



Overview of Layer 2 Security Features

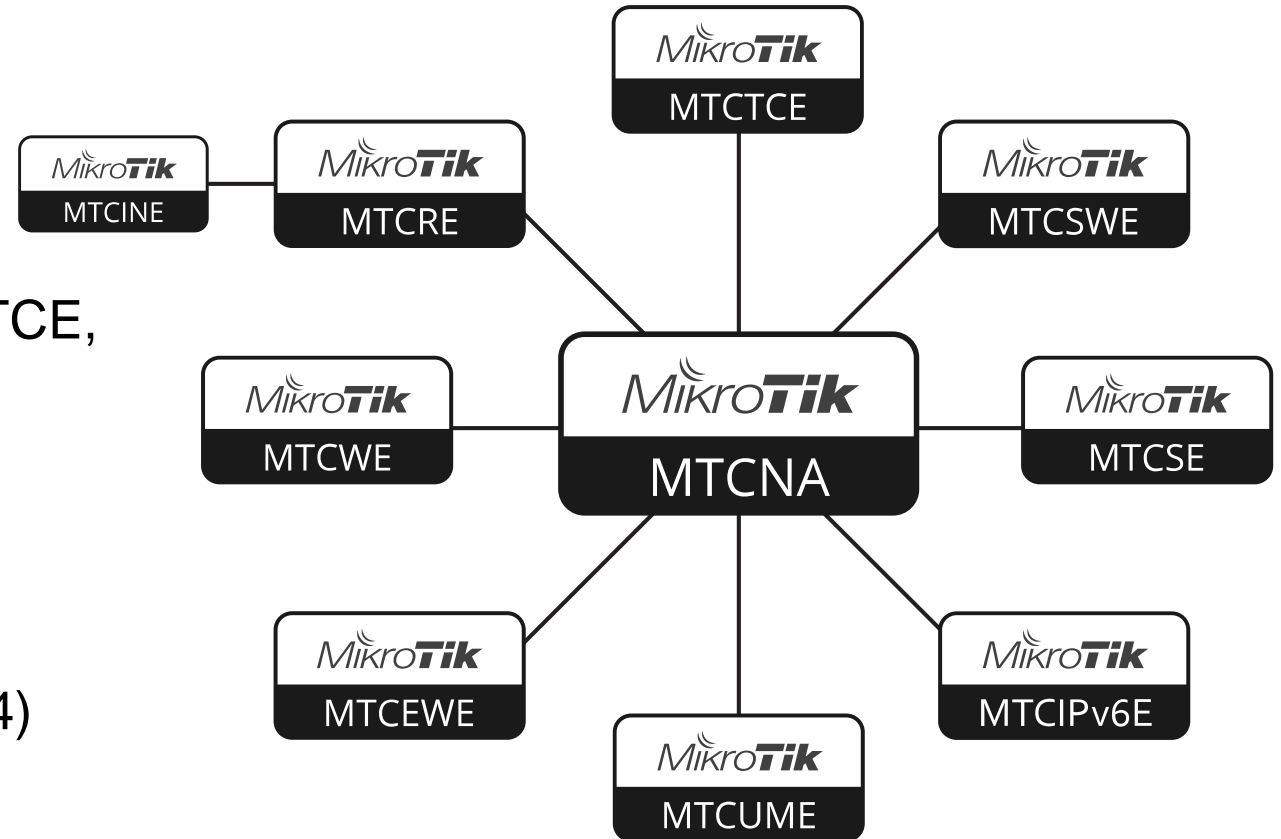
RouterOS 7.18





Me about myself

- Sebastian Inacker
- FMS Internetservice GmbH
- MikroTik Trainer (TR0011)
MTCNA, MTCRE, MTCWE, MTCTCE,
MTCUME, MTCINE, MTCIPv6E,
MTCSE, MTCWE, 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



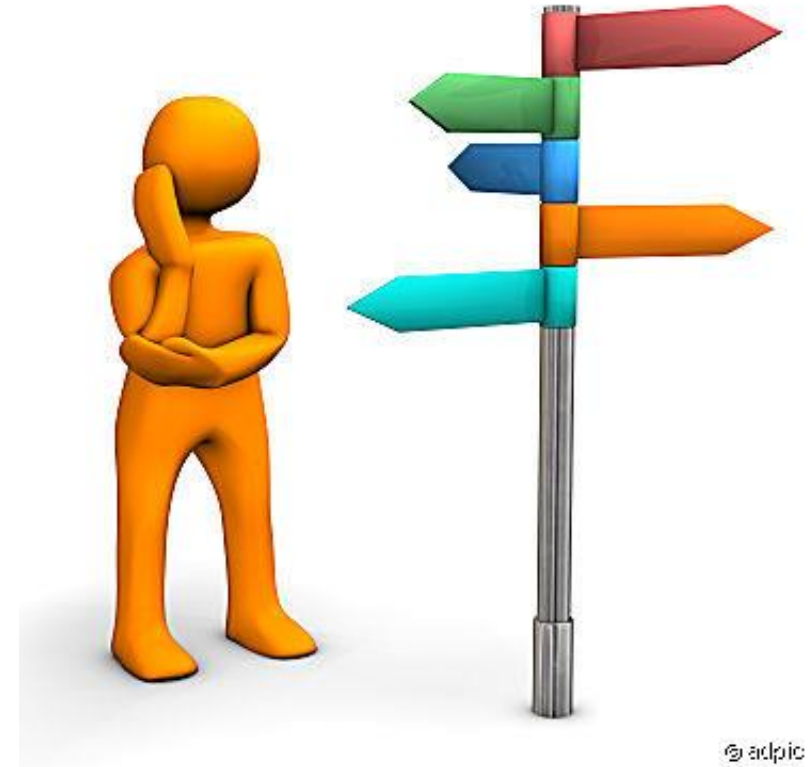


Preface



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

The screenshot shows the 'Interface List' window in RouterOS. The window has a title bar 'Interface List' and a toolbar with various icons. Below the toolbar is a table with two columns: 'List' and 'Interface'. The table contains the following data:

| List | Interface |
|----------|---------------------|
| TRUNK | <i>sfp-sfpplus1</i> |
| TRUNK | <i>sfp-sfpplus2</i> |
| VLAN_100 | <i>ether1</i> |
| VLAN_100 | <i>ether2</i> |
| VLAN_100 | <i>ether3</i> |
| VLAN_200 | <i>ether4</i> |
| VLAN_200 | <i>ether5</i> |

At the bottom of the window, it says '7 items'.

Interfaces → Interface List



VLAN

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

Bridge VLAN <100>

Bridge: lan-bridge

VLAN IDs: 100

Tagged: TRUNK

Untagged:

MVRP Forbidden:

Current Tagged:

Current Untagged:

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Interface List "TRUNK"

Bridge → VLANs → VLAN 100



VLAN

- Since RouterOS 6.41: Interface Lists for Bridge Ports

The image shows two overlapping screenshots of the RouterOS Bridge Port configuration window for VLAN_100. The left screenshot shows the 'General' tab with the 'Interface' field set to 'VLAN_100' and the 'Bridge' field set to 'lan-bridge'. The right screenshot shows the 'VLAN' tab with the 'PVID' field set to '100' and the 'Frame Types' field set to 'admit only untagged and priority tagged'. The 'Status' tab at the bottom of both windows shows the port is 'enabled' and 'Hw. Offload' is checked.

Bridge → Ports



VLAN

- Result...

dynamic, based on
Interface List Members



| # | Interface | Bridge | PVID | Comment |
|-------|--------------|------------|------|---------------------------|
| 0 | TRUNK | lan-bridge | 1 | Interface List "TRUNK" |
| 1 DH | sfp-sfpplus1 | lan-bridge | 1 | Interface List "TRUNK" |
| 2 DH | sfp-sfpplus2 | lan-bridge | 1 | Interface List "TRUNK" |
| 3 | VLAN_100 | lan-bridge | 100 | Interface List "VLAN_100" |
| 4 DH | ether1 | lan-bridge | 100 | Interface List "VLAN_100" |
| 5 DH | ether2 | lan-bridge | 100 | Interface List "VLAN_100" |
| 6 DH | ether3 | lan-bridge | 100 | Interface List "VLAN_100" |
| 7 | VLAN_200 | lan-bridge | 200 | Interface List "VLAN_200" |
| 8 DH | ether4 | lan-bridge | 200 | Interface List "VLAN_200" |
| 9 DIH | ether5 | lan-bridge | 200 | Interface List "VLAN_200" |

10 items

Bridge → Ports



Access Control List (ACL)

Wirespeed filtering



Switch ACL rules

- Filtering at core router might be too late
- Wirespeed, but no stateful 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)

The screenshot shows the RouterOS WinBox interface for configuring ACL rules. A table lists two rules, and an error dialog box is displayed over the top right. A red box highlights the '128 items' count at the bottom left of the table.

| # | Switch: | Ports: |
|---|---------|--------|
| 0 | switch1 | ether1 |
| 1 | switch1 | ether1 |

RouterOS WinBox Error

Couldn't add New Switch Rule - only 128 rules supported (6)

OK

128 items

Switch → Rule



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>

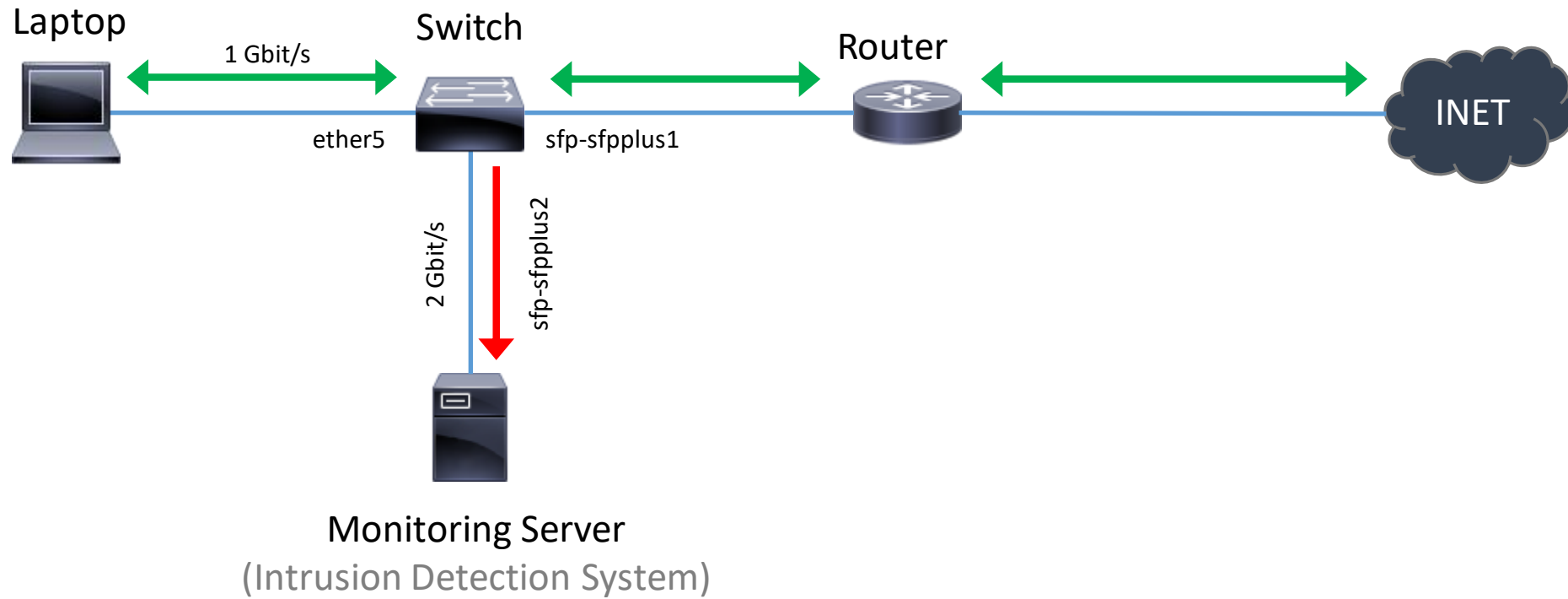


Port Mirroring



Port Mirroring

Mirroring traffic of interface...





Port Mirroring

Mirror ether5 → sfp-sfpplus2 (same Switch Chip)

Switch Port <ether5>

Name: ether5

Switch: switch1

Ingress Rate: []

Egress Rate: []

Storm Rate: 100.00 %

- Limit Broadcasts
- Limit Unknown Unicasts
- Limit Unknown Multicasts
- Mirror Ingress
- Mirror Egress
- L3 Hw Offloading

OK

Cancel

Apply

Switch → Ports

Switch

| Name | Type | Mirror Target |
|---------|------------------|---------------|
| switch1 | Marvell 98DX3236 | sfp-sfpplus2 |

1 item

Switch <switch1>

Name: switch1

Type: Marvell 98DX3236

Mirror Target: sfp-sfpplus2

RSPAN

RSPAN Ingress Vlan ID: 1

RSPAN Egress Vlan ID: 1

Switch All Ports

Cpu Flow Control: []

L3 Hw Offloading

QoS Hw Offloading

OK

Cancel

Apply

Switch → Settings



Port Mirroring

Interfaces

| | Name | Tx | Rx | Tx Packet (p/s) | Rx Packet (p/s) |
|-------------------|--------------|-------------|------------|-----------------|-----------------|
| ::: Mirror Source | | | | | |
| RS | ether5 | 962.7 Mbps | 962.8 Mbps | 79 287 | 79 288 |
| ::: Mirror Target | | | | | |
| R | sfp-sfpplus2 | 1927.2 Mbps | 5.9 kbps | 158 706 | 4 |

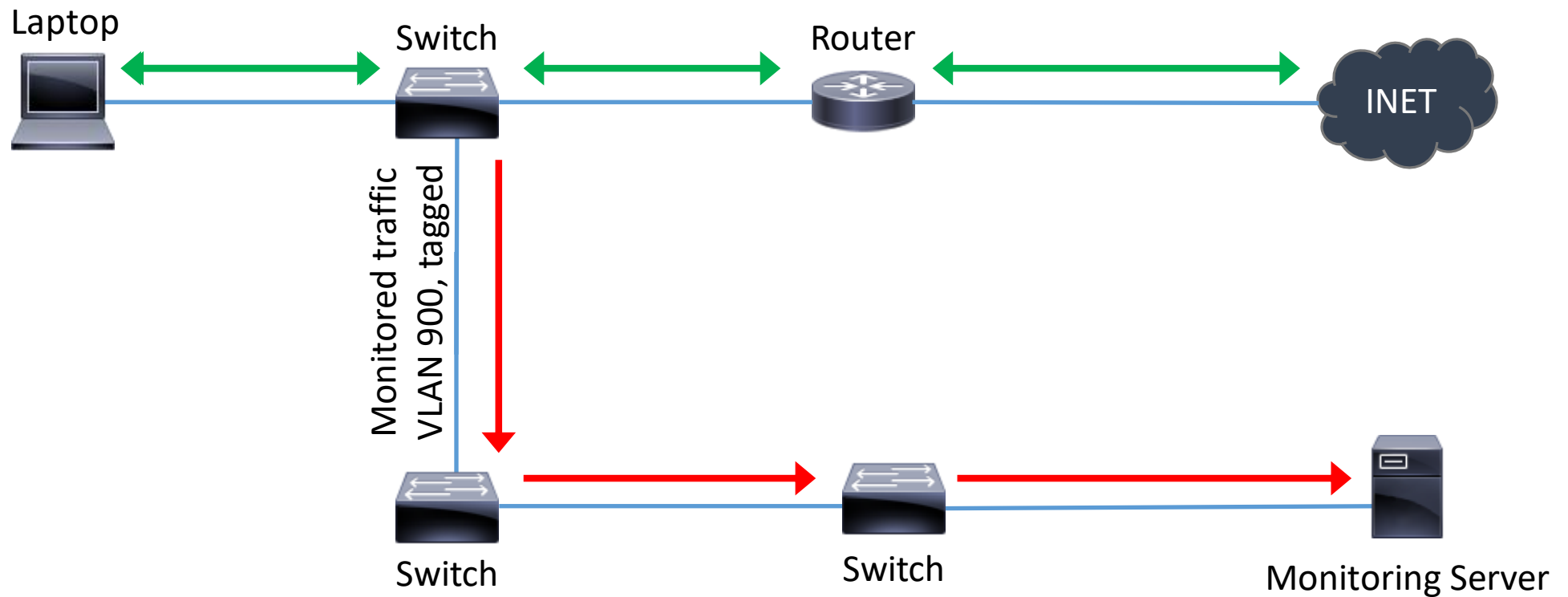
2 items out of 28

Can you handle 2 Gbit/s?



Port Mirroring

Mirrored traffic: VLAN tagged through the net...





Mirroring with ACL filtering & RSPAN

Switch Rule <>

Match Action

Copy To CPU

Redirect To CPU

Mirror

Set New Dst. Ports

New Dst. Ports:

New VLAN ID:

New VLAN Priority:

New QoS Profile:

Keep QoS Fields:

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Switch → Rule → Action

RSPAN = Remote Switched Port Analyzer

Switch → Settings

Switch <switch1>

Name:

Type:

Mirror Target:

RSPAN

RSPAN Ingress Man ID:

RSPAN Egress Man ID:

Switch All Ports

Cpu Flow Control:

L3 Hw Offloading

QoS Hw Offloading

OK
Cancel
Apply



Mirroring with ACL filtering

Filtered to DNS requests from client

The image shows a Wireshark capture of a network packet. The packet list pane shows a single entry: No. 63, Time 4.482825, Source 10.30.0.2, Destination 8.8.8.8, Protocol DNS, Length 80, Info Standard query 0xcdad AAAA upgrade.mikrotik.com. The packet details pane shows the following structure:

- Frame 63: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface Ethernet II, Src: 48:a9:8a:3a:ec:f1, Dst: dc:2c:6e:43:cc:86
- Internet Protocol Version 4, Src: 10.30.0.2, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 56446, Dst Port: 53
- Domain Name System (query)
 - Transaction ID: 0xcdad
 - [Expert Info (Warning/Protocol): DNS response missing]
 - [DNS response missing]
 - [Severity level: Warning]
 - [Group: Protocol]
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - upgrade.mikrotik.com: type AAAA, class IN
 - Name: upgrade.mikrotik.com
 - [Name Length: 20]
 - [Label Count: 3]
 - Type: AAAA (28) (IP6 Address)
 - Class: IN (0x0001)

The packet bytes pane shows the raw data of the DNS query, with the query name and type highlighted in blue:

```
0000 dc 2c 6e 43 cc 86 48 a9 8a 3a ec f1 08 00 45 00 .,nC·H· :;····E·
0010 00 42 15 75 00 00 40 11 4b 07 0a 1e 00 02 08 08 ·B·u·@· K······
0020 08 08 dc 7e 00 35 00 2e 57 1b cd ad 01 00 00 01 ····5·. W······
0030 00 00 00 00 00 00 07 75 70 67 72 61 64 65 08 6d ······u pgrade·m
0040 69 6b 72 6f 74 69 6b 03 63 6f 6d 00 00 1c 00 01 ikrotik·com·····
```

The status bar at the bottom indicates: Pakete: 66 · Angezeigt: 1 (1.5%) · Verworfen: 0 (0.0%) | Profil: Default



WireGuard and VXLAN

Secure Layer 2 around the world



WireGuard and VXLAN

WireGuard

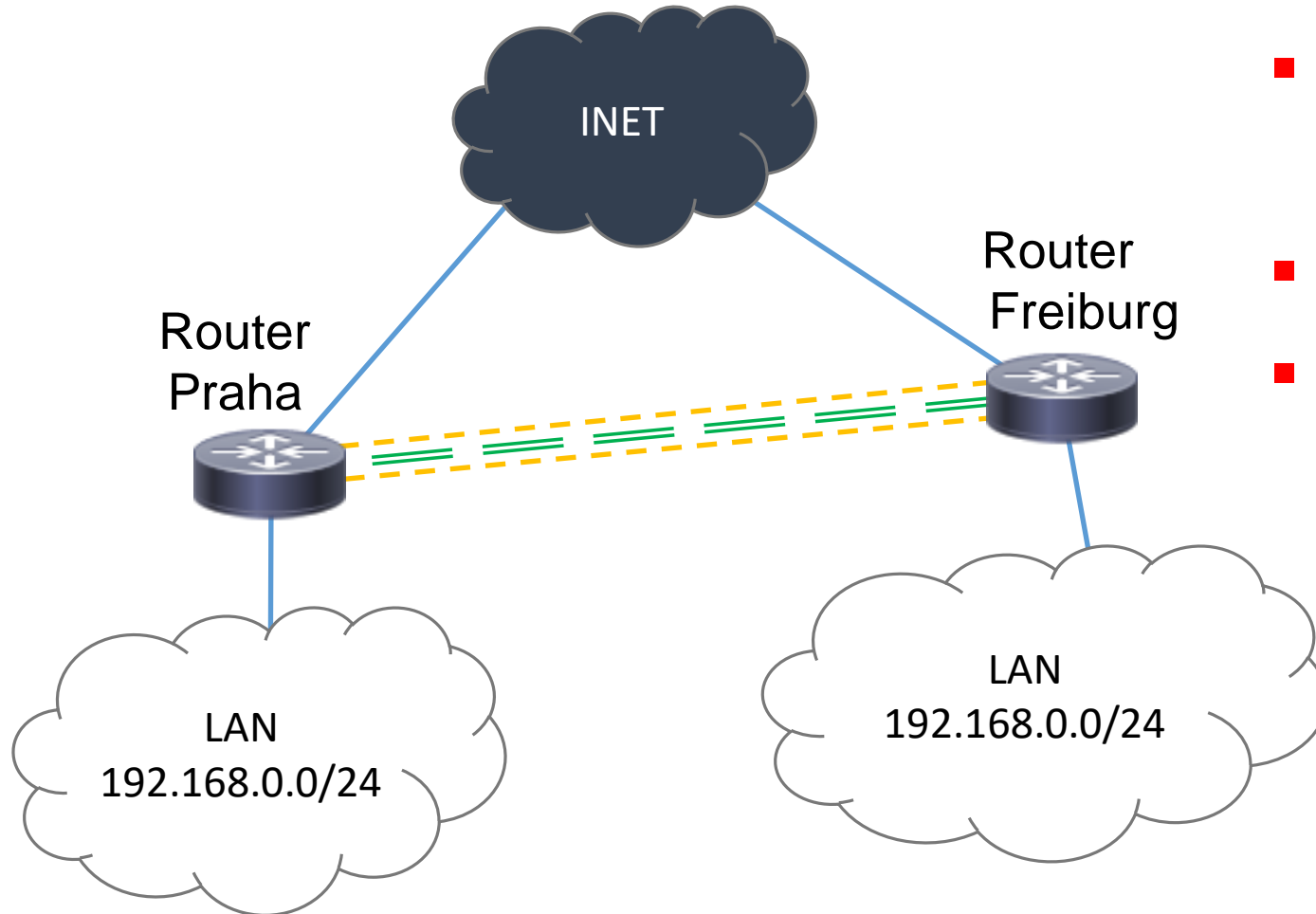
- A modern VPN (Not in scope of this presentation)

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

Interface <vxlan-peer-praha>

General | Loop Protect | Status | Traffic

Name: vxlan-peer-praha

Type: VXLAN

MTU: 1500

Actual MTU: 1500

L2 MTU: 65535

MAC Address: BA:A1:31:A5:2F:67

ARP: enabled

ARP Timeout:

VNI: 42

Group:

Interface:

Port: 4789

Local Address: 10.255.255.2

Don't Fragment: disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch
Reset Traffic Counters

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

VTEP

| Interface | Remote Ip |
|------------------|--------------|
| vxlan-peer-praha | 10.255.255.1 |

1 item

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 ax ² | 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 98DX8xxx, 98DX4xxx, 98DX325x)

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

Interface <vxlan-vlan-100>

General | Loop Protect | Status | Traffic

Name: vxlan-vlan-100
Type: VXLAN
MTU: 9500
Actual MTU: 9500
L2 MTU: 65535
MAC Address: BE:65:A7:18:72:84
ARP: enabled
ARP Timeout:
VNI: 22100
Group:
Interface:
Port: 4789
Local Address: 172.16.0.2

Bridge: vxlan-bridge
Bridge PVID: 100
 HW

enabled | running | slave | passthrough | inactive | Hw. Offloaded

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch
Reset Traffic

Bridge → Ports

Bridge

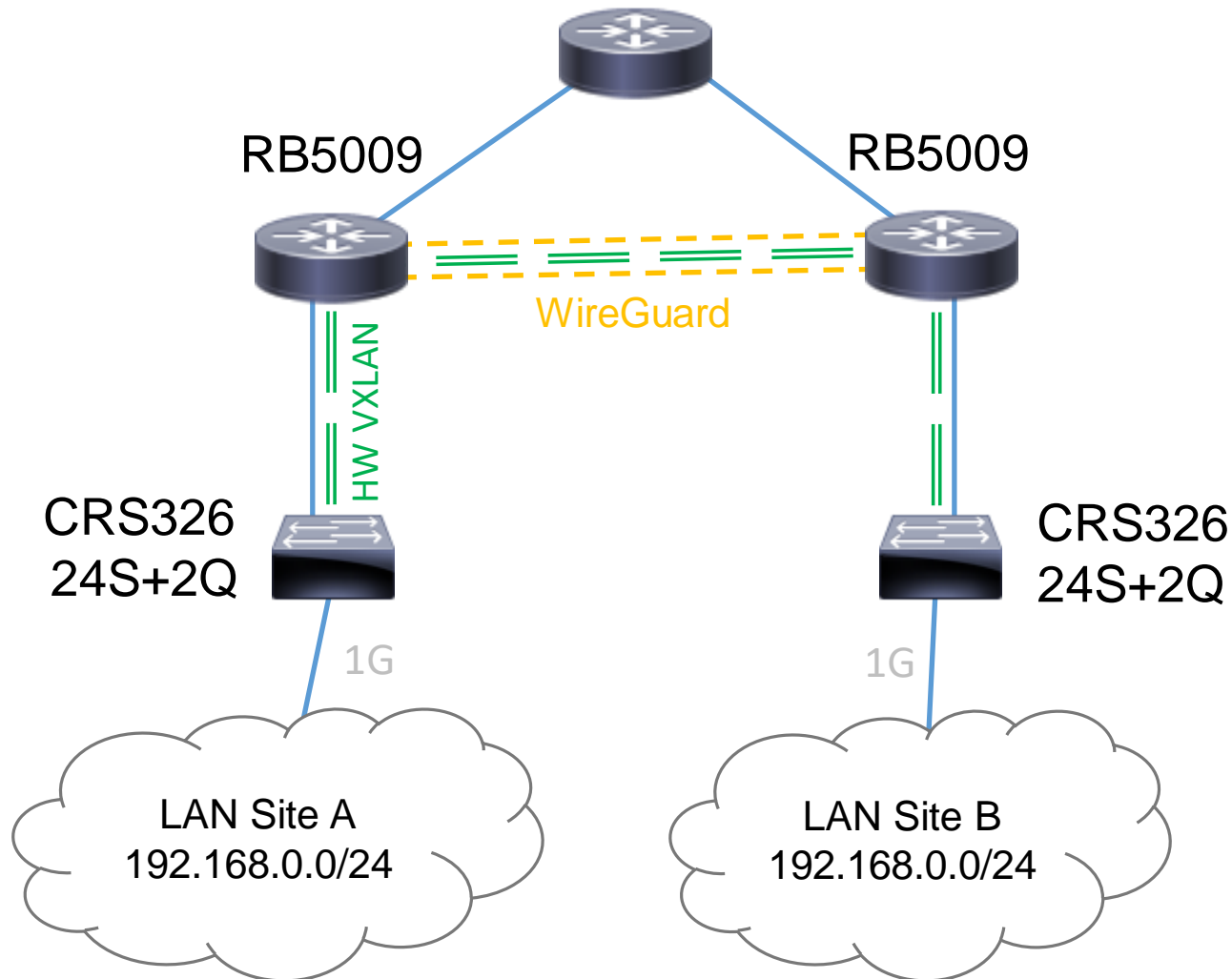
Bridge | Ports | VLANs | MSTIs | Port MST Overrides | Filters | NAT | Hosts | MDB

| # | Interface | Bridge | PVID |
|------|----------------|--------------|------|
| 0 H | sfp-sfpplus11 | vxlan-bridge | 100 |
| 1 DH | vxlan-vlan-100 | vxlan-bridge | 100 |

2 items



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

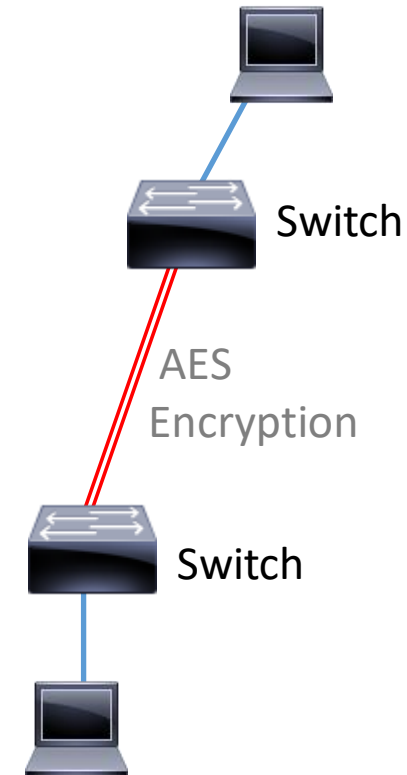


MACsec

- 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

Interface <macsec1>

General | Status | Traffic

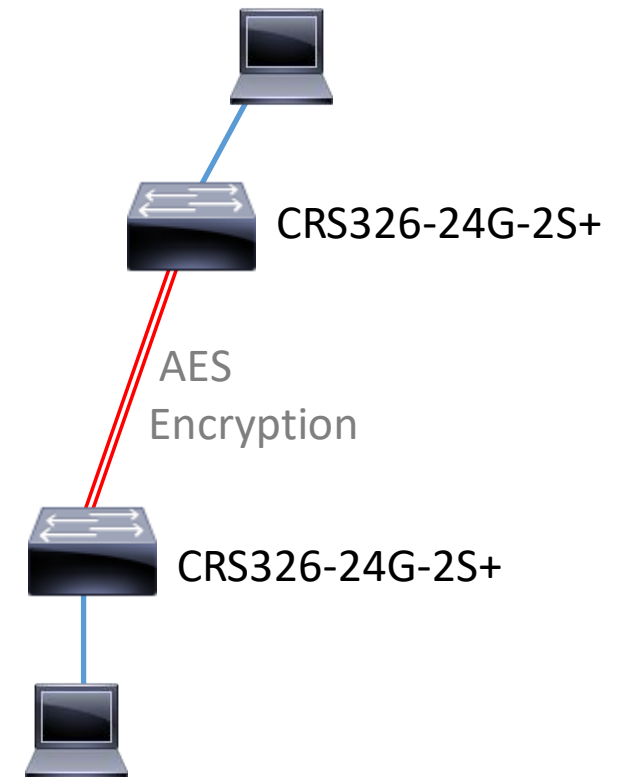
Name: macsec1
Type: MACsec
MTU: 1468
Actual MTU: 1468
L2 MTU: 1560
MAC Address: D4:01:C3:9C:70:86

Interface: ether1
CAK: eb50299b3b4cea7dd8c200fa63e1ff45
CKN: 2b5d052b31f279544be49929f4da0f5bb4e6621cf777b
Profile: default
Status: open-encrypted

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch
Reset Traffic Counters

| | | | | |
|-----------------|---------|-----------------|-------------|----------|
| enabled | running | slave | passthrough | inactive |
| tx (TCP) | | rx (TCP) | | |
| 15 Mbps | | 50 Mbps | | |

CRS326 is wrong device for MACsec





MACsec, RB5009

Interfaces → MACsec

Interface <macsec1>

General | Status | Traffic

Name: macsec1
Type: MACsec
MTU: 1468
Actual MTU: 1468
L2 MTU: 1560
MAC Address: D4:01:C3:9C:70:86

Interface: ether1
CAK: eb50299b3b4cea7dd8c200fa63e1ff45
CKN: 2b5d052b31f279544be49929f4da0f5bb4e6621cf777b
Profile: default
Status: open-encrypted

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch
Reset Traffic Counters

enabled | running | slave | passthrough | inactive

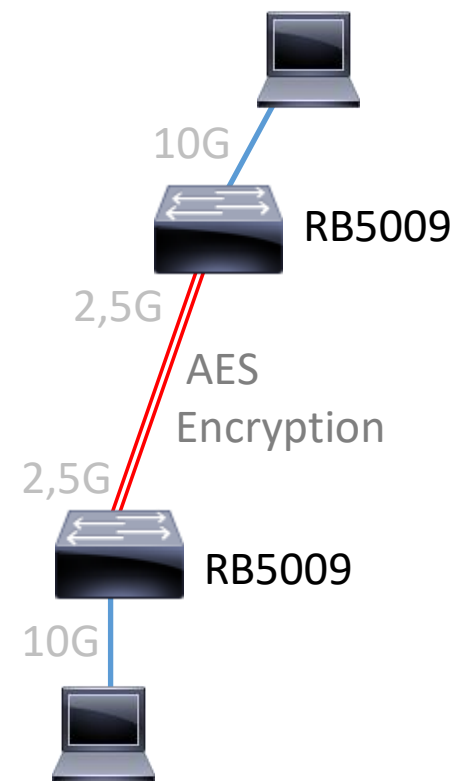
tx (TCP)

890 Mbps

rx (TCP)

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
```

DHCP Alert <ether8>

Interface: ether8

Valid Servers: DC:2C:6E:43:CC:7E

Alert Timeout: 01:00:00

Unknown Servers: 48:8F:5A:6A:2E:66
B8:69:F4:C5:5F:EE
D4:CA:6D:57:2D:66

On Alert:

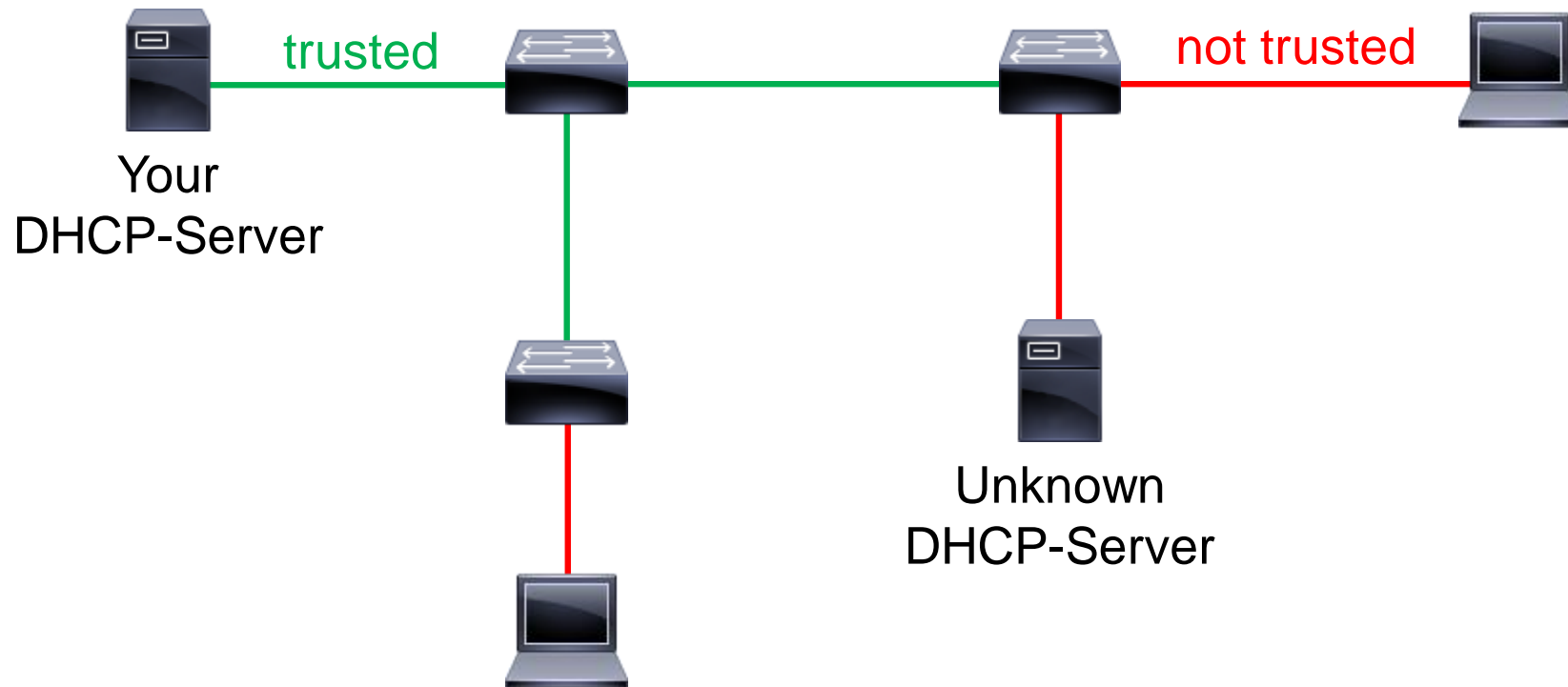
enabled

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Alert

IP → DHCP-Server → Alerts



DHCP snooping





DHCP snooping

Bridge → Bridge

Interface <bridge>

General STP VLAN Status Traffic

Name: bridge

Type: Bridge

MTU: []

Actual MTU: 1500

L2 MTU: 1592

MAC Address: D4:01:C3:9C:70:9E

ARP: enabled

ARP Timeout: []

Admin. MAC Address: []

Ageing Time: 00:05:00

Max Learned Entries: auto

IGMP Snooping

DHCP Snooping

Add DHCP Option 82

Fast Forward

enabled running slave passthrough inactive

Bridge Port <TRUNK>

General STP VLAN Status

Interface: TRUNK

Bridge: bridge

Horizon: []

Learn: auto

Unknown Unicast Flood

Unknown Multicast Flood

Broadcast Flood

Trusted

Hardware Offload

Multicast Router: Temporary Query

Fast Leave

enabled inactive Hw. Offload

Bridge → Port

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



DHCP snooping and DHCP Option 82

IP → DHCP-Server → Lease

DHCP Lease <10.200.200.253, 10.200.200.253>

General Active

Active Address: 10.200.200.253

Active MAC Address: DC:2C:6E:43:CC:82

Active Client ID: 1:dc:2c:6e:43:cc:82

Active Host Name: A-RB5009

Active Class ID:

Active Server: dhcp1

Bridge Port:

Src. MAC Address:

Expires After: 00:27:48

Last Seen: 00:02:11

Age: 00:02:11

Agent Circuit Id: SW#1 eth 0/6:200

Agent Remote Id: ether5

dynamic enabled radius blocked bound

OK

Copy

Remove

Make Static

Ping

Check Status

Info available on DHCP-Server

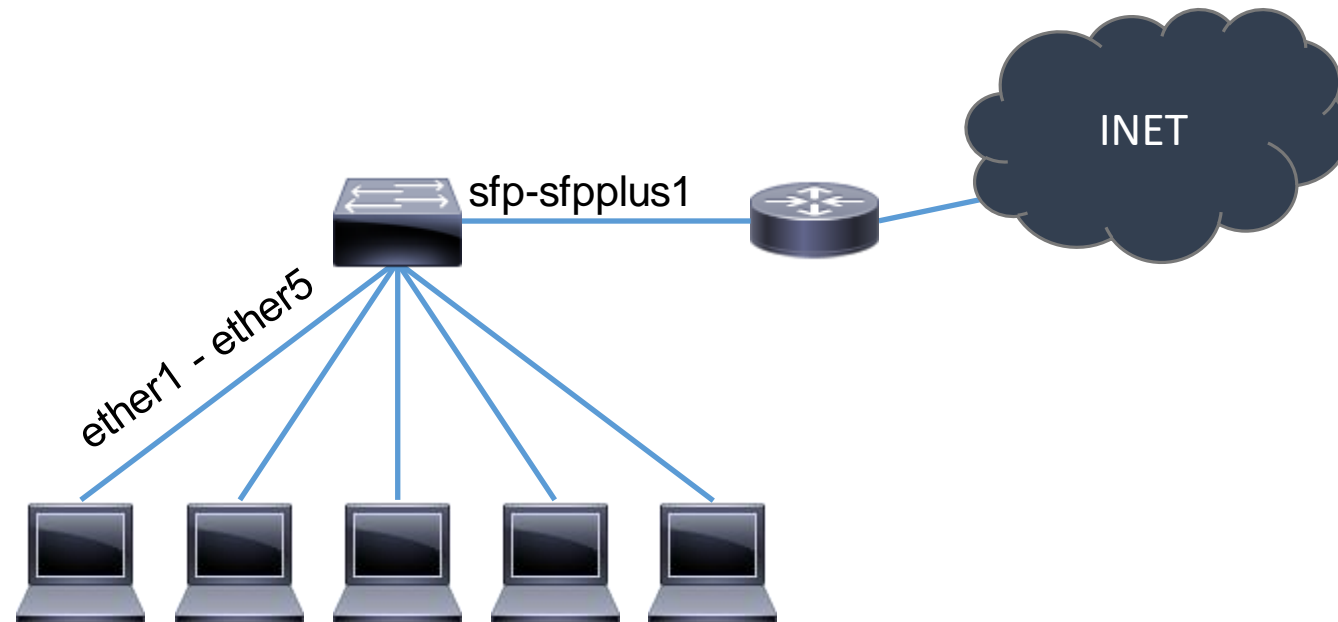
- Agent Circuit Id:
DHCP-Client is connected to switch
“SW#01” on VLAN 200
- Agent Remote Id:
Client is connected to switch port
ether5

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

| Name | Switch | Forwarding Override | Forward To |
|--------|---------|---------------------|--------------|
| ether1 | switch1 | yes | sfp-sfpplus1 |
| ether2 | switch1 | yes | sfp-sfpplus1 |
| ether3 | switch1 | yes | sfp-sfpplus1 |
| ether4 | switch1 | yes | sfp-sfpplus1 |
| ether5 | switch1 | yes | sfp-sfpplus1 |
| ether6 | switch1 | no | |
| ether7 | switch1 | no | |

27 items

Switch Port Isolation <ether5>

Name: ether5

Switch: switch1

Forwarding Override

Forward To: sfp-sfpplus1

OK

Cancel

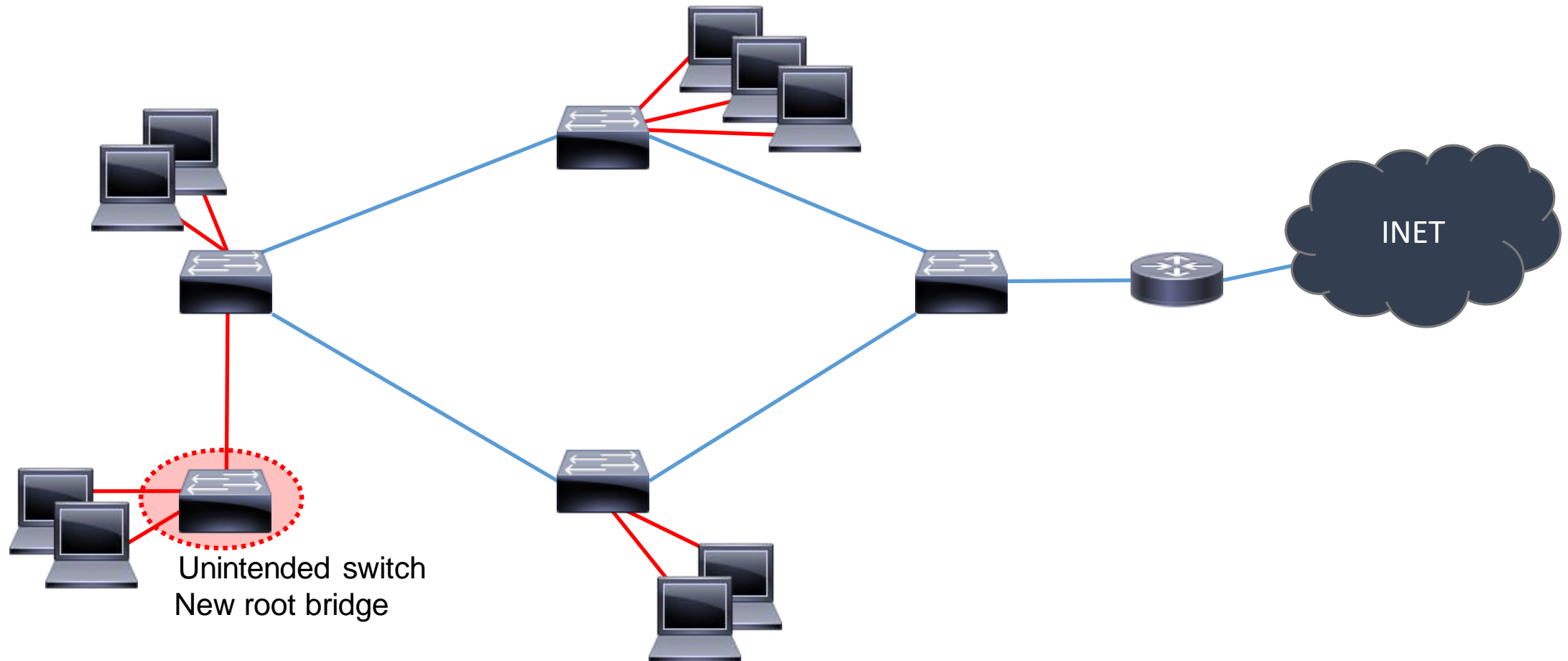
Apply

- 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 xSTP 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

Bridge

Bridge Ports VLANs MSTIs Port MST Overrides Filters NAT Hosts MDB

PVID is 200

| # | Interface | Bridge | Trusted | PVID |
|---|------------|--------|---------|------|
| 7 | VLAN_200 | bridge | no | 200 |
| 8 | DIH ether5 | bridge | no | 200 |

2 items out of 9

--- BPDU guard changed port role to disabled due to received BPDU frame, manual bridge port re-enable is required

Bridge Port <VLAN_200>

General STP VLAN Status

Priority: 80 hex

Path Cost: ▼

Internal Path Cost: ▼

Edge: yes ▼

Point To Point: auto ▼

Auto Isolate

Restricted Role

Restricted TCN

BPDU Guard

enabled inactive Hw. Offload

OK Cancel Apply Disable Comment Copy Remove

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

