

# MikroTik as mobile console for Out-of-Band management (OOB)

MBUM 2023  
Grzegorz Rakuś

# Parę słów o mnie

Specjalizuję się w rozwiązaniach VPN ( Site-to-Site / Remote Access ),  
Firewallach (L4 / ZBF / NGFW) oraz systemach AAA / SSO ( RADIUS / MFA / SAML )

- administracja i utrzymanie multi-platformowej infrastruktury sieciowej
- zarządzanie bezpieczeństwem sieci ( L2 / L3 / 802.1x / NGFW / ZTNA / FWaaS )
- wsparcie dla środowisk MS ( AD / Hyper-V / Microsoft 365 / Azure )
- wdrożenia / konsultacje / doradztwo IT



**MTCNA / MTCRE / MTCTCE / MTCSE**

**CCNA CyberOps / Security / Routing and Switching**

[grzegorz.rakus@gmail.com](mailto:grzegorz.rakus@gmail.com)

[linkedin.com/in/grzegorz-rakus/](https://linkedin.com/in/grzegorz-rakus/)

# The presentation

## Requirements:

### ▶ MikroTik hardware

64MB RAM (recommended\*)

USB port

WIFI (optional)

SFP port (optional)

### ▶ accessories

\* for RouterOS v7

# What is Out-of-Band Management (OOB) ?

(definition)

Out-of-Band management provides enterprises with secure access to critical devices, even during a disruption.

OPENGear source

Out-of-band (OOB) management is a nodegrid net services method of remotely controlling and managing critical IT assets and network equipment using a secure protocol connection through a secondary **interface that is physically separate from the primary network connection**

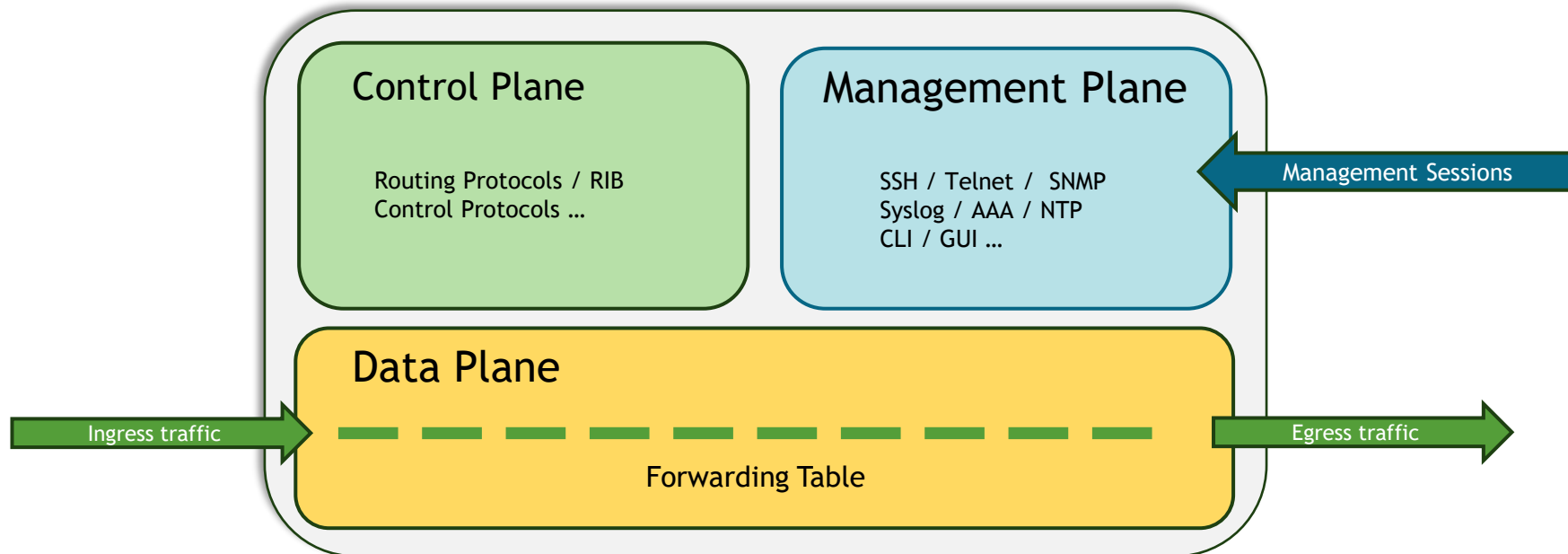
DIGI source

In systems management, out-of-band management (OOB) is a process for accessing and managing devices and infrastructure at remote locations through a separate management plane from the production network

WIKIPEDIA source

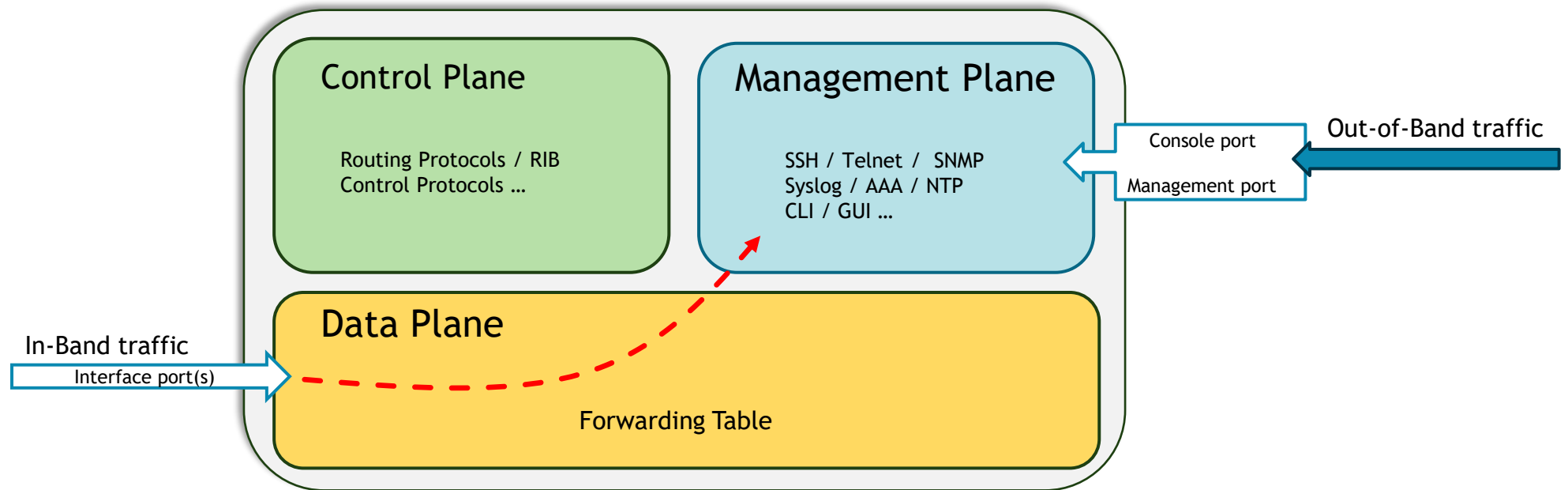
# Data Plane / Control Plane / Management Plane

(General diagram of a network device)



# In-Band vs Out-of-Band management traffic

(flow for MGMT)



# In-Band vs Out-of-Band management

(comparision)

In-Band	Out-of-Band
management by Interface (VLAN) / <b>Loopback</b>	management by dedicated Interface
access via Telnet / SSH / GUI	access via Console (terminal access) / Management port (IP)
<b>works only when network link is up</b>	<b>works as alternative path when network is down</b>
Connection speed is high	Connection speed is slow *
Connection is synchronus	Connection is asynchronus *

Based on [IPWITHEASE](#)

\* only when Console port is used

# Out-of-Band management comparsion types

(console port vs management port)

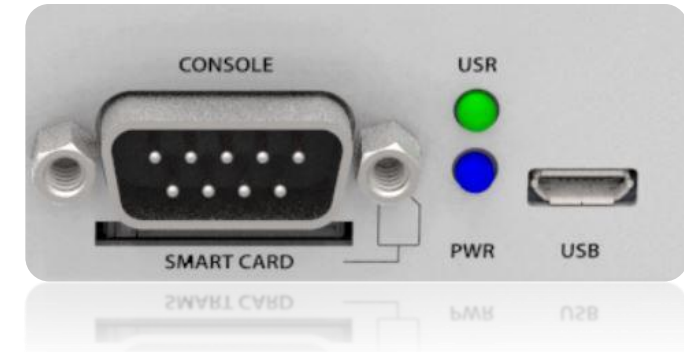
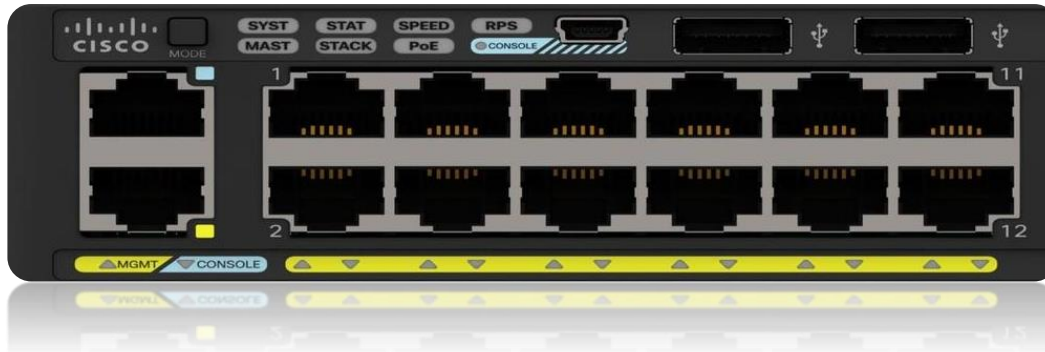
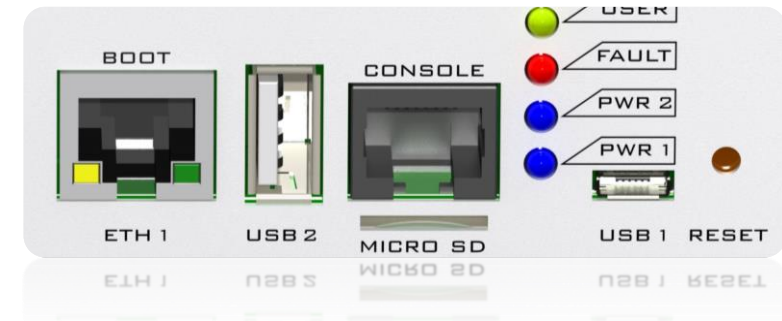
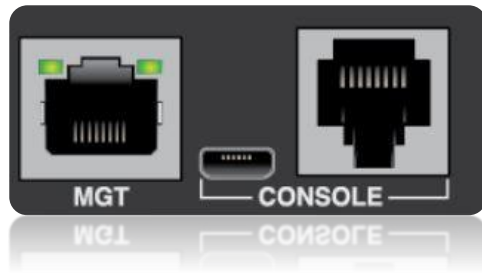
Parameter	Console Port	Management Port
IP address assignment	Not possible	Can be assigned
Connectivity Type	Serial / DE-9 / RJ45 / miniUSB / microUSB	RJ45 / SFP
Segregation type	Physical access to device required	Generally a VRF-based traffic segregation
Boot Sequence	Show boot sequence	Does not show boot sequence
Maximum speed	115200 bit/s	1 Gb/s
Application required	HyperTerminal	Telnet / SSH / GUI

Based on [IPWITHEASE](#)



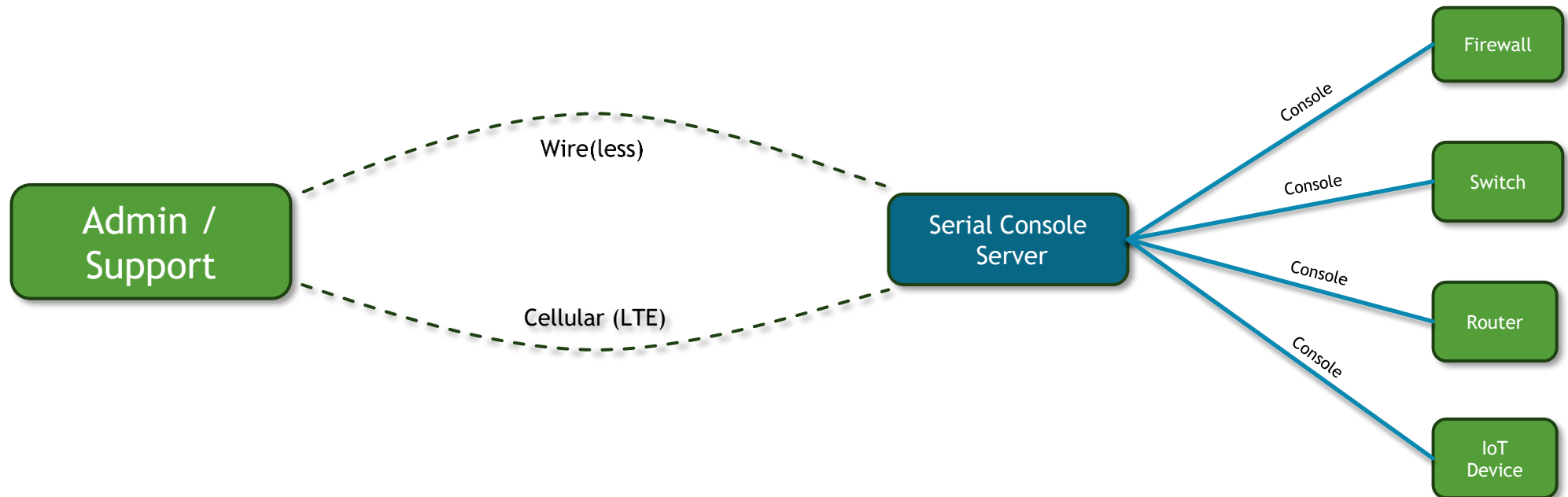
# Console / Management Port pictures

(examples)



# Out-of-Band network diagram

(example scenario)



# MikroTik hardware with USB port

(example models)

hEX (S)



hAP (ac lite)



hAP ac<sup>2</sup>



RB951Ui-2HnD



RB2011UiAS-2HnD-IN  
RB2011UiAS-IN  
(discontinued...)

# Connecting a USB-to-Serial cable

(device detection)

Resources

Uptime: 00:10:06

Free Memory: 25.1 MiB

Total Memory: 64.0 MiB

CPU: MIPS 24Kc V7.4

CPU Count: 1

CPU Frequency: 650 MHz

CPU Load: 2 %

Free HDD Space: 3600 KiB

Total HDD Size: 16.0 MiB

Sector Writes Since Reboot: 60

Total Sector Writes: 17 384

Architecture Name: mipsbe

Board Name: hAP ac lite

Version: 7.11.2 (stable)

Build Time: Aug/31/2023 13:55:47

Factory Software: 6.34.2

OK

PCI

USB

CPU

IRQ

USB

Find

Device	Vendor	Name	Serial Number	Speed	USB Version	Ports
1-0	Linux 5.6.3 ehci_hcd	RB400 EHCI	rb400_usb	480	2.00	1
1-1	FTDI	FT232R USB UART	A969VDFH	12	2.00	0

2 items (1 selected)

- Password
- Ports
- Reboot
- Reset Configuration
- Resources
- RouterBOARD

Port List

Ports Remote Access

Find

Name	Used By	Channels	Baud Rate	Flow Control
usb1		1	9600	none

1 item (1 selected)

Log

Freeze

Find all

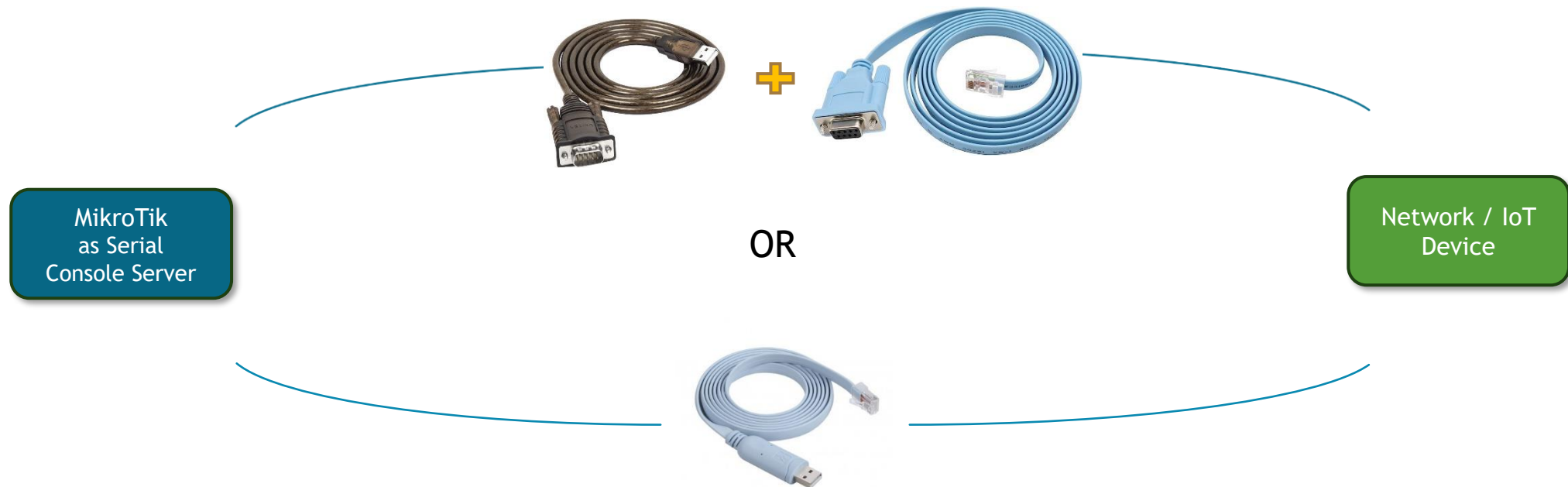
Message contains device

#	Time	Buffer	Topics	Message
6	Sep/24/2023 19:30:18	memory	system, info	device added

1 item out of 8 (1 selected)

# USB-to-Serial cable

(DE-9 and RJ45)



# USB-to-Serial cable - more combinations

(DE-9 and RJ45)

MikroTik  
as Serial  
Console Server

OR

Network / IoT  
Device



(adapter must be Rollover)

# USB-to-Serial x2

(DE-9)

MikroTik  
as Serial  
Console Server



Channel 0

Network / IoT  
Device



Channel 1

Network / IoT  
Device

Port List					
Ports Remote Access					
Name	Used By	Channels	Baud Rate	Flow Control	
usb1		2	9600	none	

1 item (1 selected)

# USB-to-Serial x4

(DE-9)

MikroTik  
as Serial  
Console Server



Channel 0

Network / IoT  
Device



Channel 1

Network / IoT  
Device



Channel 2

Network / IoT  
Device



Channel 3

Network / IoT  
Device

Port List					
Ports Remote Access					
Name	Used By	Channels	Baud Rate	Flow Control	
usb1		4	9600	none	

1 item (1 selected)



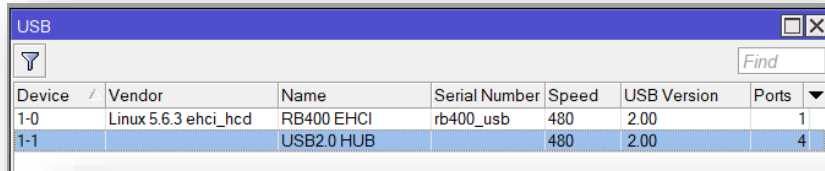
(LTE modems , USB Flash)



# Connecting peripheral devices to MikroTik (via USB hub)

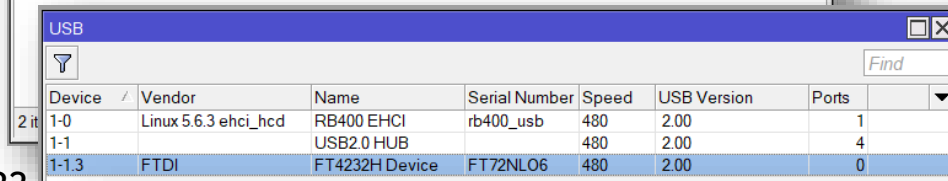
(renaming)

USB hub



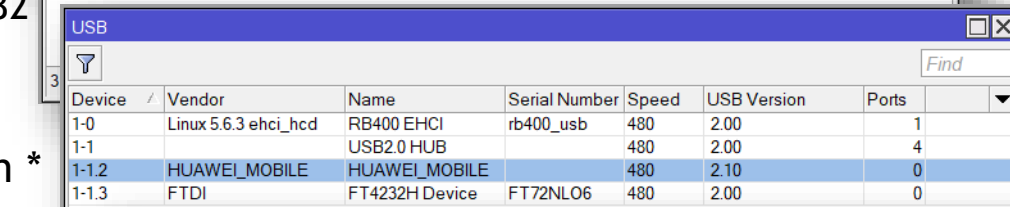
Device	Vendor	Name	Serial Number	Speed	USB Version	Ports
1-0	Linux 5.6.3 ehci_hcd	RB400 EHCI	rb400_usb	480	2.00	1
1-1		USB2.0 HUB		480	2.00	4

USB - 4xRS232



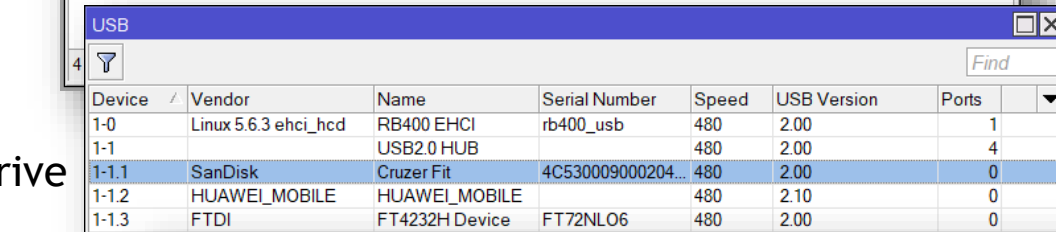
Device	Vendor	Name	Serial Number	Speed	USB Version	Ports
1-0	Linux 5.6.3 ehci_hcd	RB400 EHCI	rb400_usb	480	2.00	1
1-1		USB2.0 HUB		480	2.00	4
1-1.3	FTDI	FT232RL Device	FT232RL06	480	2.00	0

LTE modem \*



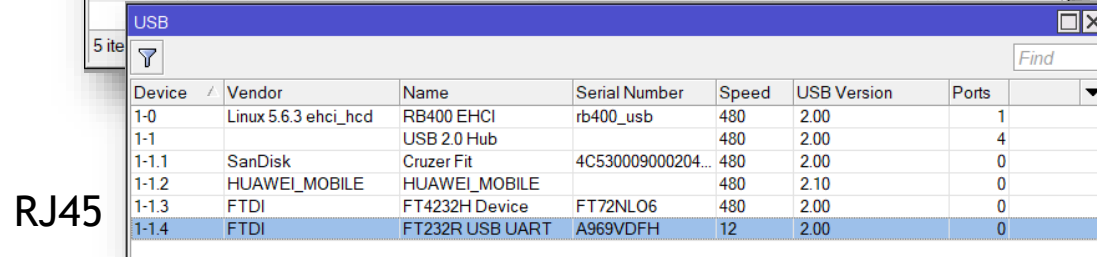
Device	Vendor	Name	Serial Number	Speed	USB Version	Ports
1-0	Linux 5.6.3 ehci_hcd	RB400 EHCI	rb400_usb	480	2.00	1
1-1		USB2.0 HUB		480	2.00	4
1-1.2	HUAWEI_MOBILE	HUAWEI_MOBILE		480	2.10	0
1-1.3	FTDI	FT232RL Device	FT232RL06	480	2.00	0

Flash drive

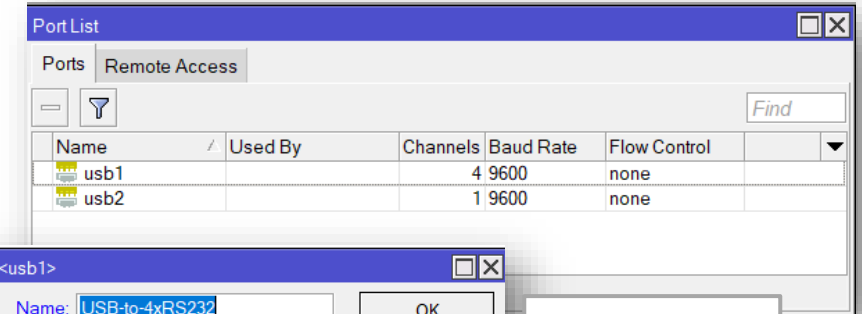


Device	Vendor	Name	Serial Number	Speed	USB Version	Ports
1-0	Linux 5.6.3 ehci_hcd	RB400 EHCI	rb400_usb	480	2.00	1
1-1		USB2.0 HUB		480	2.00	4
1-1.1	SanDisk	Cruzer Fit	4C530009000204...	480	2.00	0
1-1.2	HUAWEI_MOBILE	HUAWEI_MOBILE		480	2.10	0
1-1.3	FTDI	FT232RL Device	FT232RL06	480	2.00	0

USB to RJ45

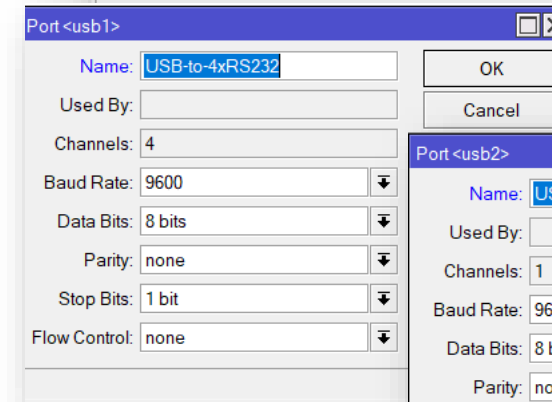


Device	Vendor	Name	Serial Number	Speed	USB Version	Ports
1-0	Linux 5.6.3 ehci_hcd	RB400 EHCI	rb400_usb	480	2.00	1
1-1		USB 2.0 Hub		480	2.00	4
1-1.1	SanDisk	Cruzer Fit	4C530009000204...	480	2.00	0
1-1.2	HUAWEI_MOBILE	HUAWEI_MOBILE		480	2.10	0
1-1.3	FTDI	FT232RL Device	FT232RL06	480	2.00	0
1-1.4	FTDI	FT232RL USB UART	A969VDFH	12	2.00	0



Name	Used By	Channels	Baud Rate	Flow Control
usb1		4	9600	none
usb2		1	9600	none

renaming ports



Port <usb1>

Name: USB-to-4xRS232

Used By:

Channels: 4

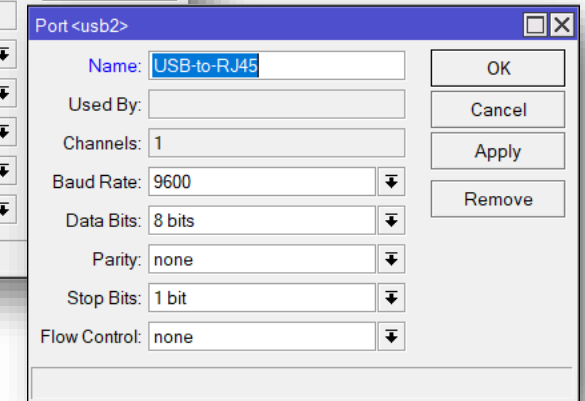
Baud Rate: 9600

Data Bits: 8 bits

Parity: none

Stop Bits: 1 bit

Flow Control: none



Port <usb2>

Name: USB-to-RJ45

Used By:

Channels: 1

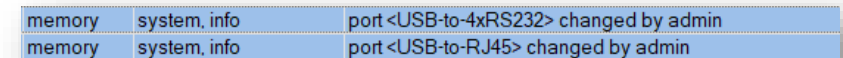
Baud Rate: 9600

Data Bits: 8 bits

Parity: none

Stop Bits: 1 bit

Flow Control: none



memory	system, info	port <USB-to-4xRS232> changed by admin
memory	system, info	port <USB-to-RJ45> changed by admin

\* MBIM modems are supported by default on RouterOS v7 - <https://help.mikrotik.com/docs/display/ROS/LTE#LTE-Summary>

# USB - host controller architecture

(very short explanation)

Open Host Controller Interface (OHCI) - max USB 1.0

Universal Host Controller Interface (UHCI) - max USB 1.0

Enhanced Host Controller Interface (EHCI) - max USB 2.0

eXtensible Host Controller Interface (xHCI) - max USB 3.0

hEX S

USB							
Device	Vendor	Name	Serial Number	Speed	USB Version	Ports	
1-0	Linux 5.6.3 xhci-hcd	xHCI Host Controller	1e1c0000.xhci	480	2.00	2	
2-0	Linux 5.6.3 xhci-hcd	xHCI Host Controller	1e1c0000.xhci	5000	3.00	1	
1-1	ALCOR	USB Hub 2.0		12	2.00	4	

3 items (1 selected)

USB Hub is too slow for LTE

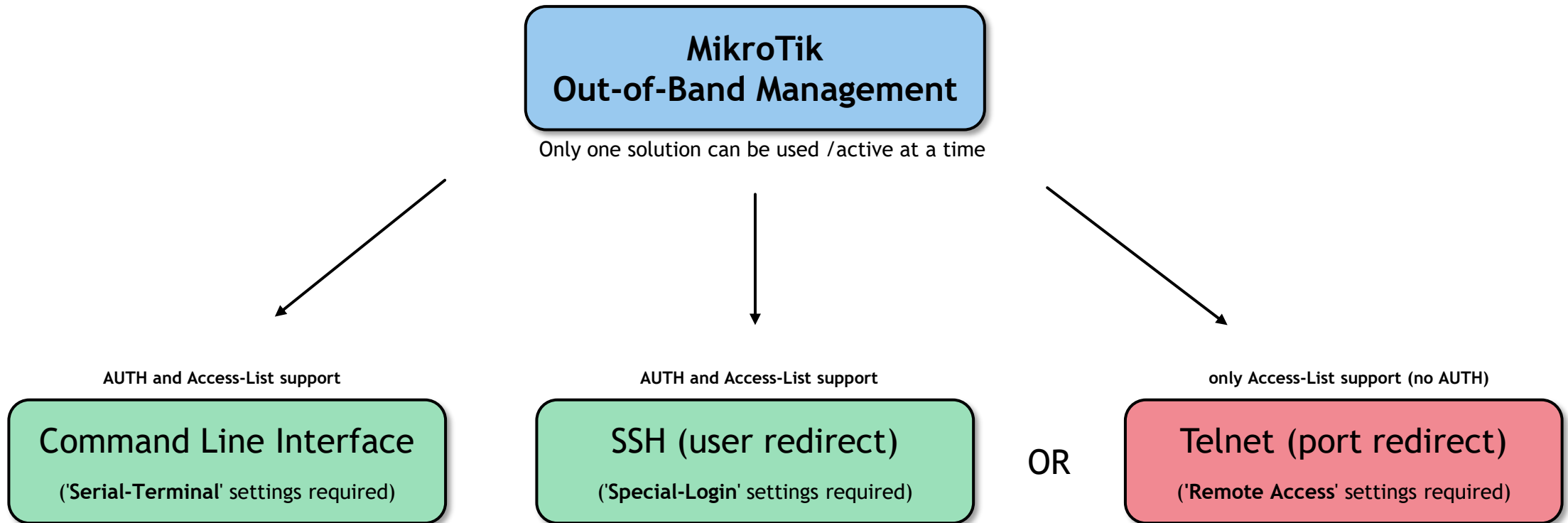
Chipset  $\neq$  USB port speed\*

USB						
Device	Vendor	Name	Serial Number	Speed	USB Version	Ports
1-0	Linux 5.6.3 ehci_hcd	RB400 EHCI	rb400_usb	480	2.00	1
1-1		USB2.0 HUB		480	2.00	4
1-1.1	FTDI	FT4232H Device	FT72NLO6	480	2.00	0

hAP ac lite

\* always check hardware specification on MikroTik website

# How it works



Important:

- multi-session to the same channel is not possible
- 'Remote Access' setting reserves the connection on the channel / serial link

# Command Line config

(Serial-Terminal command)

```
Terminal <1>

[admin@OOB-ac-lite] > system/serial-terminal
USB-to-4xRS232      USB-to-RJ45      channel      port
[admin@OOB-ac-lite] >
[admin@OOB-ac-lite] >
[admin@OOB-ac-lite] > system/serial-terminal port=USB-to-4xRS232 channel=0

[Ctrl-A is the prefix key]

FIREWALL#
FIREWALL# █
```

PortList

Ports Remote Access

Find

Name	Used By	Channels	Baud Rate	Flow Control
USB-to-4xRS232	serial-terminal	4	9600	none
USB-to-RJ45		1	9600	none

2 items (1 selected)

```
Terminal <2>

[admin@OOB-ac-lite] > system/serial-terminal port=USB-to-4xRS232 channel=3

[Ctrl-A is the prefix key]

[Q - quit connection]      [B - send break]
[A - send Ctrl-A prefix]   [R - autoconfigure rate]

trying rate 115200
timeout trying rate

trying rate 9600
rate detected

WLAN-CONTROLLER>
WLAN-CONTROLLER> █
```

# Special-Login config

(SSH user-port mapping)

New Group

Name:

OK Cancel Apply

Policies: ☐ local ☐ telnet ☒ ssh

☐ ftp ☐ reboot ☐ read

☐ write

☐ winbox

☐ sniff

☐ romon

Skin: default

System

User List

Name	Group	Allowed Address	Comment
admin	full		system default
serial-FW	serial		
serial-WLC	serial		

Special Login List

User	Port
serial-FW	USB-to-4xRS232
serial-WLC	USB-to-RJ45

```
Terminal <1>
[admin@OOB-ac-lite] > special-login/add user=serial-WLC port=USB-to-RJ45
[admin@OOB-ac-lite] >
[admin@OOB-ac-lite] > special-login/add user=serial-FW port=USB-to-4xRS232 channel=0
[admin@OOB-ac-lite] >
```

Command Line only

```
OpenSSH SSH client
PS C:\> ssh -l serial-WLC 192.168.45.142
serial-WLC@192.168.45.142's password:

[Ctrl-A is the prefix key]

WLAN-CONTROLLER>
WLAN-CONTROLLER>

PS C:\> ssh -l serial-FW 192.168.45.142
serial-FW@192.168.45.142's password:

[Ctrl-A is the prefix key]

FIREWALL#
FIREWALL#
```

Port List

Name	Used By	Channels	Baud Rate	Flow Control
USB-to-4xRS232	special-login	4	9600	none
USB-to-RJ45	special-login	1	9600	none

2 items

# Remote Access config

(telnet and logging session to file)

Remote Port <USB-to-4xRS232>

Port: USB-to-4xRS232

Channel: 0

Allowed Addresses: 0.0.0.0/0

Local Address:

TCP Port: 2222

Protocol: rfc2217

Log File: flash/serial-FW-redirect.log

Remote Address:

enabled busy logging active

Port List

Ports Remote Access

Active session

	Port	Channel	Allowed Addresses	TCP Port	Protocol	Remote Address
AL	USB-to-4xRS232	0	0.0.0.0/0	2222	rfc2217	192.168.45.145:64165

A - active, L - logging active

Port List

Ports Remote Access

Name	Used By	Channels	Baud Rate	Flow Control
USB-to-4xRS232	remote-access	4	9600	none
USB-to-RJ45		1	9600	none

File List

File Cloud Backup

Always reserved when 'Remote Access' is enabled

File Name	Type	Size
flash	disk	
flash/pub	directory	
flash/serial-FW-redirect.log	.log file	72 B
flash/skins	directory	

4 items (1 selected) 12.5 MiB of 16.0 MiB used 21% free

SmarTTY - Raw Terminal

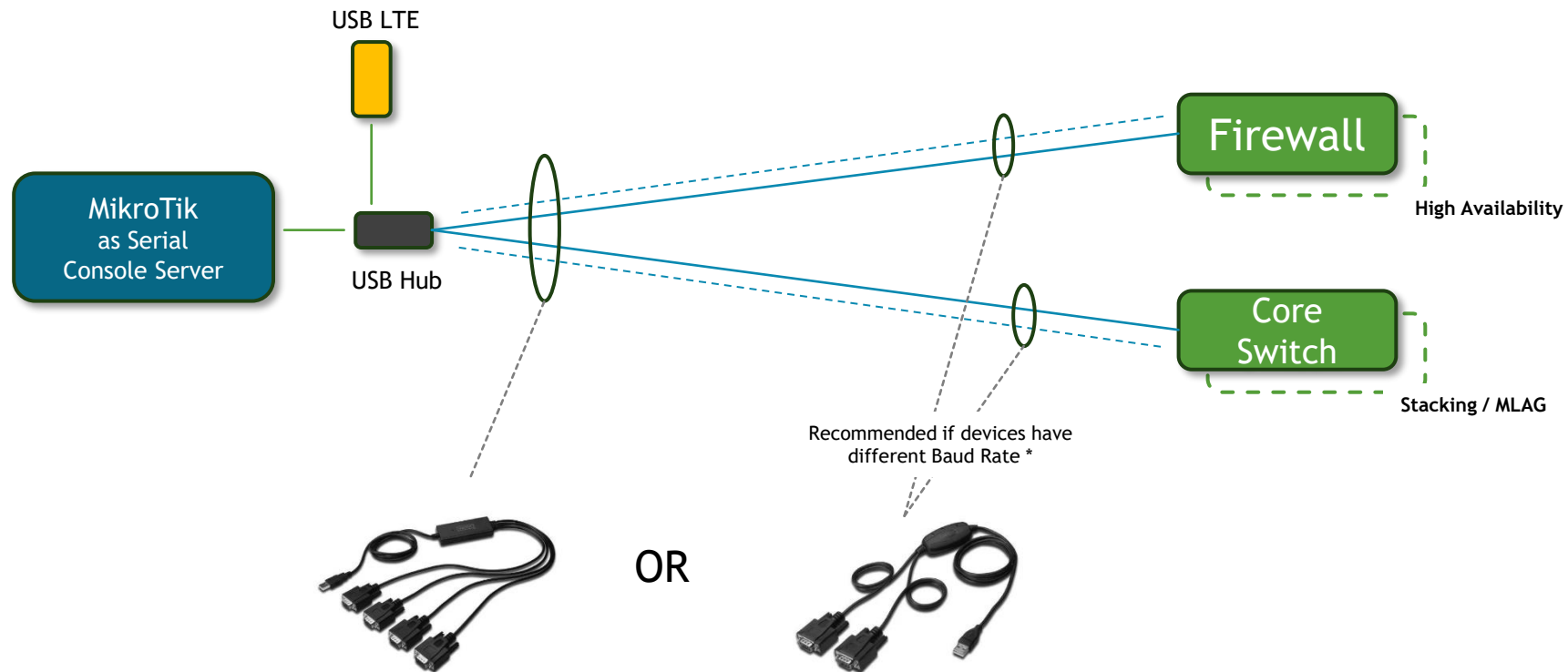
Connected to 192.168.45.142:2222

FIREWALL# \_

memory	sertcp, info	listening on 0.0.0.0:2222 for port USB-to-4xRS232
memory	system, info	serial port forwarding added by admin
memory	sertcp, info	connection to serial remote-access 0.0.0.0:2222 from 192.168.45.145:63418

# Scenario 1

(Mobile OOB)



## How to secure access

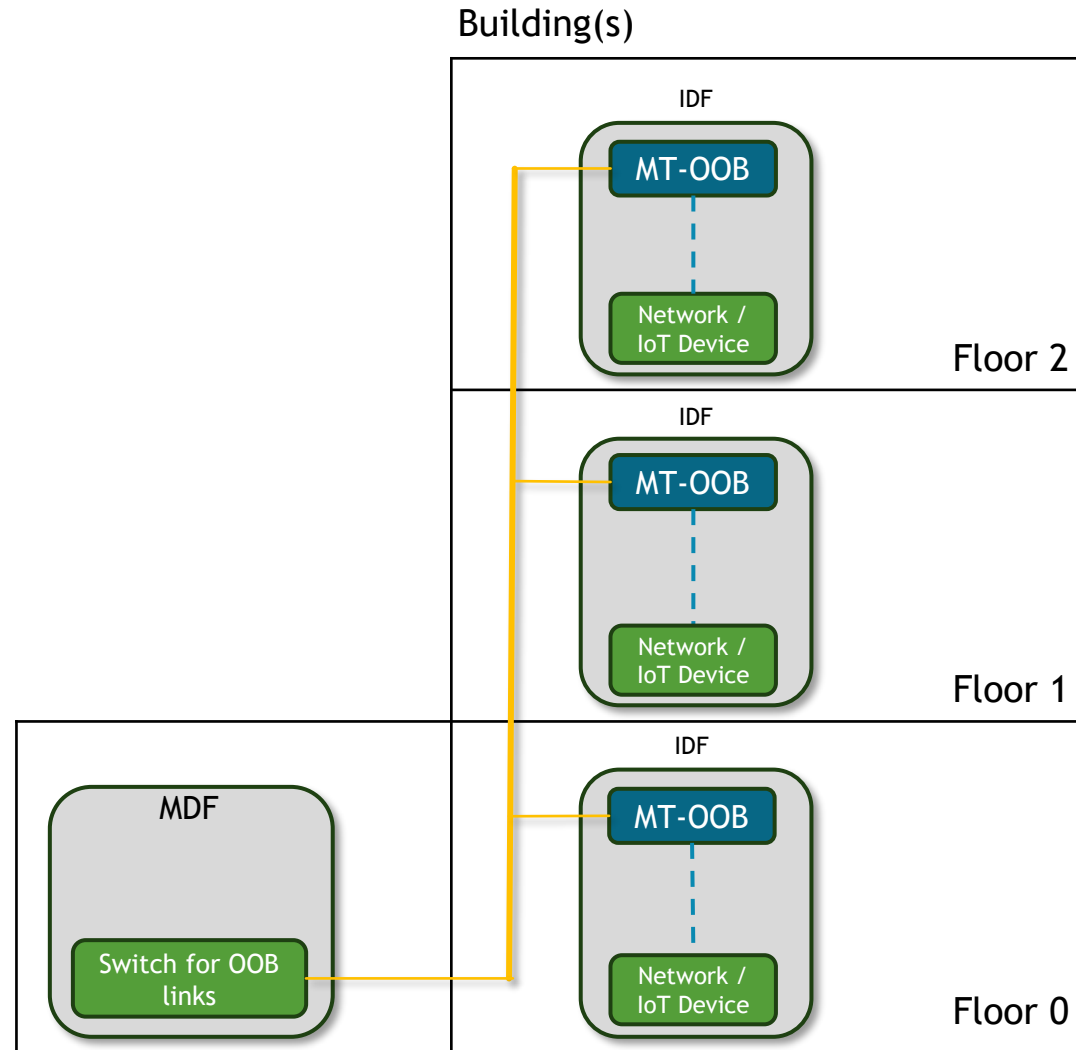
- public IP address with Access-List (plus option - route only to selected hosts without Default Gateway)
- MT-OOB as VPN Server (e.g. if using static / FQDN hosts in the Access-List is not possible)
- MT-OOB as VPN Client to our VPN server(s) (e.g. if we don't have a public IP address)
- private APN

\* - 'R - autoconfigure rate' is a nice feature but static Baud Rate is more reliable



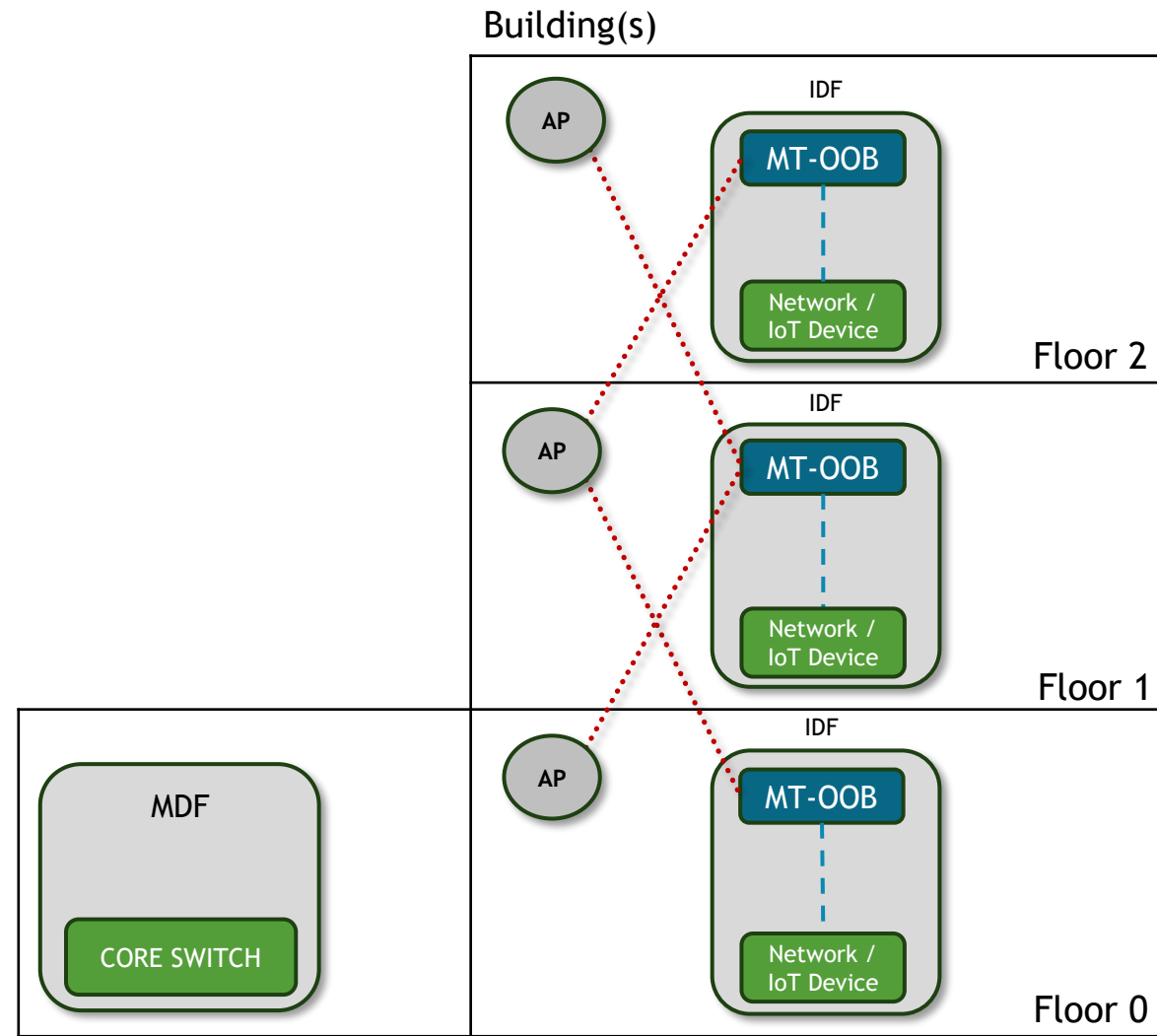
# Scenario 2

(Ethernet / SFP OOB on Campus)



# Scenario 3

(WiFi OOB on Campus / Industrial Facilities)



**Important** - associate the MT-OOB as a wifi client only with an AP that is not connected to a switch managed by this MT-OOB

# Troubleshooting

(and bugs ;) )

- Special-Login USER-PORT-CHANNEL mapping not working ([SUP-122486](#))

RouterOS 7.12beta

\*) console - improved stability when using "special-login"; (but still doesn't work :p)

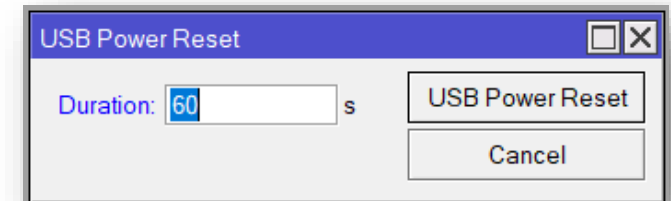
- Ports / Remote Access - wrong behavior ([SUP-122491](#))

problems with enable / disable rule and using 'Local Address' feature (ARM / MMIPS)

- USB issues (RouterOS v7.x) ([SUP-128343](#))

missing channels (MIPSBE / MMIPS) and unsuspected reboots (MMIPS)

All bugs have been verified by MikroTik Support and confirmed.  
Should be fixed in next releases (perhaps in v7.12.x ... )



# Useful Tools - part1

(TFTP server)

TFTP <>

IP Addresses:

Req. Filename:

Real Filename:

☒ Allow

☒ Read Only

Hits:

OK Cancel Apply Disable Copy Remove

enabled

File List

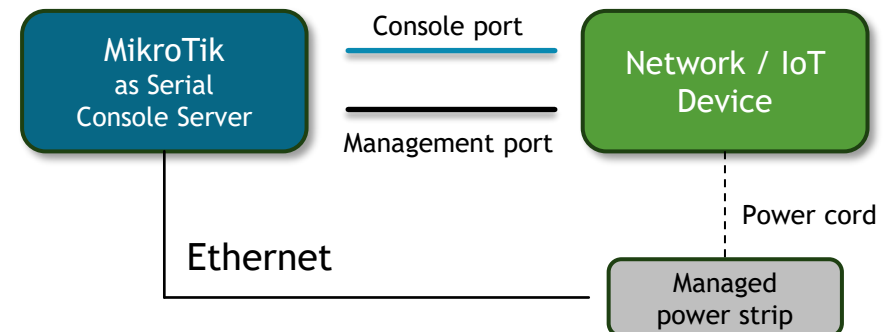
File Cloud Backup

Backup Restore Upload...

File Name	Type	Size
flash	disk	
flash/pub	directory	
flash/serial-FW-redirect.log	.log file	462 B
flash/serial-WLC-redirect.log	.log file	11.0 KiB
flash/skins	directory	
flash/test-TFTP.txt	.txt file	4 B

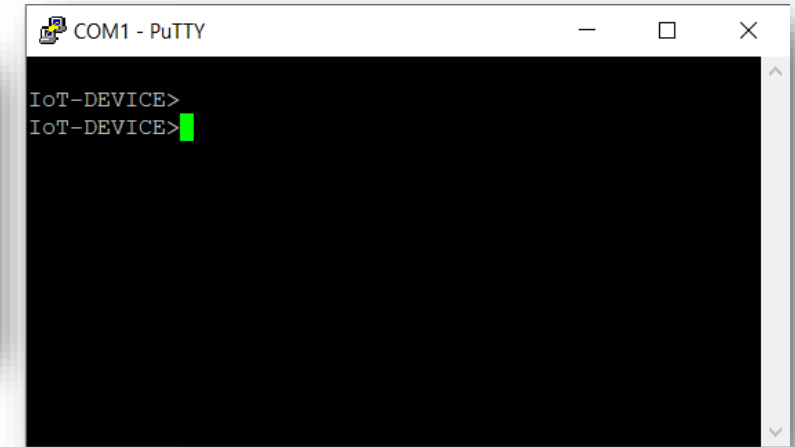
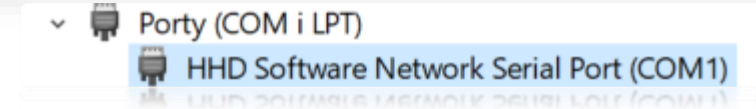
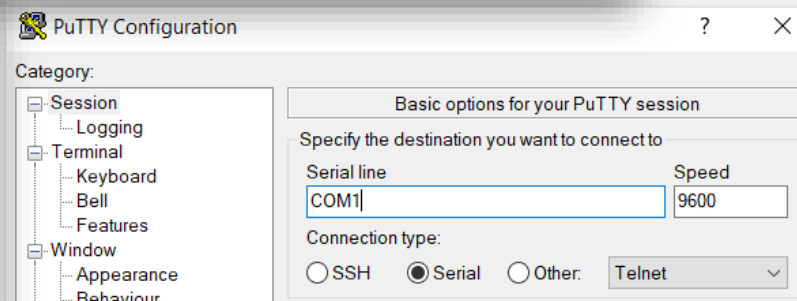
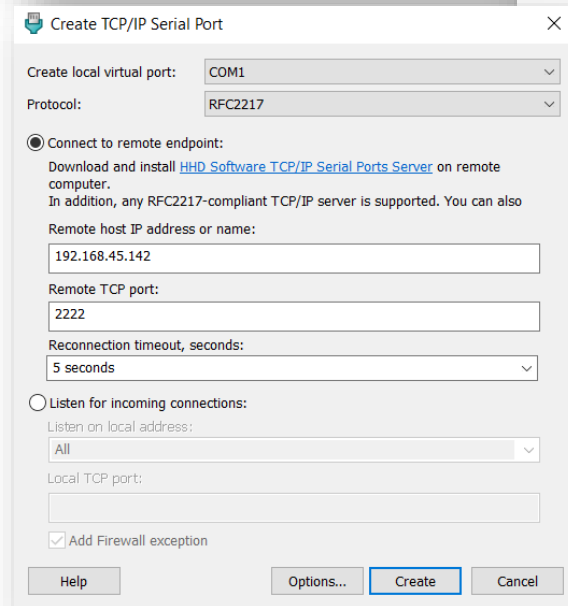
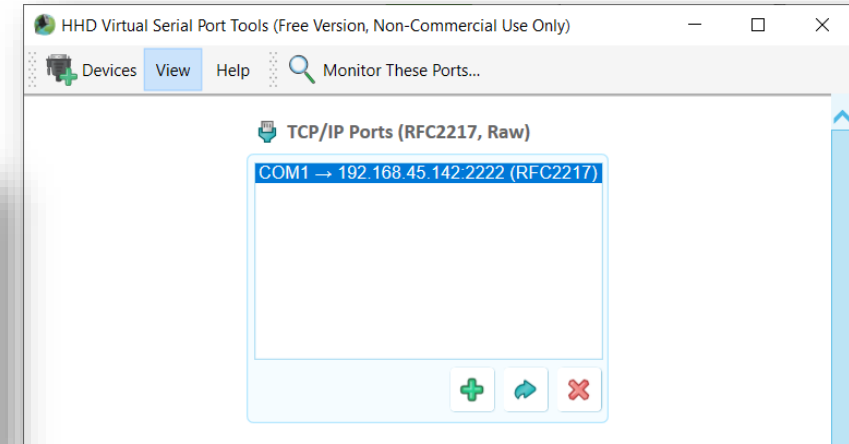
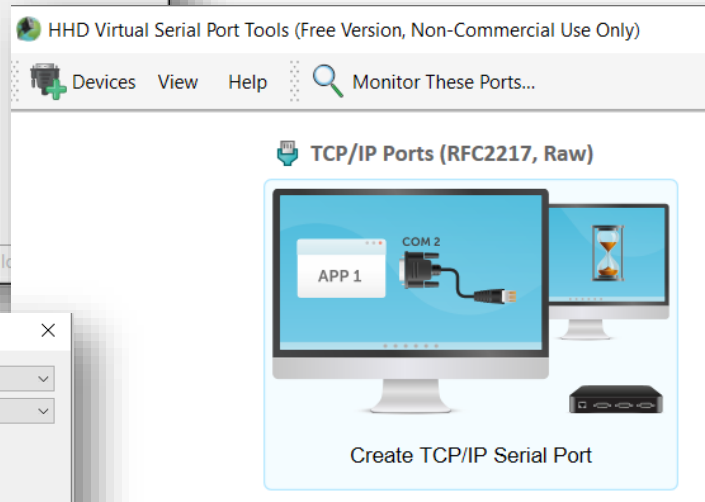
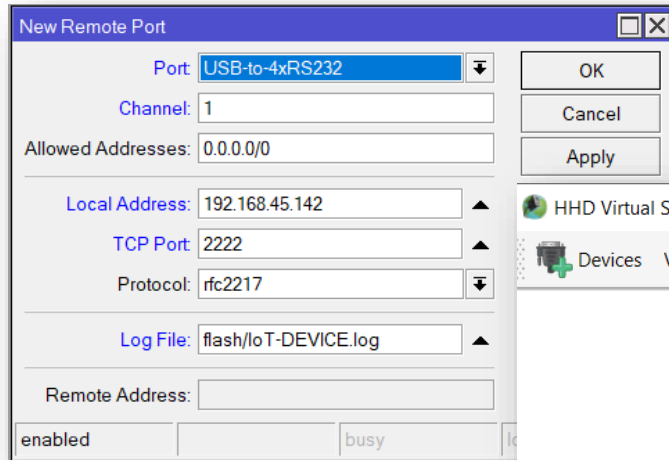
6 items (1 selected) 12.6 MiB of 16.0 MiB used 21%

memory	tftp. packet	recieved type: 1 size: 35
memory	tftp. packet	read filename: test-TFTP.txt binary: 1
memory	tftp. packet	option: blksize value: 8192
memory	tftp. debug	tftpd incoming connection from 192.168.45.155:54286 on 192.168.45.142
memory	tftp. debug	requested file(binary): test-TFTP.txt access: allowed
memory	tftp. debug	opened 192.168.45.142:50241
memory	tftp. packet	sending type: 6 size: 15
memory	tftp. packet	option: blksize value: 4096
memory	tftp. packet	recieved type: 4 seq: 0 size: 4
memory	tftp. packet	sending type: 3 seq: 1 size: 8
memory	tftp. packet	recieved type: 4 seq: 1 size: 4
memory	tftp. debug	closing connection to 192.168.45.155:54286



# Useful Tools - part 2

(Virtual COM over TCP/IP (RFC2217) - <https://freecomportredirector.com/> )



# Summary

**Q & A**