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

MikroTik Training Partner since 2007

See Training Schedule

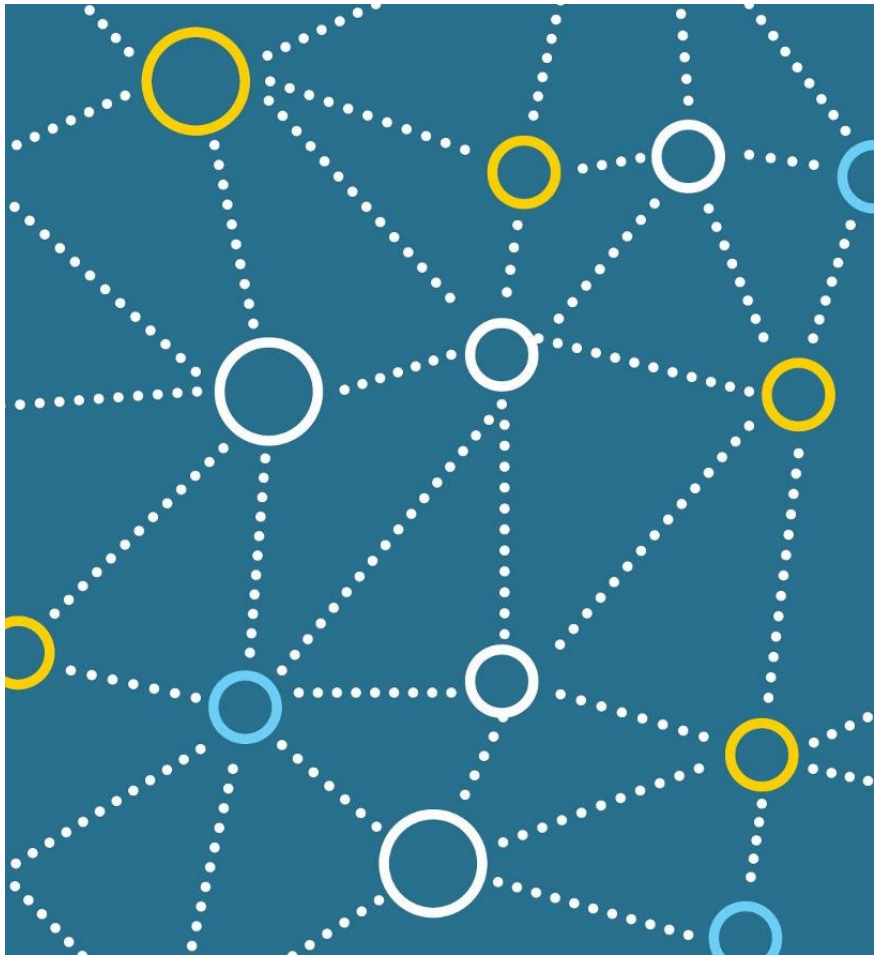
Network Operation – Big Picture

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
- Management
- Debugging
- 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 ressources
- /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 & 3rd Party Integration

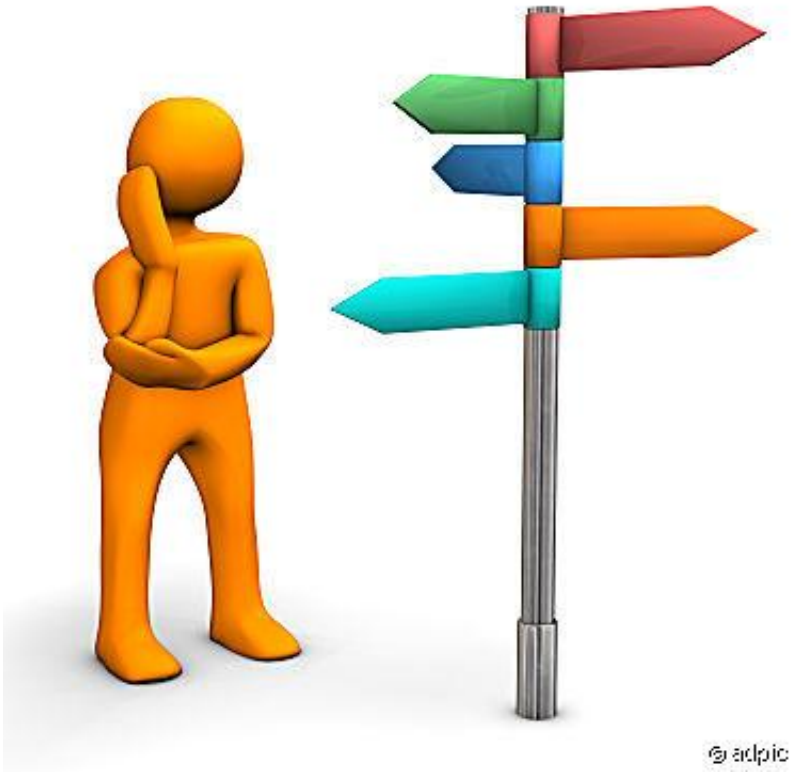
- IP Accounting
- Traffic Flow (Netflow)
- SNMP
- Graphing
- Syslog
- TR069

Management Topologies

Secure and Convenient Management Access

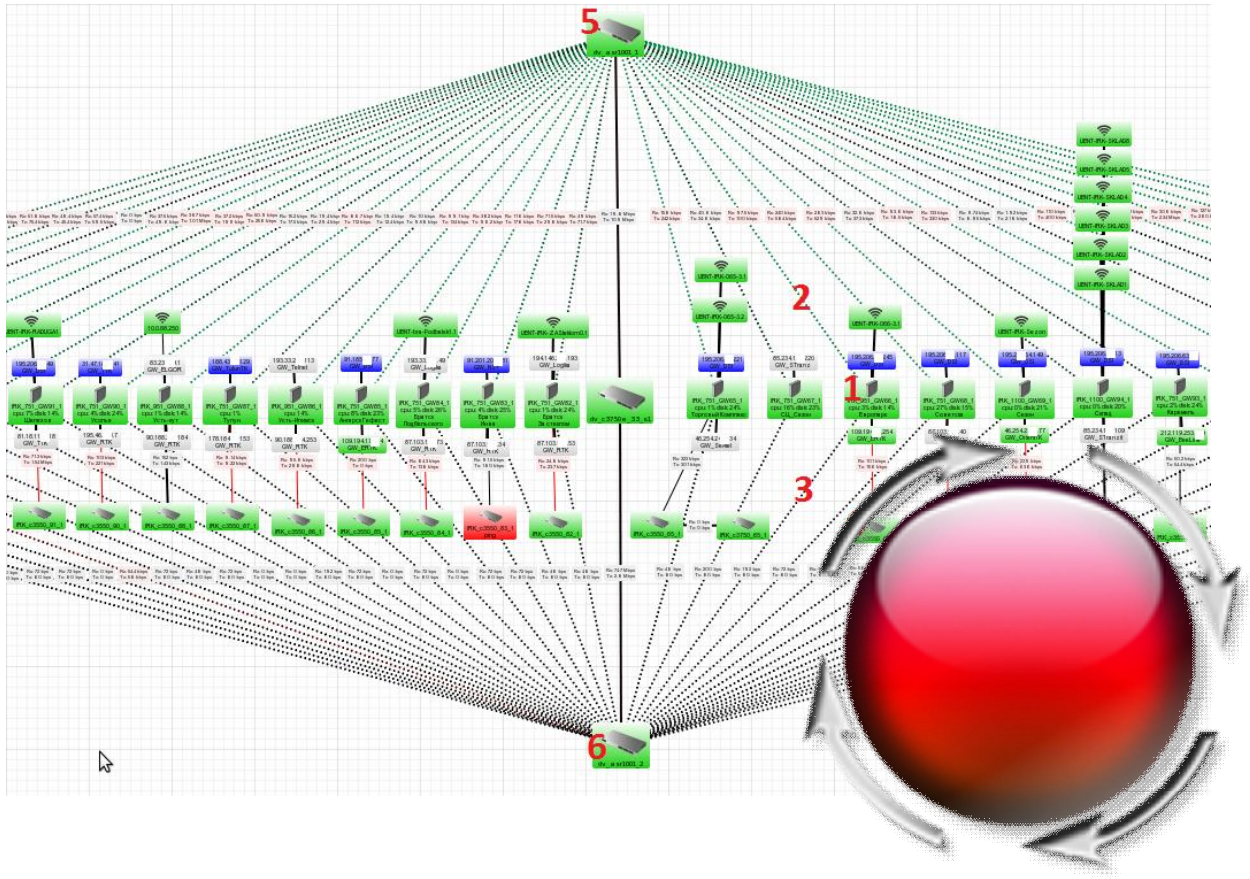
Management Approaches

- 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 (3rd party tools)
  - API (Application programming interface)



RoMON

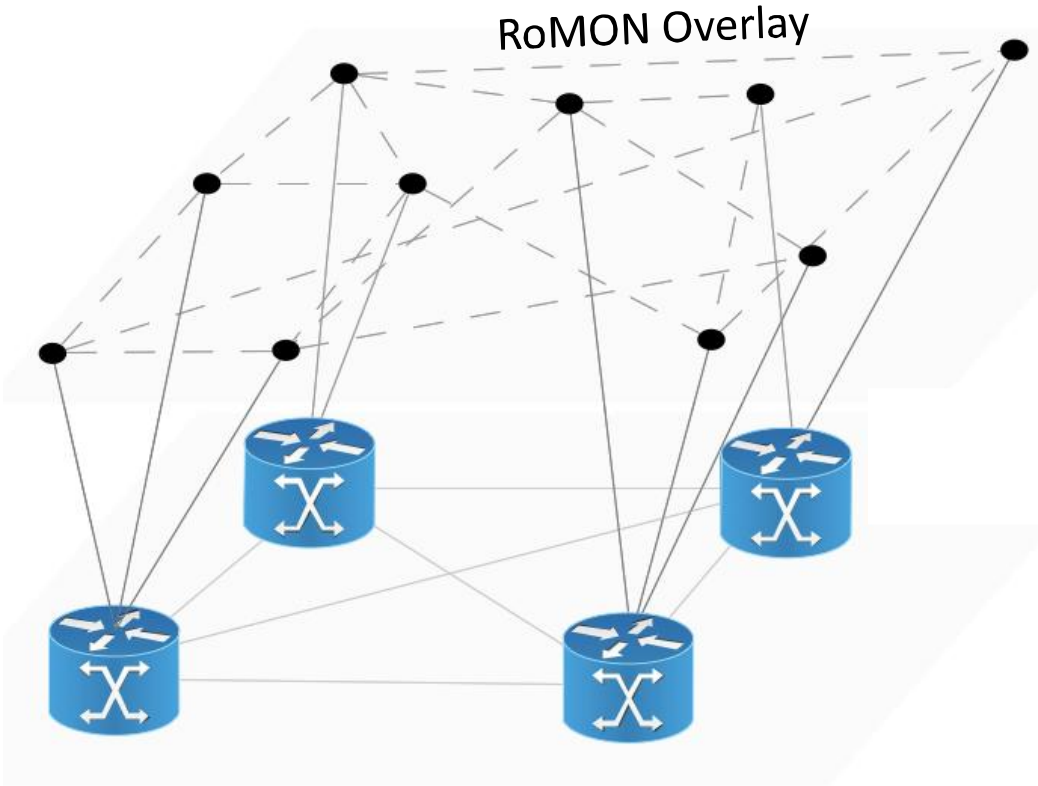
Simplify Discovery and Access

RoMON

- Router Management 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)

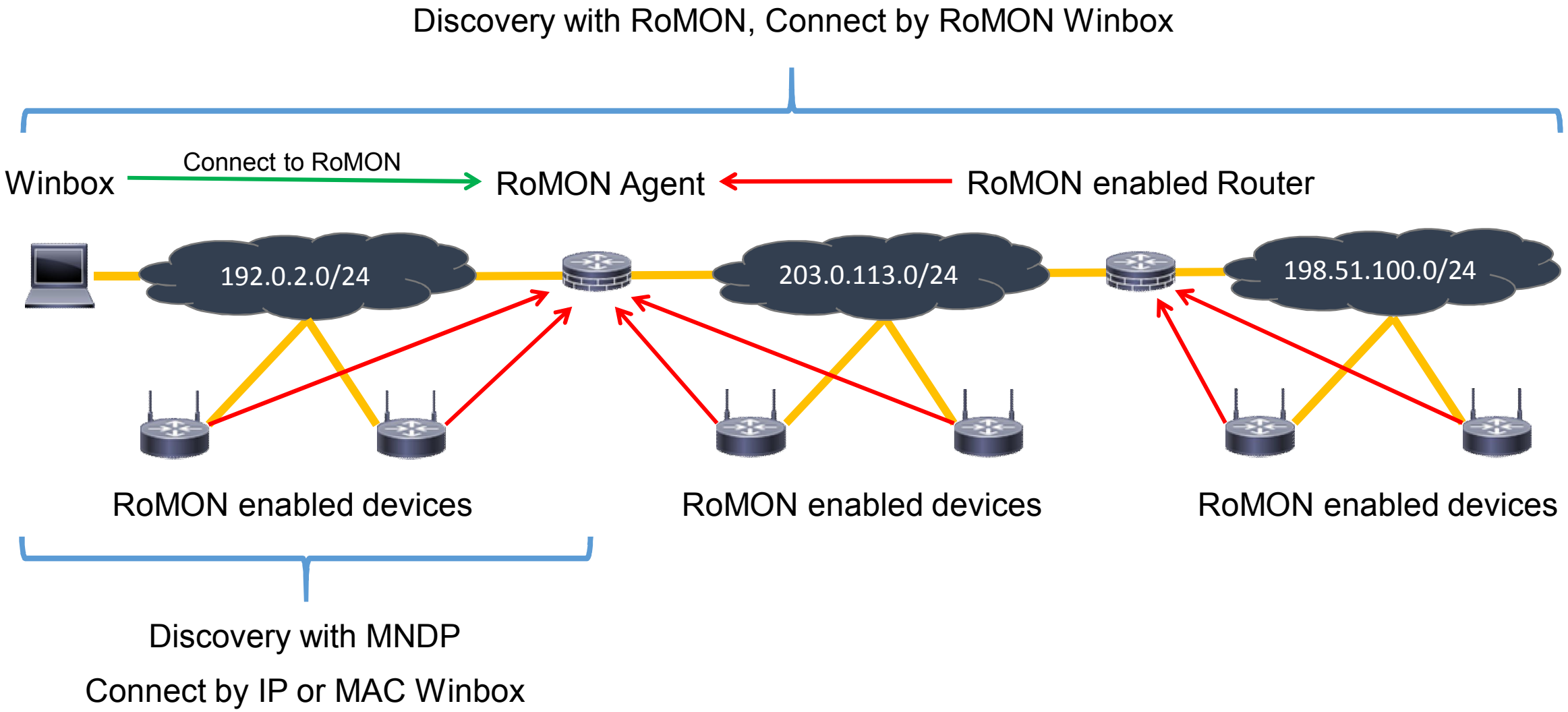
- Using existing network
- Compatible with CDP and LLDP
- Limited to layer-2 broadcast domain
- Winbox: discovery and MAC connection

RoMON

- Creates overlay network
- Only with MikroTik devices
- Not limited to layer-2 broadcast domain
- Winbox: discovery and MAC connection
- Winbox: RoMON agent connection

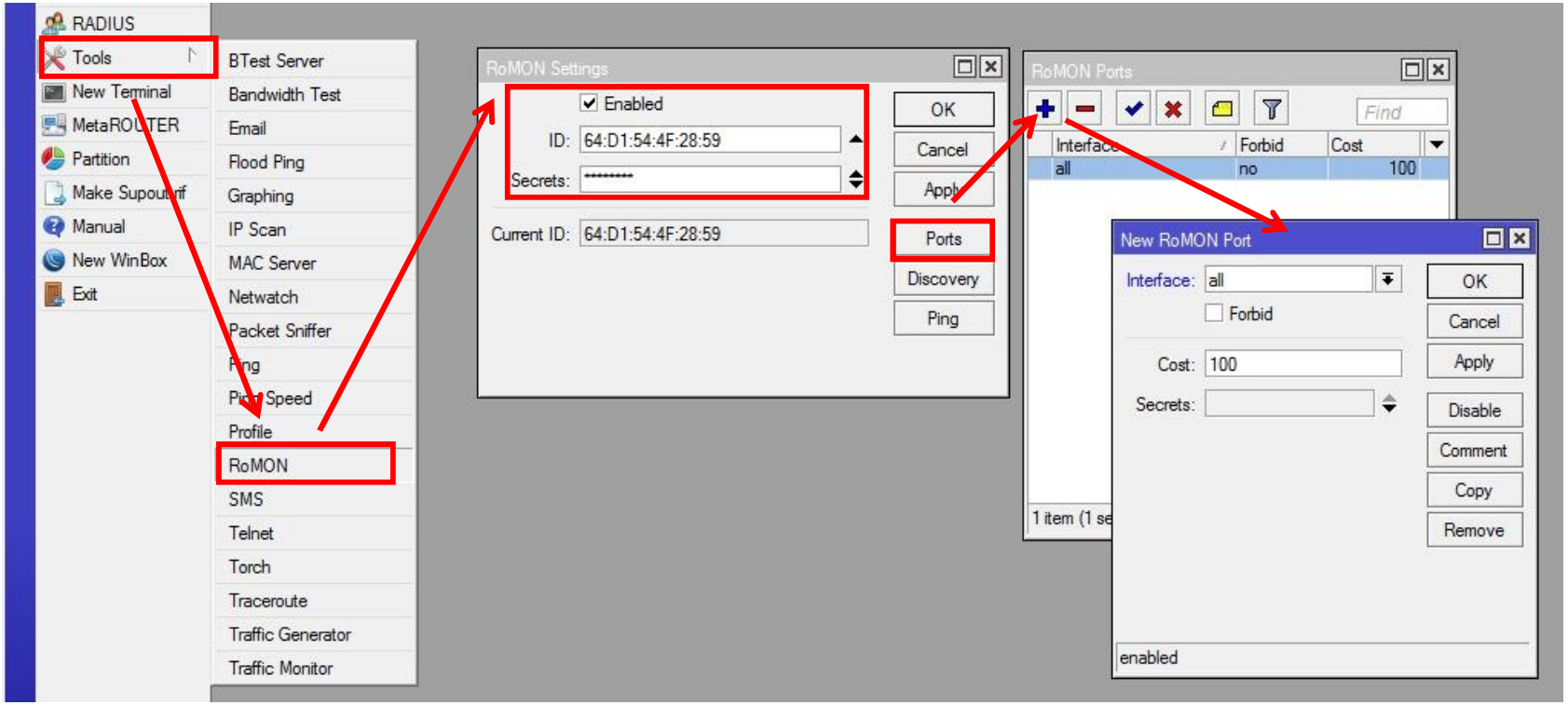
- On ethernet like interfaces (Ethernet, WLAN, EoIP, VLAN …)

Local Device Discovery across Routers

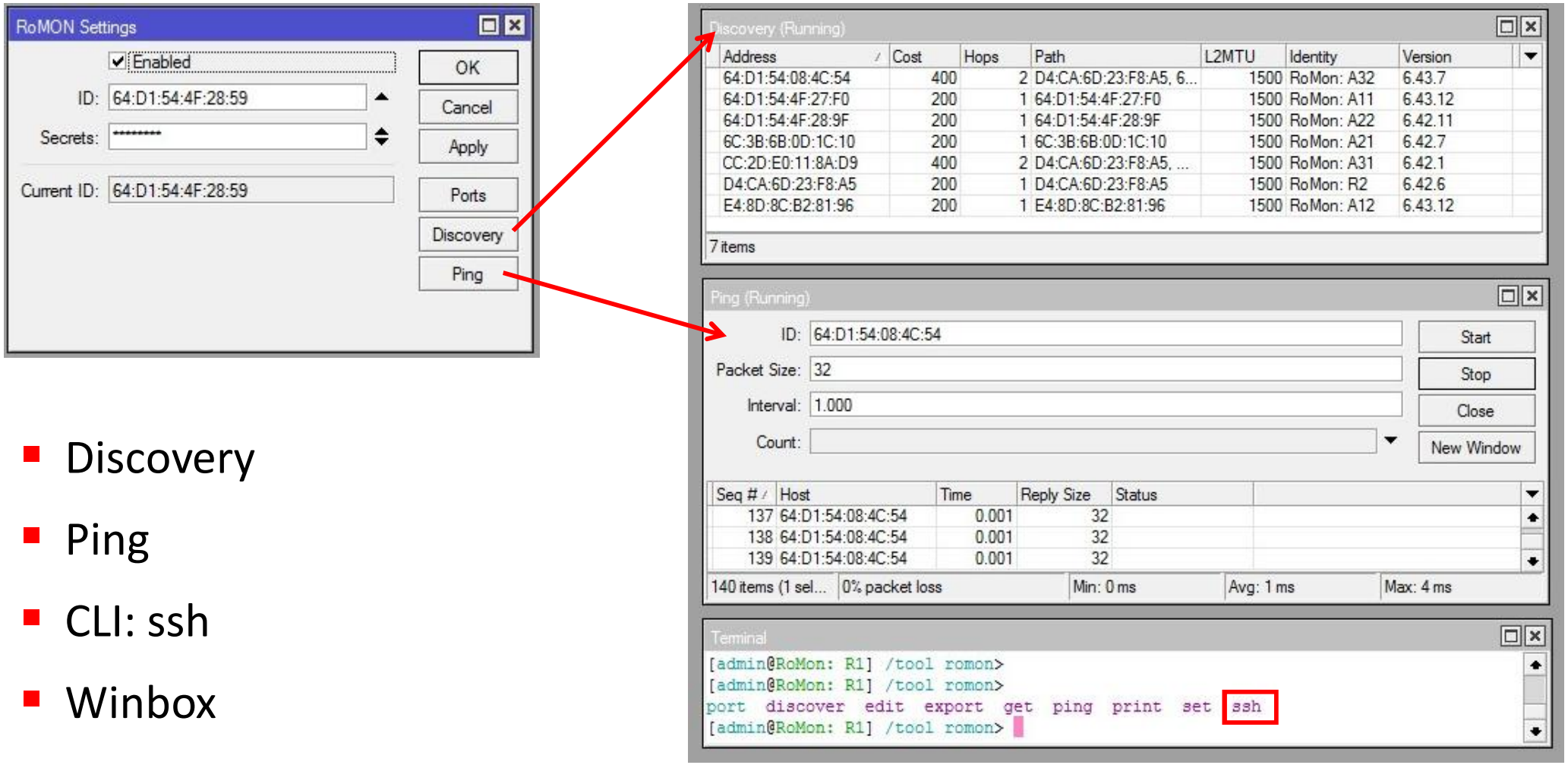


RoMON Setup

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



RoMON Tools

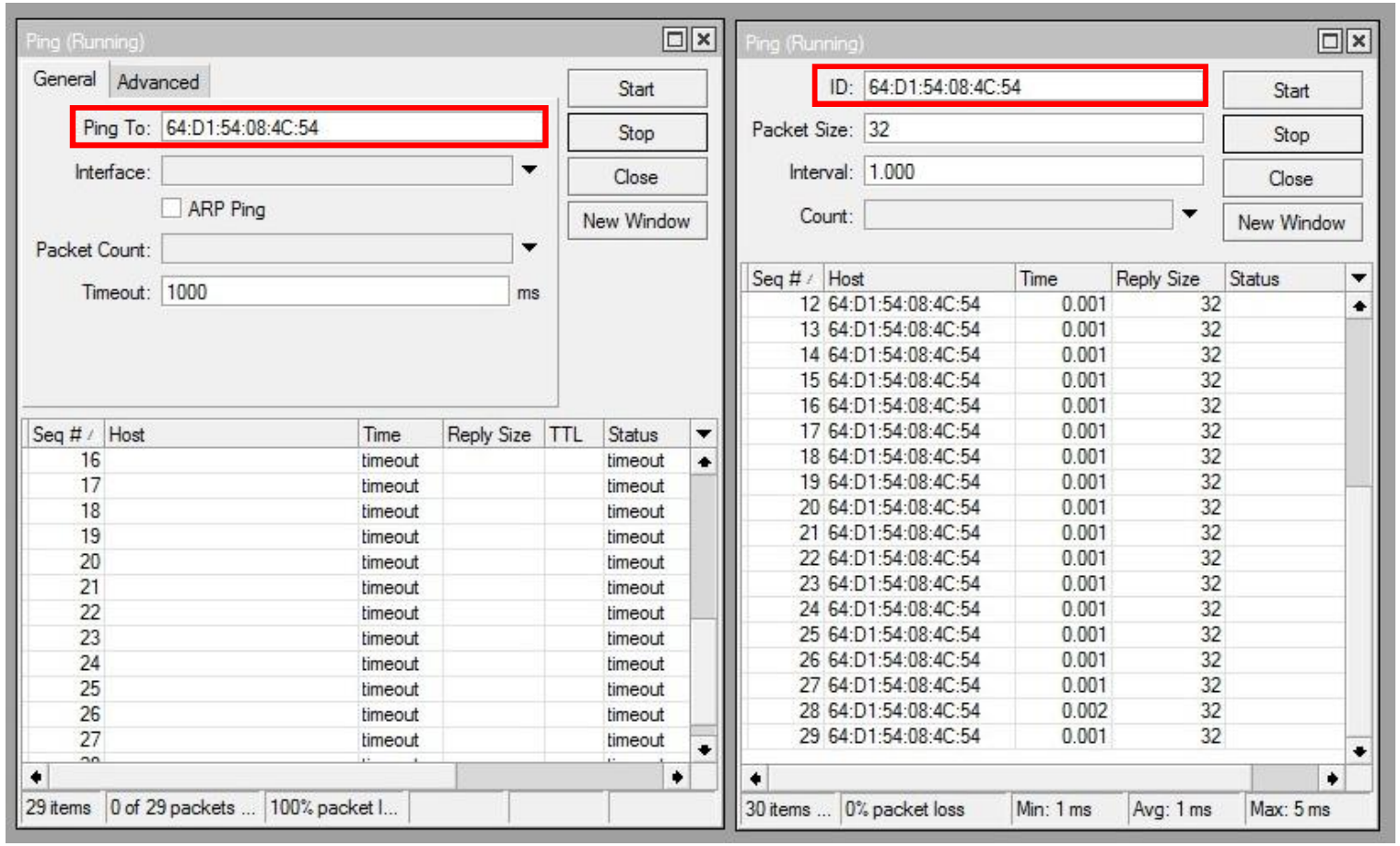


- Discovery
- Ping
- CLI: ssh
- Winbox

Standard Tools in RoMON Network

Ping / MAC Ping

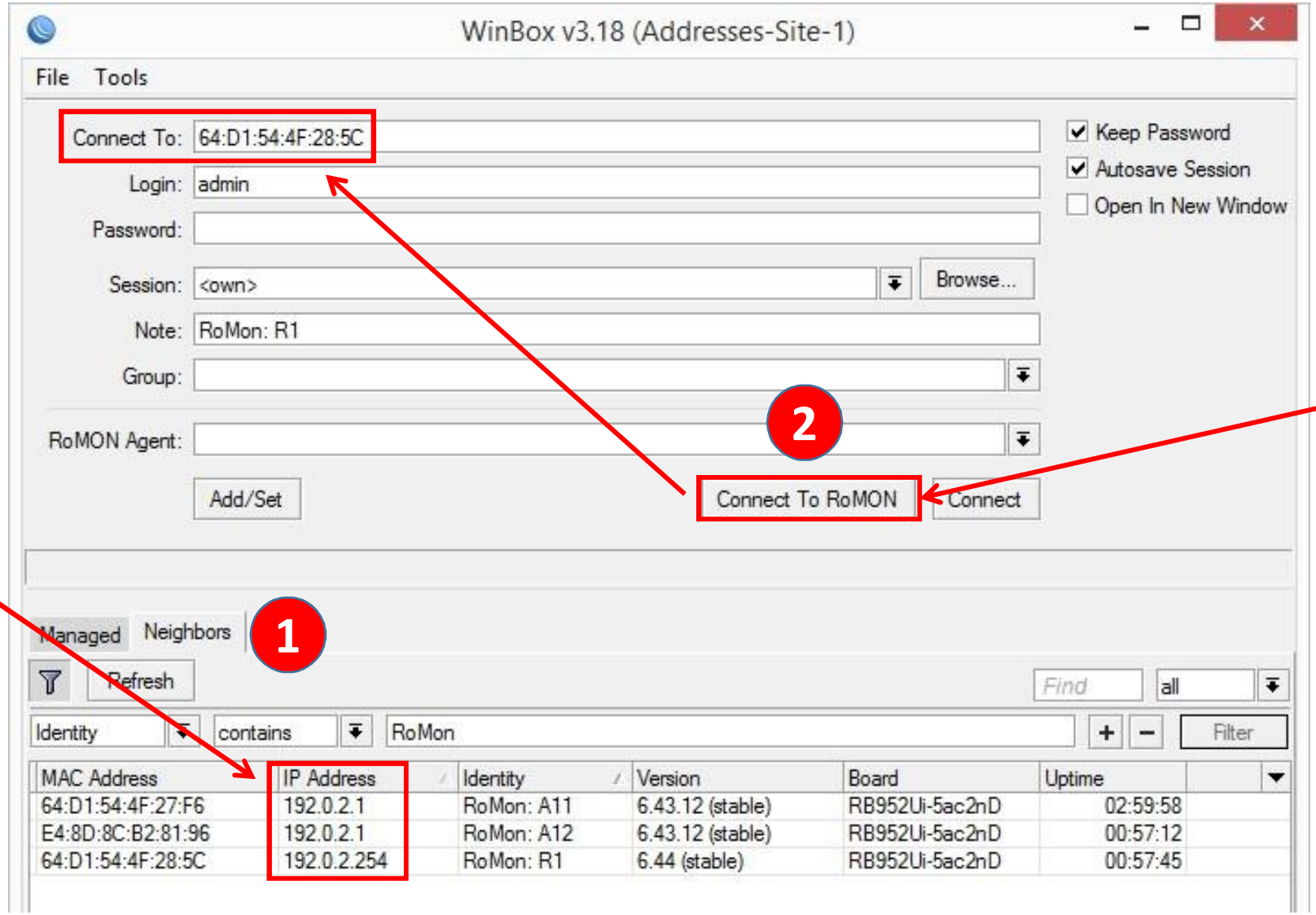
RoMON Ping



Winbox Discovery and RoMON Connection

Devices within the layer-2 network discovered

Use router as RoMON agent

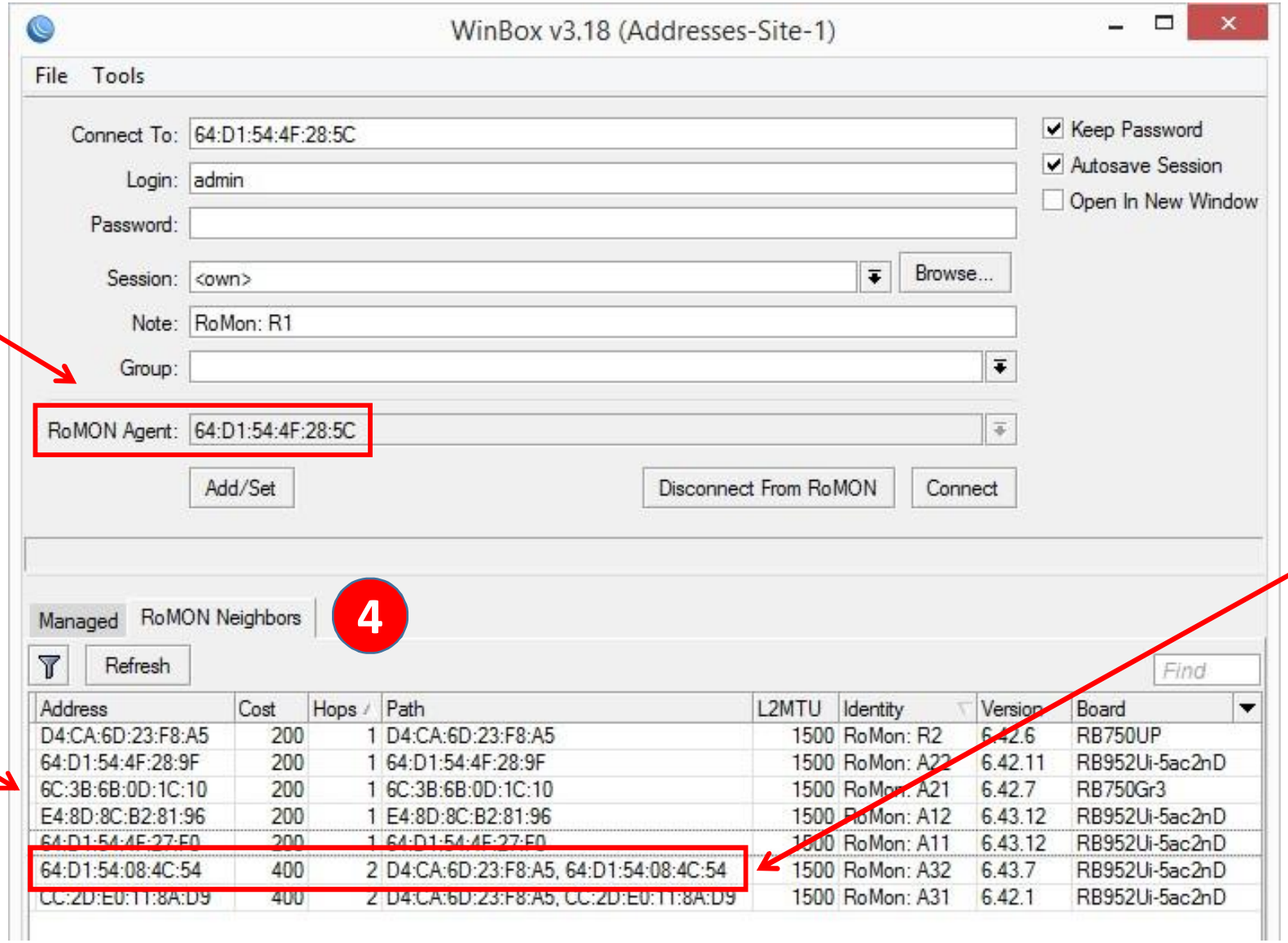


Winbox Discovery and RoMON Connection

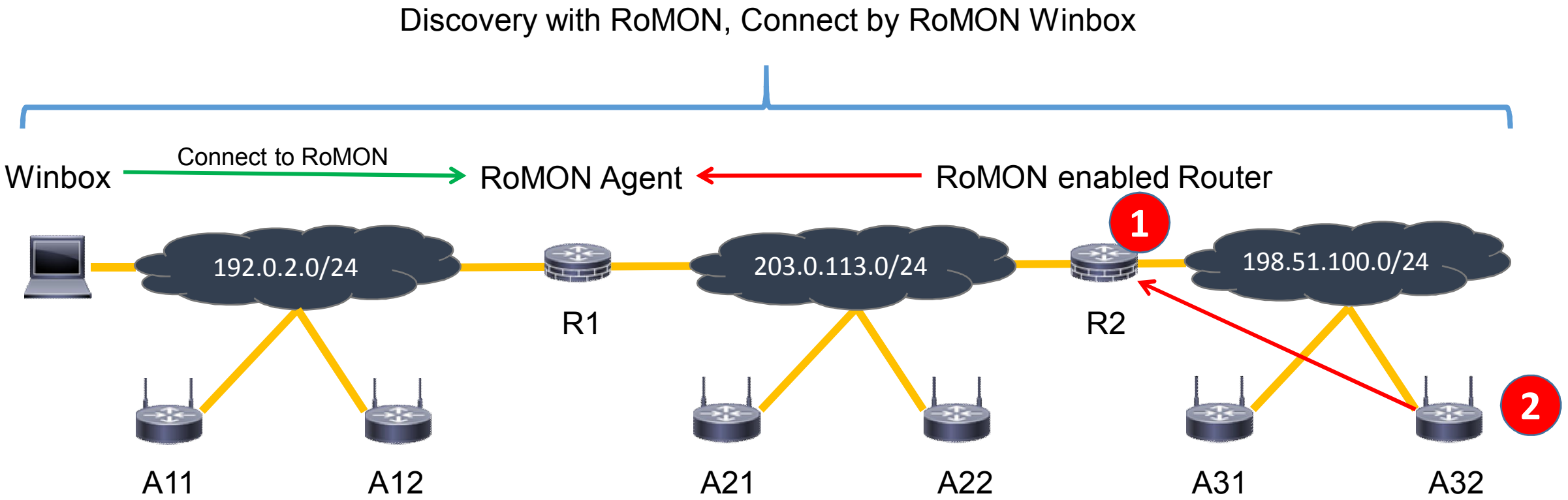
Connected to RoMON agent

RoMON discovery through agent

Two hops to reach



Local Device Discovery across Routers



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

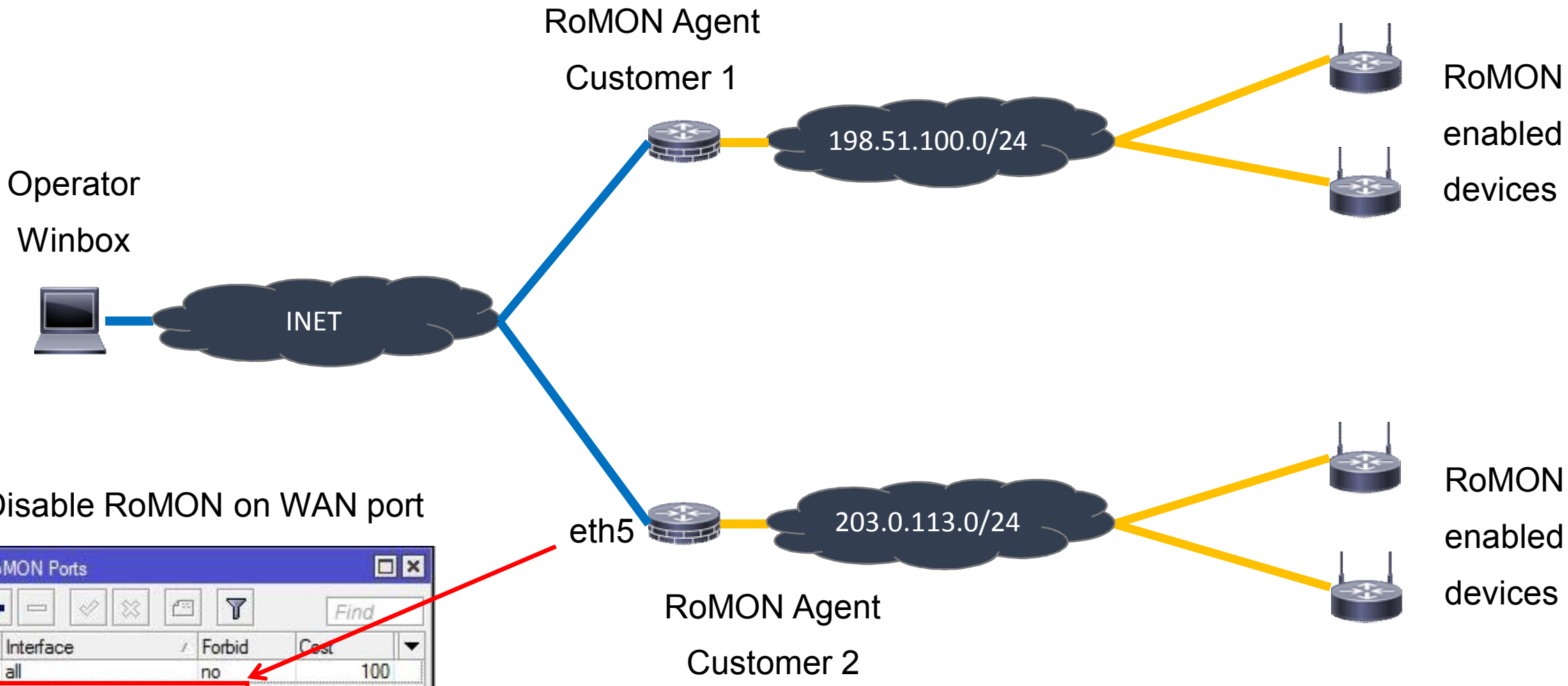
Remote RoMON Agent

- 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

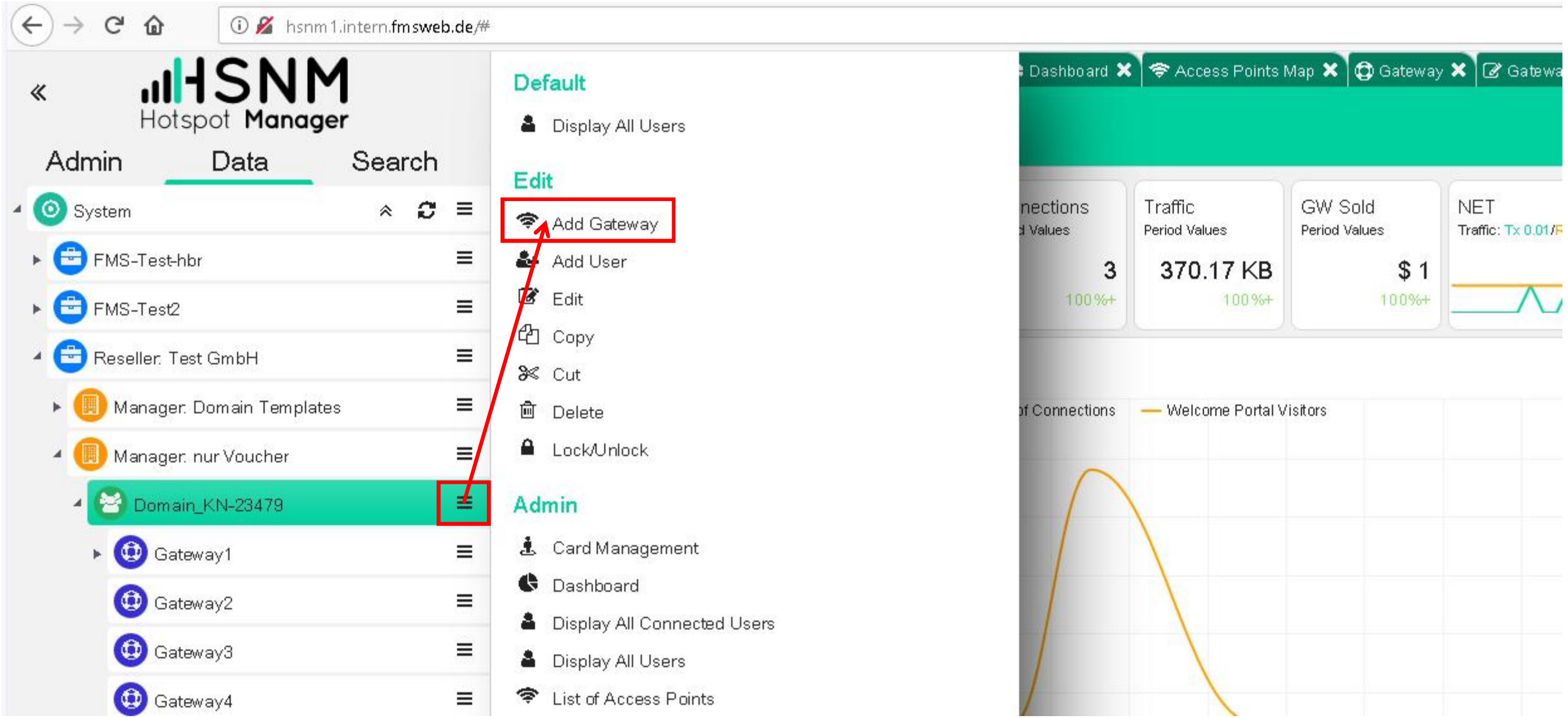
HSNM Gateway

- MikroTik hotspot
- WAN/LAN gateway

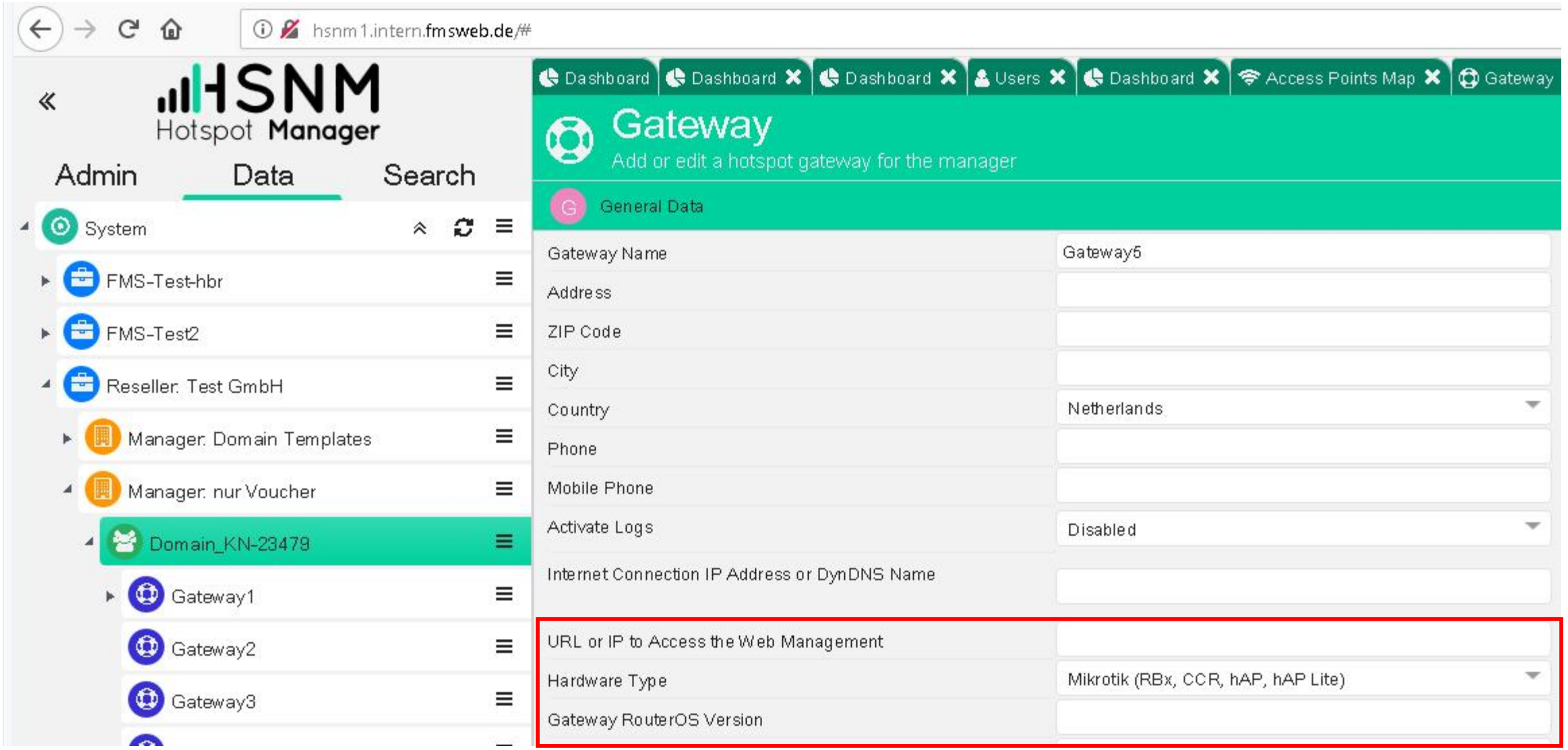
HSNM Accesspoint

- MikroTik WLAN access point

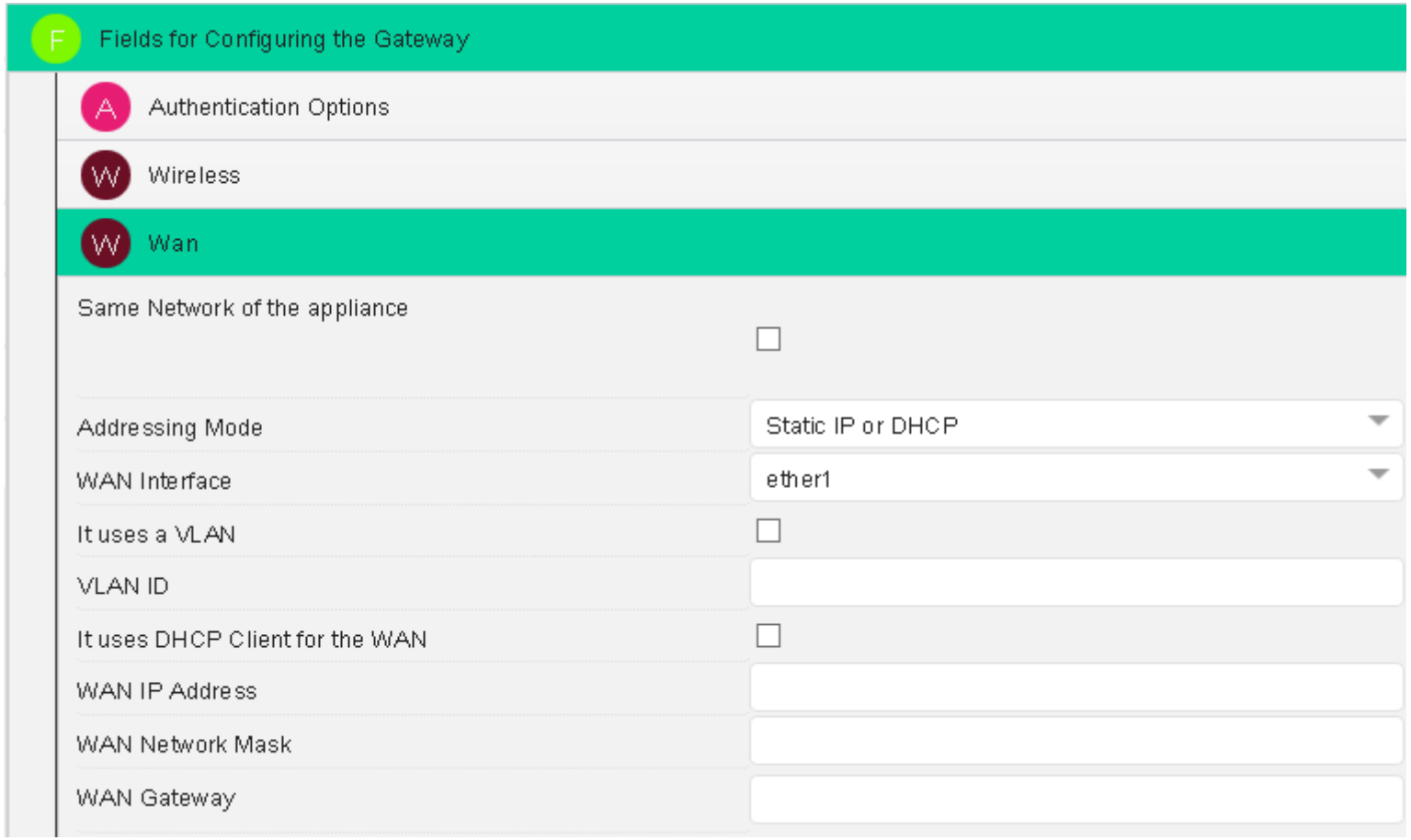
MikroTik Gateway Integration



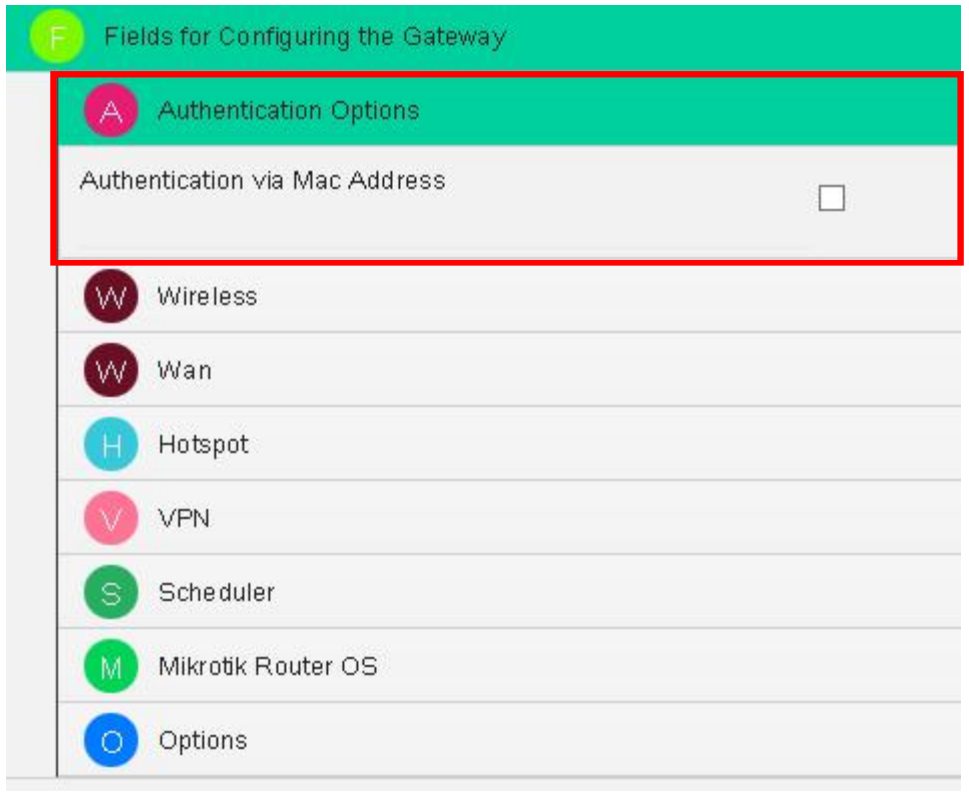
Choosing Hardware and RouterOS Type

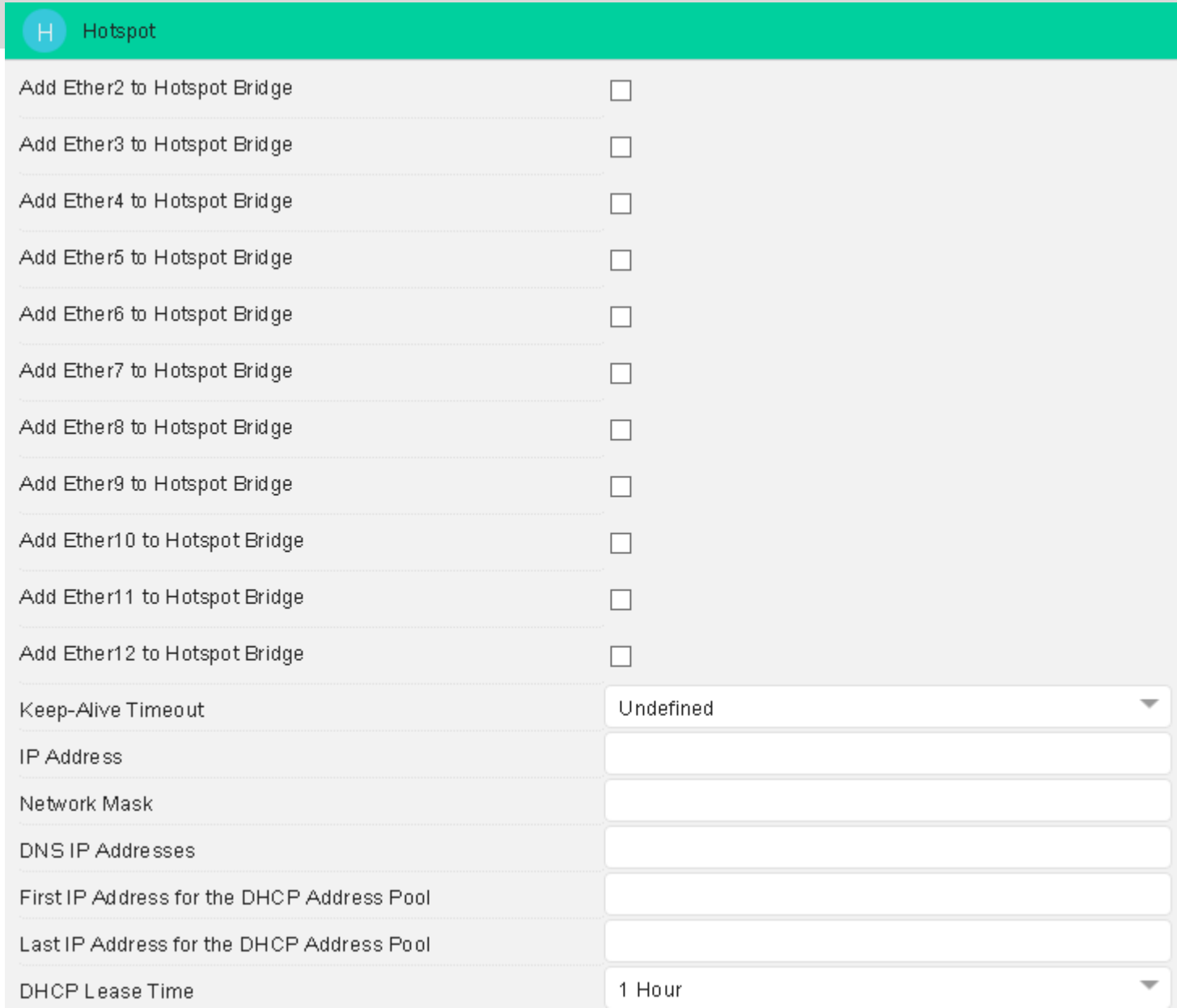


MikroTik Specific Settings: WAN

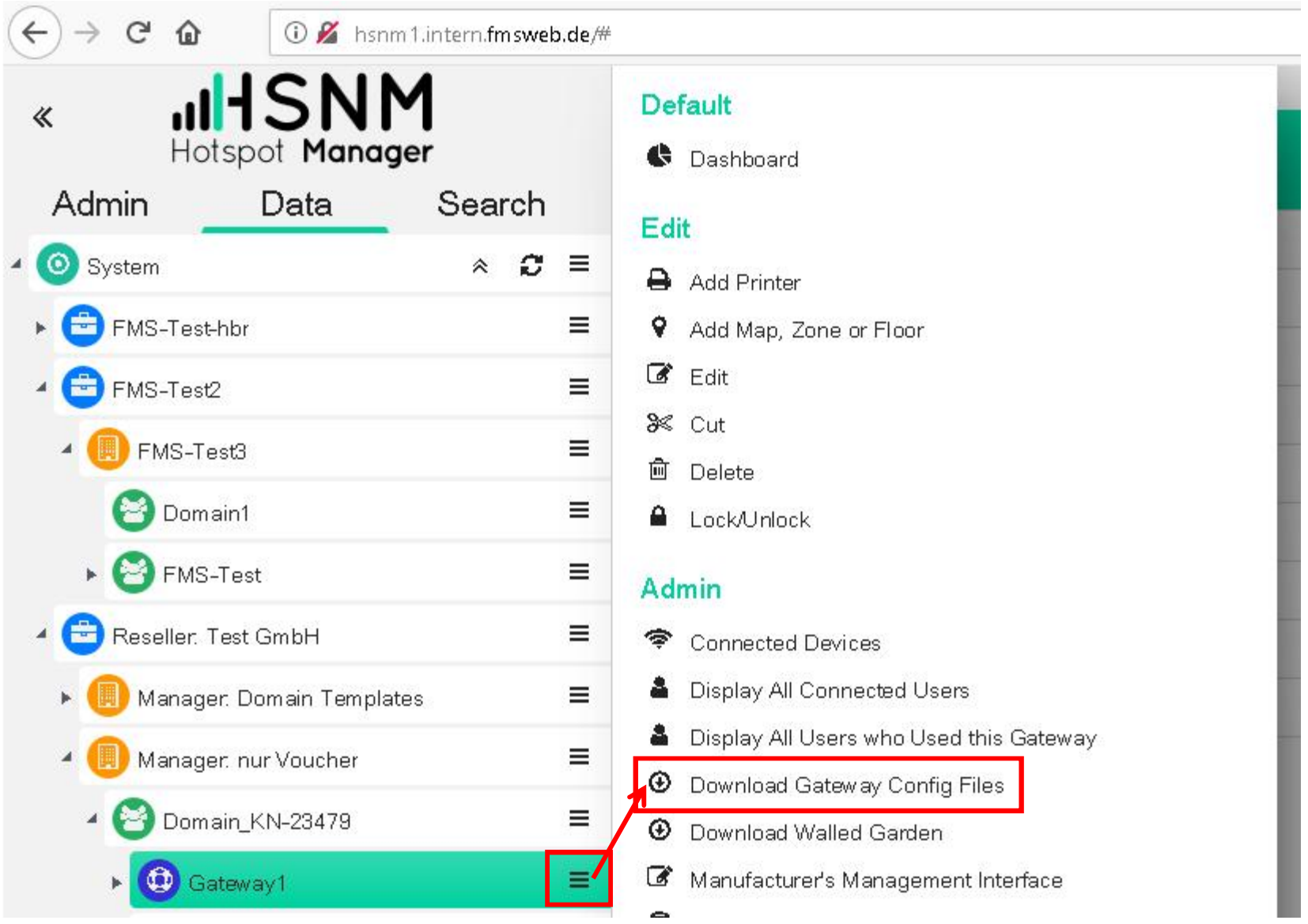


MikroTik Specific Settings: MAC Auth + Hotspot





Initial Configuration



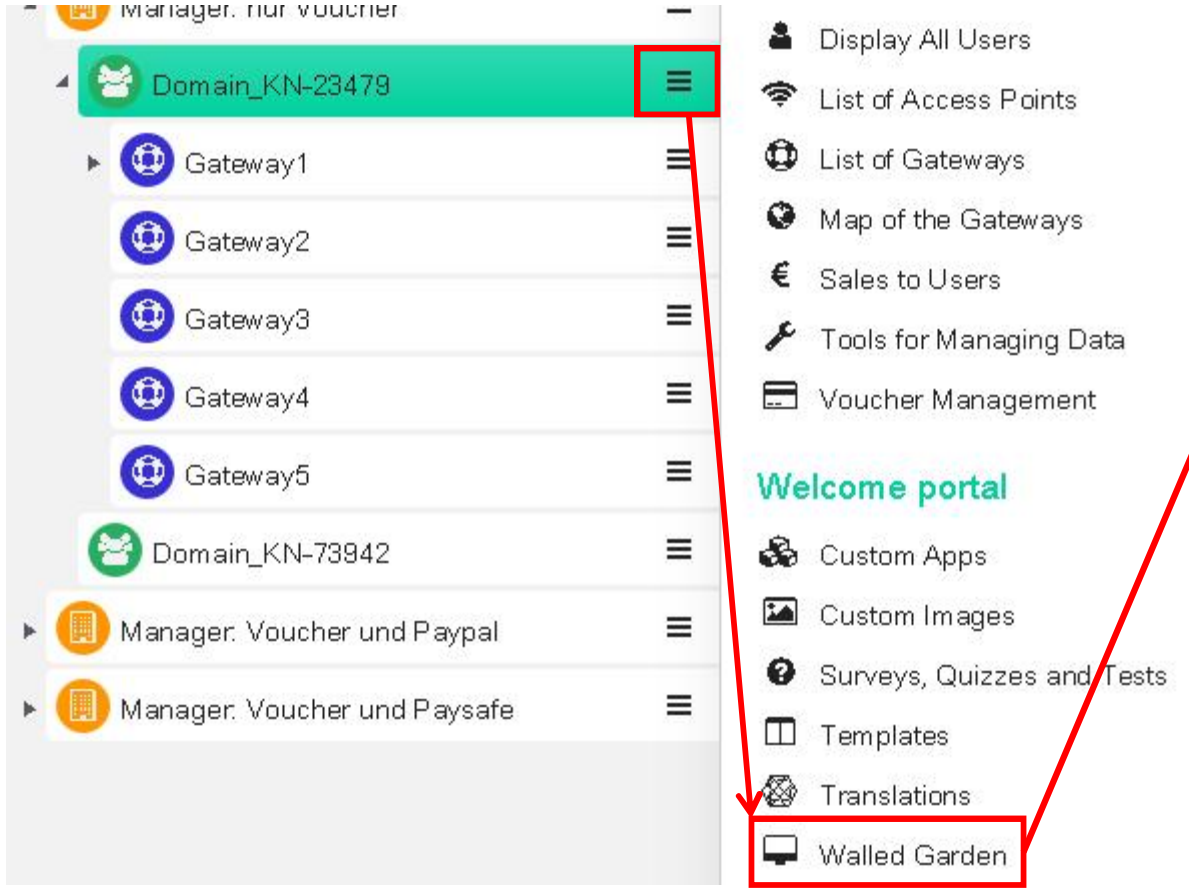
- Download .rsc
- Upload to MikroTik
- /import

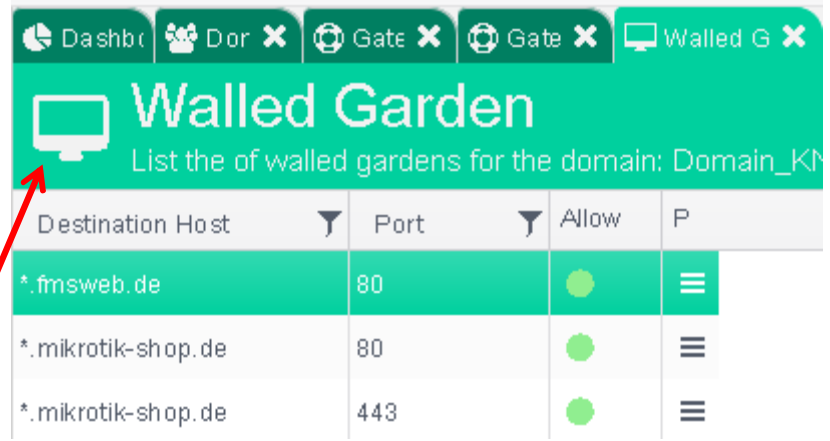
- Initial configuration
- Scripting environment

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





- Domain or gateway level
- Automatic import by script

Seamless Integration of legacy Solutions

1

Legacy ticket printer

Creating Usermanager accounts

2

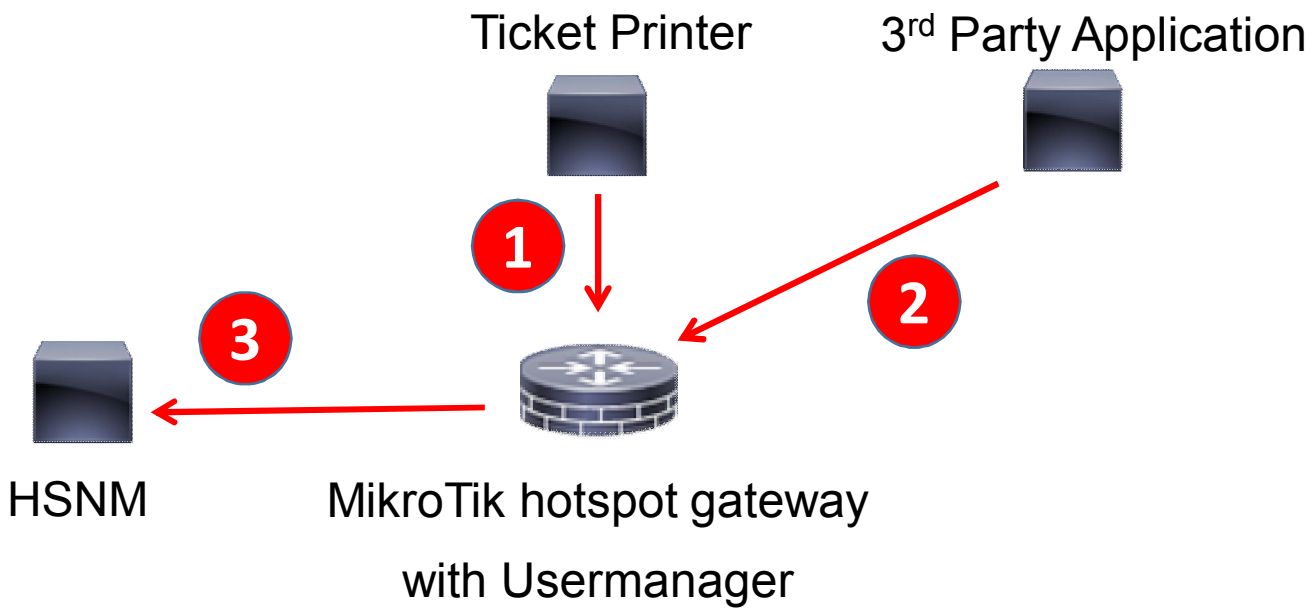
Legacy 3rd party application

Creating Usermanager accounts

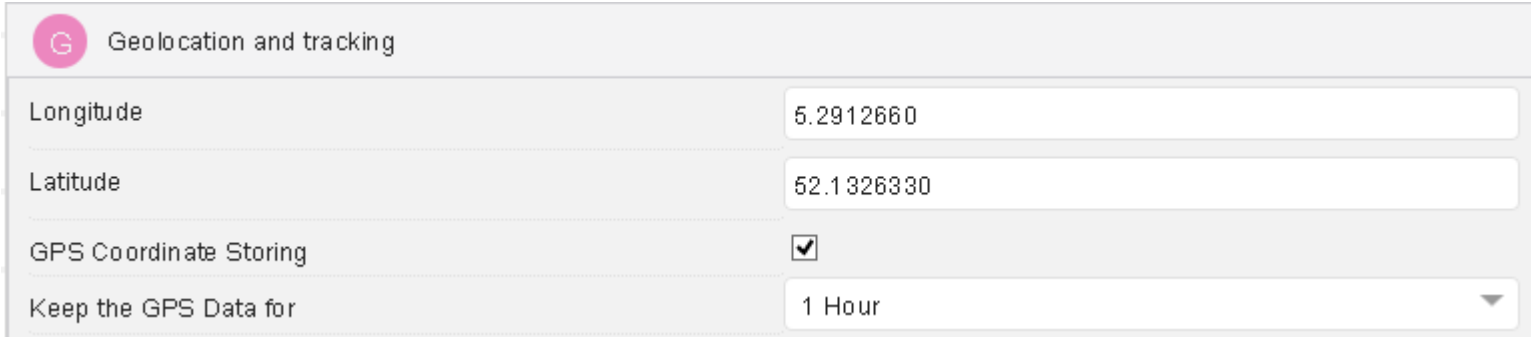
3

Exporting UM accounts to HSNM

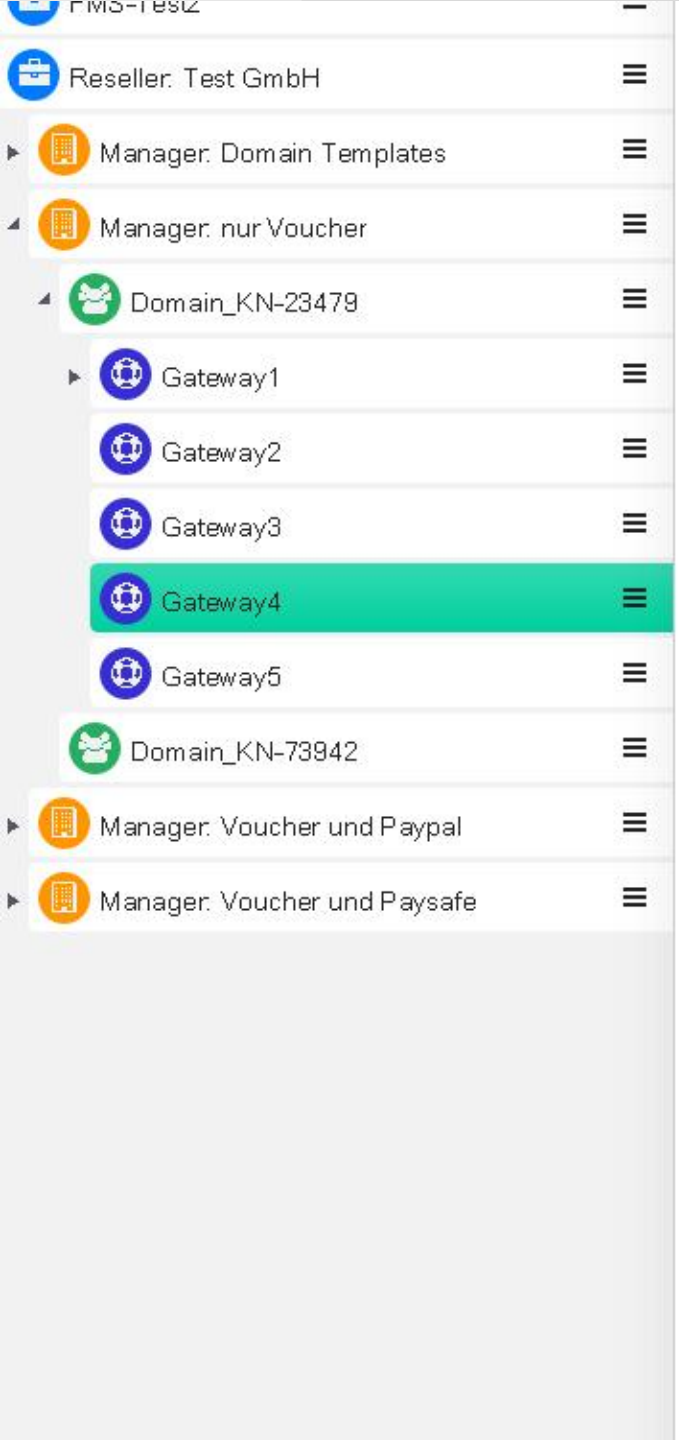
Deleting UM accounts locally

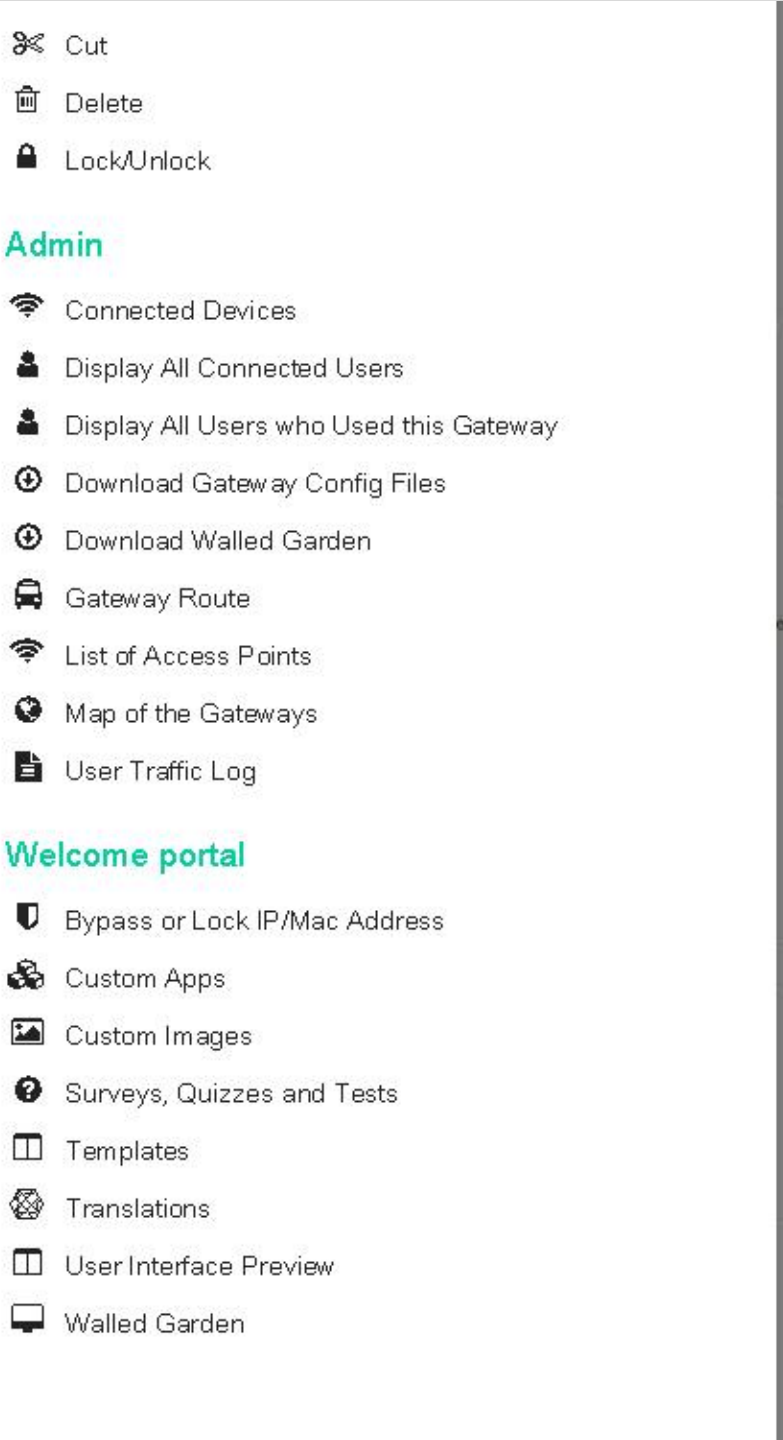


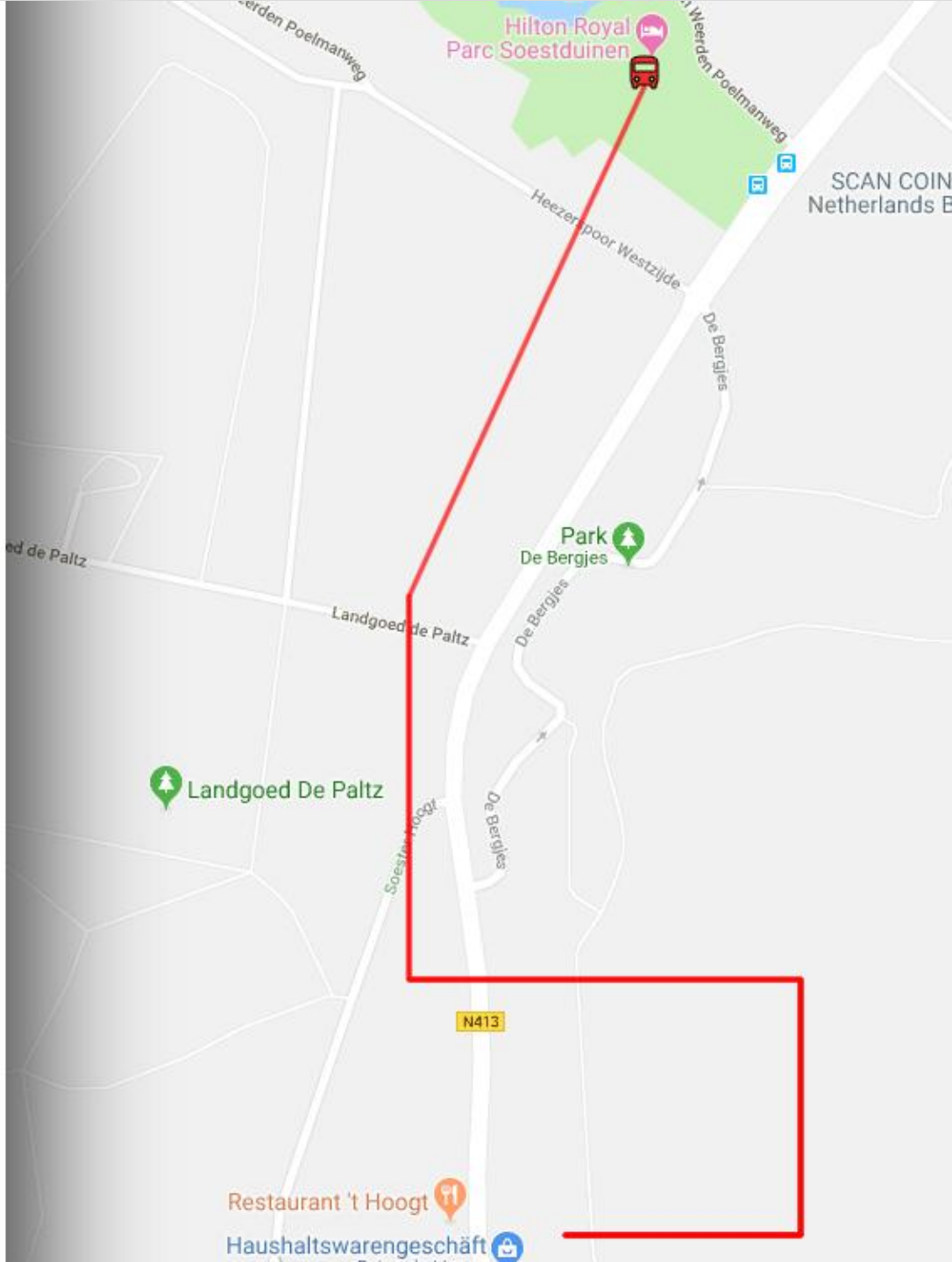
GPS based Maps and Tracking



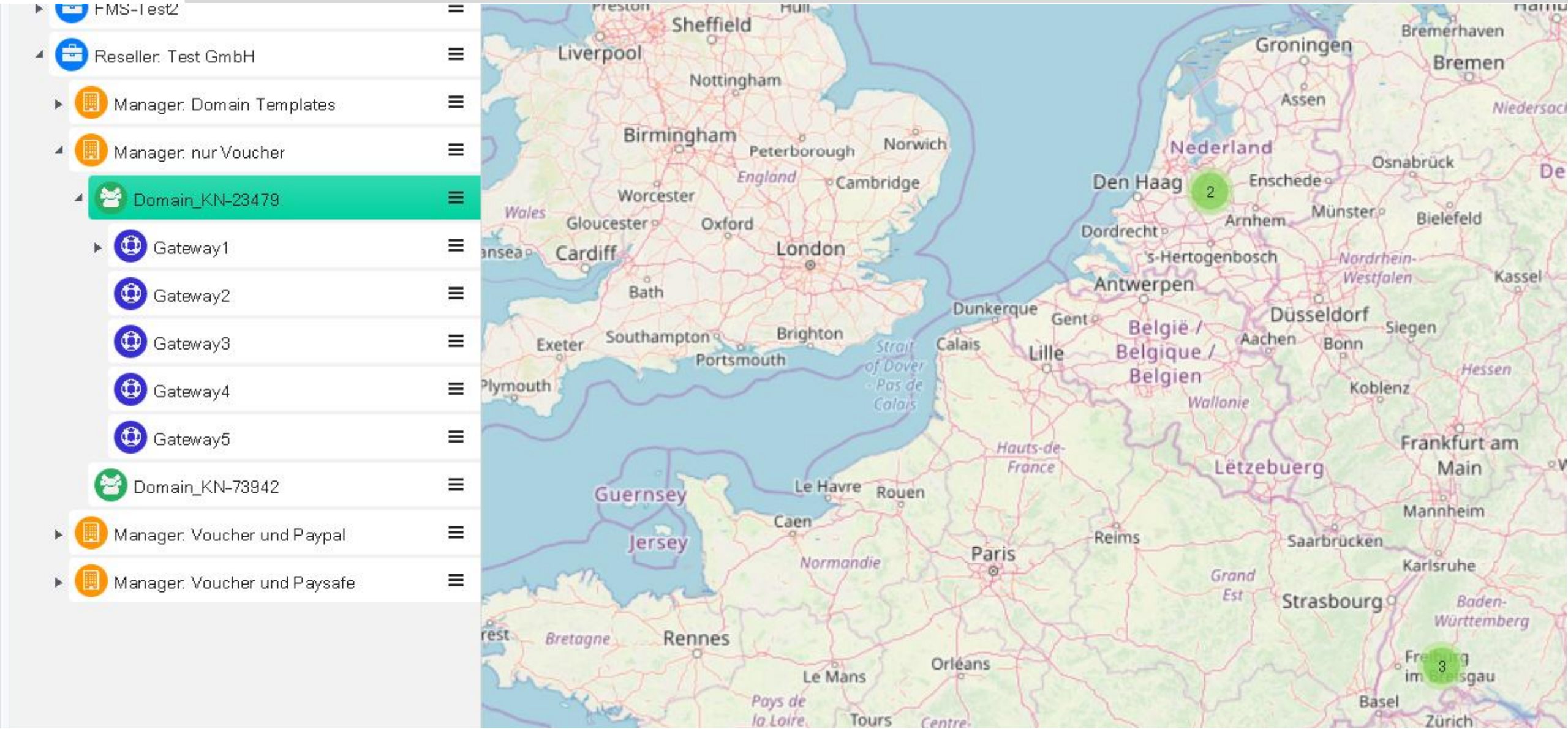
- Script sends GPS location
- Can be stored in HSNM
- Static GPS location
- Can be entered in HSNM
- Tracking of moving gateways
- E.g. busses, trains, taxies
- Visualisation of gateway location


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


Hilton Royal
Parc Soestduinen
Heezerpoor Westzijde
De Bergjes
Park
De Bergjes
Landgoed de Paltz
Landgoed De Paltz
N413
Restaurant 't Hoogt
Haushaltswarengeschäft

Hotspot Network Manager (HSNM)



Manual Positioning on Floor Plans and Maps

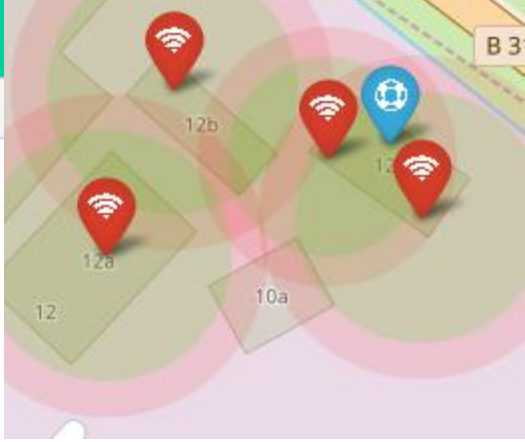
- Manual positioning
- Gateways & access points
- Maps or plans
- Coverage (in m)

Dashboard | Map, Zone or Floor | Access Points Map | Access Points Map | Gateway | Access point | Map, Zone or Floor | Gatev

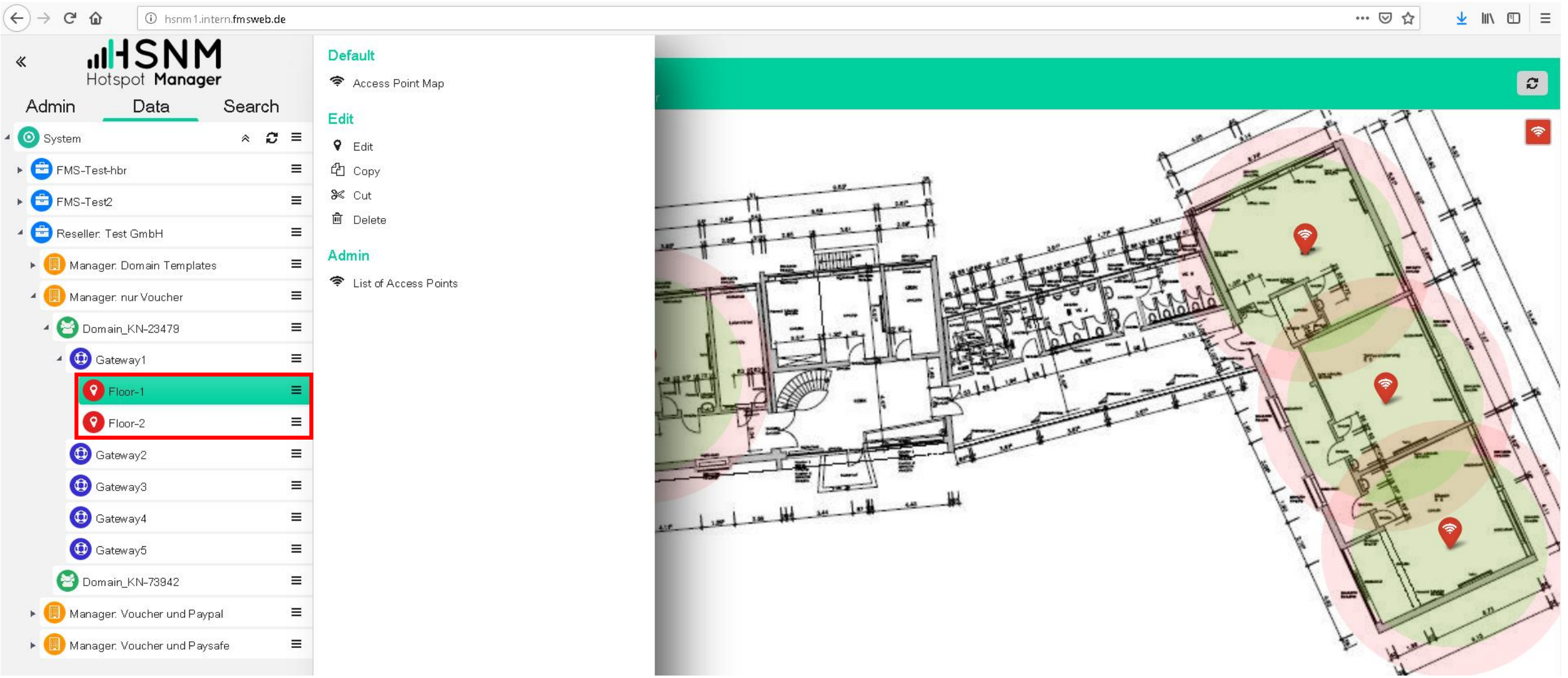
Access point

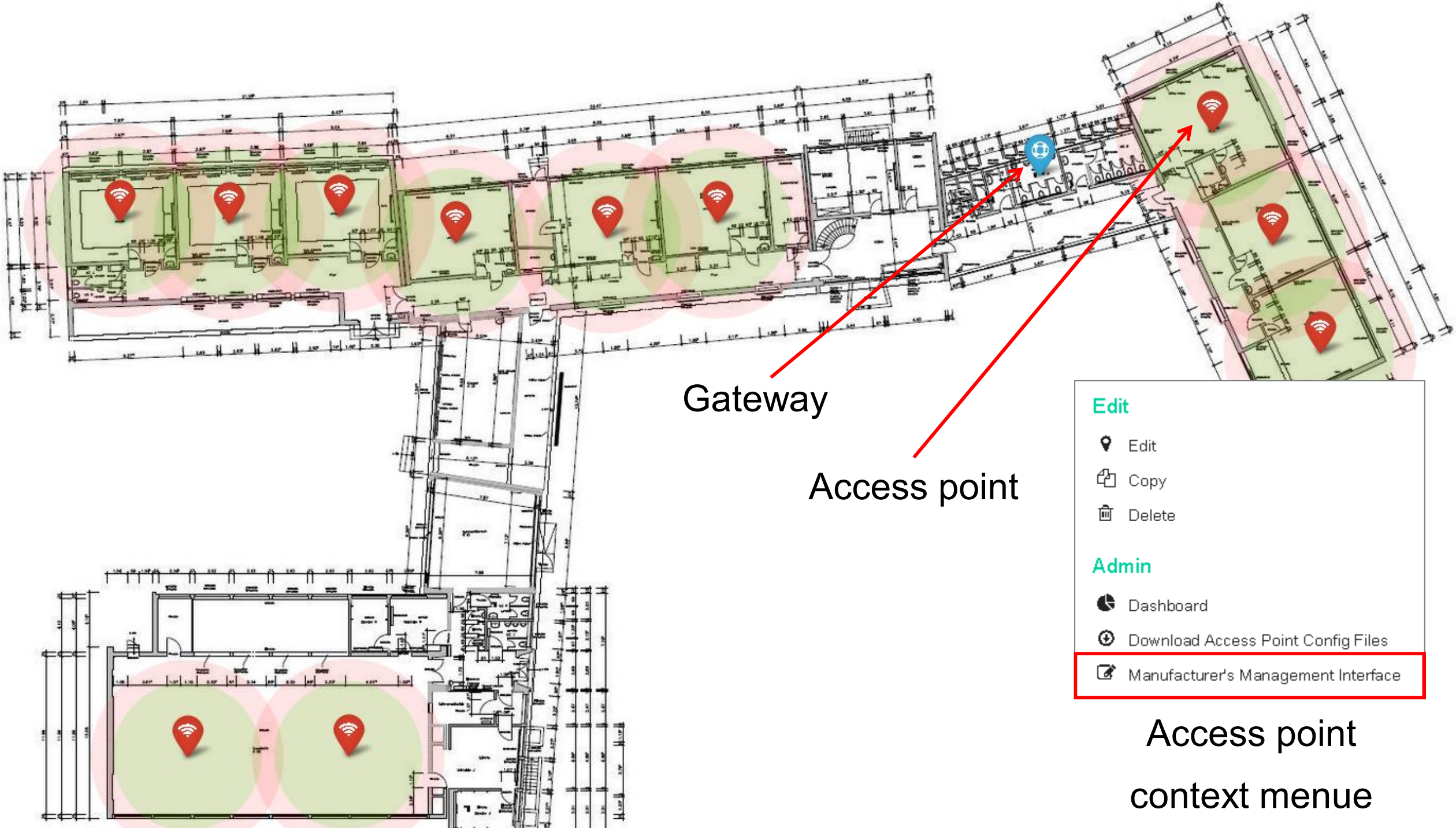
List of access point for the gateway: Gateway1

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)

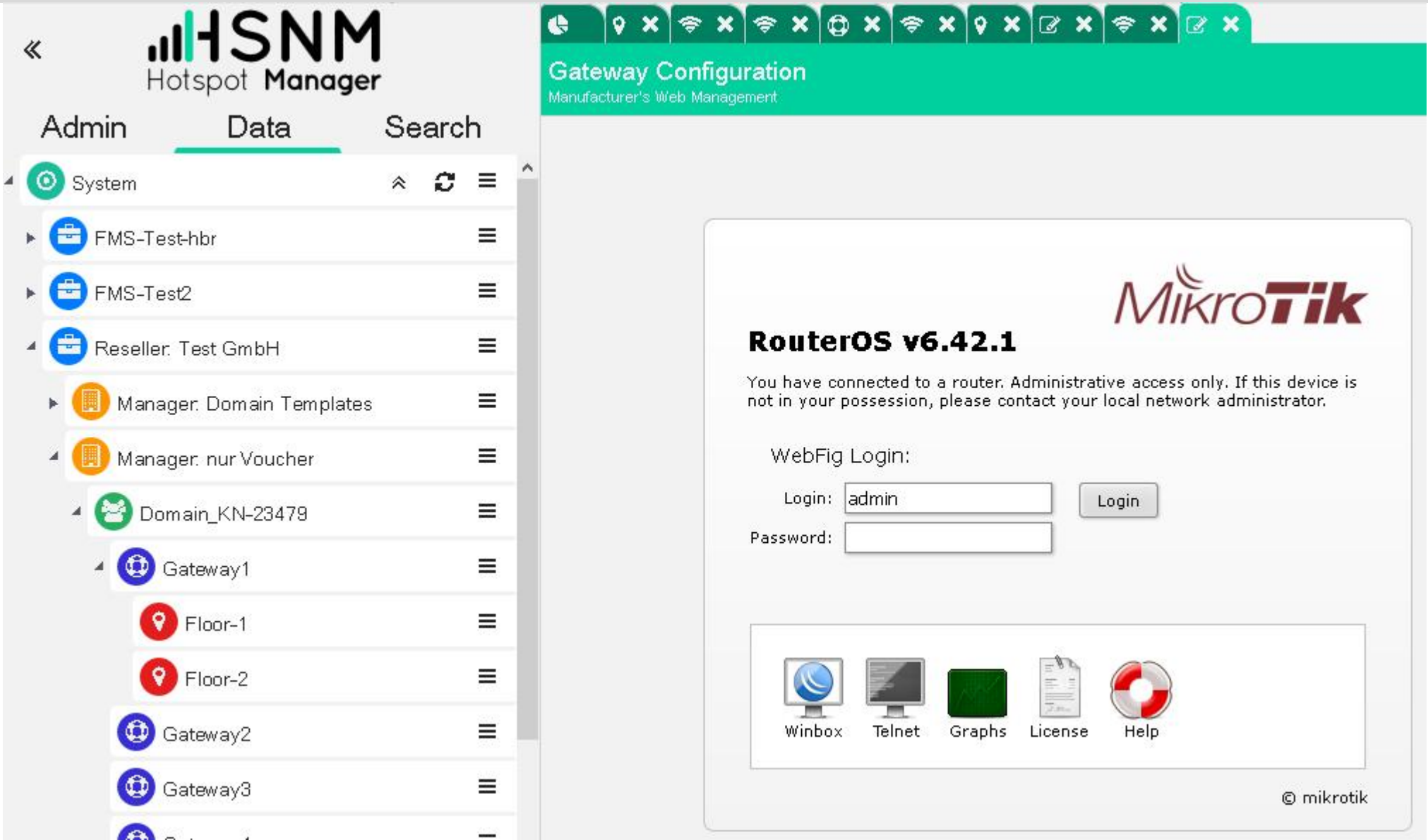




Access point context menue

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 od registrations

Get in Touch

Are you looking for a powerful

captive portal solution?

+49 761 2926500 | 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

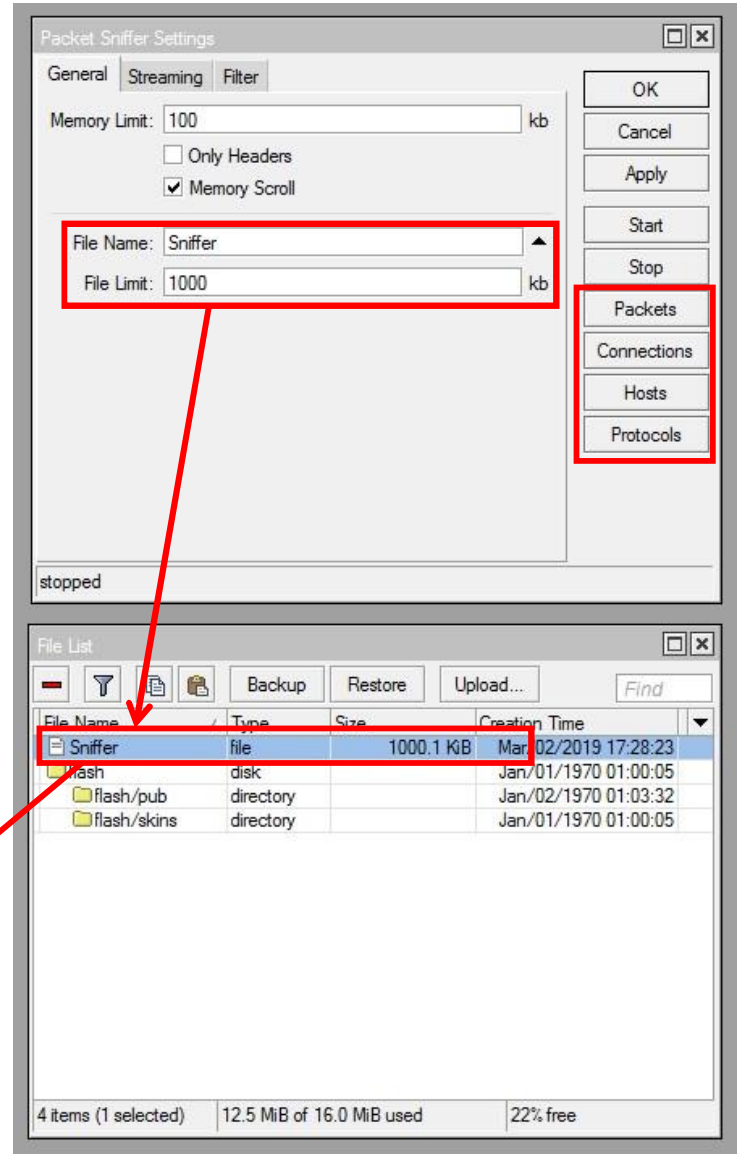
- Packet sniffing
- De facto standard: Wireshark
- RouterOS packet sniffer

MikroTik Packet Sniffer

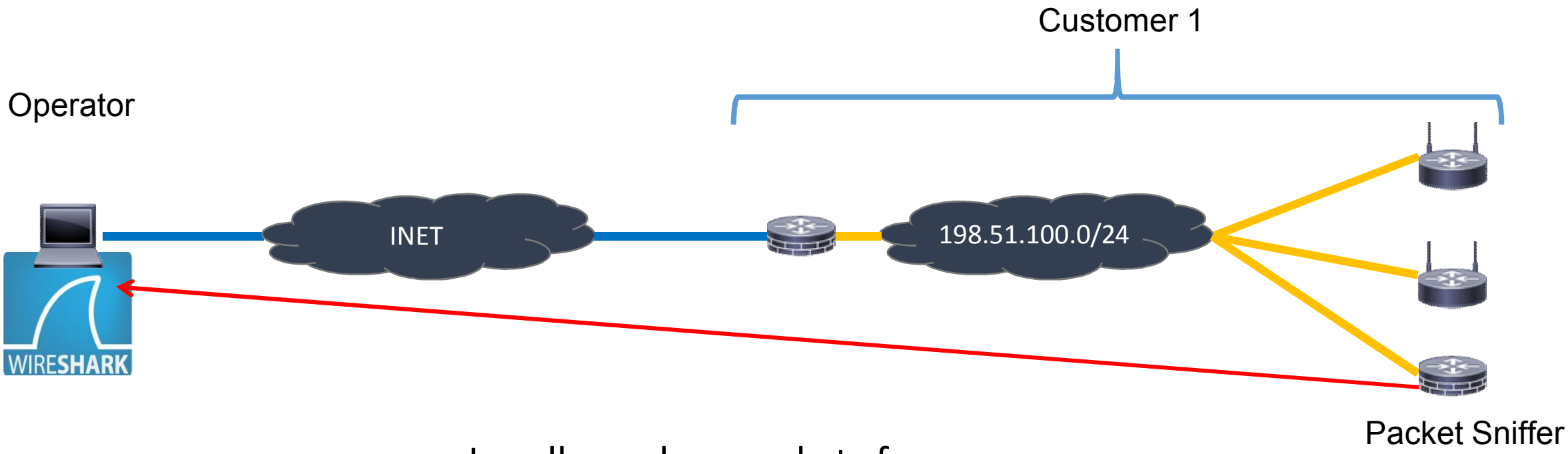
- General settings
- Filter
- Start/Stop

- 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

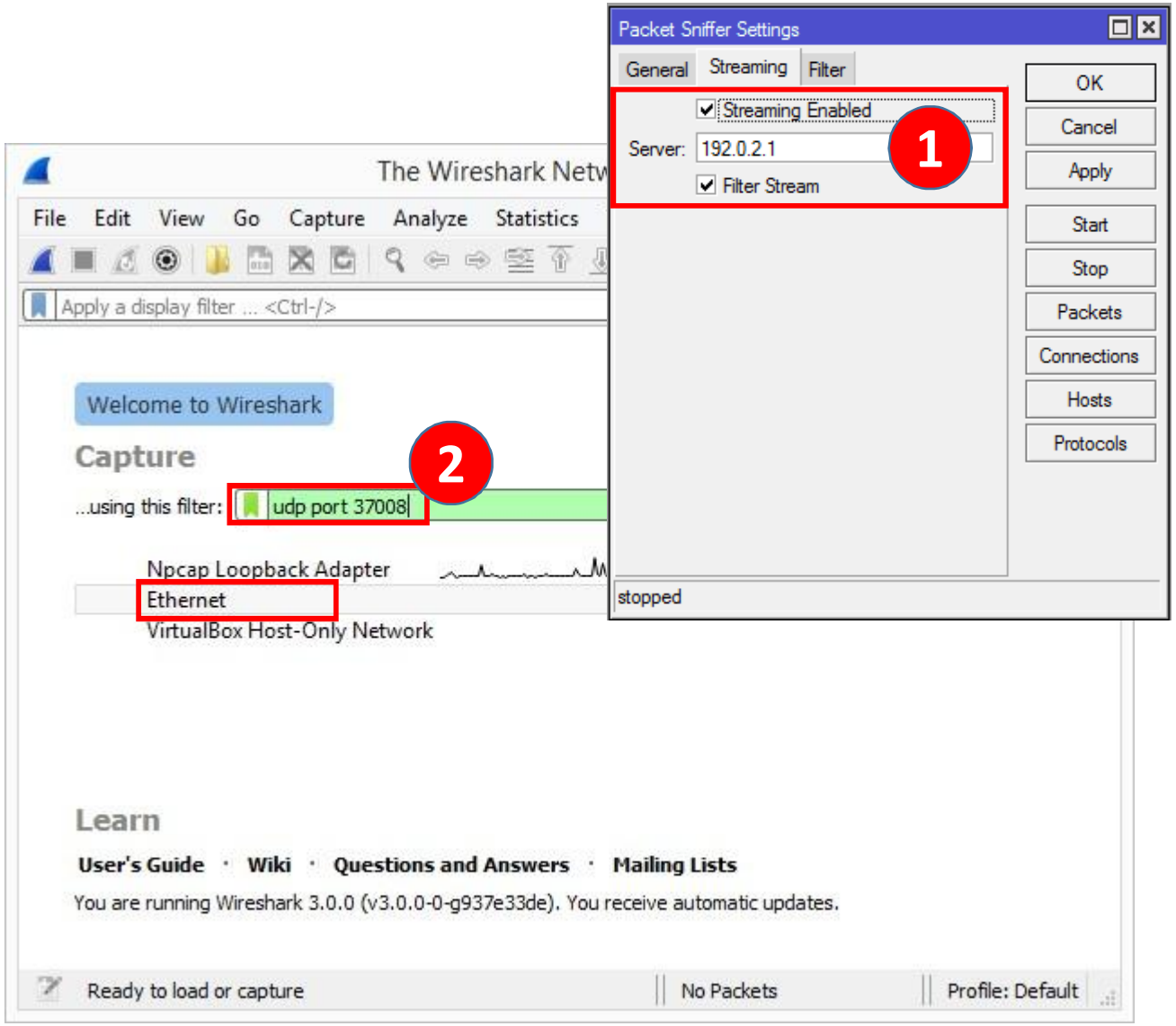
Sniffer Stream

- Enable “Stream”
- Set Wireshark host IP
- Enable “Filter Stream”

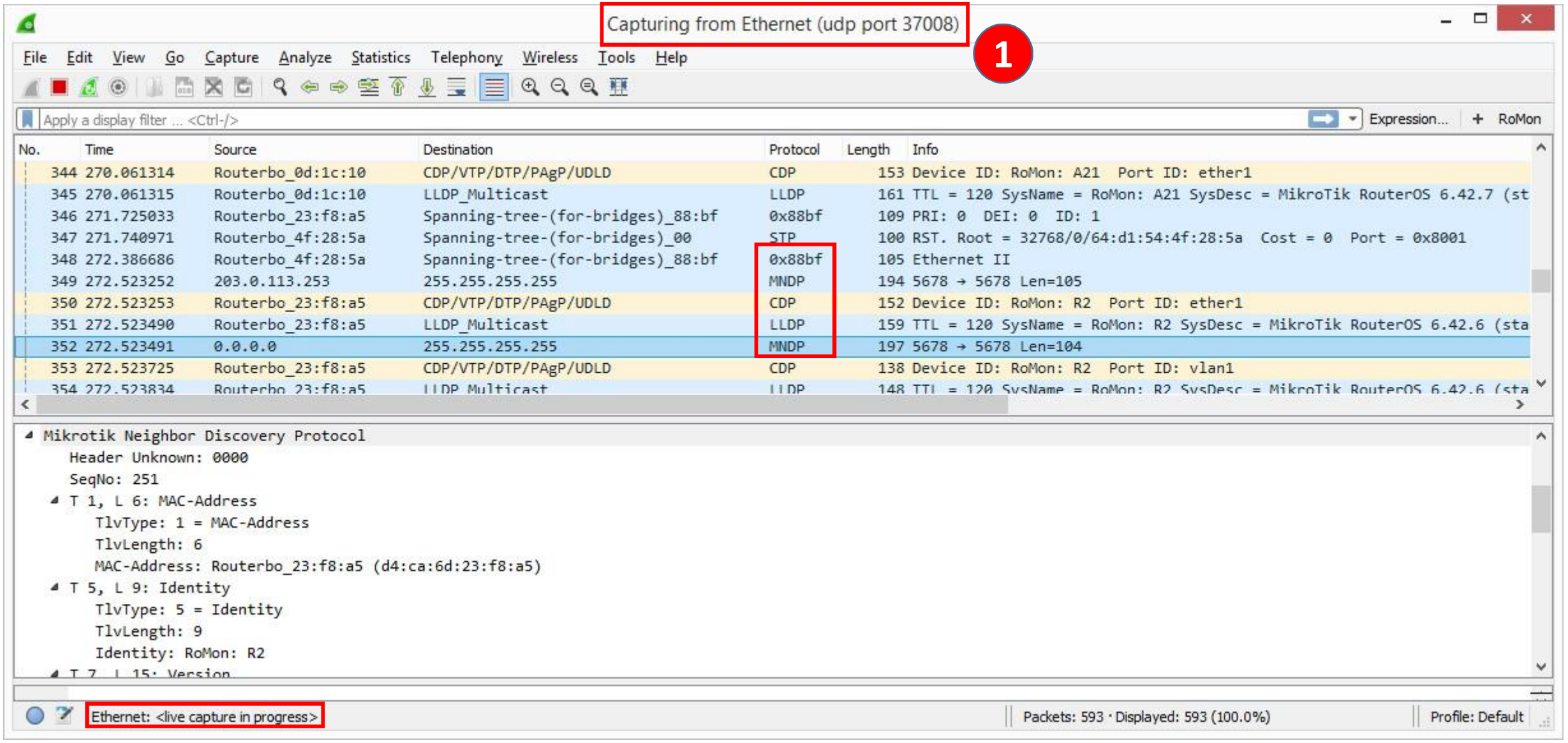
- TZSP stream is sent

- Filter stream in Wireshark
- UDP port 37008

- Start sniffer in Winbox



Live Output

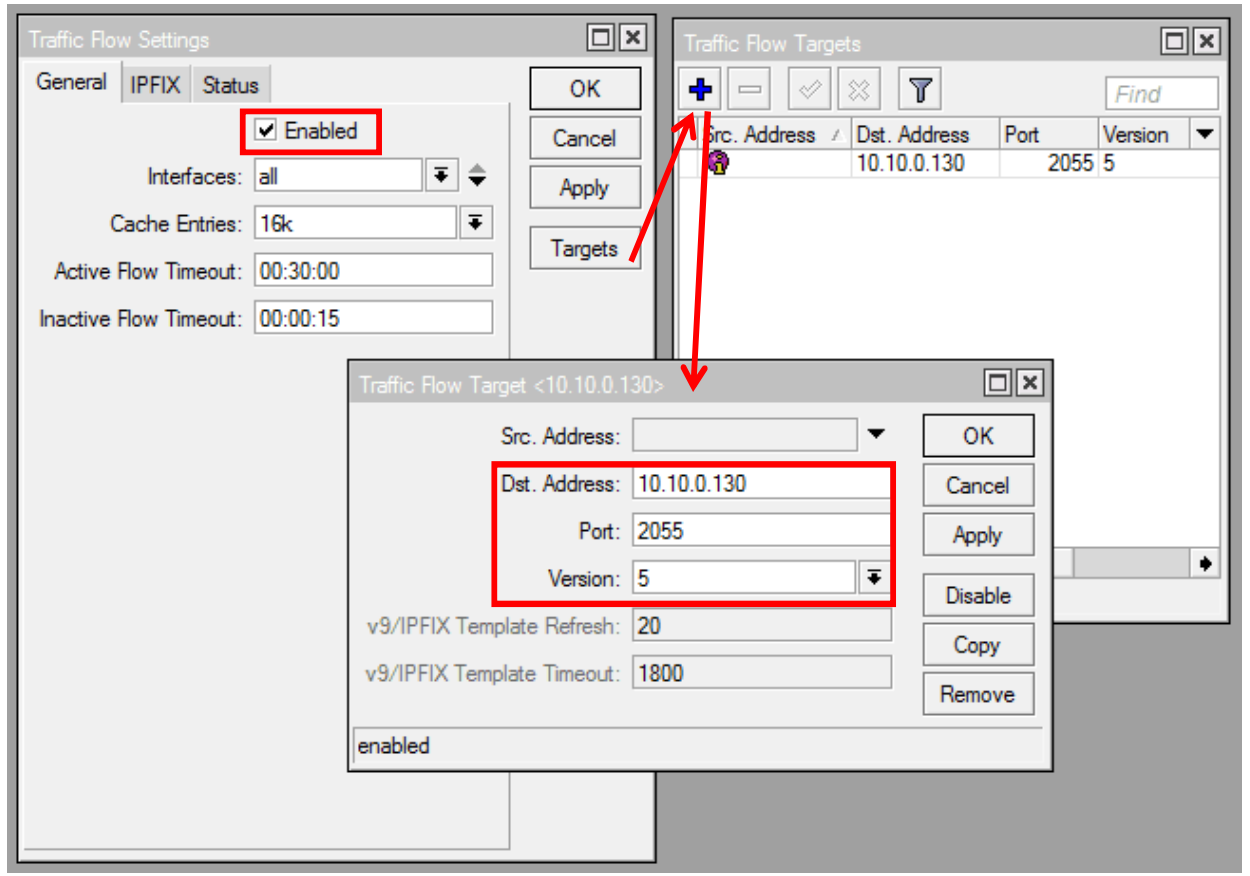

Capturing from Ethernet (udp port 37008)
1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression... + RoMon
No. Time Source Destination Protocol Length Info
344 270.061314 Routerbo_0d:1c:10 CDP/VTP/DTP/PAgP/UDLD CDP 153 Device ID: RoMon: 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
Mikrotik Neighbor Discovery Protocol
Header Unknown: 0000
SeqNo: 251
T 1, L 6: MAC-Address
TlvType: 1 = MAC-Address
TlvLength: 6
MAC-Address: Routerbo_23:f8:a5 (d4:ca:6d:23:f8:a5)
T 5, L 9: Identity
TlvType: 5 = Identity
TlvLength: 9
Identity: RoMon: R2
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



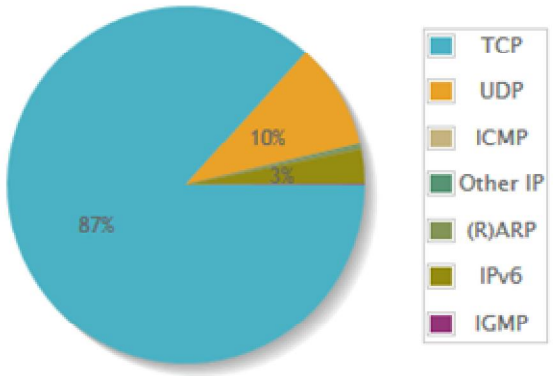
Netflow Collector and Anlysis

- ntop (former) free standard
- Successor ntop-ng
- Requires commercial nProbe to collect Netflow

- Alternative free and open source collectors available

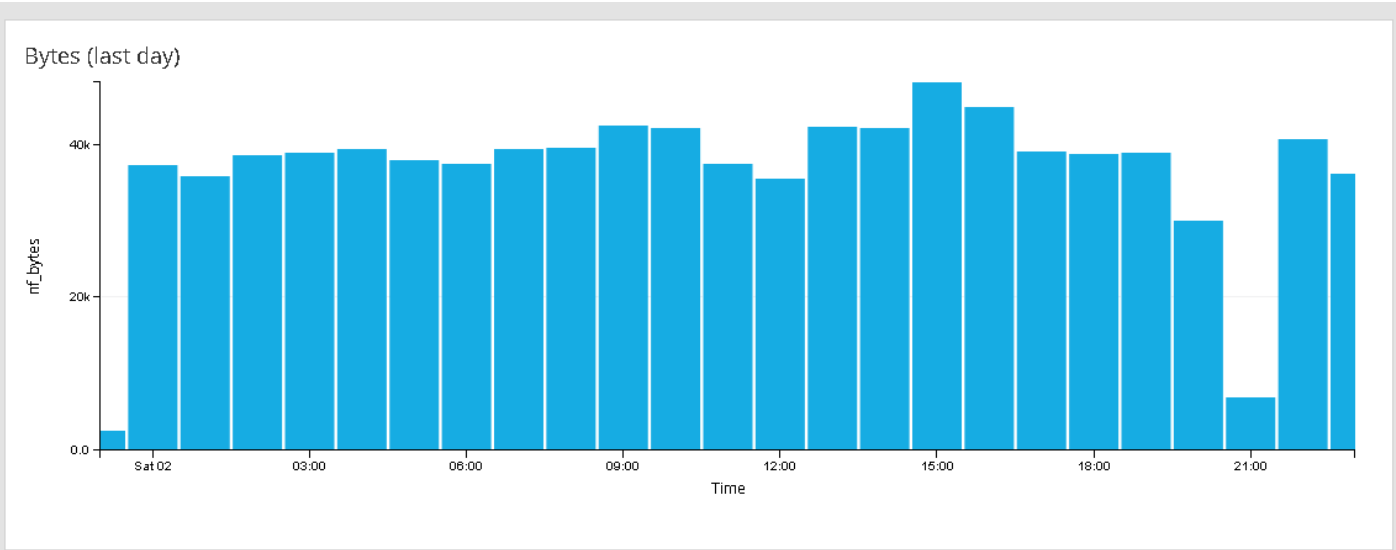
- E.g as in FMS Management Plattform

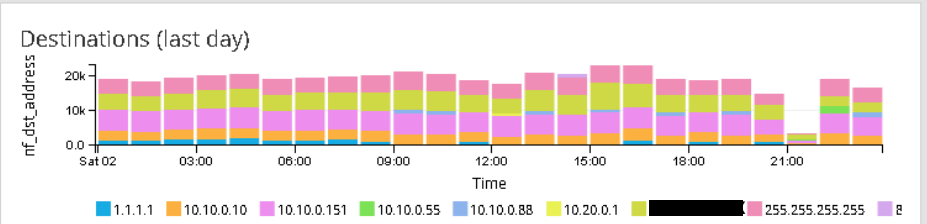
L2/L3 Protocol	Data	Percentage			
IP	905.6 KBytes	96.4%	TCP	834.7 KBytes	92.2%
			UDP	92.5 KBytes	10.2%
			ICMP	0.4 KBytes	0.0%
			ICMPv6	5.1 KBytes	0.6%
			IGMP	0.9 KBytes	0.1%
			Other IP	1.6 KBytes	0.0%
(R)ARP	2.9 KBytes	0.3%			
IPv6	29.6 KBytes	3.2%			

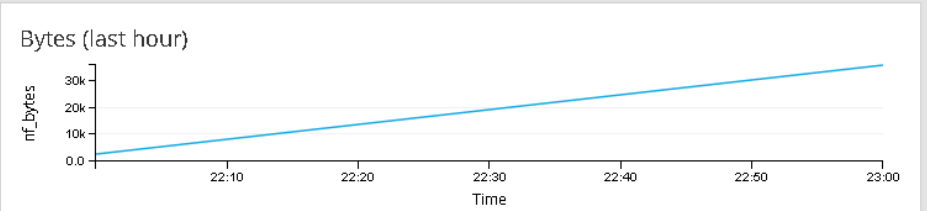


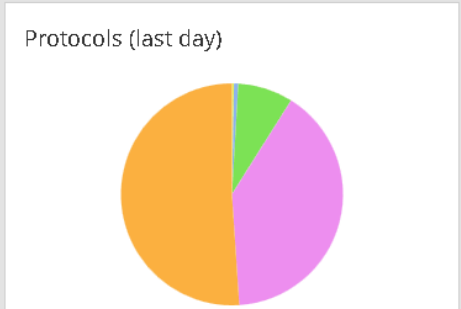
Former ntop GUI

Netflow in FMS Management Plattform

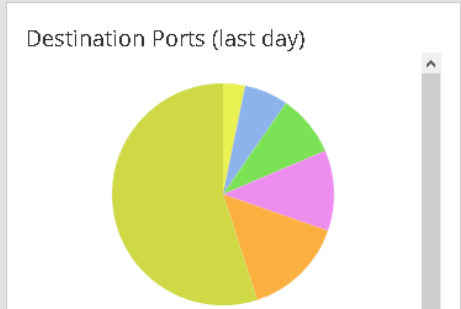




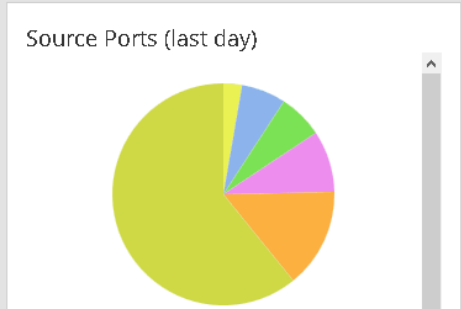




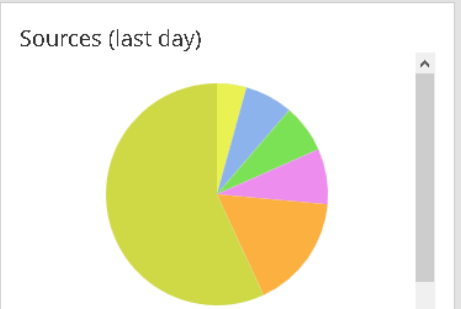
Value	%	Count
Top 5 values		
UDP	51.02%	466,298
TCP	40.01%	365,607
ICMP	8.04%	73,476
IPv6-ICMP	0.63%	5,762
IGMP	0.28%	2,563



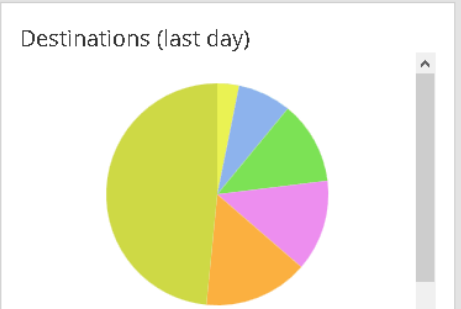
Value	%	Count
Top 5 values		
53	14.71%	134,443
5678	11.73%	107,189
0	8.97%	81,998
443	6.40%	58,520
80	3.21%	29,310



Value	%	Count
Top 5 values		
53	14.51%	132,639
0	8.97%	81,998
443	6.48%	59,250
5678	6.47%	59,105
22	2.72%	24,858



Value	%	Count
Top 5 values		
10.10.0.151	16.67%	148,162
10.10.0.10	8.08%	71,767
[redacted]	7.05%	62,676
10.10.0.55	7.01%	62,312
10.10.0.88	4.29%	38,077



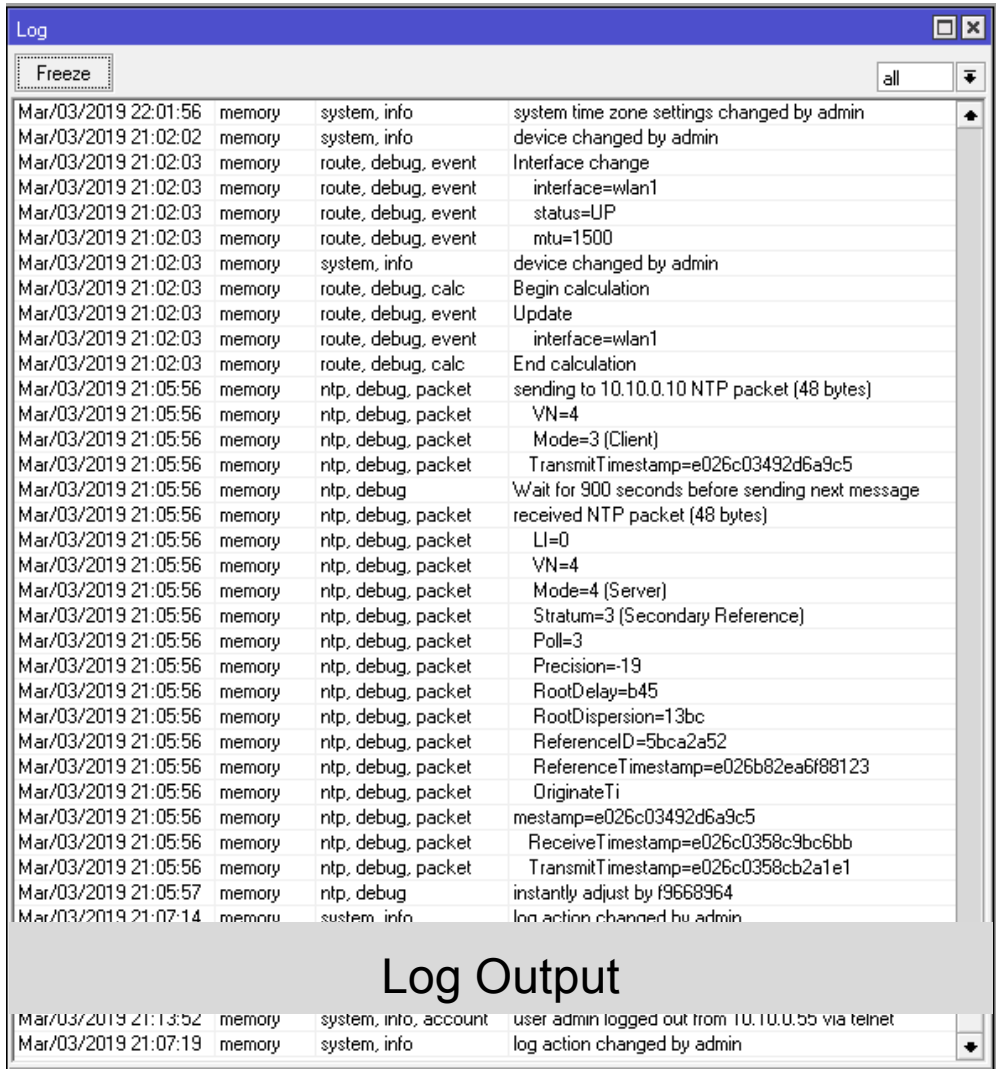
Value	%	Count
Top 5 values		
10.10.0.151	15.22%	135,255
[redacted]	13.31%	118,229
255.255.255.255	12.10%	107,507
10.10.0.10	7.77%	69,085
1.1.1.1	3.17%	28,165

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



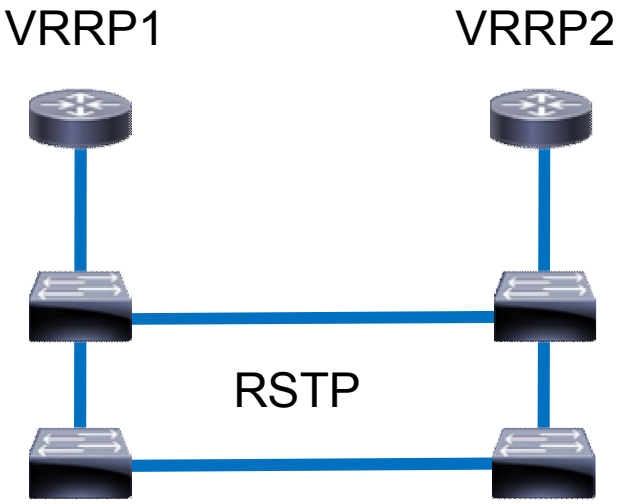
Log Output

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



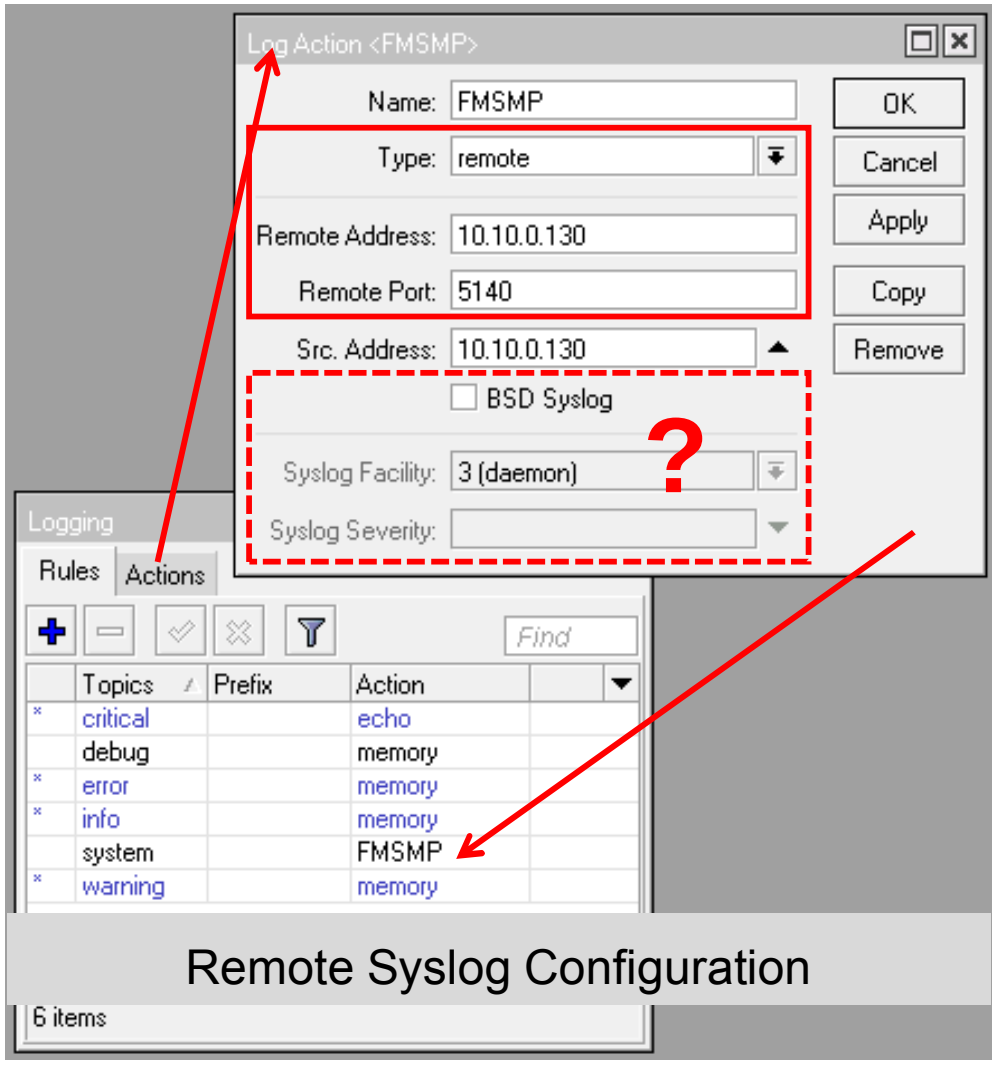
VRRP Setup

FMS Management Platform

- Syslog, Netflow, SNMP traps …
- MongoDB, Elasticsearch …

- Central storage
- Powerful search
- Dashboards
- Alerts

- Enhanced MikroTik support
- E.g. MikroTik MIB, Log syntax



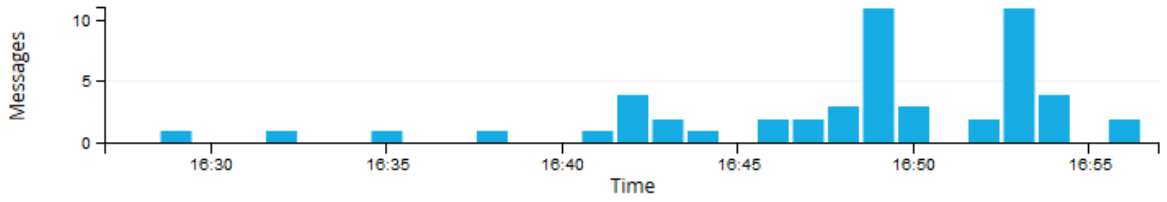
Remote Syslog Configuration

WIFI Connects from Syslog across complete Network

WLAN Connections (last 1/2 hour)

52

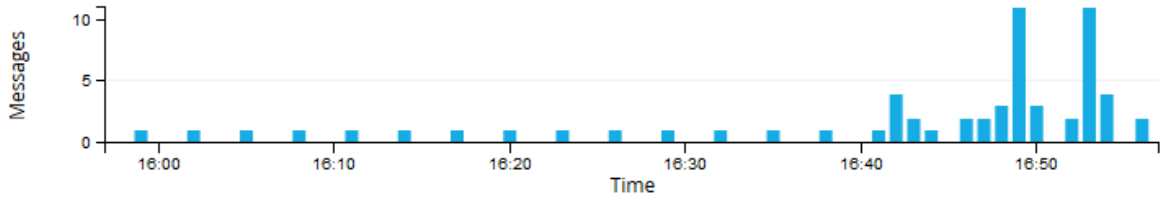
WLAN Connections (last 1/2 hour)



WLAN Connections (last hour)

62

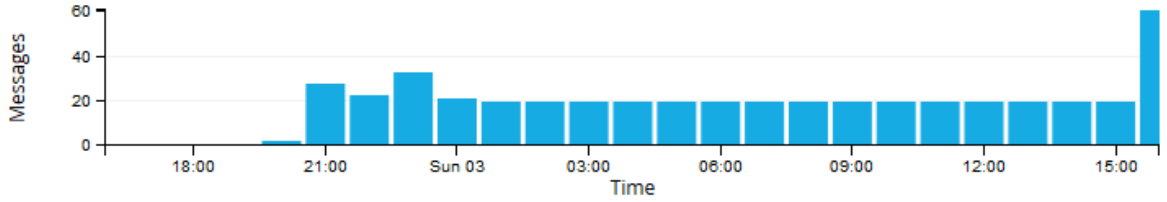
WLAN Connections (last hour)



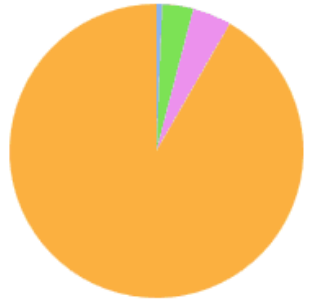
WLAN Connections (last day)

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

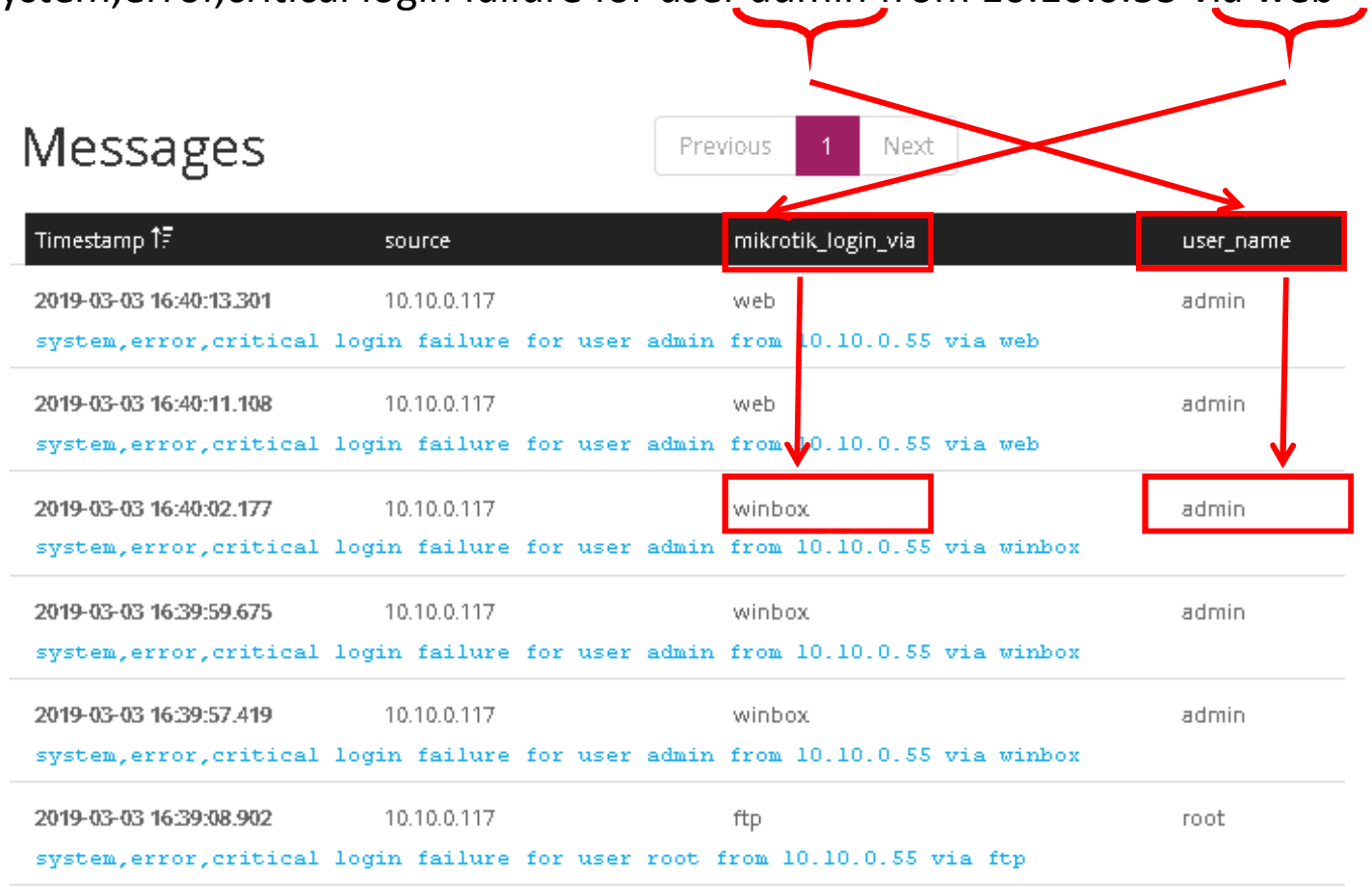
- Make syslog server understand message
- Database fields

- Search
- Sorting
- Analyse

- Login Failure Dashboard

1

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



Failed Logins including Username and Login Type

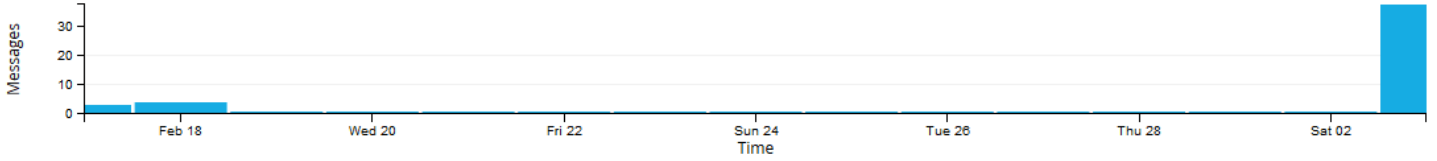
Login Failed (last hour)

37

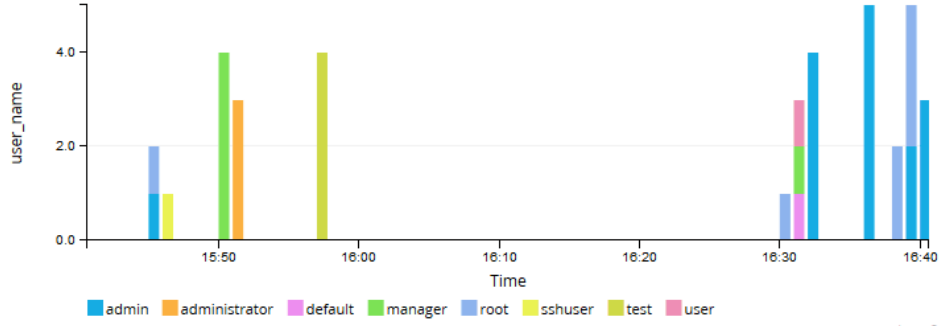
Logins failed (last 7 days)

44

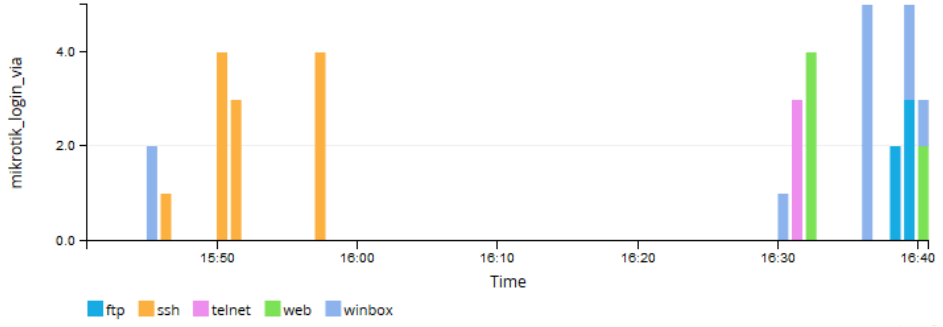
Logins Failed (last 7 days)



Login failed by Username (last hour)



Login failed by Login Type (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

Get in Touch

Are you looking for centralised

and MikroTik aware logging?

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

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

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

Dank u wel!