



Managing and Monitoring

RouterOS



Agenda

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





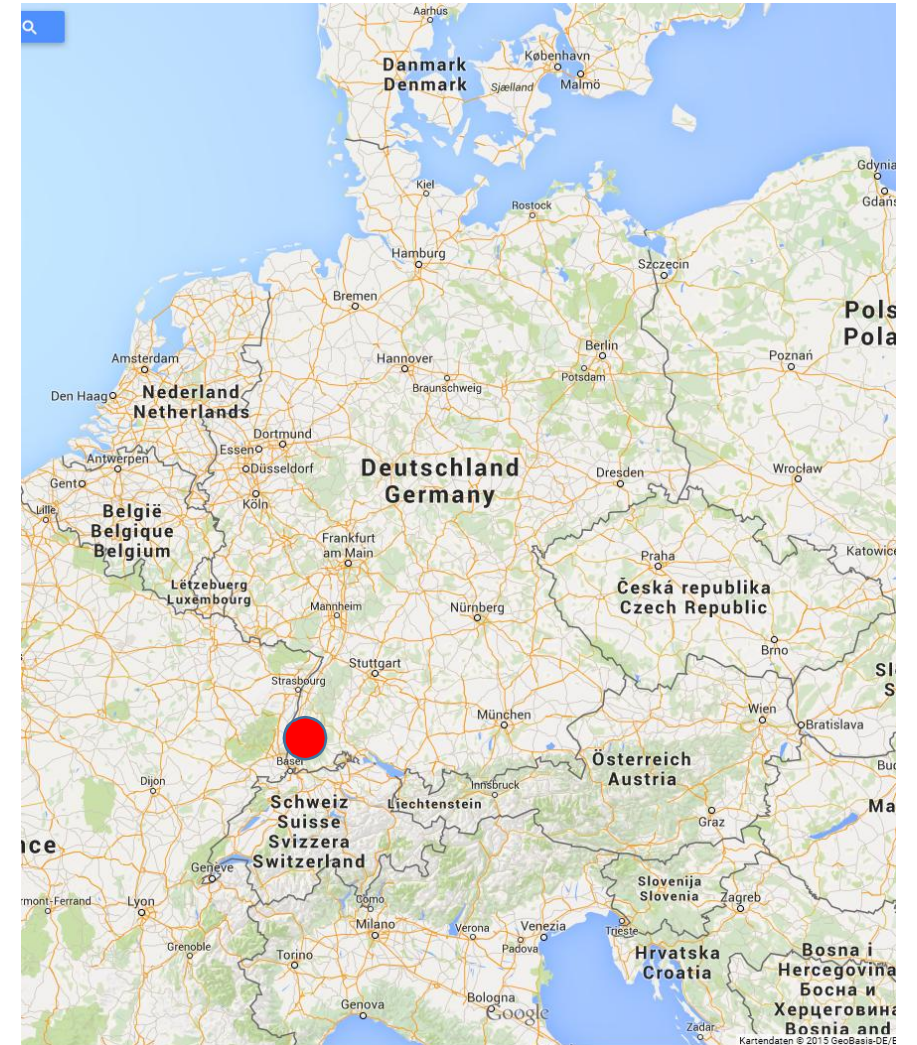
FMS Internetservice GmbH

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

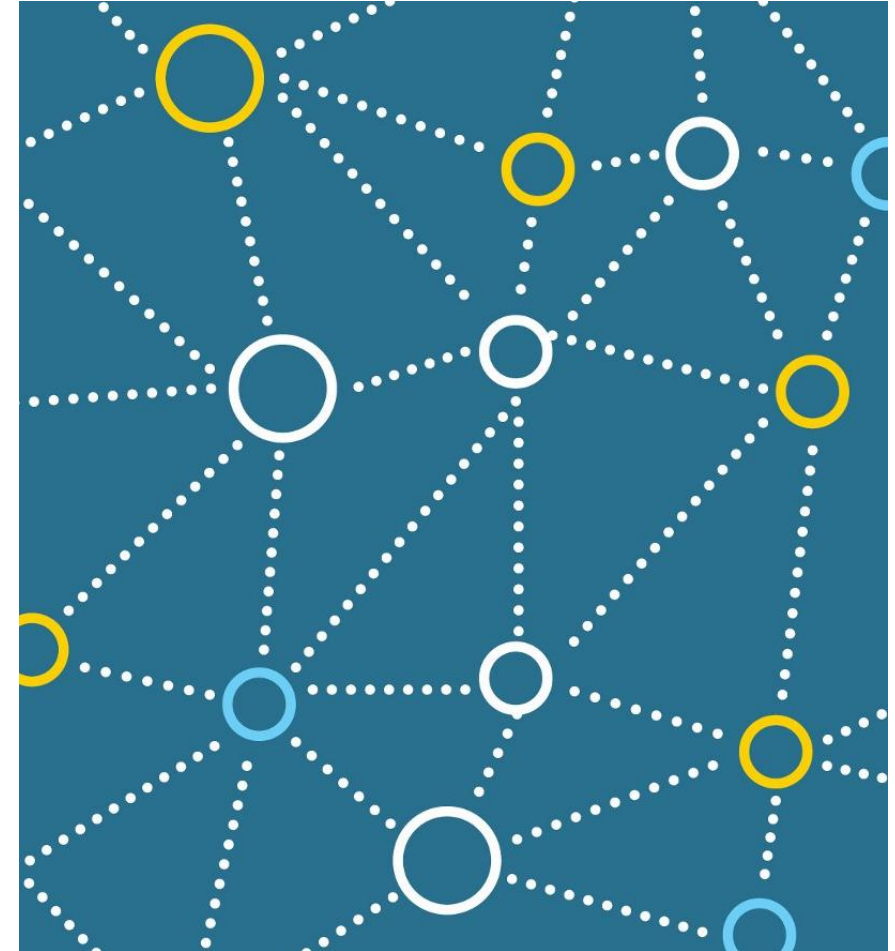
Challenges and Elements



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

■ 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 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 & 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

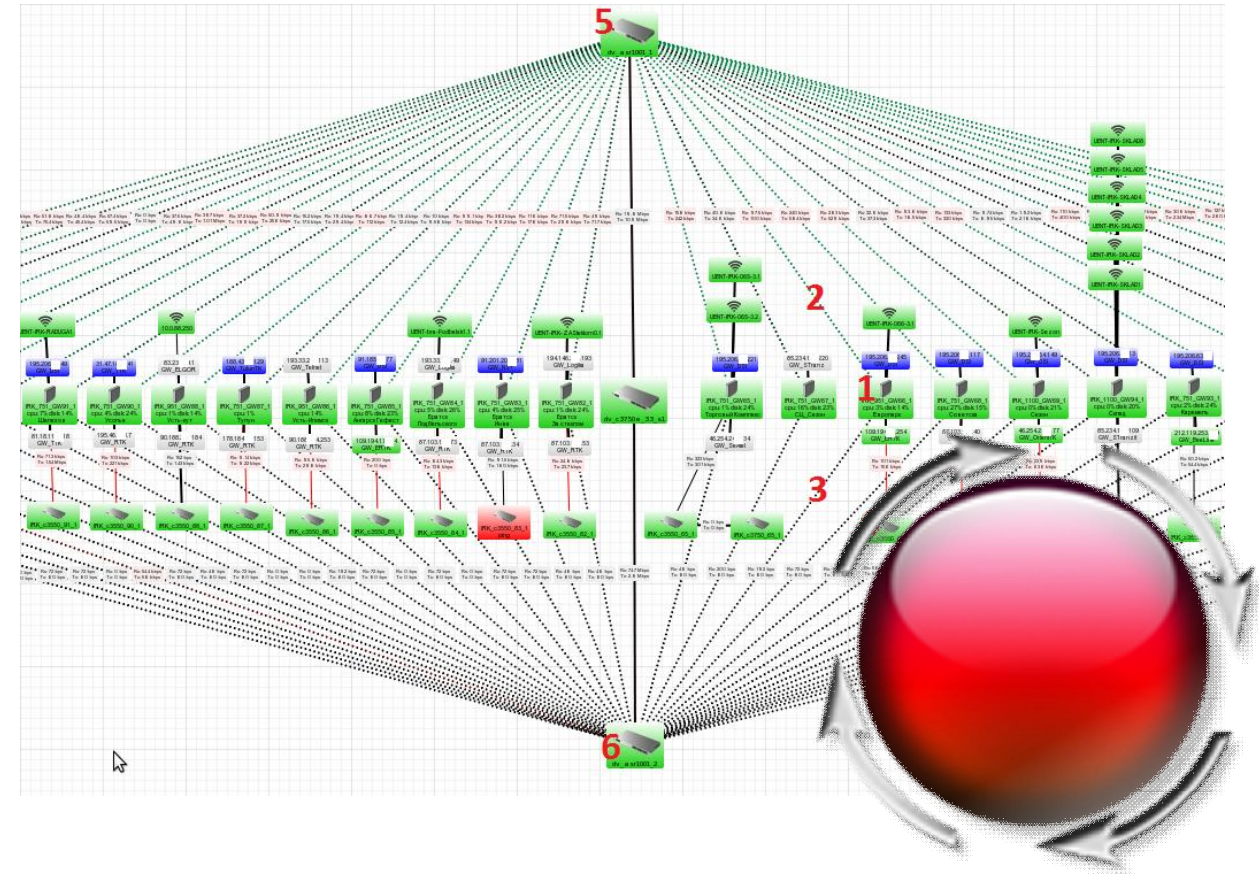
- Common Approaches
 - Separate management and user traffic
 - Management VLAN
 - Tunneling payload (e.g. PPPoE)
 - Tunneling of management (VPN)





Management Approaches

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





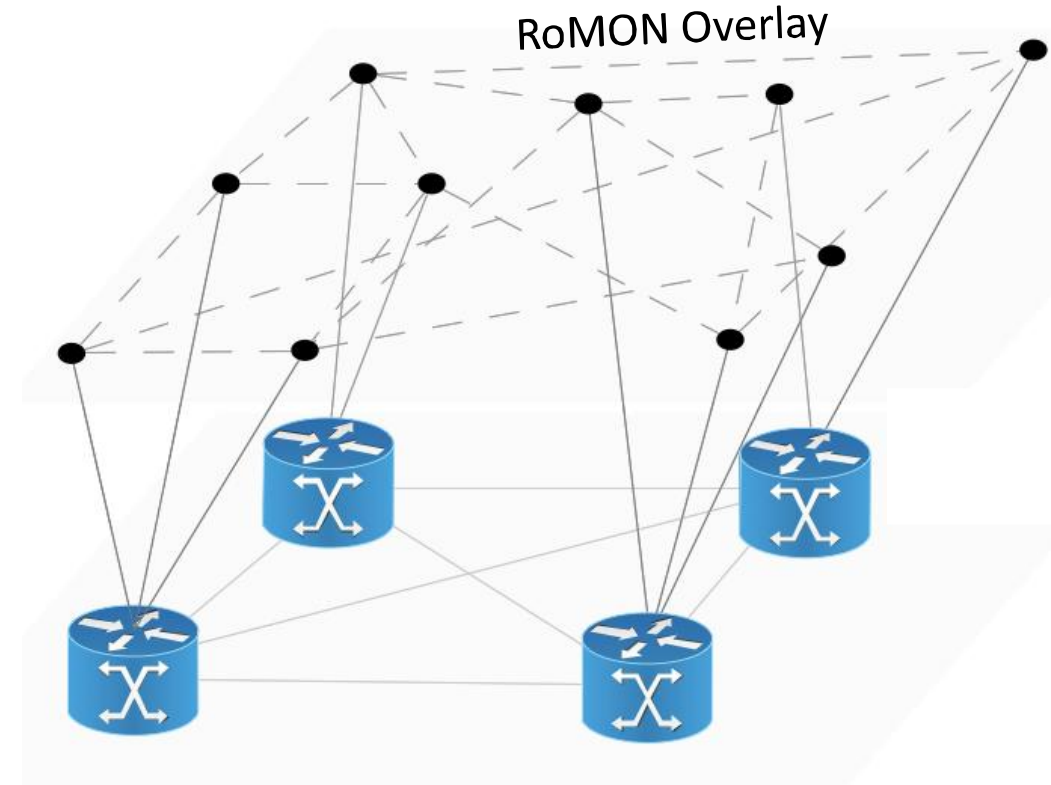
RoMON

Simplify Discovery and Access



RoMON

- 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

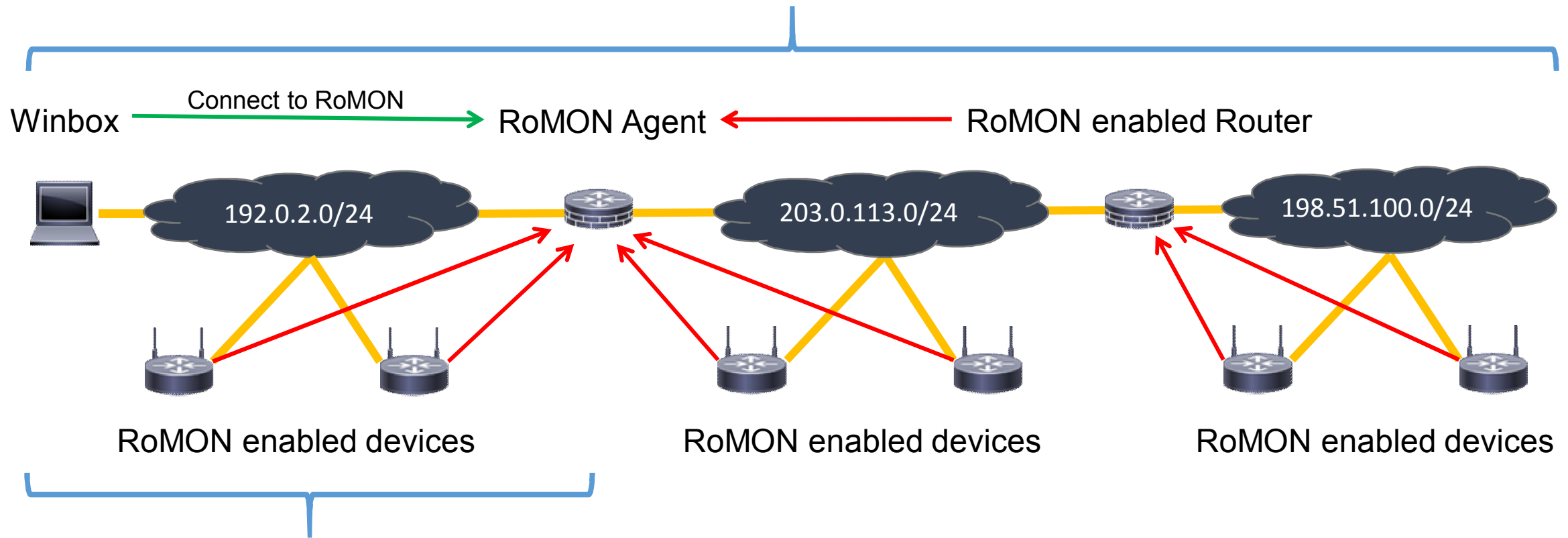
- Creates overlay network
- Only with MikroTik devices
- Not limited to layer-2 broadcast domain
- Winbox: discovery and MAC connection
- Winbox: RoMON agent connection

- 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

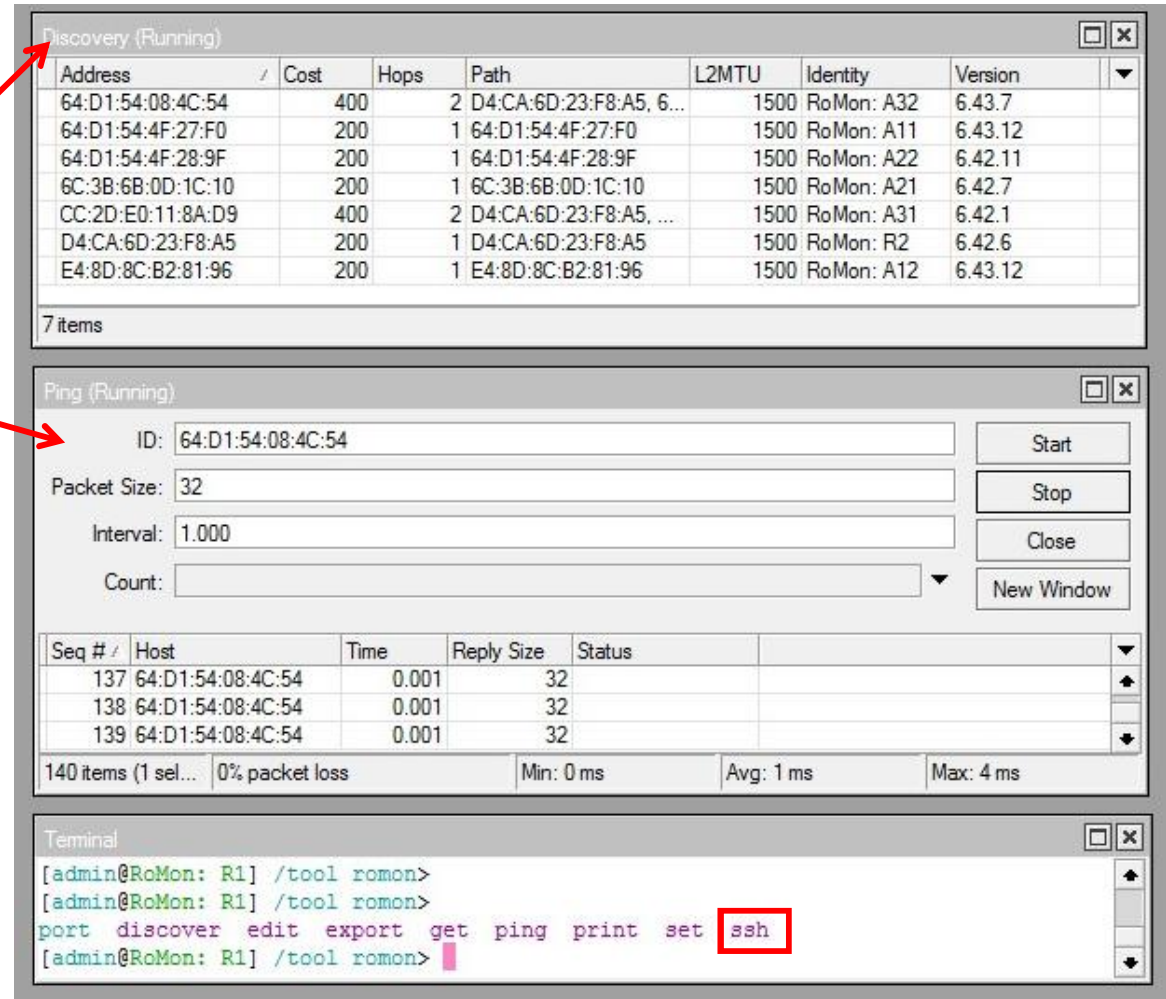
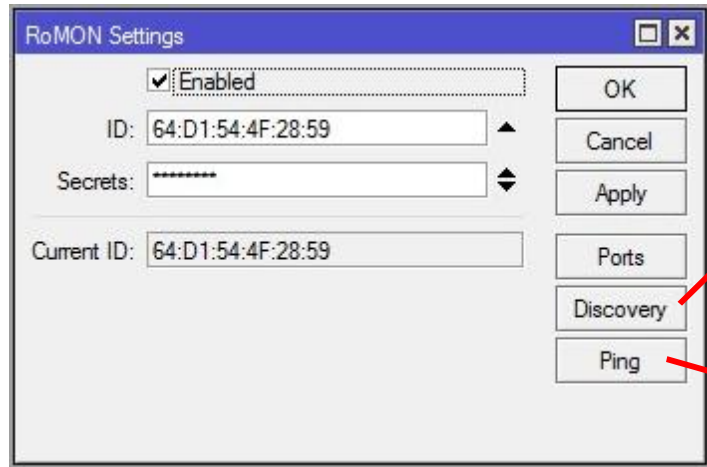
- Enable RoMON
- Optional but recommended
 - Set ID manually
 - Use secret(s)
- Optional
 - Customize interface configuration

The screenshot illustrates the steps to configure RoMON. It shows the 'Tools' menu with 'RoMON' highlighted. The 'RoMON Settings' dialog is open, showing 'Enabled' checked, 'ID: 64:D1:54:4F:28:59', and 'Secrets: *****'. The 'Ports' button is highlighted. The 'RoMON Ports' table shows one entry: 'all' with 'Forbid' set to 'no' and 'Cost' set to '100'. The 'New RoMON Port' dialog is open, showing 'Interface: all', 'Forbid' unchecked, and 'Cost: 100'.

Interface	Forbid	Cost
all	no	100



RoMON Tools



- Discovery
- Ping
- CLI: ssh
- Winbox



Standard Tools in RoMON Network

Ping / MAC Ping

The screenshot shows the 'Ping (Running)' window with the 'General' tab selected. The 'Ping To' field is highlighted with a red box and contains the MAC address '64:D1:54:08:4C:54'. Other fields include 'Interface', 'ARP Ping' (unchecked), 'Packet Count', and 'Timeout: 1000 ms'. The results table shows 29 items, all with a 'timeout' status.

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

The screenshot shows the 'Ping (Running)' window with the 'ID' field highlighted by a red box, containing the MAC address '64:D1:54:08:4C:54'. Other fields include 'Packet Size: 32', 'Interval: 1.000', and 'Count'. The results table shows 30 items with successful replies and a 0% packet loss rate.

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

The screenshot shows the WinBox v3.18 interface. The 'Connect To' field is set to '64:D1:54:4F:28:5C'. The 'Login' field is 'admin'. The 'RoMON Agent' dropdown is set to 'RoMon: R1'. The 'Connect To RoMON' button is highlighted with a red box and a '2' in a red circle. A red arrow points from this button to the 'Connect To' field. Below the configuration, the 'Managed' tab is active, showing a table of discovered devices. The 'IP Address' column is highlighted with a red box and a '1' in a red circle. A red arrow points from this column to the text 'Devices within the layer-2 network discovered' on the left. The table contains the following data:

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

WinBox v3.18 (Addresses-Site-1)

File Tools

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

Login: admin

Password:

Session: <own>

Note: RoMon: R1

Group:

Keep Password

Autosave Session

Open In New Window

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

Managed RoMON Neighbors

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:D1:54:4E:27:E0	200	1	64:D1:54:4E: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

Connected to
RoMON agent

3

RoMON
discovery
through agent

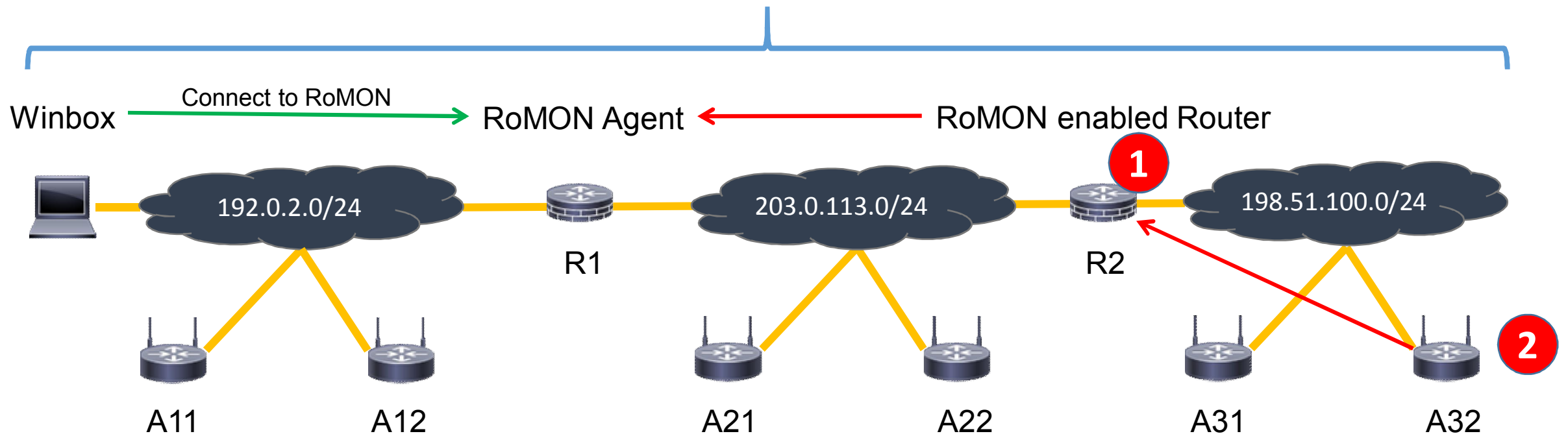
4

Two hops to
reach



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

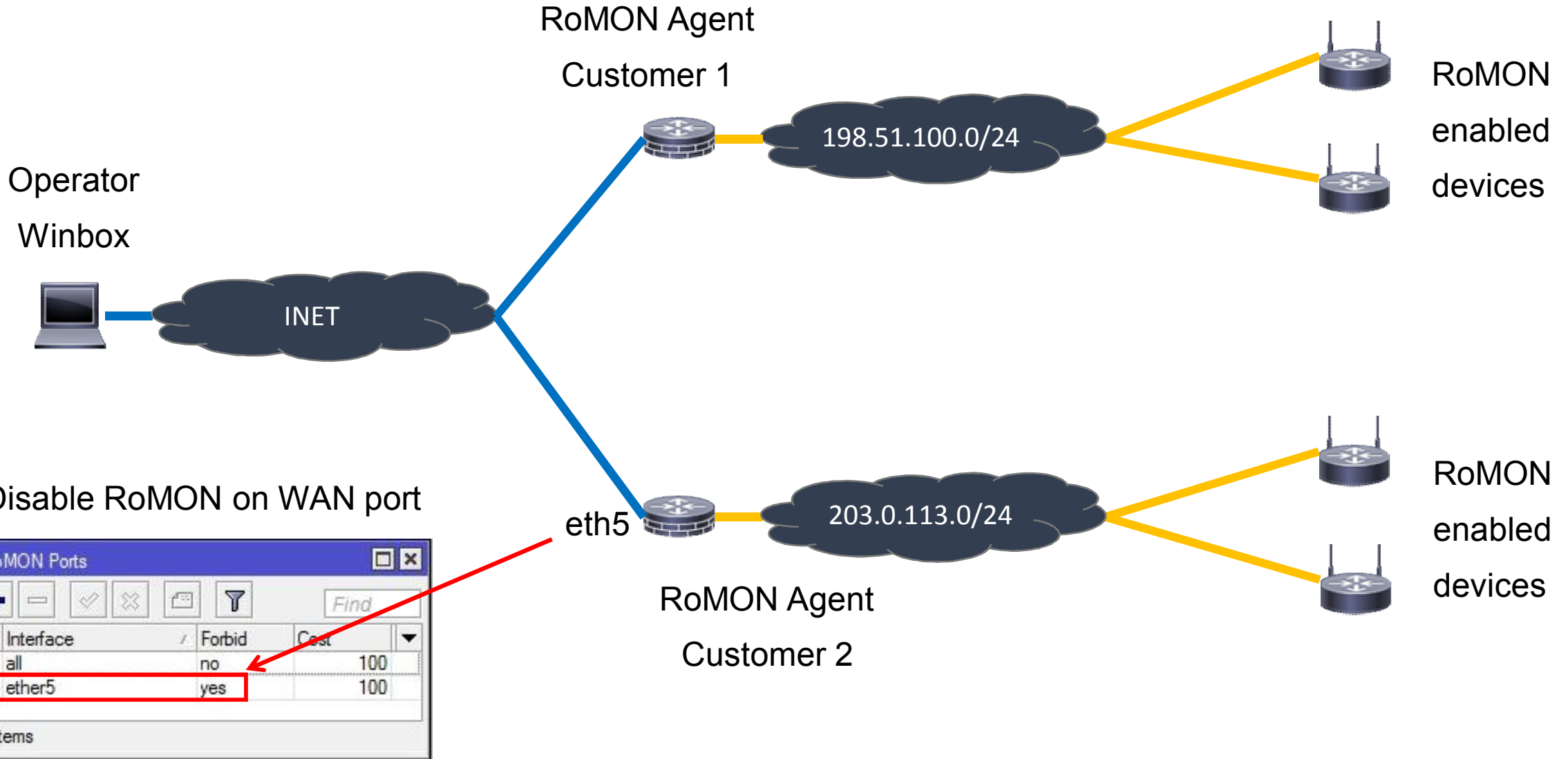
- Remote discovery and management

- Branch offices
- Customer networks





Remote Network Discovery



Disable RoMON on WAN port

Interface	Forbid	Cost
all	no	100
ether5	yes	100

2 items



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

The screenshot displays the HSNM Hotspot Manager web interface. The browser address bar shows `hsm1.intern.fmsweb.de/#`. The main navigation bar includes 'Admin', 'Data', and 'Search'. The left sidebar lists system components, with 'Domain_KN-23479' selected and highlighted in green. A red box highlights the menu icon next to this domain, and a red arrow points from it to the 'Add Gateway' option in the 'Edit' menu. The 'Edit' menu also includes 'Add User', 'Edit', 'Copy', 'Cut', 'Delete', and 'Lock/Unlock'. The 'Admin' menu includes 'Card Management', 'Dashboard', 'Display All Connected Users', 'Display All Users', and 'List of Access Points'. The right panel shows a dashboard with various metrics: 'Connections' (3), 'Traffic' (370.17 KB), 'GW Sold' (\$1), and 'NET Traffic' (Tx 0.01/F). A line graph at the bottom shows 'Welcome Portal Visitors'.

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

Access Points Map

Gateway

Gateway

Connections

Traffic

GW Sold

NET

3

370.17 KB

\$ 1

100%+

100%+

100%+

of Connections

Welcome Portal Visitors



Choosing Hardware and RouterOS Type

hsnm 1.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

Gateway

Add or edit a hotspot gateway for the manager

General Data

Gateway Name	Gateway5
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

WAN Interface

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

Undefined

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

1 Hour



Initial Configuration

hsnm1.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 lists domains and gateways. The domain 'Domain_KN-23479' is highlighted in green, and its menu icon is also highlighted with a red box. A red arrow points from this icon to the 'Walled Garden' option in the central menu, which is also highlighted with a red box. Other menu items include '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', and 'Translations'.

The screenshot shows the 'Walled Garden' configuration page. The page 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 the following 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

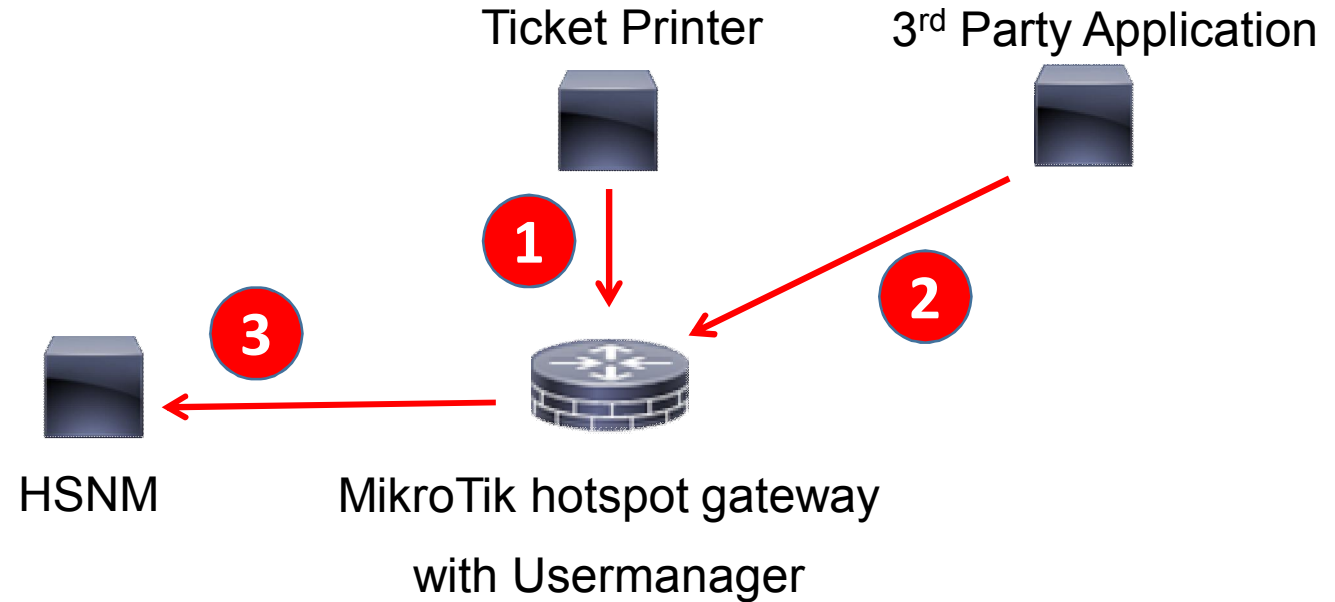
Legacy ticket printer
Creating Usermanager accounts

2

Legacy 3rd 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

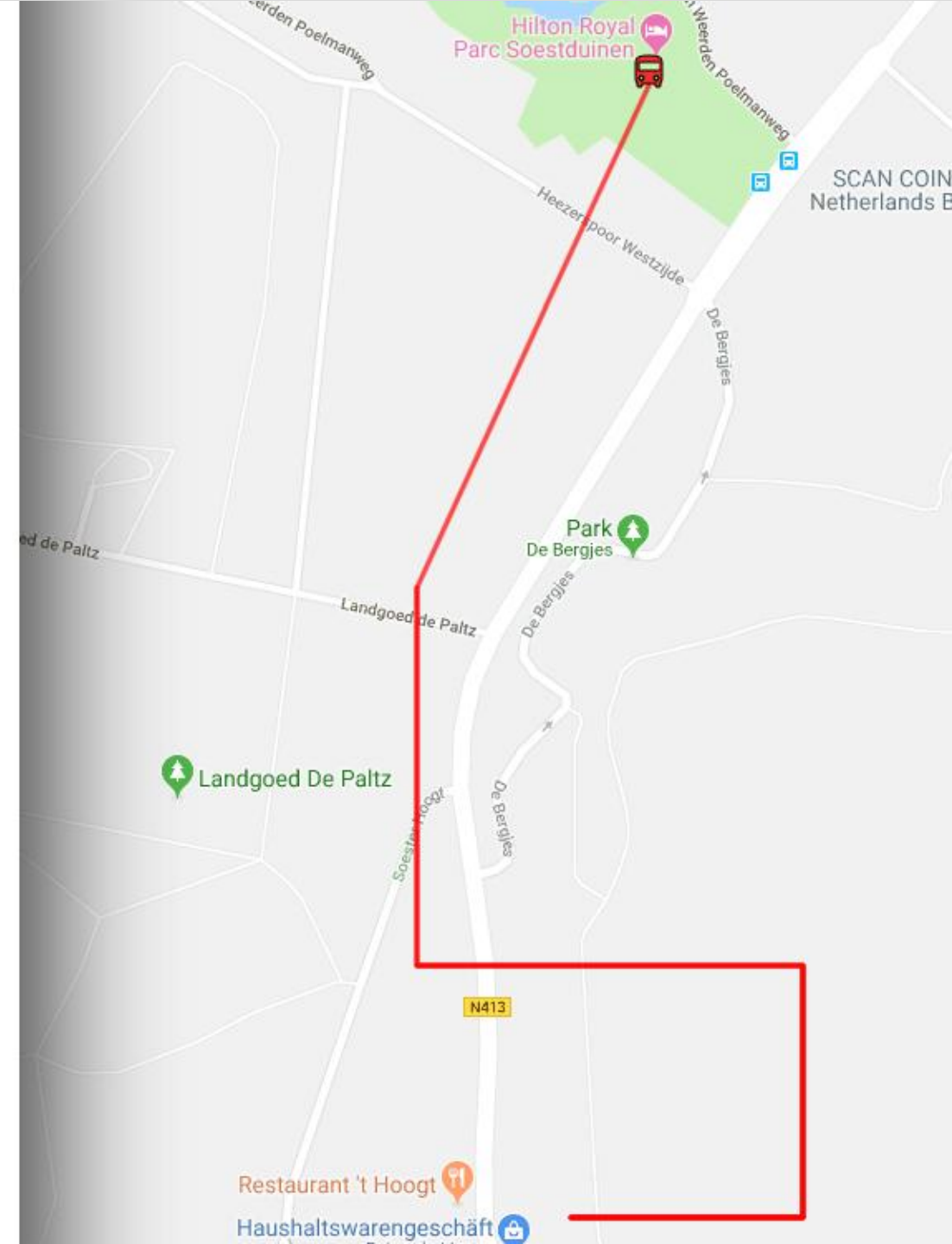
- Cut
- Delete
- Lock/Unlock

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

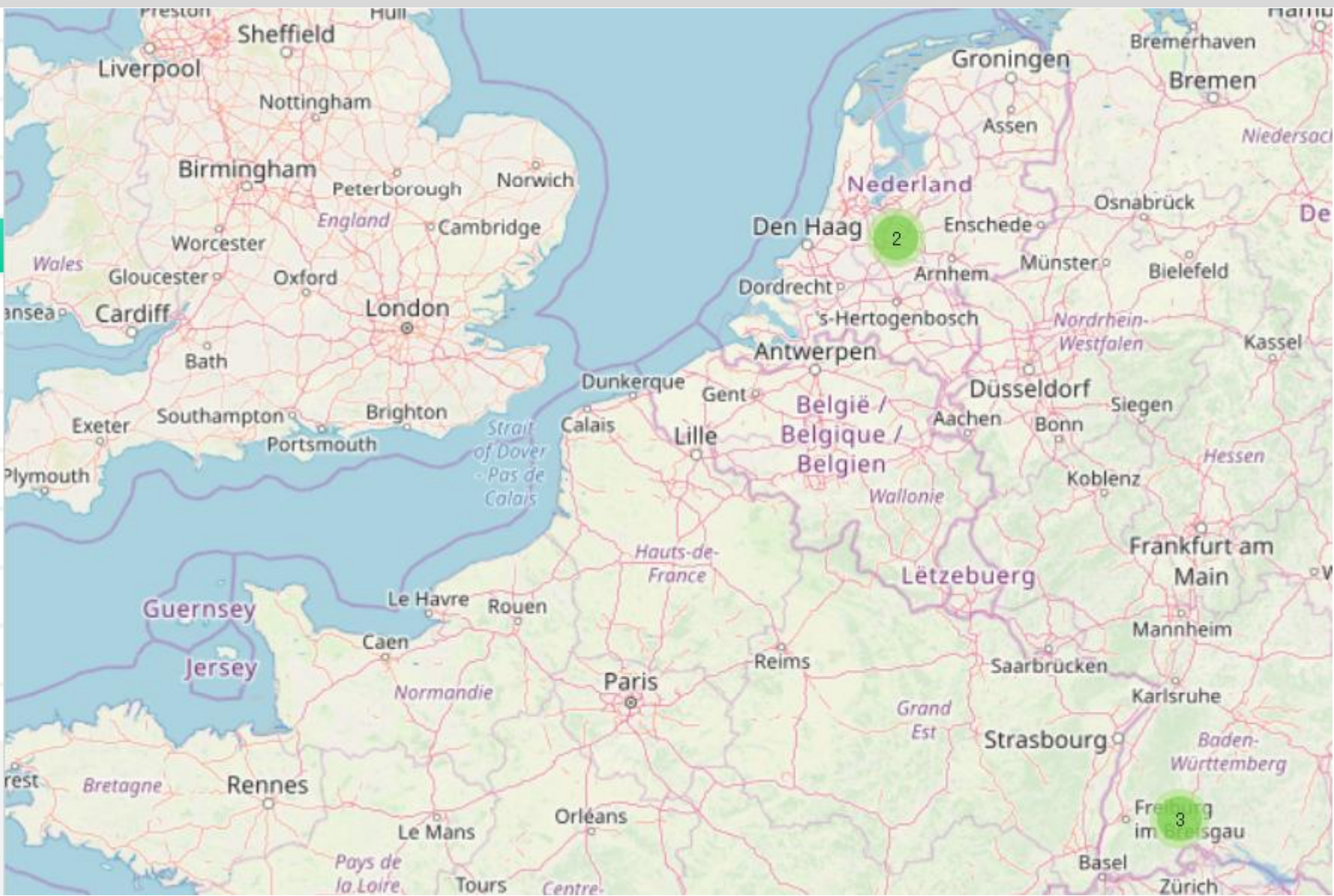
- Bypass or Lock IP/Mac Address
- Custom Apps
- Custom Images
- Surveys, Quizzes and Tests
- Templates
- Translations
- User Interface Preview
- Walled Garden





Hotspot Network Manager (HSNM)

- ▶ FMS-I estZ
- ▶ 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 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-73842
- Manager: Voucher und Paypal
- Manager: Voucher und Paysafe

Default

- Access Point Map

Edit

- Edit
- Copy
- Cut
- Delete

Admin

- List of Access Points



Gateway

Access point

Edit

- 📍 Edit
- 📄 Copy
- 🗑️ Delete

Admin

- 📊 Dashboard
- ⚙️ Download Access Point Config Files
- 🔗 Manufacturer's Management Interface**

Access point
context menu



Hotspot Network Manager (HSNM)

Direct web
interface access
for gateways and
access points

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

Gateway Configuration
Manufacturer's Web Management

MikroTik

RouterOS v6.42.1

You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

WebFig Login:

Login:

Password:

Winbox Telnet Graphs License Help

© mikrotik



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 | 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

Packet Sniffer Settings

General Streaming Filter

Memory Limit: 100 kb

Only Headers

Memory Scroll

File Name: Sniffer

File Limit: 1000 kb

OK

Cancel

Apply

Start

Stop

Packets

Connections

Hosts

Protocols

stopped

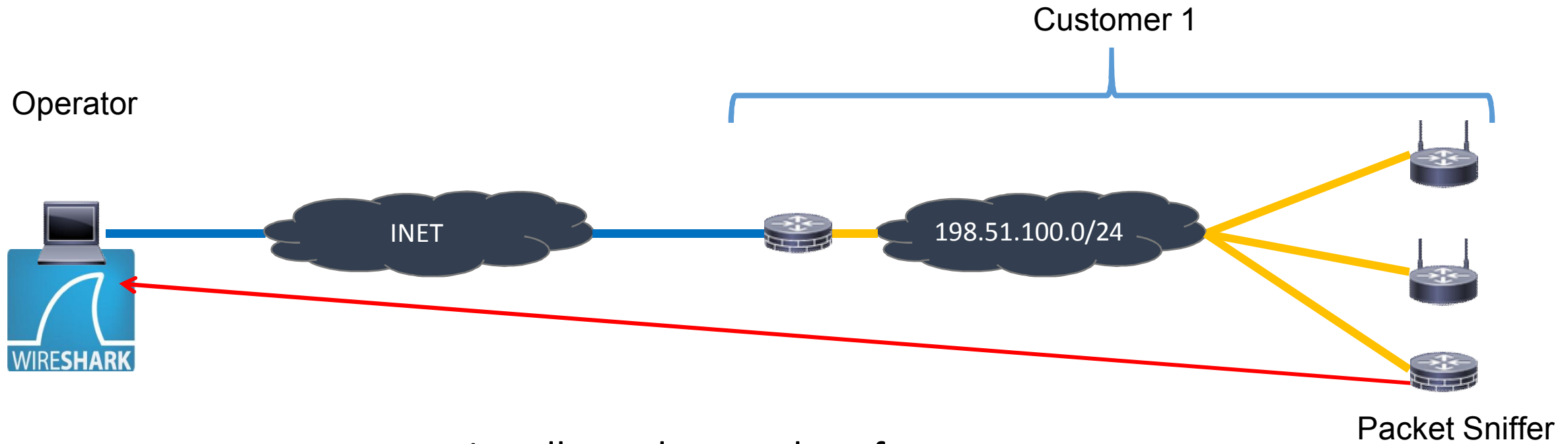
File List

File Name	Type	Size	Creation Time
Sniffer	file	1000.1 KiB	Mar 02/2019 17:28:23
flash	disk		Jan/01/1970 01:00:05
flash/pub	directory		Jan/02/1970 01:03:32
flash/skins	directory		Jan/01/1970 01:00:05

4 items (1 selected) | 12.5 MiB of 16.0 MiB used | 22% free



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

The image shows a screenshot of the Wireshark network sniffer interface and its Packet Sniffer Settings dialog box. The Wireshark window is titled "The Wireshark Network" and shows a capture filter of "udp port 37008" applied to the "Ethernet" interface. The Packet Sniffer Settings dialog box is open, showing the "Filter" tab with "Streaming Enabled" and "Filter Stream" checked, and the "Server" field set to "192.0.2.1". A red circle with the number "1" highlights the "Streaming Enabled" checkbox, and another red circle with the number "2" highlights the "udp port 37008" filter text. The status bar at the bottom of the Wireshark window indicates "Ready to load or capture", "No Packets", and "Profile: Default".



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

▲ 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
▲ T 7, L 15: Version

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



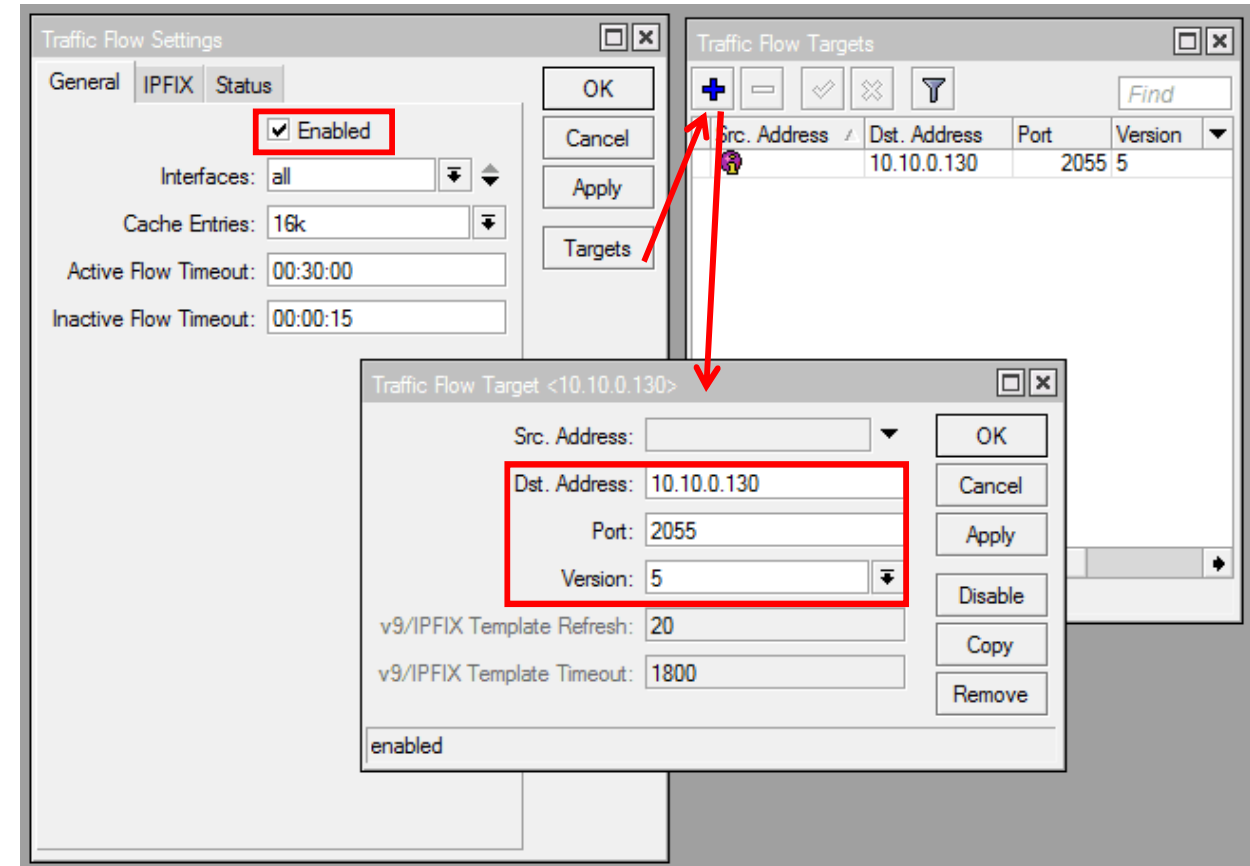
Traffic Flow

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





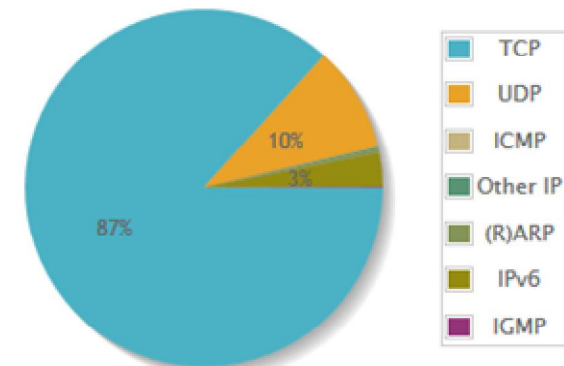
Netflow Collector and Analysis

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

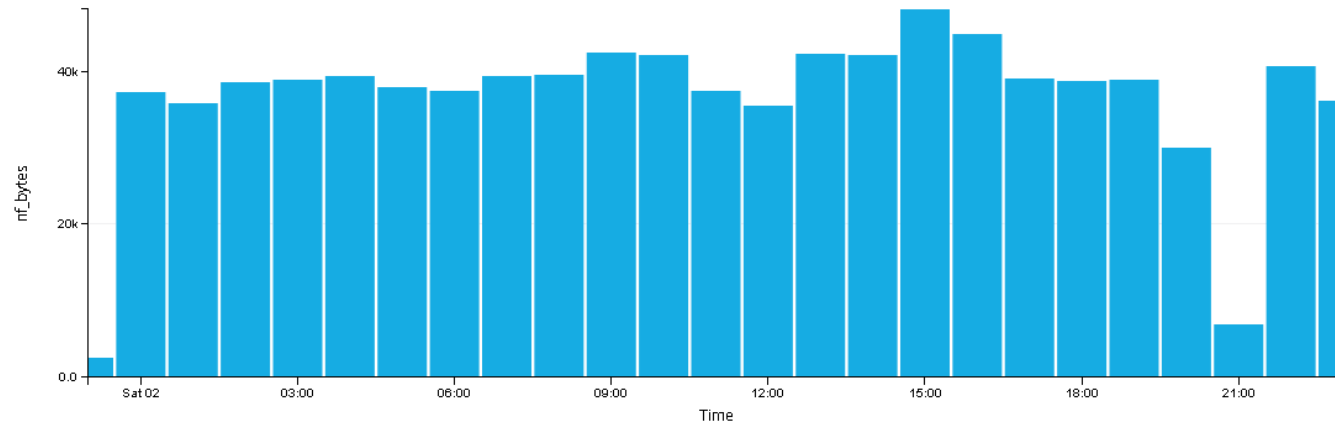


Former ntop GUI

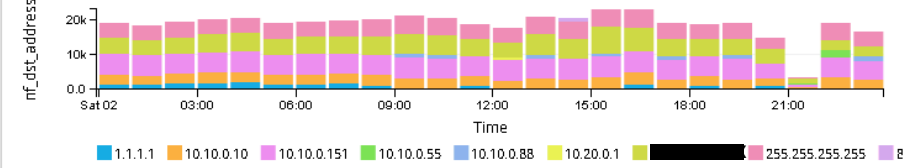


Netflow in FMS Management Platform

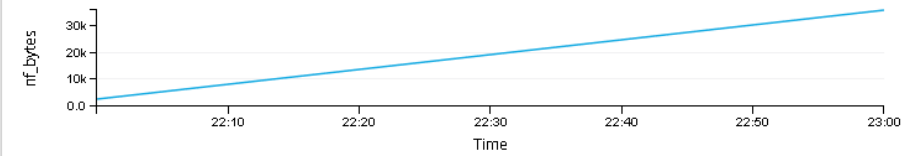
Bytes (last day)



Destinations (last day)



Bytes (last hour)



Protocols (last day)



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

Destination Ports (last day)



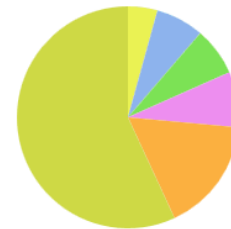
Value	%	Count
Top 5 values		
53	14.71%	134,443
5678	11.73%	107,189
0	8.97%	81,998
443	6.40%	58,520
80	3.21%	29,310

Source Ports (last day)



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

Sources (last day)



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

Destinations (last day)



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

The screenshot shows a 'Log' window with a 'Freeze' button and a dropdown menu set to 'all'. The log entries are as follows:

Time	Source	Category	Message
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=e026b82ea6f88123
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

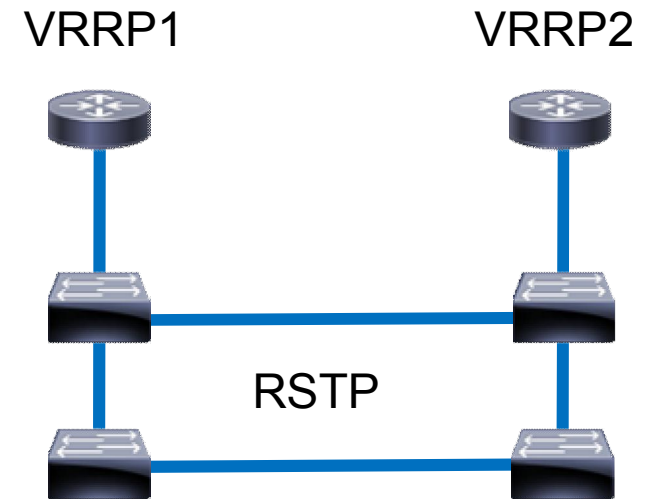
Log Output

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 'Log Action <FMSMP>' configuration window. The 'Name' field is 'FMSMP' and the 'Type' is 'remote'. The 'Remote Address' is '10.10.0.130' and the 'Remote Port' is '5140'. The 'Src. Address' is '10.10.0.130'. There is an unchecked checkbox for 'BSD Syslog'. The 'Syslog Facility' is '3 (daemon)' and the 'Syslog Severity' is empty. A red question mark is placed over the 'Syslog Facility' dropdown. Below this, a 'Logging' section shows a table of rules and actions.

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

6 items

Remote Syslog Configuration

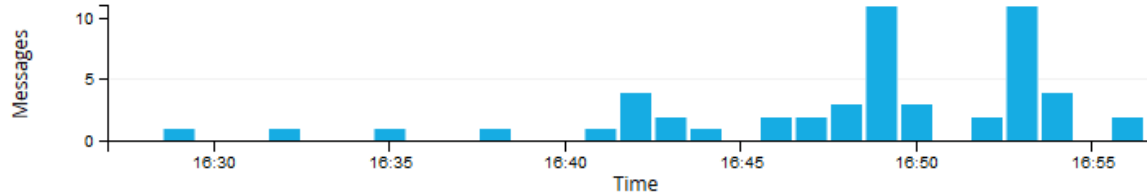


WIFI Connects from Syslog across complete Network

WLAN Connections (last 1/2 hour)

52

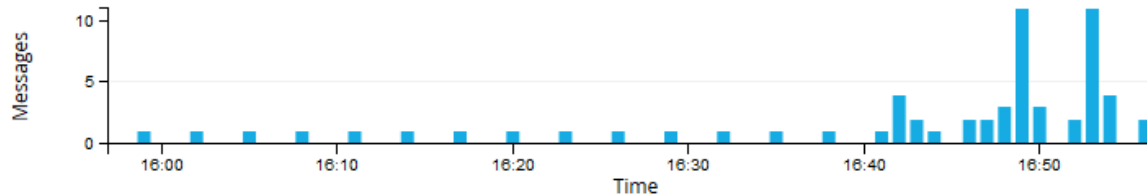
WLAN Connections (last 1/2 hour)



WLAN Connections (last hour)

62

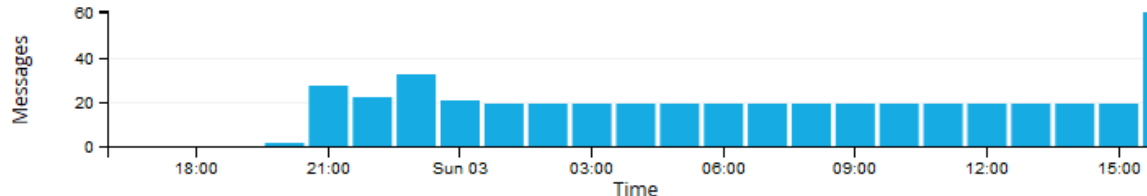
WLAN Connections (last hour)



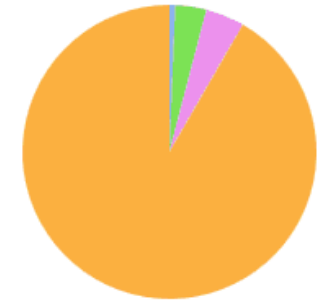
WLAN Connections (last day)

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

Previous 1 Next

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

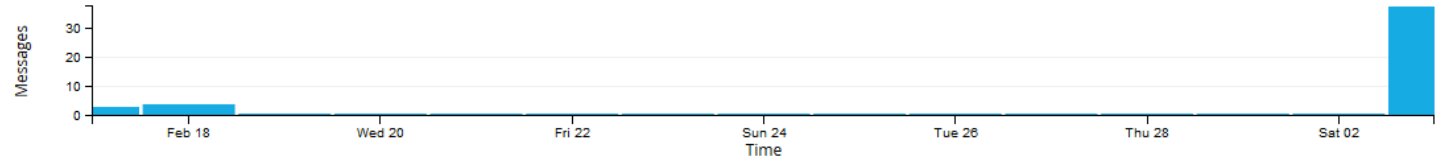
Login Failed (last hour)

37

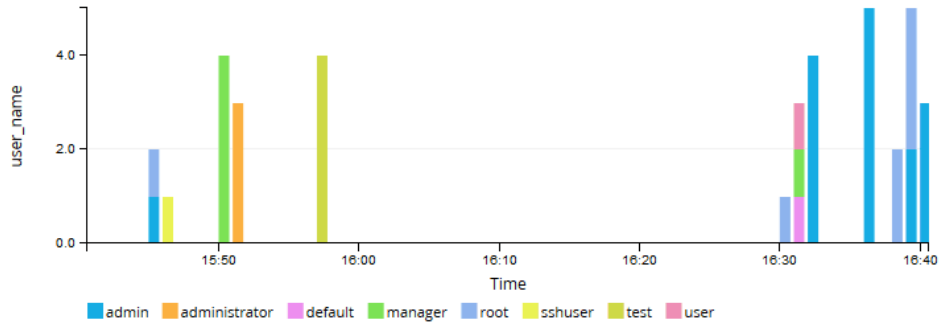
Logins failed (last 7 days)

44

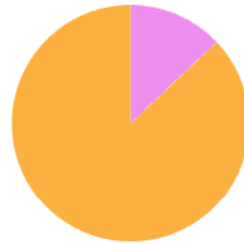
Logins Failed (last 7 days)



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)



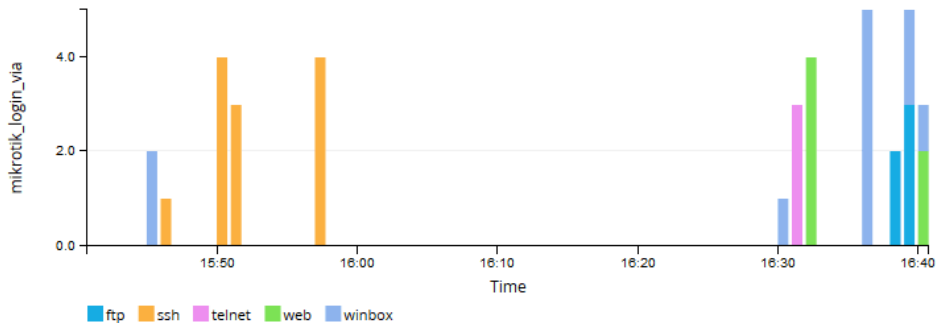
Value	%	Count
Top 5 values		
admin	40.54%	15
root	18.92%	7
manager	13.51%	5
test	10.81%	4
administrator	8.11%	3

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

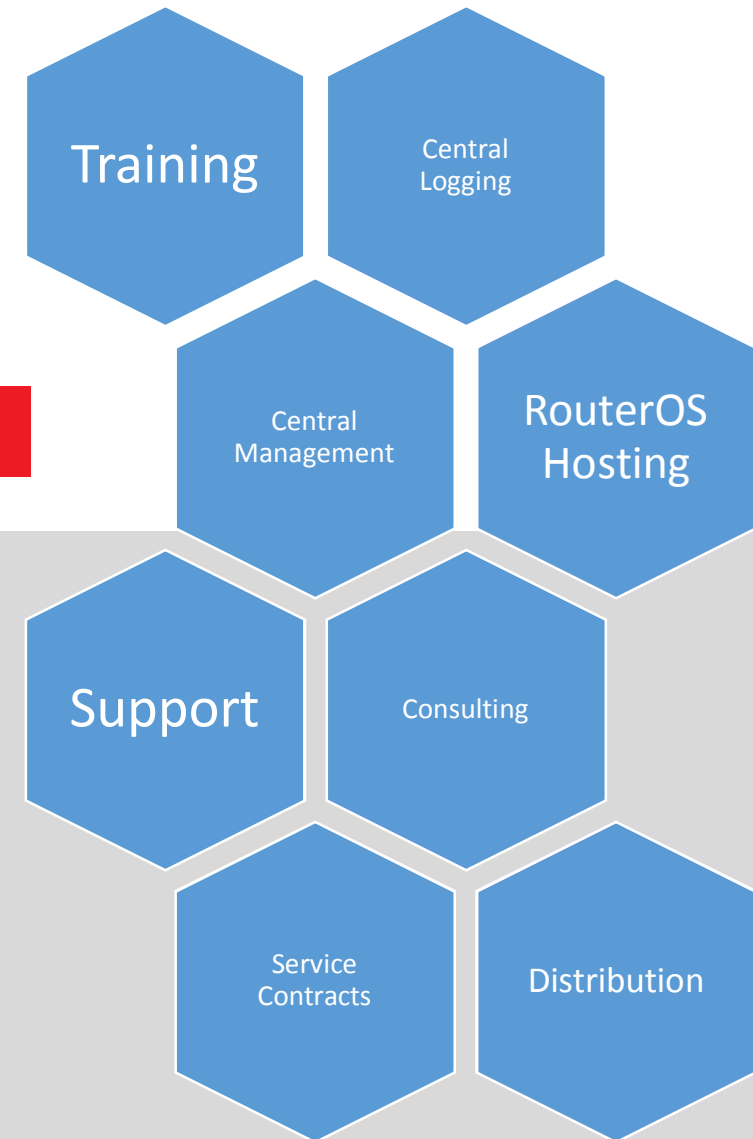
Are you looking for centralised
and MikroTik aware logging?

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



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

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





Dank u wel!