Yatuaprendes

mikrotik

CERTIFIED TRAINER

Who am I?

Yatuaprendes

I’m Jorge Castellet

I’m a Mikrotik Certified Trainer MTCNA, MTCIPv6E, MTCRE, MTCTCE, MTCWE,MTCUME, MTCINE, MTCSE,MTCSWE, MTCEWE

I’m freelancer

j.castellet@yatuaprendes.com

Yaffu!

Yet Another Flashfig Utility

Yatuaprendes

What we need?

In our company we want to configure Mikrotik routers in a simple and massive way.

- We are an isp.
- We sell a solution based on them.
- We are a reseller and we preconfigure them for our customers.

…

What does Mikrotik offer us?

Mikrotik offers us two solutions:

✓Netinstall

✓Flashfig

Netinstall

“Netinstall is a tool for installing and reinstalling MikroTik devices running RouterOS”

Allows you to recover devices by formatting the system and installing routerOS.

It also allows us:

- ✓Load default configuration
- ✓Replace the default configuration with ours

Netinstall manual on:
https://help.mikrotik.com/docs/display/ROS/Netinstall

Netinstall

Disadvantages:

For devices without serial port, you have to press and hold the reset button while the power is turned on and keep it pressed for 10 second (or until the LED goes off)

- ➢Doing it with one hand is a juggling exercise

Can only be configured one at a time.

Flashfig

“Flashfig is an application for mass router configuration. It can be used by MikroTik distributors, ISPs, or any other companies who need to apply RouterOS configuration to many routers in the shortest possible time.”

It applies config within 3 seconds.

Supported by all RouterBOARDs.

Enabled by default from factory since March 2010.

Older devices must be enabled manually.

FlashFig manual on:
https://help.mikrotik.com/docs/display/ROS/Flashfig

Flashfig

Disadvantages:

After usage on a brand new router, it is disabled to avoid unwanted configurations.

Must be enabled manually.

Can only be configured one at a time.

What we want?

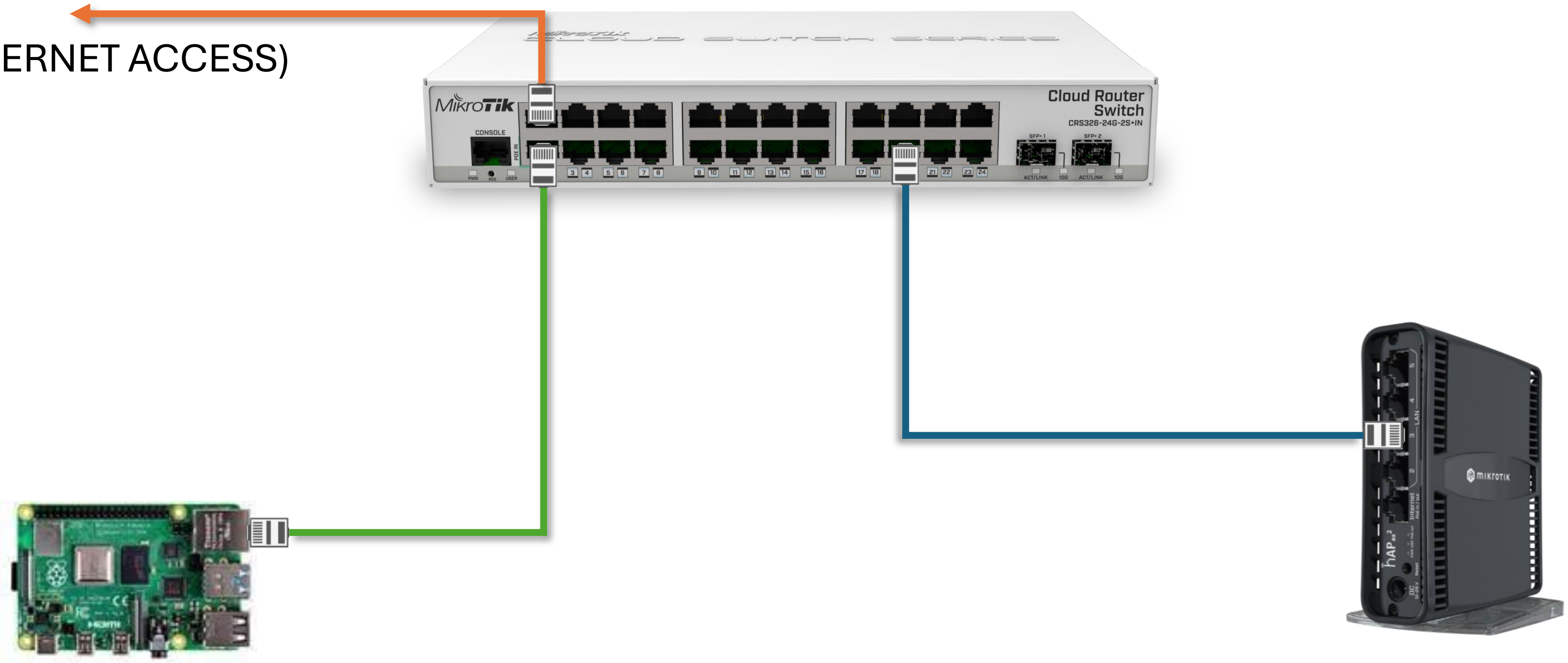
- ✓Keep it simple
- ✓Even with brand new RouterBOARD, when it still smells like a freshly baked circuit board.
- ✓Connect and configure.
- ✓Without doing a factory reset default.
  - ➢(As long as we have access to the device)
- ✓Multiple devices at once.

Yatuaprendes

What we have?

- ✓Mikrotik switch with routerOS (or a mikrotik router)
- ✓Computer
- ✓Network cables
- ✓Power cables
- ✓Soft drinks
- ✓Chips

Connections



LAN
(INTERNET ACCESS)

Yaffu!

Target

How can we access to our target device?

- ❑MAC-TELNET
- ❑TELNET
- ❑SSH
- ❑API

MAC-TELNET

Mikrotik's proprietary protocol to connect to devices that lack an IP address.

Although by name it may seem like a layer 2 protocol, it is actually a layer 3 protocol.

There is a third party implementation for Linux!

- ➢https://github.com/haakonnessjoen/MAC-Telnet

MAC-TELNET

*“**Warning** This repository is in mid-way of adding support for RouterOS v6.43 and up, which does not support the old MD5 authentication method. Expect this to be "alpha quality" for now. The new EC-SRP key sharing and authentication protocol is not implemented in mactelnetd yet.”*

TELNET

Long-standing legacy protocol, well known to those who wouldn't mistake a mobile phone with a 9x1 or 16x2 display for a calculator.

It’s a client-server protocol over port 23/TCP.

RouterOS implements the server and the client.

It is a non-secure protocol.

It is not recommended to use it with paparazzi on our network.

SSH

Protocol that encrypts the connection between the client and server.

SSH uses public-key cryptography to authenticate the remote computer and allow it to authenticate the user.

It would be a “natural evolution” of TELNET.

It’s a client-server protocol over port 22/TCP.

Mikrotik implements the server and the client.

API

“Application Programmable Interface (API) allows users to create custom software solutions to communicate with RouterOS to gather information, adjust the configuration, and manage the router. API closely follows syntax from the command-line interface (CLI). It can be used to create translated or custom configuration tools to aid ease of use running and managing routers with RouterOS”

It is limited in some functionalities.

Since ROS7, the WEB-API version has been available, more in line with the modern time.

API manual on:
https://help.mikrotik.com/docs/display/ROS/API

How can we access to our target device?

- ☒ MAC-TELNET
- ☑ TELNET
- ☑ SSH
- ☑ API

How can we access to our target device?

TELNET, SSH, API

All three methods require an IP address on the target device.

All mikrotik devices come with the same address.

- ➢192.168.88.1

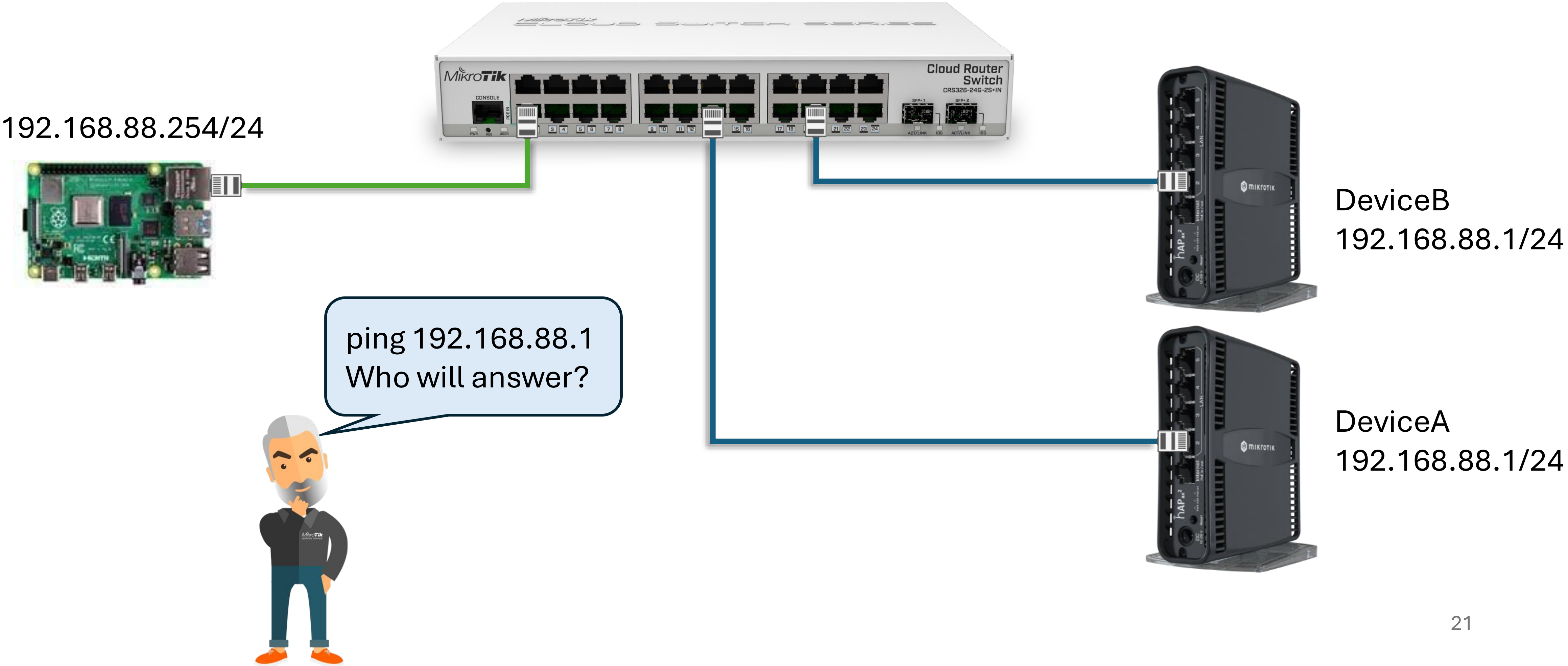
Or maybe the device doesn’t have any IP address

how can we do it?

(I had started to sweat)

Yatuaprendes

All devices with same IP



All devices with same IP

✓We need to remove the computer port from the bridge.

✓We need to assign a different network to the computer.

✓We need to use a floating network to map the duplicate IP.

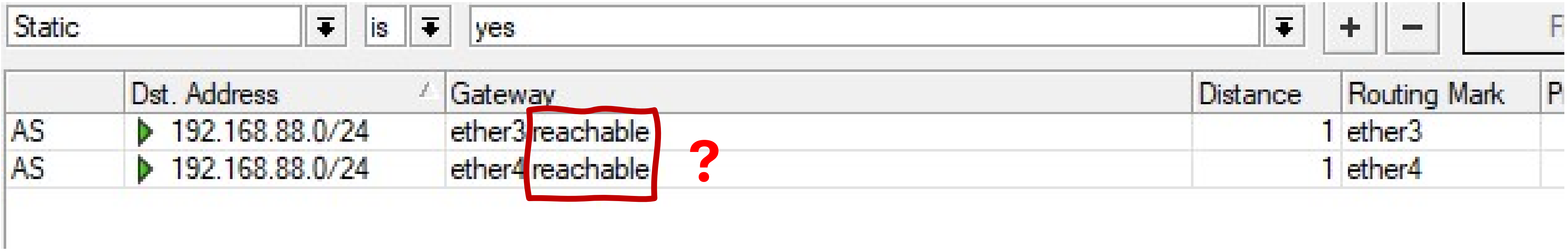
All devices with same IP

```
/ip address add address=10.0.0.1/24 interface=ether1

/ip address add address=192.168.88.254/24 interface=bridge

/ip firewall nat add chain=dstnat action=dst-nat dst-address=172.31.255.203 to-address=192.168.88.1
/ip firewall nat add chain=dstnat action=dst-nat dst-address=172.31.255.204 to-address=192.168.88.1

/ip firewall nat add chain=srcnat action=src-nat out-interface=bridge to-address=192.168.88.254

/ip firewall mangle add chain=prerouting dst-address=172.31.255.203 action=routing-mark new-routing-mark=ether3
/ip firewall mangle add chain=prerouting dst-address=172.31.255.204 action=routing-mark new-routing-mark=ether4

/ip route add 192.168.88.0/24 gateway=ether3 routing-mark=ether3
/ip route add 192.168.88.0/24 gateway=ether4 routing-mark=ether4
```

All devices with the same IP

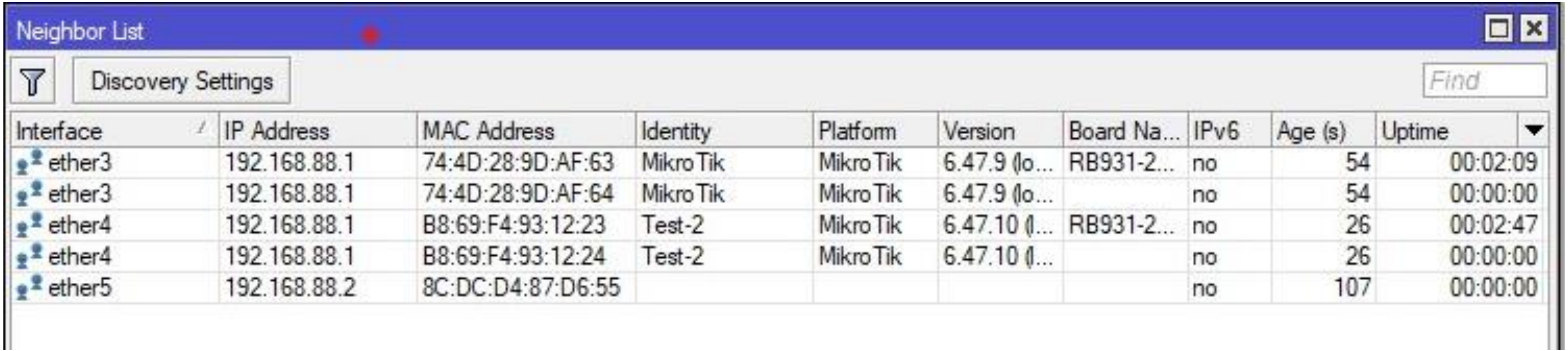
It’s not working!

Ether3 and ether4 are bridge ports, so they can’t be used as interfaces.



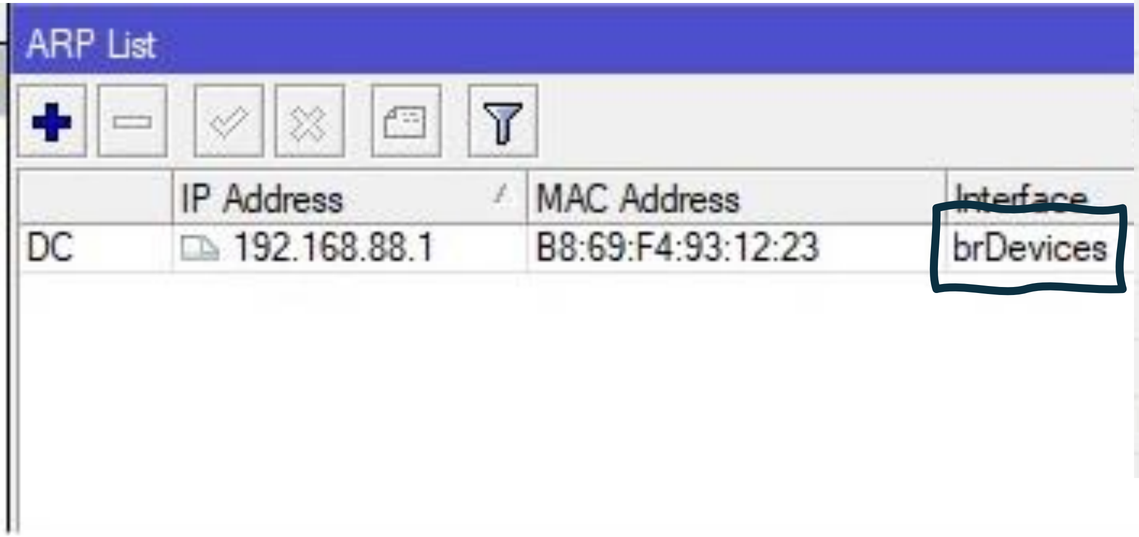
Static is yes

	Dst. Address	Gateway	Distance	Routing Mark	P
AS	▶ 192.168.88.0/24	ether3 reachable	1	ether3	
AS	▶ 192.168.88.0/24	ether4 reachable	1	ether4	



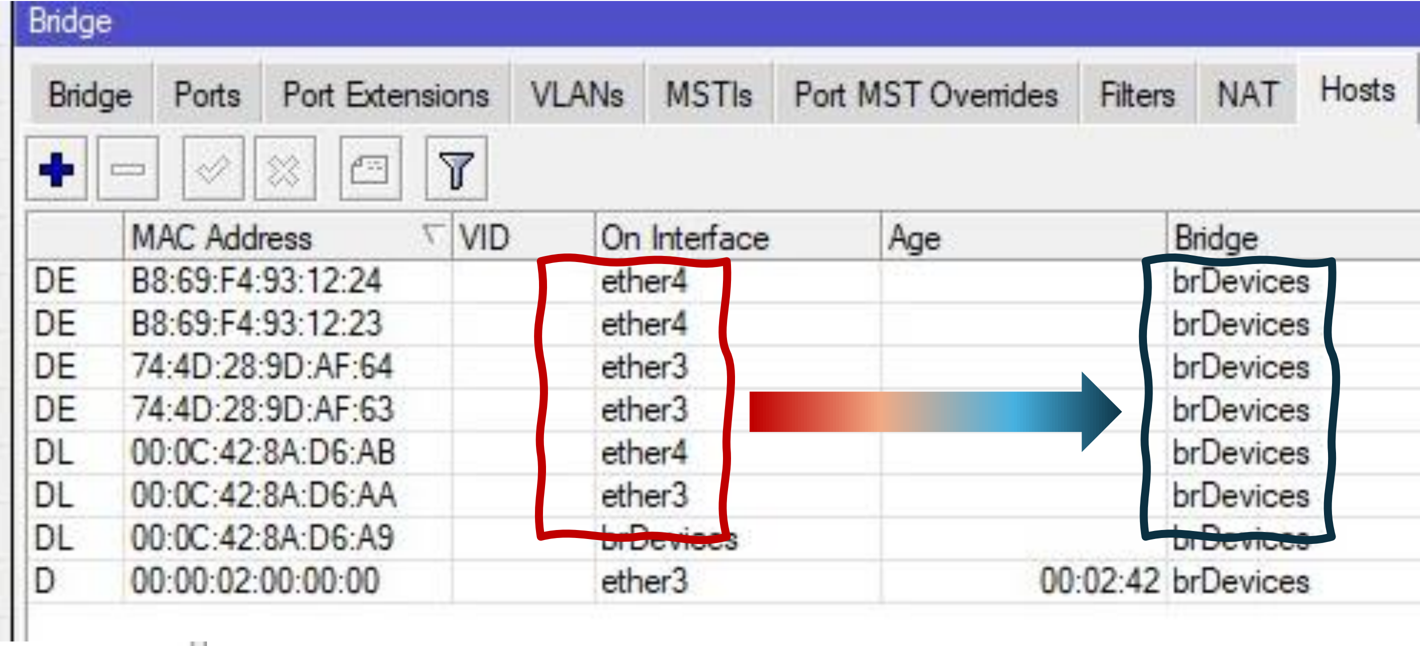
Neighbor List

Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Age (s)	Uptime
ether3	192.168.88.1	74:4D:28:9D:AF:63	MikroTik	MikroTik	6.47.9 (lo...	RB931-2...	no	54	00:02:09
ether3	192.168.88.1	74:4D:28:9D:AF:64	MikroTik	MikroTik	6.47.9 (lo...		no	54	00:00:00
ether4	192.168.88.1	B8:69:F4:93:12:23	Test-2	MikroTik	6.47.10 (l...	RB931-2...	no	26	00:02:47
ether4	192.168.88.1	B8:69:F4:93:12:24	Test-2	MikroTik	6.47.10 (l...		no	26	00:00:00
ether5	192.168.88.2	8C:DC:D4:87:D6:55					no	107	00:00:00



ARP List

	IP Address	MAC Address	Interface
DC	192.168.88.1	B8:69:F4:93:12:23	brDevices



Bridge

	MAC Address	VID	On Interface	Age	Bridge
DE	B8:69:F4:93:12:24		ether4		brDevices
DE	B8:69:F4:93:12:23		ether4		brDevices
DE	74:4D:28:9D:AF:64		ether3		brDevices
DE	74:4D:28:9D:AF:63		ether3		brDevices
DL	00:0C:42:8A:D6:AB		ether4		brDevices
DL	00:0C:42:8A:D6:AA		ether3		brDevices
DL	00:0C:42:8A:D6:A9		brDevices		brDevices
D	00:00:02:00:00:00		ether3	00:02:42	brDevices

All devices with the same IP

If we remove the mangle and routing table is still doesn’t work, because bridge only “resolves” one.

- ➢Only can be one entry ip/mac per interface.

We need to remove the bridge and repeat the setup for each interface previously on the bridge.

All devices with same IP

```
/ip address add address=10.0.0.1/24 interface=ether1

/ip address add address=192.168.88.254/24 interface=ether3
/ip address add address=192.168.88.254/24 interface=ether4

/ip firewall nat add chain=dstnat action=dst-nat dst-address=172.31.255.203 to-address=192.168.88.1
/ip firewall nat add chain=dstnat action=dst-nat dst-address=172.31.255.204 to-address=192.168.88.1

/ip firewall nat add chain=srcnat action=src-nat out-interface=ether3 to-address=192.168.88.254
/ip firewall nat add chain=srcnat action=src-nat out-interface=ether4 to-address=192.168.88.254

/ip firewall mangle add chain=prerouting dst-address=172.31.255.203 action=routing-mark new-routing-mark=ether3
/ip firewall mangle add chain=prerouting dst-address=172.31.255.204 action=routing-mark new-routing-mark=ether04

/ip route add 192.168.88.0/24 gateway=ether3 routing-mark=ether3
/ip route add 192.168.88.0/24 gateway=ether4 routing-mark=ether4
```

The device doesn’t have IP

We have seen that access to the device via mac address must be done via mac-telnet

- ➢In Linux it does not support the new encryption.
- ➢In CLI I cannot launch mac-telnet by giving it a command file or like the linux expect command does.

We’re in a dead end?

The device doesn't have IP

✓I will use the switch as a MAC-Telnet proxy.

✓I will use Linux's *"expect"* command to interact with them.

The device doesn’t have IP

```
spawn "telnet" “192.168.88.1" "-l" "admin+ctw80h25"
set ses $spawn_id
set timeout 200
expect -i $ses "Password:"
exp_send -i $ses “\r"
expect -i $ses "*admin*@*]*>"
exp_send -i $ses "/tool mac-telnet $mac\r"
expect -i $ses "Login:"
exp_send -i $ses "admin+ctw80h25\r"
expect -i $ses "Password:"
exp_send -i $ses “\r"
expect -i $ses "*admin*@*]*>"
exp_send -i $ses "/system routerboard pr\r"
expect -i $ses "*admin*@*]*>"
exp_send -i $ses "quit\r"
expect -i $ses "*admin*@*]*>"
exp_send -i $ses "quit\r"
```

I missing a piece of cake

- To use mac-telnet I will need the mac address.
- I need to know the mac address of the devices connected to the switch.

- Mikrotik comes to our rescue with the solution : MNDP

MNDP

“Neighbor Discovery protocols allow us to find devices compatible with MNDP (MikroTik Neighbor Discovery Protocol), CDP (Cisco Discovery Protocol), or LLDP (Link Layer Discovery Protocol) in the Layer2 broadcast domain. It can be used to map out your network.”

Send announcements to the destination multicast address.

CDP	LLDP	MNDP
01:00:0c:cc:cc:cc	01:80:c2:00:00:0e 01:80:c2:00:00:03 01:80:c2:00:00:00	01:80:c2:00:00:0b

API manual on:
https://help.mikrotik.com/docs/display/ROS/Neighbor+discovery

MNDP

Data is transmitted in TLV (Type – Length - Value) format.

LLDP’s TLV structure		
Type	**Length**	**Value**
7 bits	9 bits	0-511 octets

MNDP’s TLV structure		
Type	**Length**	**Value**
2 bytes	2 bytes	0-65535 octets

MNDP

LLDP types	
TLV Type	**TLV Name**
0	End of LLDPDU
1	Chassis ID
2	Port ID
3	TTL
4	Port description
6	System name
7	System capabilities
8	Management address
9-126	Reserved
127	Custom TLV’s

MNDP types	
TLV Type	**TLV Name**
1	MAC address
5	Identity
7	ROS version
8	Platform
10	Uptime
11	Software ID
12	Board
15	IPv6 address
16	Interface name
17	IPv4 address

MNDP

Among all the properties retrieved by mndp we are insterested in:

✓**Address**: The highest IP address configured on a discovered device.

✓**Board**: RouterBoard model. Displayed only to devices with installed RouterOS.

✓**Identity**: Configured system identity.

✓**Interface**: Interface name to which discovered device is connected.

✓**Mac-address**: Mac address of the remote device. Can be used to connect with mac-telnet.

✓**Platform**: Name of the platform. "MikroTik", "cisco", etc.

✓**Version**: Version number of installed software on a remote device.

Yatuaprendes

Let’s do it

Switch:

✓Monitor the status of the ports.

✓Retrieve target device information via ip neighbor (mndp).

✓Connects to the target device using mac-telnet.

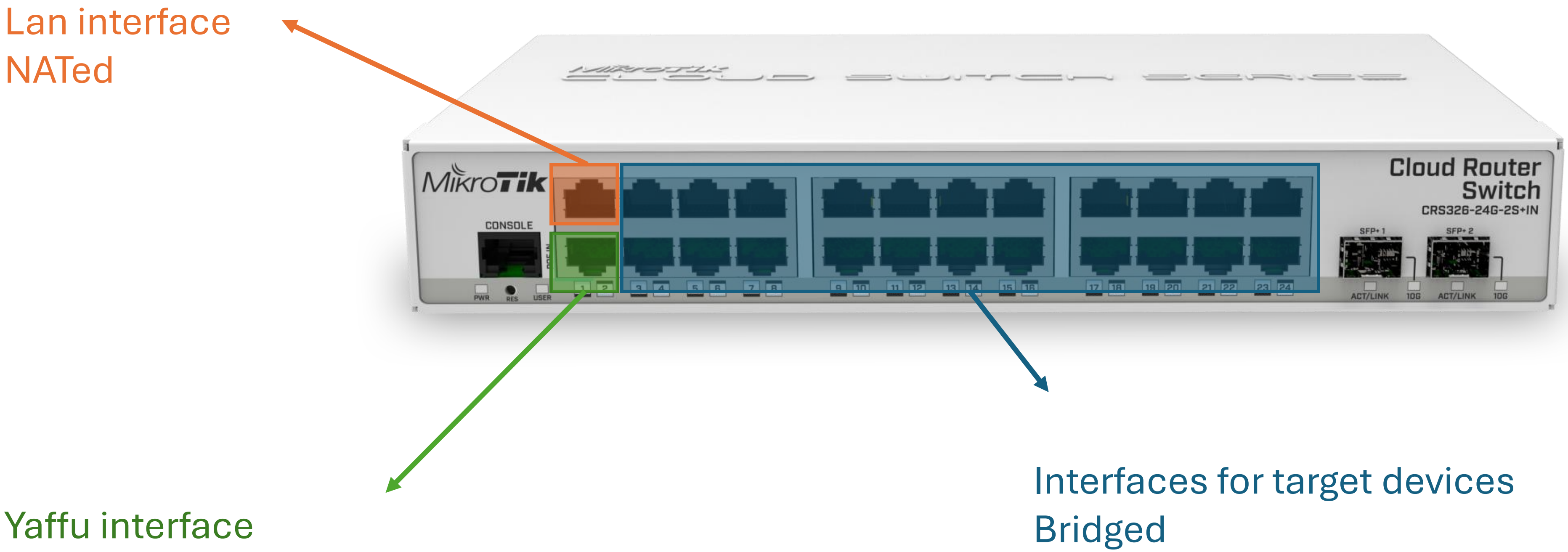
Yaffu:

✓Set a temporary IP on the target device.

✓Installs the tr-069 package on the target device and configures it.

Switch

- To achive our goal, first of all we need to configure our switch



Lan interface
NATed

Yaffu interface

Interfaces for target devices
Bridged

Lan, Yaffu and Bridge are in different broadcast domains

Yaffu setup wizard

✓Executed on first run.

✓Searches for the switch (mndp).

✓Prompt for switch password (if not blank).

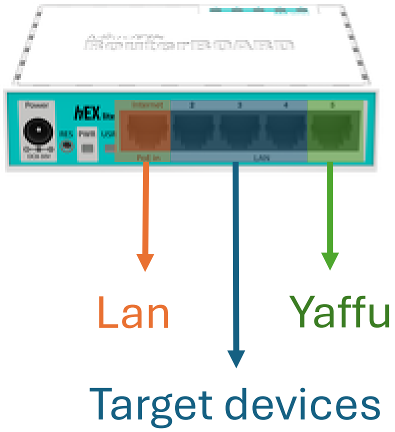
✓Prompt for Lan port selection (if not connected).

✓Prompt for yaffu port (automatically selected).

✓The rest of the Ethernet ports are intended for the target devices.

Space on my carry-on luggage is limited

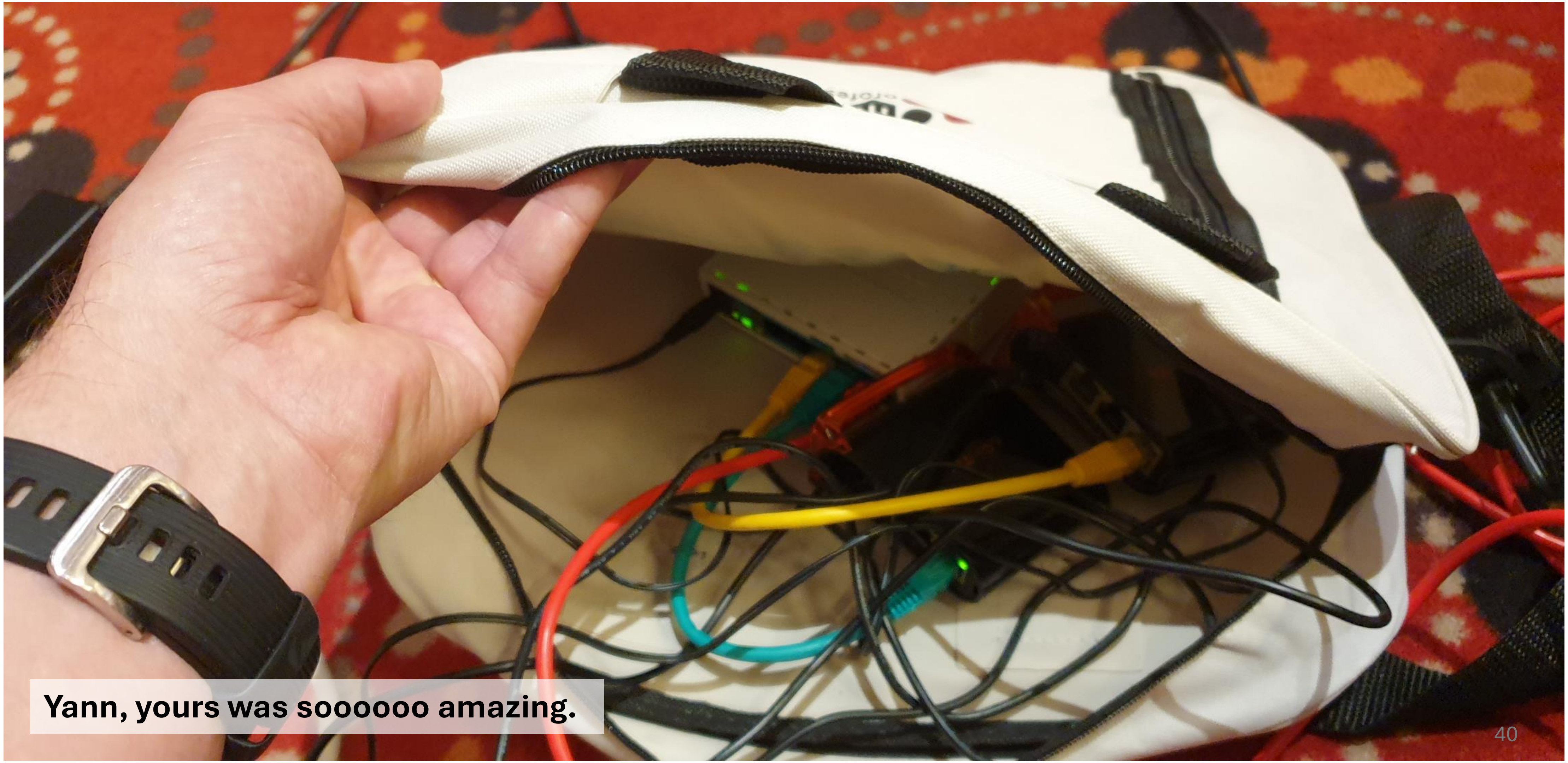
So we are using...



```
# Wait for 30 seconds until the ethernet interfaces avaliable
# (from Mikrotik default-script)
:local count 0;
:while ([/interface ethernet find] = "") do={
  :if ($count = 30) do={
    :log warning "DefConf: Unable to find ethernet interfaces";
    /quit;
  }
  :delay 1s; :set count ($count +1);
};

# Ready, Go!

# Set an ip address on the interface connected to Yaffu
/ip address add address=172.31.0.1/30 interface="ether5"

# Set up a dhcp client on interface connected to internet
/ip dhcp-client add interface="ether1" disabled=no add-default-route=yes

#
/ip firewall nat add chain=srcnat out-interface="ether1" action=masquerade

# Create the bridge where we are going to plug the target devices
/int bridge add name=brDevices
/int bridge port add interface=ether2 bridge=brDevices
/int bridge port add interface=ether3 bridge=brDevices
/int bridge port add interface=ether4 bridge=brDevices
```

Yatuaprendes

My portable laboratory



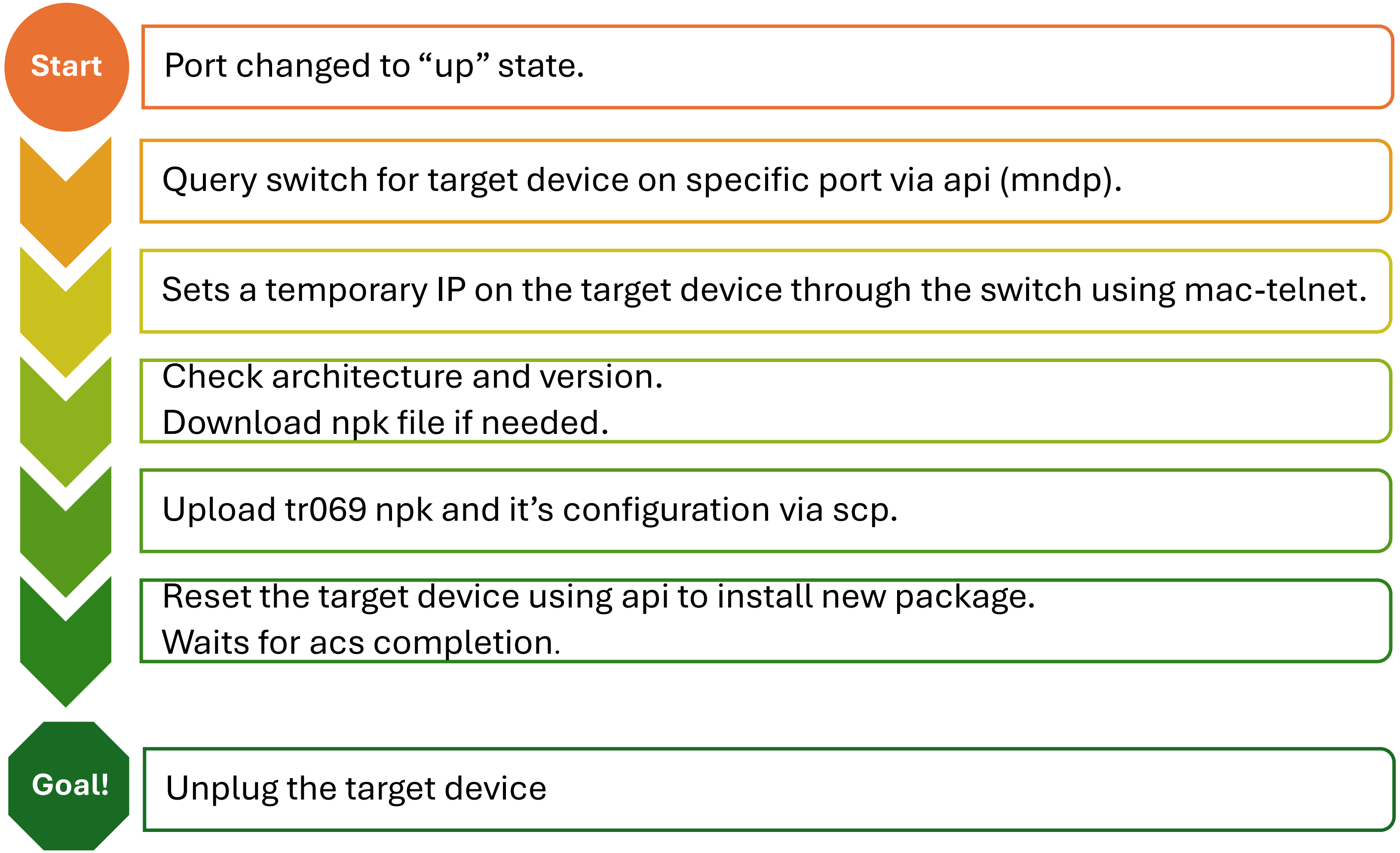
Yann, yours was soooooo amazing.

Switch

Monitors ports using the script scheduled every 5 seconds

```
:global wanport
:global yaffuport
:global ifaceStatus
:foreach i in=[/interface ethernet find] do={
  :local name  [/interface ethernet  get $i name];
  :local running  [/interface ethernet get $i running];
  :if ("$name" != "$yaffuport" && "$name" != "$wanport") do={
      :local value  ($ifaceStatus->$name);
      :if ("$value" = "" || $value != $running) do={
          :local data "{\"port\":\"$name\",\"running\":$running}";
          /tool fetch http-method=post http-header-field="Content-Type: application/json" http-data=$data\
           url="http://172.31.0.2:5000/switch/port"
      }
      :set ($ifaceStatus->$name) $running;
  }
};
```

Configuring target device



Start

Port changed to “up” state.

Query switch for target device on specific port via api (mndp).

Sets a temporary IP on the target device through the switch using mac-telnet.

Check architecture and version.
Download npk file if needed.

Upload tr069 npk and it’s configuration via scp.

Reset the target device using api to install new package.
Waits for acs completion.

Goal!

Unplug the target device

Want to see a demo?

Me too

maybe .... shit happens

References

https://help.mikrotik.com/docs/display/ROS/Neighbor+discovery

https://help.mikrotik.com/docs/display/ROS/MAC+server

https://help.mikrotik.com/docs/display/ROS/Flashfig

https://help.mikrotik.com/docs/display/ROS/Upgrading+and+installation

https://help.mikrotik.com/docs/display/ROS/Netinstall

https://help.mikrotik.com/docs/display/ROS/API

References

https://en.wikipedia.org/wiki/Cisco_Discovery_Protocol

https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

https://en.wikipedia.org/wiki/CDP_spoofing

https://d1gdqjscev06po.cloudfront.net/es/2021/01/14/lldp/

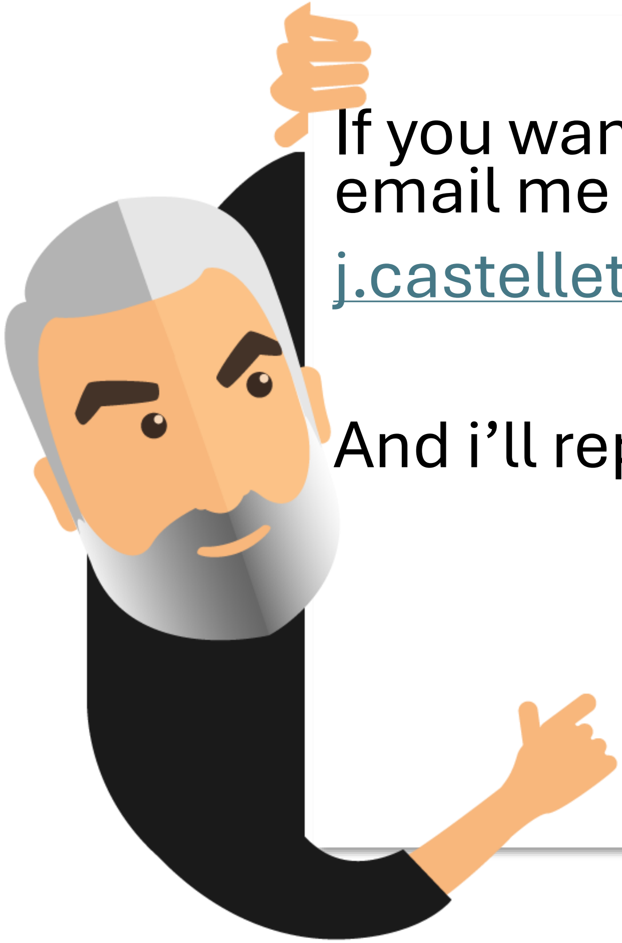
https://help.mikrotik.com/docs/display/ROS/Reset+Button

https://github.com/gtjoseph/mikronode-ng

https://github.com/pheinrichs/node-mndp

https://docs.genieacs.com/en/latest/installation-guide.html

More information?



If you want more information about this presentation, please email me at

j.castellet@yatuaprendes.com

And i’ll reply you as soon as posible.

Thank for your time!

Thank for not having questions