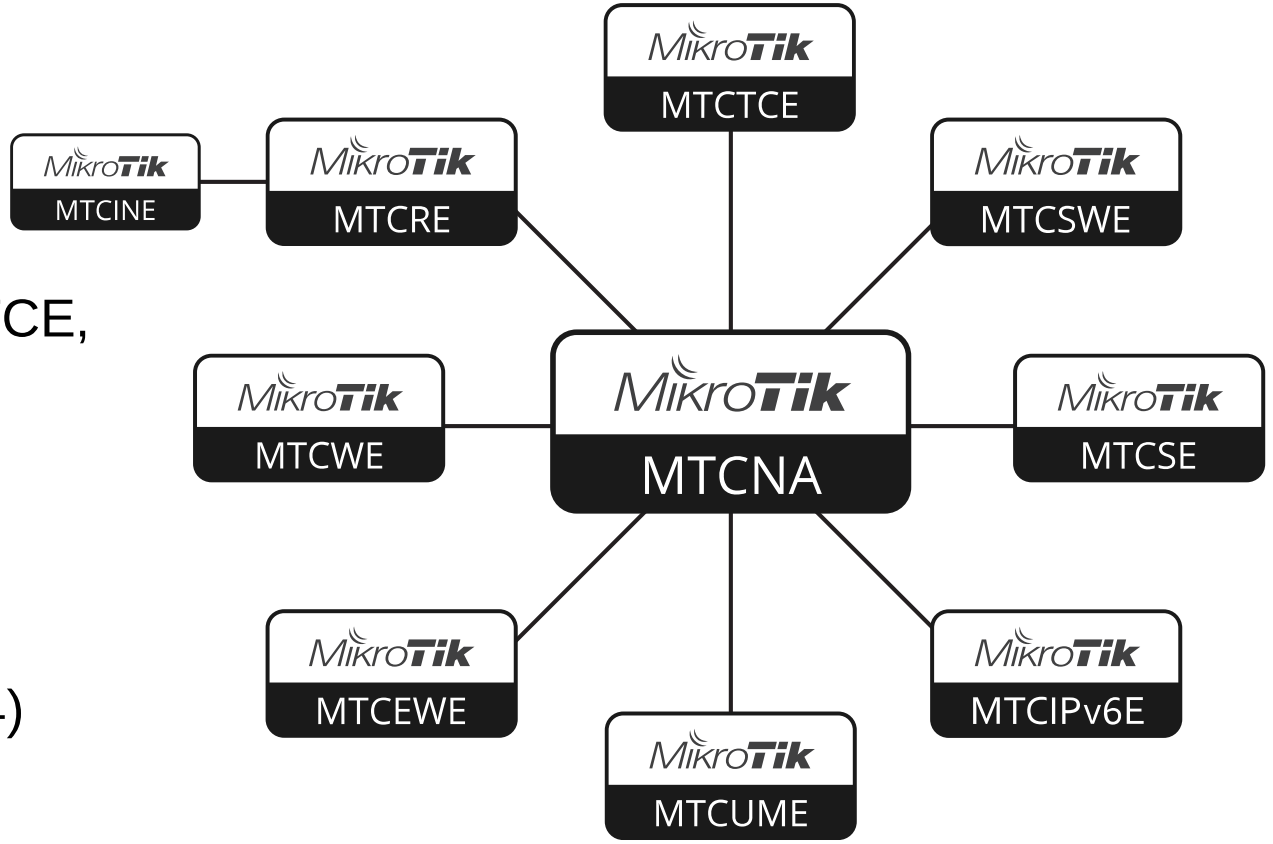
Overview of Layer 2 Security Features

RouterOS 7.18

Me about myself

- Sebastian Inacker
- FMS Internetservice GmbH
- MikroTik Trainer (TR0011)

  MTCNA, MTCRE, MTCWE, MTCTCE, MTCUME, MTCINE, MTCIPv6E, MTCSE, MTCSWE, MTCEWE



- First MTPC 2025 (missed 2024)
- First MikroTik Presentation since 2019

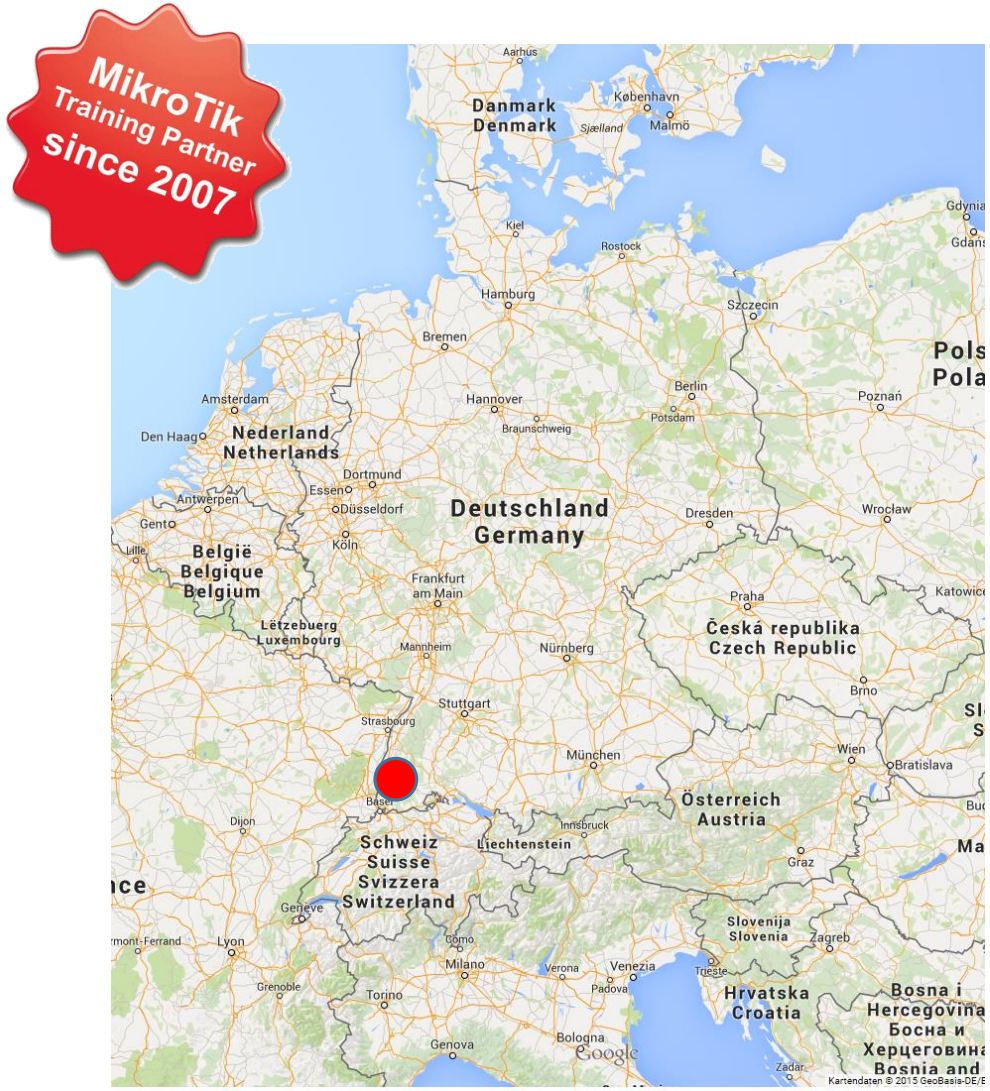
FMS Internetservice GmbH

Value Added Distribution

FMS Internetservice GmbH

- Value Added Distributor
  - Distribution
  - Training
  - Consulting
  - Support

- Founded 1997
- Southwest of Germany



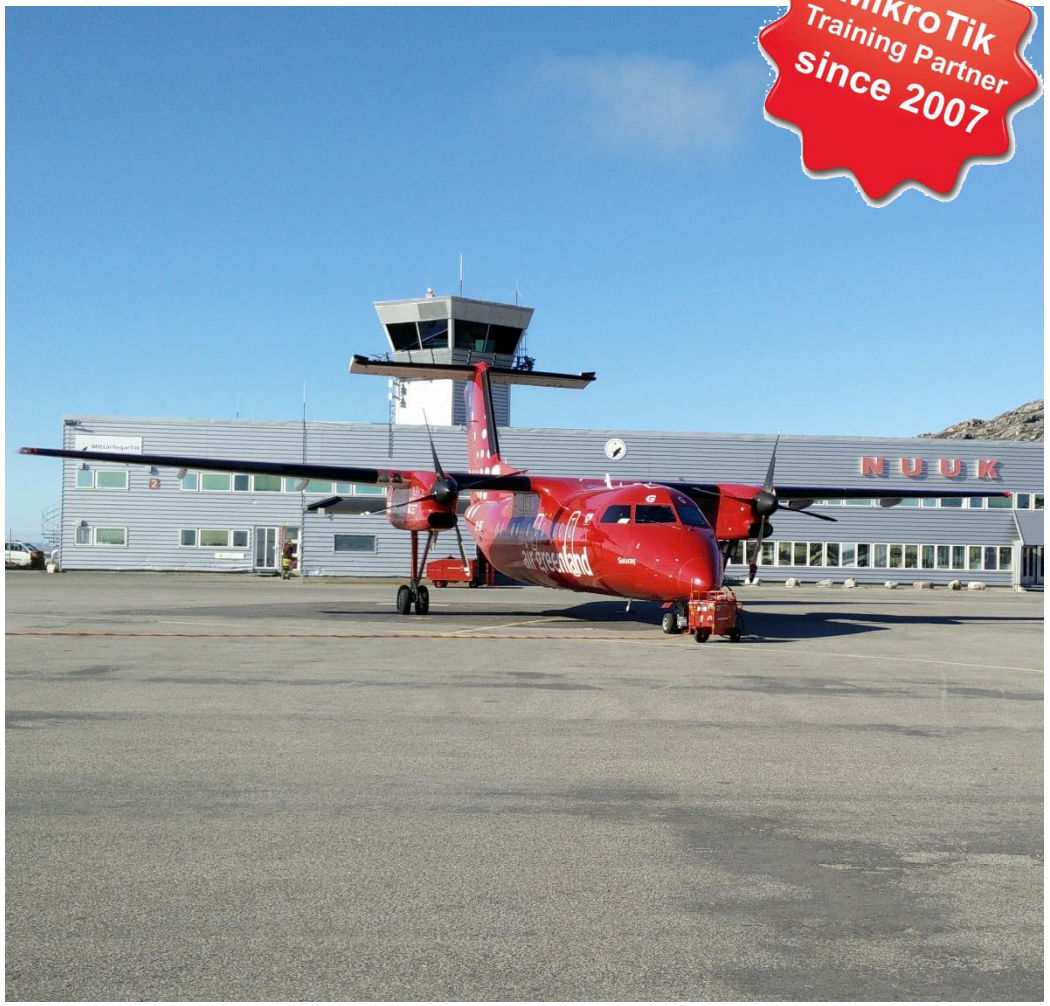
MikroTik Consulting, Support and Projects

- 4 certified MikroTik consultants
- > 60 years of MikroTik experience

- Trainings and workshops:

  3 continents on site - so far
- One personal highlight:

  Nuuk, Greenland



Preface

Preface

- Incomplete Overview (of course)
- *Fast* overview of features with focus on (some) details

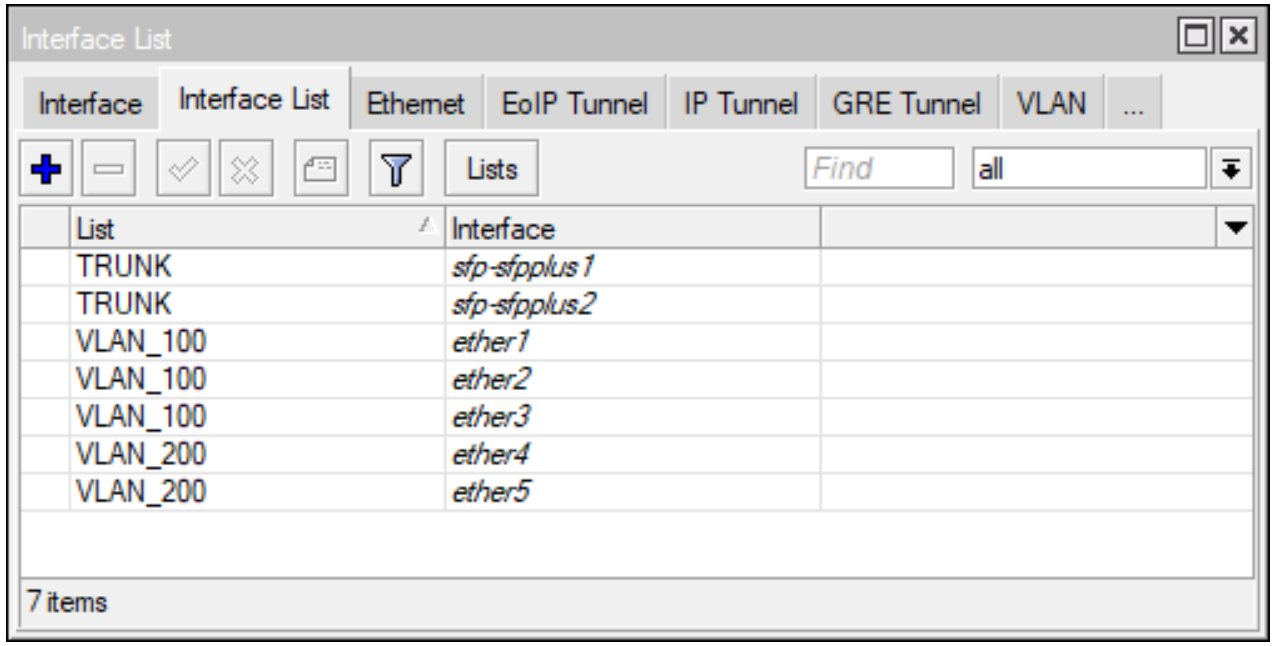
- RouterOS 7.18
- WinBox 3.x
- 2025-03-07

VLAN

Virtual Local Area Network

VLAN

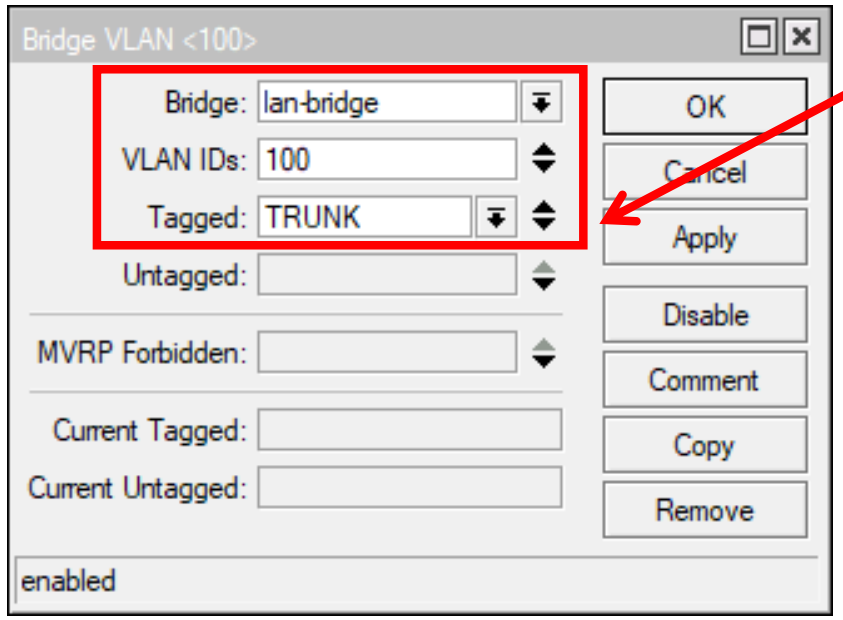
- Since RouterOS 7.17: Interface Lists for Bridge VLAN config
  - Create Interface Lists, for example TRUNK, VLAN_100, VLAN_200, …
  - Assign Interfaces



Interfaces → Interface List

VLAN

- Since RouterOS 7.17: Interface Lists for Bridge VLAN config
  - Use Interface List, not ports at Bridge VLANs

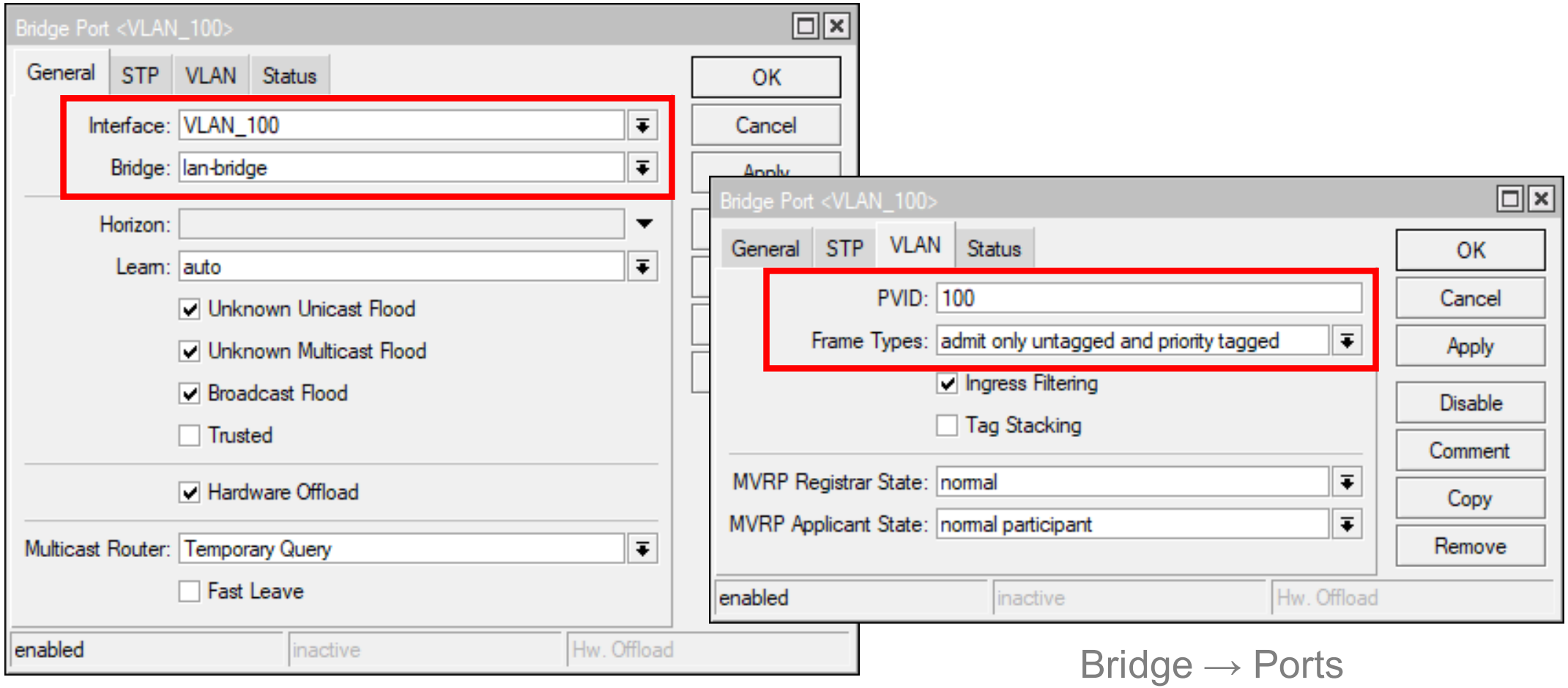


Interface List “TRUNK”

Bridge → VLANs → *VLAN 100*

VLAN

- Since RouterOS 6.41: Interface Lists for Bridge Ports

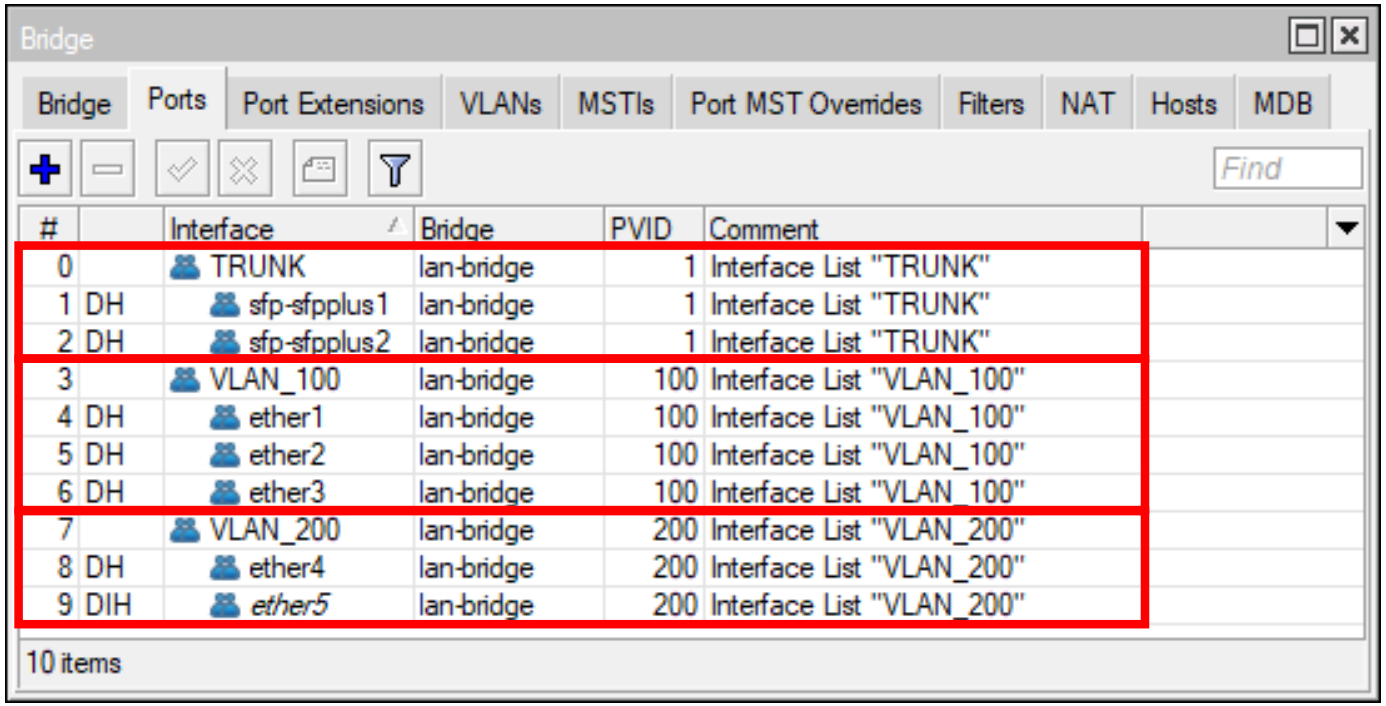


Bridge → Ports

VLAN

- Result…

dynamic, based on Interface List Members



Bridge → Ports

Access Control List (ACL)

Wirespeed filtering

Switch ACL rules

- Filtering at core router might be to late
- Wirespeed, but no statefull filtering (don't drop returning packets)
- With “ports” condition: ACL will match incoming traffic on port(s)
- Number of ACL rules depends on Switch Chip

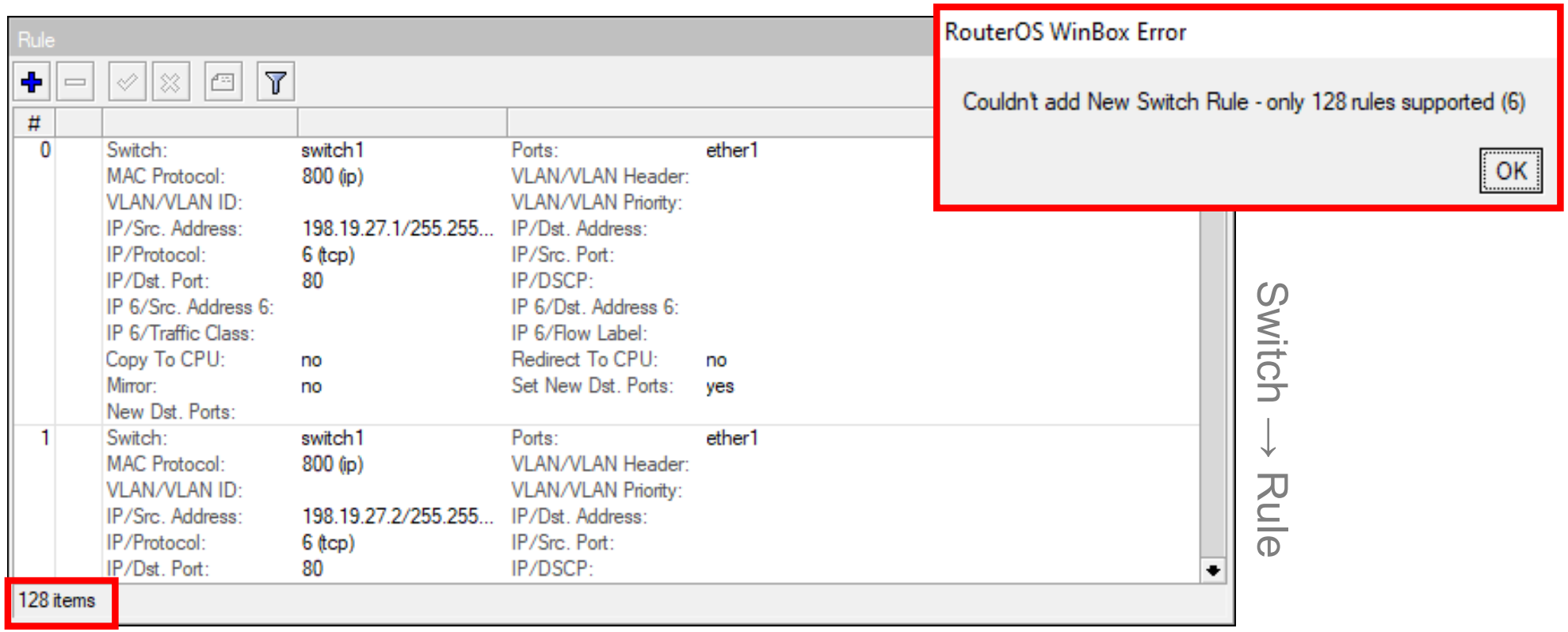
Switch	Switch Chip	ACL Rules
CRS326-24G-2S+	Marvell-98DX3236	128
CRS354-48G-4S+2Q+	Marvell-98DX3257	170
CRS326-24S+2Q+	Marvell-98DX8332	256
CRS520-4XS-16XQ-RM	Marvell-98CX8410	682
CRS510-8XS-2XQ-IN	Marvell-98DX4310	1024

Some examples. Incomplete list

Switch ACL rules

- Example: CRS326-24G-2S+ (Marvell-98DX3236): 128 ACL rules

  (see CRS3xx, CRS5xx, CCR2116, CCR2216 switch chip features)



Example ACL

- Allow only web access from specific ports

  (don't forget DHCP, DNS, ARP, …)

```
/interface ethernet switch rule
add comment="Allow HTTPS" mac-protocol=ip protocol=tcp dst-port=443 \
   ports="ether1,ether2,ether3,ether4,ether5"
add comment="Allow HTTP" mac-protocol=ip protocol=tcp dst-port=80 \
   ports="ether1,ether2,ether3,ether4,ether5"
add comment="Allow DNS" dst-port=53 mac-protocol=ip protocol=udp ports=ether1,ether2,ether3,ether4,ether5
add comment="Allow DHCP" mac-protocol=ip protocol=udp src-port=68 dst-port=67 \
   ports=ether1,ether2,ether3,ether4,ether5
add comment="Allow ARP" mac-protocol=arp ports=ether1,ether2,ether3,ether4,ether5
add comment="DROP all others" new-dst-ports="" \
   ports="ether1,ether2,ether3,ether4,ether5"
```

Example ACL

- Allow PPPoE from specific vendor and send rest to different VLAN

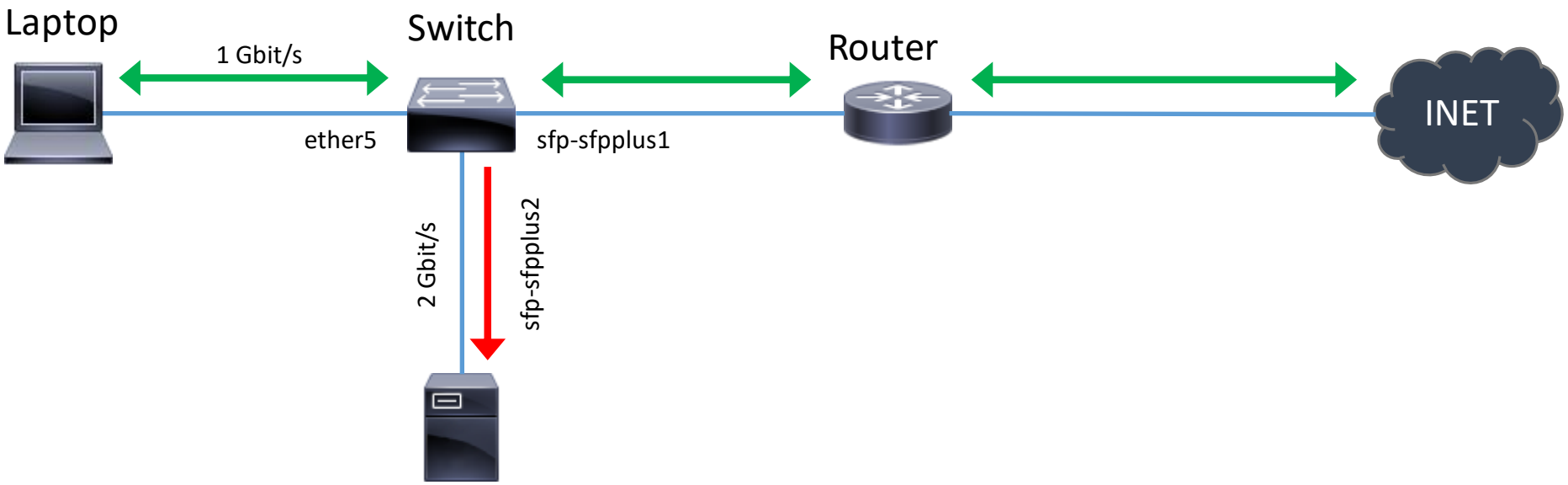
```
/interface ethernet switch rule
add src-mac-address=00:0C:42:00:00:00/FF:FF:FF:00:00:00 \
    mac-protocol=pppoe \
    ports="ether1,ether2,ether3,ether4,ether5"
add src-mac-address=00:0C:42:00:00:00/FF:FF:FF:00:00:00 \
    mac-protocol=pppoe-discovery \
    ports="ether1,ether2,ether3,ether4,ether5"
add new-vlan-id=200 ports="ether1,ether2,ether3,ether4,ether5“
```

MikroTik MAC-Addresses (German): https://wiki.fmsweb.de/mikrotik/infos/routerboard-oui

Port Mirroring

Port Mirroring

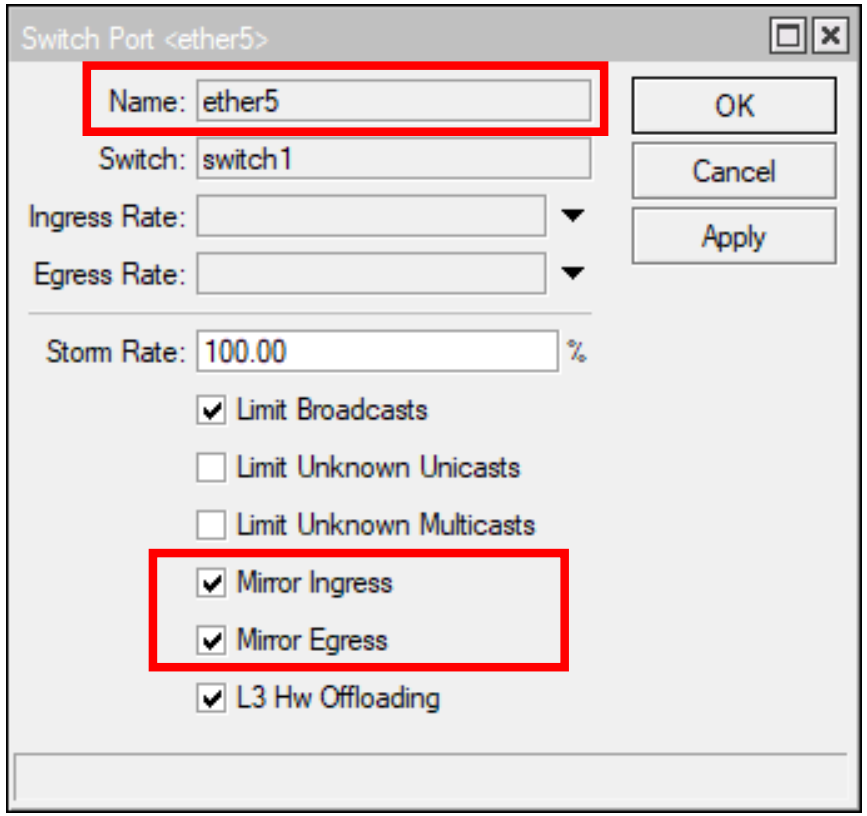
Mirroring traffic of interface…



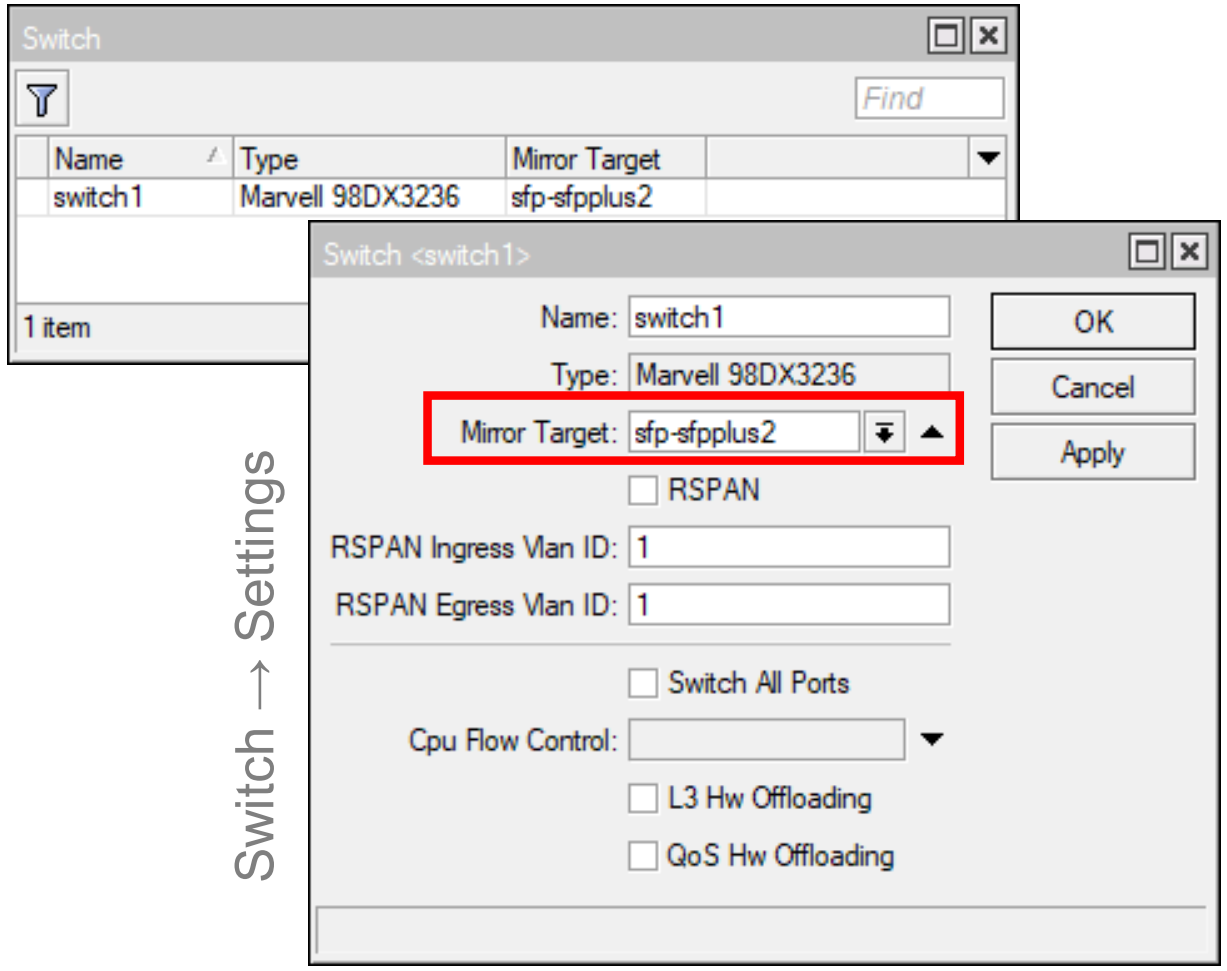
Monitoring Server
(Intrusion Detection System)

Port Mirroring

Mirror ether5 → sfp-sfpplus2 (same Switch Chip)



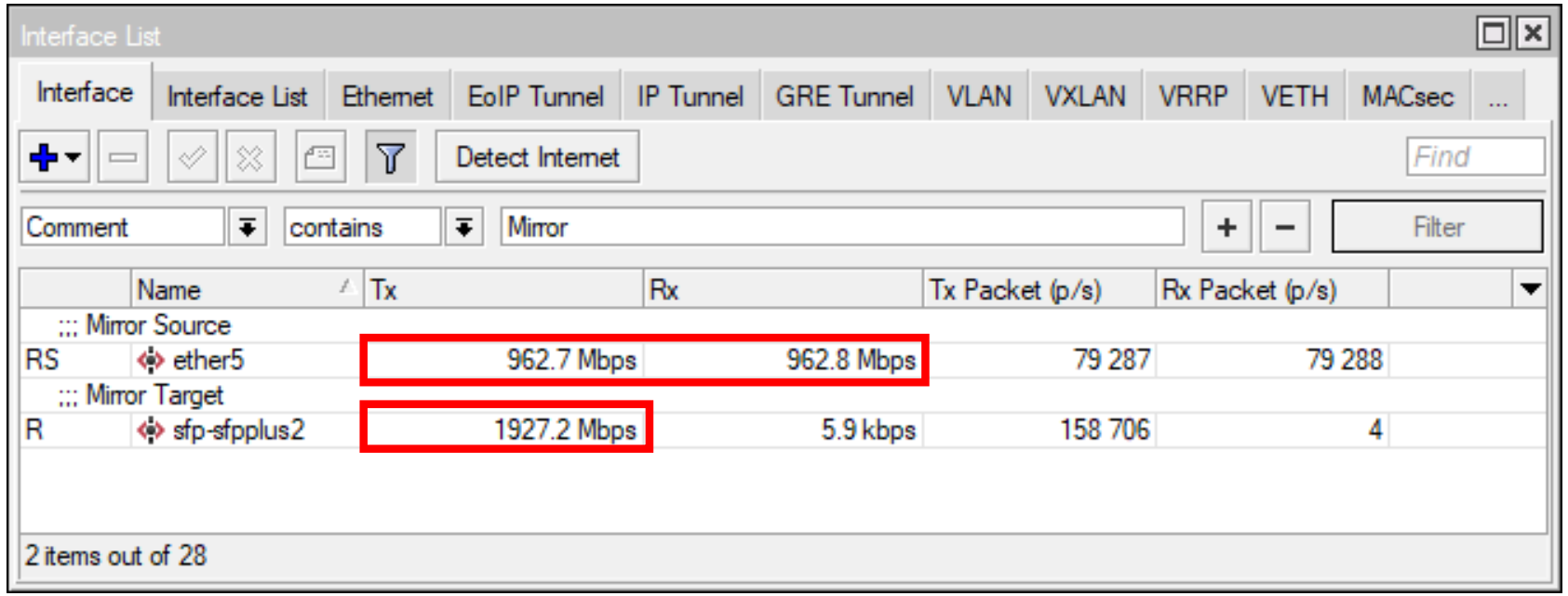
Switch → Ports



Switch → Settings

Port Mirroring

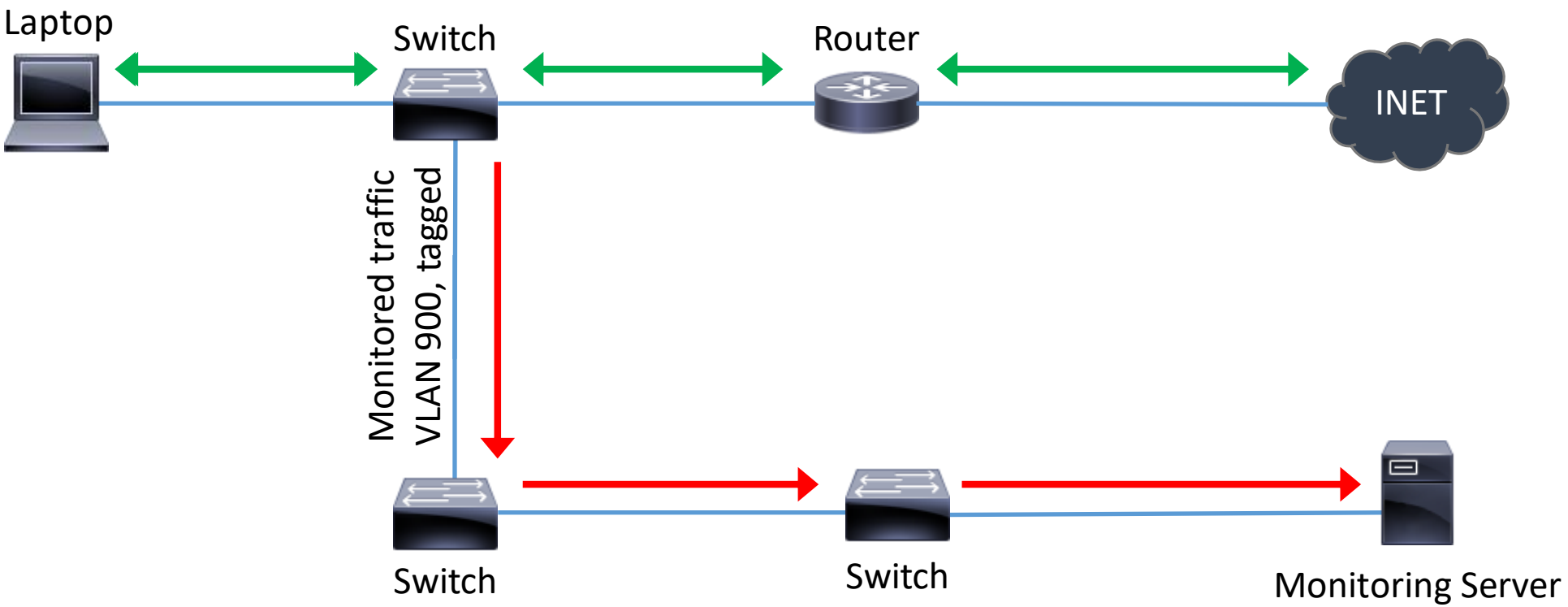
Interfaces



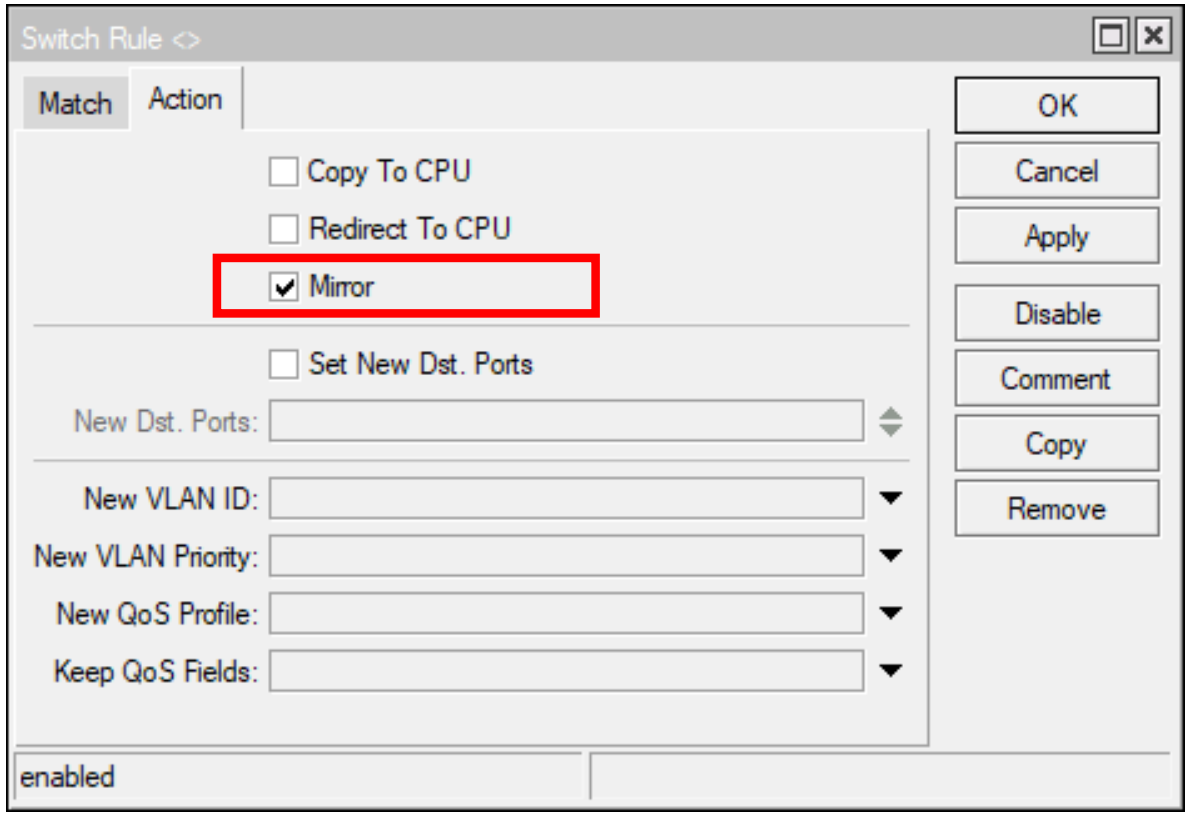
Can you handle 2 Gbit/s?

Port Mirroring

Mirrored traffic: VLAN tagged through the net…



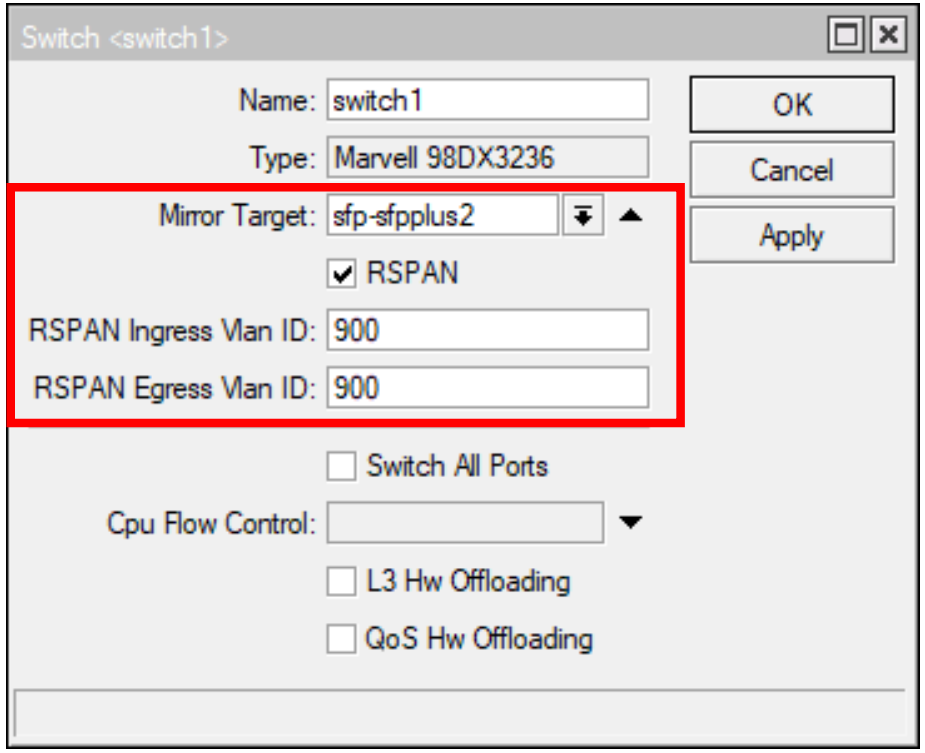
Mirroring with ACL filtering & RSPAN



Switch → Rule → Action

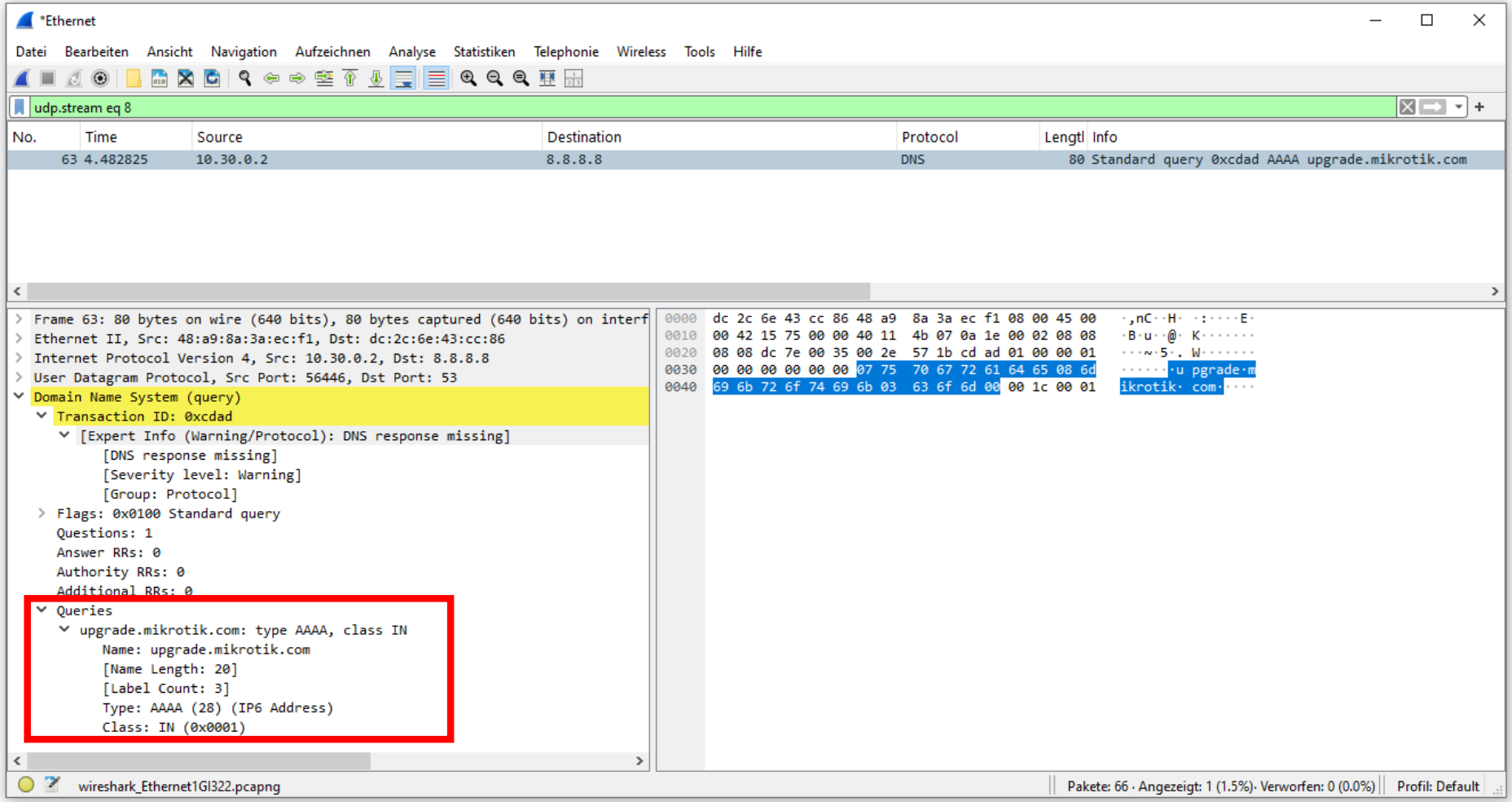
RSPAN = Remote Switched Port Analyzer

Switch → Settings



Mirroring with ACL filtering

Filtered to DNS requests from client



WireGuard and VXLAN

Secure Layer 2 around the world

WireGuard and VXLAN

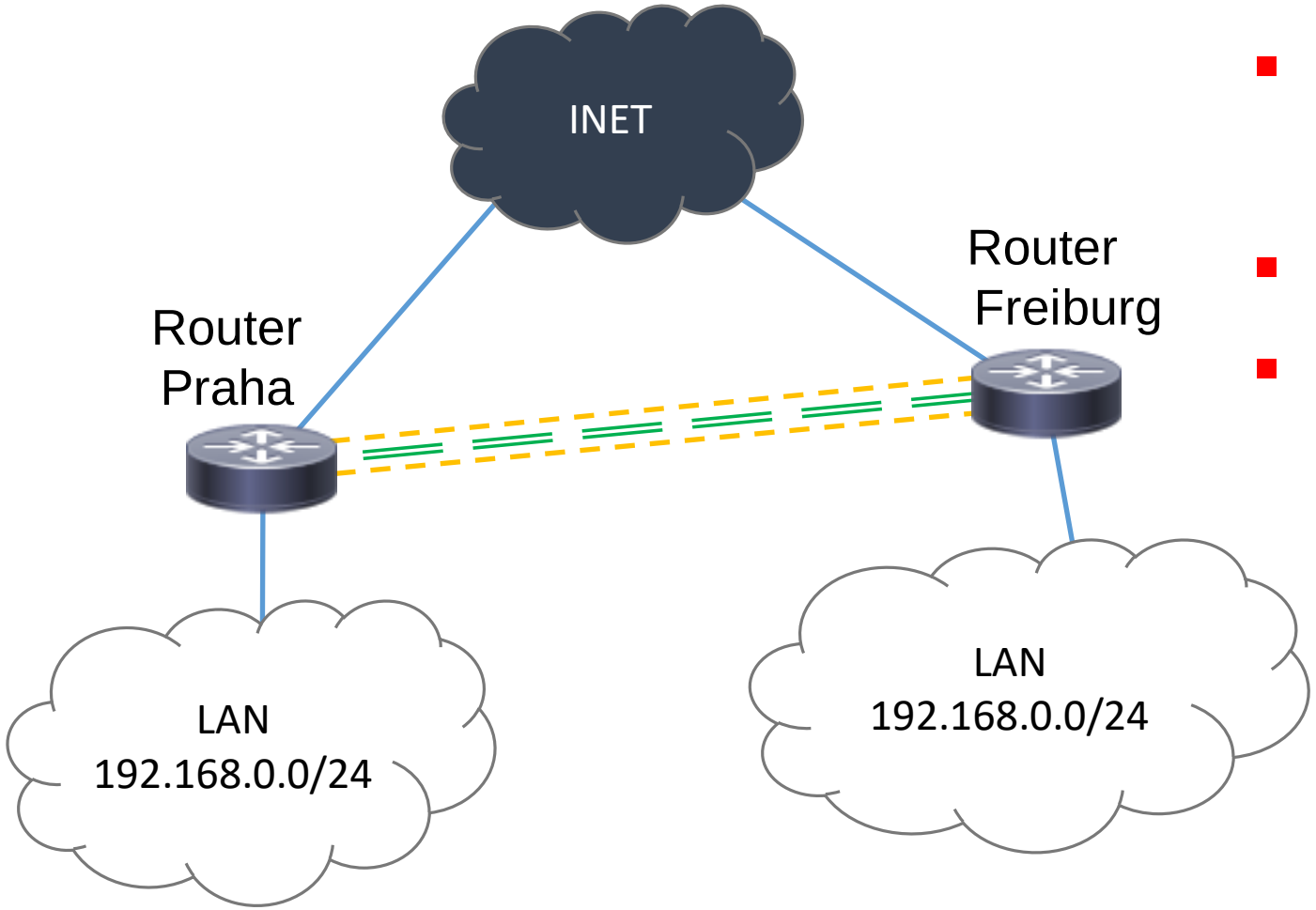
WireGuard

- A modern VPN (Not in scope of this presentation)

VXLAN (Virtual eXtensible Local Area Network)

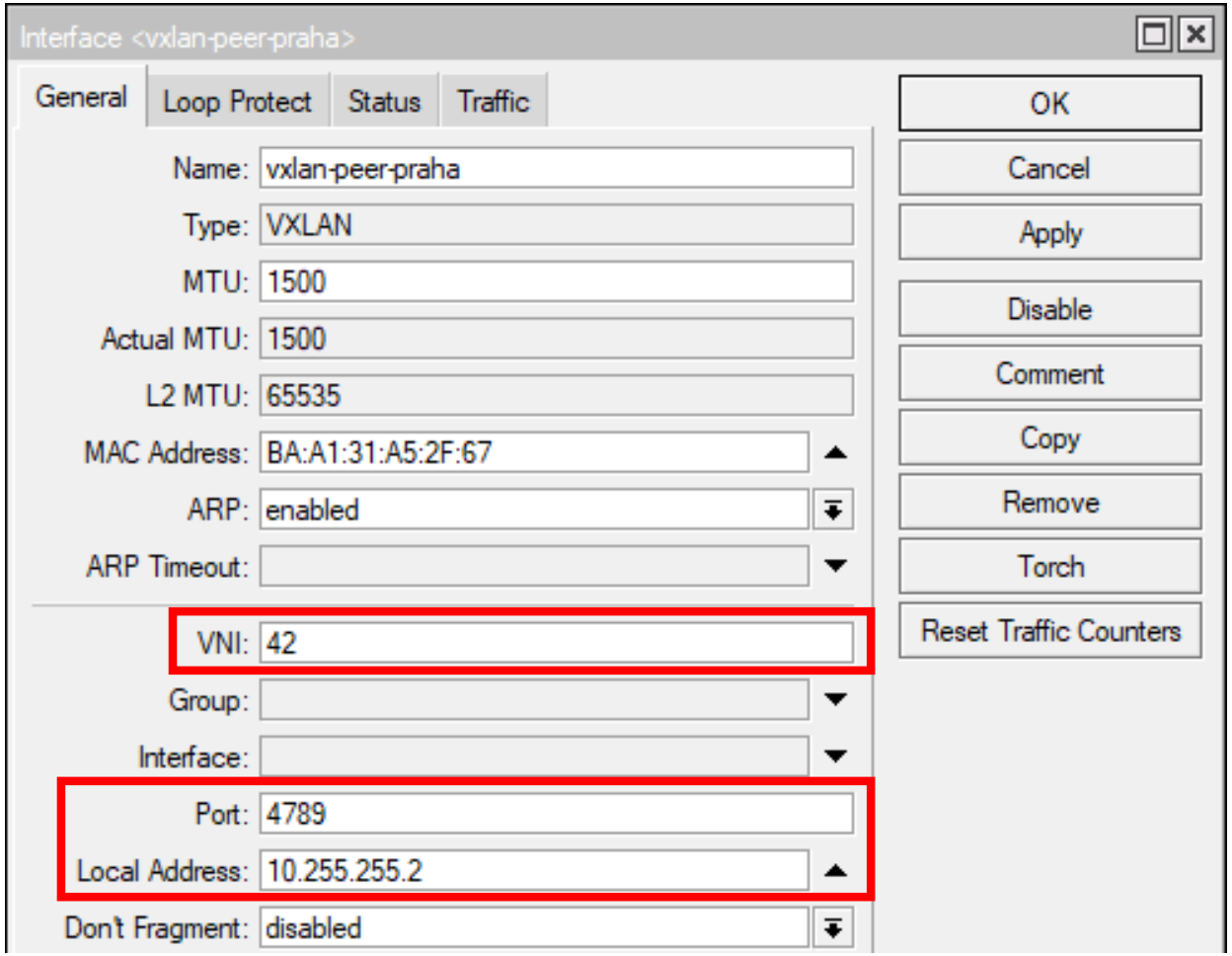
- Layer 2 tunnel, routed via IPv4 or IPv6, UDP
- Expands 2^{12} = 4096 VLAN IDs to 2^{24} = 16.777.216 IDs

WireGuard and VXLAN



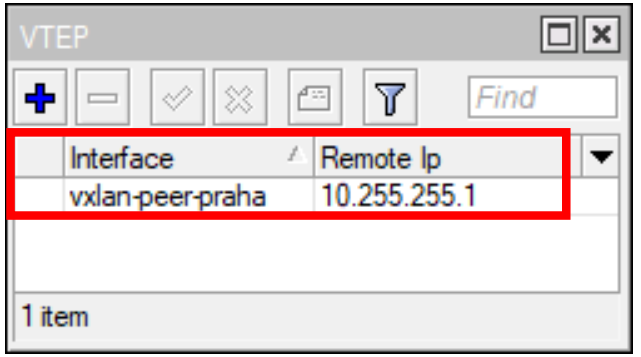
- WireGuard tunnel between Praha and Freiburg
- VXLAN on top of WireGuard
- VXLAN bridged with LAN interface

VXLAN



Interfaces → VXLAN

- VNI: VXLAN Network Identifier
- Port: UDP Port (rx/tx)
- Local Address: Source address, address of *wireguard* interface
- Remote Address: Address of remote *wireguard* interface



Interfaces → VXLAN → VTEP

WireGuard and VXLAN

Bandwidth test through VXLAN via WireGuard.

1 minute, average results (rounded)

	tx (TCP)	rx (TCP)
hEX refresh	100 Mbps	80 Mbps
hAP ax²	145 Mbps	200 Mbps
RB5009	320 Mbps	380 Mbps

```
/tool/bandwidth-test user=admin password=admin
      direction=both protocol=tcp address=192.168.0.1
      duration=60 connection-count=20
```

Hardware offloaded VXLAN

- *Initial* HW support for VXLAN is available since 7.18beta.
- Not supported (yet):
  - VLAN tagging over VXLAN - one vxlan interface for each local VLAN
  - VTEPs (VXLAN tunnel endpoints) on VRF, IPv6, VLAN, …
  - …

Currently supported Devices (Switch chips 98DX8*xxx*, 98DX4*xxx*, 98DX325*x*)

CCR2116-12G-4S+, CCR2216-1G-12XS-2XQ,

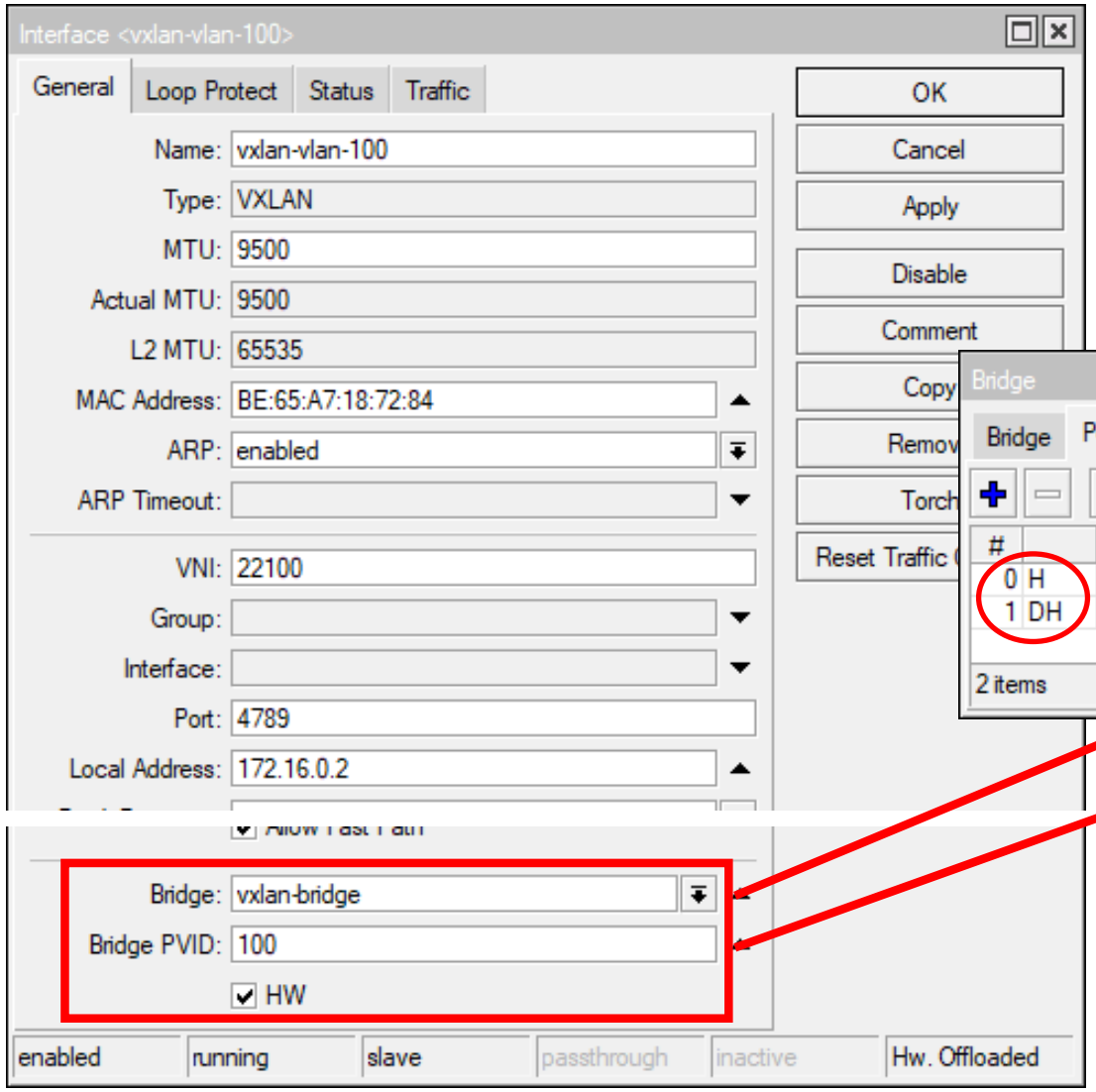
CRS309-1G-8S+, CRS312-4C+8XG, CRS317-1G-16S+, CRS326-24S+2Q+,

CRS326-4C+20G+2Q+, CRS354-48G-4S+2Q+, CRS354-48P-4S+2Q+,

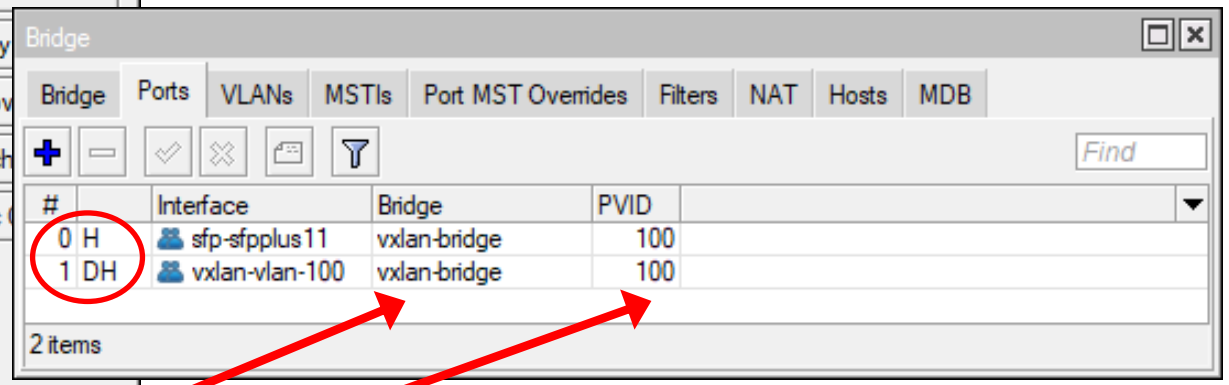
CRS504-4XQ, CRS510-8XS-2XQ, CRS518-16XS-2XQ, CRS520-4XS-16XQ-RM

Hardware offloaded VXLAN

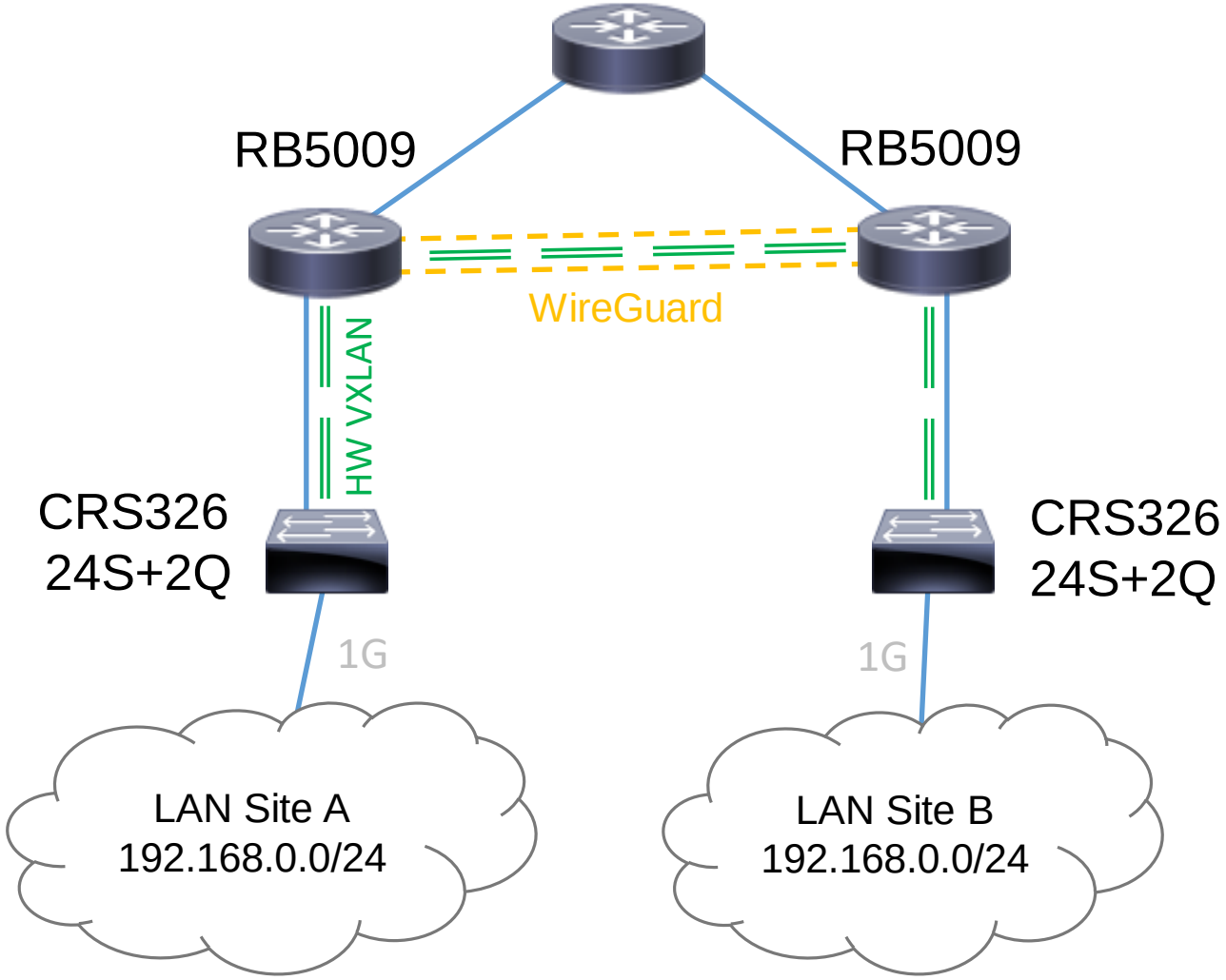
Interfaces → VXLAN



Bridge → Ports



WireGuard and HW VXLAN



With increased MTU

tx (TCP)	rx (TCP)
940 Mbps	930 Mbps

Test from devices behind CRS326.
Connected by 1G interface.

MACsec

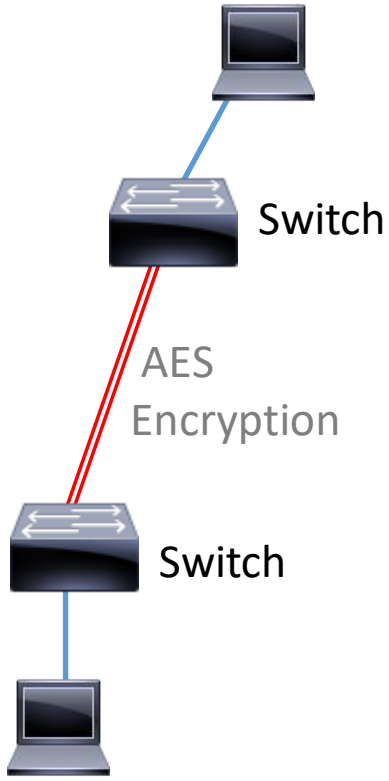
Feature and hardware limitations

MACsec

- MACsec (Media Access Control Security), IEEE standard 802.1AE
- Encryption over Ethernet → HTTP, ARP, DNS, …

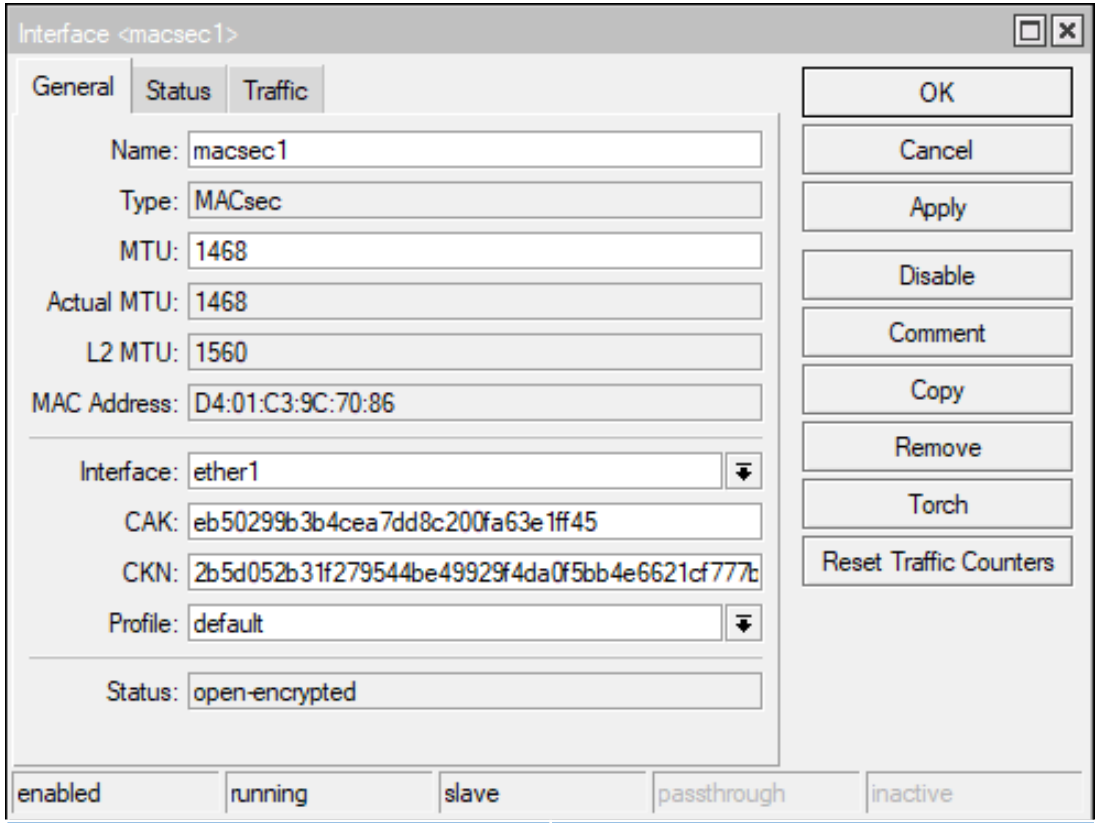
Current situation on RouterOS

- “early stage”
- No HW support (!)
  - MikroTik: Use devices with powerfull CPU
- MACsec interface can be handled as other interfaces (routing, bridging)



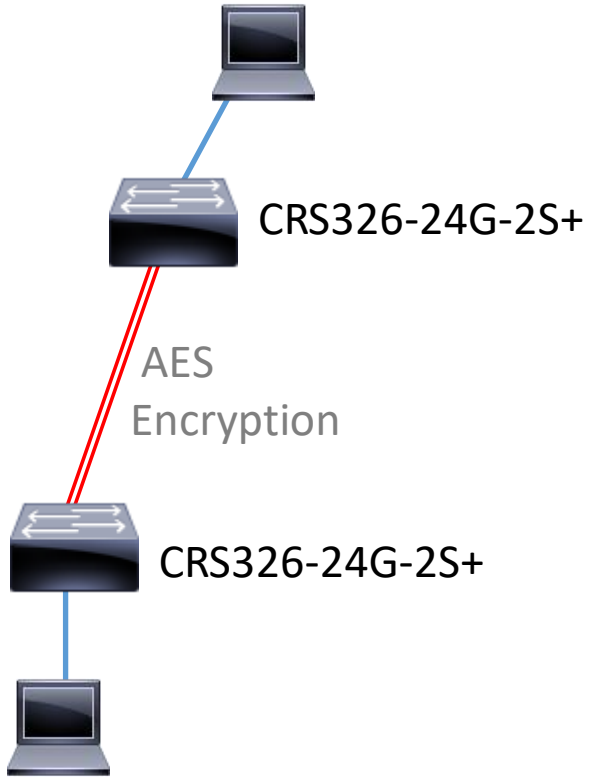
MACsec, CRS326

Interfaces → MACsec



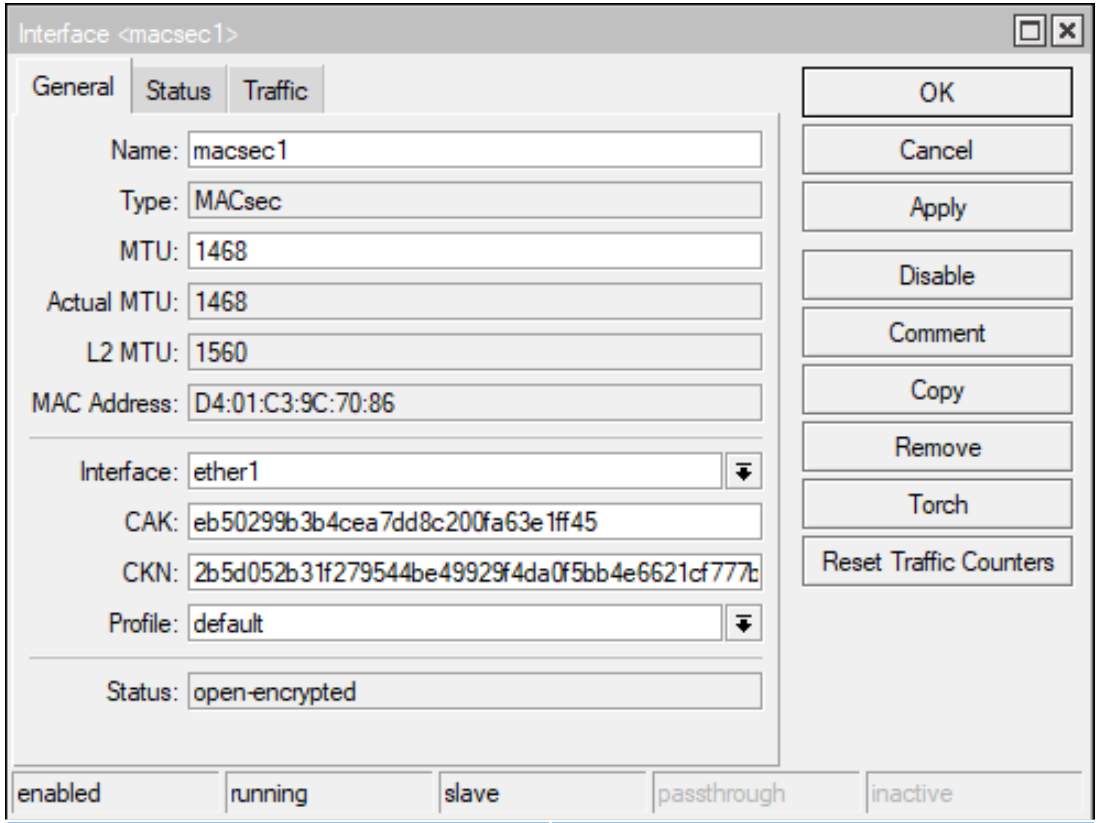
tx (TCP)	rx (TCP)
15 Mbps	50 Mbps

CRS326 is wrong device for MACsec

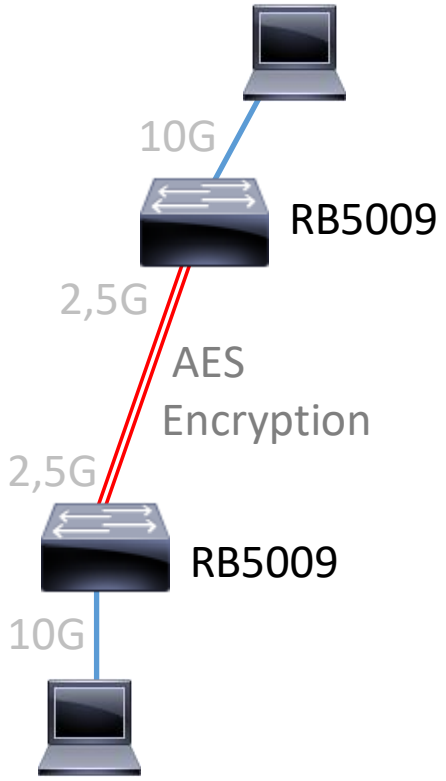


MACsec, RB5009

Interfaces → MACsec



tx (TCP)	rx (TCP)
890 Mbps	1030 Mbps
No benefit from larger MACsec MTU	



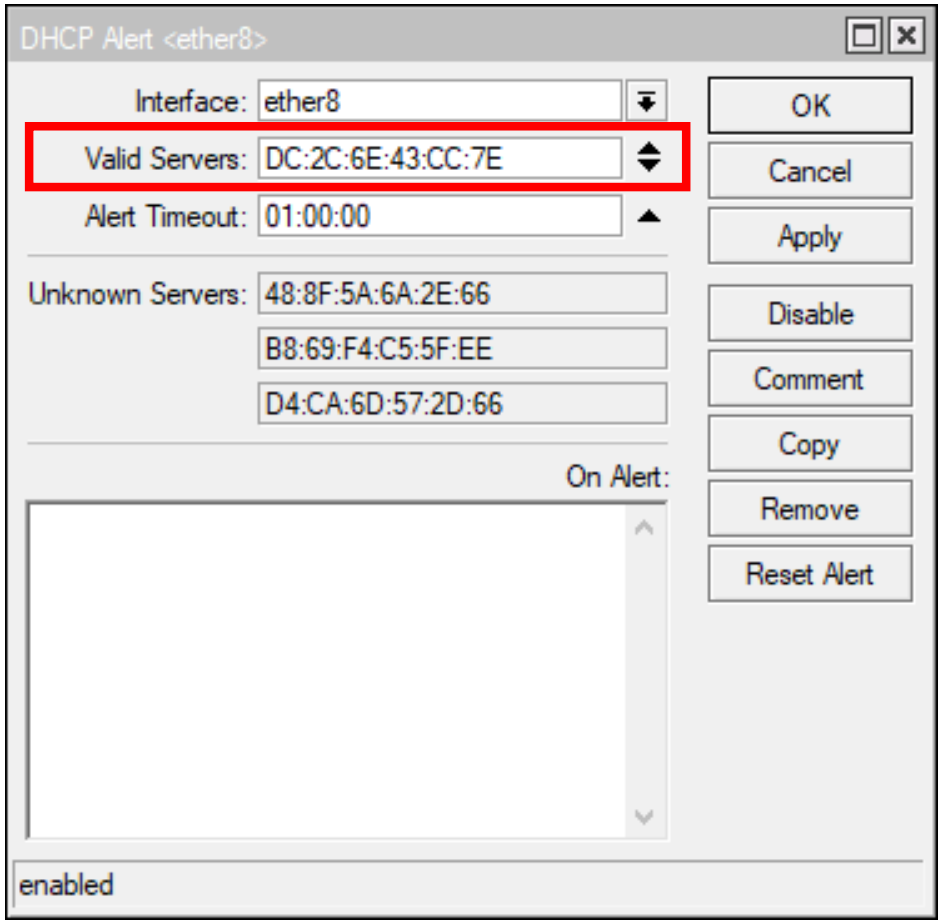
Restrictions for local user communication

DHCP snooping

- You don’t want DHCP-servers on end-user ports

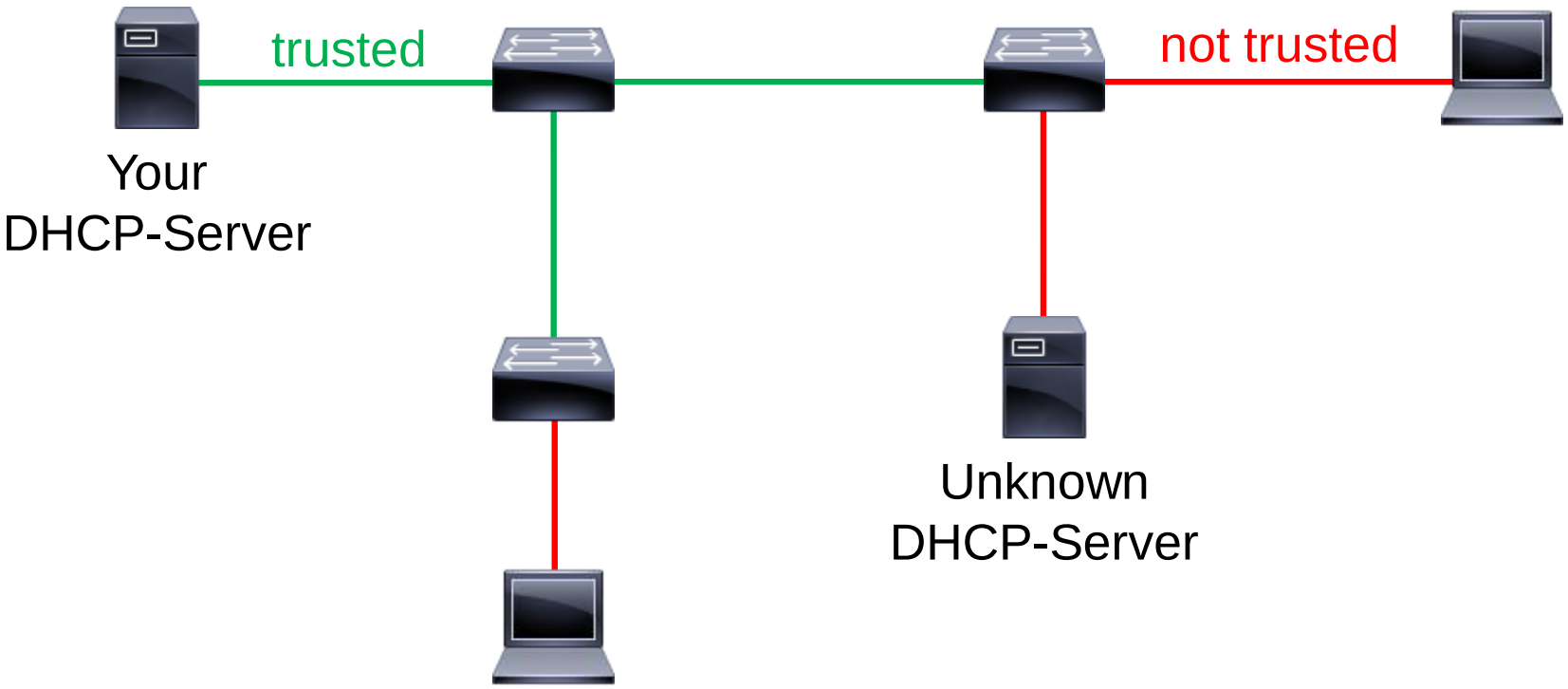
Detection: DHCP Alert

```
2025-02-29 12:05:10 dhcp,critical,error
    dhcp alert on ether8: discovered unknown
    dhcp server, mac D4:CA:6D:57:2D:66,
    ip 198.19.27.254
```



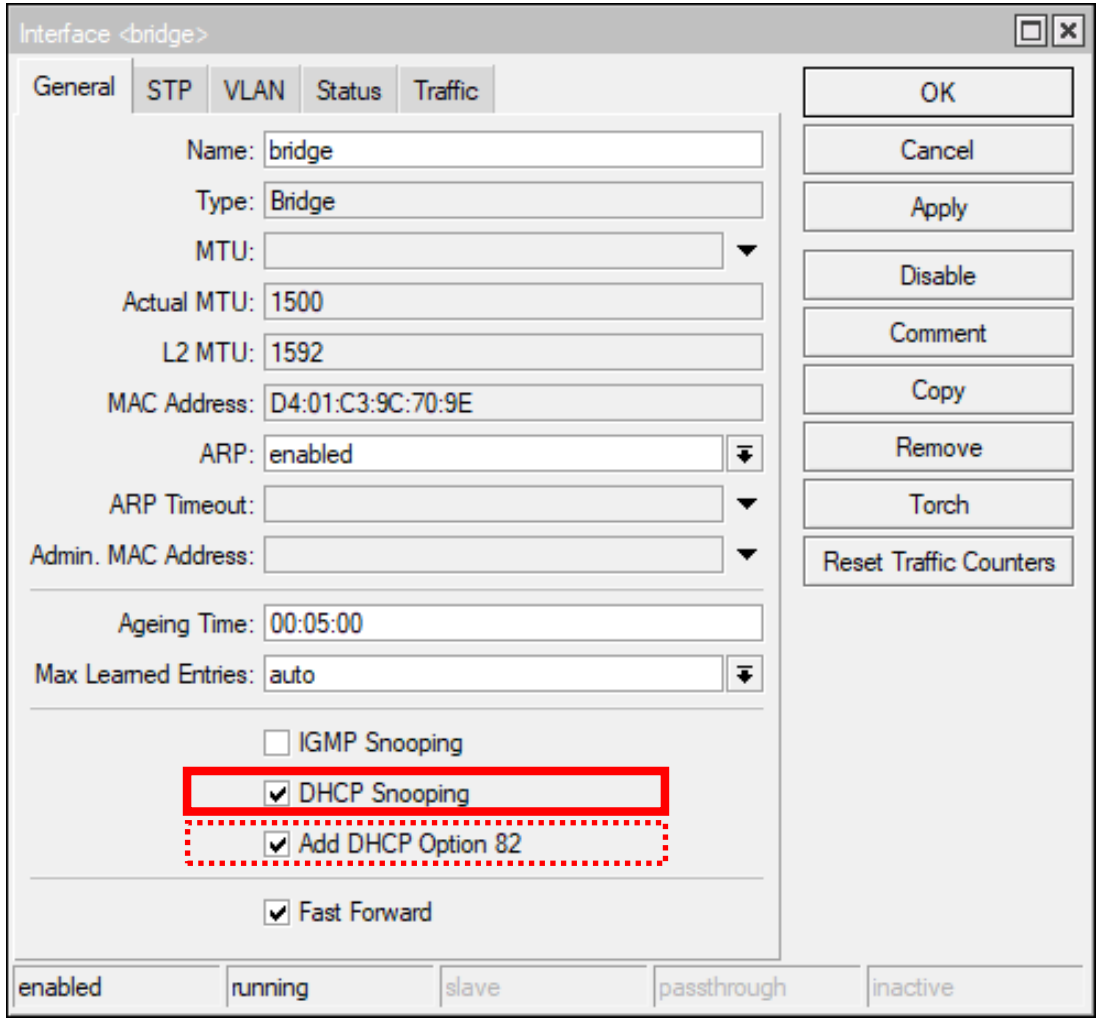
IP → DHCP-Server → Alerts

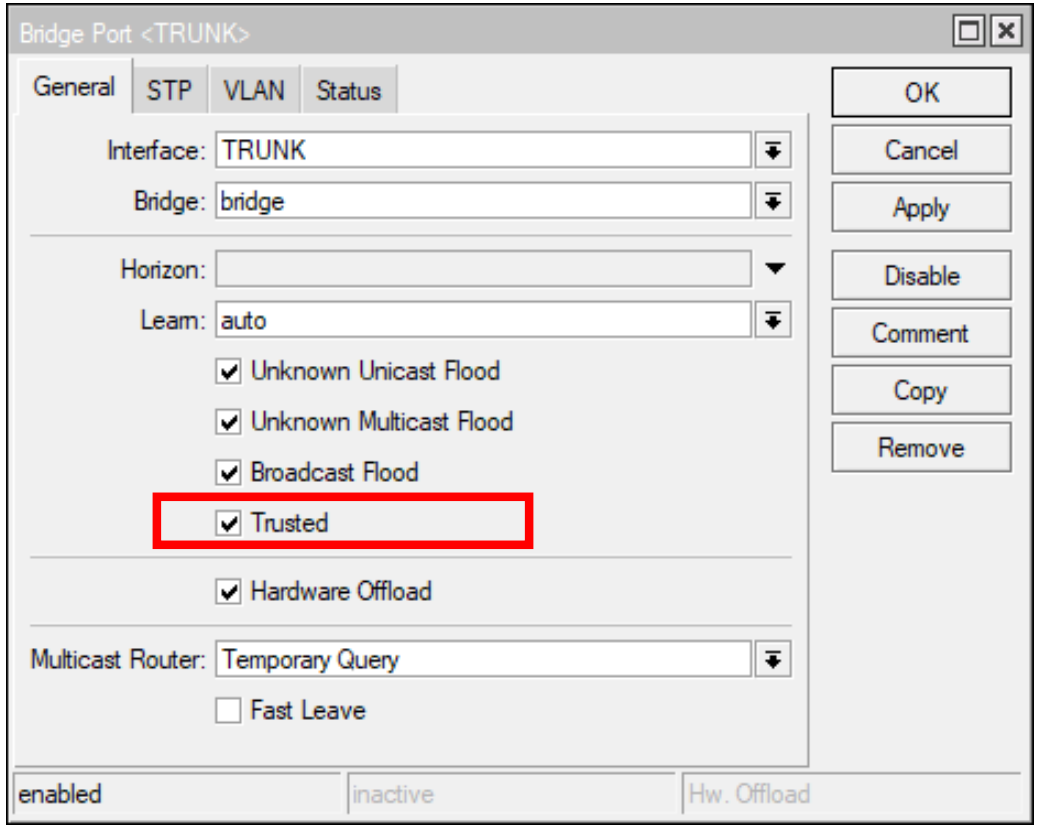
DHCP snooping



DHCP snooping

Bridge → Bridge



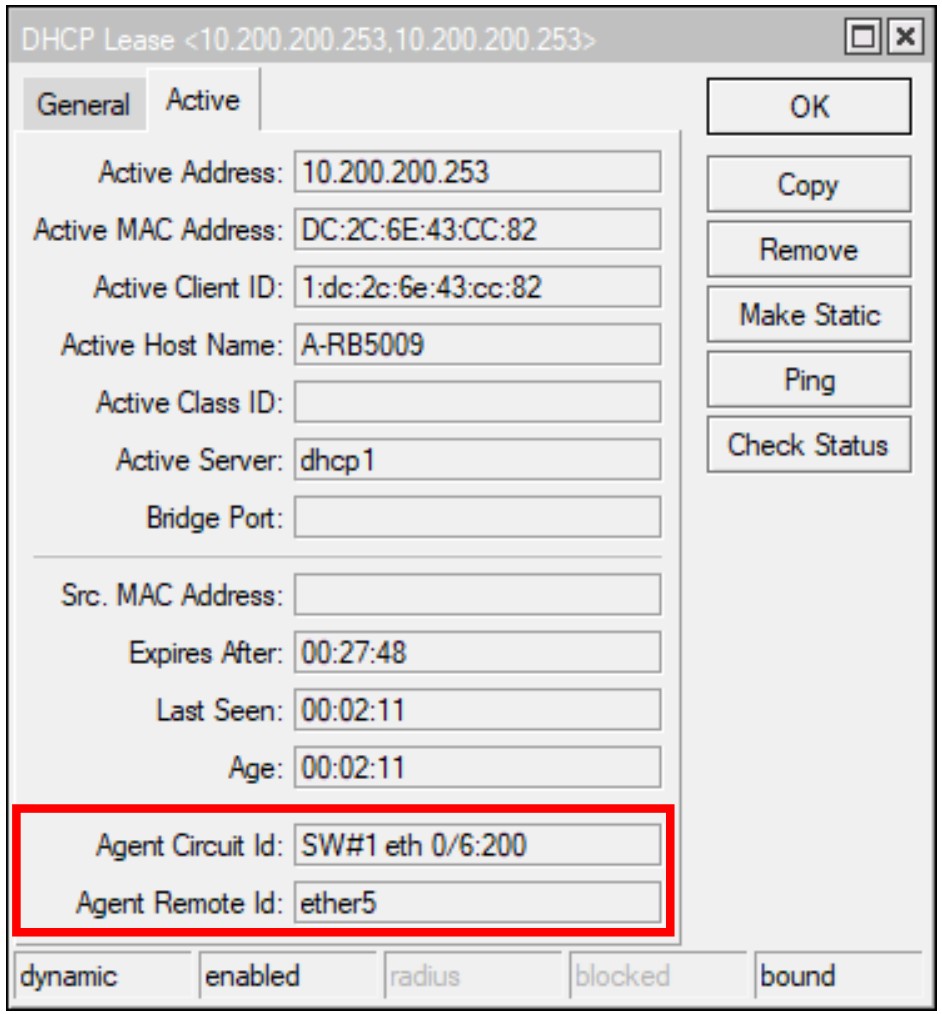


Bridge → Port

DHCP snooping will create dynamic ACL rule for udp/67-68

DHCP snooping and DHCP Option 82

IP → DHCP-Server → Lease



Info available on DHCP-Server

- Agent Circuit Id:

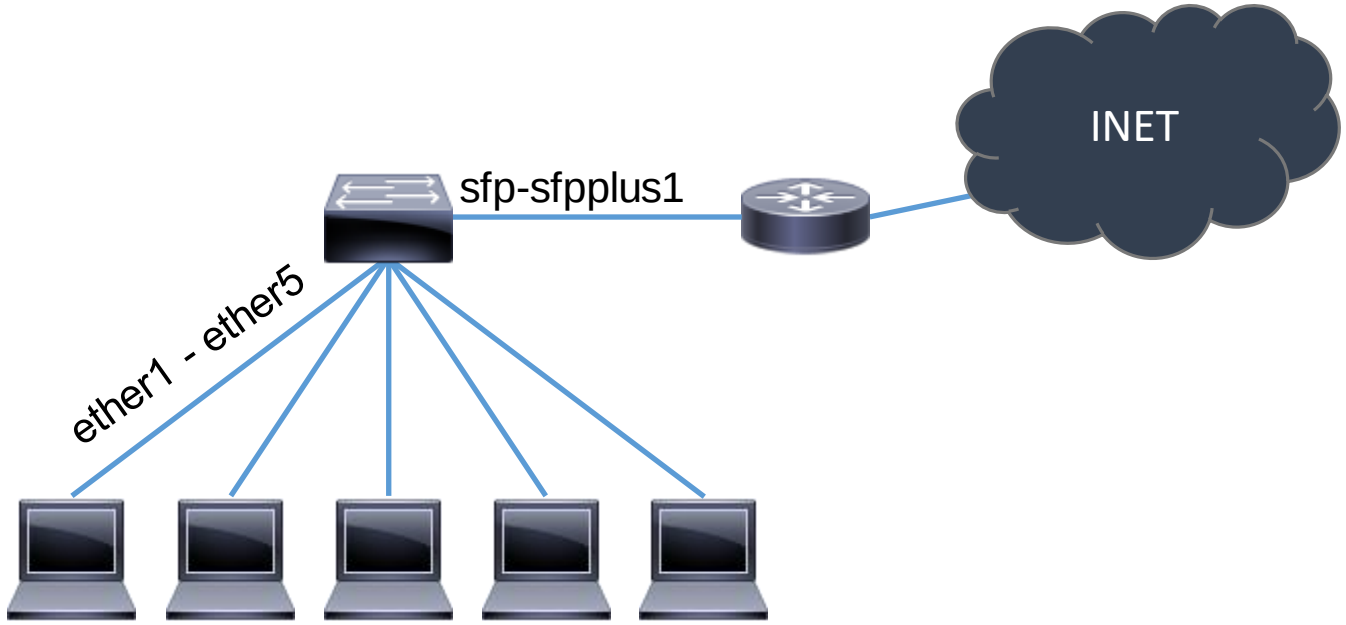
  DHCP-Client is connected to switch “SW#01” on VLAN 200
- Agent Remote Id:

  Client is connected to switch port ether5

At the moment: Only informational.

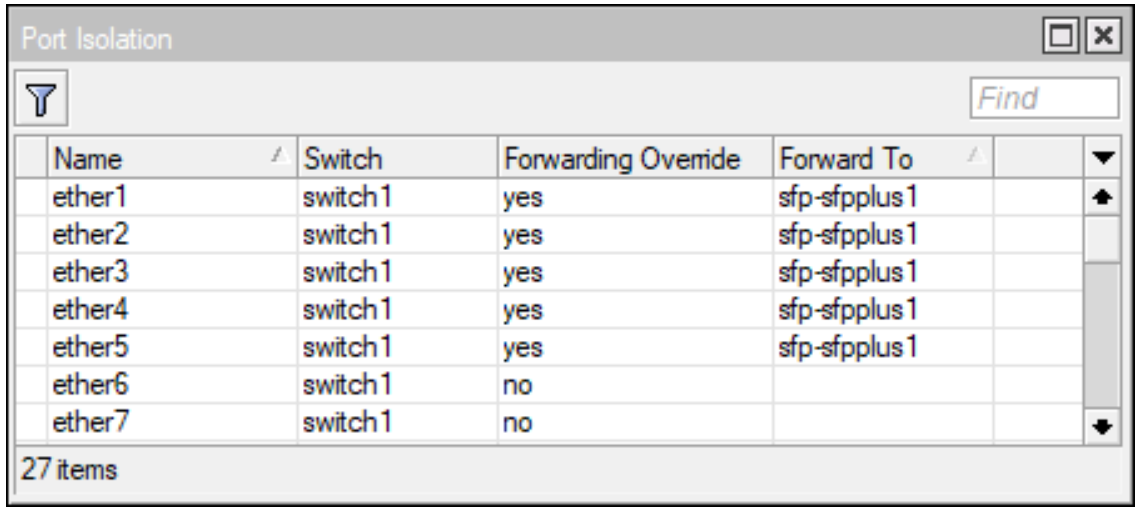
Port isolation

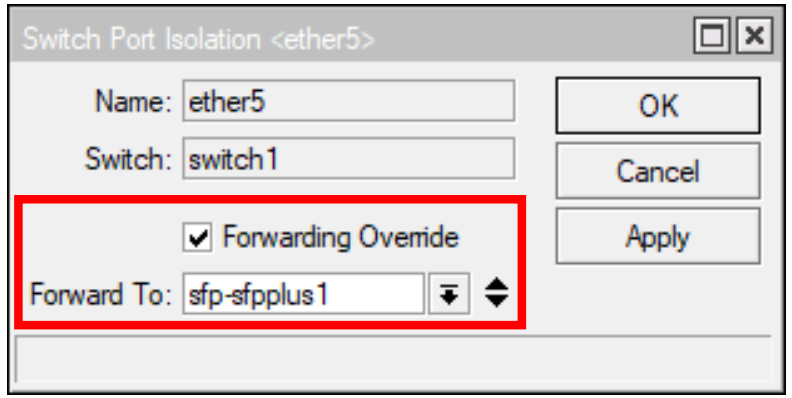
- You might not want layer2 between end-users
  - WiFi with client isolation
  - ISP customers
  - Hotel, …



Port isolation

Switch → Port Isolation





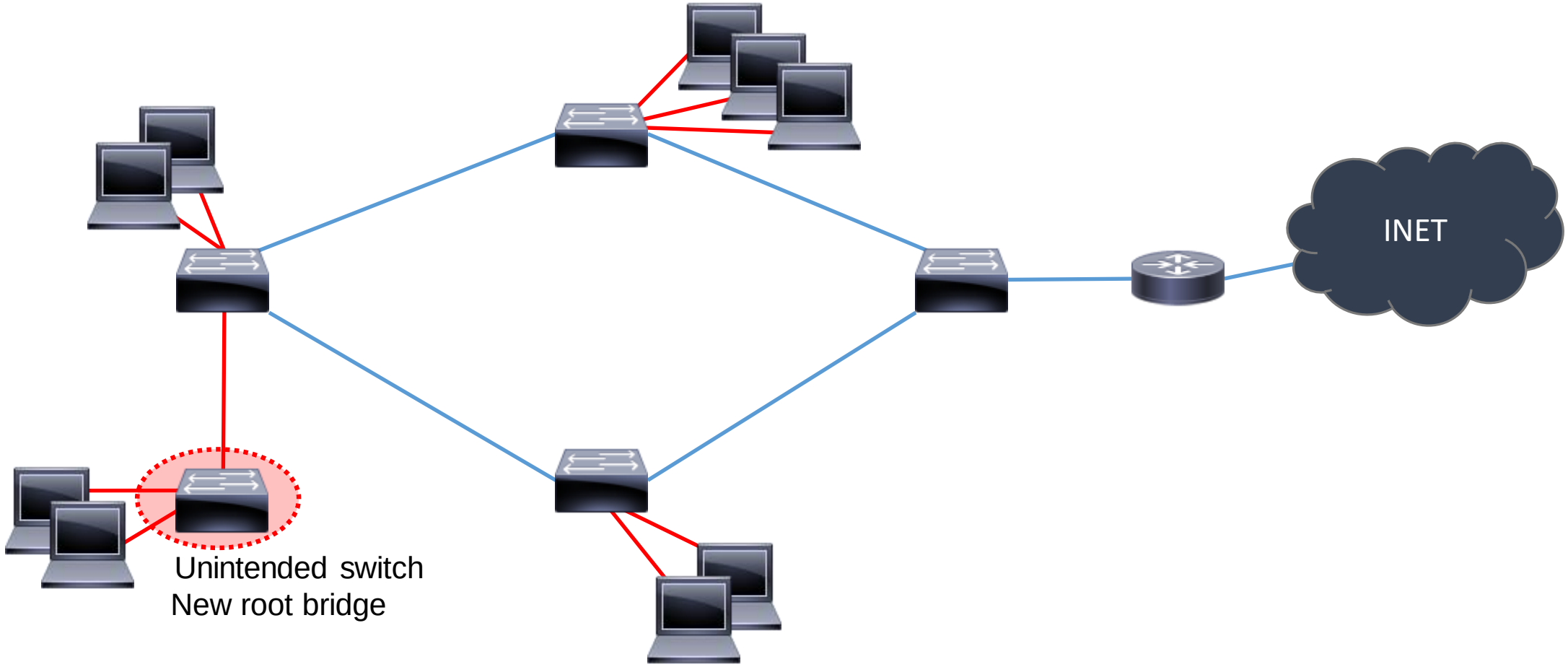
- Forwarding Override:

  Force incoming traffic to one/more outgoing interfaces
- Forward To:

  Outgoing interface(s)

Users connecting devices

- You don’t want “unknown” switches on end-user ports



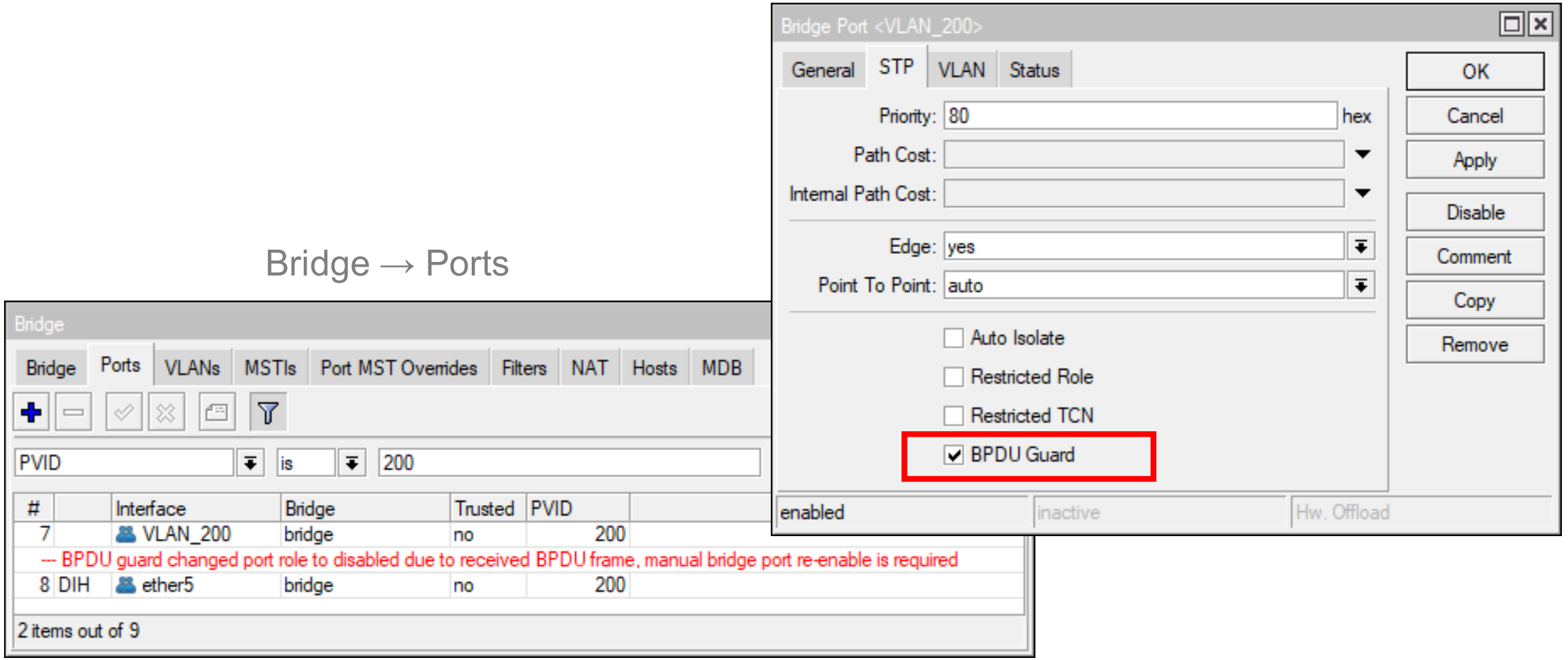
BPDU guard

BPDU (Bridge Protocol Data Unit): Used in *x*STP networks

- An “edge port” will not send BPDUs and ignore received BPDUs
- BPDU guard will *disable* affected port
  - Port (or Interface List) have to be re-enabled by you
  - You can talk to responsible person

BPDU guard

Bridge → Ports




```
2025-02-29 15:33:53 bridge,stp,warning bpdu-guard disabling ether5 due to received bpdu
```

Thank You

+49 761 2926500 | sales@fmsweb.de | Web form

www.fmsweb.de | www.mikrotik-shop.de