



Monitoring and Debugging

(with) RouterOS



Agenda

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





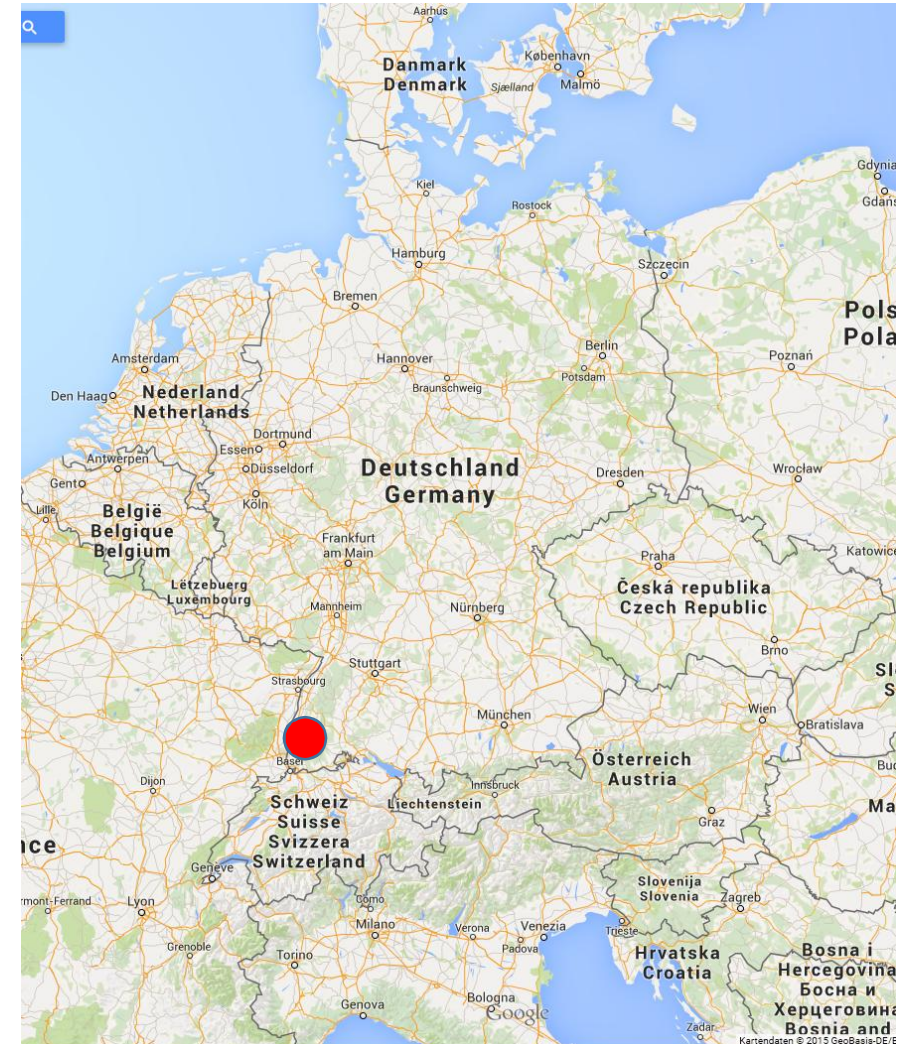
FMS Internetservice GmbH

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





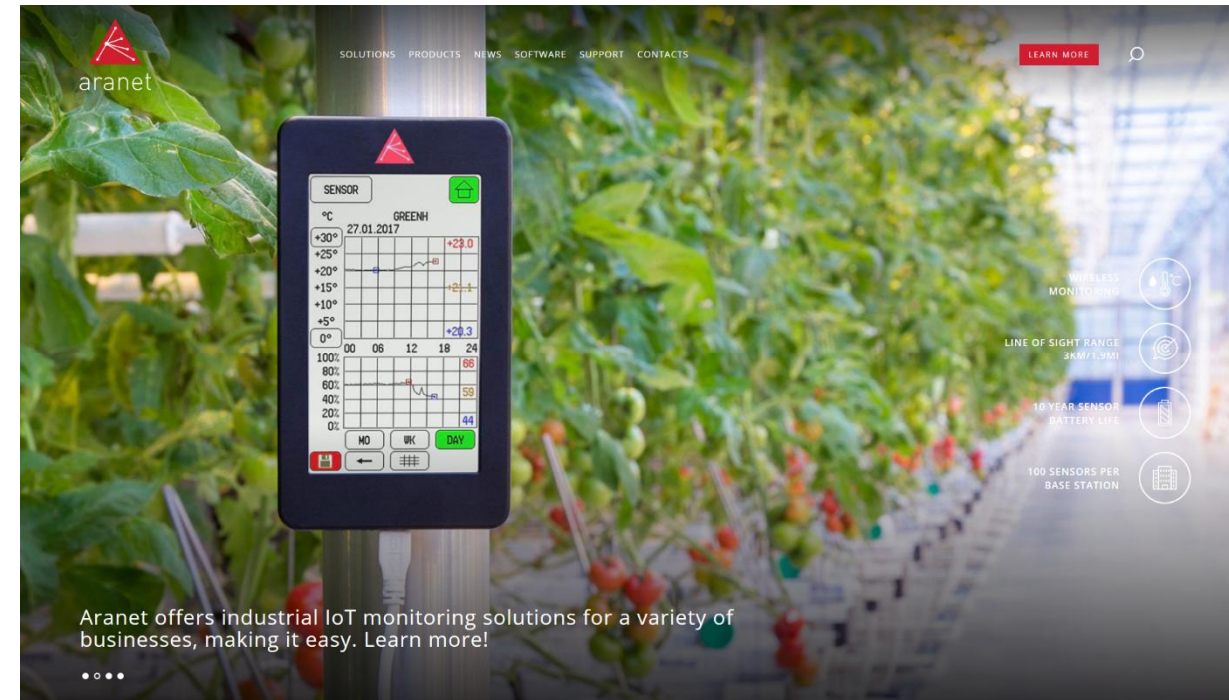
Distributor Table

10G Radio Links



5 year warranty & next day replacement

Wireless LoRaWAN IoT Solution



3km transmtion & 10 years battery life



Network Operation – Big Picture

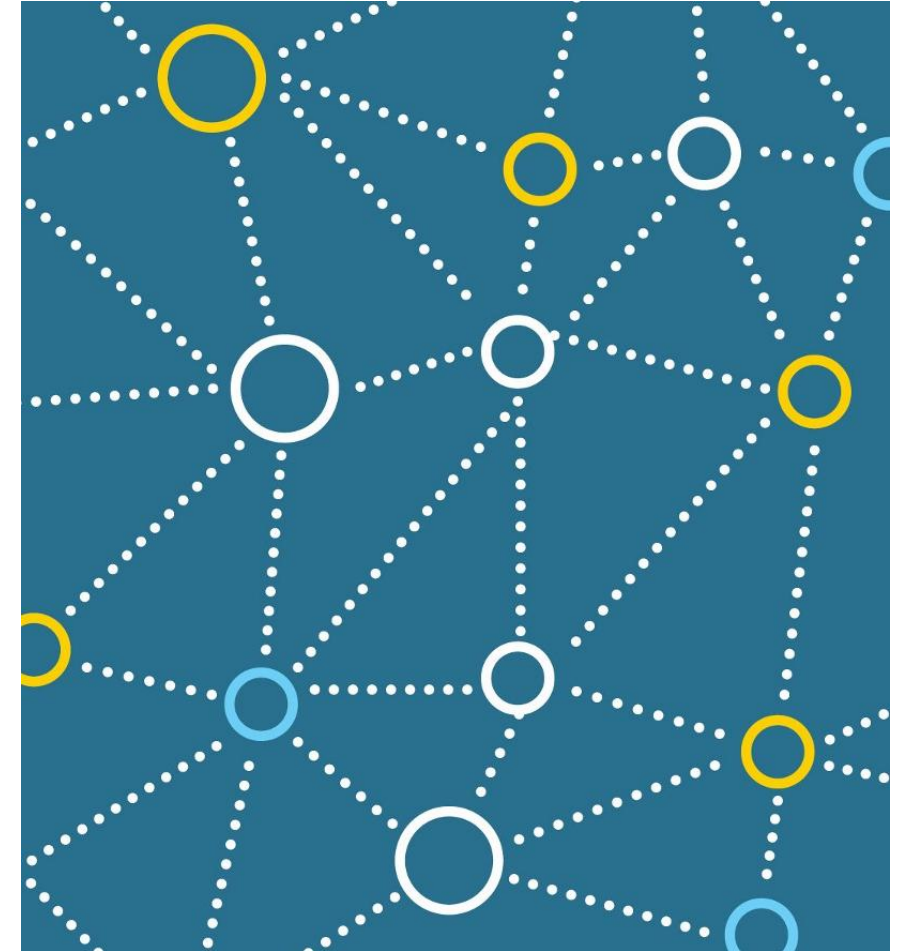
Challenges and Elements



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 & 3rd Party Integration

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



Management Topologies

Secure and Convenient Management Access



Management Approaches

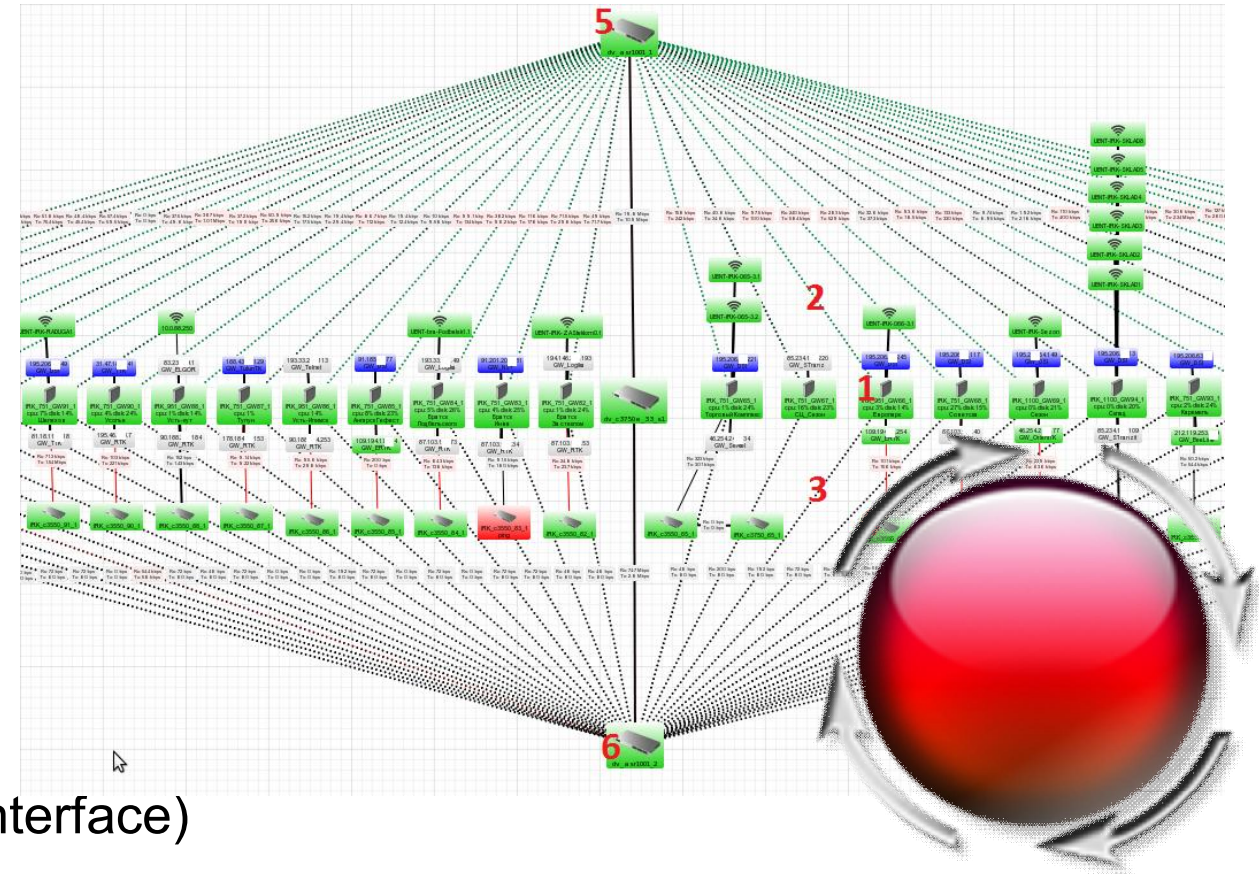
- Considerations
 - Security
 - Convenience
 - Efficiency
- Common Approaches
 - Separate management and user traffic
 - Management VLAN
 - Tunneling payload (e.g. PPPoE)
 - Tunneling of management (VPN)





Management Approaches

- Central MikroTik tools
 - The Dude
 - CAPsMAN
 - Usermanager
- Detailed examples
 - RoMON
 - API (Application programming interface)





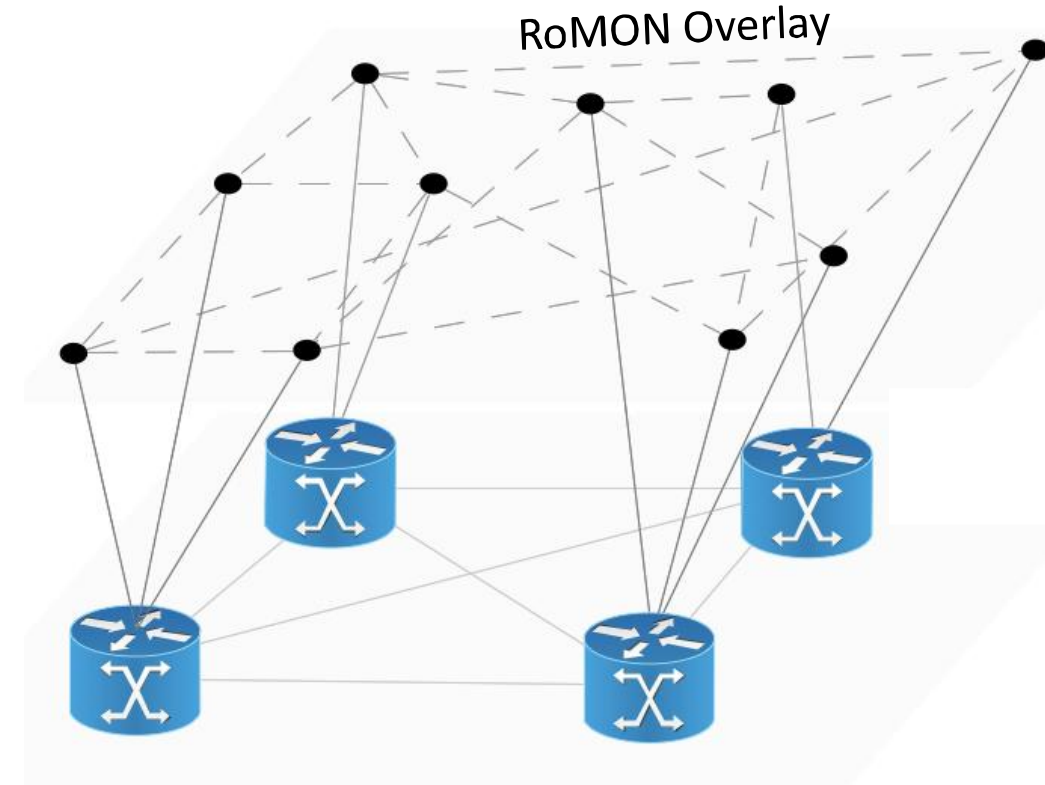
RoMON

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

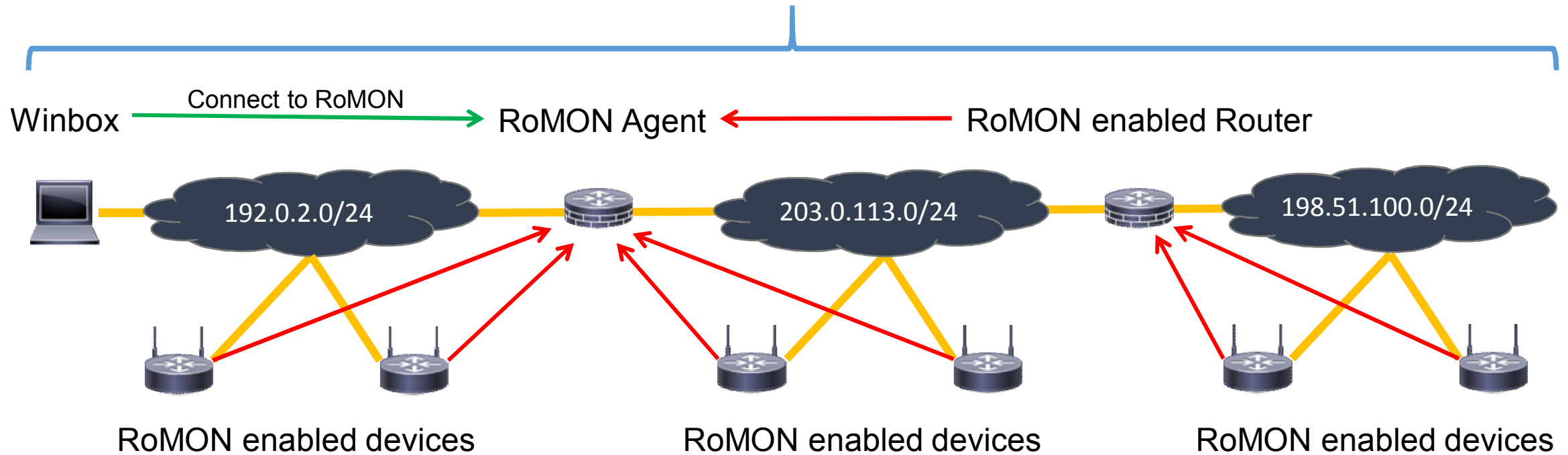
RoMON

- 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



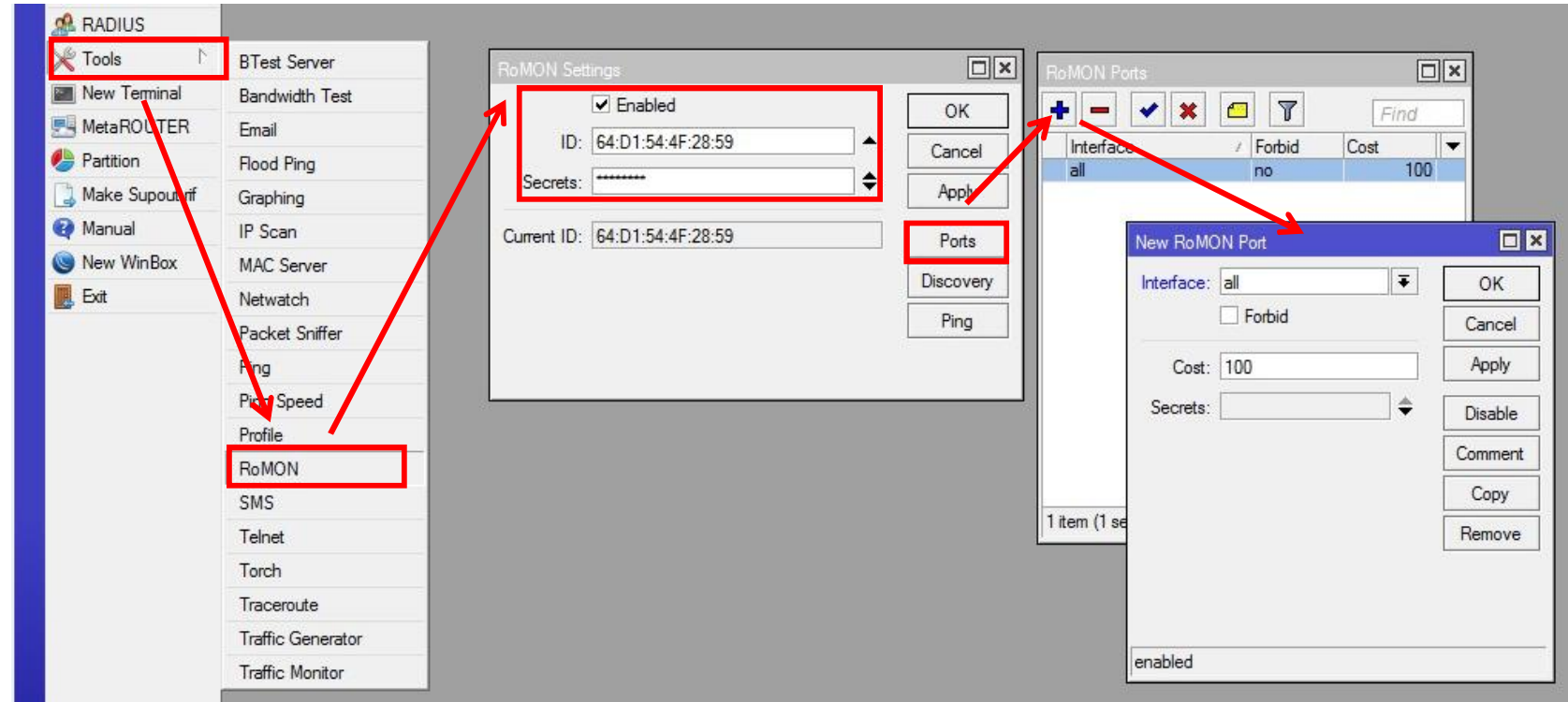
Discovery with MNDP

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

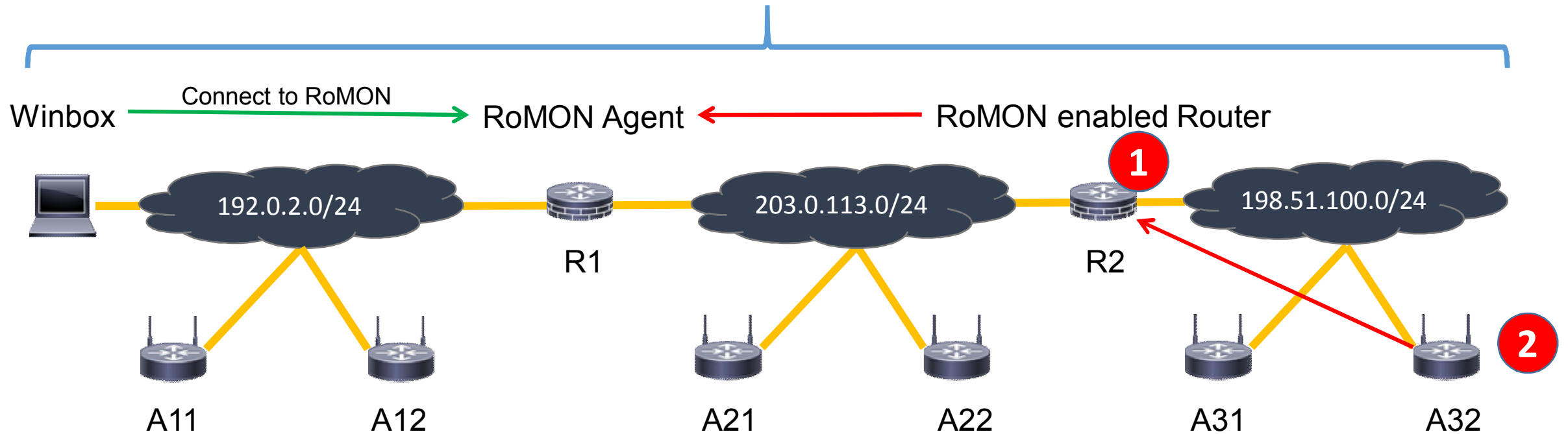
Refresh Find

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



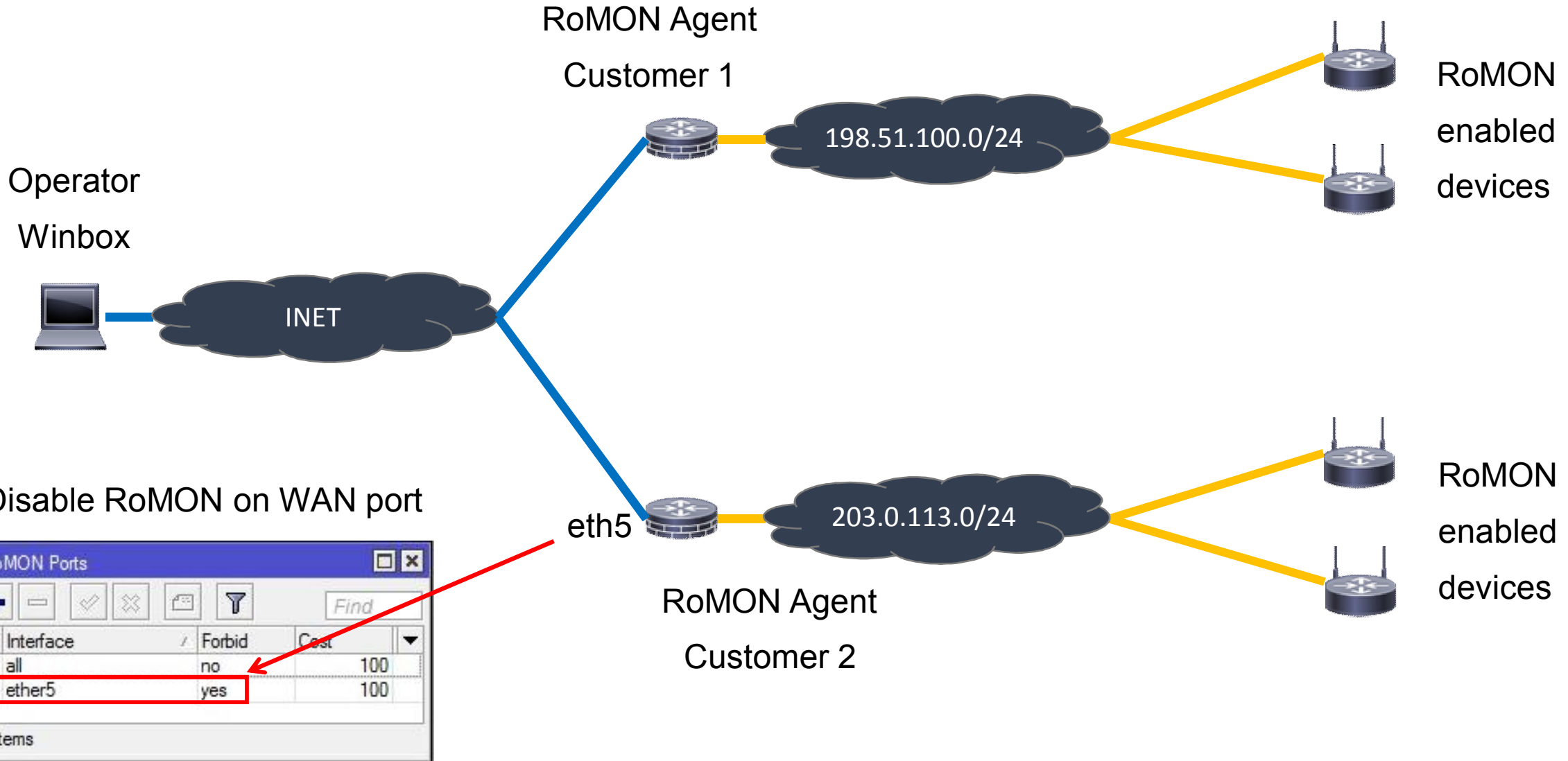
Remote RoMON Agent

- 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





MikroTik API

Custom-tailored Management Access



FMS Management Platform

Initial situation:

- Distributed Hotspot System
- Hundreds of sites
- New gateways will be deployed
- 100+ third party devices per site
- Fixed local IPv4 addresses
- Conflicting local subnets
- Two small NOCs, Road Warrior

Initial requirements:

- Easy operation
- Auto configuration of gateways
 - site to site VPN, INET access, basics
- Third party devices
 - Direct access to WEB interfaces
 - Central inventory
 - Central monitoring with dependencies



FMS Management Platform



[SITES](#) [DEVICES](#) [CONFIGURATION](#) ▾

Sites

Customer Number	Name	RBD52G-5HacD2	Description	Gateway with Load-Balancin	Submit
--	-----------------------------------	--	--	---	---------------------------------------

SUBMIT

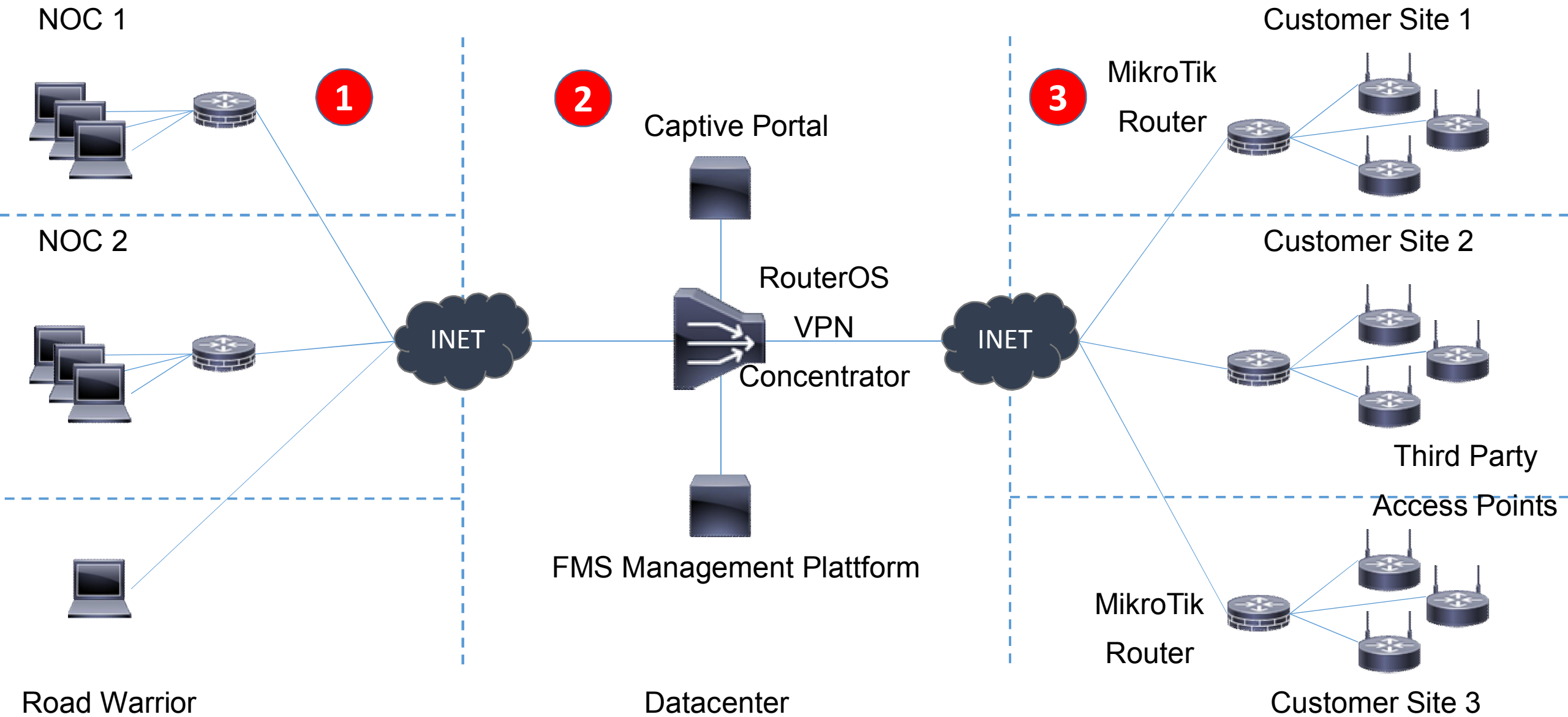
Show 10 entries

Search:

Status	Customer Number	Name	Gateway	Type	Description	Options
	Client-1010_01	Global Munich	HAPAC	Gateway with Load-Balancing	Guest WIFI only	DELETE MANAGE DEVICES CREATE CONFIG
	Client-1011_01	YHA Munich	RB4011 Rackmount	Gateway with Load-Balancing	Guest WIFI only	DELETE MANAGE DEVICES CREATE CONFIG
	Client-1012_01	Palace Inn Munich	HAPAC	Gateway with Load-Balancing	Guest WIFI only	DELETE MANAGE DEVICES CREATE CONFIG



FMS Management Platform





Adding new Sites

NOC 1



Captive Portal



RouterOS

VPN

Concentrator

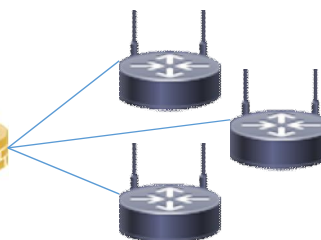


FMS Management Platform



Customer Site 1

MikroTik
Router



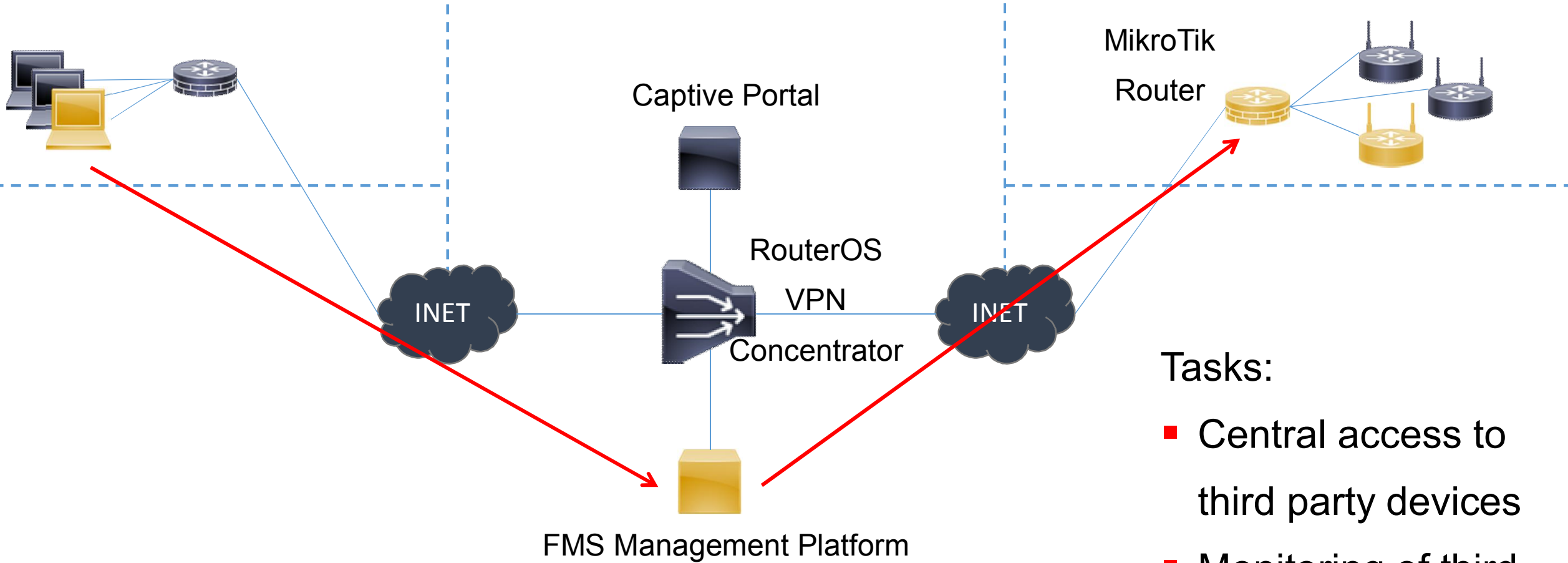
- Site router configuration
- VPN server configuration

- Captive Portal configuration
- Monitoring of site router



Adding new Devices

NOC 1



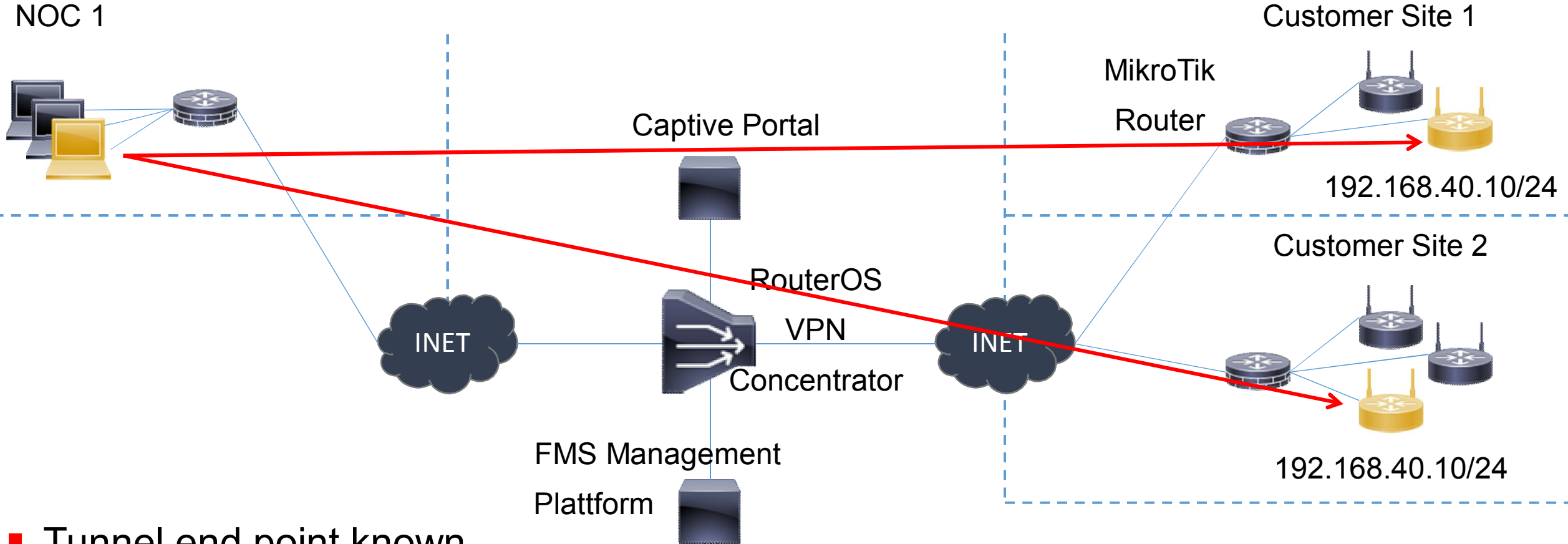
Tasks:

- Central access to third party devices
- Monitoring of third party devices



Coping with IP Conflicts / Management

NOC 1



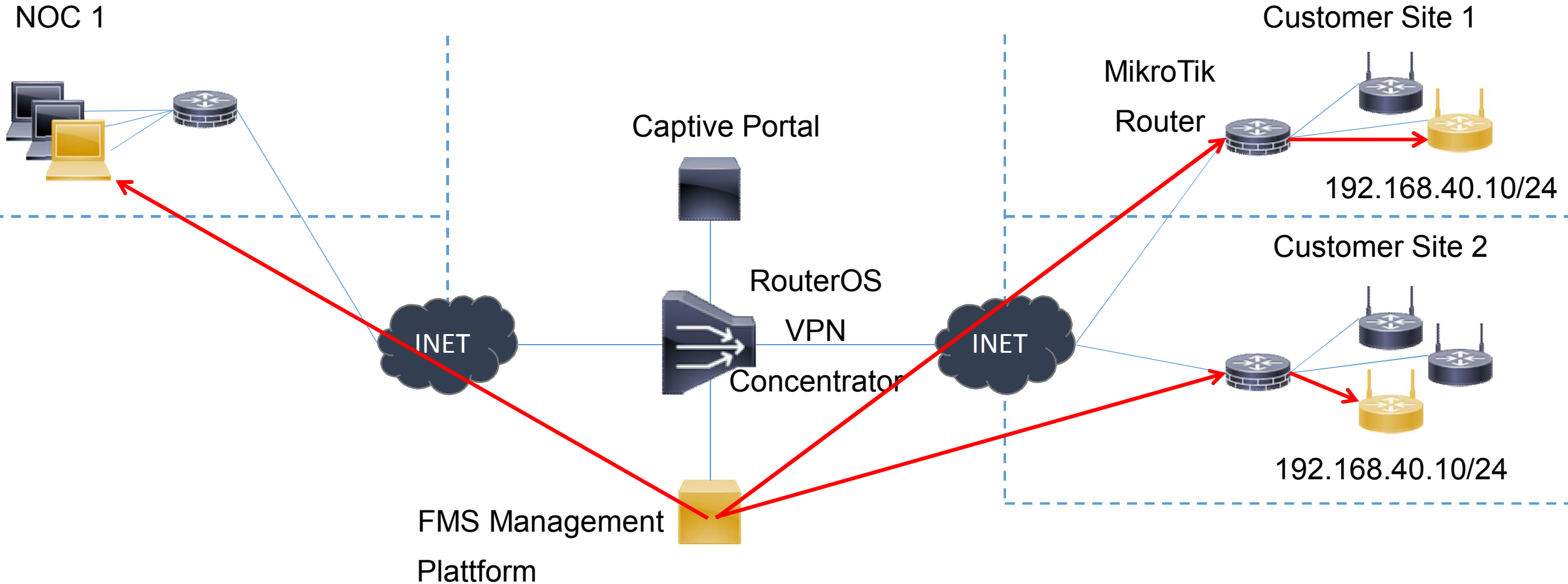
- Tunnel end point known
- Port forwarding on site router by API

■ EndPointIP:DevicePort



Coping with IP Conflicts / Monitoring

NOC 1



- API to execute ping on MikroTik site router

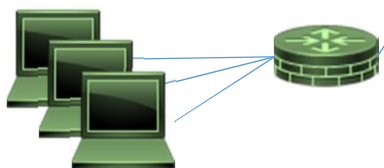
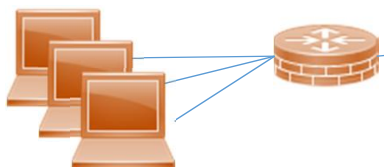


Local Retailer

NOC



Security Services



Stock & Payment Management



ERP /
Cash register



Captive
Portal



DVR /
Surveillance



RouterOS
VPN
Concentrator

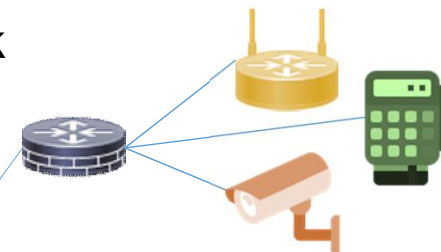


FMS Management Plattform

Datacenter

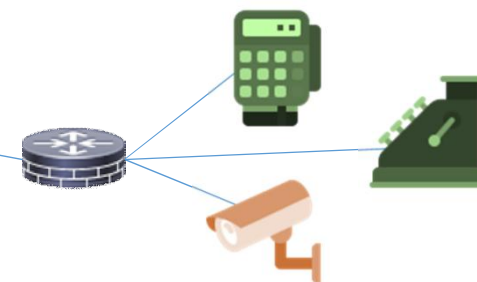


MikroTik
Router

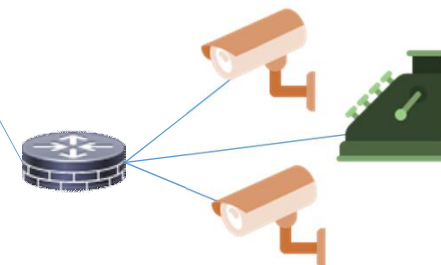


Customer Site 1

Customer Site 2



Third Party
Access Points



Customer Site 3



IoT – Management “only” Networks

- Dedicated networks for management and monitoring
- Often small but many sites
- Only purpose is management
- Lack of trained network staff
- Efficiency and simplicity most important



Access for vendors
(e.g. CNC machines)



Smart metering for
transformer stations



Get in Touch

Are you looking for a centralised and
individual management platform?

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



Network Debugging

The Needle in a (huge) Haystack



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

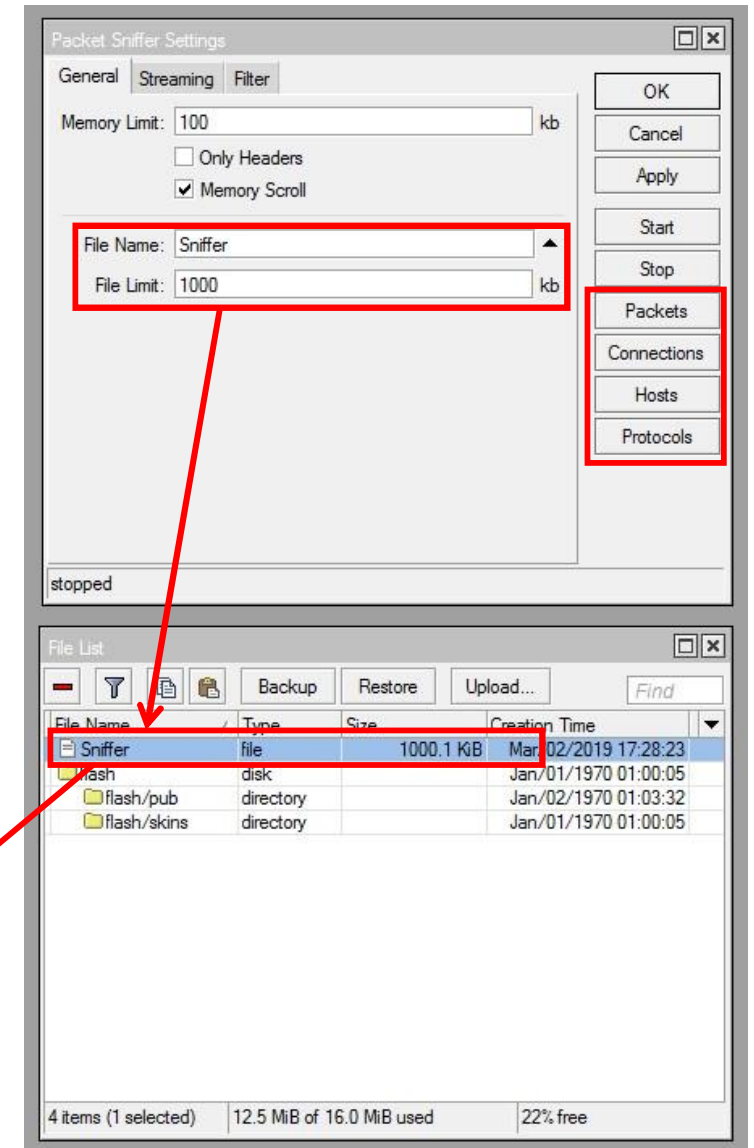
- Packet sniffing
- De facto standard: Wireshark
- RouterOS packet sniffer





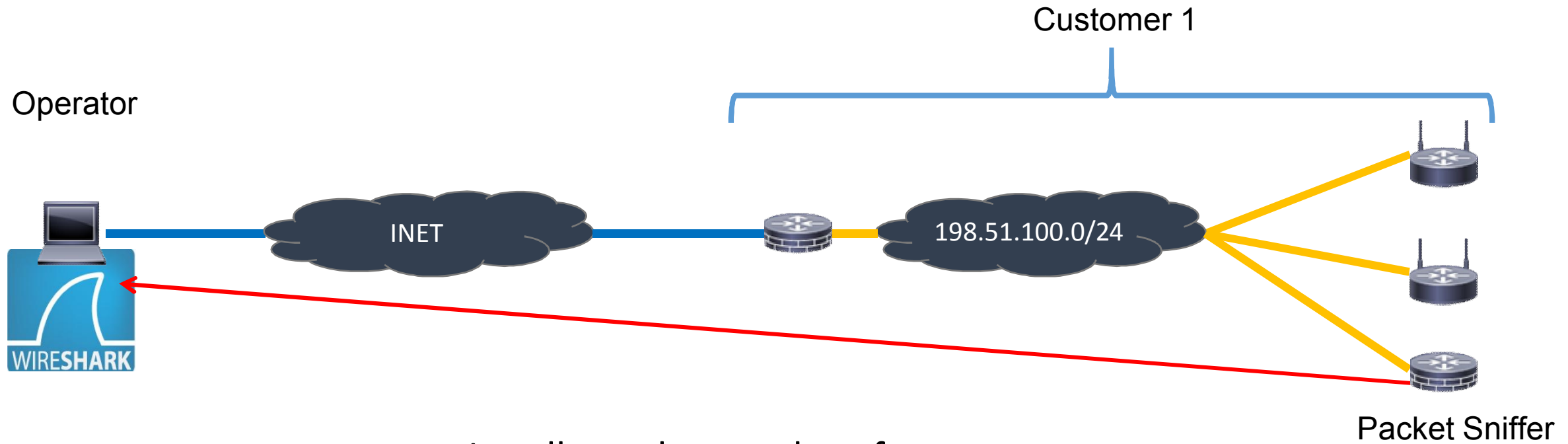
MikroTik Packet Sniffer

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





Remote Packet Sniffing

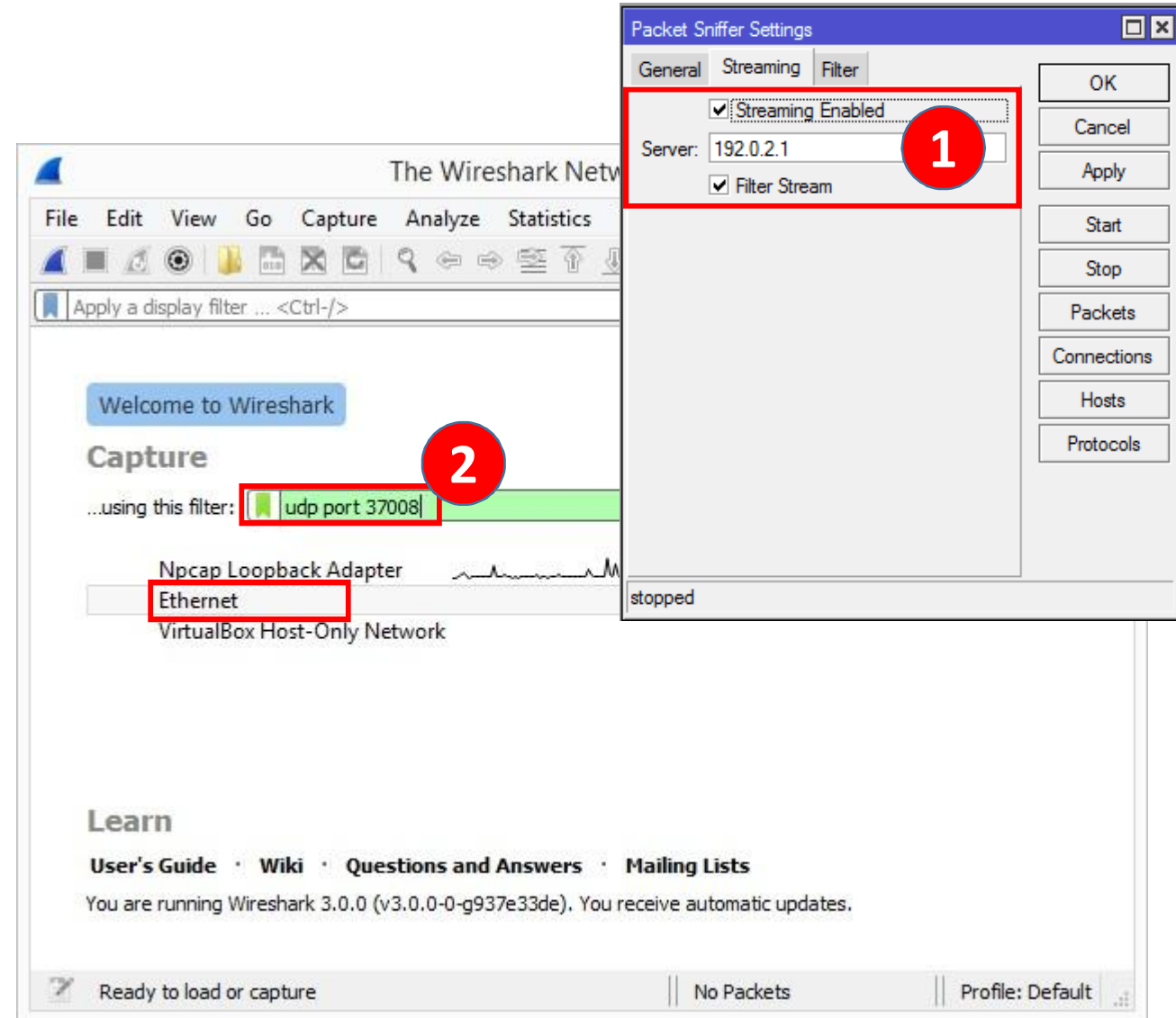


Locally analyse packets from
a remote sniffer in real time



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



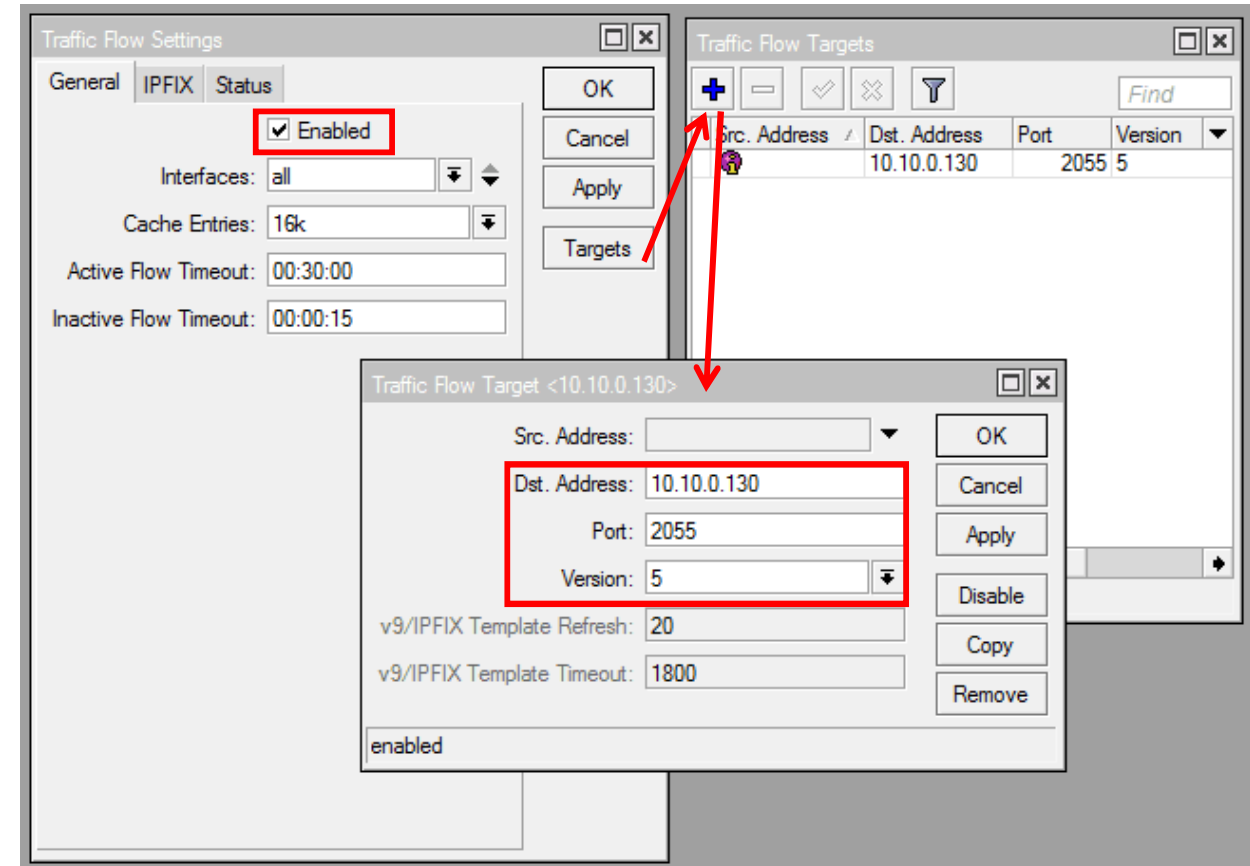
Traffic Flow

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

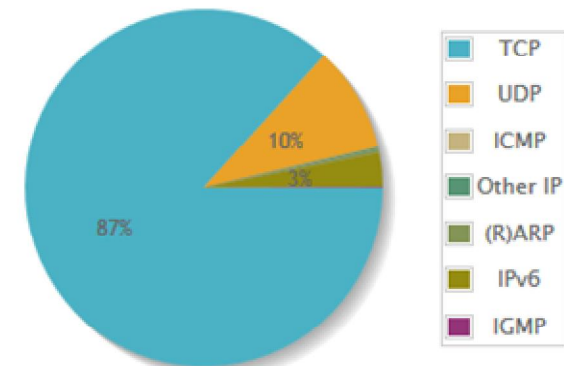




Netflow Collector and Analysis

- 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%			

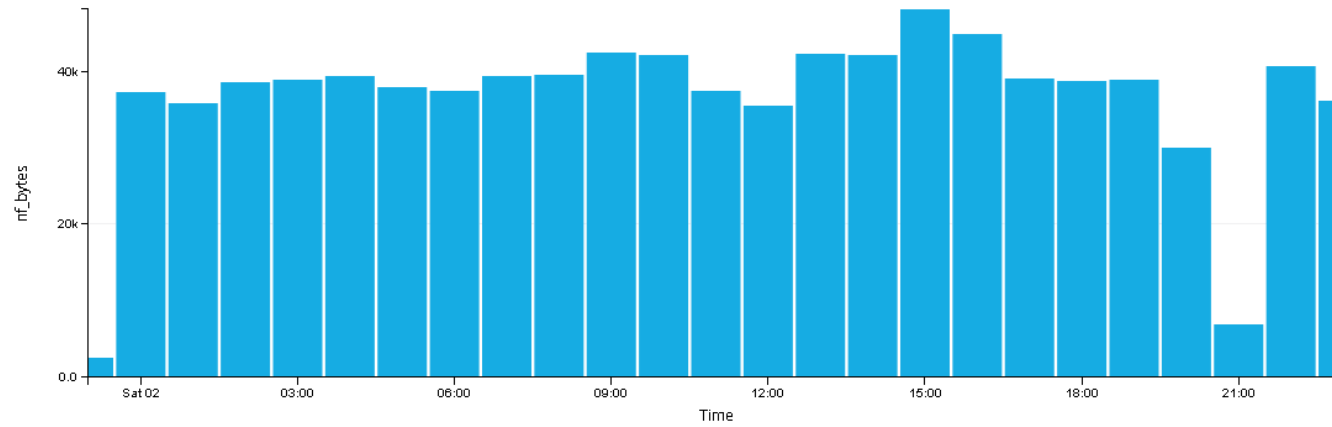


Former ntop GUI

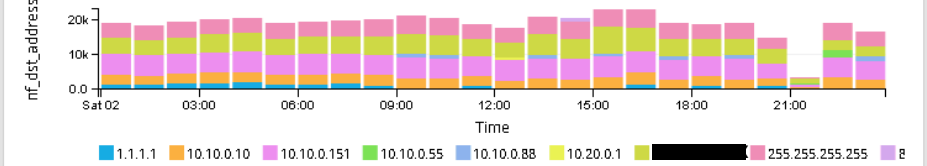


Netflow in FMS Management Plattform

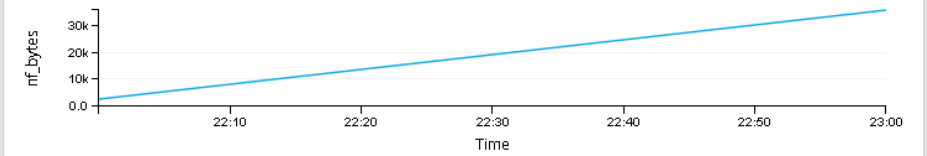
Bytes (last day)



Destinations (last day)



Bytes (last hour)



Protocols (last day)



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)



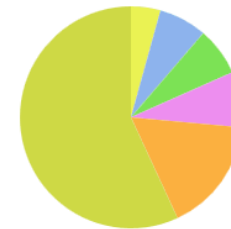
Value	%	Count
Top 5 values		
53	14.71%	134,443
5678	11.73%	107,189
0	8.97%	81,998
443	6.40%	58,520
80	3.21%	29,310

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
10.10.0.55	7.05%	62,676
10.10.0.88	7.01%	62,312
10.10.0.1	4.29%	38,077

Destinations (last day)



Value	%	Count
Top 5 values		
10.10.0.151	15.22%	135,255
255.255.255.255	13.31%	118,229
10.10.0.10	12.10%	107,507
10.10.0.1	7.77%	69,085
1.1.1.1	3.17%	28,165



Debugging RouterOS Installations

The other Needle in another (huge) Haystack



RouterOS Debugging

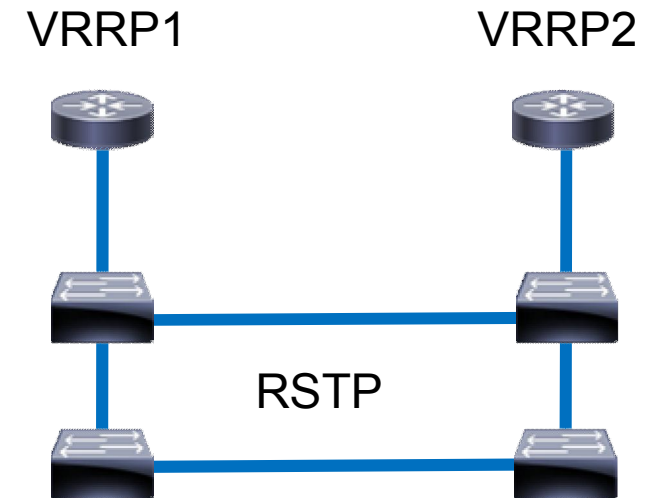
- Source for network debugging = packets and packet statistics
- Source for device debugging = local status information
- SNMP
- Local logging

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 'Log Action <FMSMP>' configuration window, which is a modal dialog for setting up a remote syslog action. The window contains the following fields:

- Name: FMSMP
- Type: remote
- Remote Address: 10.10.0.130
- Remote Port: 5140
- Src. Address: 10.10.0.130
- ☐ BSD Syslog
- Syslog Facility: 3 (daemon)
- Syslog Severity: (empty)

Buttons on the right include OK, Cancel, Apply, Copy, and Remove. A red dashed box highlights the 'BSD Syslog', 'Syslog Facility', and 'Syslog Severity' section, with a large 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.

The 'Logging' table in the background shows the following data:

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

At the bottom of the interface, the text 'Remote Syslog Configuration' is displayed.

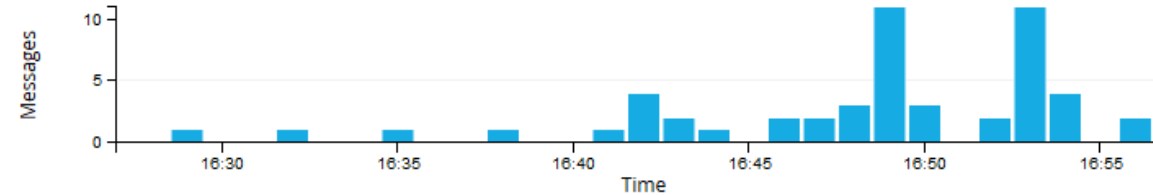


WIFI Connects from Syslog across complete Network

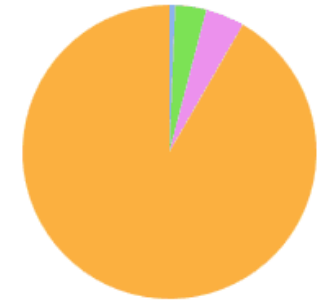
WLAN Connections (last 1/2 hour)

52

WLAN Connections (last 1/2 hour)



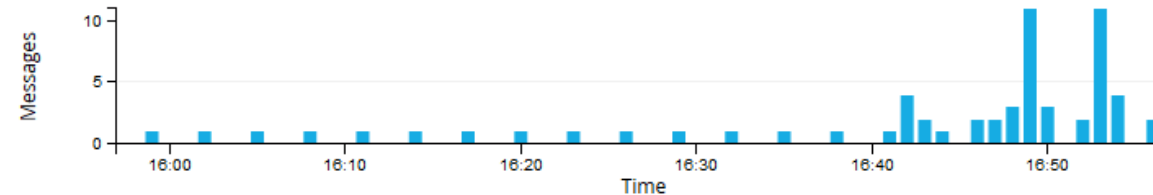
Connections by Access Point (last day)



WLAN Connections (last hour)

62

WLAN Connections (last hour)

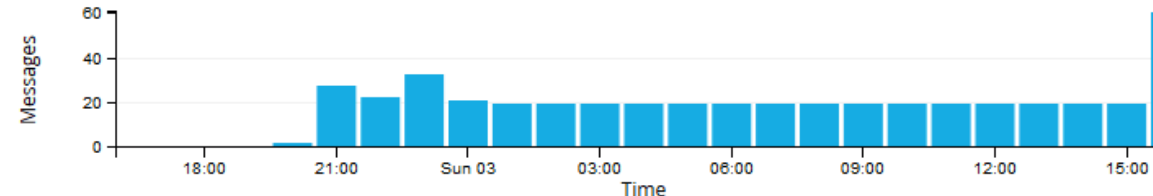


Value	%	Count
Top 5 values		
10.10.0.40	91.67%	429
10.10.0.29	4.27%	20
10.10.0.128	3.42%	16
10.10.0.22	0.64%	3

WLAN Connections (last day)

468

WLAN Connections (last day)





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

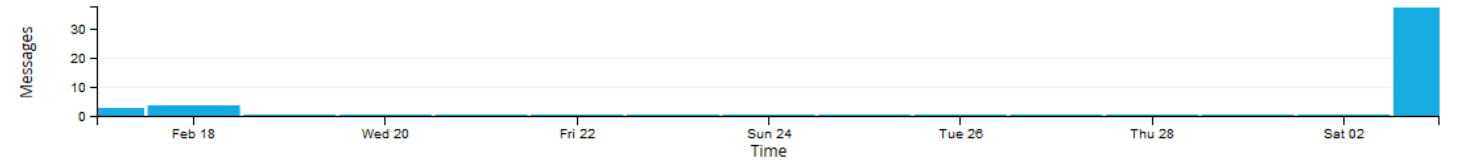
Login Failed (last hour)

37

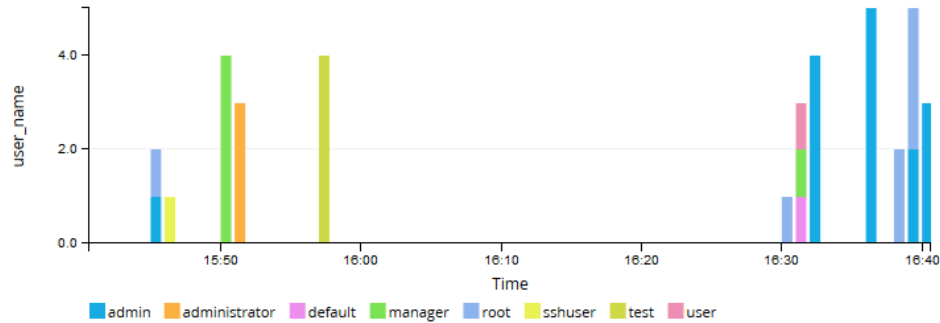
Logins failed (last 7 days)

44

Logins Failed (last 7 days)



Login failed by Username (last hour)



Logins failed (last 7 days)



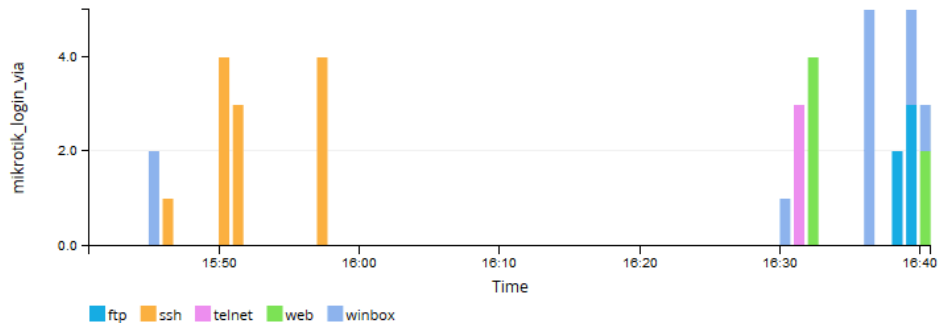
Login failed by Username (last 7 days)



Login failed by Login Type (last 7 days)



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



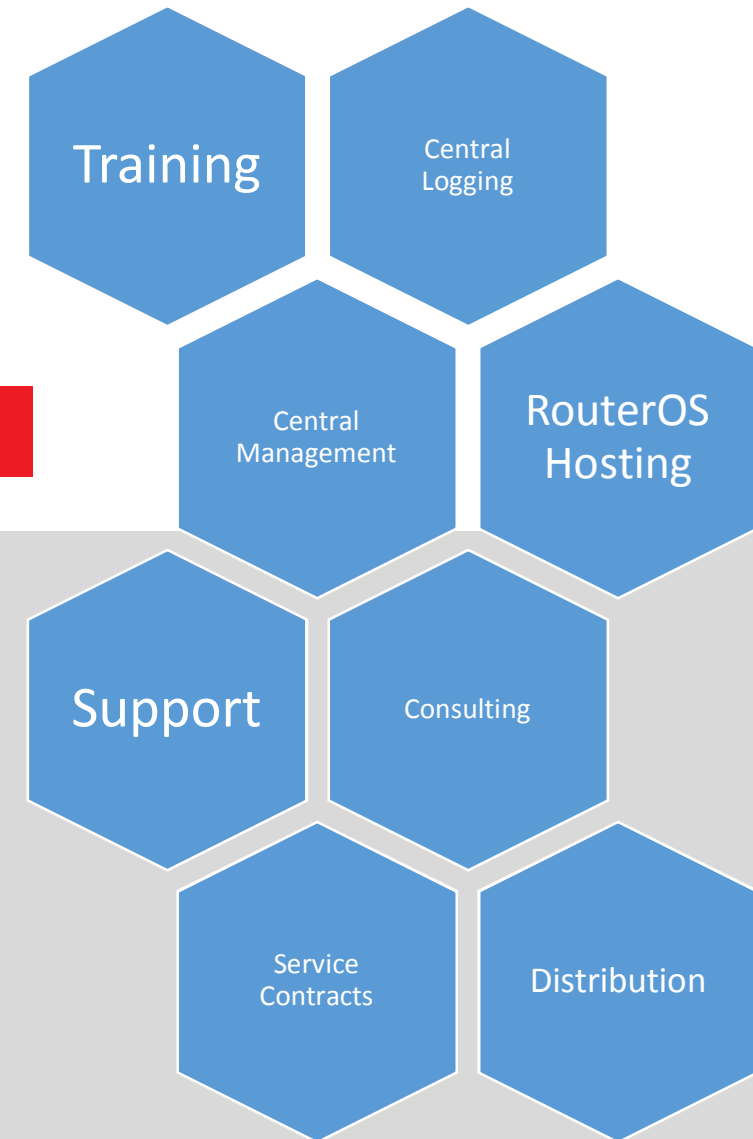
FMS Internetservice GmbH

Services and Contact



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

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





Thank You