



# Managing and Monitoring

RouterOS



# Agenda

- Company introduction
- Network operation  
the big picture
- Management approaches
- Network monitoring
- RouterOS monitoring





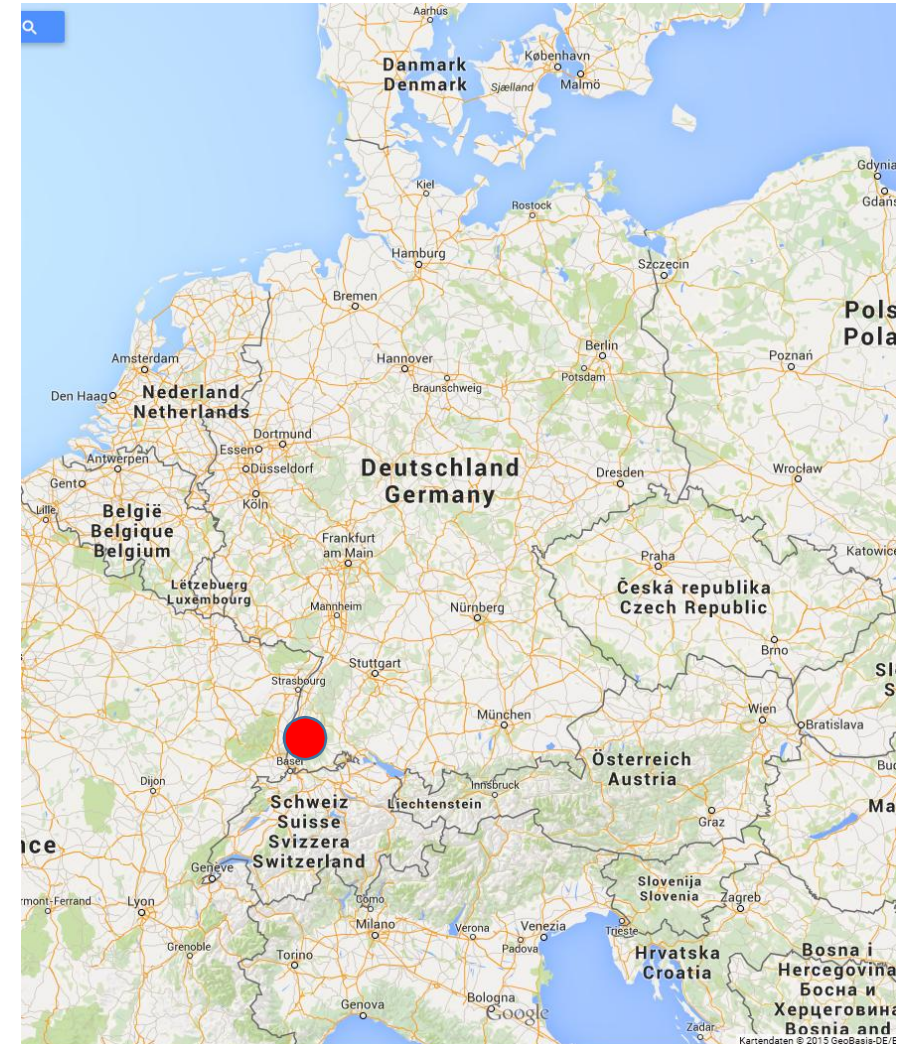
# FMS Internetservice GmbH

Value Added Distribution



# FMS Internetservice GmbH

- Value Added Distributor
  - Distribution
  - Training
  - Consulting
  - Support
- Founded 1997
- 11 employees
- Southern Germany







# FMS Internetservice GmbH

- Inhouse training facility
- All certification levels
- First German speaking Training partner TR11 & TR23
- First MTCSA certified German distributor

See Training Schedule





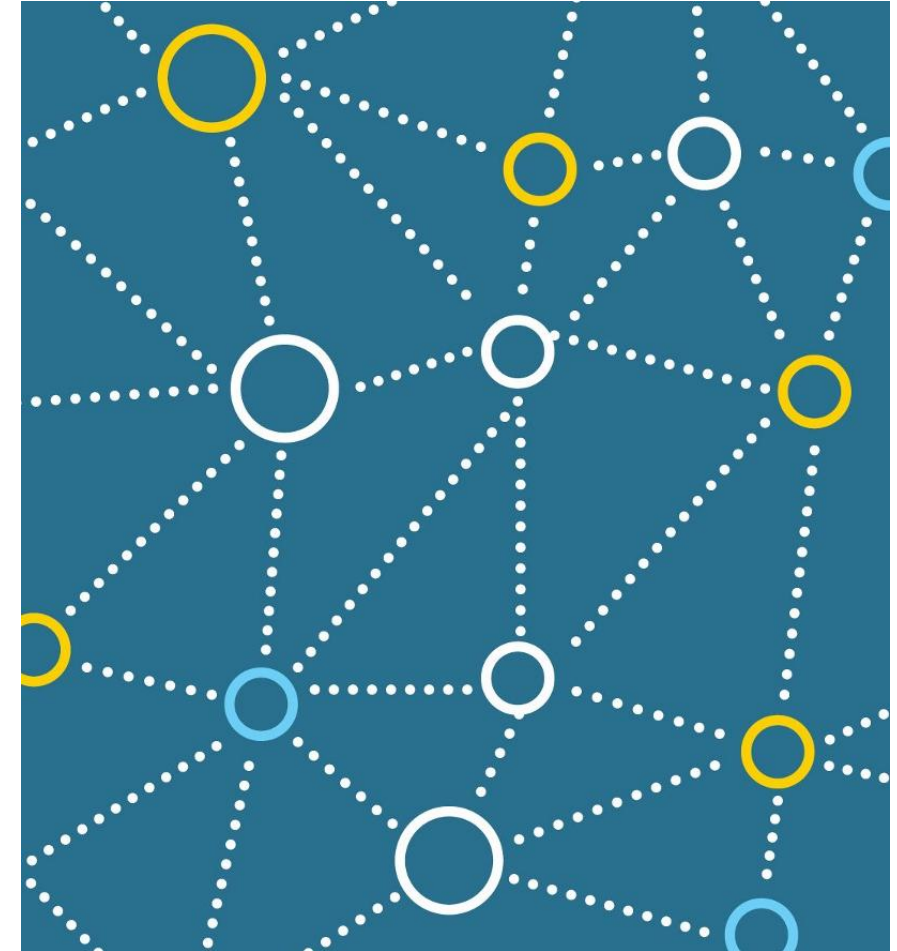
# Network Operation – Big Picture

Challenges and Elements



# The Challenge of Operation

- Growing number of devices
- More critical services
- Higher bandwidth (more packets)
- Heavy interconnection of sites
  
- Networks
  - Become larger
  - Become more complex
  - Require higher availability
  - Require effective security





# Operational Tasks

- Inventory

- Debugging



- Management

- Maintenance

- Monitoring





# RouterOS

## Network Inventory Management

- Dude
- Script based database
- TR069
- CAPsMAN

## Access to management

- Dude
- Management VLAN
- RoMON
- CAPsMAN

## Management technologies

- Webbox
- Winbox
- Terminal
- API
- TR069
- SNMP
- App
- CAPsMAN

## General Tools

- Time / SNTP
- Watchdog
- Scripting & API
- Netwatch
- SSH keys

## Maintenance

- RouterOS & bootloader updates
- Backup/Restore & Import-Export



# RouterOS

## Debugging (Router)

- Health
- History
- local logging
- /system resources
- /system routerboard
- /tools profile
- Supout

## Debugging (Traffic and Network)

- Neighbours
- Bandwidth test (old and new)
- Traffic generator
- Torch
- Ping, Flood Ping, Ping Speed
- Traceroute
- IP Scan
- Packet Sniffer (and TZSP streams)
- Port Mirroring (Switch chip)

## Logging & 3<sup>rd</sup> Party Integration

- IP Accounting
- Traffic Flow (Netflow)
- SNMP
- Graphing
- Syslog
- TR069



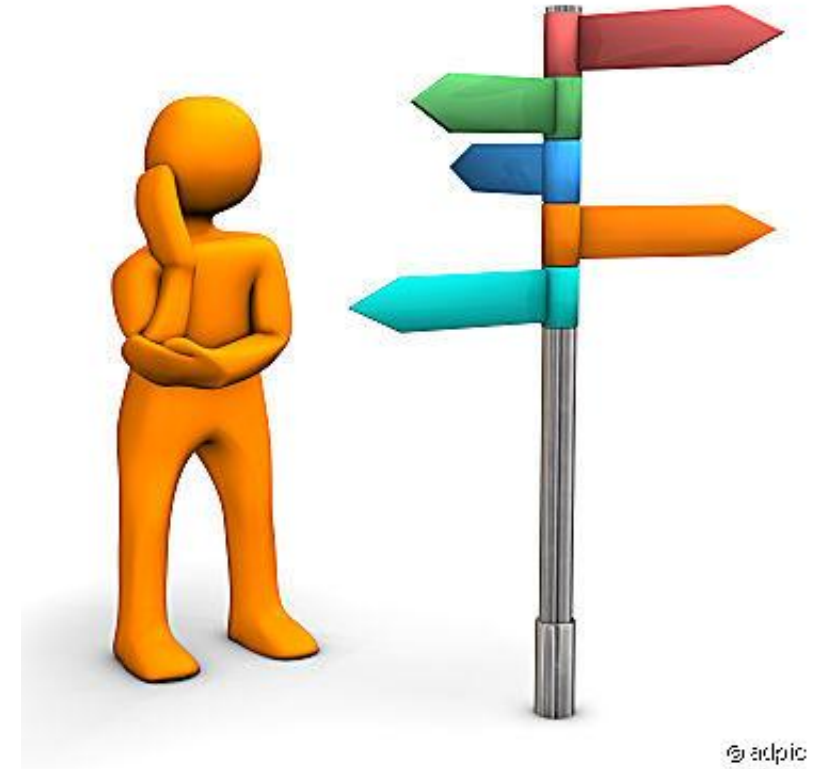
# Management Topologies

Secure and Convenient Management Access



# Management Approaches

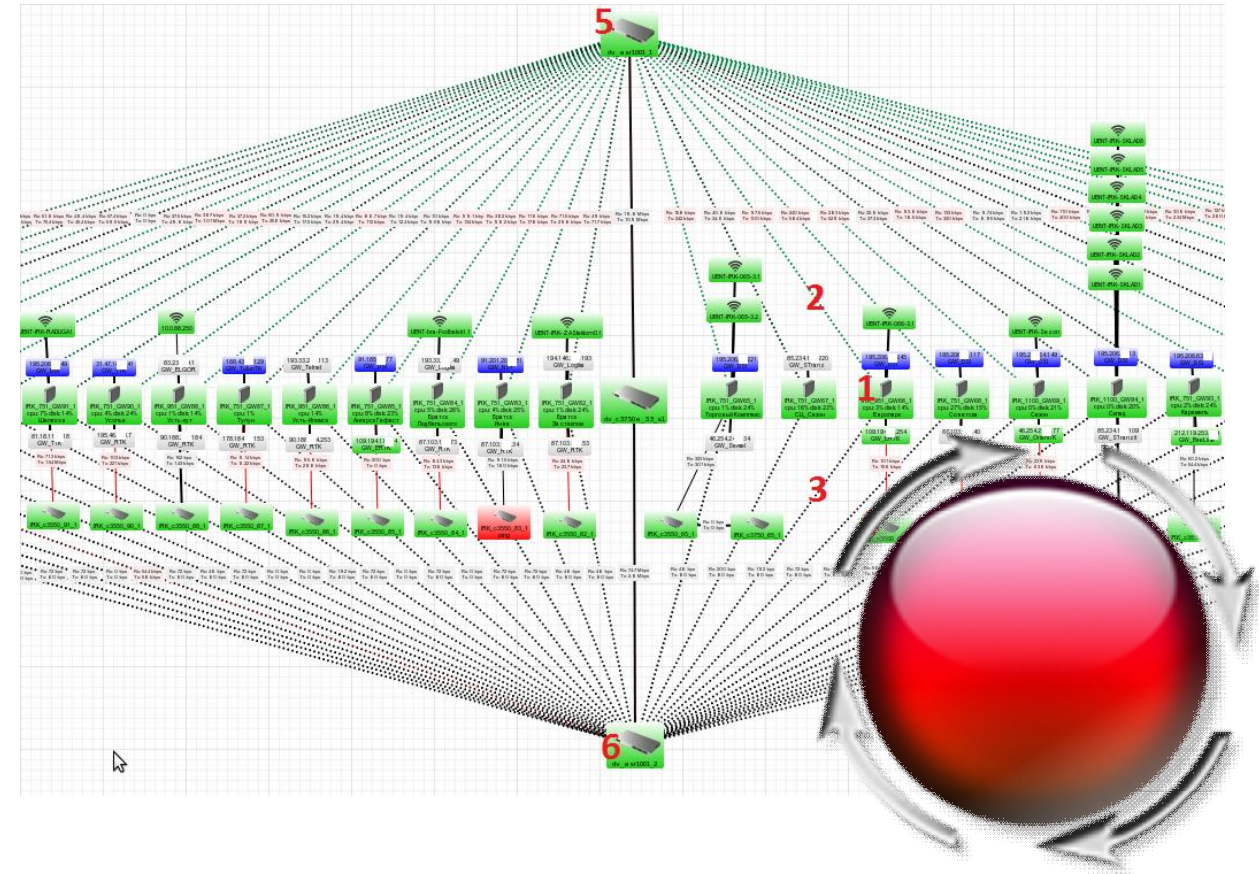
- Considerations
  - Security
  - Convenience
  - Efficiency
- Common Approaches
  - Separate management and user traffic
  - Management VLAN
  - Tunneling payload (e.g. PPPoE)
  - Tunneling of management (VPN)





# Management Approaches

- Central MikroTik tools
  - The Dude
  - CAPsMAN
  - Usermanager
- Detailed examples
  - RoMON
  - CLI/scripting (3<sup>rd</sup> party tools)
  - API (Application programming interface)





## RoMON

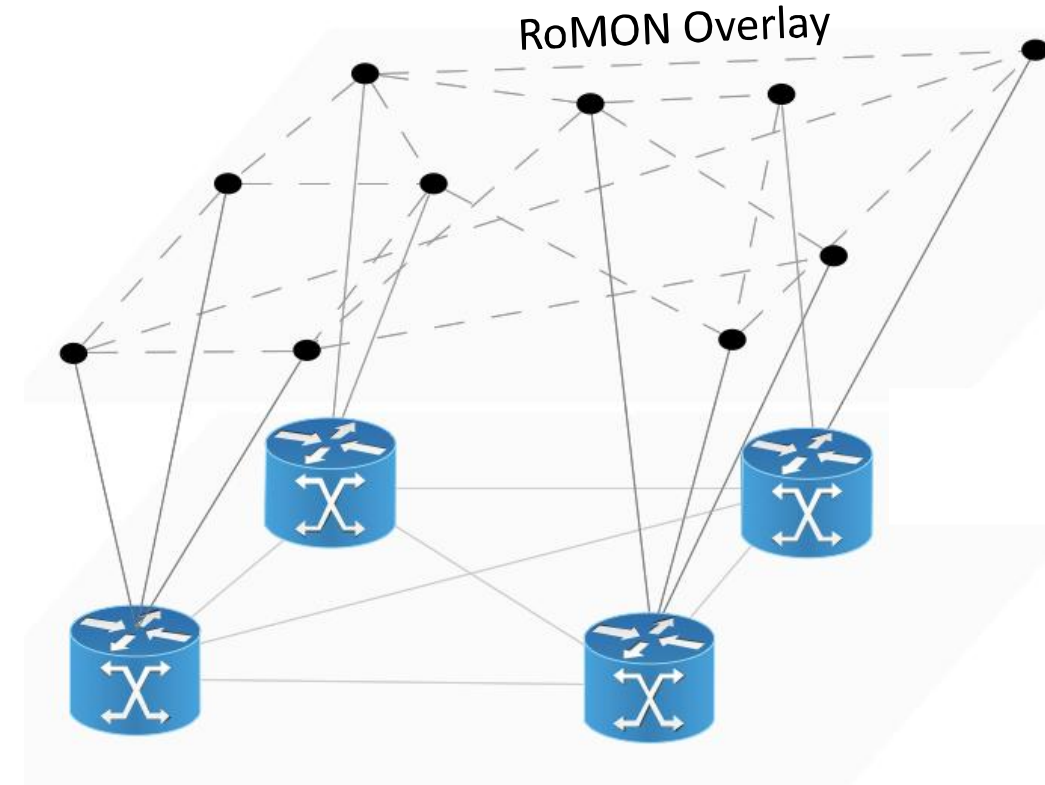
Simplify Discovery and Access





# RoMON

- RoMoN Overlay Network
- Proprietary MikroTik protocol
- Device discovery
- Device access
- Layer-2 & layer-3 networks
- Without layer-3 routing
- Winbox support





# RoMON + MAC Winbox vs. Neighbours + MAC Winbox

## Neighbour discovery (MNDP)

- Using existing network
- Compatible with CDP and LLDP
- Limited to layer-2 broadcast domain
- Winbox: discovery and MAC connection

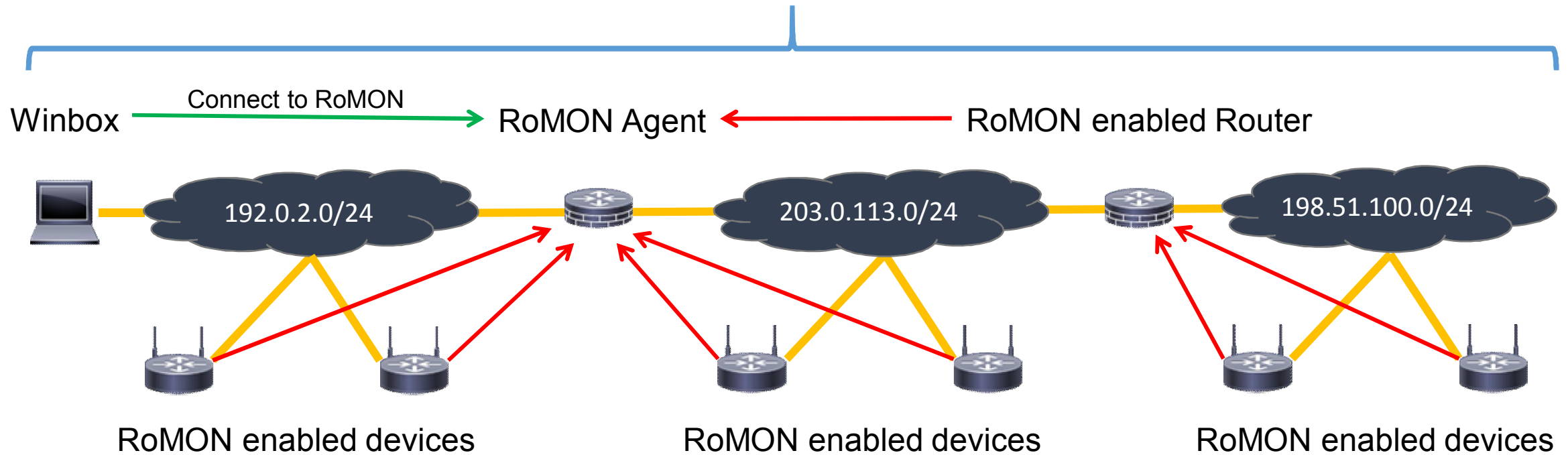
## RoMON

- Creates overlay network
- Only with MikroTik devices
- Not limited to layer-2 broadcast domain
- Winbox: discovery and MAC connection
- Winbox: RoMON agent connection
- On ethernet like interfaces (Ethernet, WLAN, EoIP, VLAN ...)



# Local Device Discovery across Routers

Discovery with RoMON, Connect by RoMON Winbox



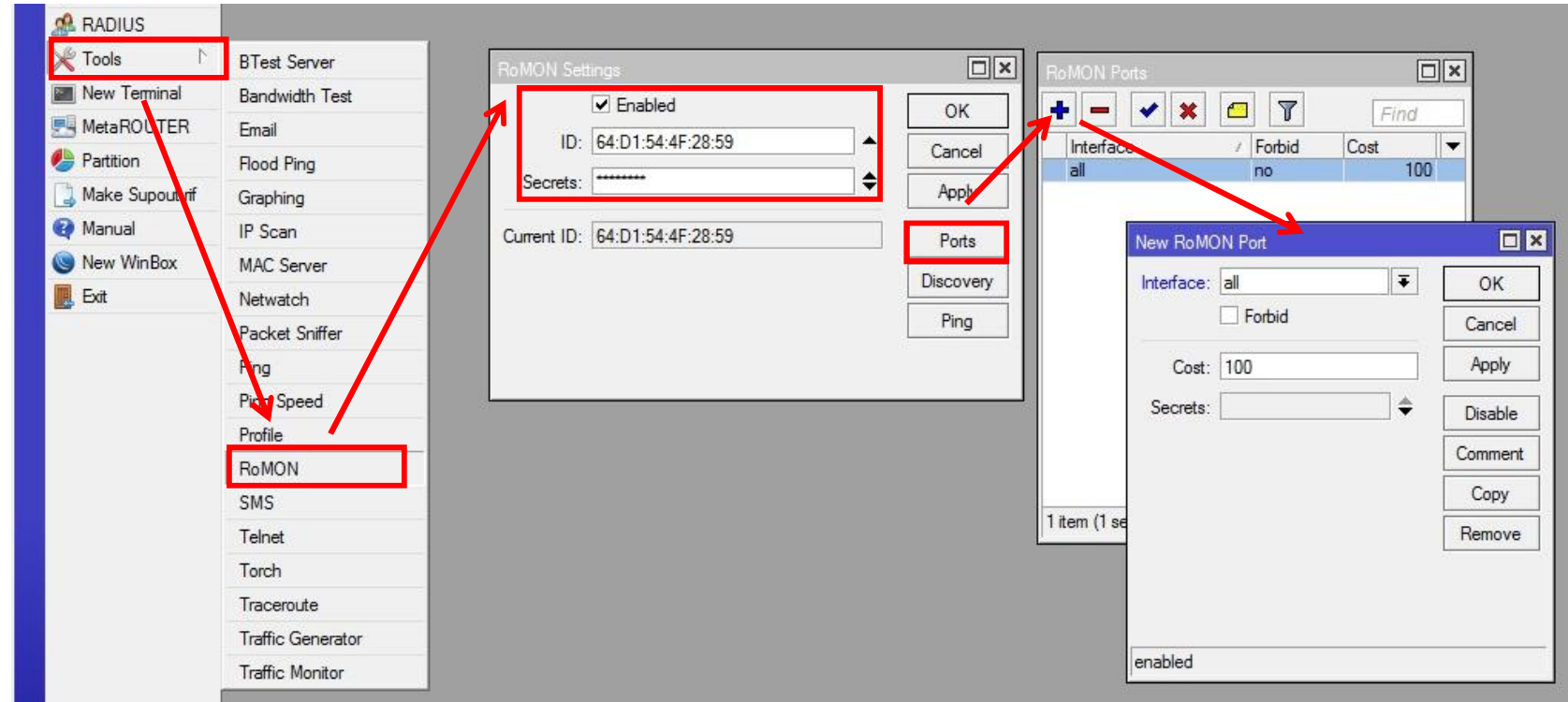
Discovery with MNDP

Connect by IP or MAC Winbox



# RoMON Setup

- Enable RoMON
- Optional but recommended
  - Set ID manually
  - Use secret(s)
- Optional
  - Customize interface configuration





# RoMON Tools

RoMON Settings

☒ Enabled

ID: 64:D1:54:4F:28:59

Secrets: \*\*\*\*\*

Current ID: 64:D1:54:4F:28:59

OK  
Cancel  
Apply  
Ports  
Discovery  
Ping

- Discovery
- Ping
- CLI: ssh
- Winbox

Discovery (Running)

Address	Cost	Hops	Path	L2MTU	Identity	Version
64:D1:54:08:4C:54	400	2	D4:CA:6D:23:F8:A5, 6...	1500	RoMon: A32	6.43.7
64:D1:54:4F:27:F0	200	1	64:D1:54:4F:27:F0	1500	RoMon: A11	6.43.12
64:D1:54:4F:28:9F	200	1	64:D1:54:4F:28:9F	1500	RoMon: A22	6.42.11
6C:3B:6B:0D:1C:10	200	1	6C:3B:6B:0D:1C:10	1500	RoMon: A21	6.42.7
CC:2D:E0:11:8A:D9	400	2	D4:CA:6D:23:F8:A5, ...	1500	RoMon: A31	6.42.1
D4:CA:6D:23:F8:A5	200	1	D4:CA:6D:23:F8:A5	1500	RoMon: R2	6.42.6
E4:8D:8C:B2:81:96	200	1	E4:8D:8C:B2:81:96	1500	RoMon: A12	6.43.12

7 items

Ping (Running)

ID: 64:D1:54:08:4C:54

Packet Size: 32

Interval: 1.000

Count:

Start  
Stop  
Close  
New Window

Seq #	Host	Time	Reply Size	Status
137	64:D1:54:08:4C:54	0.001	32	
138	64:D1:54:08:4C:54	0.001	32	
139	64:D1:54:08:4C:54	0.001	32	

140 items (1 sel... 0% packet loss Min: 0 ms Avg: 1 ms Max: 4 ms)

Terminal

```
[admin@RoMon: R1] /tool romon>
[admin@RoMon: R1] /tool romon>
port discover edit export get ping print set ssh
[admin@RoMon: R1] /tool romon>
```



# Standard Tools in RoMON Network

## Ping / MAC Ping

Ping (Running)

General Advanced

Ping To: 64:D1:54:08:4C:54

Interface:

☐ ARP Ping

Packet Count:

Timeout: 1000 ms

Start Stop Close New Window

Seq #	Host	Time	Reply Size	TTL	Status
16		timeout			timeout
17		timeout			timeout
18		timeout			timeout
19		timeout			timeout
20		timeout			timeout
21		timeout			timeout
22		timeout			timeout
23		timeout			timeout
24		timeout			timeout
25		timeout			timeout
26		timeout			timeout
27		timeout			timeout

29 items 0 of 29 packets ... 100% packet l...

## RoMON Ping

Ping (Running)

ID: 64:D1:54:08:4C:54

Packet Size: 32

Interval: 1.000

Count:

Start Stop Close New Window

Seq #	Host	Time	Reply Size	Status
12	64:D1:54:08:4C:54	0.001	32	
13	64:D1:54:08:4C:54	0.001	32	
14	64:D1:54:08:4C:54	0.001	32	
15	64:D1:54:08:4C:54	0.001	32	
16	64:D1:54:08:4C:54	0.001	32	
17	64:D1:54:08:4C:54	0.001	32	
18	64:D1:54:08:4C:54	0.001	32	
19	64:D1:54:08:4C:54	0.001	32	
20	64:D1:54:08:4C:54	0.001	32	
21	64:D1:54:08:4C:54	0.001	32	
22	64:D1:54:08:4C:54	0.001	32	
23	64:D1:54:08:4C:54	0.001	32	
24	64:D1:54:08:4C:54	0.001	32	
25	64:D1:54:08:4C:54	0.001	32	
26	64:D1:54:08:4C:54	0.001	32	
27	64:D1:54:08:4C:54	0.001	32	
28	64:D1:54:08:4C:54	0.002	32	
29	64:D1:54:08:4C:54	0.001	32	

30 items ... 0% packet loss Min: 1 ms Avg: 1 ms Max: 5 ms





# Winbox Discovery and RoMON Connection

WinBox v3.18 (Addresses-Site-1)

File Tools

Connect To: 64:D1:54:4F:28:5C

Login: admin

Password:

Session: <own> Browse...

Note: RoMon: R1

Group:

RoMON Agent:

Add/Set

Keep Password

Autosave Session

Open In New Window

2

Connect To RoMON

Connect

Managed Neighbors

Refresh

Find all

Identity contains RoMon

MAC Address	IP Address	Identity	Version	Board	Uptime
64:D1:54:4F:27:F6	192.0.2.1	RoMon: A11	6.43.12 (stable)	RB952Ui-5ac2nD	02:59:58
E4:8D:8C:B2:81:96	192.0.2.1	RoMon: A12	6.43.12 (stable)	RB952Ui-5ac2nD	00:57:12
64:D1:54:4F:28:5C	192.0.2.254	RoMon: R1	6.44 (stable)	RB952Ui-5ac2nD	00:57:45

Devices within  
the layer-2  
network  
discovered

Use router as  
RoMON agent



# Winbox Discovery and RoMON Connection

Connected to  
RoMON agent

3

RoMON  
discovery  
through agent

4

Two hops to  
reach

WinBox v3.18 (Addresses-Site-1)

File Tools

Connect To: 64:D1:54:4F:28:5C

Login: admin

Password:

Session: <own> Browse...

Note: RoMon: R1

Group:

RoMON Agent: 64:D1:54:4F:28:5C

Add/Set Disconnect From RoMON Connect

Managed RoMON Neighbors

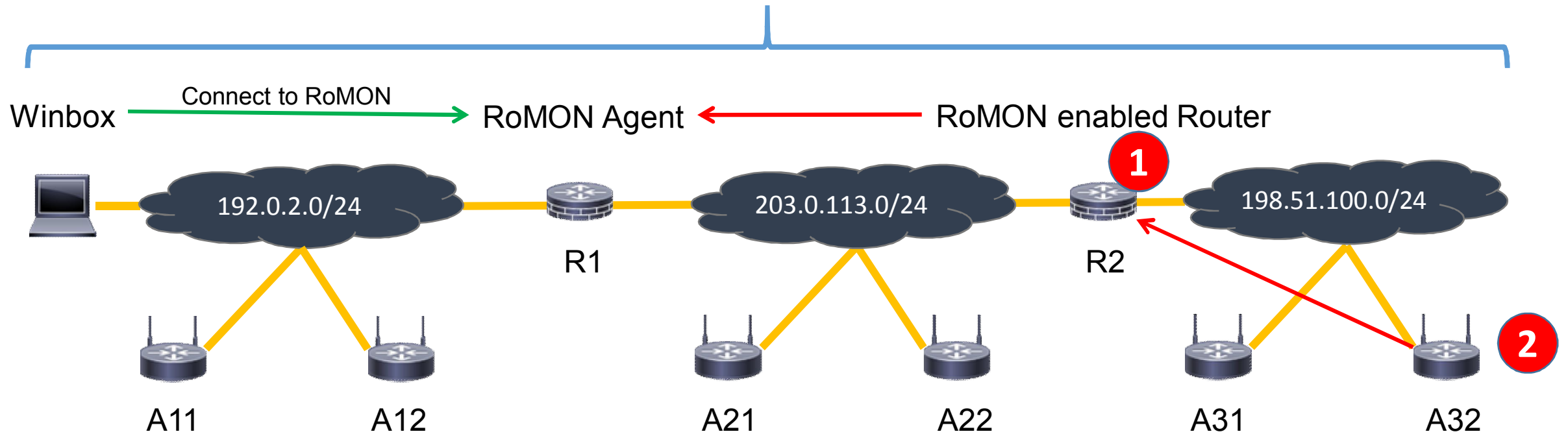
Refresh Find

Address	Cost	Hops	Path	L2MTU	Identity	Version	Board
D4:CA:6D:23:F8:A5	200	1	D4:CA:6D:23:F8:A5	1500	RoMon: R2	6.42.6	RB750UP
64:D1:54:4F:28:9F	200	1	64:D1:54:4F:28:9F	1500	RoMon: A22	6.42.11	RB952Ui-5ac2nD
6C:3B:6B:0D:1C:10	200	1	6C:3B:6B:0D:1C:10	1500	RoMon: A21	6.42.7	RB750Gr3
E4:8D:8C:B2:81:96	200	1	E4:8D:8C:B2:81:96	1500	RoMon: A12	6.43.12	RB952Ui-5ac2nD
64:D1:54:4F:27:E0	200	1	64:D1:54:4F:27:E0	1500	RoMon: A11	6.43.12	RB952Ui-5ac2nD
64:D1:54:08:4C:54	400	2	D4:CA:6D:23:F8:A5, 64:D1:54:08:4C:54	1500	RoMon: A32	6.43.7	RB952Ui-5ac2nD
CC:2D:E0:11:8A:D9	400	2	D4:CA:6D:23:F8:A5, CC:2D:E0:11:8A:D9	1500	RoMon: A31	6.42.1	RB952Ui-5ac2nD



# Local Device Discovery across Routers

Discovery with RoMON, Connect by RoMON Winbox



Path to A32 as seen from agent R1

64:D1:54:08:4C:54	400	2	D4:CA:6D:23:F8:A5, 64:D1:54:08:4C:54	1500	RoMon: A32	6.43.7	RB952Ui-5ac2nD
-------------------	-----	---	--------------------------------------	------	------------	--------	----------------

1

2



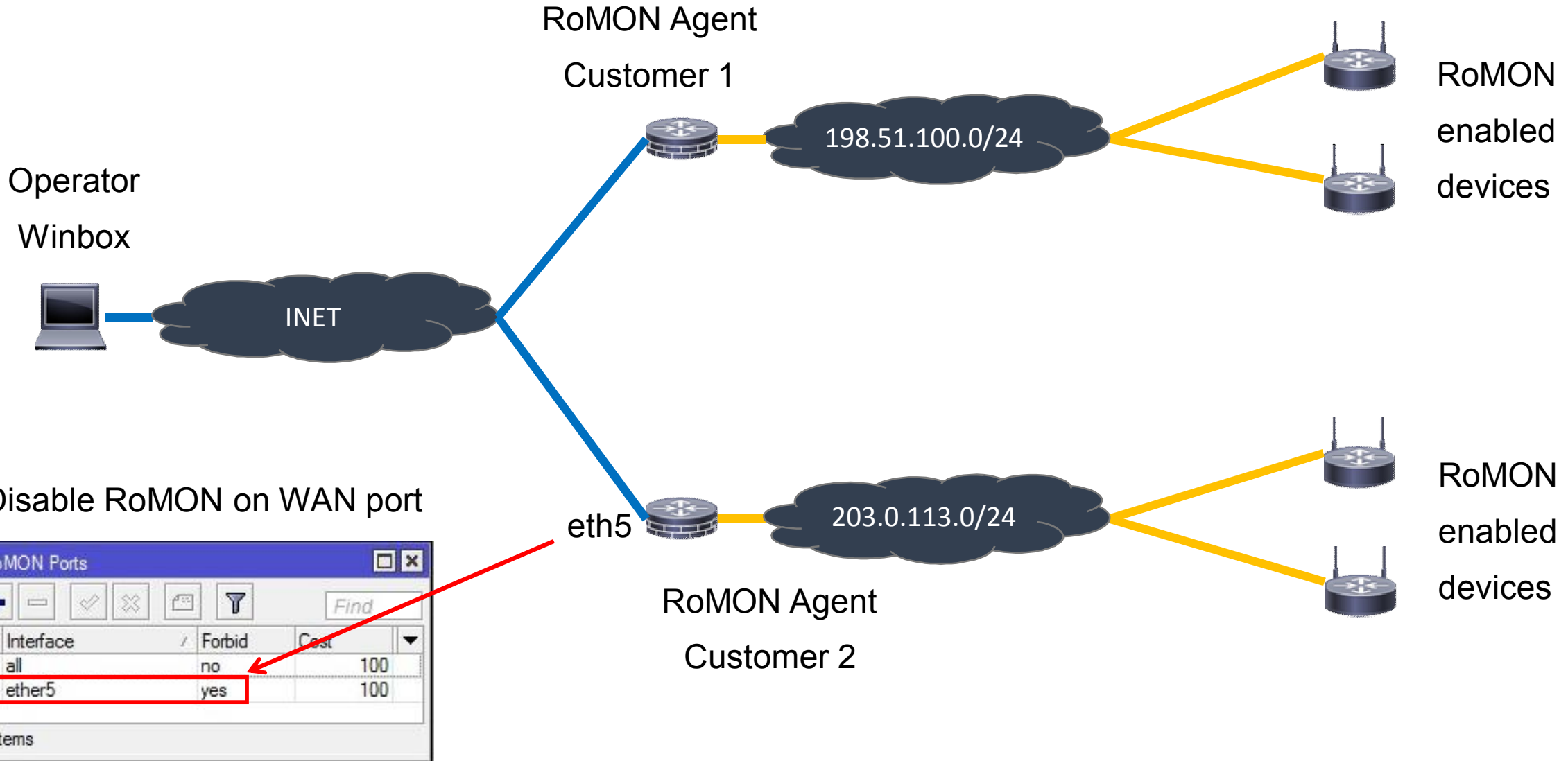
# Remote RoMON Agent

- RoMON agent connection by IP
- Across layer-3 network
- E.g. internet
- Remote discovery and management
- Branch offices
- Customer networks





# Remote Network Discovery





# Security Considerations

- Disable RoMON on WAN
- Don't enable Winbox on WAN
- Management VPN
  - VPN to reach RoMON agent
  - RoMON to reach remote devices
  - VLAN to limit RoMON locally







# HSNM Integration

With CLI and Scripting



# Hotspot Network Manager (HSNM)

- Commercial Captive Portal solution
- Tight MikroTik integration

- Management
- Monitoring

- /import
- Scripting host
- Scheduler

## HSNM Gateway

- MikroTik hotspot
- WAN/LAN gateway

## HSNM Accesspoint

- MikroTik WLAN access point



# MikroTik Gateway Integration

hsnm1.intern.fmsweb.de/#

**HSNM**  
Hotspot Manager

Admin Data Search

System

- FMS-Test-hbr
- FMS-Test2
- Reseller: Test GmbH
- Manager: Domain Templates
- Manager: nur Voucher
- Domain\_KN-23479**
- Gateway1
- Gateway2
- Gateway3
- Gateway4

**Default**

- Display All Users

**Edit**

  - Add Gateway**
  - Add User
  - Edit
  - Copy
  - Cut
  - Delete
  - Lock/Unlock

**Admin**

  - Card Management
  - Dashboard
  - Display All Connected Users
  - Display All Users
  - List of Access Points

Dashboard x Access Points Map x Gateway x Gateway

Connections  
Period Values  
3  
100%+

Traffic  
Period Values  
370.17 KB  
100%+

GW Sold  
Period Values  
\$ 1  
100%+

NET  
Traffic: Tx 0.01/F

of Connections — Welcome Portal Visitors



# Choosing Hardware and RouterOS Type

hsnm1.intern.fmsweb.de/#

**HSNM**  
Hotspot Manager

Admin Data Search

System

- FMS-Test-hbr
- FMS-Test2
- Reseller: Test GmbH
  - Manager: Domain Templates
  - Manager: nur Voucher
  - Domain\_KN-23479**
    - Gateway1
    - Gateway2
    - Gateway3

Dashboard Dashboard Dashboard Users Dashboard Access Points Map Gateway

## Gateway

Add or edit a hotspot gateway for the manager

### General Data

Gateway Name	Gateway6
Address	
ZIP Code	
City	
Country	Netherlands
Phone	
Mobile Phone	
Activate Logs	Disabled
Internet Connection IP Address or DynDNS Name	
URL or IP to Access the Web Management	
Hardware Type	Mikrotik (RBx, CCR, hAP, hAP Lite)
Gateway RouterOS Version	



# MikroTik Specific Settings: WAN

F

Fields for Configuring the Gateway

A

Authentication Options

W

Wireless

W

Wan

Same Network of the appliance

☐

Addressing Mode

Static IP or DHCP

▼

WAN Interface

ether1

▼

It uses a VLAN

☐

VLAN ID

It uses DHCP Client for the WAN

☐

WAN IP Address

WAN Network Mask

WAN Gateway



# MikroTik Specific Settings: MAC Auth + Hotspot

**F** Fields for Configuring the Gateway

**A** Authentication Options

Authentication via Mac Address ☐

**W** Wireless

**W** Wan

**H** Hotspot

**V** VPN

**S** Scheduler

**M** Mikrotik Router OS

**O** Options

**H** Hotspot

Add Ether2 to Hotspot Bridge ☐

Add Ether3 to Hotspot Bridge ☐

Add Ether4 to Hotspot Bridge ☐

Add Ether5 to Hotspot Bridge ☐

Add Ether6 to Hotspot Bridge ☐

Add Ether7 to Hotspot Bridge ☐

Add Ether8 to Hotspot Bridge ☐

Add Ether9 to Hotspot Bridge ☐

Add Ether10 to Hotspot Bridge ☐

Add Ether11 to Hotspot Bridge ☐

Add Ether12 to Hotspot Bridge ☐

Keep-Alive Timeout

IP Address

Network Mask

DNS IP Addresses

First IP Address for the DHCP Address Pool

Last IP Address for the DHCP Address Pool

DHCP Lease Time





# Initial Configuration

hsnm 1.intern.fmsweb.de/#

« HSNM Hotspot Manager

Admin Data Search

System

- FMS-Test-hbr
- FMS-Test2
- FMS-Test3
  - Domain1
  - FMS-Test
- Reseller: Test GmbH
- Manager: Domain Templates
- Manager: nur Voucher
- Domain\_KN-23479
  - Gateway1

Default

- Dashboard

Edit

- Add Printer
- Add Map, Zone or Floor
- Edit
- Cut
- Delete
- Lock/Unlock

Admin

- Connected Devices
- Display All Connected Users
- Display All Users who Used this Gateway
- Download Gateway Config Files
- Download Walled Garden
- Manufacturer's Management Interface

- Download .rsc
- Upload to MikroTik
- /import
- Initial configuration
- Scripting environment



# Scripting Environment

- Updating MikroTik gateway configuration
  - Changes of initial configuration will be transferred to gateway
- Importing data from HSNM
  - E.g. walled garden
- Exporting data to HSNM
  - E.g. User Manager accounts, GPS data
- Monitoring
  - Gateway and accesspoint availability



# Central Walled Garden

The screenshot shows the FMS management interface. On the left, a sidebar menu lists various domains and gateways. The 'Domain\_KN-23479' entry is highlighted in green. A red box highlights the hamburger menu icon next to it. A red arrow points from this icon to the 'Walled Garden' option in the main menu on the right. The main menu includes options like 'Display All Users', 'List of Access Points', 'List of Gateways', 'Map of the Gateways', 'Sales to Users', 'Tools for Managing Data', 'Voucher Management', 'Welcome portal', 'Custom Apps', 'Custom Images', 'Surveys, Quizzes and Tests', 'Templates', 'Translations', and 'Walled Garden'.

The screenshot shows the 'Walled Garden' configuration page. The title is 'Walled Garden' and the subtitle is 'List the of walled gardens for the domain: Domain\_KN'. Below the title is a table with columns: Destination Host, Port, Allow, and P. The table contains three rows of data.

Destination Host	Port	Allow	P
*.fmsweb.de	80	●	≡
*.mikrotik-shop.de	80	●	≡
*.mikrotik-shop.de	443	●	≡

- Domain or gateway level
- Automatic import by script



# Seamless Integration of legacy Solutions

1

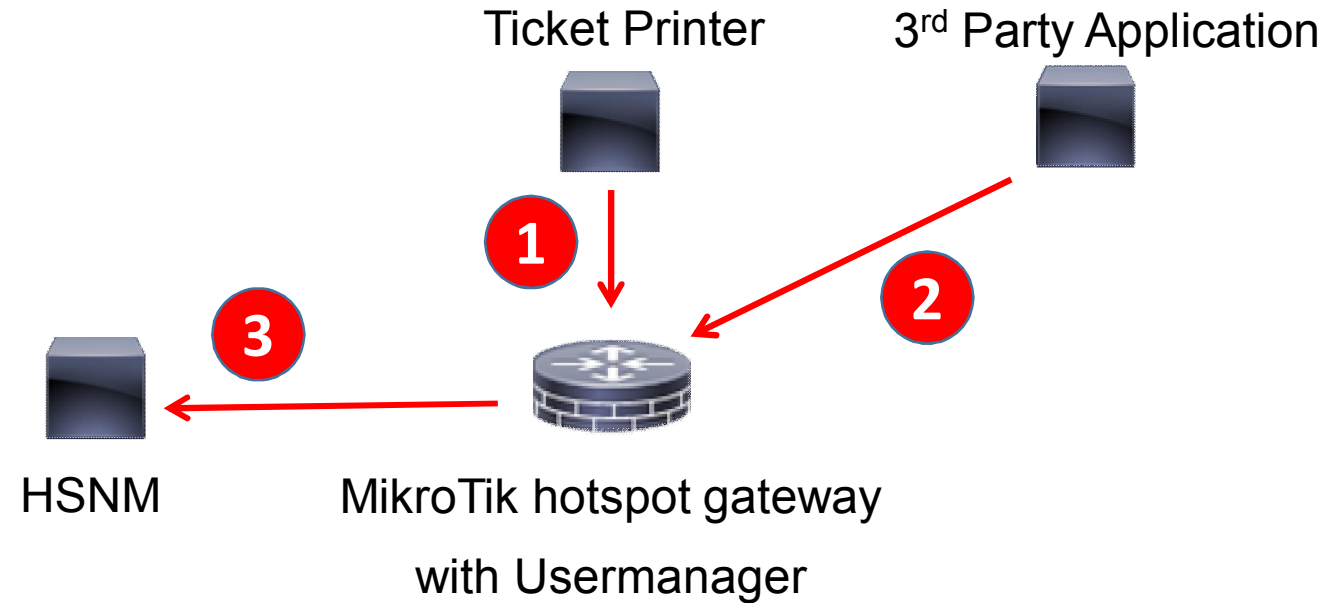
Legacy ticket printer  
Creating Usermanager accounts

2

Legacy 3<sup>rd</sup> party application  
Creating Usermanager accounts

3

Exporting UM accounts to HSNM  
Deleting UM accounts locally





# GPS based Maps and Tracking

G

Geolocation and tracking

Longitude	<input type="text" value="5.2912660"/>
Latitude	<input type="text" value="52.1326330"/>
GPS Coordinate Storing	<input checked="" type="checkbox"/>
Keep the GPS Data for	<input type="text" value="1 Hour"/>

- Script sends GPS location
- Can be stored in HSNM
- Tracking of moving gateways
- E.g. busses, trains, taxis
- Static GPS location
- Can be entered in HSNM
- Visualisation of gateway location

- Reseller: Test GmbH
- Manager: Domain Templates
- Manager: nur Voucher
- Domain\_KN-23479
  - Gateway1
  - Gateway2
  - Gateway3
  - Gateway4
  - Gateway5
- Domain\_KN-73942
- Manager: Voucher und Paypal
- Manager: Voucher und Paysafe

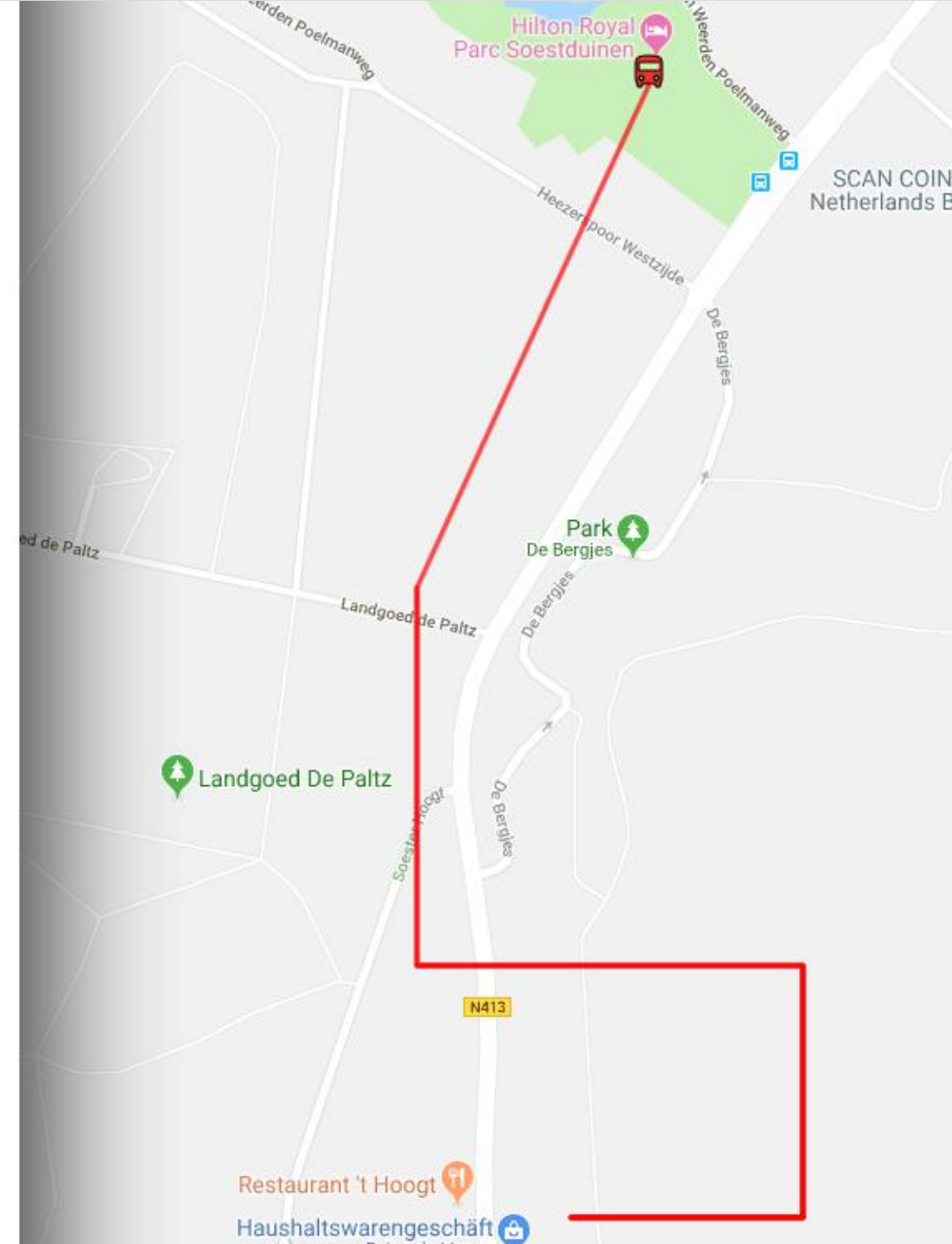
- Cut
- Delete
- Lock/Unlock

### Admin

- Connected Devices
- Display All Connected Users
- Display All Users who Used this Gateway
- Download Gateway Config Files
- Download Walled Garden
- Gateway Route
- List of Access Points
- Map of the Gateways
- User Traffic Log

### Welcome portal

- Bypass or Lock IP/Mac Address
- Custom Apps
- Custom Images
- Surveys, Quizzes and Tests
- Templates
- Translations
- User Interface Preview
- Walled Garden

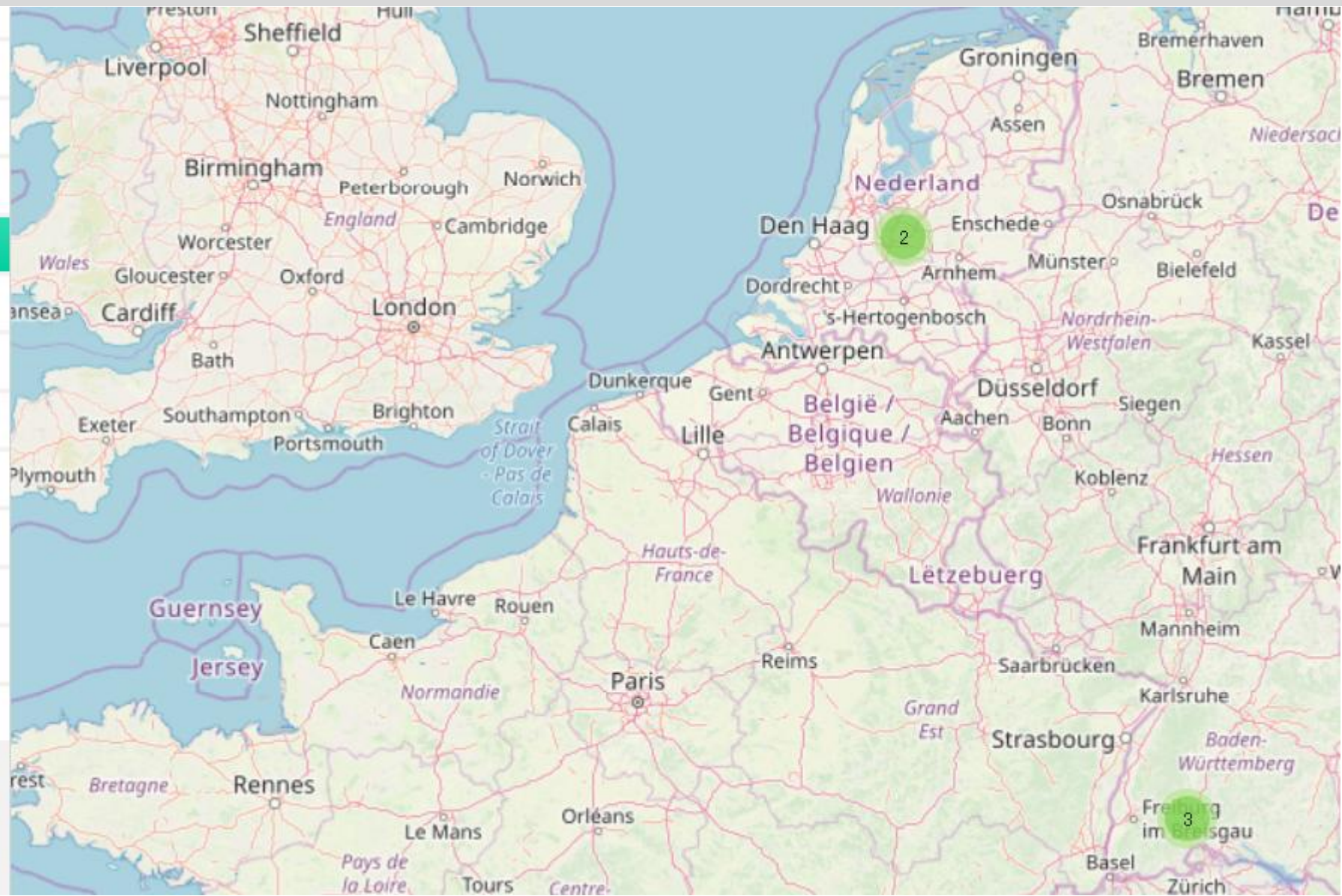






# Hotspot Network Manager (HSNM)

- ▶ FMS-Test2
- ▶ Reseller: Test GmbH
- ▶ Manager: Domain Templates
- ▶ Manager: nur Voucher
- ▶ **Domain\_KN-23479**
  - ▶ Gateway1
  - ▶ Gateway2
  - ▶ Gateway3
  - ▶ Gateway4
  - ▶ Gateway5
- ▶ Domain\_KN-73942
- ▶ Manager: Voucher und Paypal
- ▶ Manager: Voucher und Paysafe








# Manual Positioning on Floor Plans and Maps

- Manual positioning
- Gateways & access points
- Maps or plans
- Coverage (in m)

## Access Points Map

Management of access points on the map or on the floor



Dashboard

Map, Zone or Floor

Access Points Map

Access Points Map

Gateway

Access point


Map, Zone or Floor

Gateway

## Access point

List of access point for the gateway: Gateway1

	S	ID	Retailer	Manager	Domain	Gateway	Zone	AccessPointName	P
▶	●	2	Reseller: Test GmbH	Manager: nur Voucher	Domain_KN-23479	Gateway1	FMS	AccessPoint2	≡
▶	●	4	Reseller: Test GmbH	Manager: nur Voucher	Domain_KN-23479	Gateway1	FMS	Main-Warehouse-AP-1	≡
▶	●	3	Reseller: Test GmbH	Manager: nur Voucher	Domain_KN-23479	Gateway1	FMS	OfficeBuildingAP-1	≡
▶	●	1	Reseller: Test GmbH	Manager: nur Voucher	Domain_KN-23479	Gateway1	FMS	Storage-Depot-AP-1	≡
▶	●	16	Reseller: Test GmbH	Manager: nur Voucher	Domain_KN-23479	Gateway1	FMS	Training-Center-AP-1	≡





# Hotspot Network Manager (HSNM)

hsnm1.intern.fmsweb.de

**HSNM**  
Hotspot Manager

Admin Data Search

System

- FMS-Test-hbr
- FMS-Test2
- Reseller: Test GmbH
- Manager: Domain Templates
- Manager: nur Voucher
- Domain\_KN-23479
  - Gateway1
  - Floor-1**
  - Floor-2**
  - Gateway2
  - Gateway3
  - Gateway4
  - Gateway5
- Domain\_KN-73942
- Manager: Voucher und Paypal
- Manager: Voucher und Paysafe

**Default**

- Access Point Map

**Edit**

- Edit
- Copy
- Cut
- Delete

**Admin**

- List of Access Points

Access Point Map



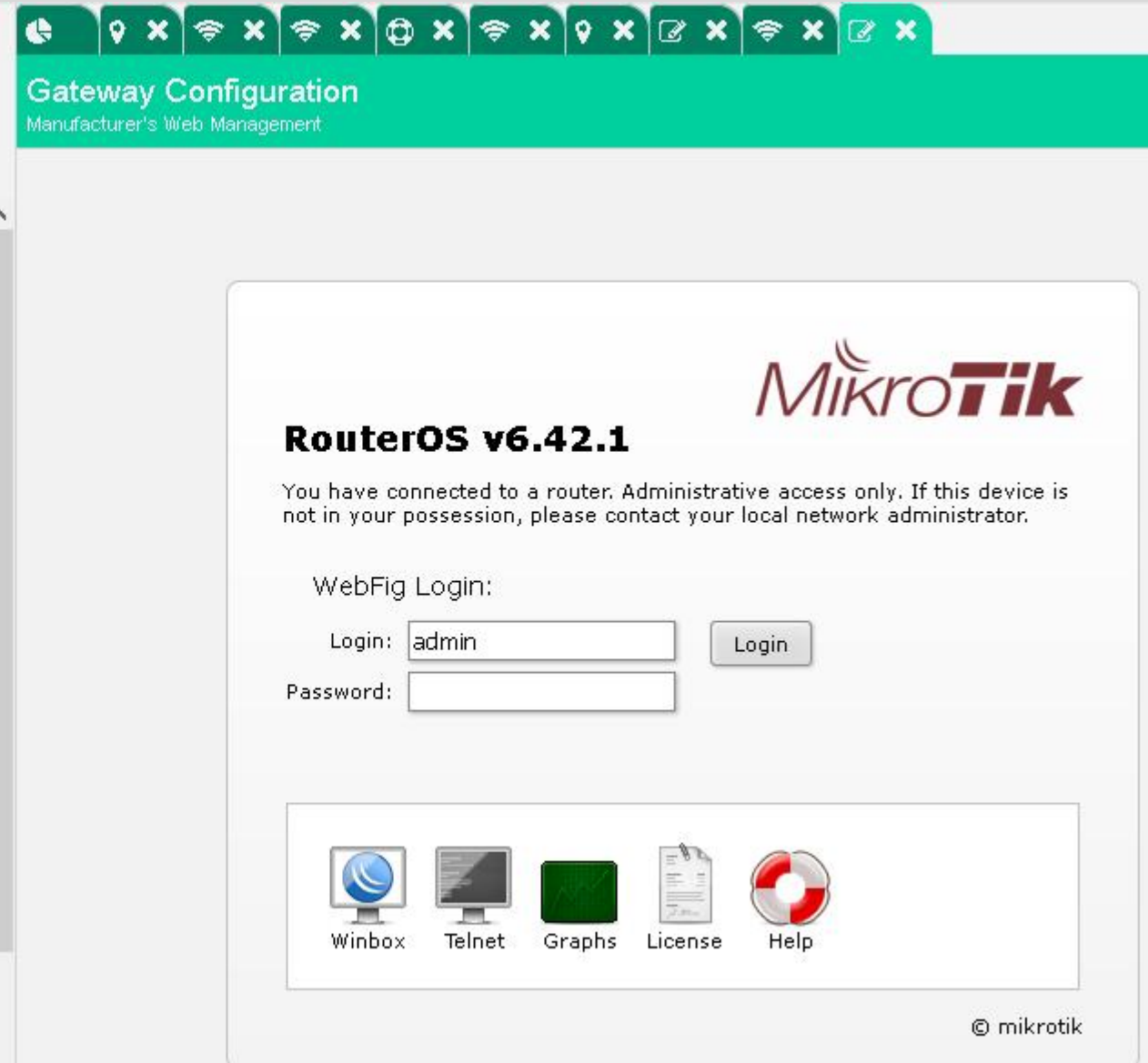
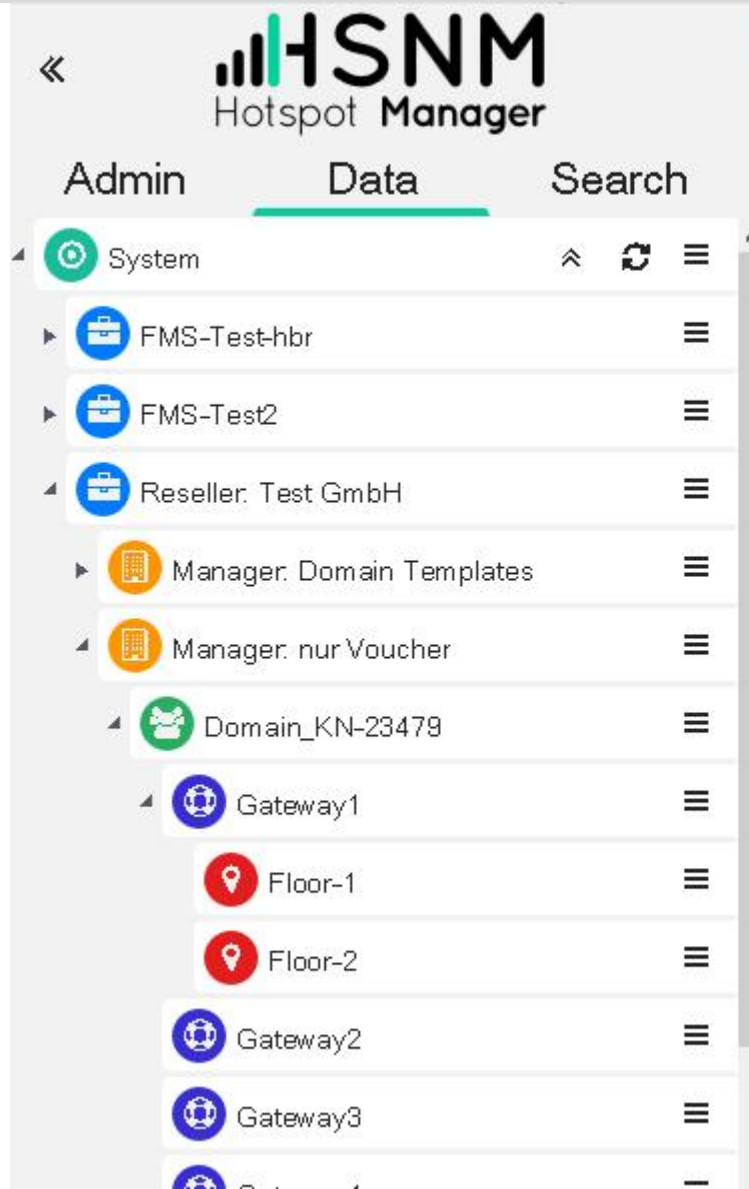


Access point  
context menu



# Hotspot Network Manager (HSNM)

Direct web  
interface access  
for gateways and  
access points





# Monitoring (HSNM)

- Availability and latency
- Captive portal related values
  - Bandwidth
  - Amount of transferred data
  - Number of connected users
  - Number of registrations



## Get in Touch

Are you looking for a powerful  
captive portal solution?

+49 761 2926500 | [sales@fmsweb.de](mailto:sales@fmsweb.de) | Web form



# Network Monitoring

Tracking Packets and Flows





# Packet Sniffer

Last Resort for Networking Problems



# Network Debugging

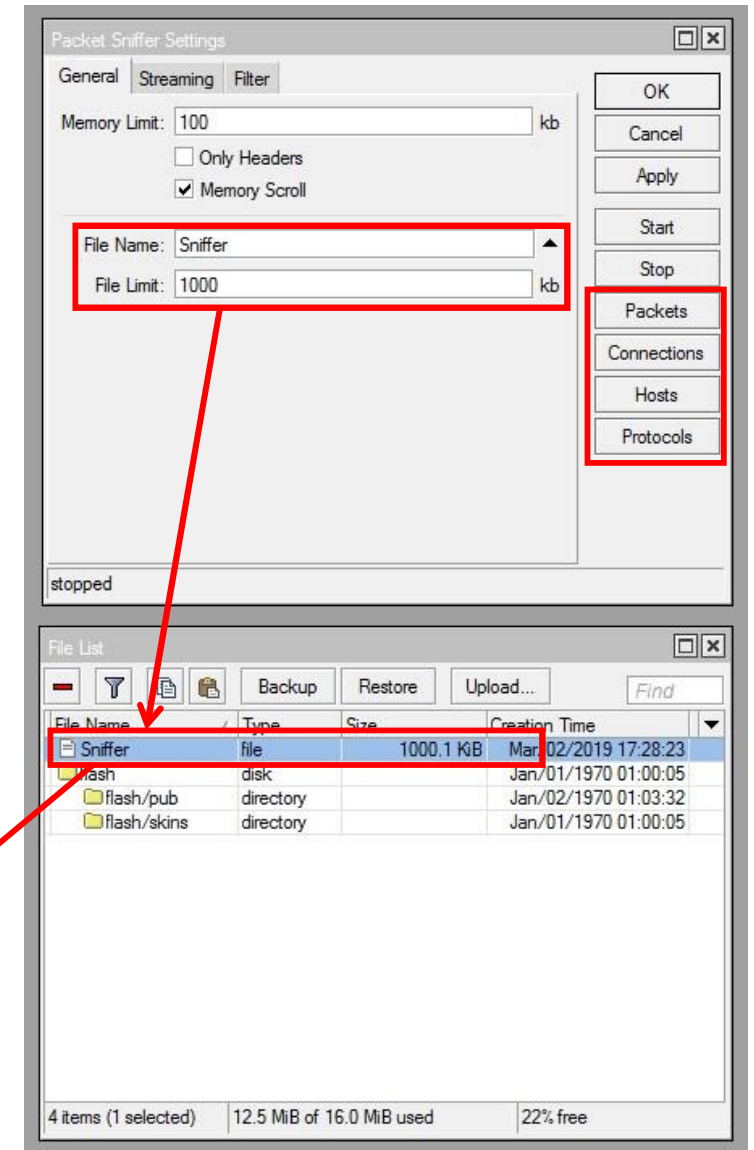
- Planning / checking firewall settings
- Networking problems
- Faulty client / server applications
  
- Things go wrong?
- Real insight is necessary
  
- Packet sniffing
- De facto standard: Wireshark
- RouterOS packet sniffer





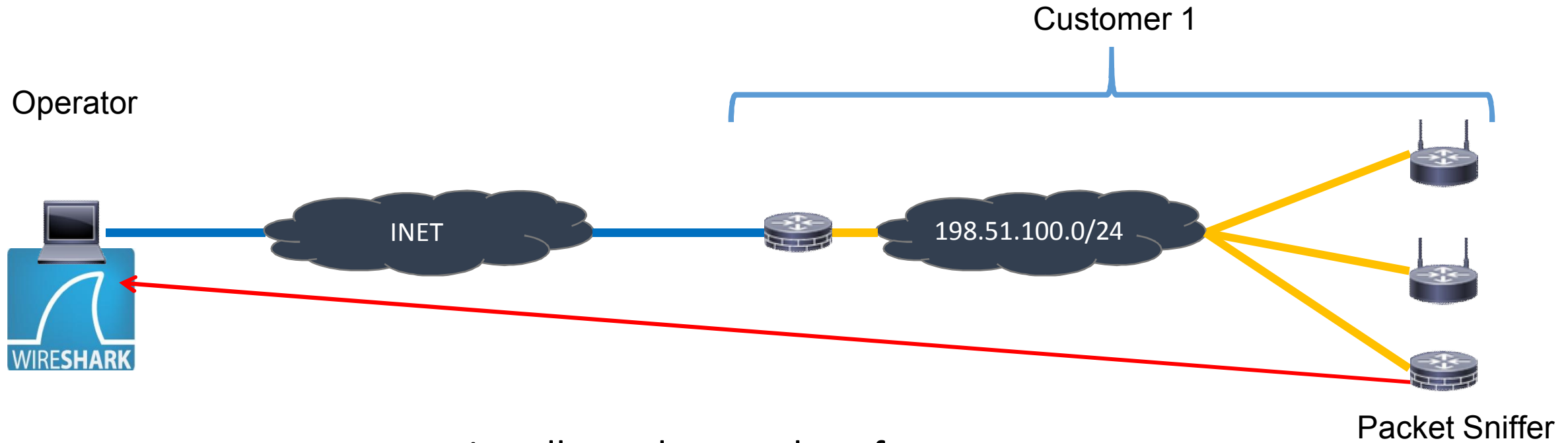
# MikroTik Packet Sniffer

- General settings
- Filter
- Start/Stop
- Results in CLI / Winbox
- Results in file, analyse in Wireshark
- Streaming to Wireshark





# Remote Packet Sniffing

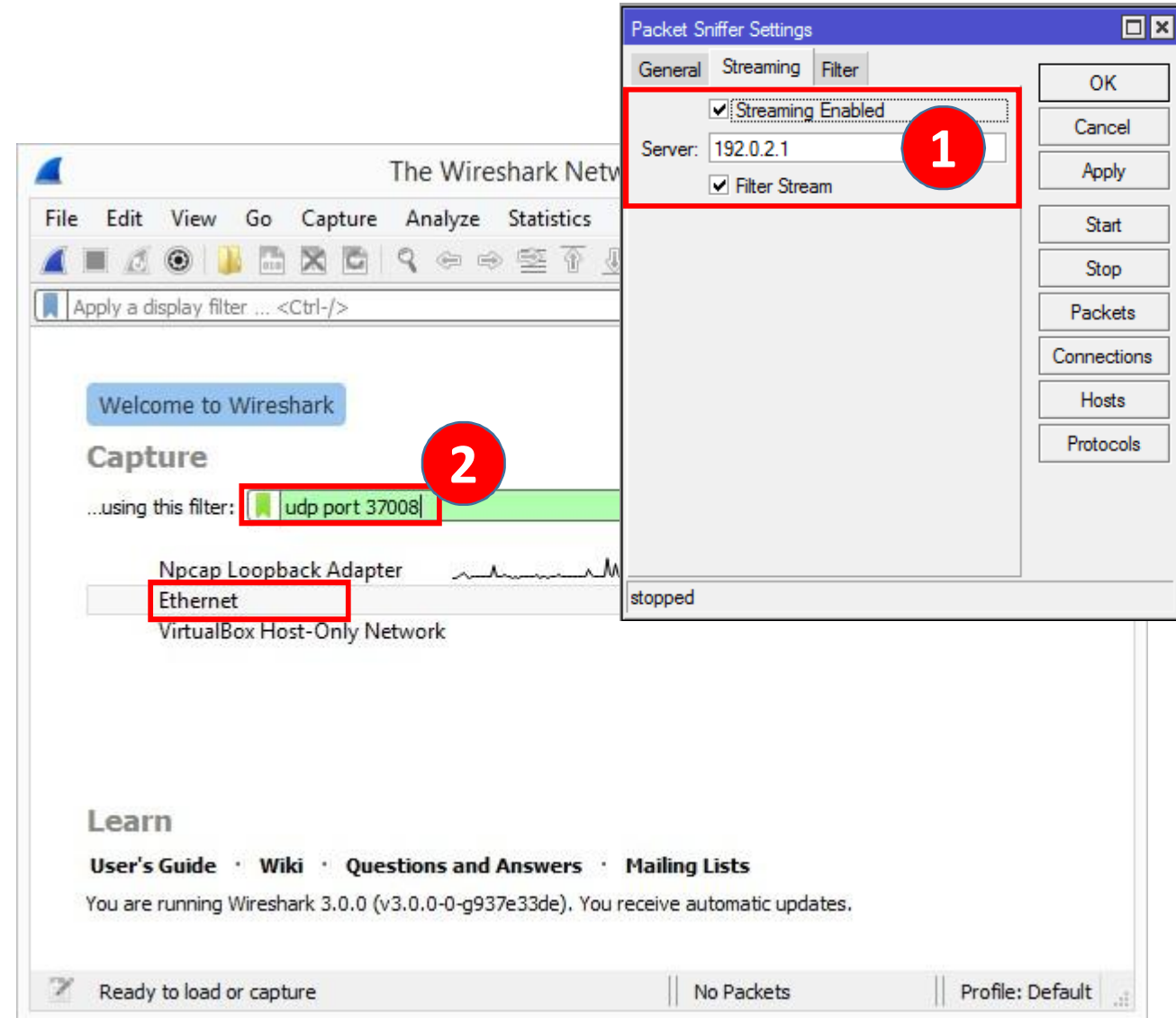


Locally analyse packets from  
a remote sniffer in real time



# Sniffer Stream

- Enable “Stream”
- Set Wireshark host IP
- Enable “Filter Stream”
- TZSP stream is sent
- Filter stream in Wireshark
- UDP port 37008
- Start sniffer in Winbox





# Live Output

Capturing from Ethernet (udp port 37008) **1**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + RoMon

No.	Time	Source	Destination	Protocol	Length	Info
344	270.061314	Routerbo_0d:1c:10	CDP/VTP/DTP/PAgP/UDLD	CDP	153	Device ID: RoMon: A21 Port ID: ether1
345	270.061315	Routerbo_0d:1c:10	LLDP_Multicast	LLDP	161	TTL = 120 SysName = RoMon: A21 SysDesc = MikroTik RouterOS 6.42.7 (st
346	271.725033	Routerbo_23:f8:a5	Spanning-tree-(for-bridges)_88:bf	0x88bf	109	PRI: 0 DEI: 0 ID: 1
347	271.740971	Routerbo_4f:28:5a	Spanning-tree-(for-bridges)_00	STP	100	RST. Root = 32768/0/64:d1:54:4f:28:5a Cost = 0 Port = 0x8001
348	272.386686	Routerbo_4f:28:5a	Spanning-tree-(for-bridges)_88:bf	0x88bf	105	Ethernet II
349	272.523252	203.0.113.253	255.255.255.255	MNDP	194	5678 → 5678 Len=105
350	272.523253	Routerbo_23:f8:a5	CDP/VTP/DTP/PAgP/UDLD	CDP	152	Device ID: RoMon: R2 Port ID: ether1
351	272.523490	Routerbo_23:f8:a5	LLDP_Multicast	LLDP	159	TTL = 120 SysName = RoMon: R2 SysDesc = MikroTik RouterOS 6.42.6 (sta
352	272.523491	0.0.0.0	255.255.255.255	MNDP	197	5678 → 5678 Len=104
353	272.523725	Routerbo_23:f8:a5	CDP/VTP/DTP/PAgP/UDLD	CDP	138	Device ID: RoMon: R2 Port ID: vlan1
354	272.523834	Routerbo_23:f8:a5	LLDP_Multicast	LLDP	148	TTL = 120 SysName = RoMon: R2 SysDesc = MikroTik RouterOS 6.42.6 (sta

4 Mikrotik Neighbor Discovery Protocol

- Header Unknown: 0000
- SeqNo: 251
- 4 T 1, L 6: MAC-Address
  - TlvType: 1 = MAC-Address
  - TlvLength: 6
  - MAC-Address: Routerbo\_23:f8:a5 (d4:ca:6d:23:f8:a5)
- 4 T 5, L 9: Identity
  - TlvType: 5 = Identity
  - TlvLength: 9
  - Identity: RoMon: R2
- 4 T 7, L 15: Version

Ethernet: <live capture in progress> | Packets: 593 · Displayed: 593 (100.0%) | Profile: Default



# Traffic Flow

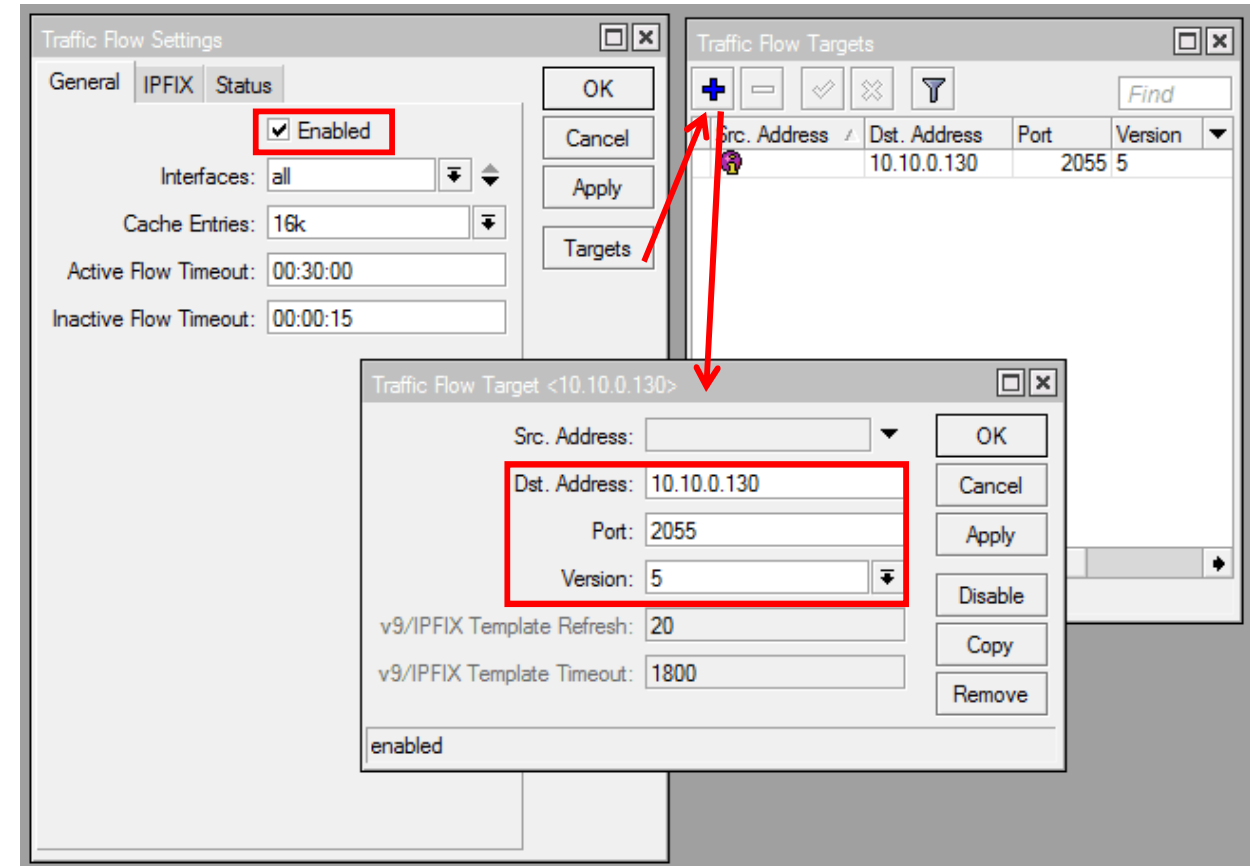
Statistical Network Information





# Traffic Flow

- Compatible with Netflow
- Statistical network information
  - Byte and packet counter
  - Source and destination IP addresses
  - Source and destination ports
- Top talkers
- Top protocols
- Utilisation

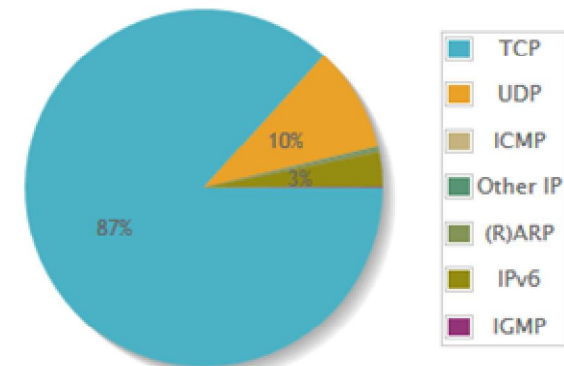




# Netflow Collector and Analysis

- ntop (former) free standard
- Successor ntop-ng
- Requires commercial nProbe to collect Netflow
- Alternative free and open source collectors available
- E.g as in FMS Management Plattform

L2/L3 Protocol	Data	Percentage			
IP	905.6 KBytes	96.4%	TCP	834.7 KBytes	92.2%
			UDP	92.5 KBytes	10.2%
			ICMP	0.4 KBytes	0.0%
			ICMPv6	5.1 KBytes	0.6%
			IGMP	0.9 KBytes	0.1%
			Other IP	1.6 KBytes	0.0%
(R)ARP	2.9 KBytes	0.3%			
IPv6	29.6 KBytes	3.2%			

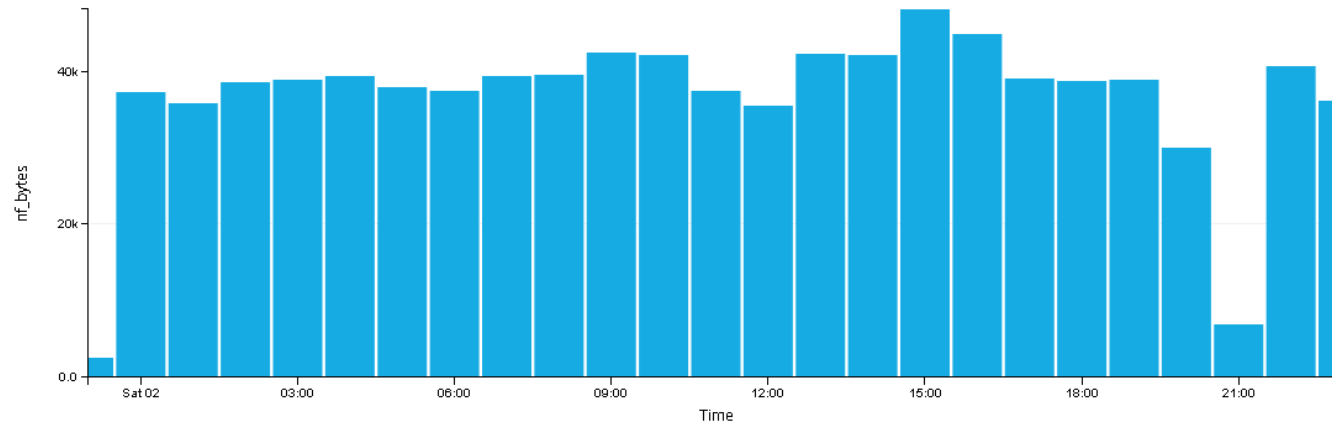


Former ntop GUI

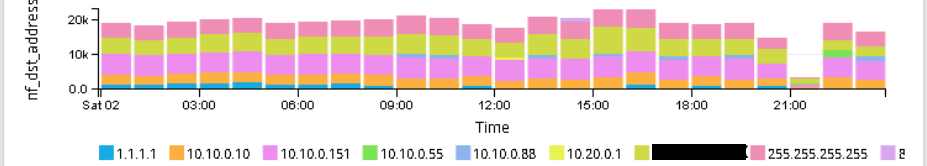


# Netflow in FMS Management Plattform

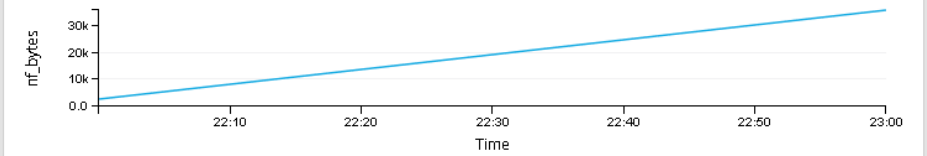
Bytes (last day)



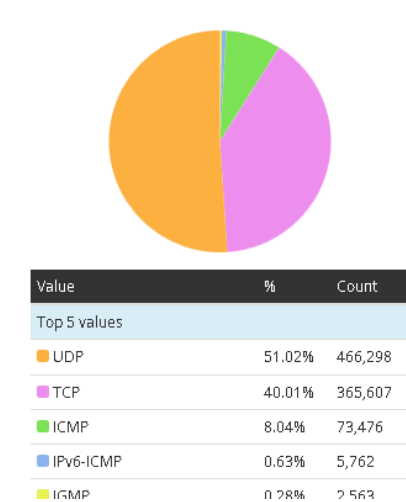
Destinations (last day)



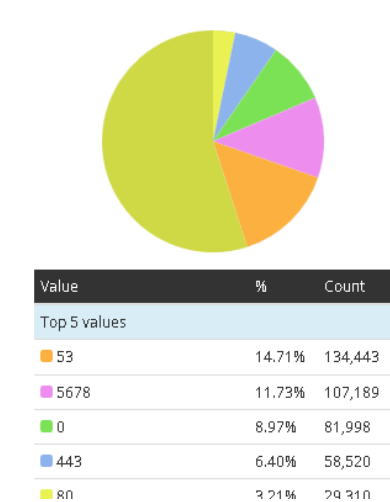
Bytes (last hour)



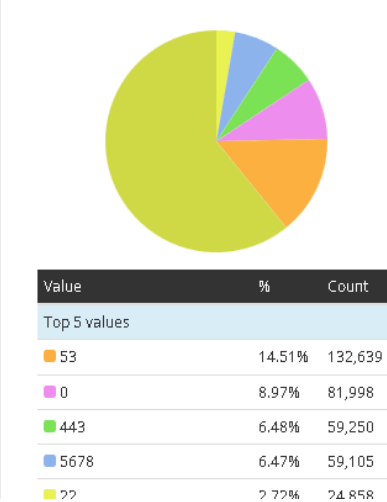
Protocols (last day)



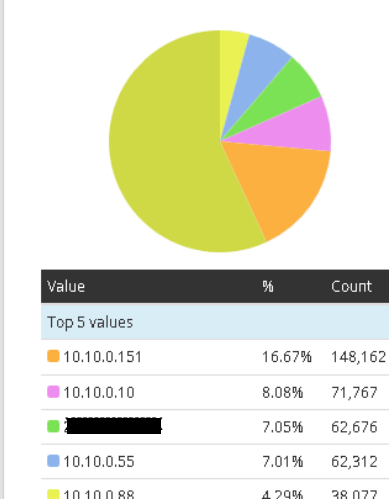
Destination Ports (last day)



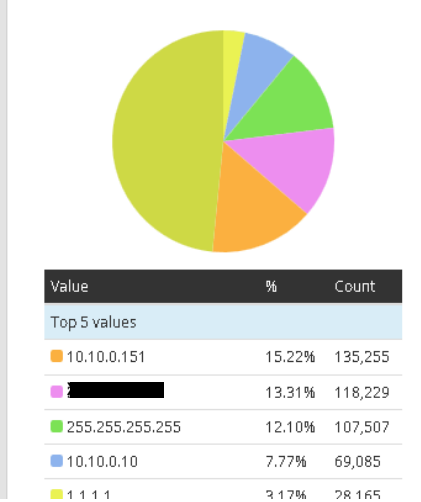
Source Ports (last day)



Sources (last day)



Destinations (last day)





# RouterOS Monitoring

Tracking Events



# Local RouterOS Logging

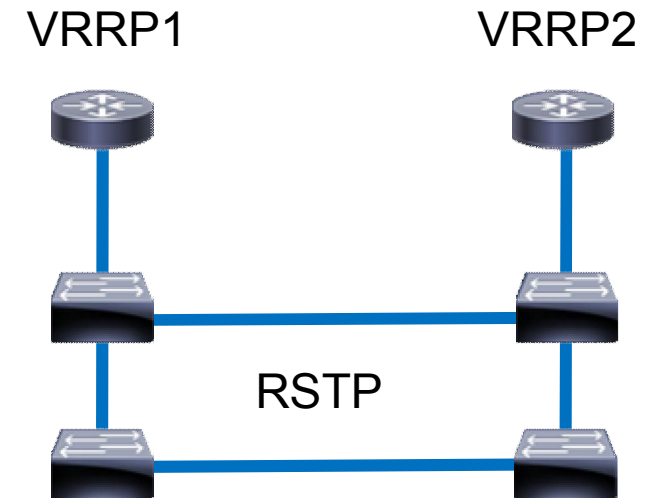
- Source for network debugging = packets and packet statistics
- Source for device debugging = local status information
- SNMP
- Local logging

Log			
Freeze			
all			
Mar/03/2019 22:01:56	memory	system, info	system time zone settings changed by admin
Mar/03/2019 21:02:02	memory	system, info	device changed by admin
Mar/03/2019 21:02:03	memory	route, debug, event	Interface change
Mar/03/2019 21:02:03	memory	route, debug, event	interface=wlan1
Mar/03/2019 21:02:03	memory	route, debug, event	status=UP
Mar/03/2019 21:02:03	memory	route, debug, event	mtu=1500
Mar/03/2019 21:02:03	memory	system, info	device changed by admin
Mar/03/2019 21:02:03	memory	route, debug, calc	Begin calculation
Mar/03/2019 21:02:03	memory	route, debug, event	Update
Mar/03/2019 21:02:03	memory	route, debug, event	interface=wlan1
Mar/03/2019 21:02:03	memory	route, debug, calc	End calculation
Mar/03/2019 21:05:56	memory	ntp, debug, packet	sending to 10.10.0.10 NTP packet (48 bytes)
Mar/03/2019 21:05:56	memory	ntp, debug, packet	VN=4
Mar/03/2019 21:05:56	memory	ntp, debug, packet	Mode=3 (Client)
Mar/03/2019 21:05:56	memory	ntp, debug, packet	TransmitTimestamp=e026c03492d6a9c5
Mar/03/2019 21:05:56	memory	ntp, debug	Wait for 900 seconds before sending next message
Mar/03/2019 21:05:56	memory	ntp, debug, packet	received NTP packet (48 bytes)
Mar/03/2019 21:05:56	memory	ntp, debug, packet	LI=0
Mar/03/2019 21:05:56	memory	ntp, debug, packet	VN=4
Mar/03/2019 21:05:56	memory	ntp, debug, packet	Mode=4 (Server)
Mar/03/2019 21:05:56	memory	ntp, debug, packet	Stratum=3 (Secondary Reference)
Mar/03/2019 21:05:56	memory	ntp, debug, packet	Poll=3
Mar/03/2019 21:05:56	memory	ntp, debug, packet	Precision=-19
Mar/03/2019 21:05:56	memory	ntp, debug, packet	RootDelay=b45
Mar/03/2019 21:05:56	memory	ntp, debug, packet	RootDispersion=13bc
Mar/03/2019 21:05:56	memory	ntp, debug, packet	ReferenceID=5bca2a52
Mar/03/2019 21:05:56	memory	ntp, debug, packet	ReferenceTimestamp=e026c0358c9bc6bb
Mar/03/2019 21:05:56	memory	ntp, debug, packet	OriginateTi
Mar/03/2019 21:05:56	memory	ntp, debug, packet	mestamp=e026c03492d6a9c5
Mar/03/2019 21:05:56	memory	ntp, debug, packet	ReceiveTimestamp=e026c0358c9bc6bb
Mar/03/2019 21:05:56	memory	ntp, debug, packet	TransmitTimestamp=e026c0358cb2a1e1
Mar/03/2019 21:05:57	memory	ntp, debug	instantly adjust by f9668964
Mar/03/2019 21:07:14	memory	system, info	log action changed by admin
Log Output			
Mar/03/2019 21:13:52	memory	system, info, account	user admin logged out from 10.10.0.55 via telnet
Mar/03/2019 21:07:19	memory	system, info	log action changed by admin



# Central Syslog

- External, central syslog server
  - Will survive reboots / crashes
  - No tampering from device
  - Better search
  - Correlation across devices
- 
- Example: Investigate VRRP change
  - Involved: Master, slave, crosslink switch



VRRP Setup



# FMS Management Platform

- Syslog, Netflow, SNMP traps ...
- MongoDB, Elasticsearch ...
- Central storage
- Powerful search
- Dashboards
- Alerts
- Enhanced MikroTik support
- E.g. MikroTik MIB, Log syntax

The screenshot displays the FMS Management Platform interface. A 'Log Action <FMSMP>' configuration window is open, showing fields for Name (FMSMP), Type (remote), Remote Address (10.10.0.130), Remote Port (5140), Src. Address (10.10.0.130), and Syslog Facility (3 (daemon)). A red box highlights the 'Type', 'Remote Address', and 'Remote Port' fields. A red dashed box highlights the 'Syslog Facility' and 'Syslog Severity' fields, with a red question mark next to the 'Syslog Facility' dropdown. A red arrow points from the 'FMSMP' entry in the 'Logging' table to the 'Log Action <FMSMP>' window. Another red arrow points from the 'Syslog Facility' dropdown to the 'Syslog Severity' dropdown.

Logging

Rules Actions

	Topics	Prefix	Action
*	critical		echo
	debug		memory
*	error		memory
*	info		memory
	system		FMSMP
*	warning		memory

Find

6 items

Remote Syslog Configuration



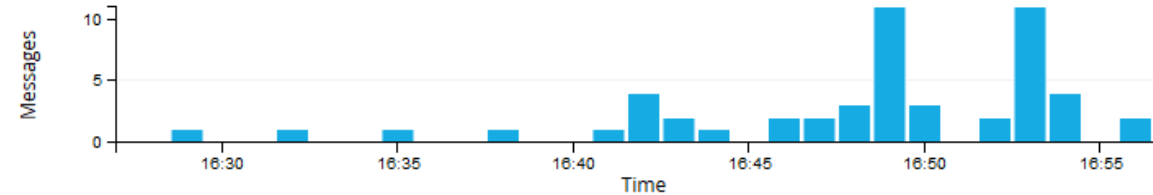


# WIFI Connects from Syslog across complete Network

WLAN Connections (last 1/2 hour)

52

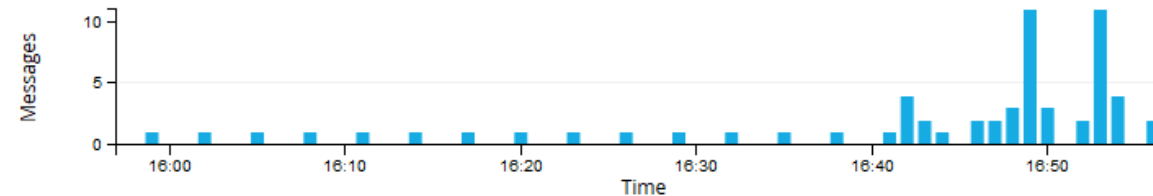
WLAN Connections (last 1/2 hour)



WLAN Connections (last hour)

62

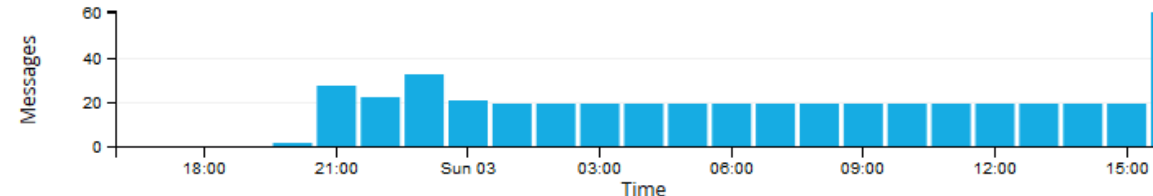
WLAN Connections (last hour)



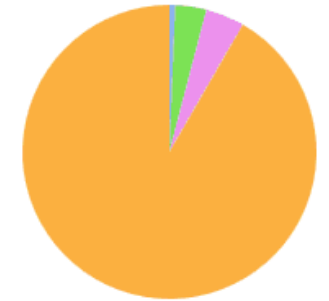
WLAN Connections (last day)

468

WLAN Connections (last day)



Connections by Access Point (last day)



Value	%	Count
Top 5 values		
10.10.0.40	91.67%	429
10.10.0.29	4.27%	20
10.10.0.128	3.42%	16
10.10.0.22	0.64%	3



# Enhanced Log Message Processing

- Make syslog server understand message
- Database fields
- Search
- Sorting
- Analyse
- Login Failure Dashboard

1

system,error,critical login failure for user admin from 10.10.0.55 via web

## Messages

Timestamp ↑	source	mikrotik_login_via	user_name
2019-03-03 16:40:13.301	10.10.0.117	web	admin
system,error,critical login failure for user admin from 10.10.0.55 via web			
2019-03-03 16:40:11.108	10.10.0.117	web	admin
system,error,critical login failure for user admin from 10.10.0.55 via web			
2019-03-03 16:40:02.177	10.10.0.117	winbox	admin
system,error,critical login failure for user admin from 10.10.0.55 via winbox			
2019-03-03 16:39:59.675	10.10.0.117	winbox	admin
system,error,critical login failure for user admin from 10.10.0.55 via winbox			
2019-03-03 16:39:57.419	10.10.0.117	winbox	admin
system,error,critical login failure for user admin from 10.10.0.55 via winbox			
2019-03-03 16:39:08.902	10.10.0.117	ftp	root
system,error,critical login failure for user root from 10.10.0.55 via ftp			



# Failed Logins including Username and Login Type

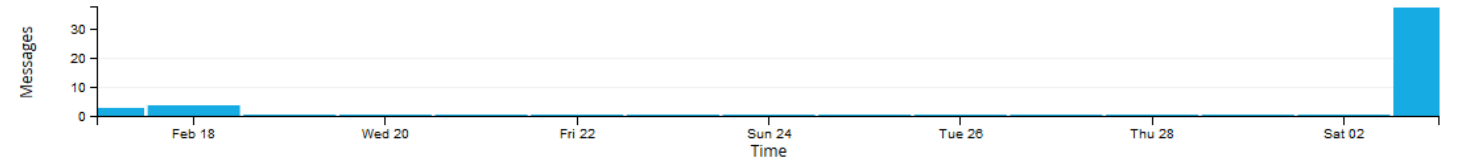
Login Failed (last hour)

37

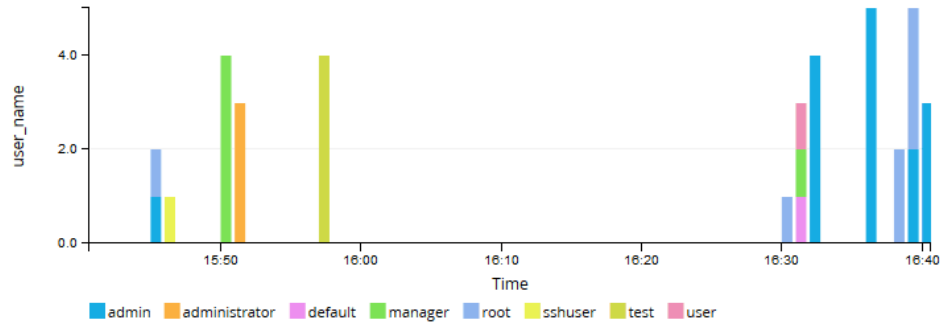
Logins failed (last 7 days)

44

Logins Failed (last 7 days)



Login failed by Username (last hour)



Logins failed (last 7 days)



Value	%	Count
Top 5 values		
10.10.0.117	87.04%	47
10.10.0.10	12.96%	7

Login failed by Username (last 7 days)



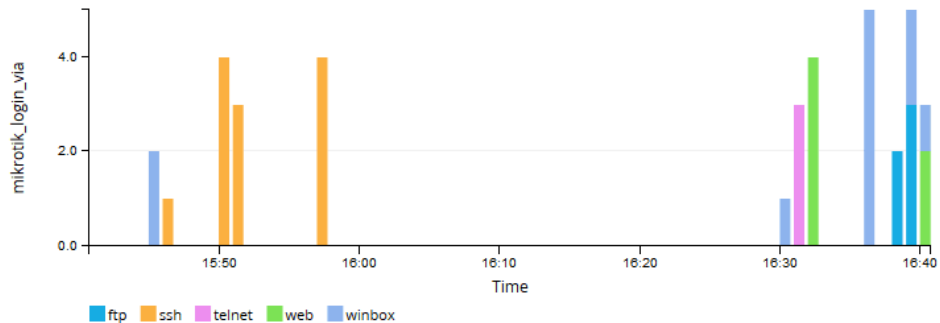
Value	%	Count
Top 5 values		
admin	40.54%	15
root	18.92%	7
manager	13.51%	5
test	10.81%	4
administrator	8.11%	3

Login failed by Login Type (last 7 days)



Value	%	Count
Top 5 values		
ssh	32.43%	12
winbox	29.73%	11
web	16.22%	6
ftp	13.51%	5
telnet	8.11%	3

Login failed by Login Type (last hour)





## Get in Touch

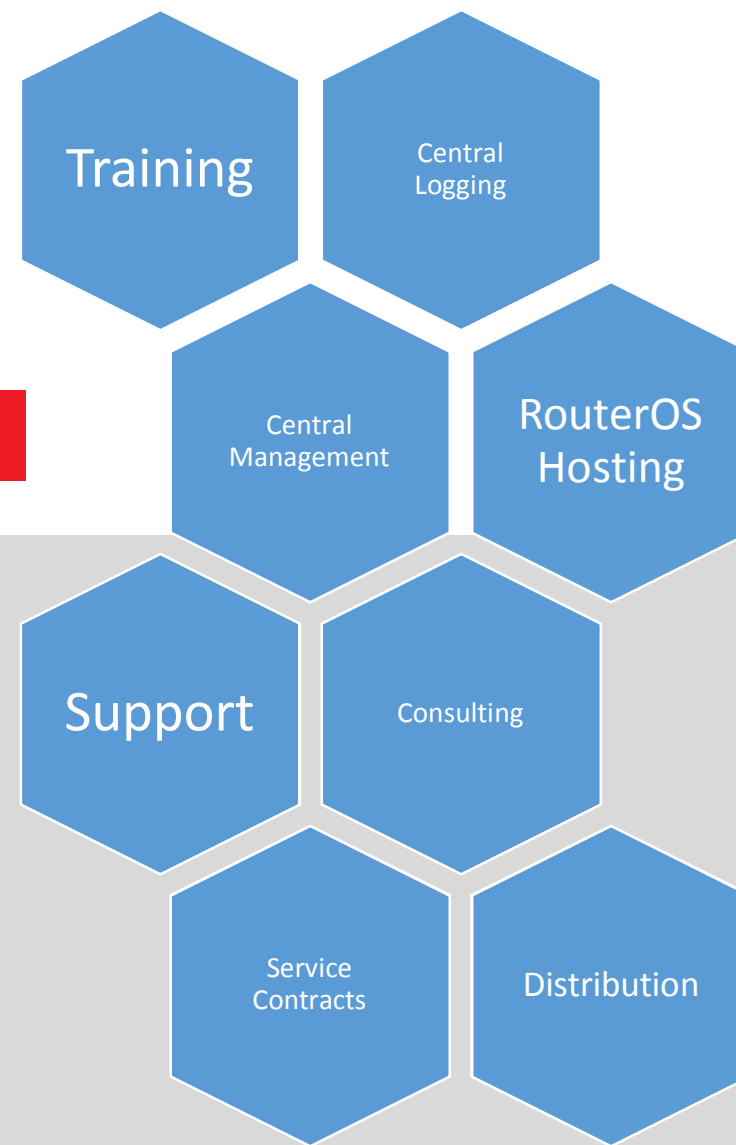
Are you looking for centralised  
and MikroTik aware logging?

+49 761 2926500 | [sales@fmsweb.de](mailto:sales@fmsweb.de) | Web form



+49 761 2926500 | [sales@fmsweb.de](mailto:sales@fmsweb.de) | Web form

[www.fmsweb.de](http://www.fmsweb.de) | [www.mikrotik-shop.de](http://www.mikrotik-shop.de)





Dank u wel!