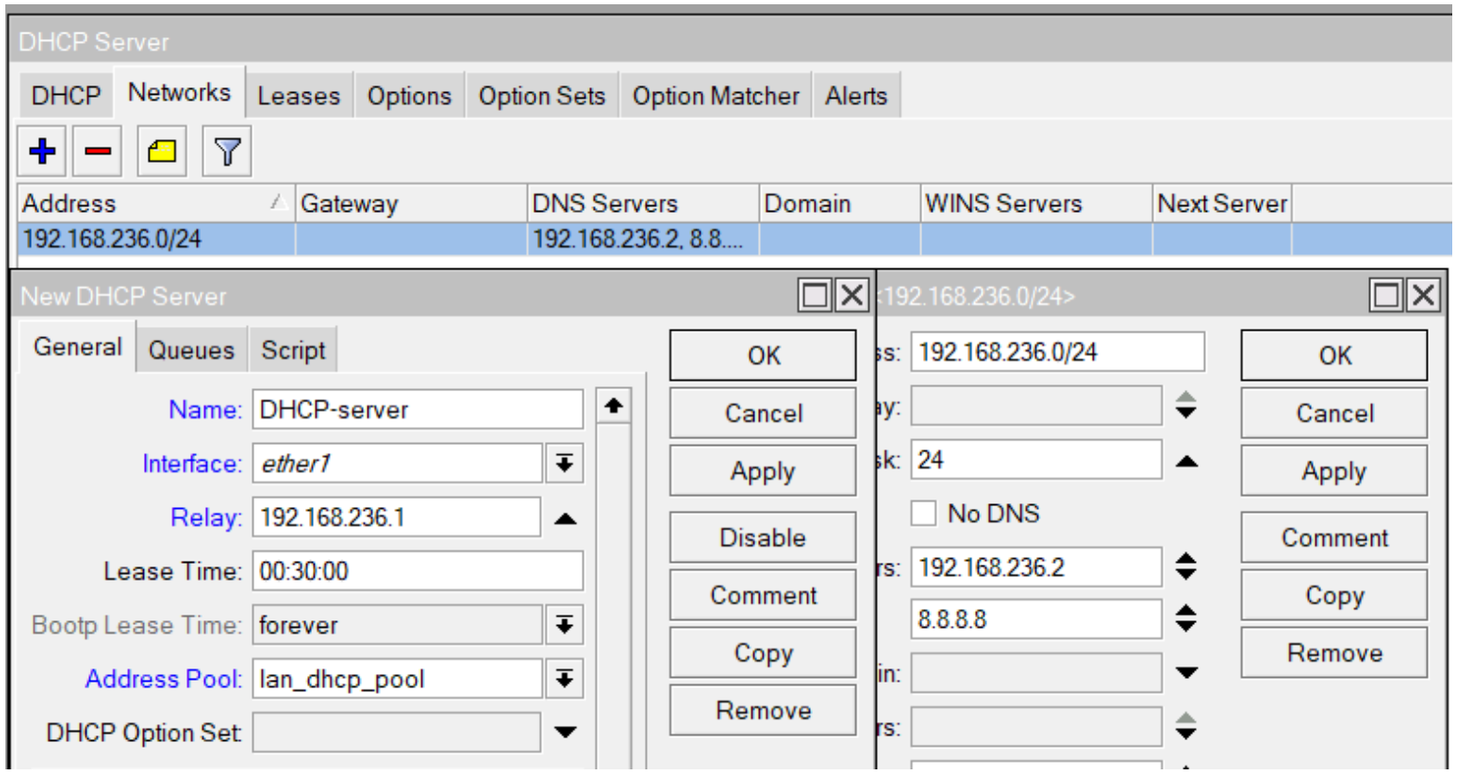
Convert dynamic lease to static

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.





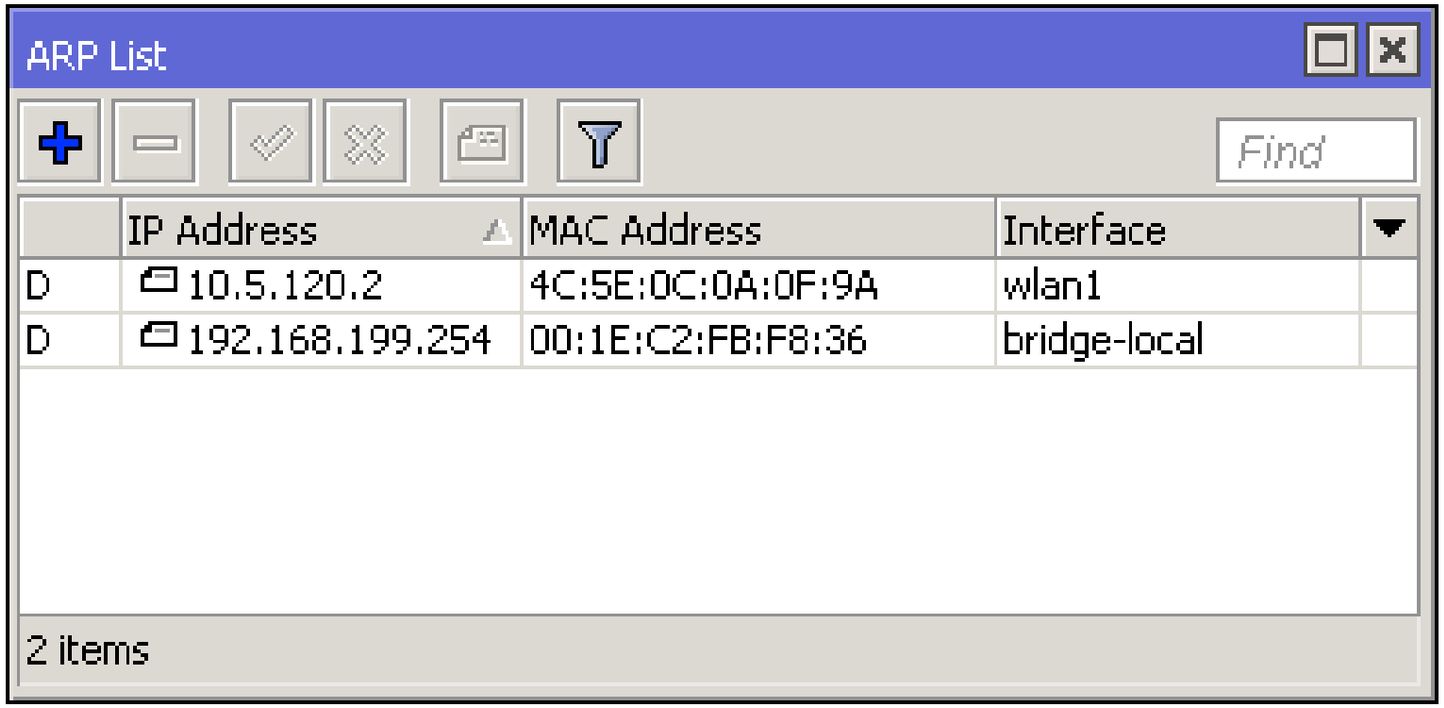
ARP

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

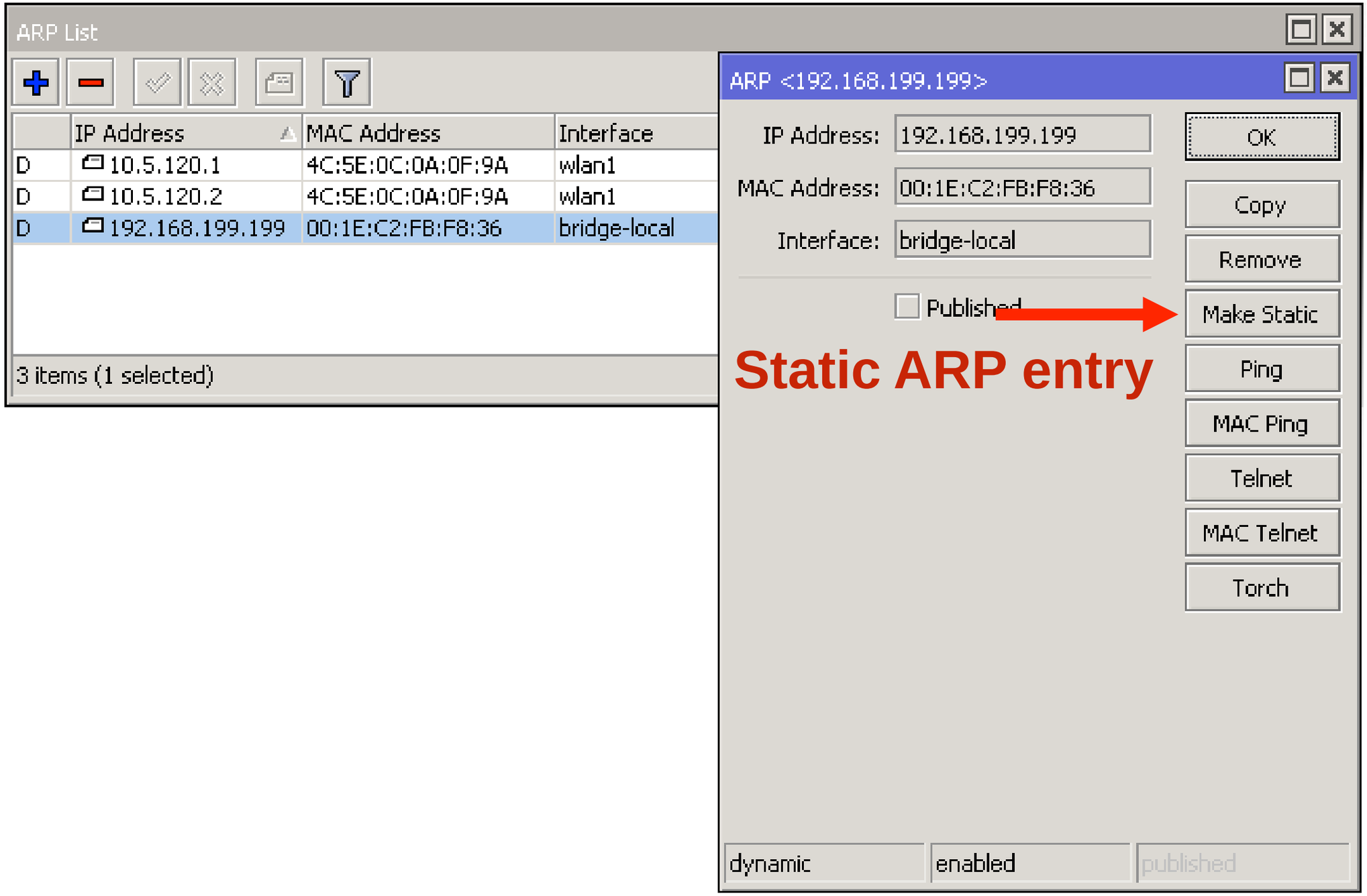


IP → ARP

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

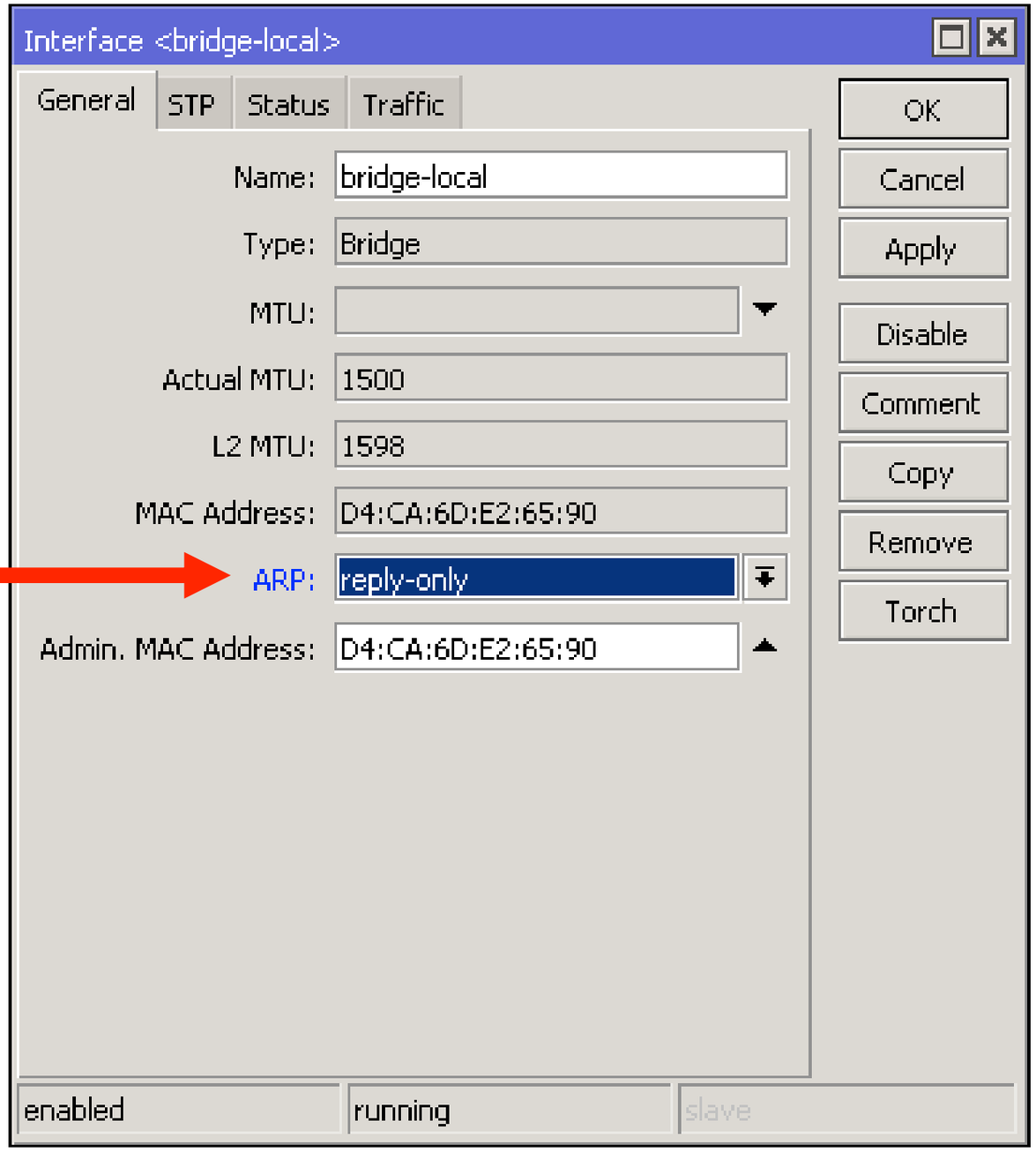
Static ARP



IP → ARP

ARP mode

Interface will reply only to known ARP entries

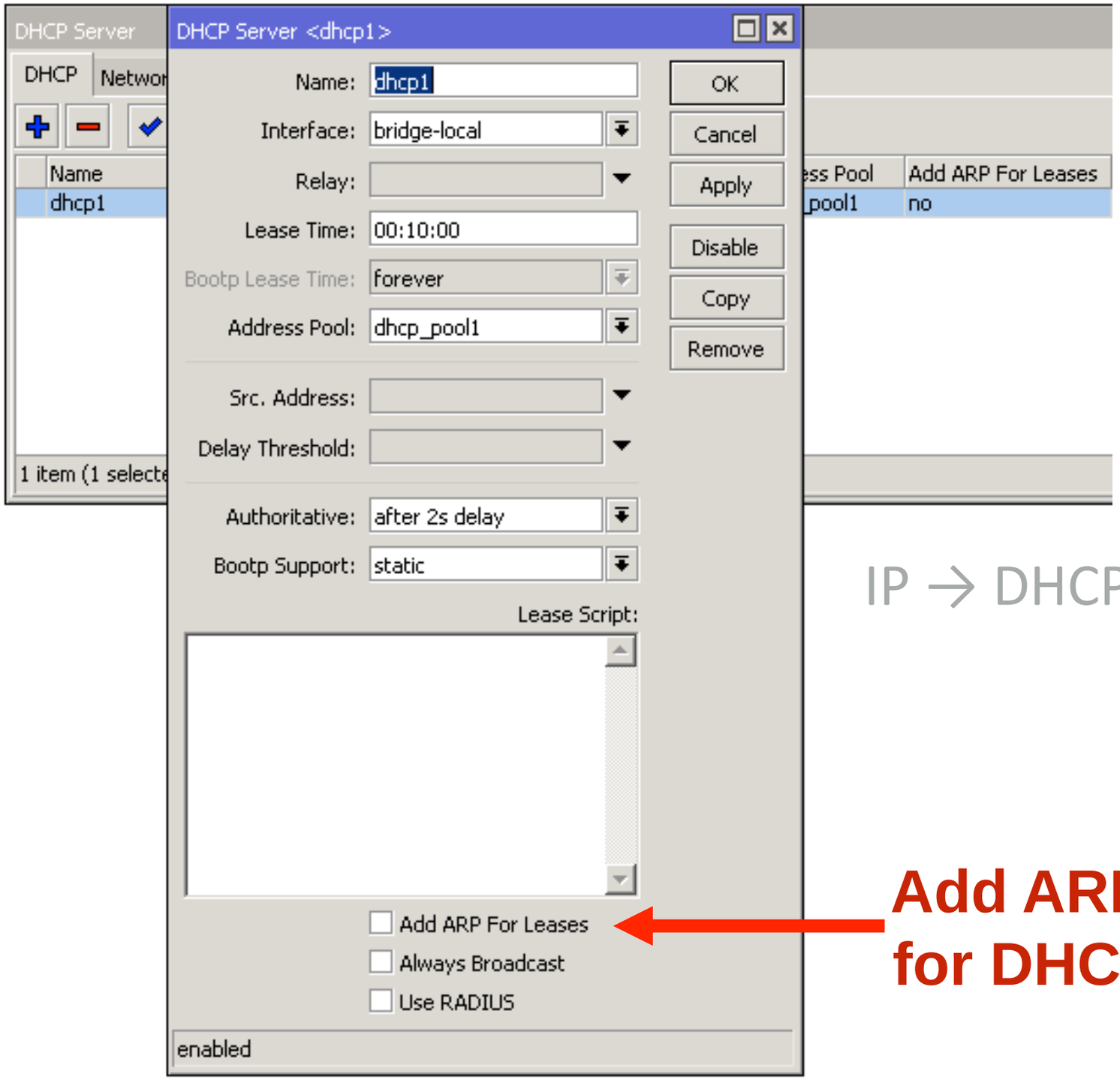


Interfaces → bridge-local

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



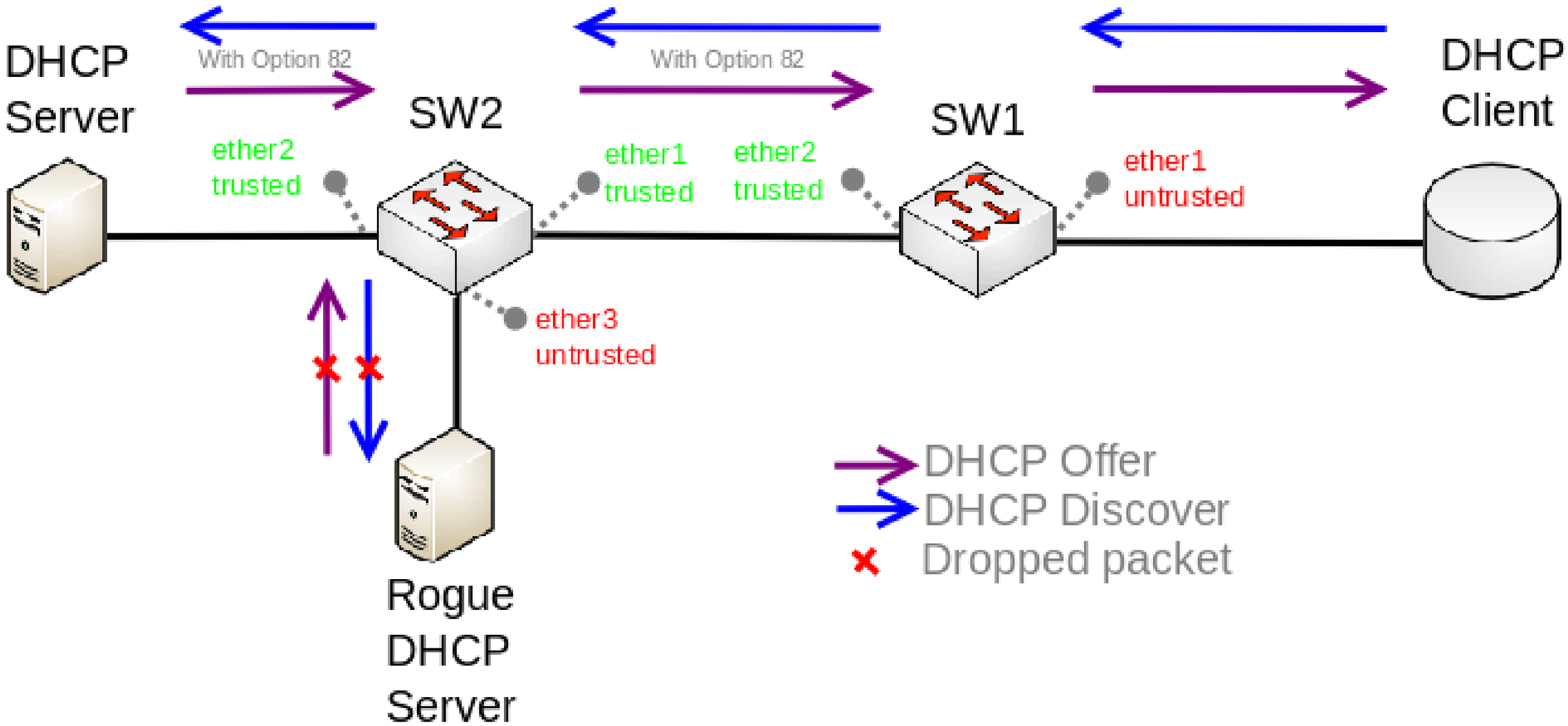
IP → DHCP Server

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

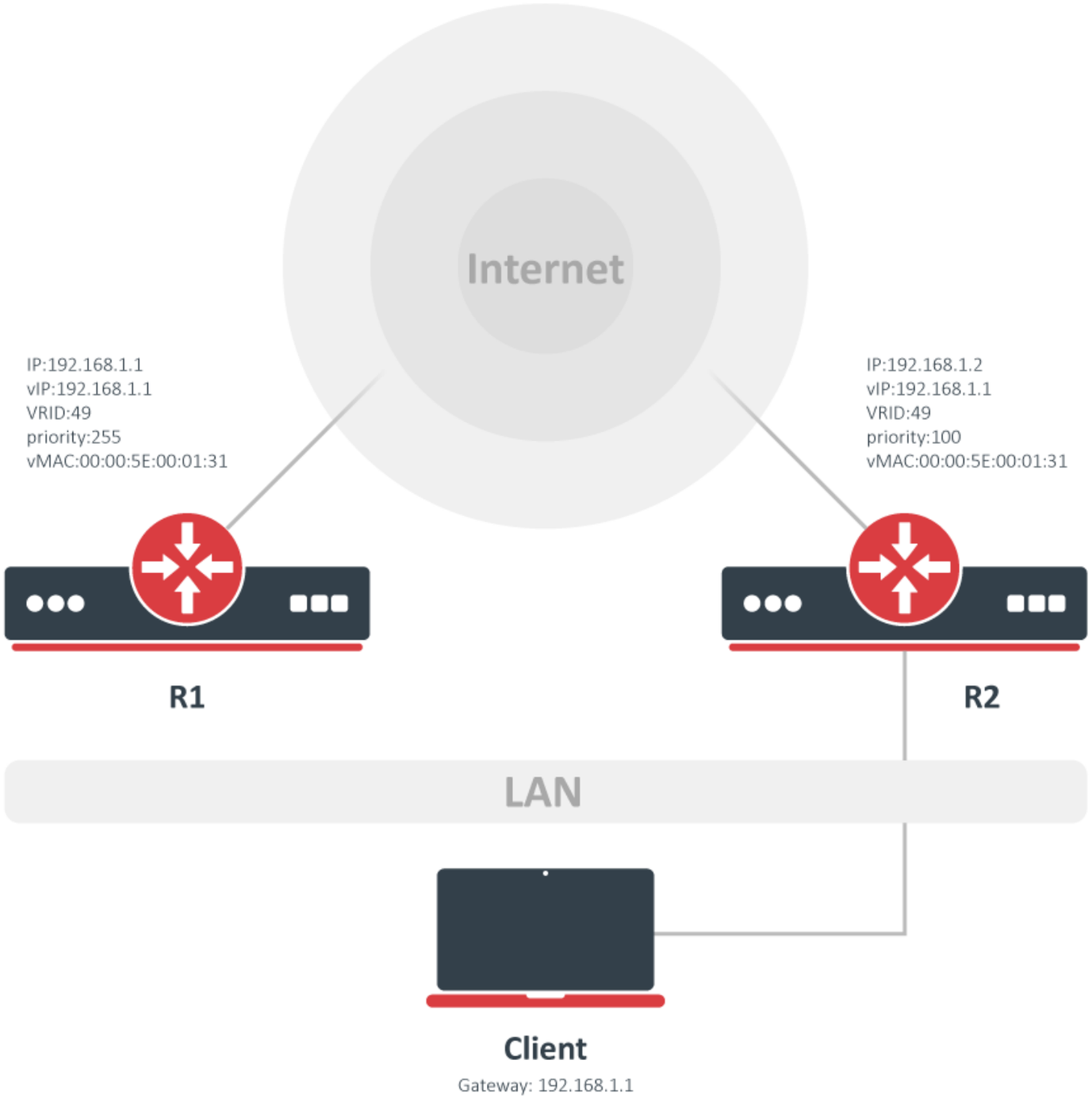


VRRP

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



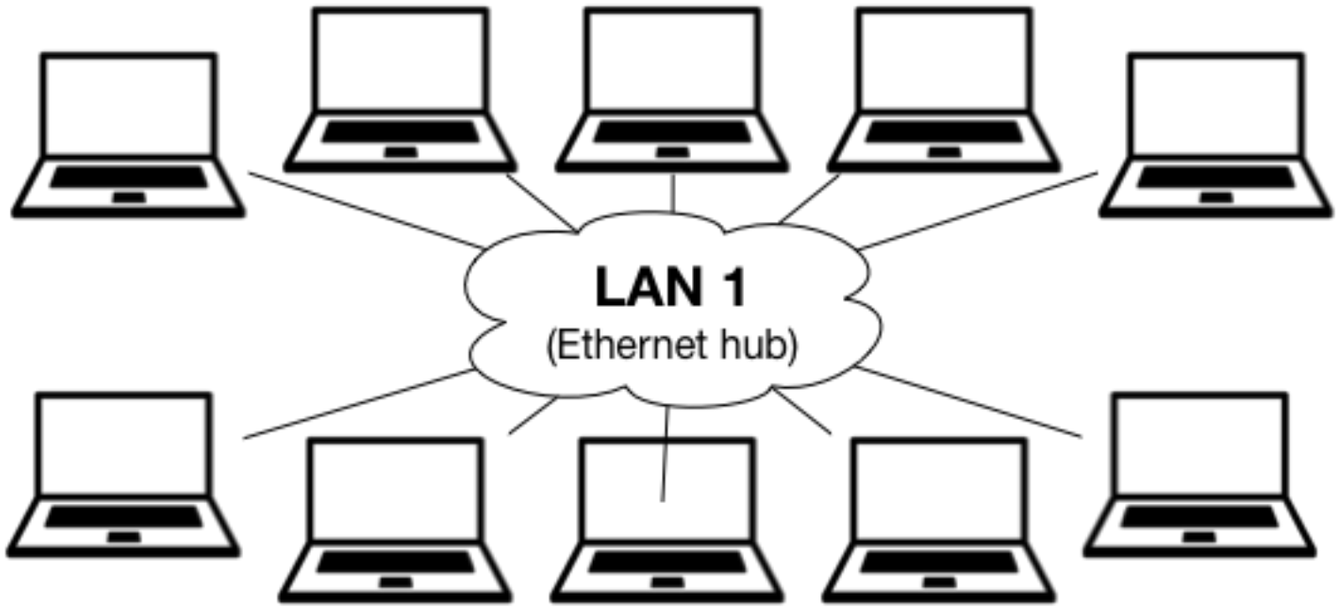
Switching

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

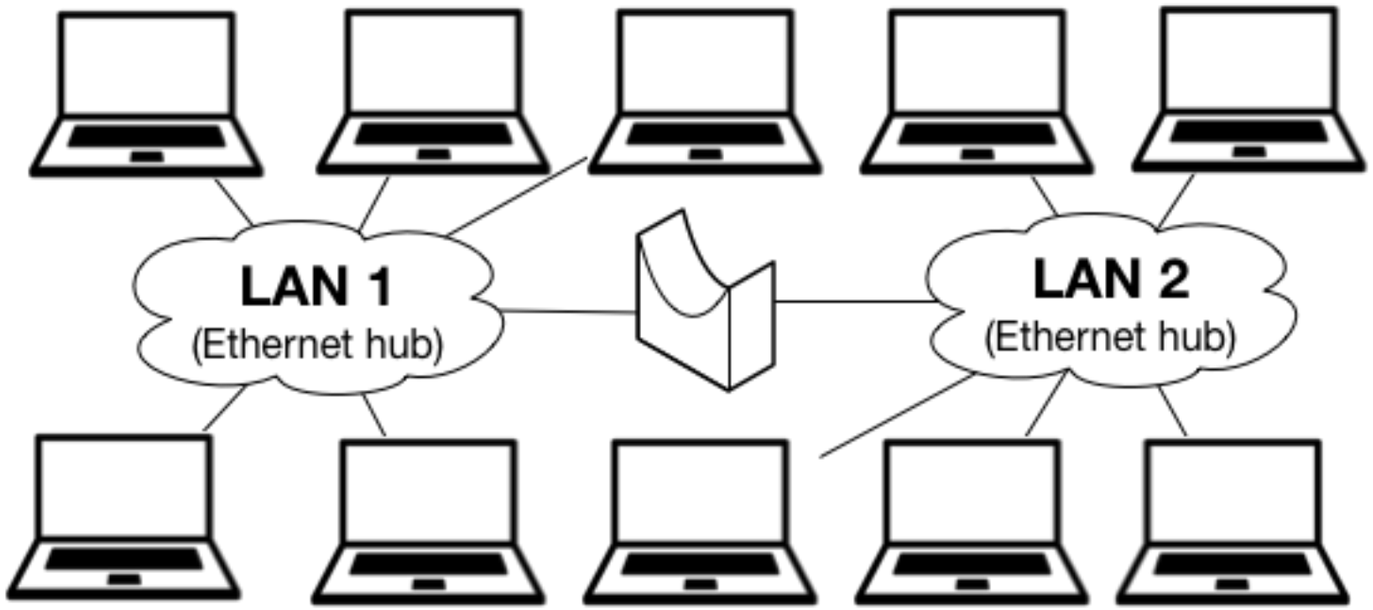
Hub – historic principle

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



Bridge (switch)

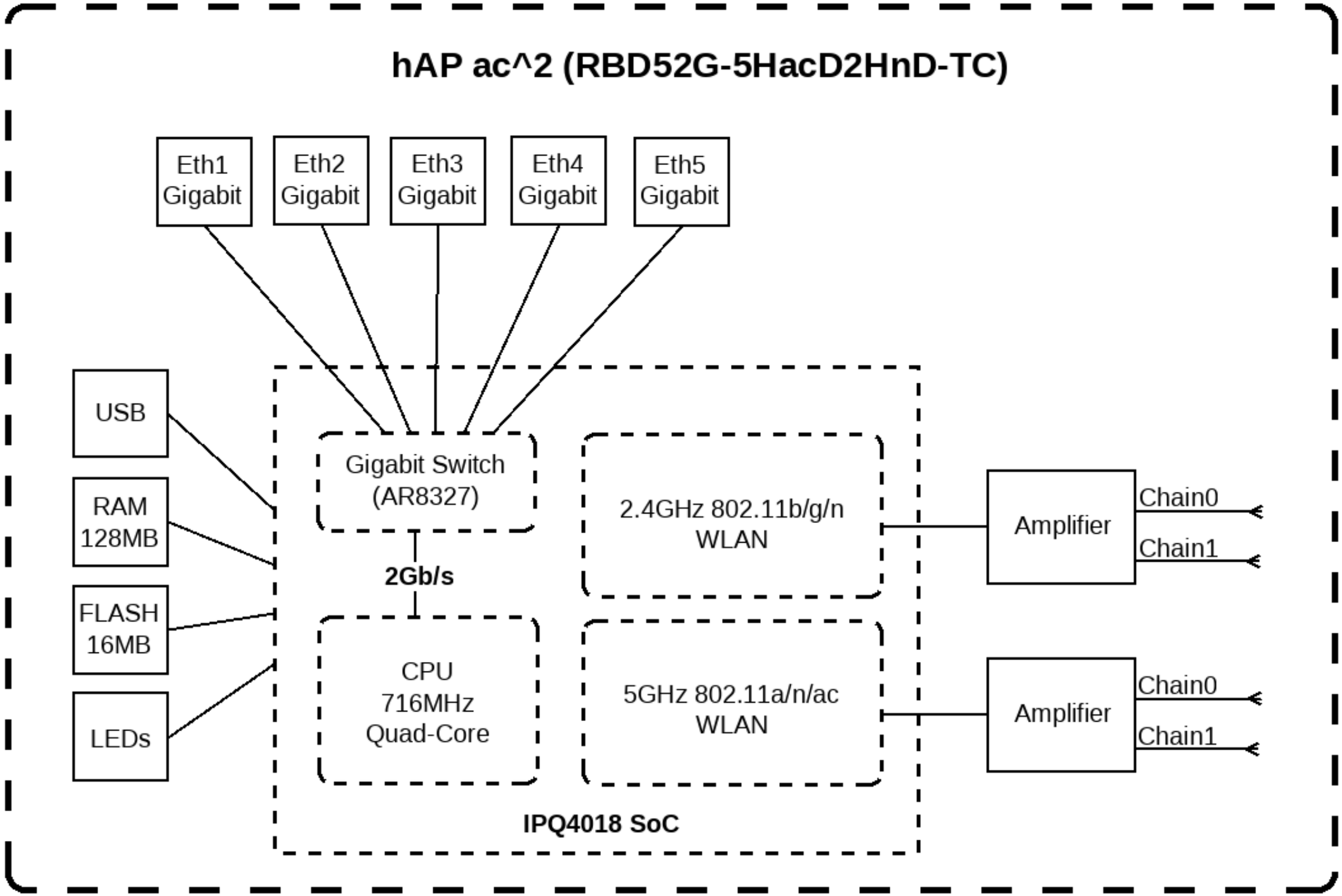
- All hosts still can communicate with each other
- Now there are 2 collision domains



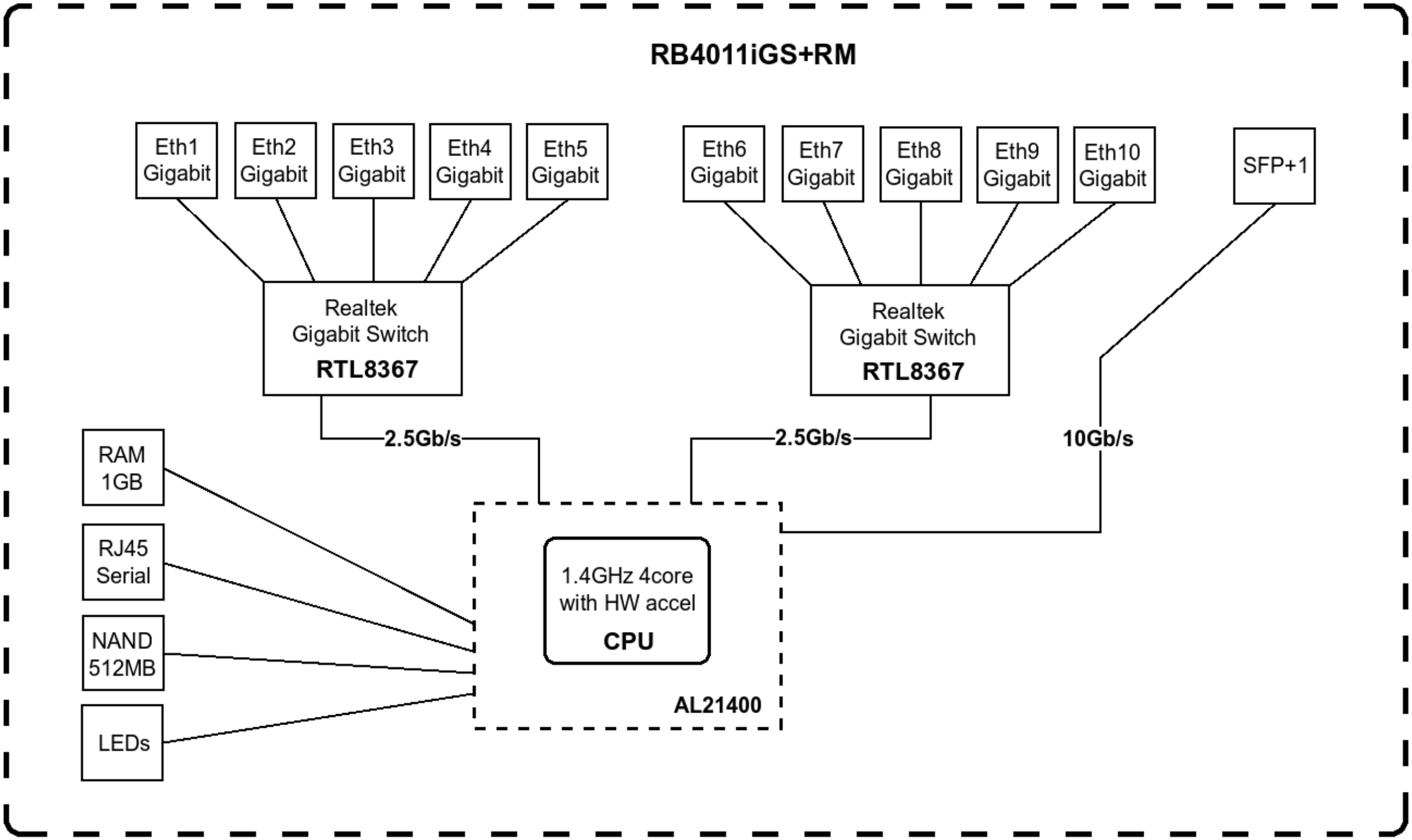
Bridge

- 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

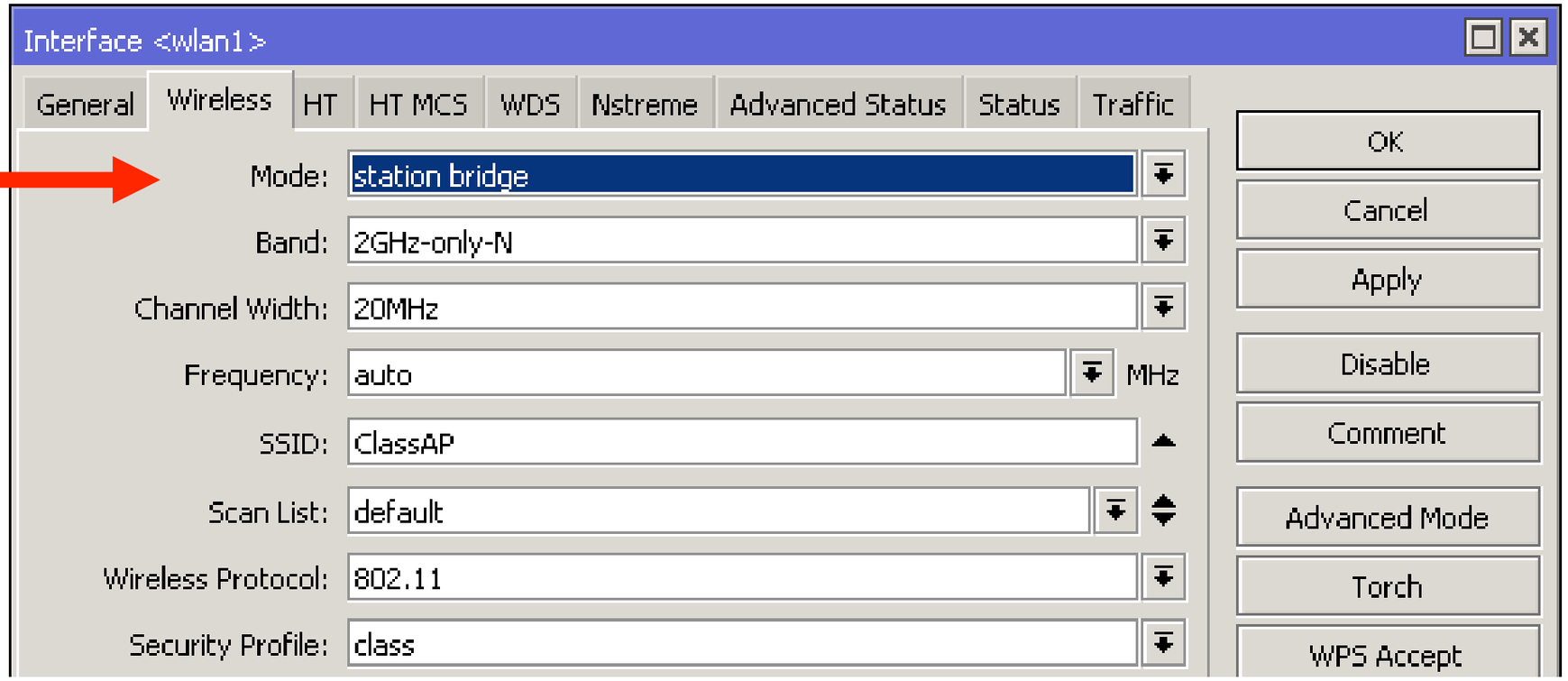
- Port switching
- CAM table
- Port mirroring
- Tx/Rx limit
- Host table (ARP)
- VLAN table, VLAN header check
- Port isolation, Private VLAN

Bridge

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

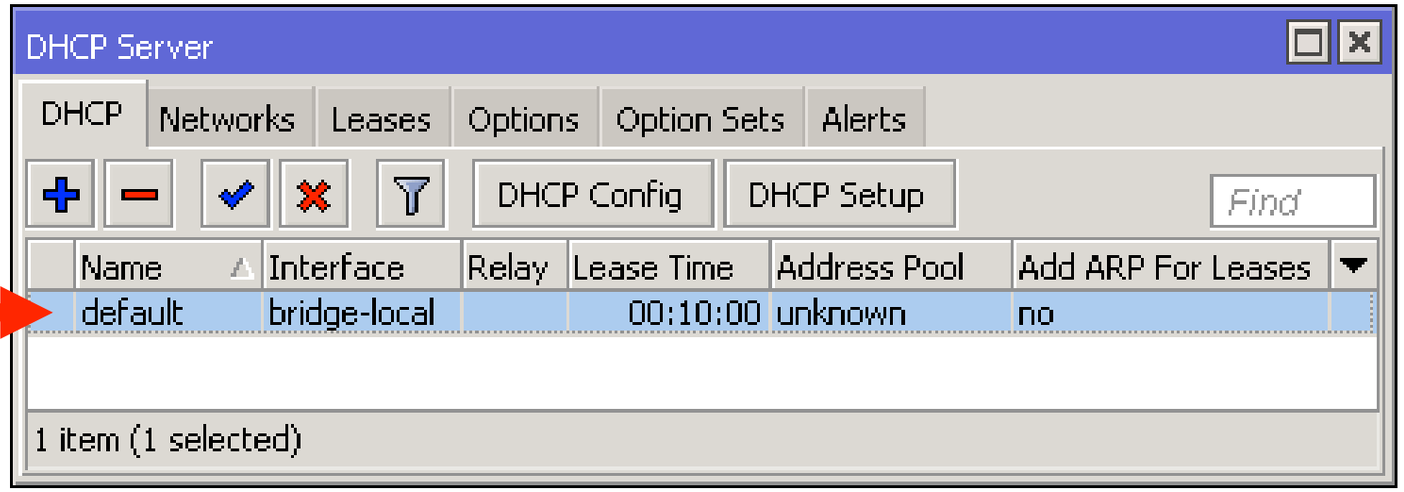
Bridge

Set mode to station bridge



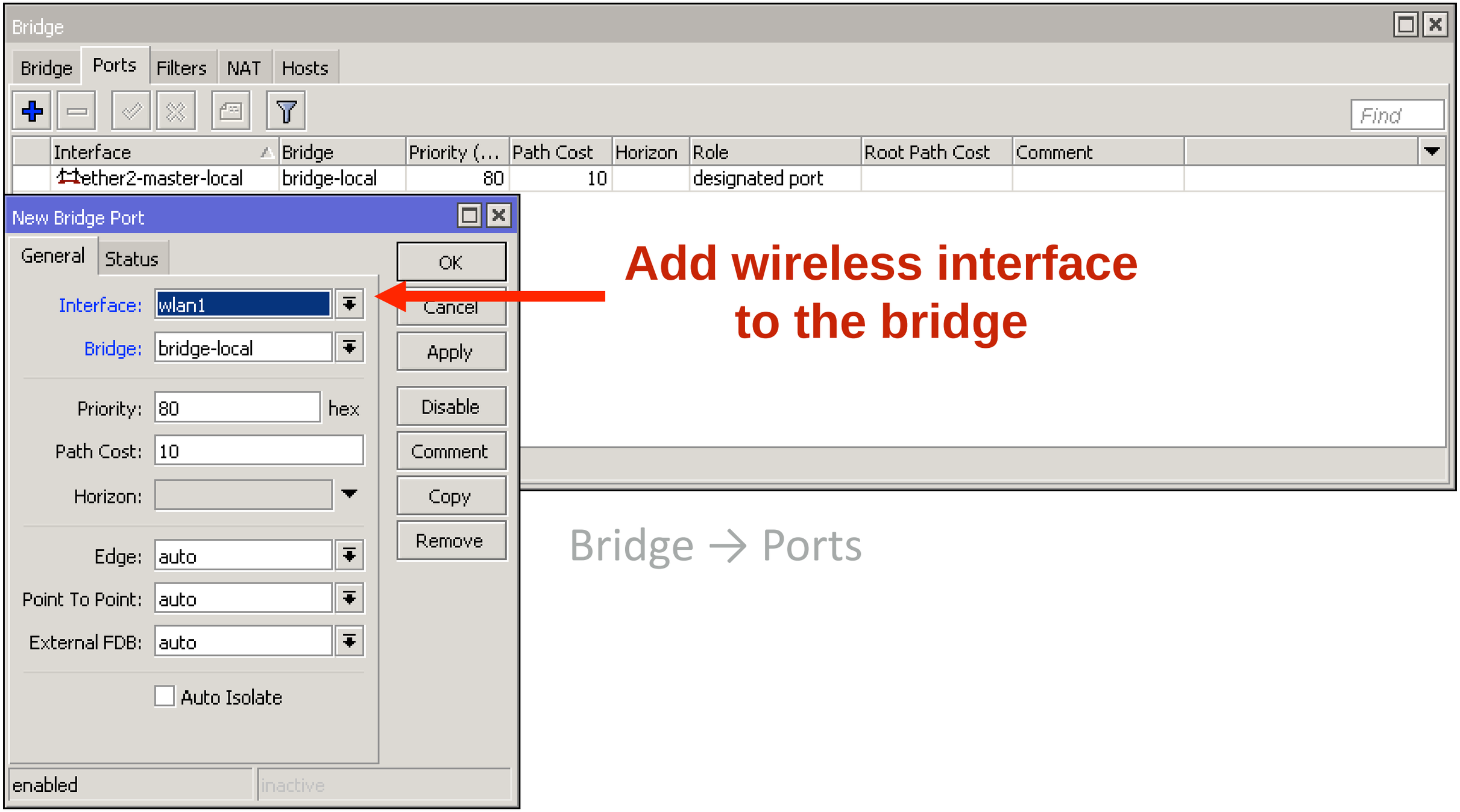
Wireless → wlan1

Disable DHCP Server



IP → DHCP Server

Bridge



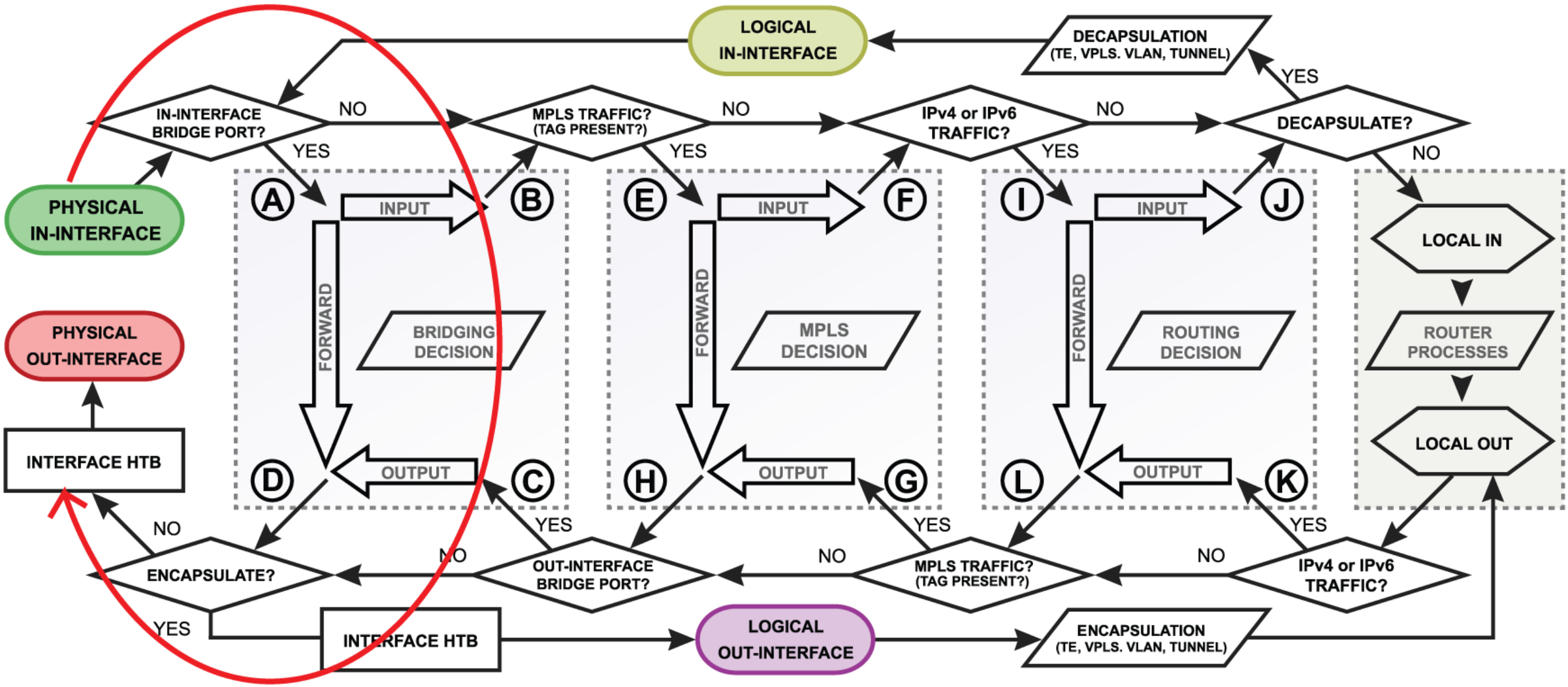
Add wireless interface to the bridge

Bridge → Ports

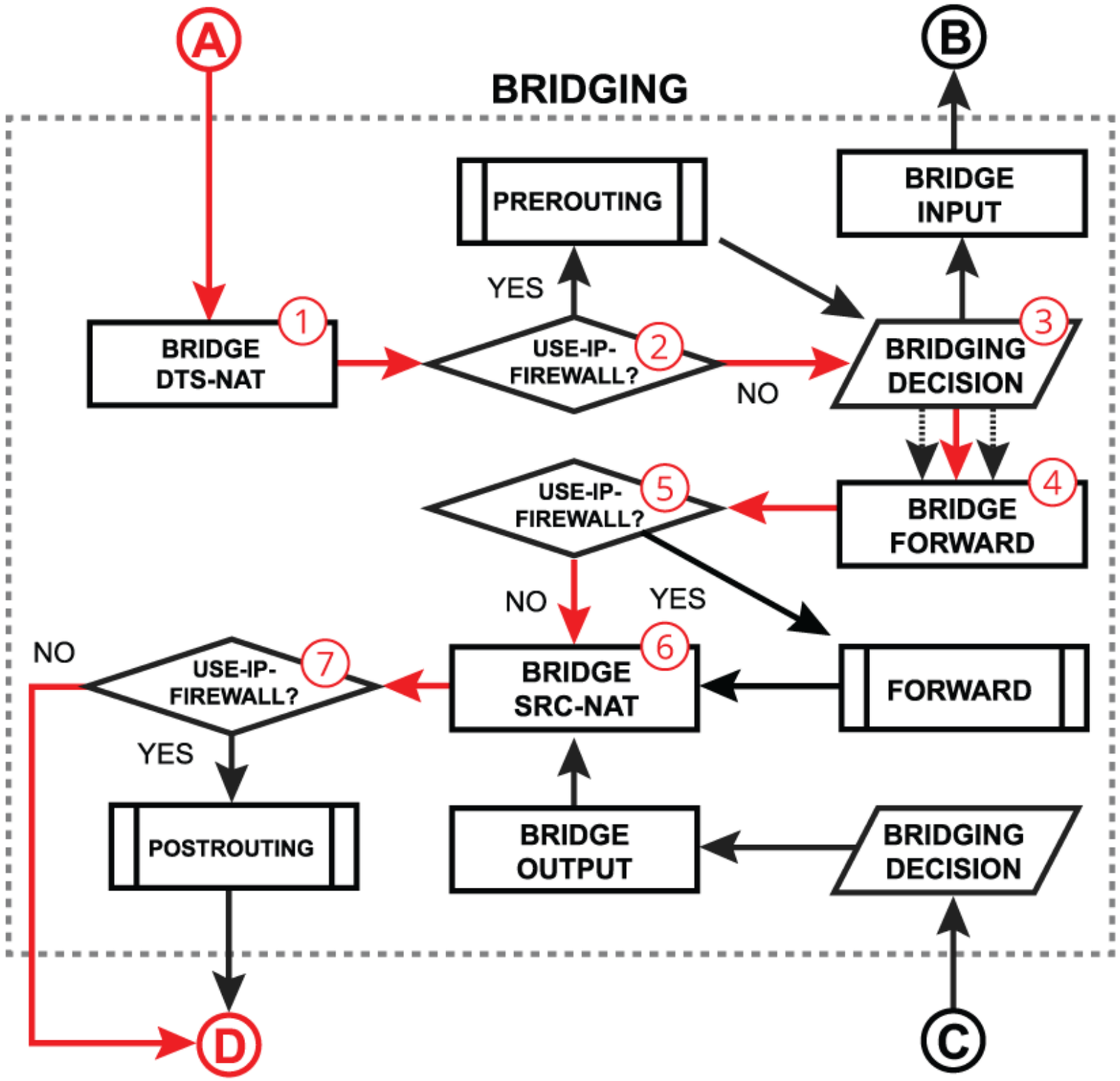
Bridge Firewall

- 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



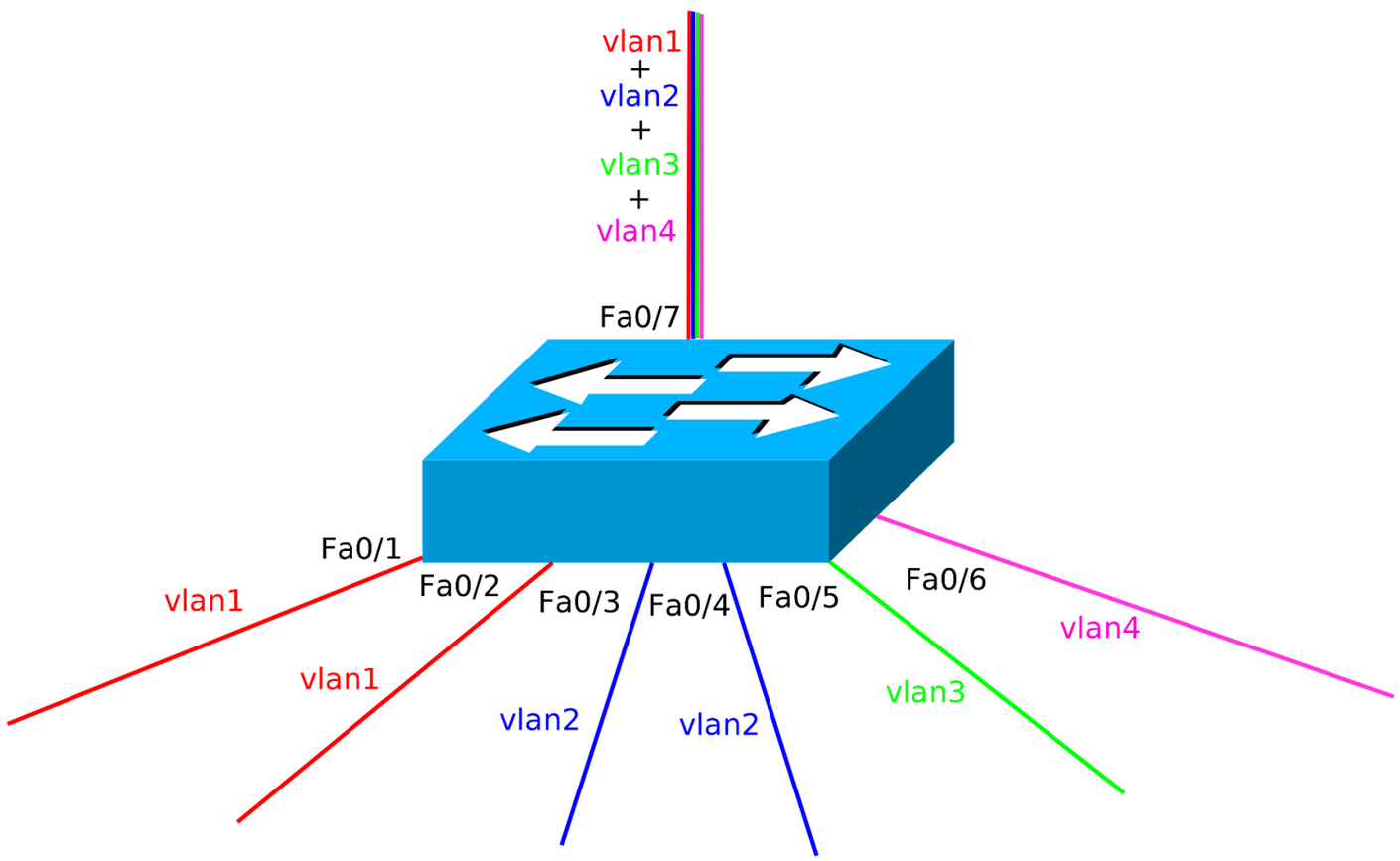
Bridge Firewall



VLAN

VLAN – Virtual Local Area Network

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



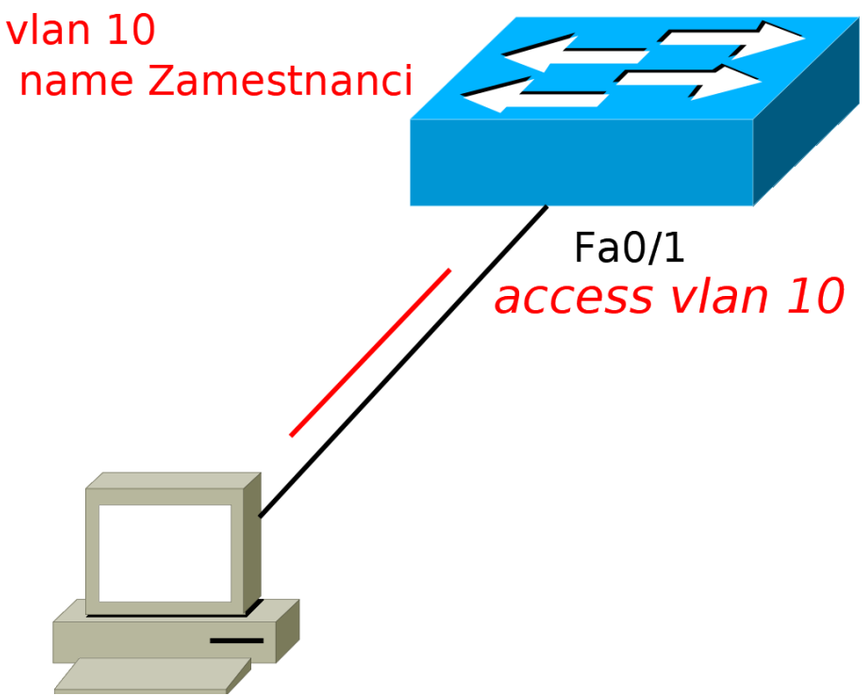
Access port vs. trunk port

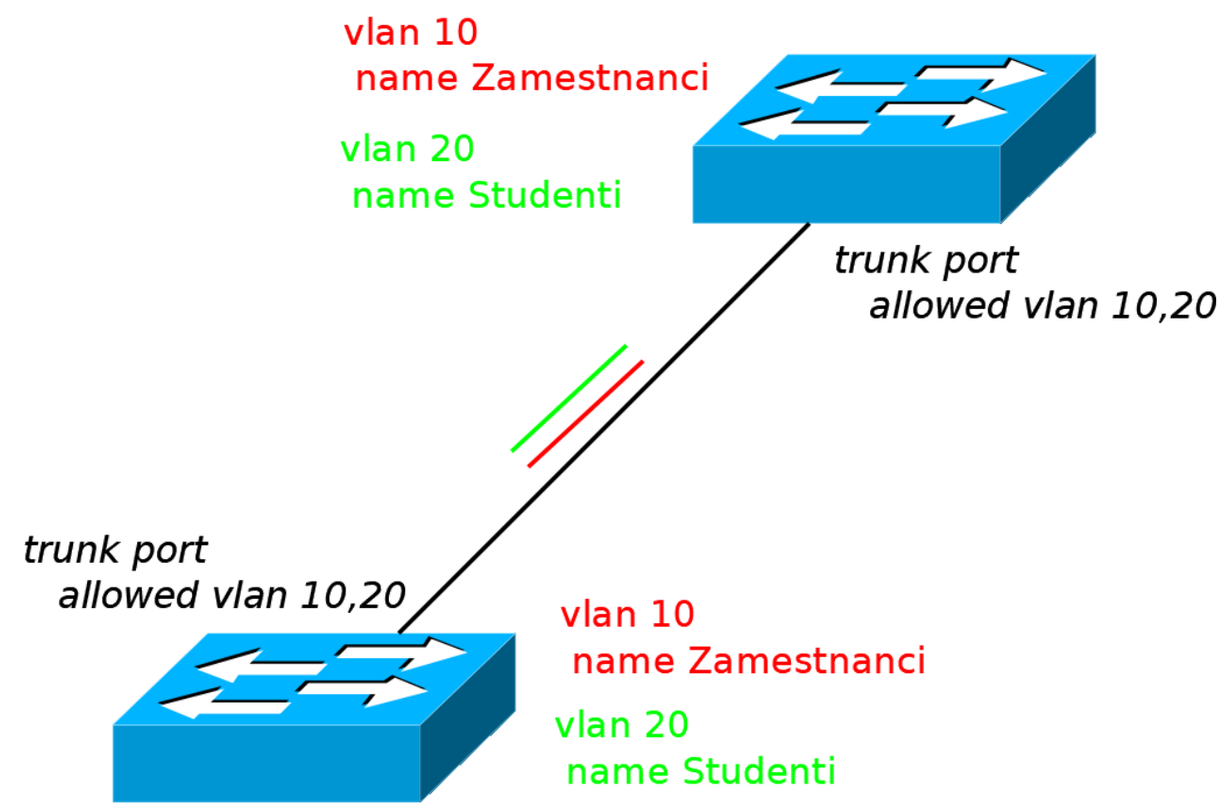
- Usually for end device connection (PC, server,…)
- Interface and all traffic is in one VLAN

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 |
```

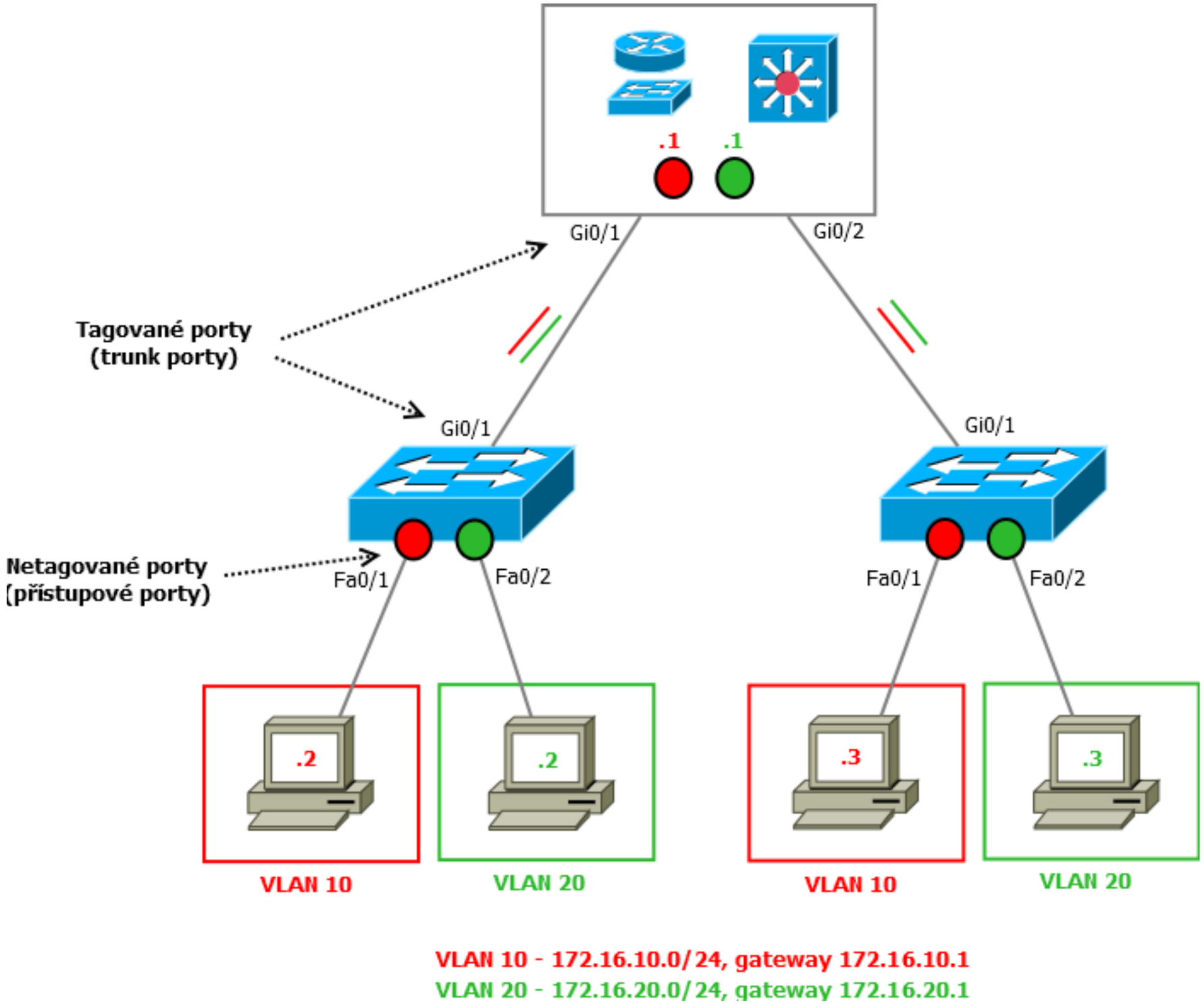
- Ethernet frame with VLAN tag (802.1q):

```
| 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

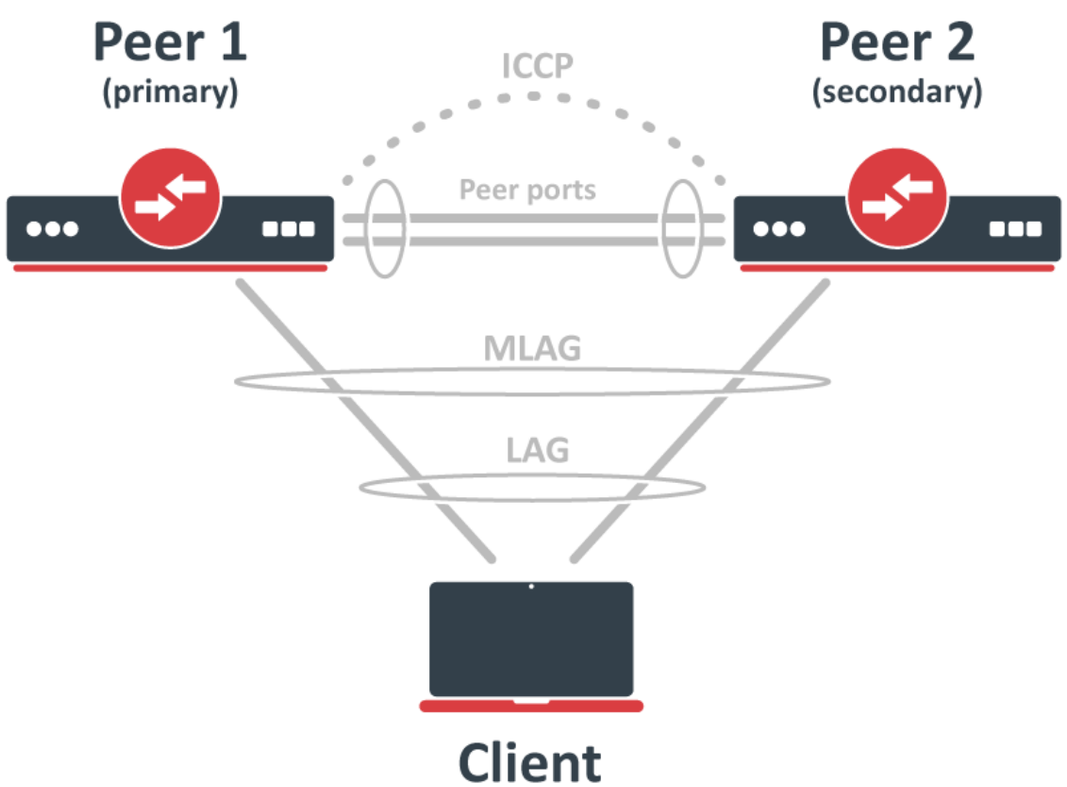
- All ports in bonding share same settings
- Prefered even number of links, max. 8 active

Bonding modes and balancig

- 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

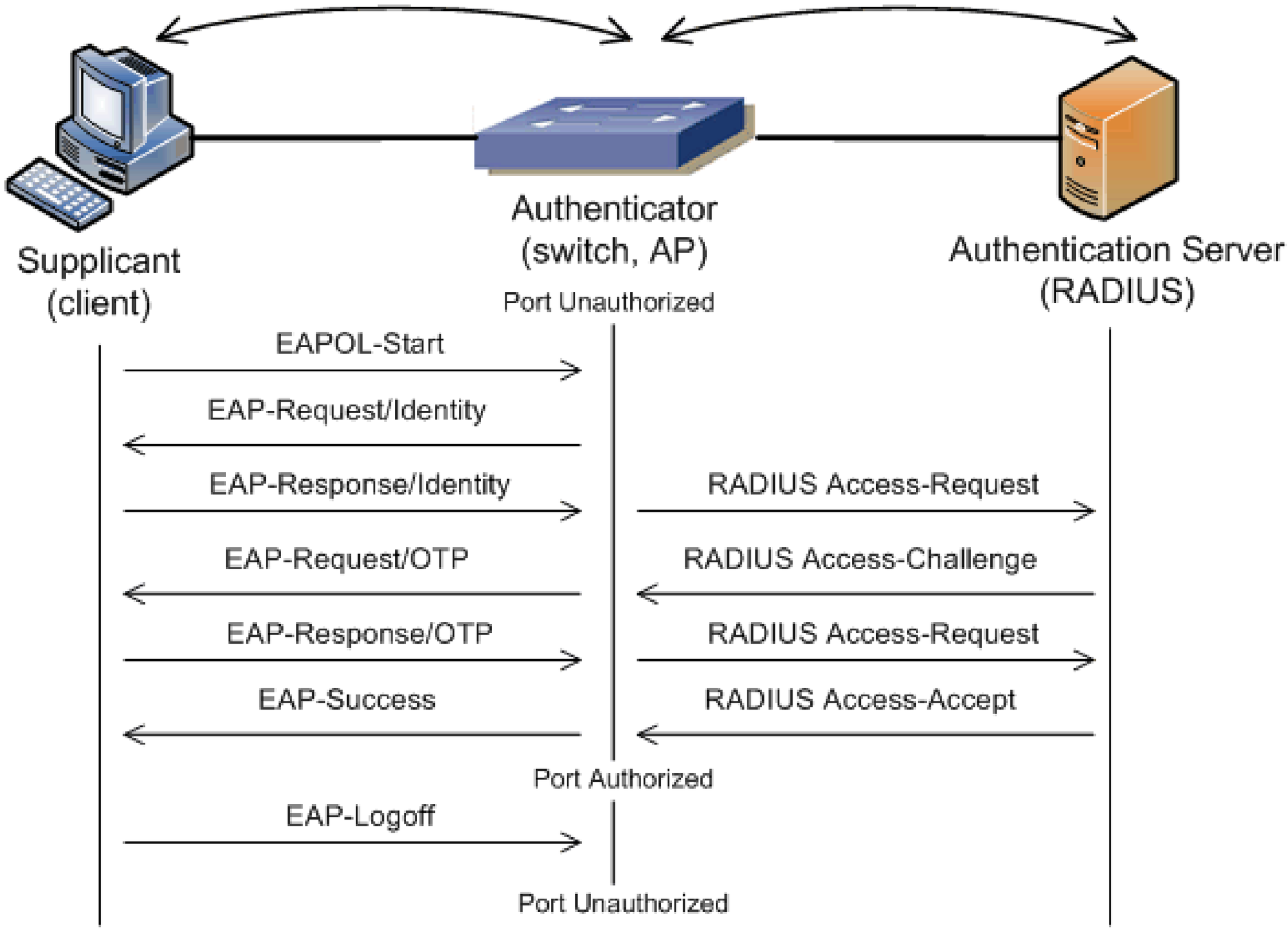


dot1x (802.1x)

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

?