RouterOS bridge/switch configuration changes and possibilities in latest RouterOS versions?

Budapest, Hungary May 31, 2019

About Me

- Péter Major

- AccessPoint Kft.

- Using MikroTik for 9 years

- IgniteNet, Cambium and Ubiquiti trainer

- More test videos in AccessPoint Kft. YouTube channel

AccessPoint

About Company

- AccessPoint Kft

- Started in 2002

- One of the biggest Wireless equipment distributor

- We deals in:
    - Wire and Wireless network devices
    - Passive networks (Fibrain, etc.)
    - Trainings

AccessPoint

About Presentation

- What is the typical problems with CRS?

- What happened to the master-port?

- Switch vs Bridge with VLANs

- LACP

- DHCP Snooping

AccessPoint

Informations from partners

Who have used MikroTik Switces?

Who love MikroTik Switces?

What is the problem with MikroTik Switces?

AccessPoint

Problems with MikroTik Switches?

- Slow throughput

- Programming is hard

- Unstable operation

- **If you set it properly, you won't any problem!**

Let's see some typical problems

- Configuration

- Device selection

- Measurement method

- Configuration

Configuration

Configuration

Configuration

Configuration

Configuration

Configuration

Configuration

Configuration

AccessPoint

What was the Master-port?

Before 6.41 ROS

After 6.41 ROS

AccessPoint
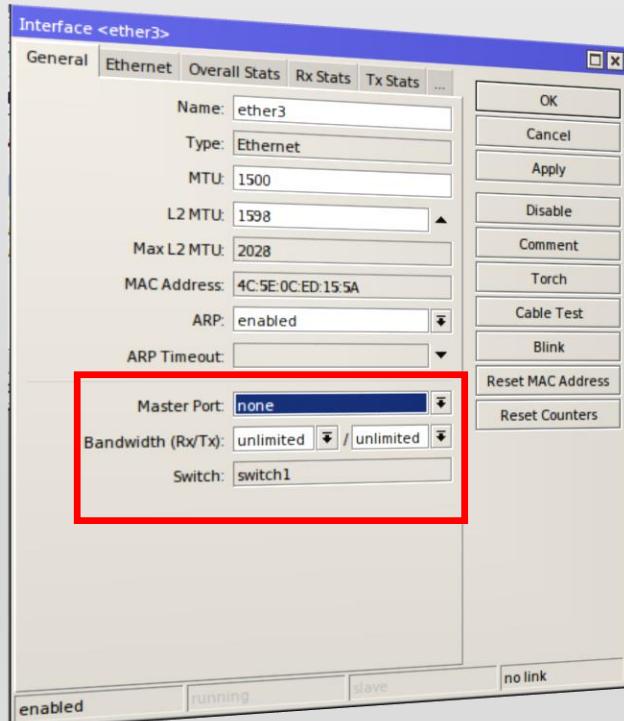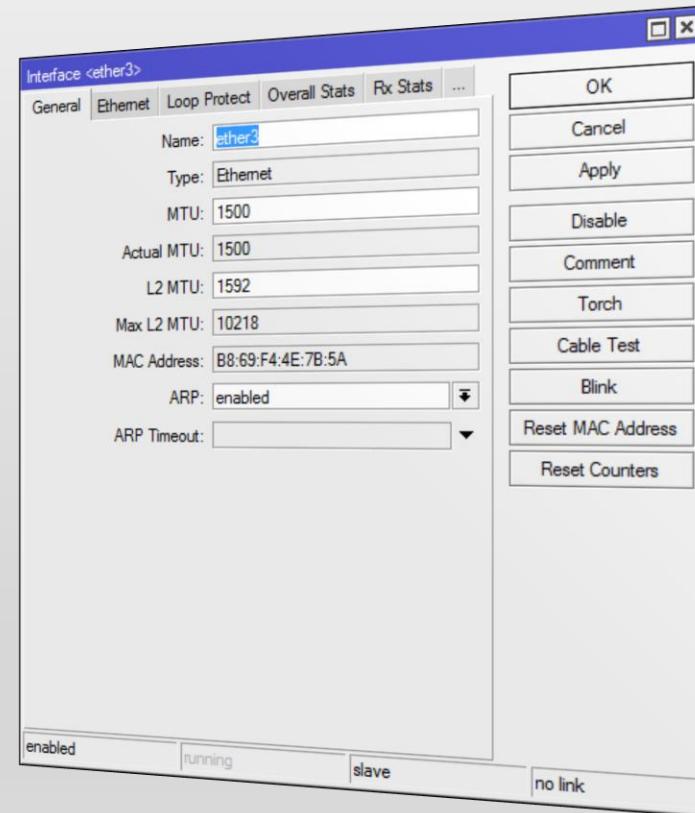
So we can't switch?

- You can!

- Actually it's easier then ever!

- Only put the Interfaces to the Bridge

AccessPoint

So how we can switch?

How it works?

Does is work with my RouterBOARD?

- https://wiki.mikrotik.com/wiki/Manual:Switch_Chip_Features

|	
RB1100AH	Atheros8327 (ether1-ether5); Atheros8327 (ether6-ether10)
RB1100AHx2	Atheros8327 (ether1-ether5); Atheros8327 (ether6-ether10)
CCR1009 series	Atheros8327 (ether1-ether4)
RB493G	Atheros8316 (ether1+ether6-ether9); Atheros8316 (ether2-ether5)
RB435G	Atheros8316 (ether1-ether3) with ether1 optional [more⧉]
RB450G	Atheros8316 (ether1-ether5) with ether1 optional [more⧉]
RB450Gx4	Atheros8327 (ether1-ether5)
RB433GL	Atheros8327 (ether1-ether3)
RB750G	Atheros8316 (ether1-ether5)
RB1200	Atheros8316 (ether1-ether5)
RB1100	Atheros8316 (ether1-ether5); Atheros8316 (ether6-ether10)
DISC Lite5	Atheros8227 (ether1)

etc…

AccessPoint

It can only switch?

- Come on! It is a MikroTik!

- It could be STP, RSTP, MSTP, IGMP Snooping, DHCP Snooping, VLAN Filtering, Bonding with very low CPU load

| RouterBoard/[Switch Chip] Model	Features in Switch menu	Bridge STP/RSTP	Bridge MSTP	Bridge IGMP Snooping	Bridge DHCP Snooping	Bridge VLAN Filtering	Bonding
CRS3xx series	+	+	+	+	+	+	+
CRS1xx/CRS2xx series	+	+	-	+ 1	+ 1	-	-
[QCA8337]	+	+	-	-	+ 2	-	-
[Atheros8327]	+	+	-	-	+ 2	-	-
[Atheros8227]	+	+	-	-	-	-	-
[Atheros8316]	+	+	-	-	+ 2	-	-
[Atheros7240]	+	+	-	-	-	-	-
[MT7621]	+	-	-	-	-	-	-
[RTL8367]	+	-	-	-	-	-	-
[ICPlus175D]	+	-	-	-	-	-	-

What is the VLAN?
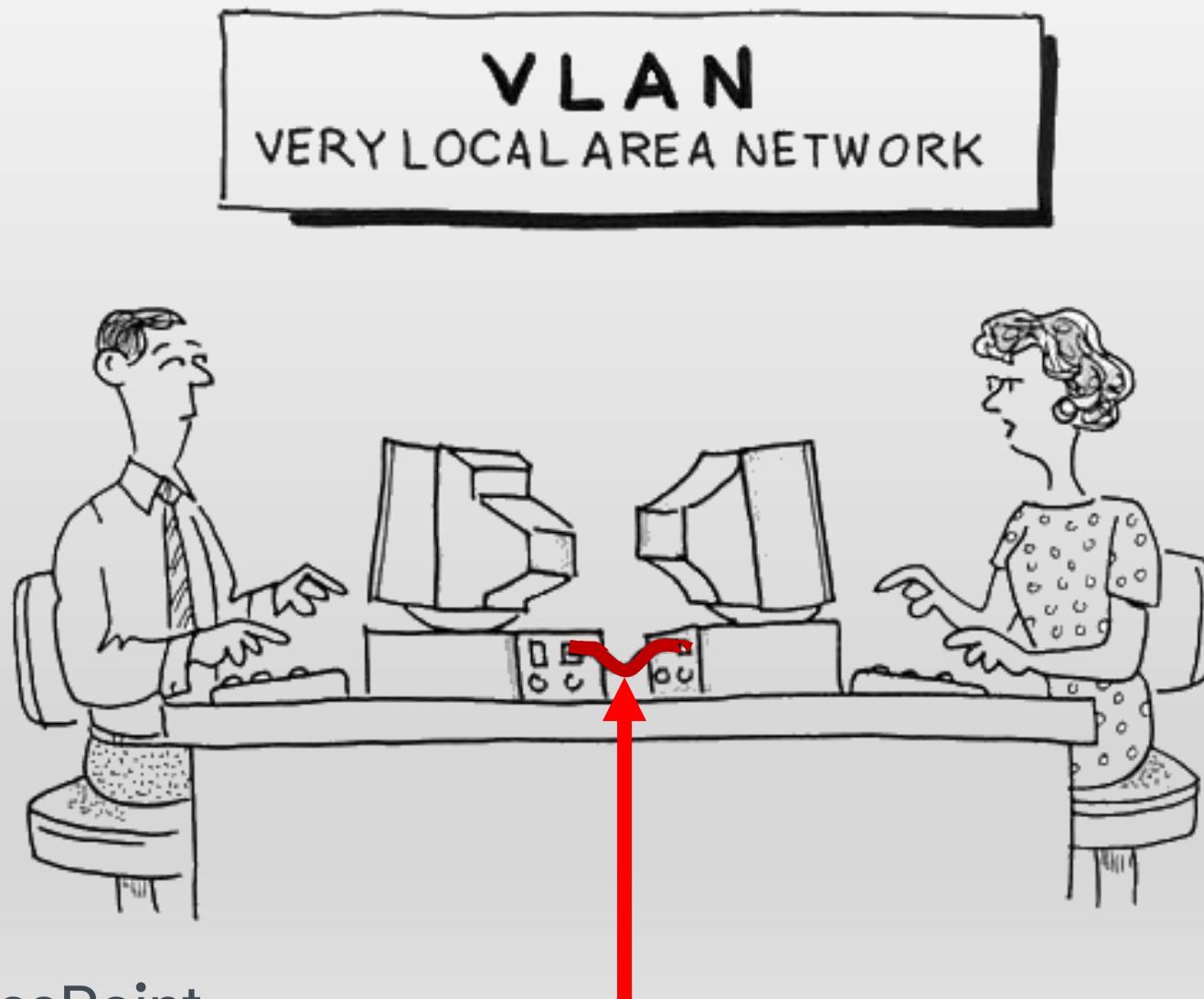
What is the VLAN?

- What is the VLAN?
  - IEEE 802.1Q
  - 4 extra bytes

| Preamble	Destination MAC address	Source MAC address	Type	PayLoad	CRC/FCS

Preamble	Destination MAC address	Source MAC address	802.1Q header (VLAN ID)	Type	PayLoad	Recalculated field CRC/FCS

AccessPoint

How I use the VLANs?

VLAN10 - STAFF
VLAN20 - GUEST
VLAN30 - VoIP
VLAN40 - MGNT

AccessPoint

Let's see some examples

VLAN 100 PRIVATE
VLAN 200 GUEST
VLAN 300 MGNT

Ether1

Ether2
Ether3
Ether4

untagged
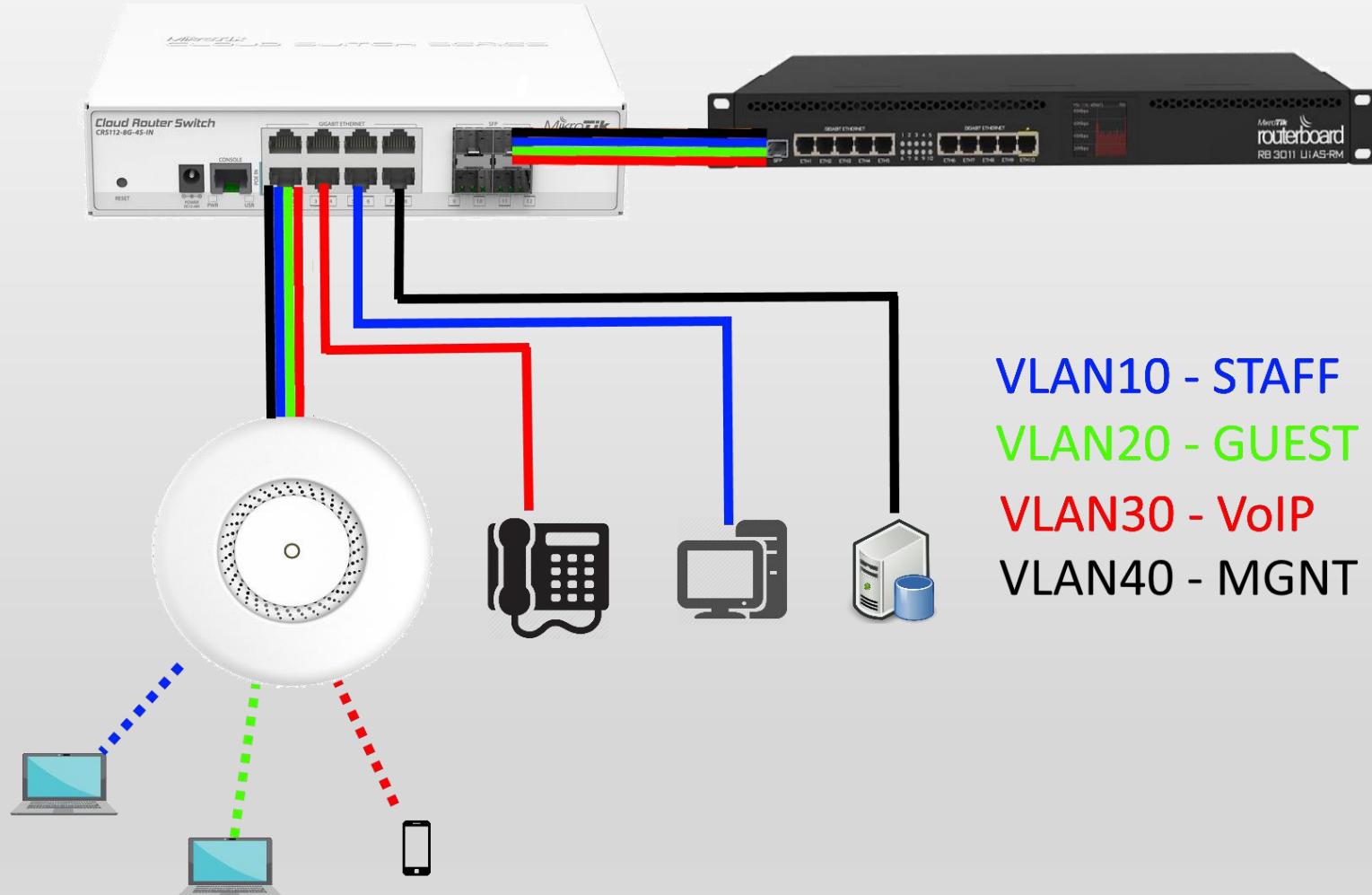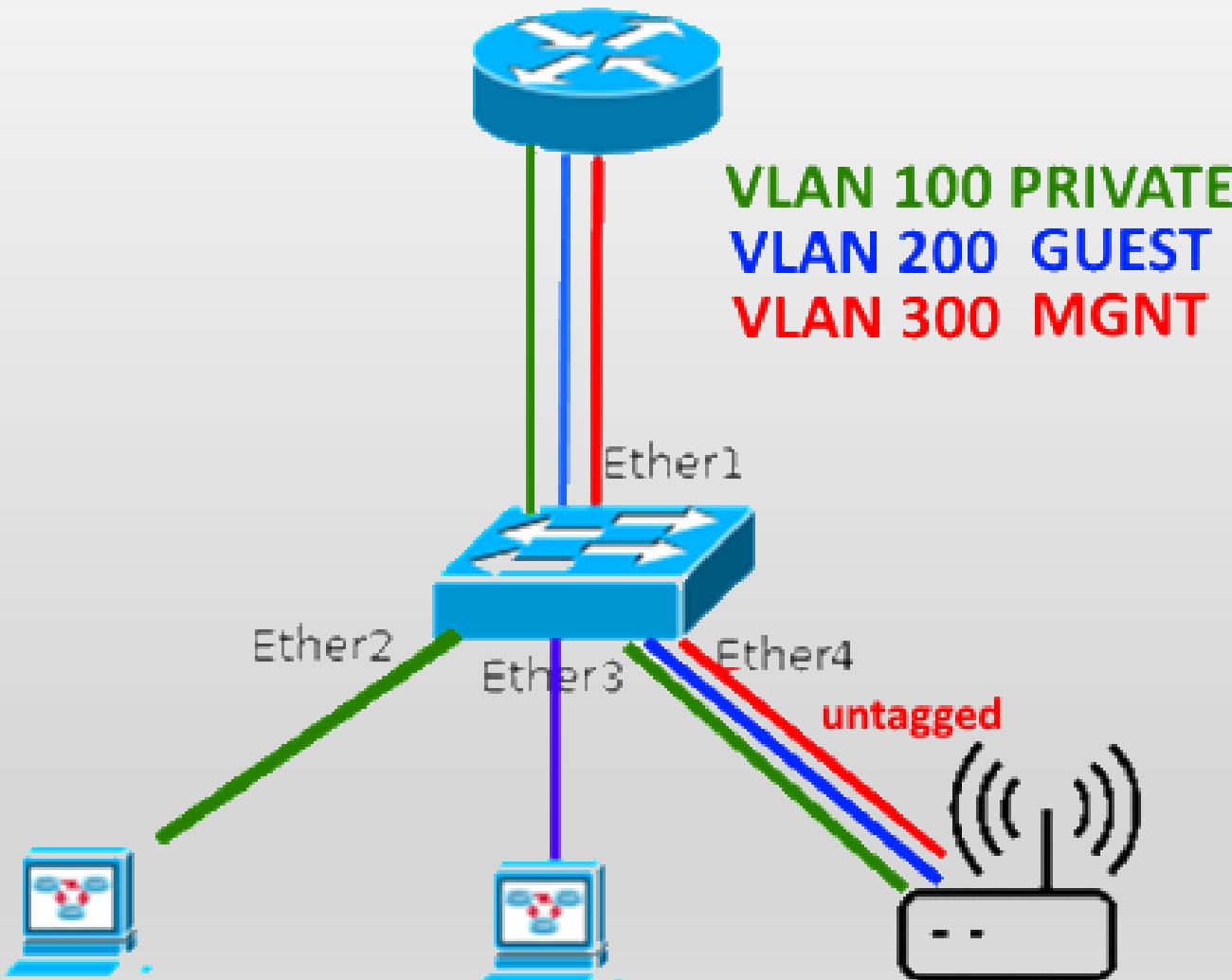
Let's see a **wrong** example

```
/interface vlan
add interface=ether1 name="vlan100 - ETH1" vlan-id=100
add interface=ether4 name="vlan100 - ETH4" vlan-id=100
add interface=ether1 name="vlan200 - ETH1" vlan-id=200
add interface=ether4 name="vlan200 - ETH4" vlan-id=200
add interface=ether1 name="vlan300 - ETH1" vlan-id=300
```

```
/interface bridge
add fast-forward=no name="bridge - VLAN100"
add fast-forward=no name="bridge - VLAN200"
add fast-forward=no name="bridge - VLAN300"
```

```
/interface bridge port
add bridge="bridge - VLAN100" interface="vlan100 - ETH1"
add bridge="bridge - VLAN100" interface=ether2
add bridge="bridge - VLAN100" interface="vlan100 - ETH4"
add bridge="bridge - VLAN200" interface="vlan200 - ETH1"
add bridge="bridge - VLAN200" interface=ether3
add bridge="bridge - VLAN200" interface="vlan200 - ETH4"
add bridge="bridge - VLAN300" interface="vlan300 - ETH1"
add bridge="bridge - VLAN300" interface=ether4
```

VLAN 100 PRIVATE
VLAN 200 GUEST
VLAN 300 MGNT

Ether1
Ether2
Ether3
Ether4
untagged
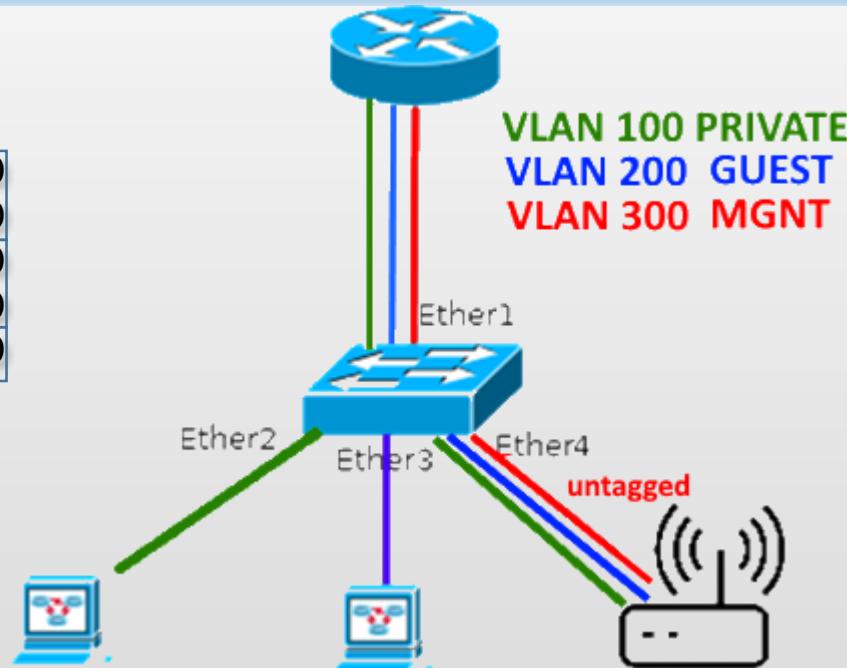
Let's see a **<u>wrong</u>** example
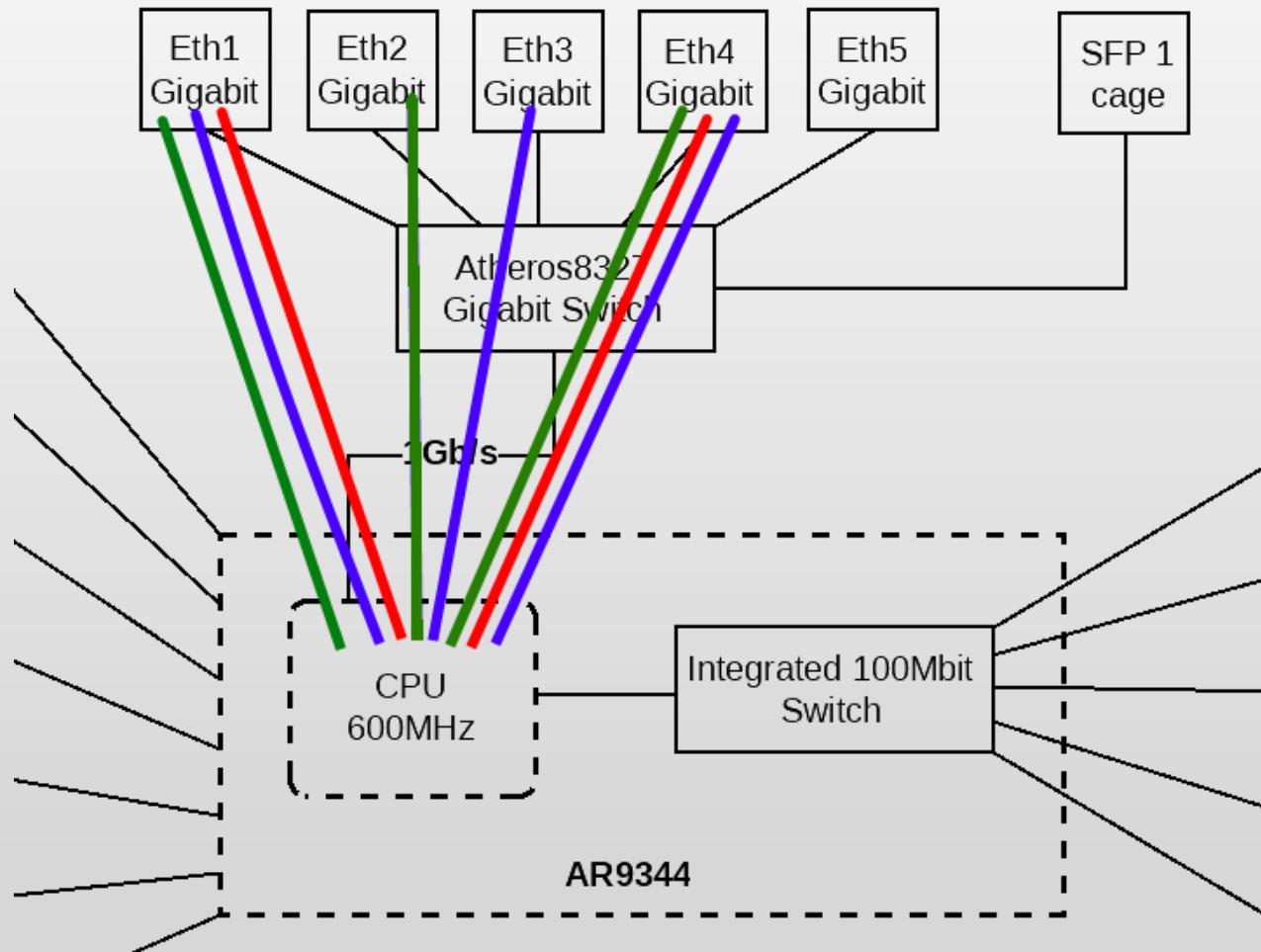


Throughput: ~975Mbps with **60% CPU load**

How can i do it correctly?
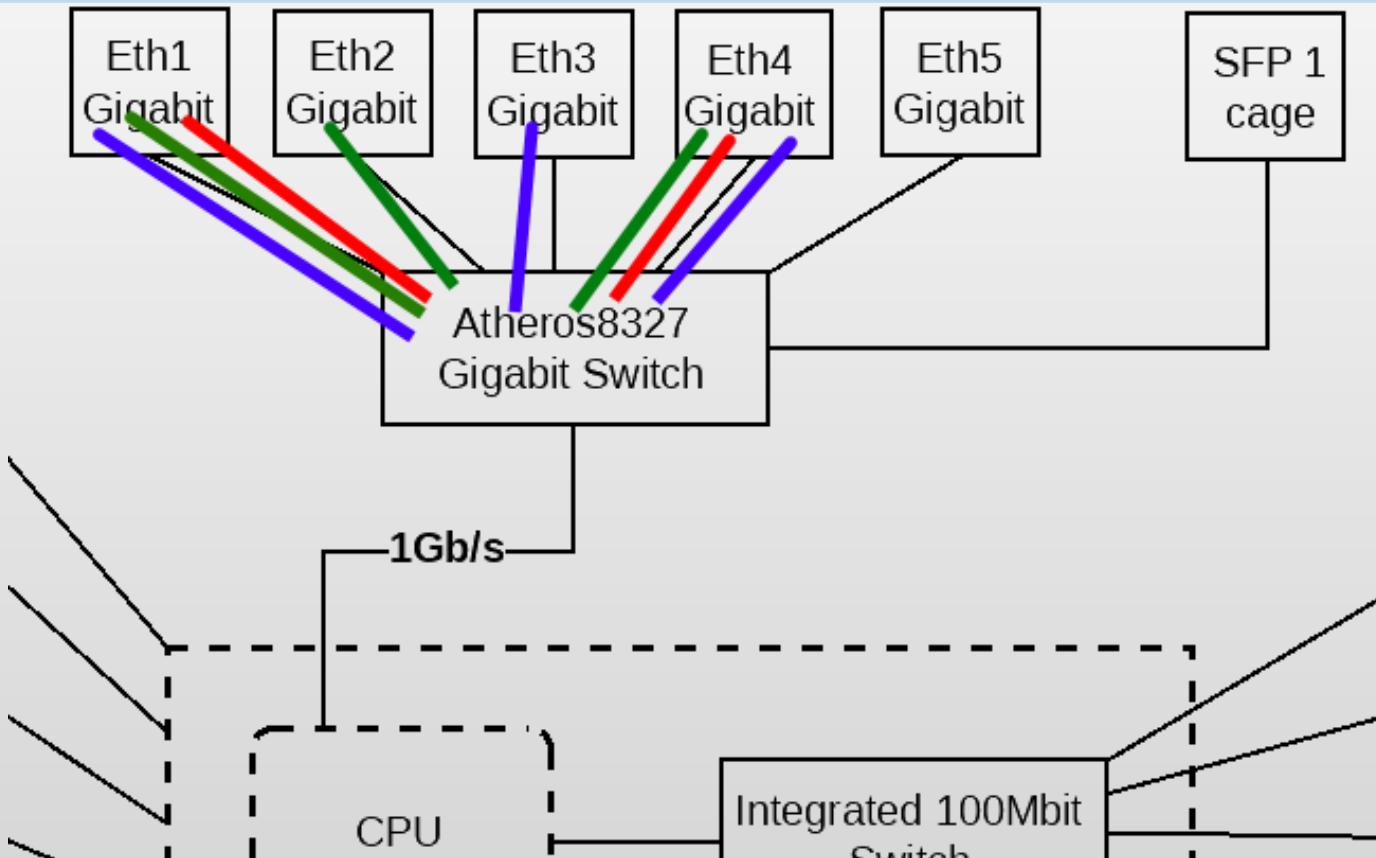
Throughput: ~995Mbps with 2% CPU load

How can i do it correctly with 2011? (Atheros8327) What was the difference before 6.41?

VLAN 100 PRIVATE
VLAN 200 GUEST
VLAN 300 MGNT

```
/interface ethernet
set ether2 master-port=ether1
set ether3 master-port=ether1
set ether4 master-port=ether1
```

```
/interface ethernet switch port
set 1 vlan-header=add-if-missing vlan-mode=secure
set 2 default-vlan-id=100 vlan-mode=secure
set 3 default-vlan-id=200 vlan-mode=secure
set 4 default-vlan-id=300 vlan-header=add-if-missing vlan-mode=secure
```

```
/interface ethernet switch vlan
add ports=ether1,ether2,ether4 switch=switch1 vlan-id=100
add ports=ether1,ether3,ether4 switch=switch1 vlan-id=200
add ports=ether1,ether4 switch=switch1 vlan-id=300
```

Ether1

Ether2

Ether3

Ether4

untagged

AccessPoint
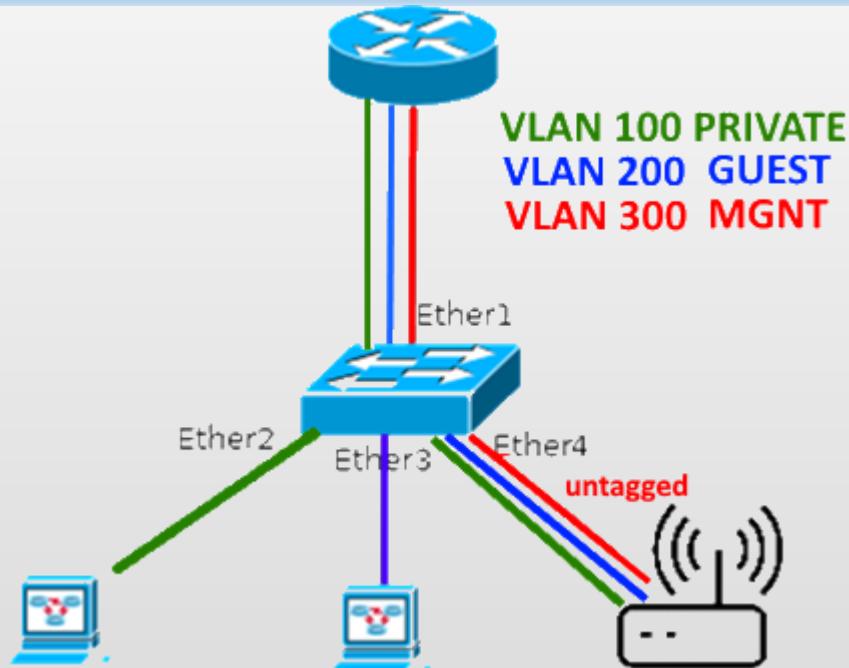
How can i do it with 2011? (Atheros8327)

VLAN 100 PRIVATE
VLAN 200 GUEST
VLAN 300 MGNT

Ether1

Ether2 Ether3 Ether4

untagged

```
/interface bridge port
add bridge=bridge1 interface=ether1
add bridge=bridge1 interface=ether2
add bridge=bridge1 interface=ether3
add bridge=bridge1 interface=ether4


/interface ethernet switch port
set 1 vlan-header=add-if-missing vlan-mode=secure
set 2 default-vlan-id=100 vlan-mode=secure
set 3 default-vlan-id=200 vlan-mode=secure
set 4 default-vlan-id=300 vlan-header=add-if-missing vlan-mode=secure


/interface ethernet switch vlan
add ports=ether1,ether2,ether4 switch=switch1 vlan-id=100
add ports=ether1,ether3,ether4 switch=switch1 vlan-id=200
add ports=ether1,ether4 switch=switch1 vlan-id=300
```

AccessPoint

22
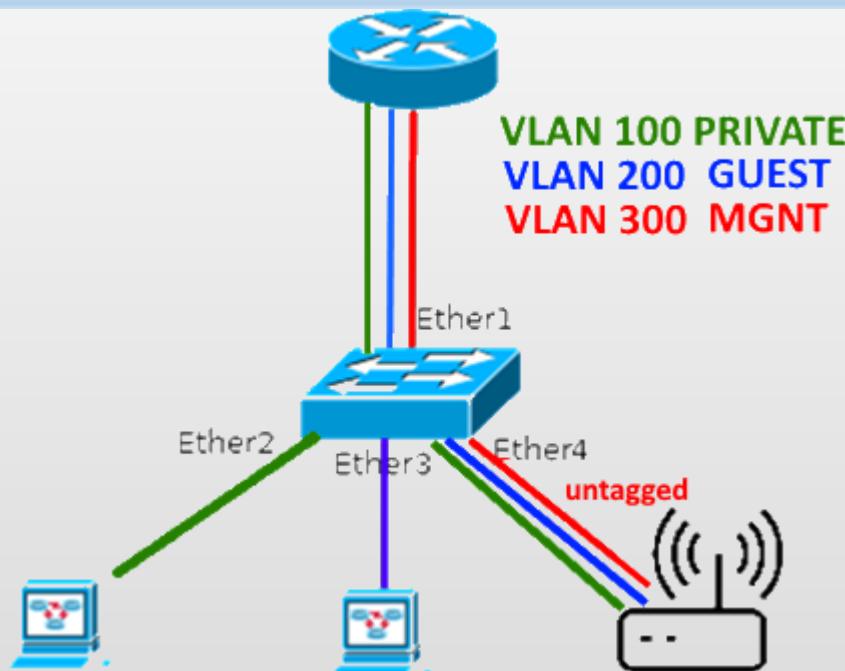
How can i do it with CRS3XX?

/interface bridge
add fast-forward=no name=bridge1 vlan-filtering=yes

/interface bridge port
add bridge=bridge1 interface=ether1
add bridge=bridge1 interface=ether2 pvid=100
add bridge=bridge1 interface=ether3 pvid=200
add bridge=bridge1 interface=ether4 pvid=300

/interface bridge vlan
add bridge=bridge1 tagged=ether1,ether4 untagged=ether2 vlan-ids=100
add bridge=bridge1 tagged=ether1,ether4 untagged=ether3 vlan-ids=200
add bridge=bridge1 tagged=ether1 untagged=ether4 vlan-ids=300

VLAN 100 PRIVATE
VLAN 200 GUEST
VLAN 300 MGNT

Ether1

Ether2
Ether3
Ether4
untagged

AccessPoint
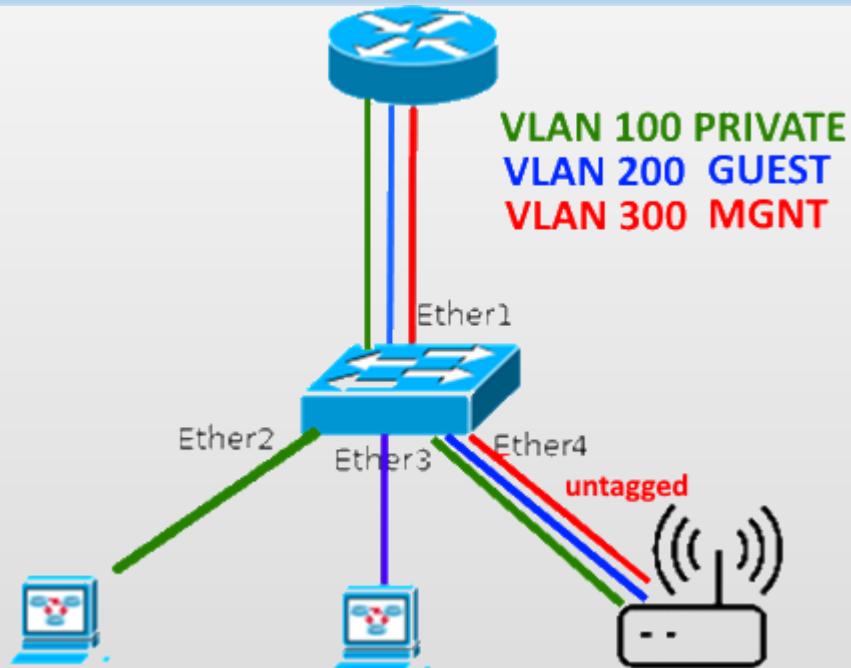
Conclusion

Misconfiguration or
Not proper device selection

can cause problems!

AccessPoint

1 Gigabit sometimes isn't enough

Possibilities?

- Use more compressed data streams $$$$

- Use 2.5G, 10G, 40G link speed $$

- Use Link aggregation $

What is the LAG?

- IEEE 802.3ad
- IEEE 802.1ax

PORT 1   PORT 1

PORT2   PORT2

Link aggregation
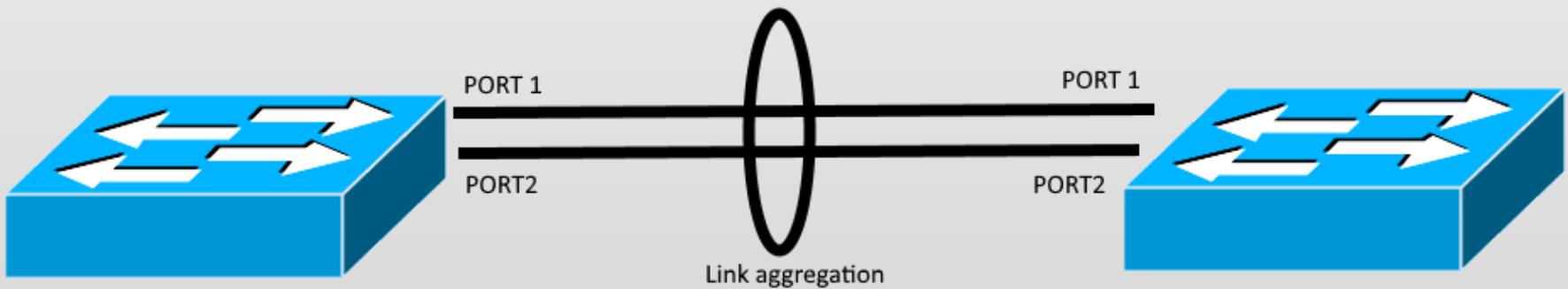
Is it make too high CPU load?

- Yes, could be, if you chosen a bad device

RouterBoard/[Switch Chip] Model	Features in Switch menu	Bridge STP/RSTP	Bridge MSTP	Bridge IGMP Snooping	Bridge DHCP Snooping	Bridge VLAN Filtering	Bonding
CRS3xx series	+	+	+	+	+	+	+
CRS1xx/CRS2xx series	+	+	-	+ 1	+ 1	-	-
[QCA8337]	+	+	-	-	+ 2	-	-
[Atheros8327]	+	+	-	-	+ 2	-	-
[Atheros8227]	+	+	-	-	-	-	-
[Atheros8316]	+	+			+ 2	-	-
[Atheros7240]	+					-	-
[MT7621]	+					-	-
[RTL8367]	+					-	-
[ICPlus175D]	+					-	-

Let's create a bonding!
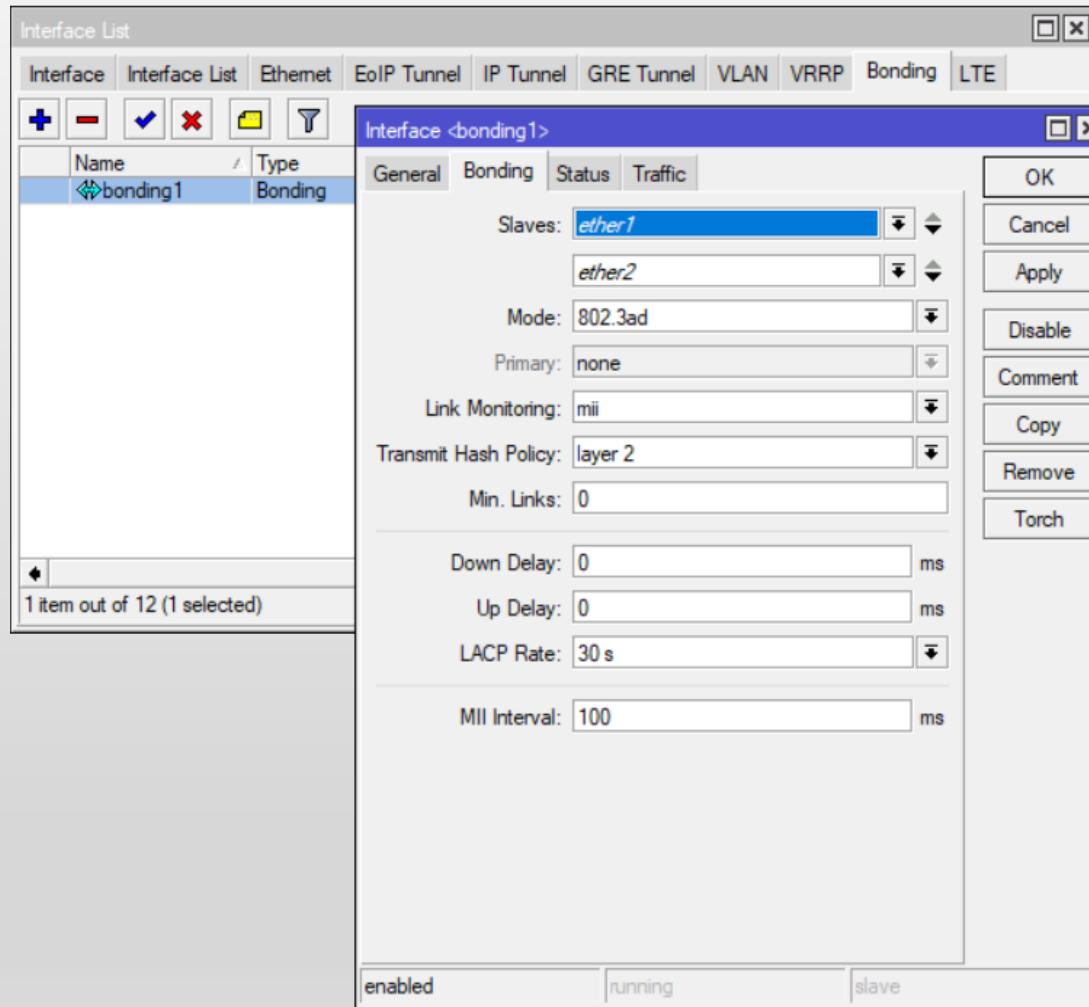
We created a bonding, but it can only 1G

LACP
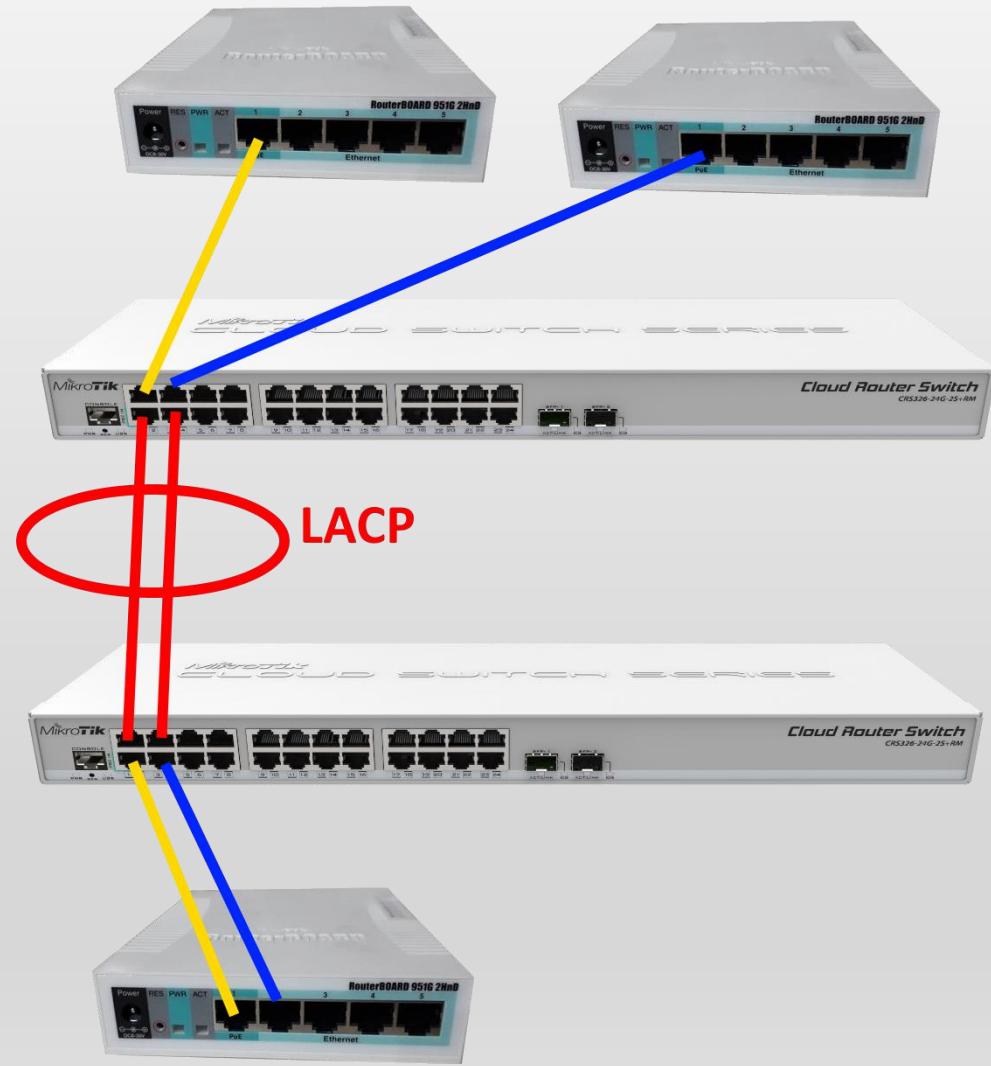
Now, we have 2G

What was the problem?

LACP
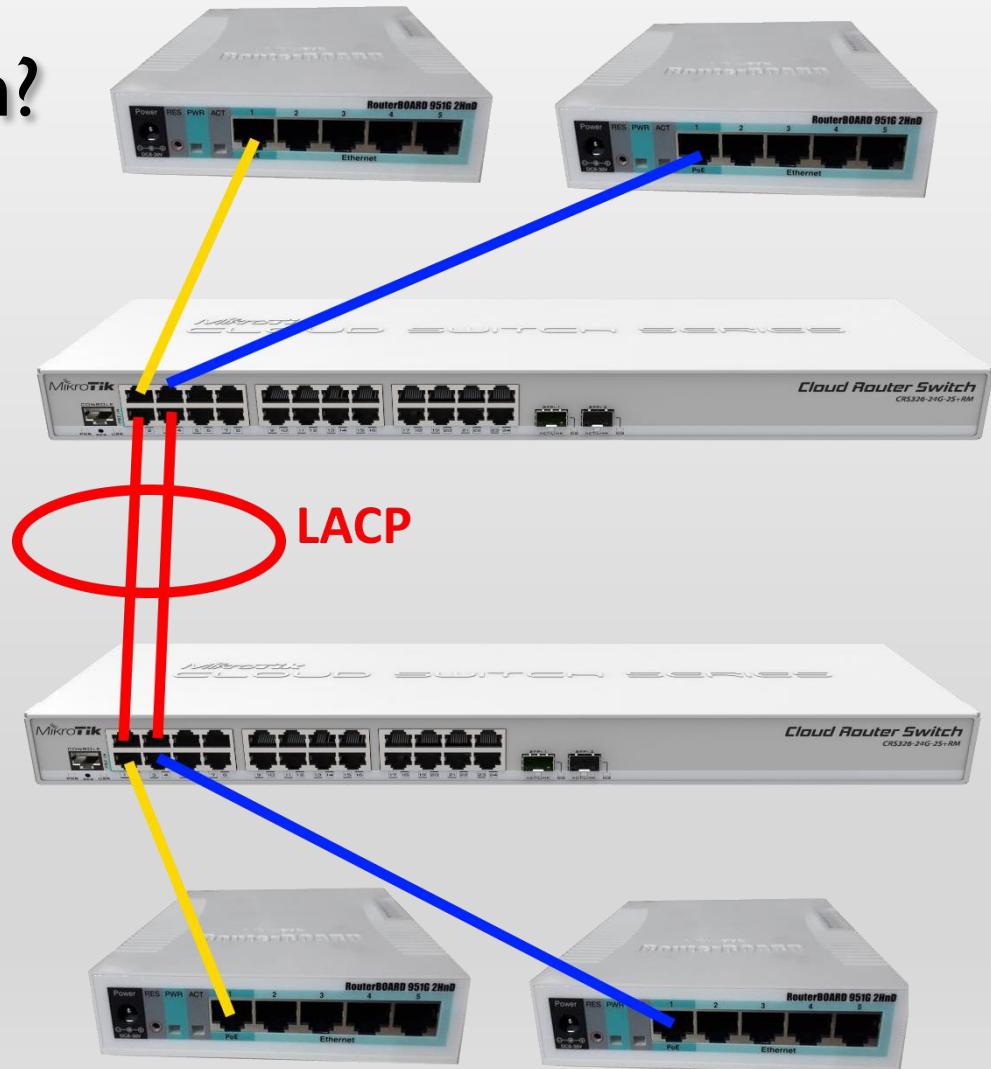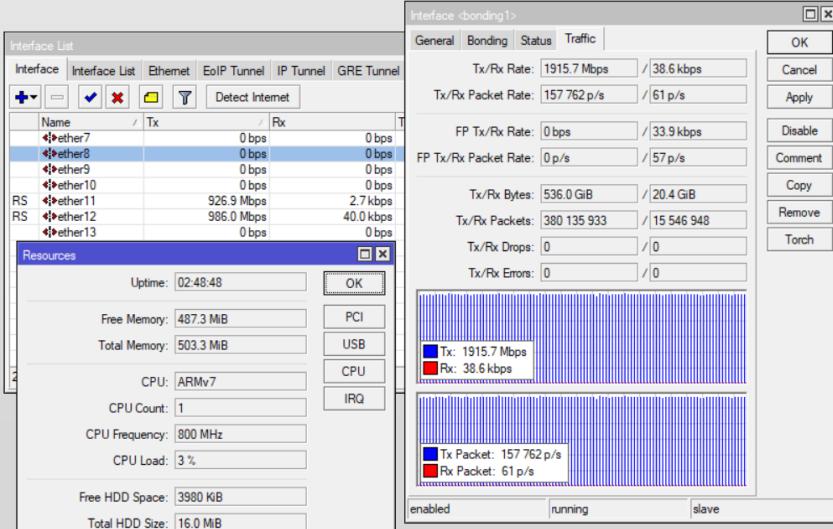
Now, we have 2G
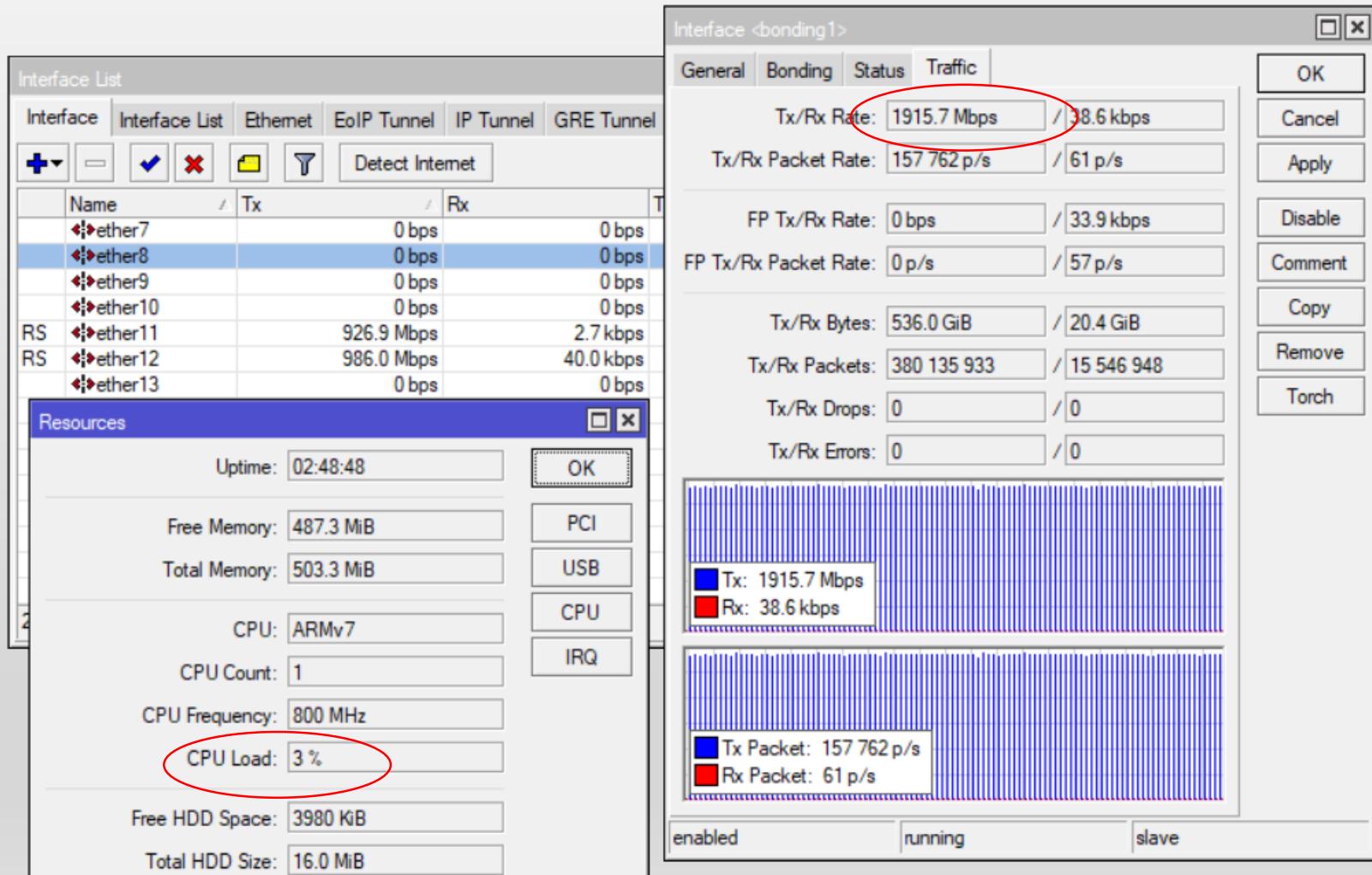
The bottleneck was the 1Gb/s to the CPU
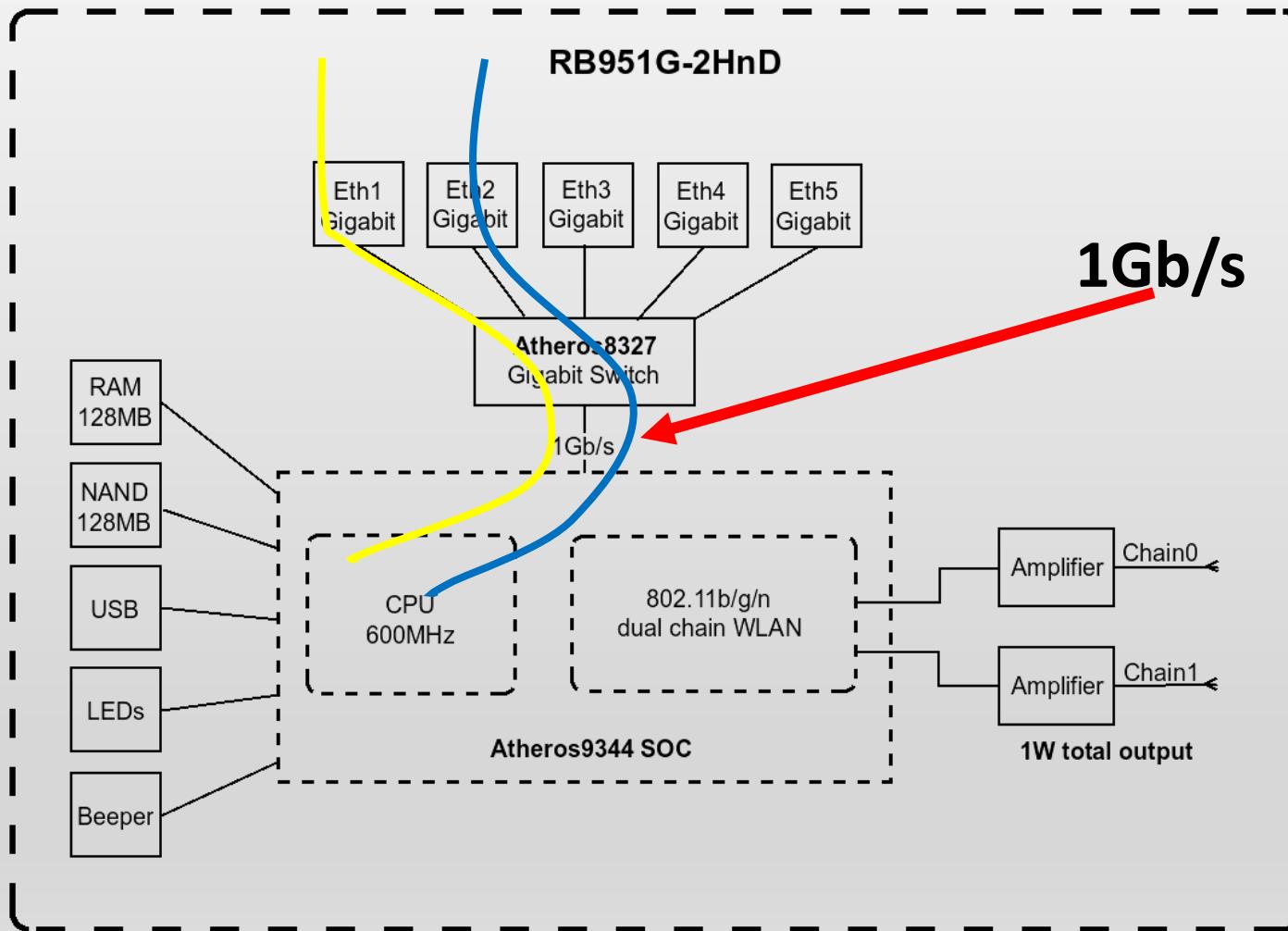
Conclusion

Bad measurement mislead us!

AccessPoint

The DHCP could be dangerous!

- Use Static IPs

- Use ARP for Leases

- Use DHCP Snooping

DHCP Snooping

- What is the DHCP Snooping?

Orginal Server

3   2

4   🚫   3

1   2

Fake Server
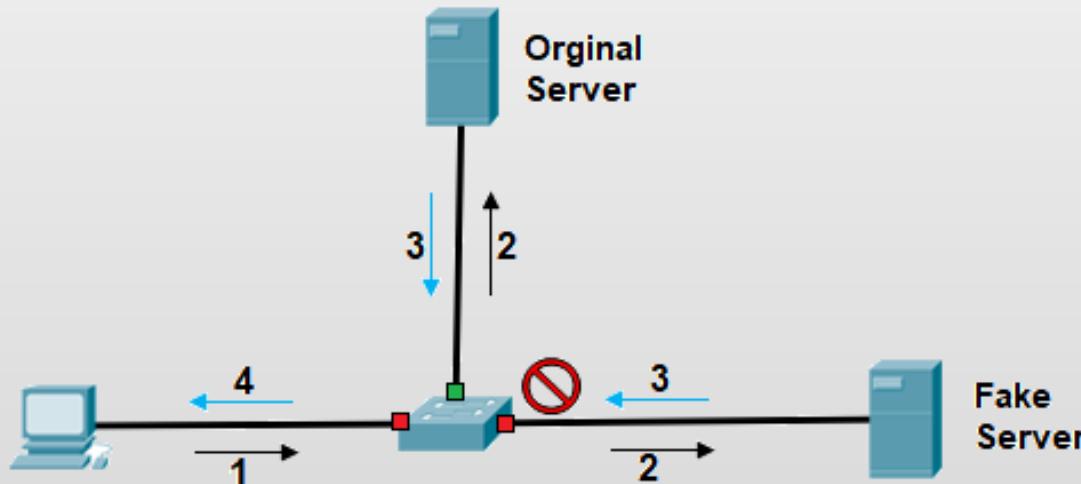
Legend

| 💻 DHCP Client | 🔌 L2 Switch | → DHCPDISCOVER Path | ■ Untrusted port |
| 🗄 DHCP Server | — Link | → DHCPOFFER Path | ■ Trusted port |

DHCP Snooping

- How could we do in legacy ROS?

/interface bridge filter
add **action=accept** chain=forward dst-port=67 ip-protocol=udp \
    mac-protocol=ip **out-interface=ether2** src-port=68
add **action=drop** chain=forward dst-port=67 ip-protocol=udp \
    mac-protocol=ip src-port=68
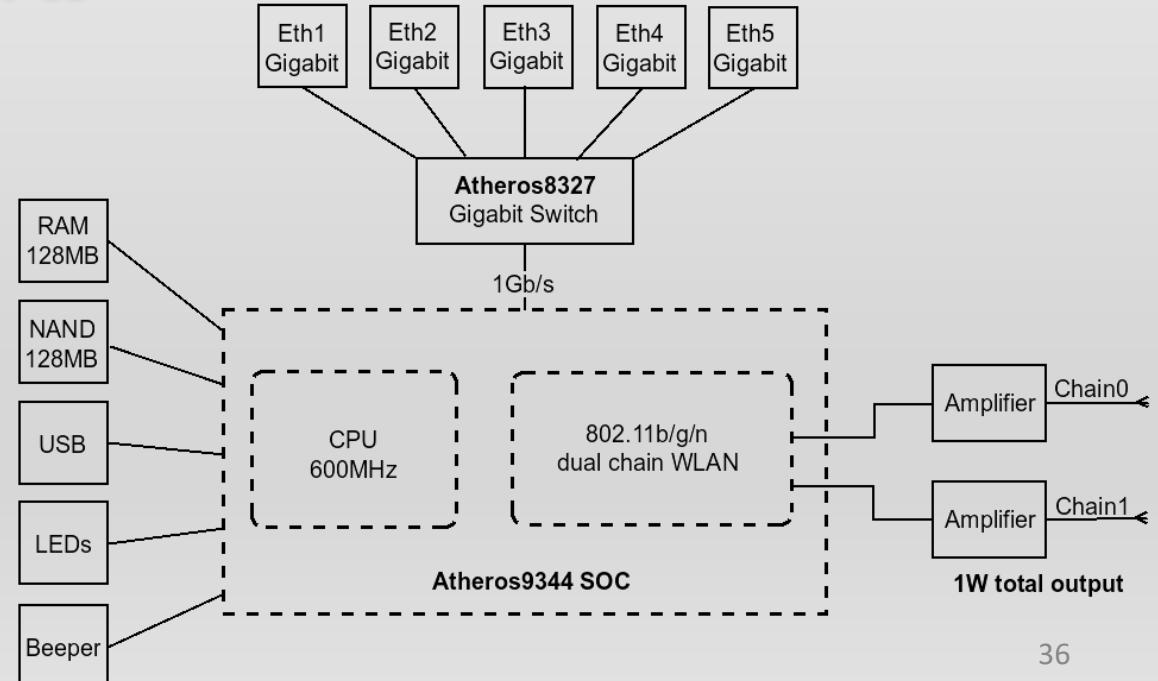
DHCP Snooping

- How can we do in latest ROS (v6.43+)?

/interface bridge
add dhcp-snooping=yes fast-forward=no name=bridge1

/interface bridge port
add bridge=bridge1 interface=ether2 trusted=yes
add bridge=bridge1 interface=ether3
add bridge=bridge1 interface=ether4

AccessPoint
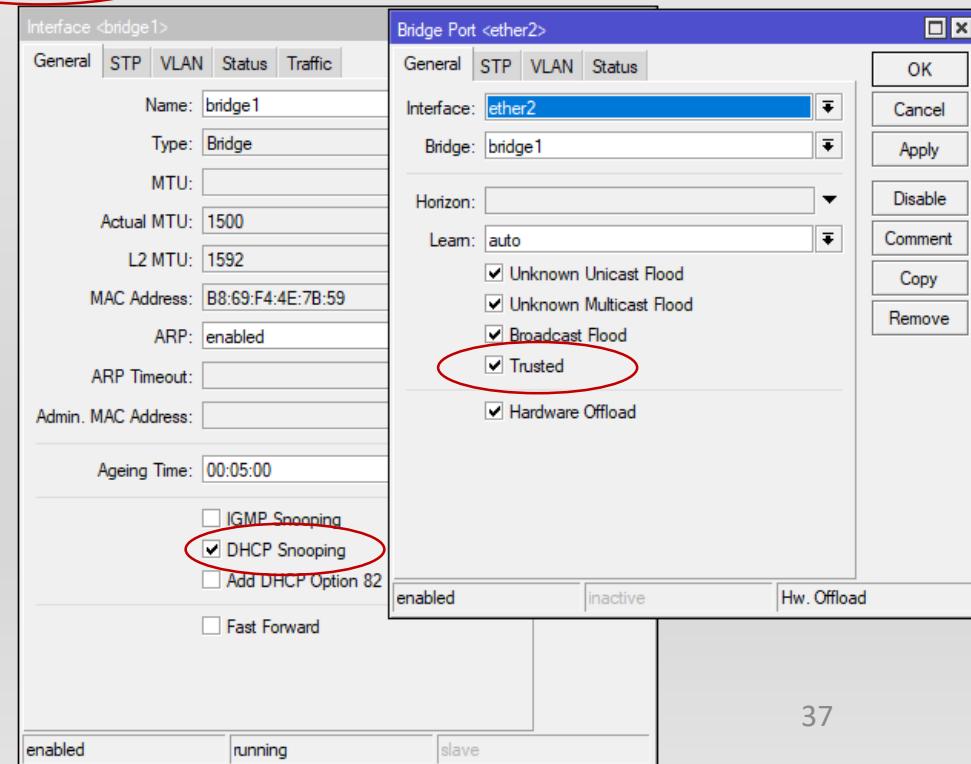
Conclusion

If you have a good device, the programming is easy!

Work smarter, not harder!

AccessPoint

Any other features?

MAC/Protocol based VLAN

Q-in-Q

Bonding ACL rules VLAN translation

MPLS HW Offload

Port Security STP/RSTP/MSTP

QoS (Port, MAC, VLAN, Protocol based)

Port Isolation Mirroring DHCP Option 82

IGMP snooping

Traffic Storm Control

Questions

Or you have a not public question, please send me an email
to major.peter@accesspoint.hu

AccessPoint

Thanks for your attention!

AccessPoint