Playing with RouterOS's VLANs

By Lorenzo Busatti

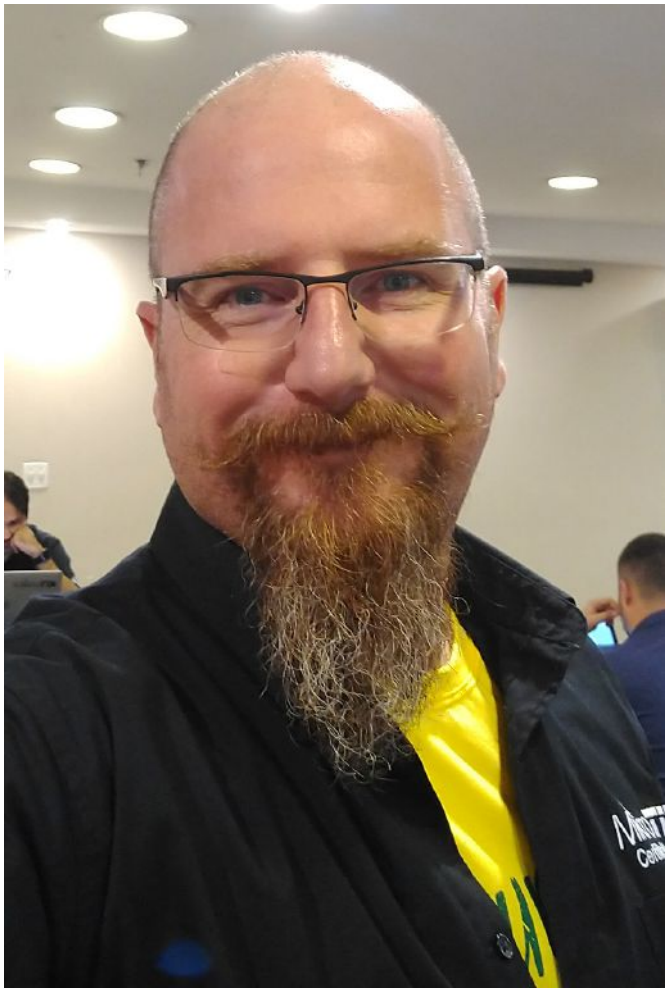
About me

Lorenzo Busatti - Grosseto – ITALY

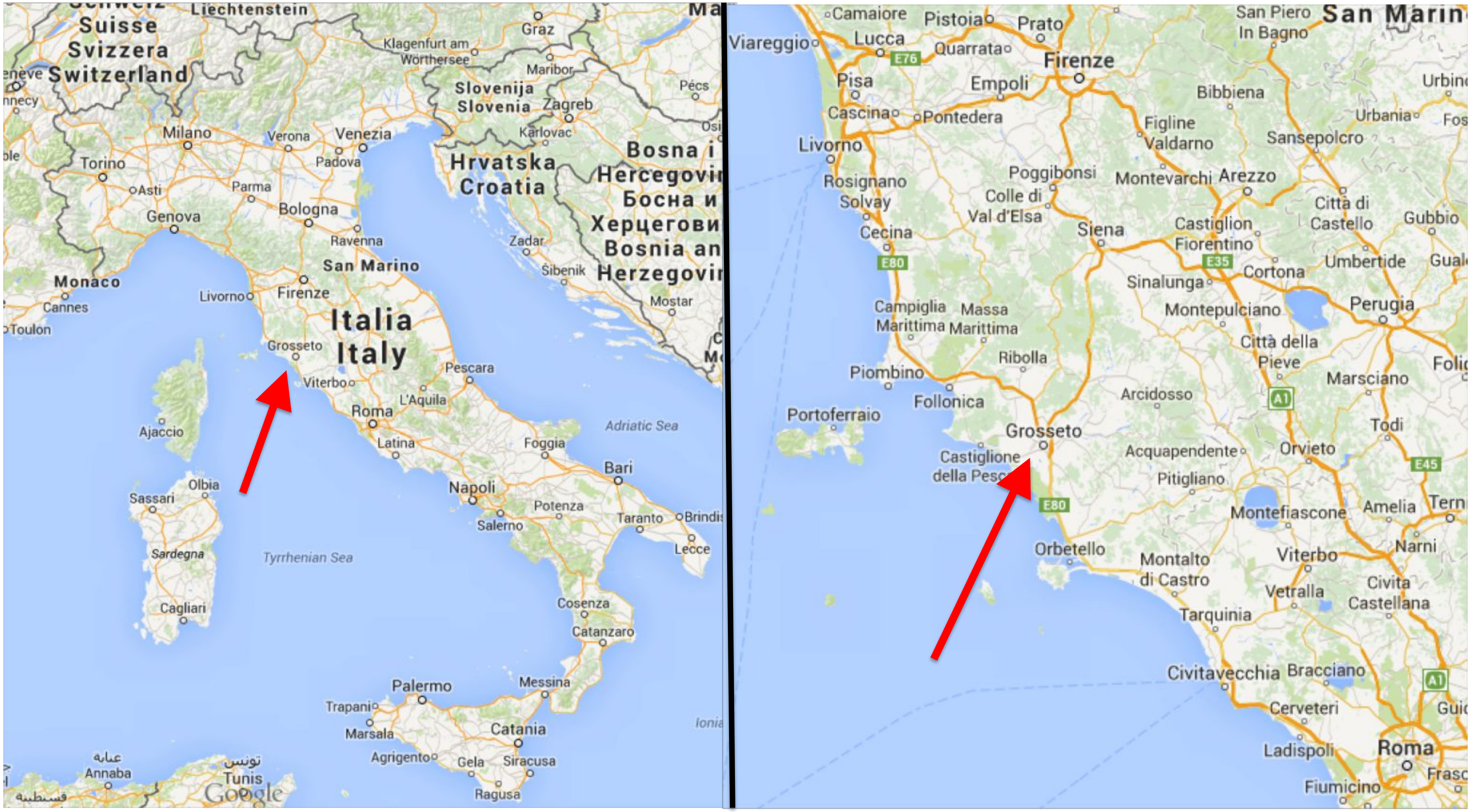
- Founder of Grifonline S.r.l. [ISP] 1997
- A user of MikroTik since 2006
- Founder of Linkwave [WISP] 2006
- MikroTik Trainer since 2010:

  MTCNA, MTCWE, MTCRE, MTCTCE, MTCUME,

  MTCINE, MTCIPv6E, MTCSE
- Member of RIPE, AMS-IX, MIX-IT
- Proud member of RoutedWorld.com



About me



Suisse
Svizzera
Switzerland
Liechtenstein
Graz
Klagenfurt am Wörthersee
Maribor
Slovenija
Slovenia
Zagreb
Pécs
Karlovac
Milano
Verona
Venezia
Padova
Torino
Asti
Parma
Genova
Bologna
Ravenna
Hrvatska
Croatia
Zadar
Šibenik
Bosna i Hercegovina
Босна и Херцеговина
Bosnia and Herzegovina
Mostar
San Marino
Monaco
Cannes
Toulon
Livorno
Firenze
Italia
Italy
Grosseto
Viterbo
Pescara
L'Aquila
Roma
Latina
Adriatic Sea
Foggia
Bari
Ajaccio
Olbia
Sassari
Napoli
Potenza
Salerno
Taranto
Brindisi
Lecce
Sardegna
Tyrrhenian Sea
Cagliari
Cosenza
Catanzaro
Palermo
Messina
Trapani
Marsala
Catania
Agrigento
Gela
Siracusa
Ragusa
Annaba
Tunis
Camaiore
Pistoia
Prato
Viareggio
Lucca
Quarrata
Firenze
San Piero In Bagno
San Marino
Pisa
Empoli
Bibbiena
Urbino
Cascina
Pontedera
Figline Valdarno
Urbania
Livorno
Sansepolcro
Poggibonsi
Montevarchi
Arezzo
Rosignano Solvay
Colle di Val d'Elsa
Città di Castello
Gubbio
Cecina
Siena
Castiglion Fiorentino
Cortona
Umbertide
Sinalunga
Campiglia Marittima
Massa Marittima
Montepulciano
Perugia
Città della Pieve
Ribolla
Piombino
Marsciano
Follonica
Arcidosso
Portoferraio
Todi
Grosseto
Castiglione della Pescaia
Acquapendente
Orvieto
Pitigliano
Montefiascone
Amelia
Terni
Orbetello
Montalto di Castro
Viterbo
Narni
Vetralla
Civita Castellana
Tarquinia
Civitavecchia
Bracciano
Cerveteri
Ladispoli
Roma
Fiumicino

About me

- Access Point Redundancy (2011 Las Vegas/US - 2012 Warsaw/PL)
- A redundant router for $79,99 (2012 Dubai/UAE)
- Peering the World (Fortaleza 2014/BR - 2015 Prague/CZ - 2016 Copenhagen/DK)
- The mAP and the mAP lite: The wireless swiss knife always in your pocket (2016 Dallas/US)
- UserManager: a free radius server for Wireless, Hotspot, PPP, users and DHCP. (2016 Copenhagen/DK)
- NetFlow: what happens in your network? (2016 Ljubljana/SL)
- What's new in wireless since RouterOS v6.37 (2017 Milan/IT)
- The evolution of the wireless package 6.40-6.42 (2018 Berlin/DE)
- Common MikroTik OSPF mistakes and how to avoid them (2019 Vienna/A)

About me

Founder (2016) of the

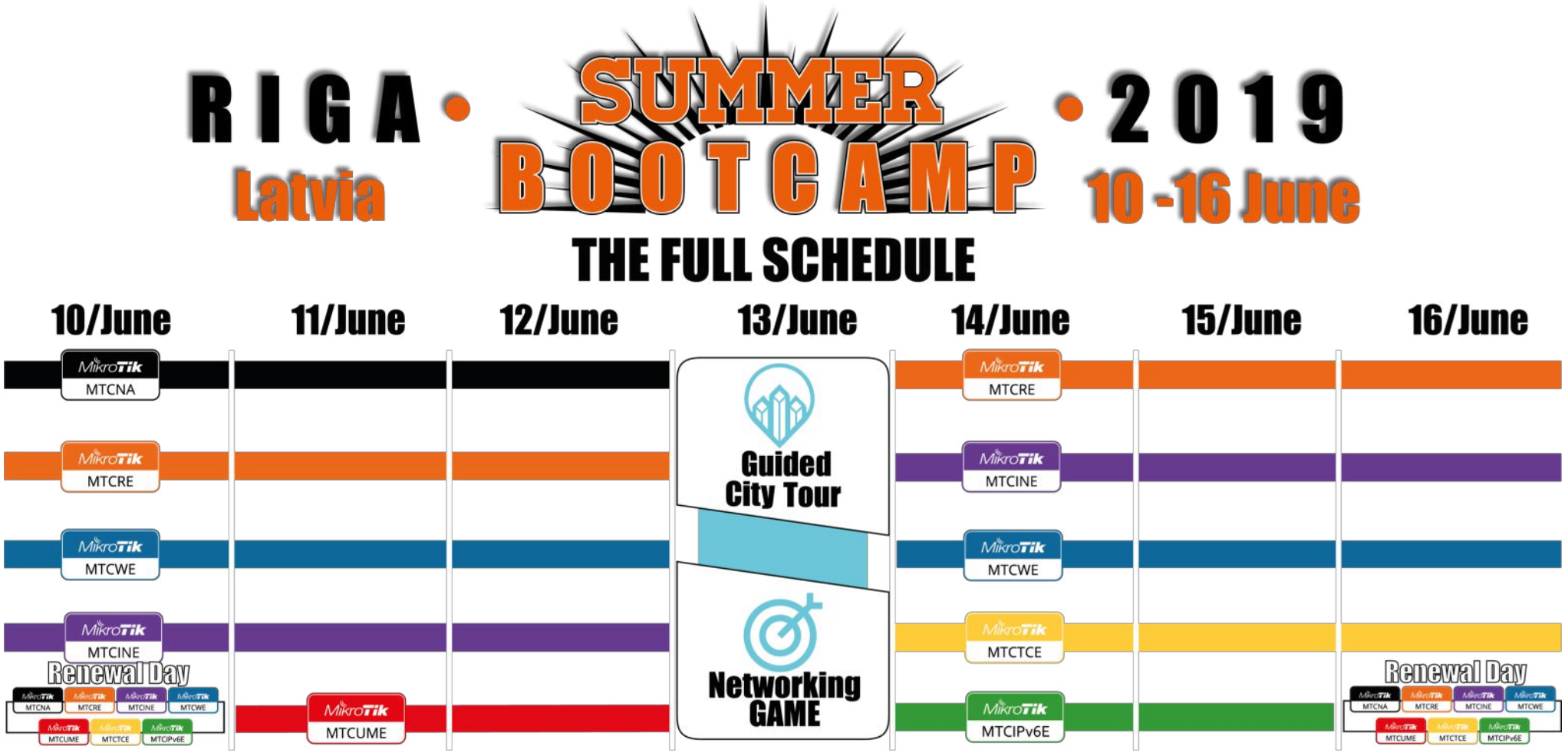
High Quality Training Classes

About me

One of the founders (2017) of the Riga Bootcamp!


Stub network Scenarios
Multihomed
Private ASN is used
Can be used:
As main/backup link
Load sharing
Upstream ISP advertises networks
Stub network has the same policy as ISP
Stub network Scenarios
Multihomed
Private ASN is used
Can be used:
As main/backup link
Load sharing
Upstream ISP advertises networks
Stub network has the same policy as ISP
37 / 171
MikroTik
CAMP

The Schedule



https://www.mikrotik.camp


MikroTik
CAMP
BOOTCAMP
MikroTik
CAMP
Riga • Bootcamp • 2018

Dedicated to Max

Abstract

RouterOS allows you to work with VLANs in different ways.

By software, by the switch chip and by the bridges .

This presentation will try to cover the pros/cons of these approaches and to show some tips.

About the VLANs

VLANs seem to be simple to deploy, but can actually be very complex.

Even simple operations can be tricky if you don't know where and how to put your hands.

While delivering many training courses I discovered that VLANs are often used improperly: that's why I made this presentation ☺

About the VLANs

The target of this presentation is to understand how you can made the VLANs in these 3 places and the differences between them.

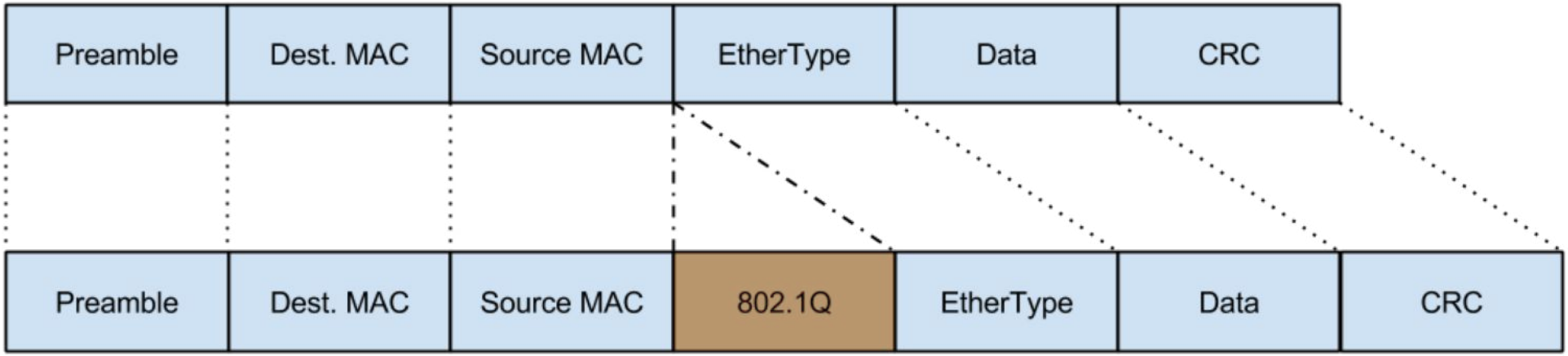
Is not a step-by-step tutorial about all the VLANs things.

About the VLANs

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated at the data link layer (OSI layer 2), invented by Dr. W. David Sincoskie and then described in the first edition of the IEEE 802.1Q standard in the 2003.

About the VLANs

They are made adding a VLAN ID header [0-4095] into Ethernet header:



A VLAN is a VPN (without authentication and without encryption).

I'm used to say that's for free ☺

About the VLANs

The definitions of the "port role" are not uniformed as standard, they are usually different between vendors.

But the following ones are almost universally adopted by technicians.

VLAN Terms

Tagged: All packets forwarded by the interface contain VLAN information.

Untagged: Packets forwarded by the interface are untagged.

Access port: Belong to one VLAN – Port is untagged

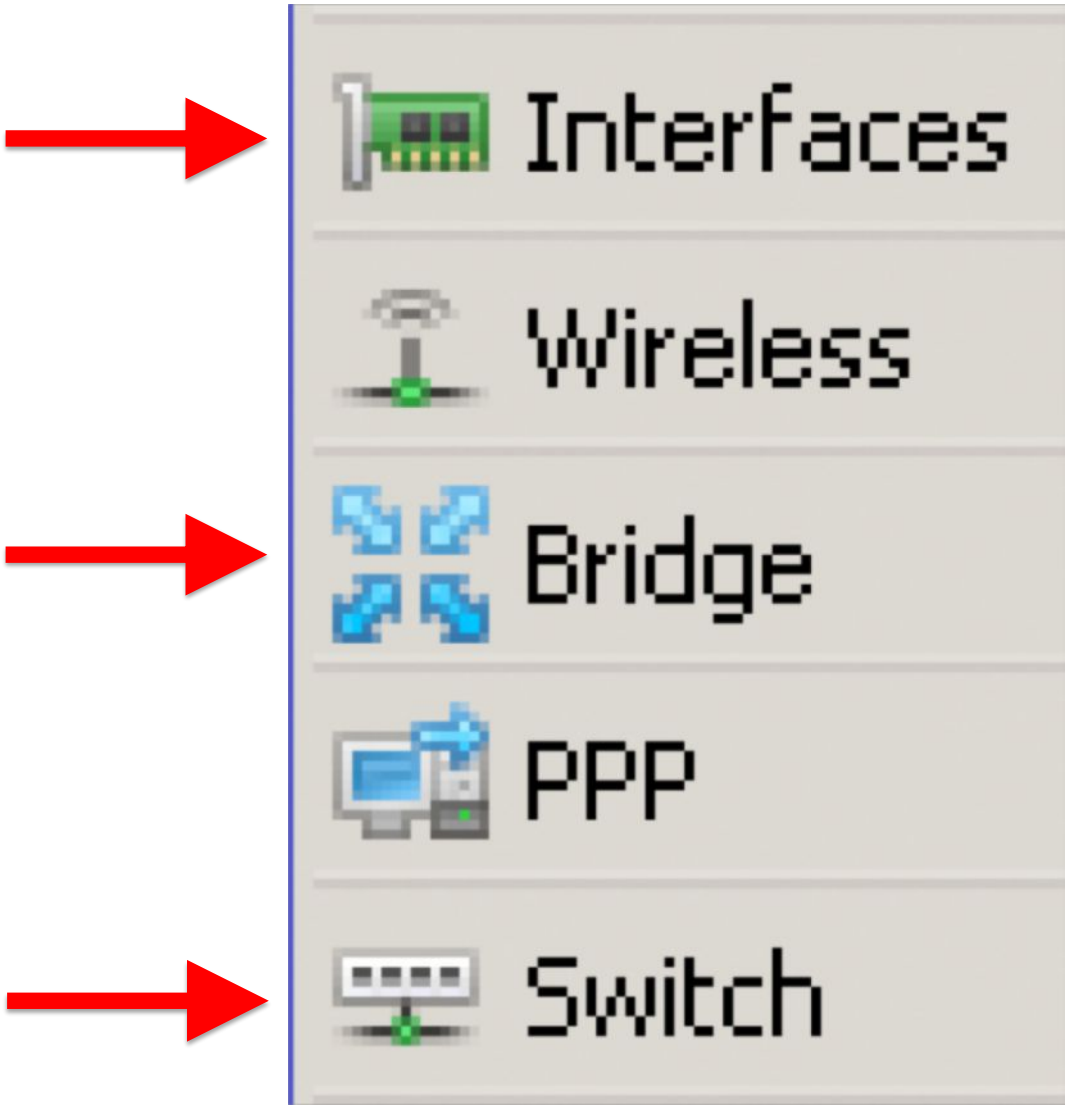
Hybrid port: Multiple VLANs can be untagged and tagged

Trunk port: Carry multiple VLANs on a single physical link

The VLANs in RouterOS

The VLANs in RouterOS

Today is possible to manage the VLANs in RouterOS in 3 different main places:



The VLANs in RouterOS

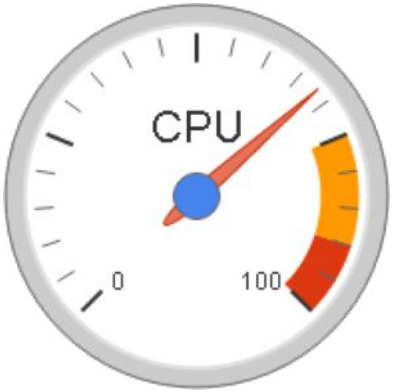
- They are managed in the same manner?
- They can be setup using the same commands?
- They have the same performances?

No, **No** and **No**.

So let me show you the differences between them and you will enjoy the VLANs under RouterOS ☺

The software VLANs

These are **software** VLANs, I mean that the traffic will affect and will be affected by the **CPU**.

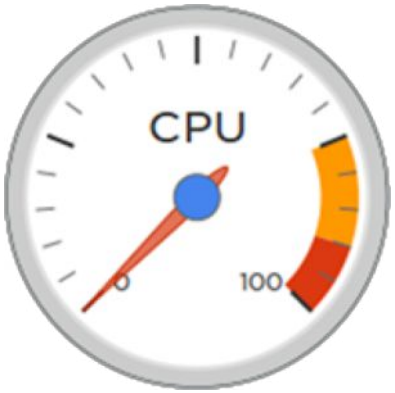


They are available on **any** the RouterOS devices.

The hardware VLANs

These are **hardware** VLANs,

The traffic will be managed by the switch chip at wire speed and will **not** affect the CPU.

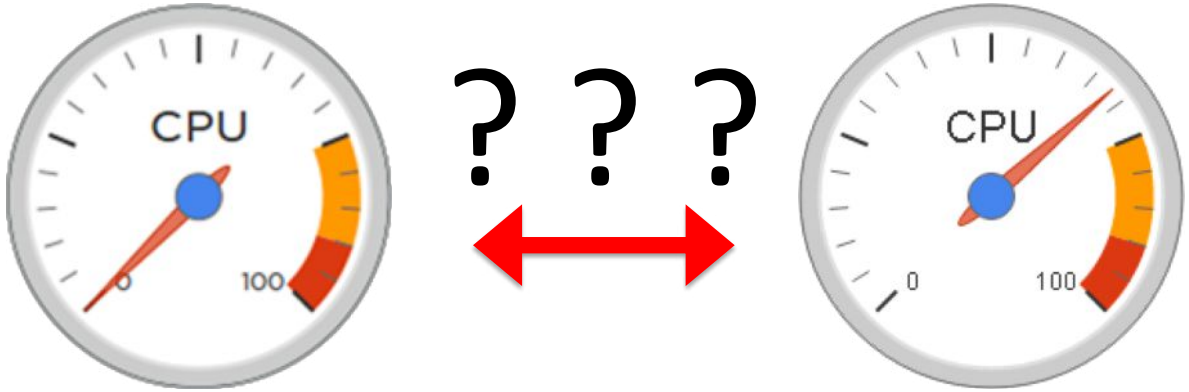


They are only available on the RouterOS devices with the **switch chip**.

The VLANs in the Bridge

The VLANs managed in the bridge can be **software or hardware**, depending of the presence of the switch chip and how is configured!

Your knowledge will determine if the CPU will be affected or not!



The VLANs in RouterOS

We have different "places" to manage them, and with different performances, due the evolution of RouterOS and the MikroTik hardware devices in the last decade.

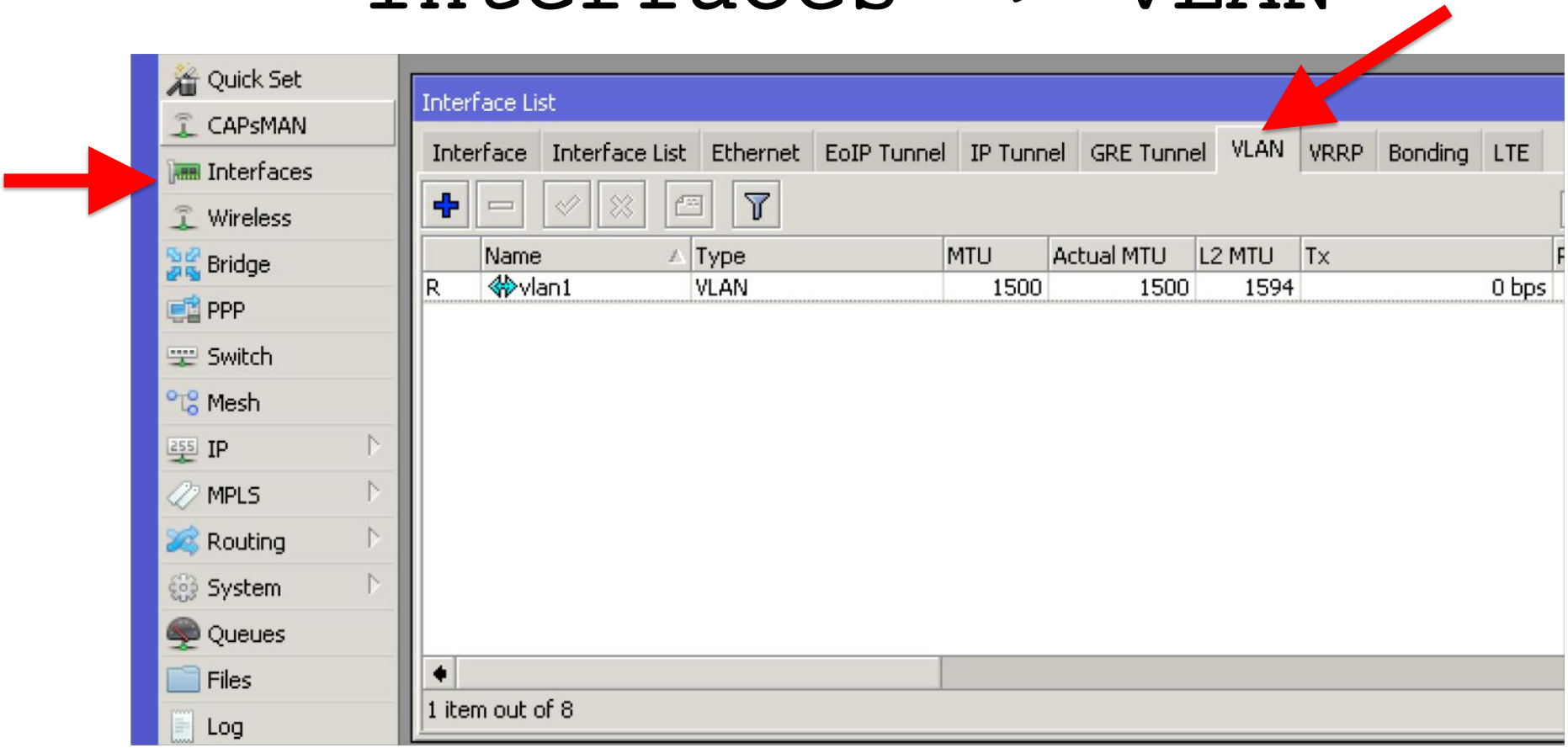
That's why is up to you to know the differences.

The software VLANs

The software VLANs

Can be created and managed from

`Interfaces -> VLAN`

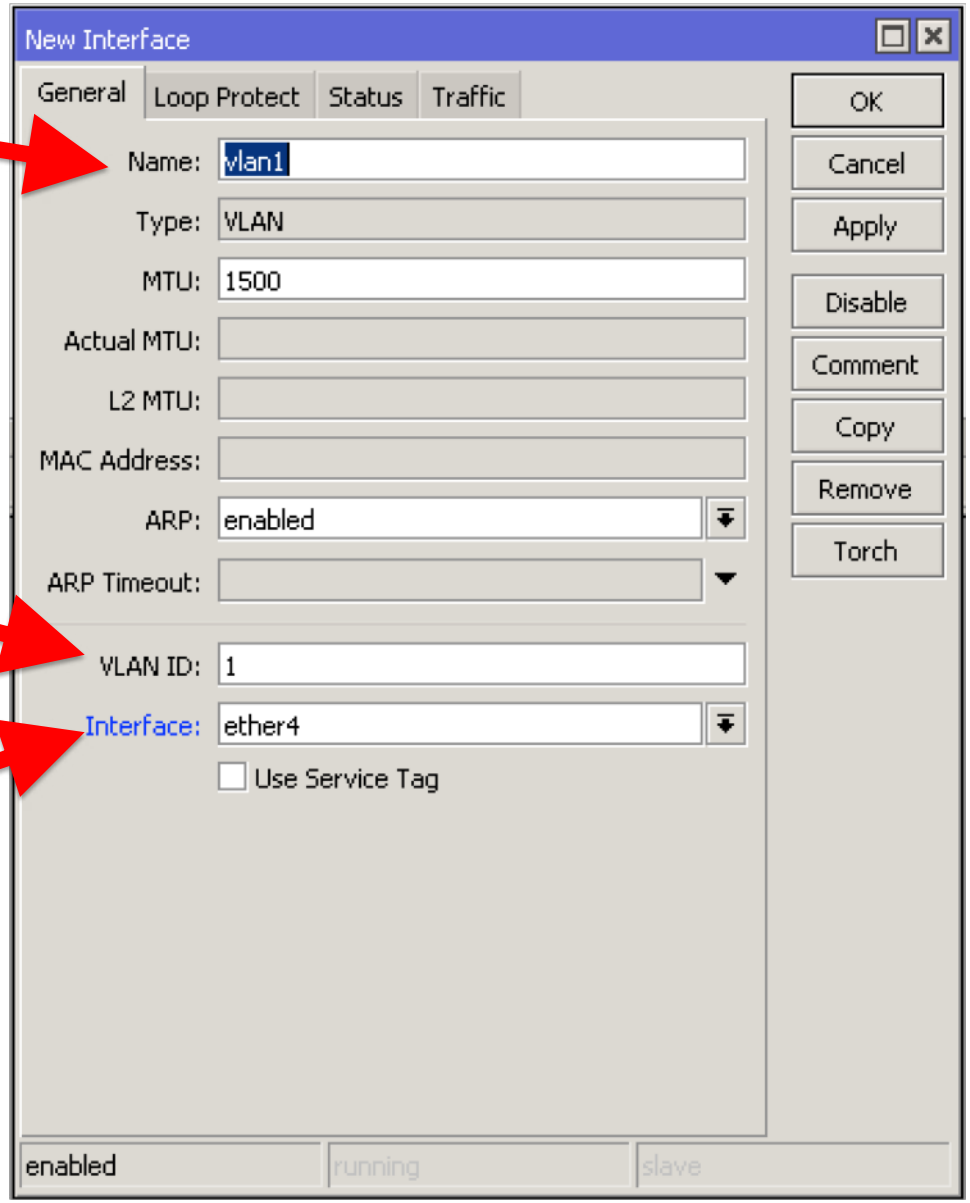


The software VLANs

Name of the interface

The VLAN ID

The L2 interface where to ADD the tag (at egress) or check and remove it (at ingress)

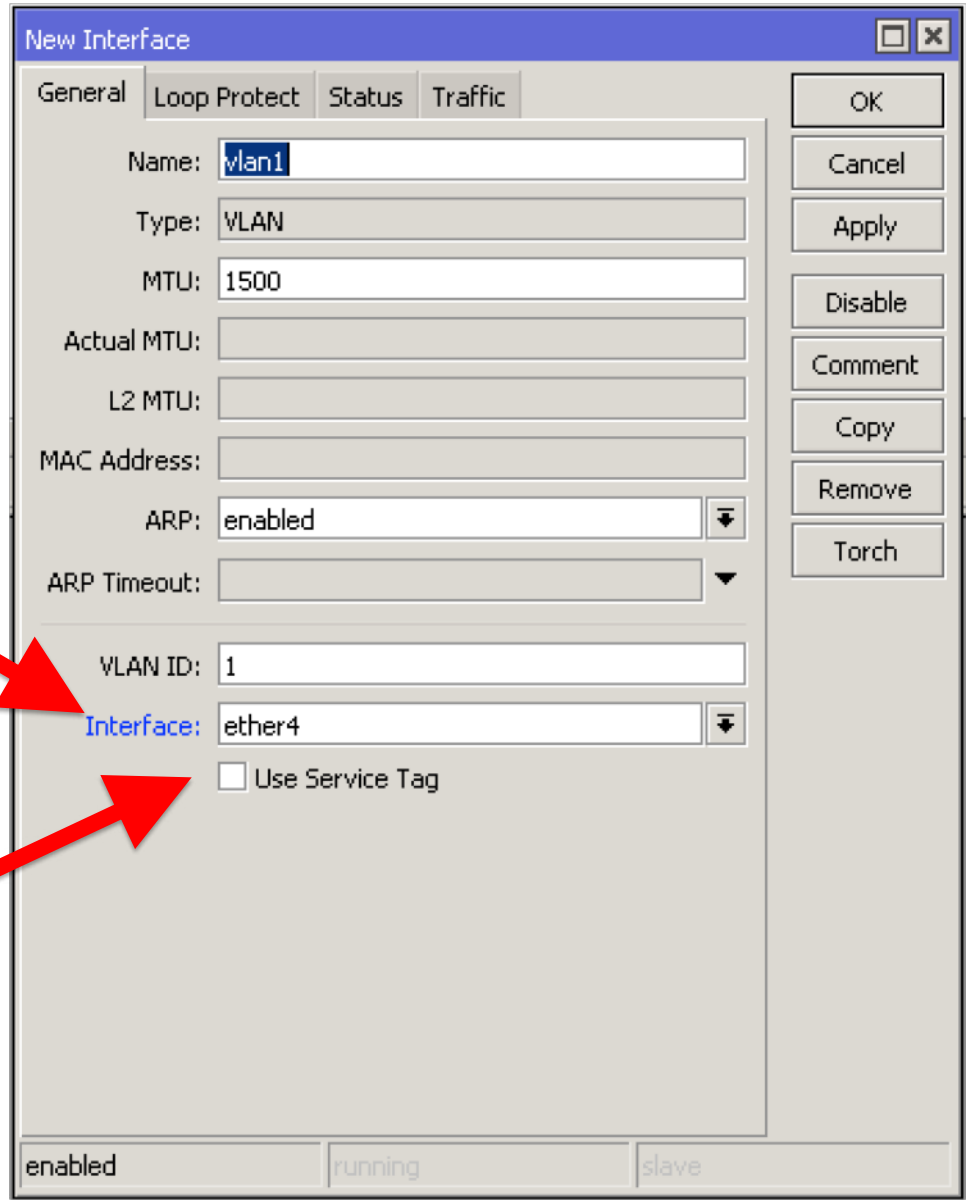


The software VLANs

Can be ANY L2 interface.

But in case it's a port of a bridge, use the bridge interface!

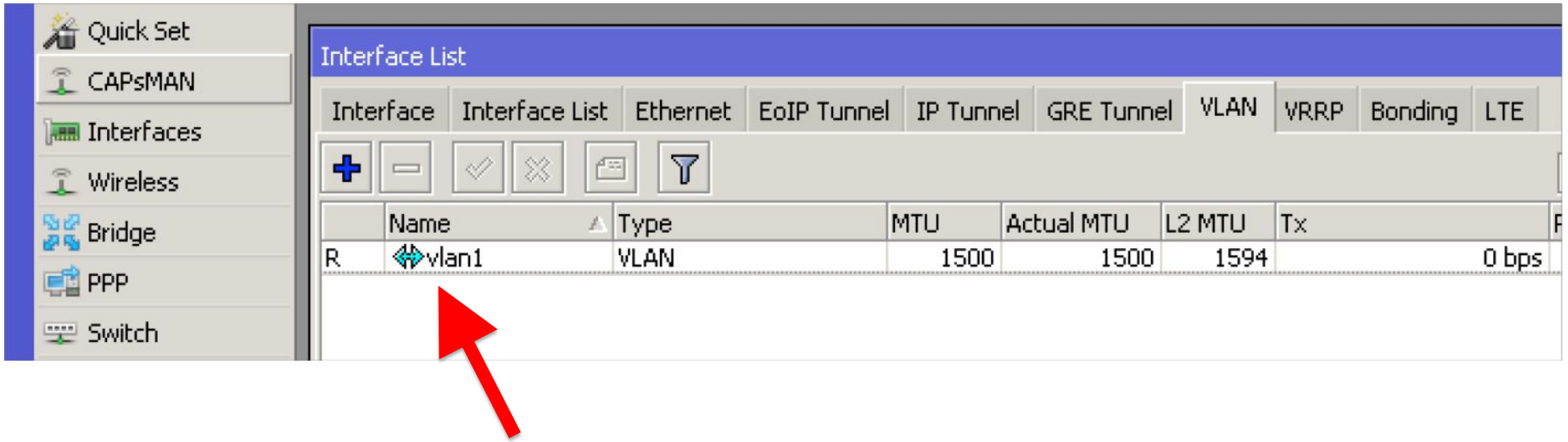
For using the 802.1ad compatible Service Tag, useful with some vendors.



The software VLANs

Useful to send some kind of traffic to the cpu, to run a service in a VLAN (dhcp, PPP, etc.).

Will appear as a "virtual interface".



The software VLANs

With the software VLANs you can TAG/UNTAG a traffic from any L2 interface.

Pros: can be used on **any device** (with or without the switch chip) even on the CHRs.

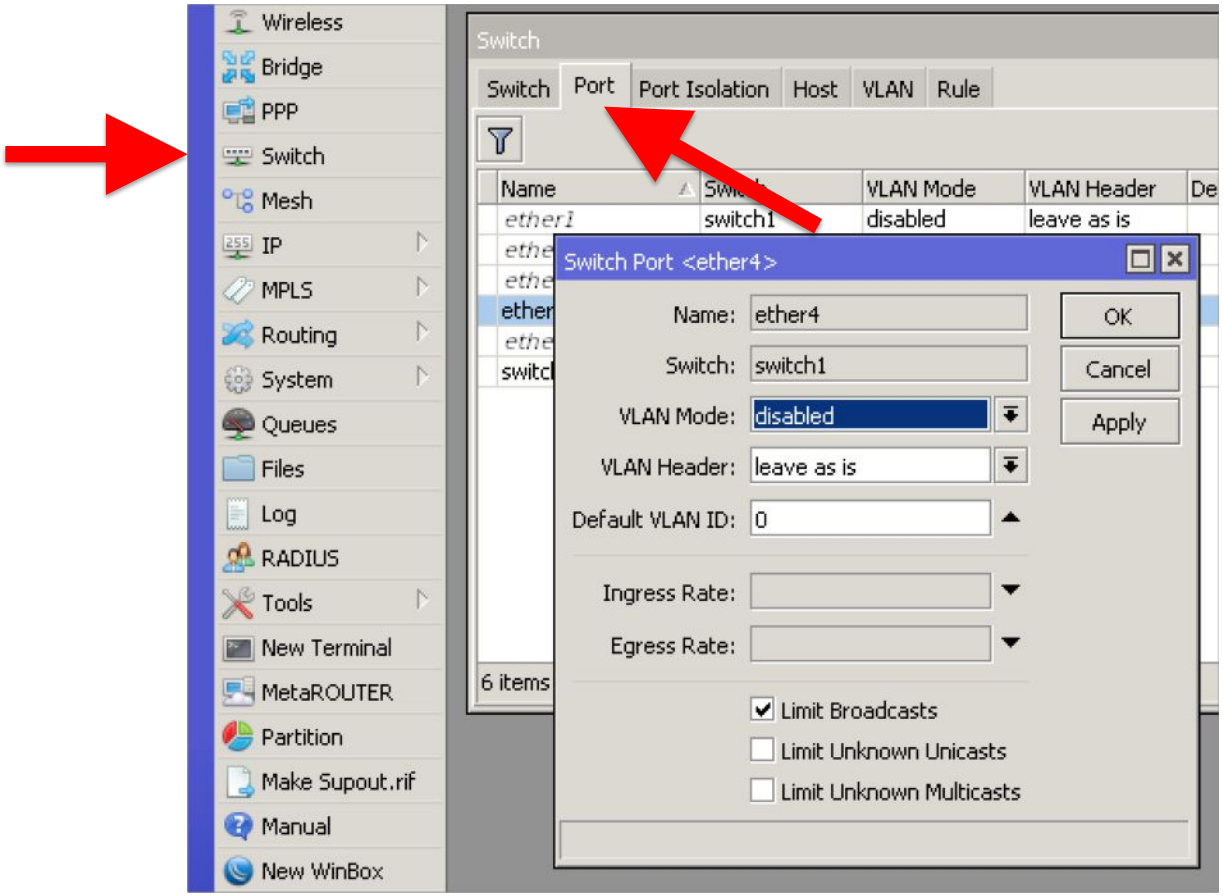
Cons: will use the **CPU**

The hardware VLANs

The hardware VLANs

Can be created and managed from

`Switch -> Port / VLAN / Rule`



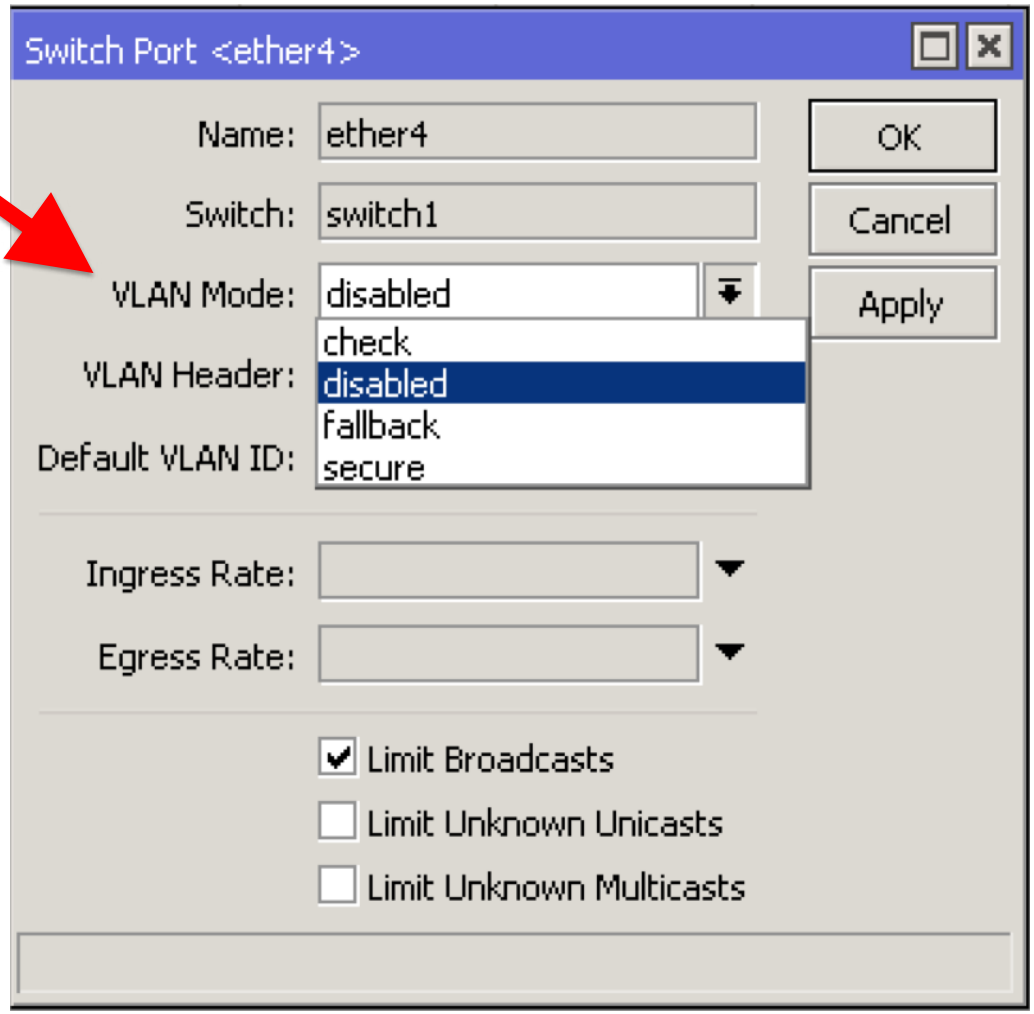
The hardware VLANs

For each ethernet port you can setup the VLAN Mode **for ingress traffic** as:

`Disabled`: will not check VLANs

`fallback`: checks for tagged traffic, forwards all untagged traffic.

`Check`/**`secure`**: checks for tagged traffic, drops all untagged traffic



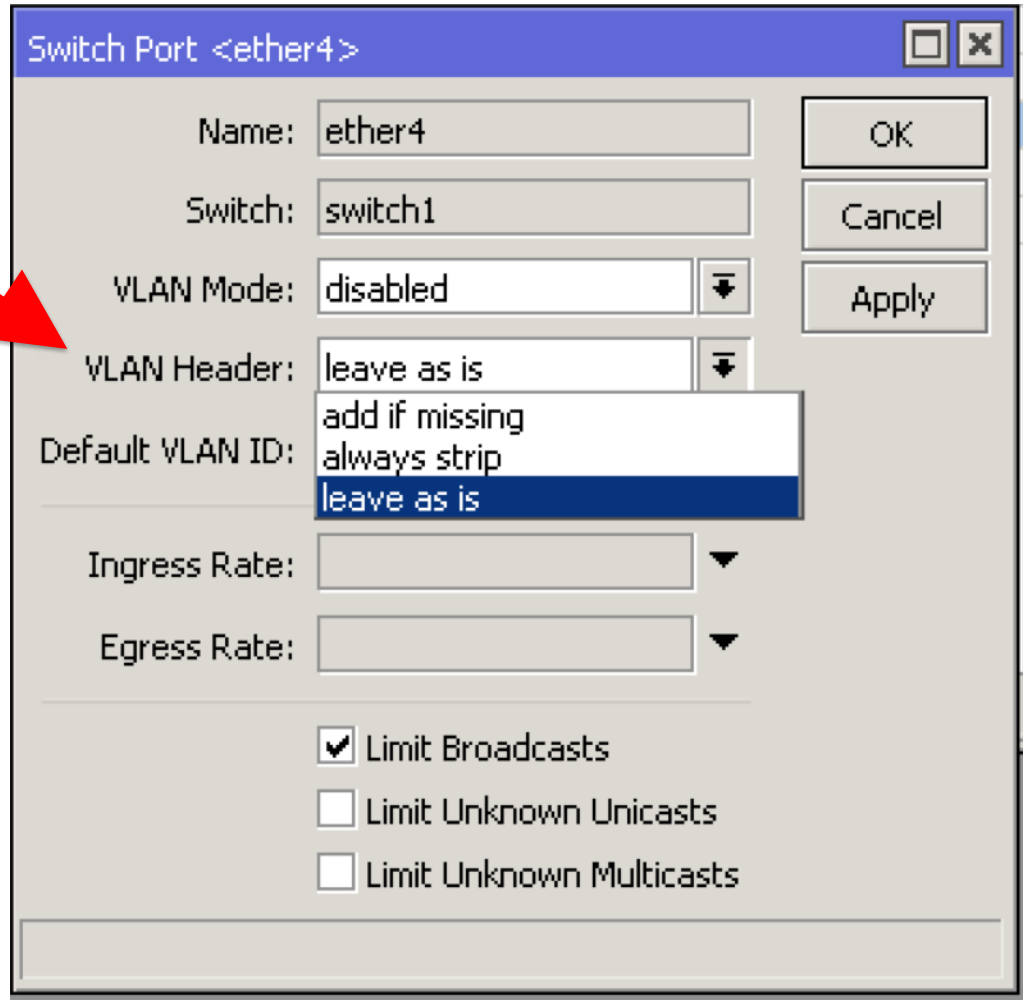
The hardware VLANs

The VLAN Header sets action which is performed on the port for **egress traffic** as:

`add-if-missing`: adds a VLAN tag on egress traffic. *Should be used for trunk ports.*

`always-strip`: removes a VLAN tag on egress traffic. *Should be used for access ports.*

`leave-as-is`: does not add nor removes a VLAN tag on egress traffic. *Should be used for hybrid ports.*

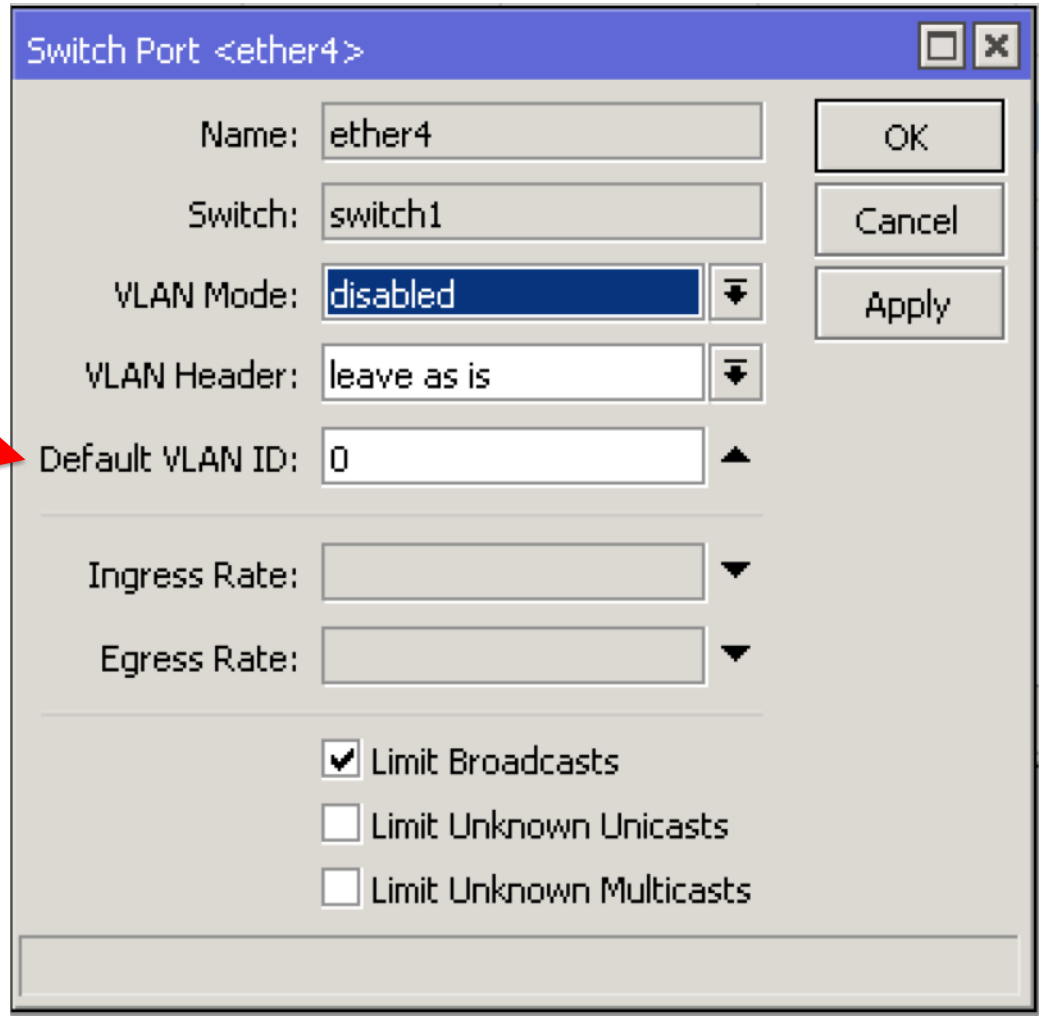


The hardware VLANs

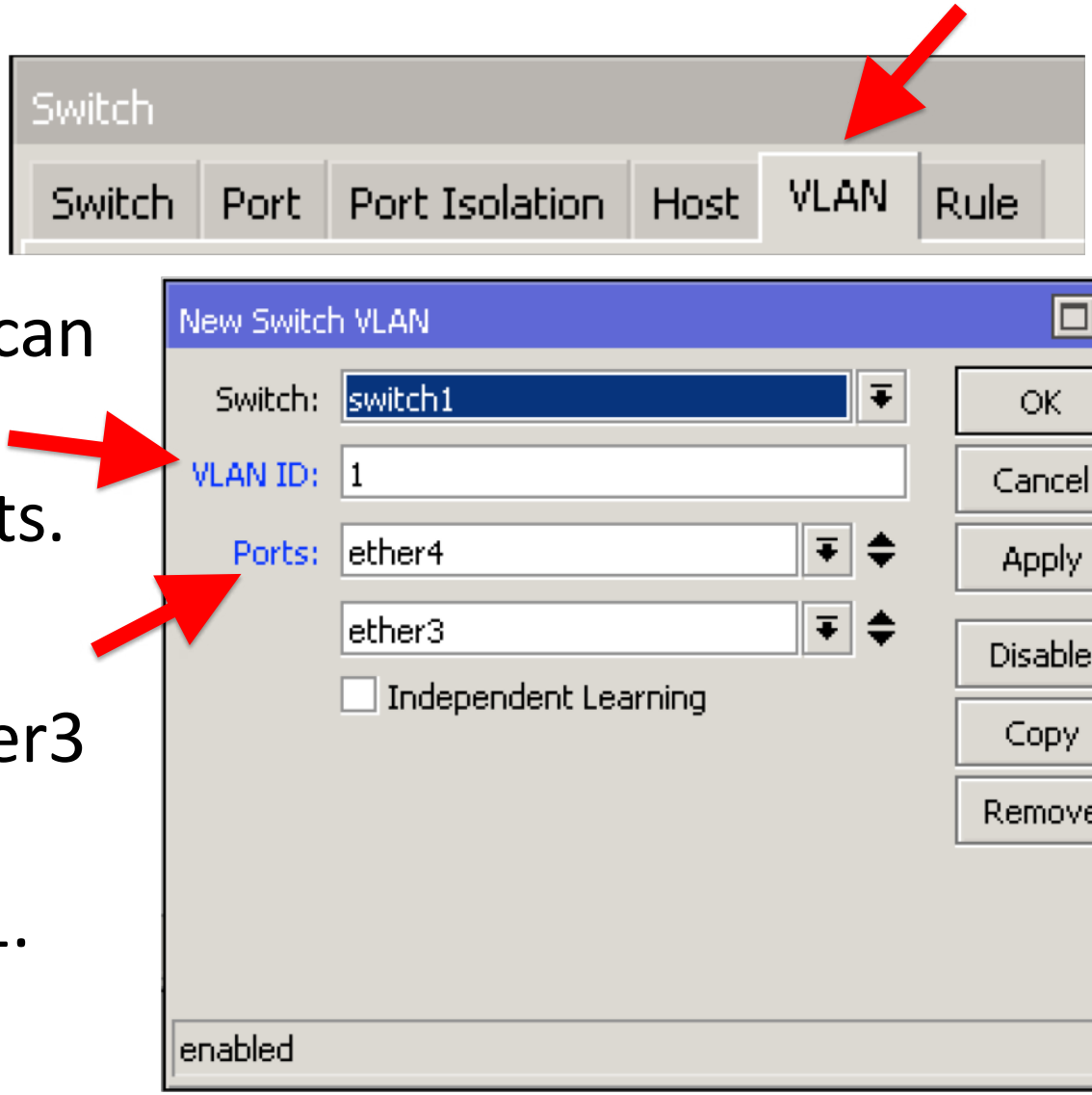
The default VLAN ID is used when

`vlan-header=always-strip`

and for hybrid ports to tag untagged traffic.



The hardware VLANs

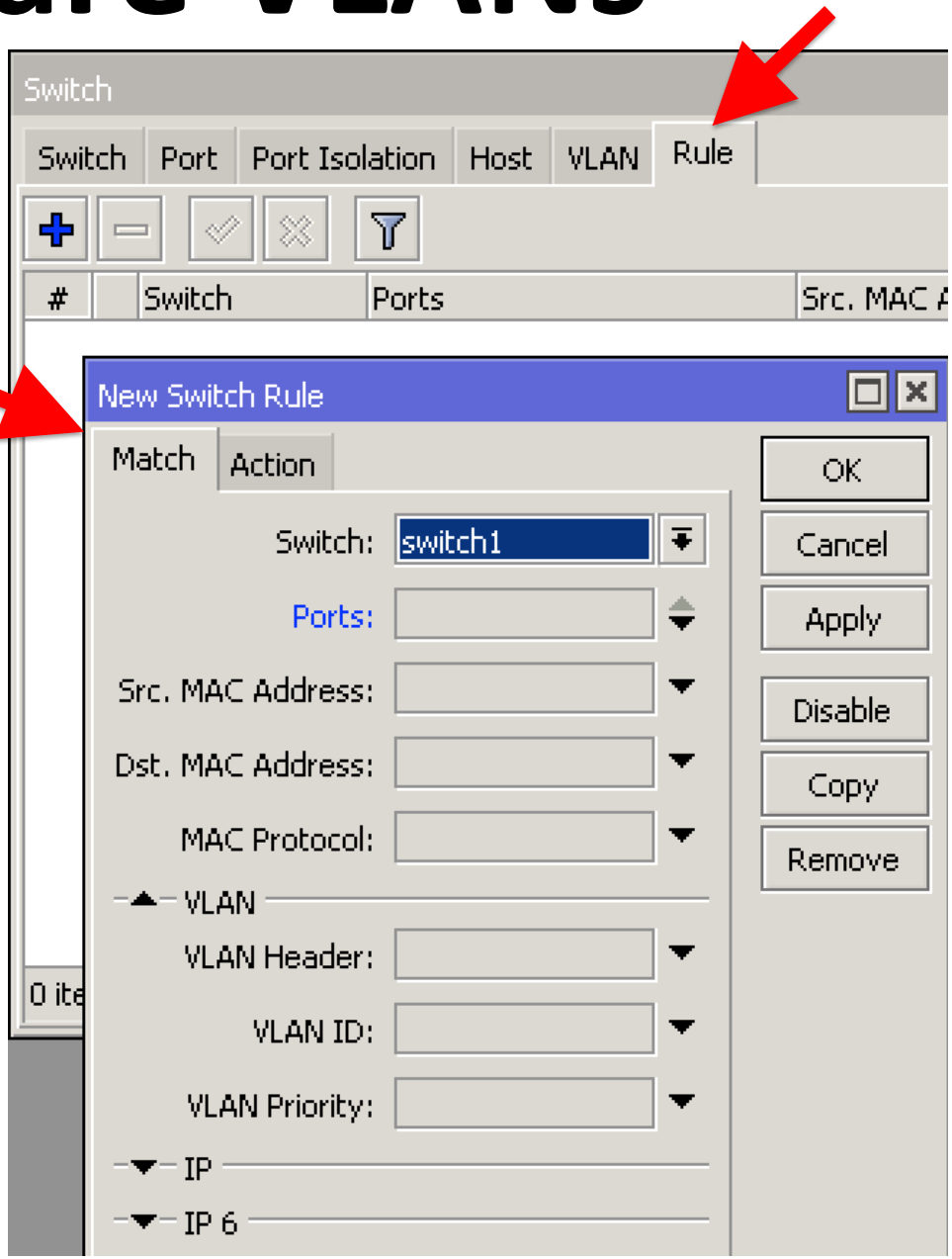


From the VLAN tab we can define the VLAN membership of the ports.

In this example the ether3 and the ether4 are members of the VLAN 1.

The hardware VLANs

Depending the chip switch functionality will be possible to create VLANs based rules also.



The hardware VLANs

Using the switch chip you can create almost any kind of port with the VLANs. Useful to manage VLANs "like in a switch".

Pros: will not use the CPU, able to provide wire speed

Cons: available only on devices provided with a chip switch, different functions depending the **chip model (check the specs before buy!)**.

The VLANs in the Bridge

The VLANs in the Bridge

Since version 6.41 RouterOS had major changes to the bridge configuration.

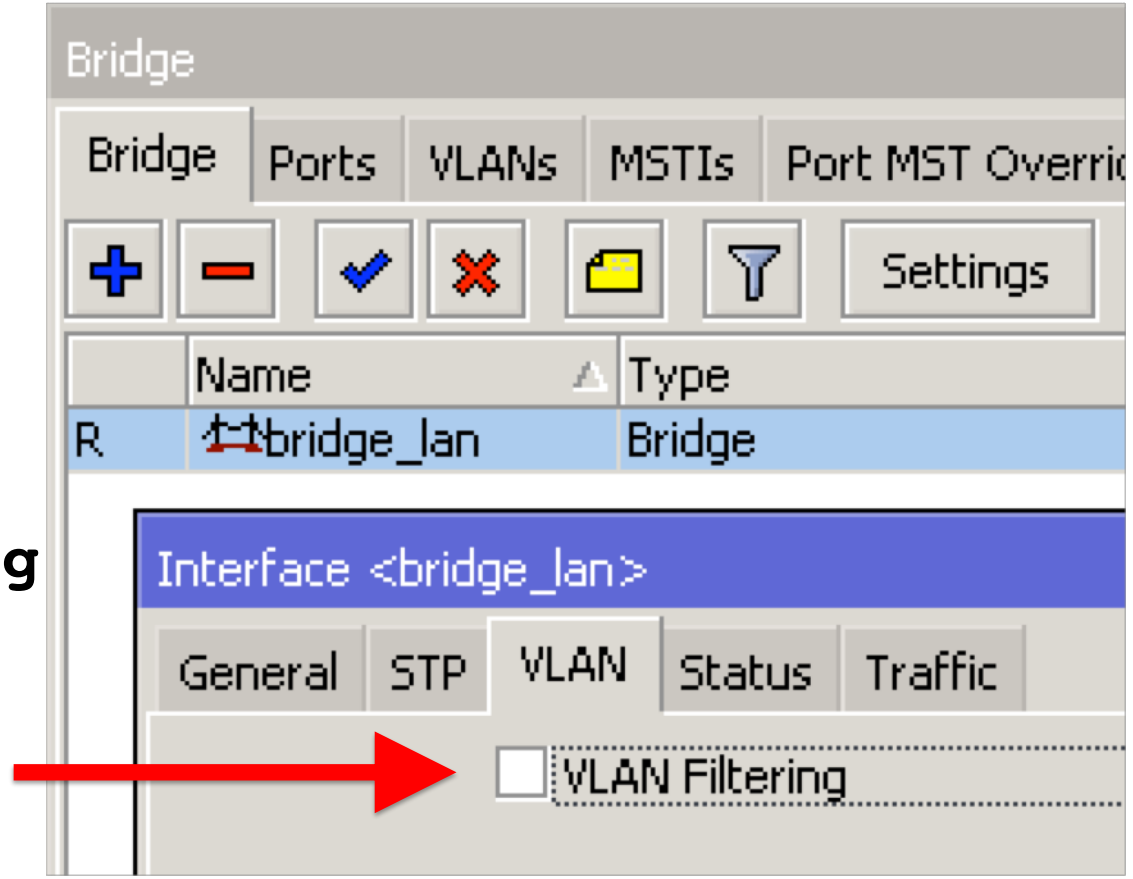
Today the bridge must be used for setting up basic switching functions (if your hardware have a chip switch).

The VLANs in the Bridge

The main VLAN setting is vlan-filtering which globally controls vlan-awareness and VLAN tag processing in the bridge.

If **`vlan-filtering=no`**, bridge ignores VLAN tags and cannot modify VLAN tags of packets.

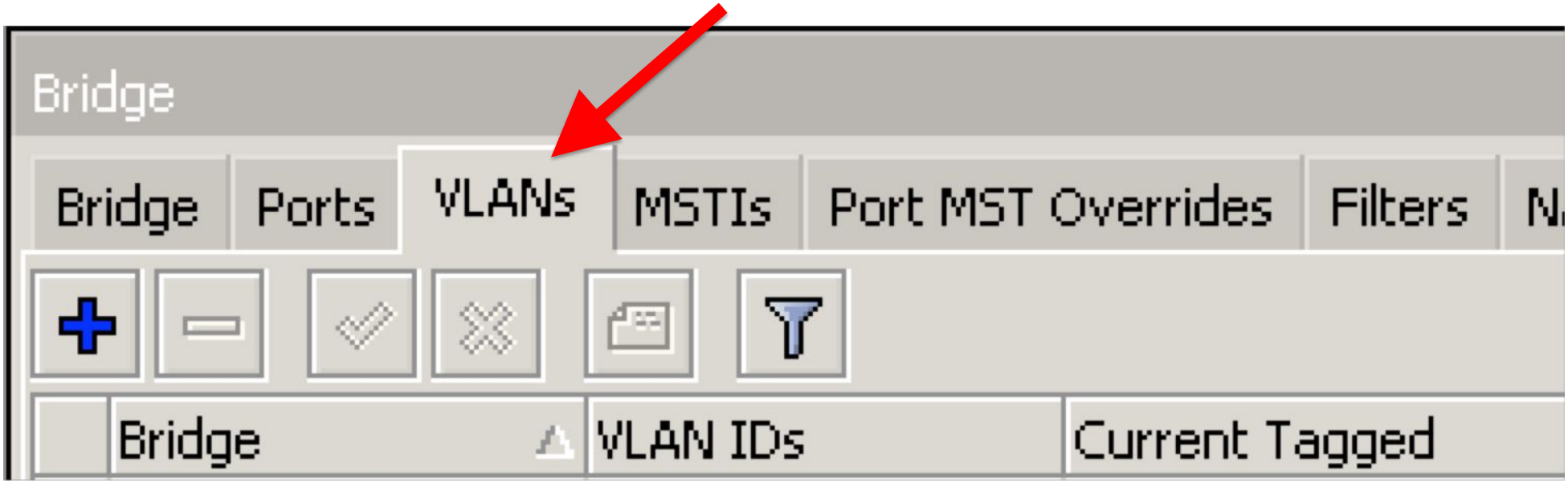
Turning on `vlan-filtering` enables all bridge VLAN related functionality.



The VLANs in the Bridge

Can be created and managed from

`Bridge -> VLANs`

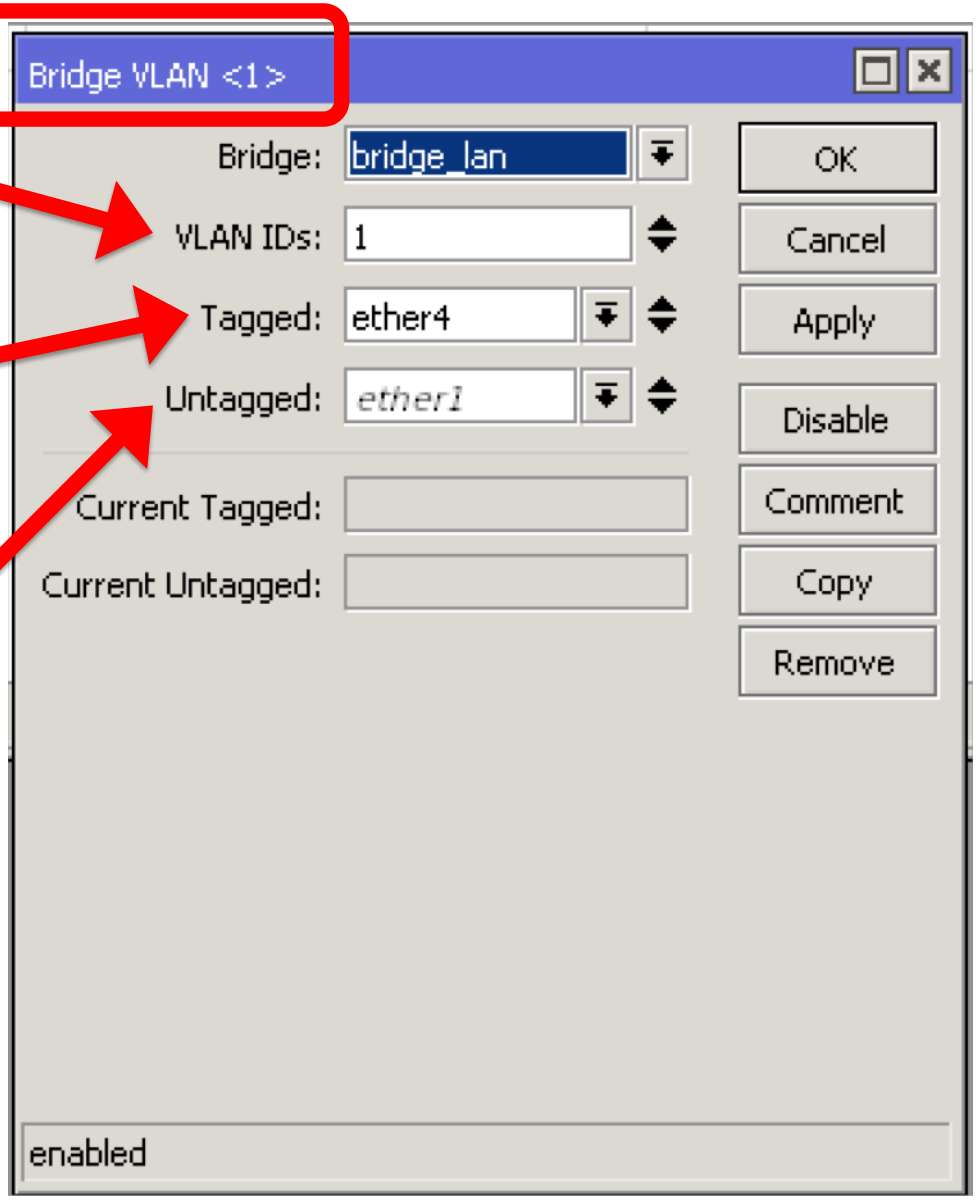


The VLANs in the Bridge

The list of VLAN IDs

Interfaces with a VLAN tag adding action in egress

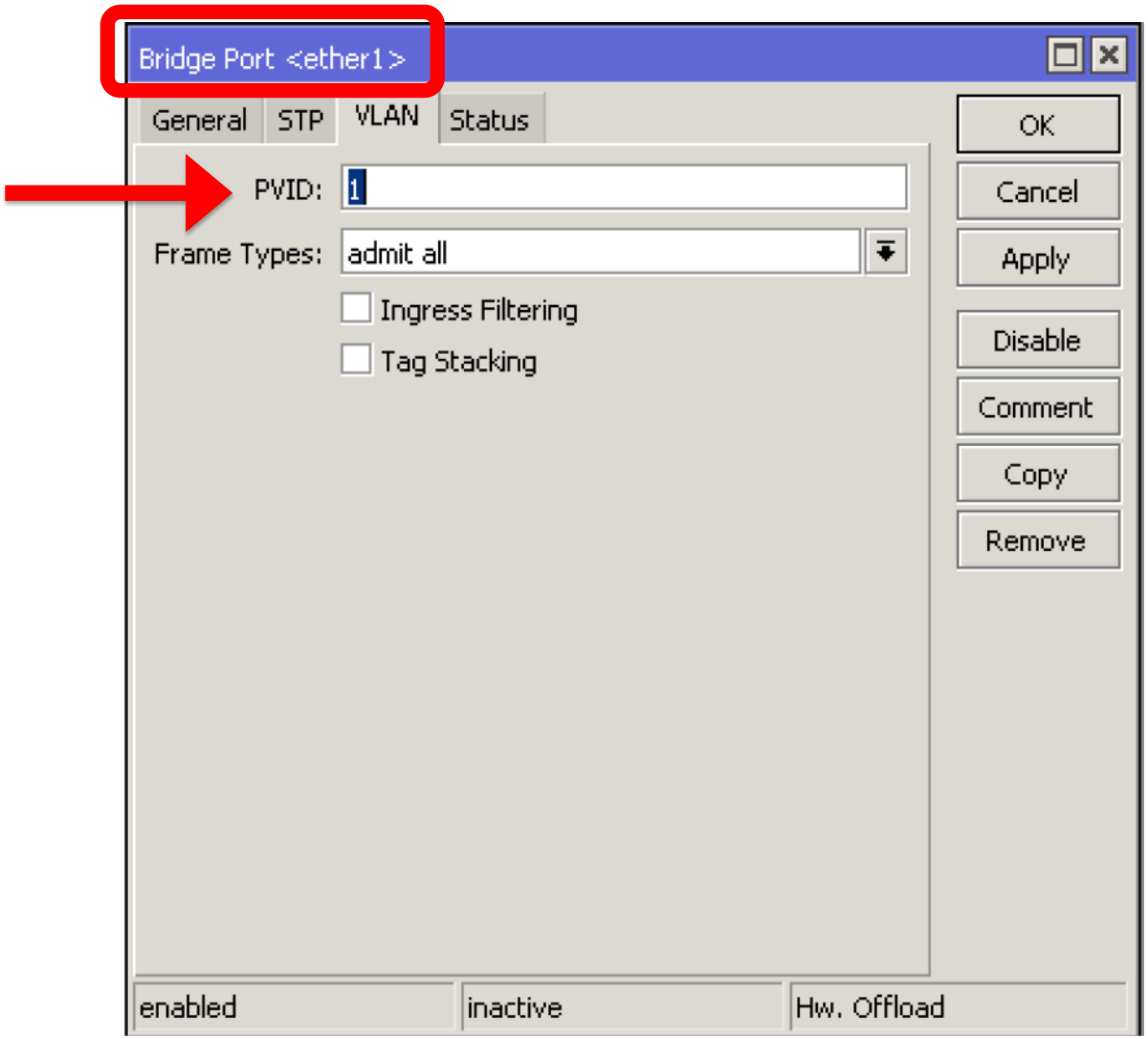
Interfaces with a VLAN tag removing action in egress



The VLANs in the Bridge

Port VLAN ID (**pvid**):

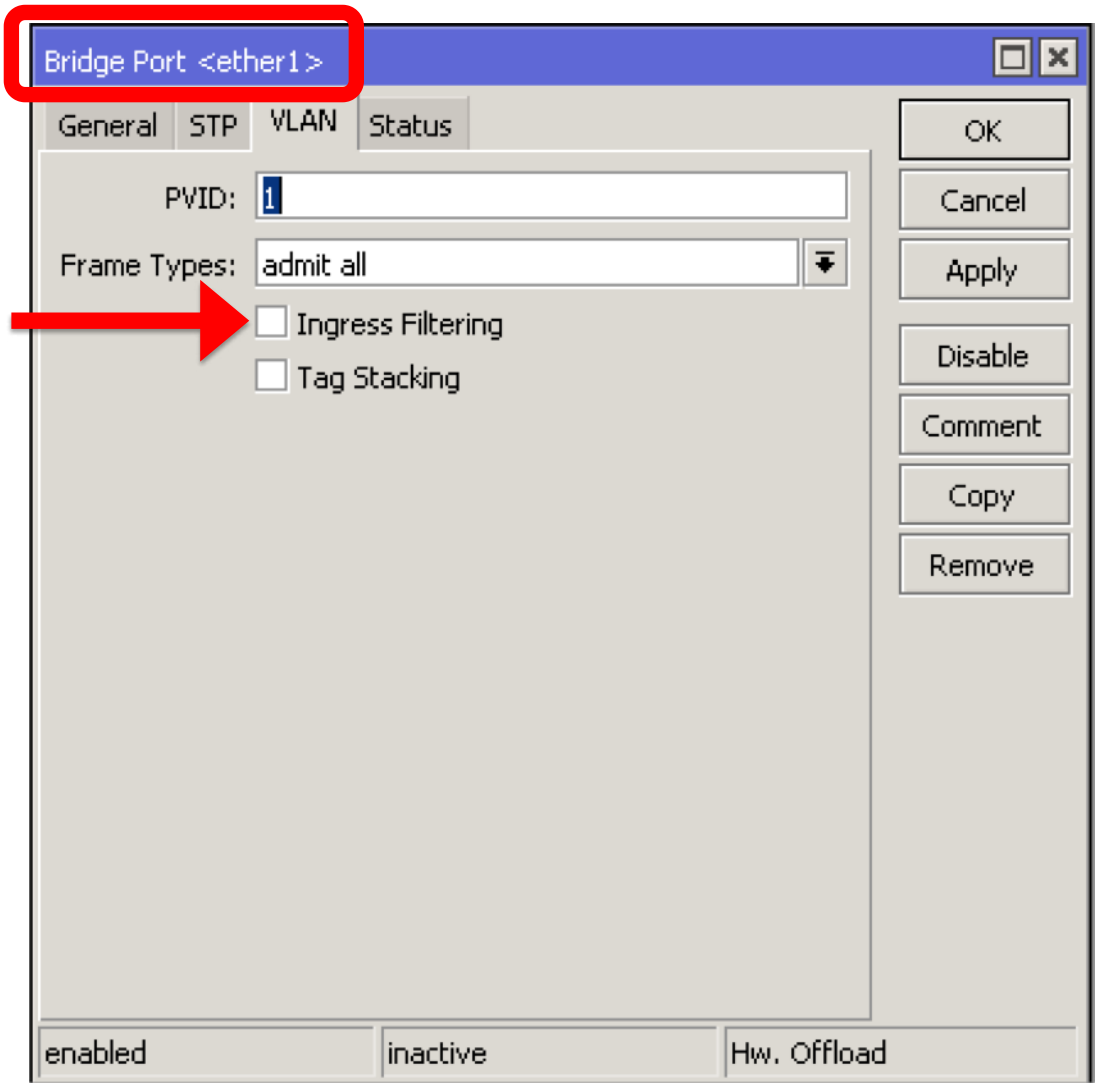
specifies which VLAN the **untagged ingress** traffic is assigned to.



The VLANs in the Bridge

Ingress Filtering:

Will check if the **ingress port** is a member of the received VLAN ID in the bridge VLAN table.

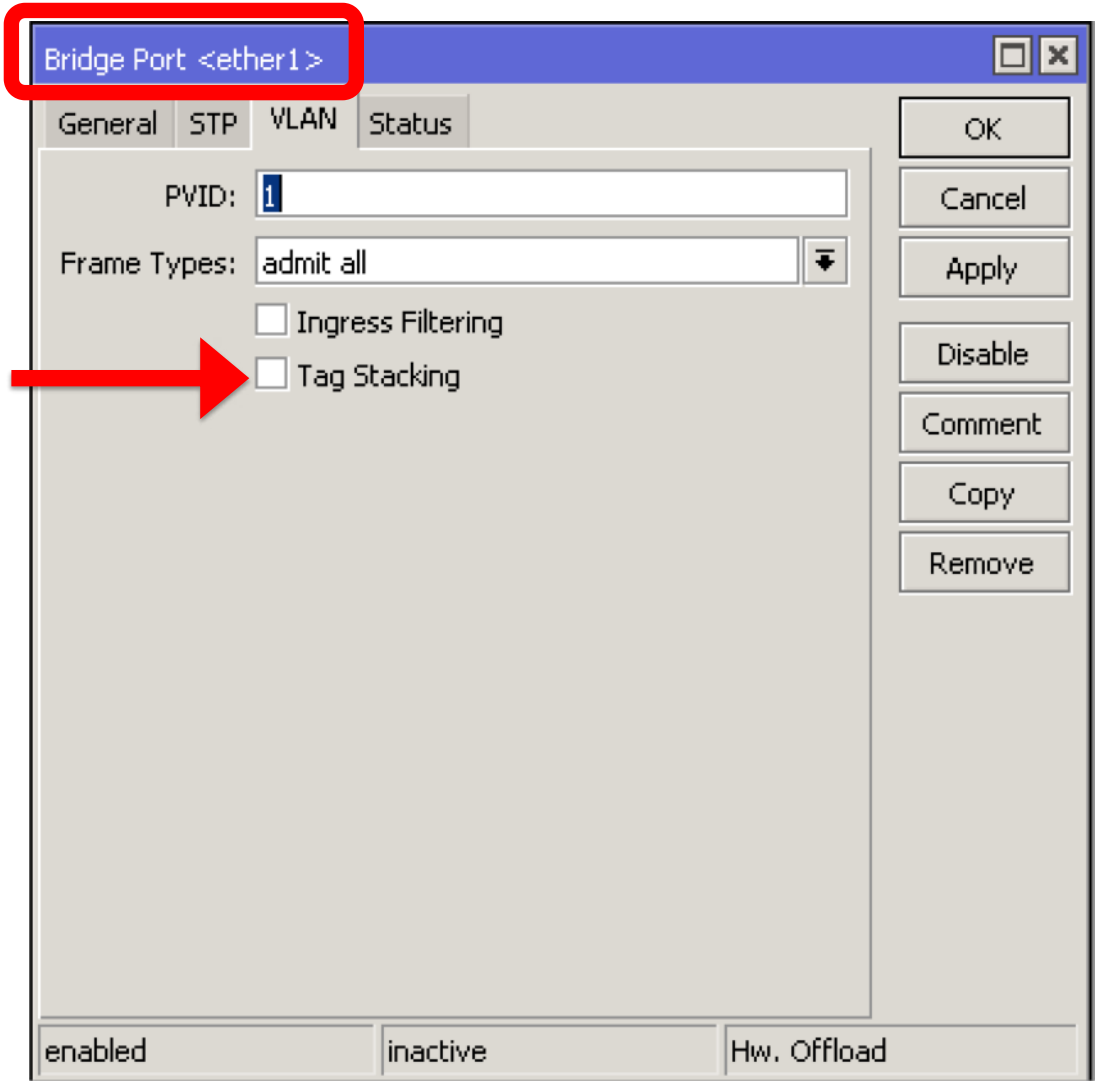


The VLANs in the Bridge

Tag Stacking:

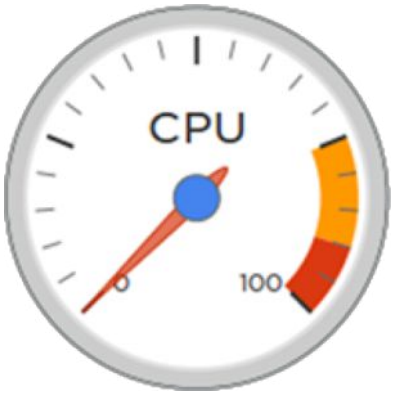
Forces all packets to be treated as untagged packets. Packets on **ingress port** will be tagged with another VLAN tag regardless if a VLAN tag already exists.

The packets will be tagged with a VLAN ID that matches the pvid value.

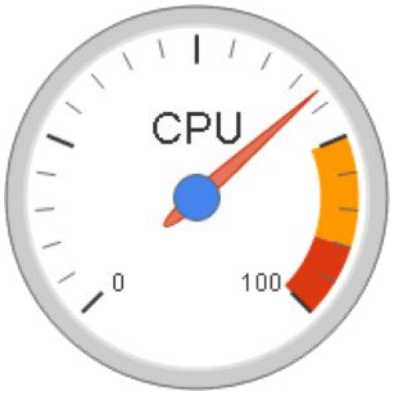


The VLANs in the Bridge

But as I told you before, the bridge can be:



Hardware or Software



The VLANs in the Bridge

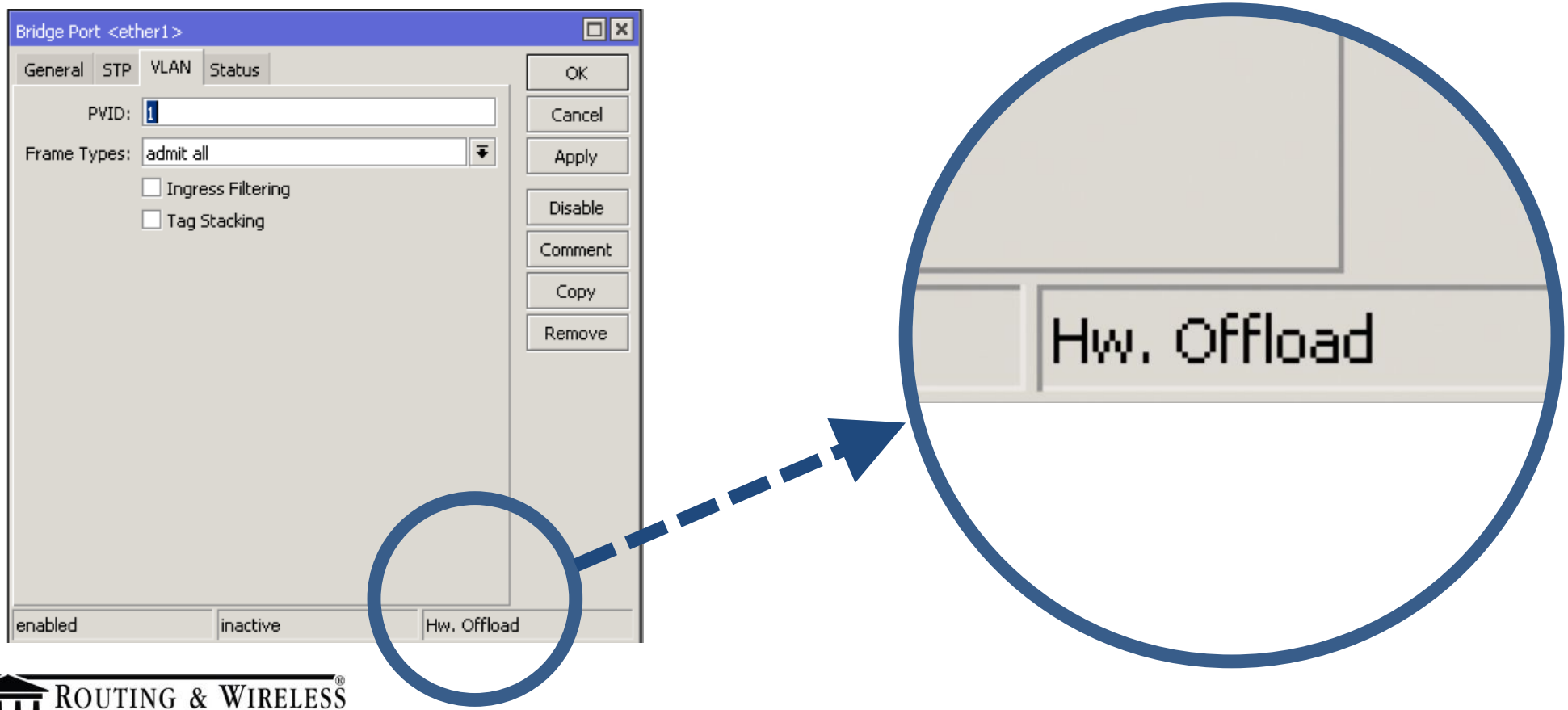
A bridge can be “hardware” if:

- the device have a switch chip;
- The ports have the `hw=yes`
- We’re using a bridge “function” that is supported by that switch chip.

If all the above conditions are satisfied then the cpu will not be used for these tasks.

The VLANs in the Bridge

The **Hardware Offloading,** when available and enabled, will do the job. The status bar will tell us **when is activated** (**=hardware**).



The VLANs in the Bridge

Hw Offload in the bridge, based on the chip switch model

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]	+	-	-	-	-	-	-

The VLANs in the Bridge

As show in the previous table, **currently only CRS3xx** series devices are capable of using bridge **VLAN filtering and hardware offloading** at the same time.

The VLANs in the Bridge

Using the bridge you can create almost any kind of port with the VLANs. Useful to manage VLANs "like in a switch" and "like in a bridge" also ☺.

Pros: Very fexible configs, but will use the CPU (or not) depending the hardware and the settings that you made.

Cons: will use the CPU (or not) depending the hardware and the settings that you made. **(check the specs before buy!)**

VLANs examples

Are you now looking for some practical examples about the VLANs?

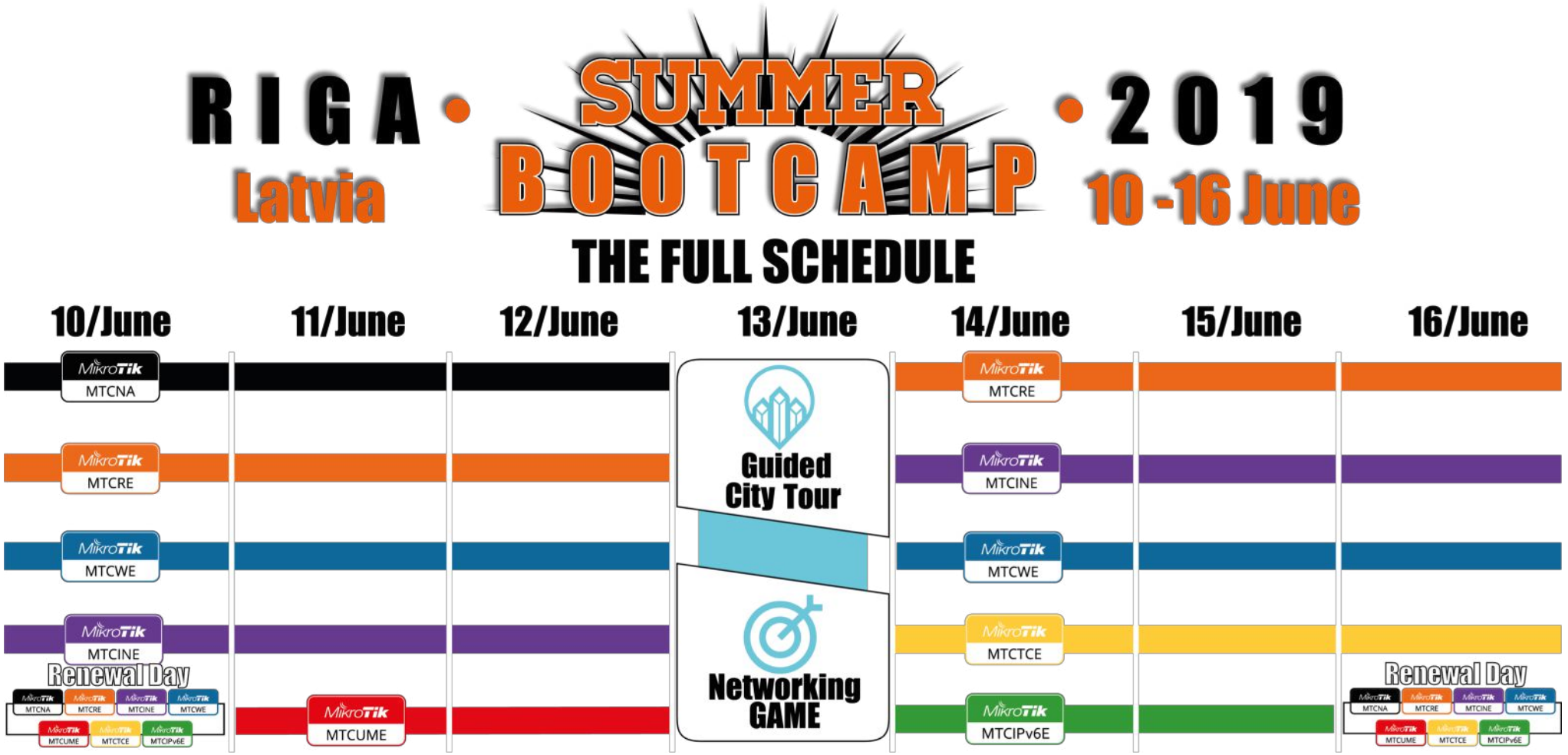
Check on wiki.mikrotik.com: there are plenty examples of the VLANs in these different "flavours”

(hoping that now you understand the differences between them)

Wrap up

- ✓ I hope you enjoyed my presentation and that you learned the differences about the VLANs on RouterOS.
- ✓ Plan your setup using the right hardware.
- ✓ Please don’t make a mess with the VLANs!

See you in Riga!



Thank you for listening!

Q & A

https://routing.wireless.academy
routing@wireless.academy