

VLAN-y «po nowemu»

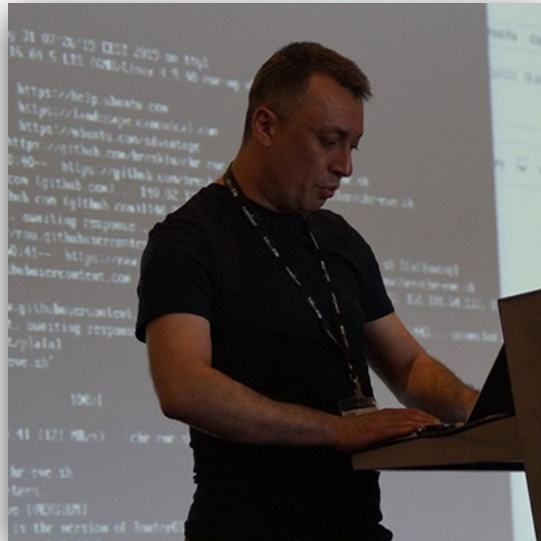
MBUM #4

Warszawa

Listopad 2019

MikroTik Certified Trainer

Ihor Hreskiv



Administrator systemów informatycznych oraz architekt z ponad 20-letnim doświadczeniem. Przygodę z informatyką rozpoczął od programowania na komputerach ZX Spectrum, które stały się hobby i pracą. Studiował na Politechnice w Tarnopolu na kierunku Programowania systemów automatyki przemysłowej. Pracował zarówno jak w małych firmach prywatnych, tak i państwowych, od administracji sieci po projektowanie systemów informatycznych. Moją główną specjalizacją jest virtualizacja, ale mam też doświadczenie w:

- ✓ **BSD systemach**
- ✓ **systemy prioryteżacji ruchu QoS**
- ✓ **tuneli VPN**
- ✓ **VmWare w jakości desktopowej oraz serwerowej virtualizacji**
- ✓ **Linux systemach**

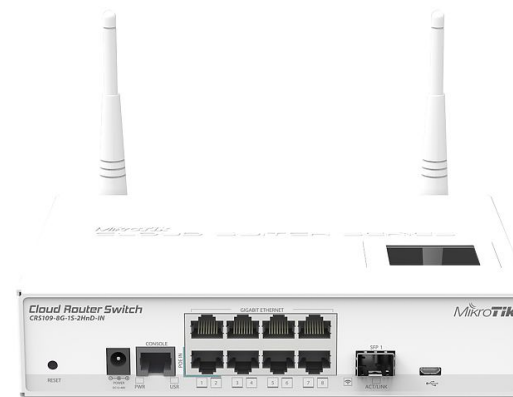


Jestem certyfikowanym trenerem MikroTik, prowadzę szkolenia na Ukrainie oraz w Polsce.

Brałem udział w MikroTik User Meeting (MUM) w Kijowie (Ukraina) oraz w Budapeszcie (Węgry) jako prelegent.

Urządzenia MikroTik

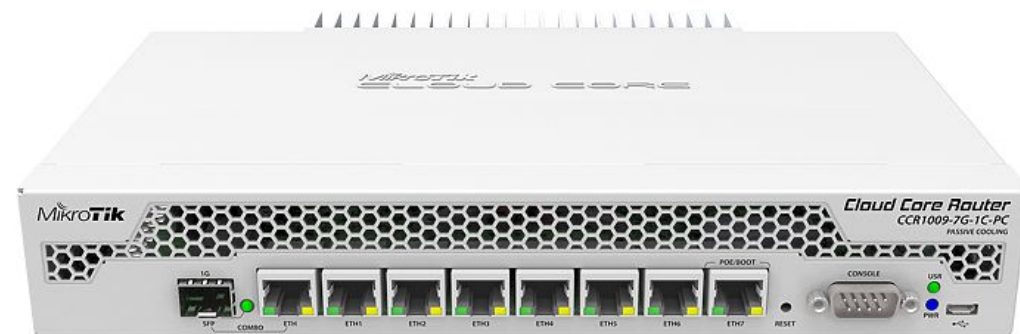
Umowny podział urządzeń MikroTik



Urządzenia posiadające układ switchujący (CRSxxx/CSSxxx)

Urządzenia MikroTik

Umowny podział urządzeń MikroTik



Urządzenia nie posiadające układu switchującego (CCRxxx)

Urządzenia MikroTik

Umowny podział urządzeń MikroTik

CHR

x86

Softwarowe rozwiązania (CHR/x86)

VLAN
Czym jest?

Czym jest vlan?

Definicja

Wirtualna sieć lokalna, VLAN (od ang. virtual local area network) – sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej.

https://pl.wikipedia.org/wiki/Wirtualna_sieć_lokalna

Czym jest vlan?

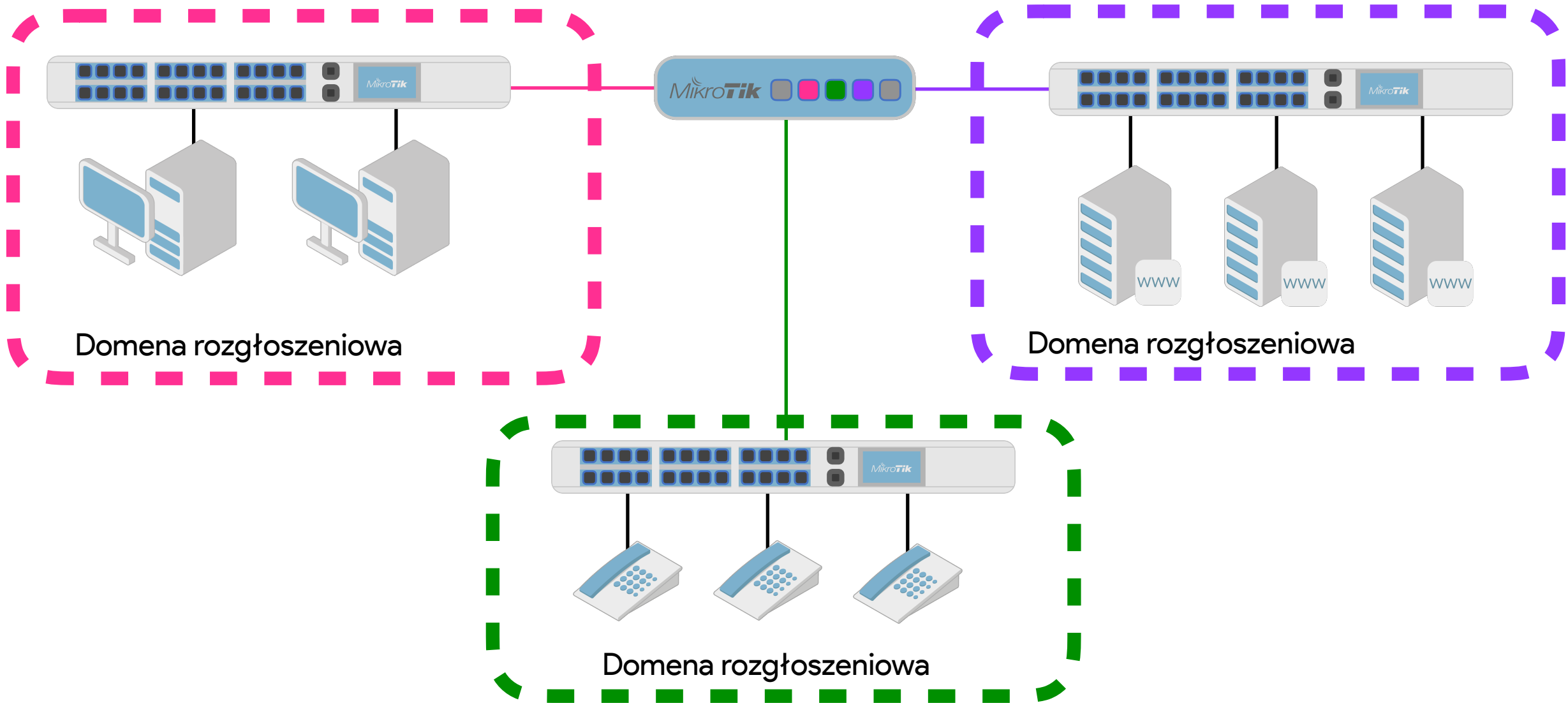
Rodzaje sieci wirtualnych

- Sieci wirtualne określone jako grupy portów
- Sieci wirtualne jako grupy adresów fizycznych MAC
- Sieci wirtualne definiowane przez wykorzystywany protokół warstw wyższych modelu OSI
- Sieci wirtualne określone na podstawie parametrów przekazanych przez serwer uwierzytelniania

https://pl.wikipedia.org/wiki/Wirtualna_sieć_lokalna

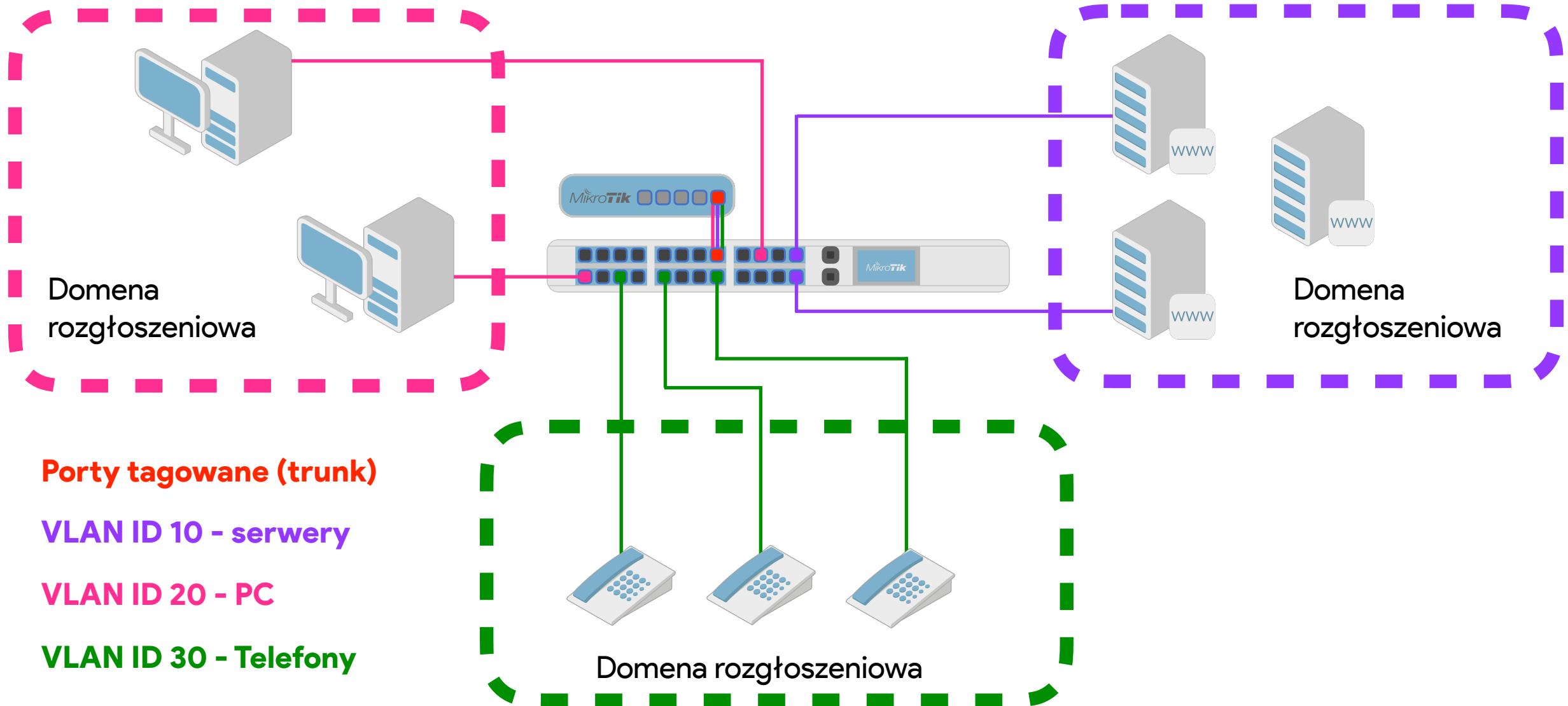
Czym jest vlan?

Typowy schemat sieci



Czym jest vlan?

Typowy schemat sieci



802.1Q

Czym jest vlan?

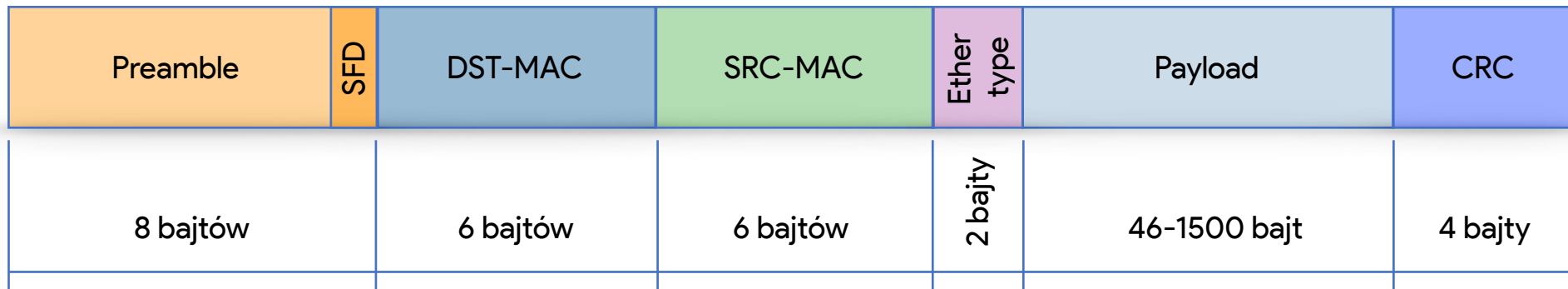
802.1Q

W przełącznikach zarządzalnych zgodnych z IEEE 802.1Q możliwe jest znakowanie ramek (*tagowanie*) poprzez dołączenie do nich informacji o VLAN-ie, do którego należą. Dzięki temu możliwe jest transmitowanie ramek należących do wielu różnych VLAN-ów poprzez jedno fizyczne połączenie (*trunking*).

https://pl.wikipedia.org/wiki/Wirtualna_sieć_lokalna

Czym jest vlan?

Ethernet frame / Ramka ethernetowa



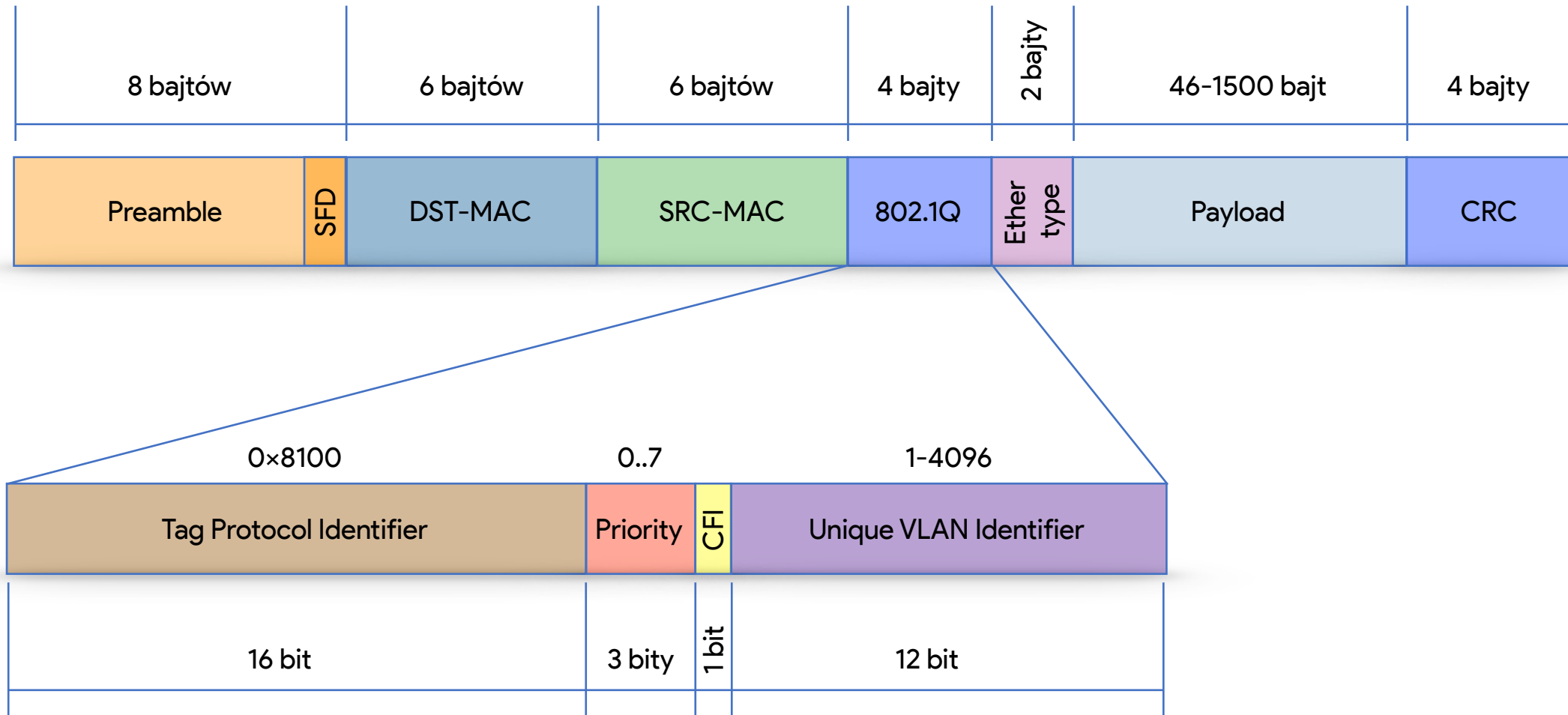
Czym jest vlan?

Ethernet frame 802.1Q / Ramka ethernetowa 802.1Q

Preamble	SFD	DST-MAC	SRC-MAC	802.1Q	Ether type	Payload	CRC
8 bajtów		6 bajtów	6 bajtów	4 bajty	2 bajty	46-1500 bajt	4 bajty

Czym jest vlan?

Ethernet frame 802.1Q / Ramka ethernetowa 802.1Q



Czym jest vlan?

Dodawanie znacznika VLAN do ramki ethernetowej

Żeby zobaczyć co dokładnie się zmienia w nagłówku ramki ethernetowej, pod czas dodawania znacznika VLAN ID (inaczej można spotkać określenie CVID - Client VLAN ID), spójrzmy na ramkę bez znacznika VLAN oraz z dodanym znacznikiem.

- ▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
- ▼ Ethernet II, Src: Private_66:68:07 (00:50:79:66:68:07), Dst: Private_66:68:08 (00:50:79:66:68:08)
 - ▶ Destination: Private_66:68:08 (00:50:79:66:68:08)
 - ▶ Source: Private_66:68:07 (00:50:79:66:68:07)
 - Type: IPv4 (0x0800)
- ▶ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
- ▶ Internet Control Message Protocol

Niemodyfikowany nagłówek

Czym jest vlan?

Dodawanie znacznika VLAN do ramki ethernetowej

- ▶ Frame 22: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
- ▼ Ethernet II, Src: Private_66:68:07 (00:50:79:66:68:07), Dst: Private_66:68:08 (00:50:79:66:68:08)
 - ▶ Destination: Private_66:68:08 (00:50:79:66:68:08)
 - ▶ Source: Private_66:68:07 (00:50:79:66:68:07)
 - Type: 802.1Q Virtual LAN (0x8100)
- ▼ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 20
 - 000. = Priority: Best Effort (default) (0)
 - ...0 = DEI: Ineligible
 - 0000 0001 0100 = ID: 20
 - Type: IPv4 (0x0800)
- ▶ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
- ▶ Internet Control Message Protocol

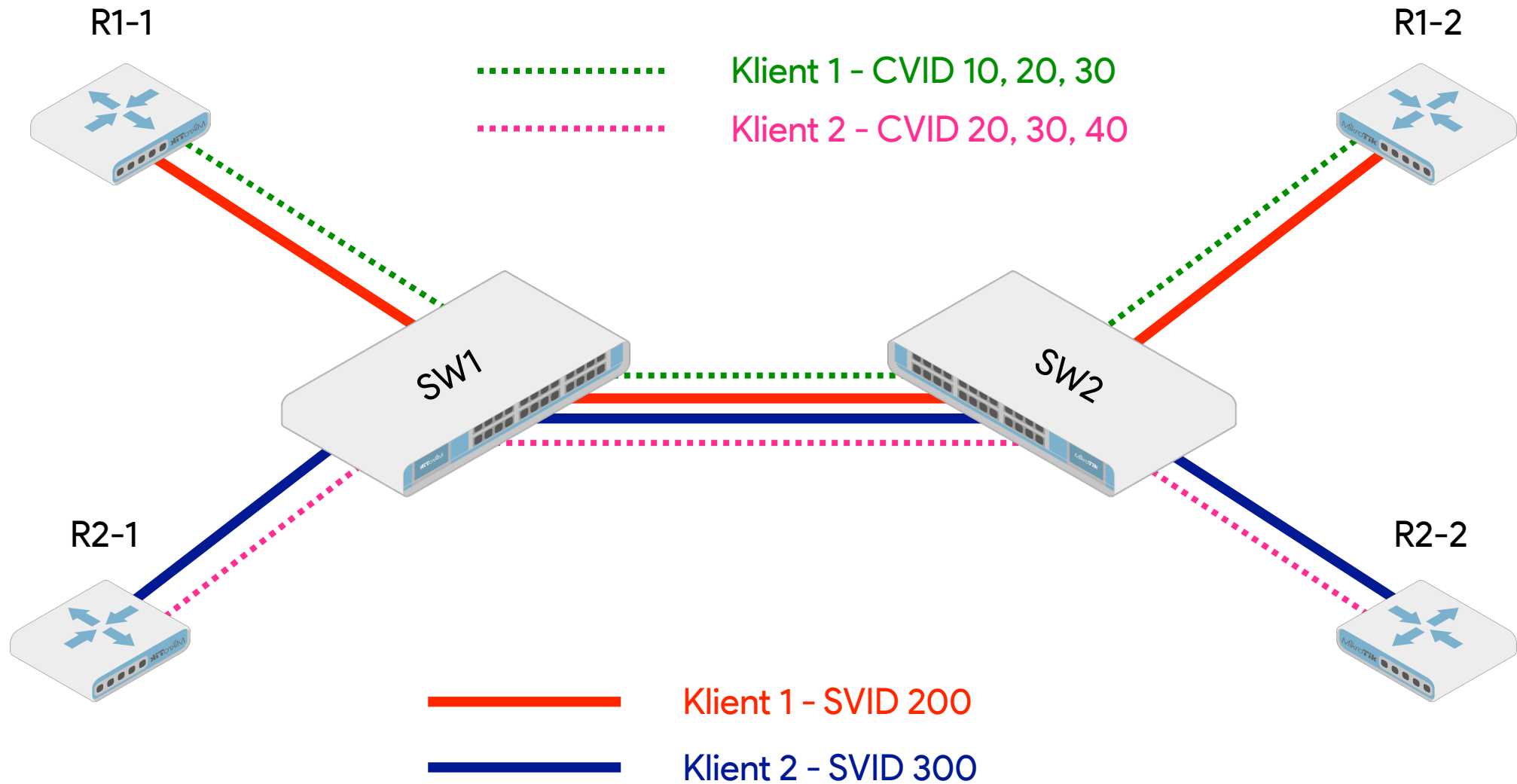
802.1Q - VLAN ID tag

Niemodyfikowany nagłówek

Q-in-Q

Czym jest vlan?

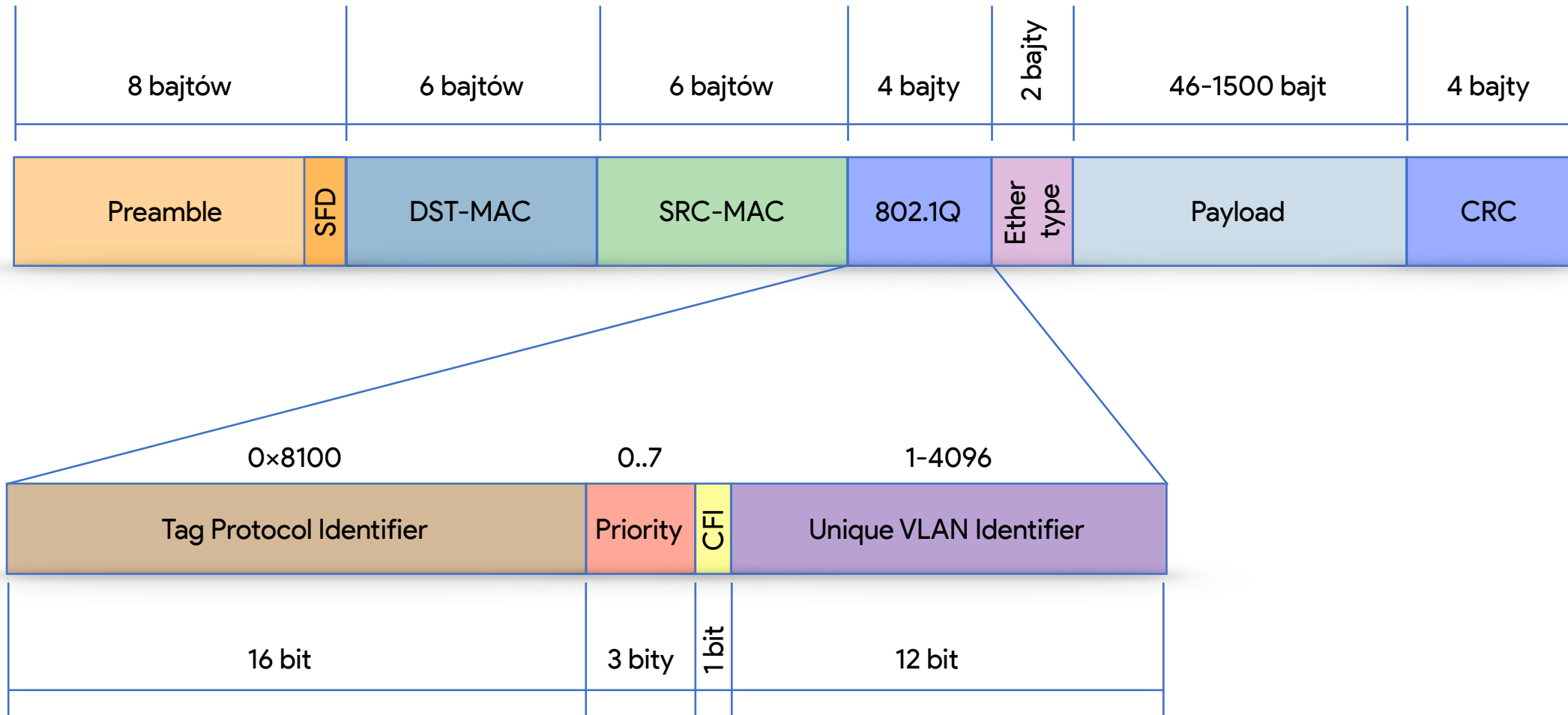
Q-in-Q



802.1ad

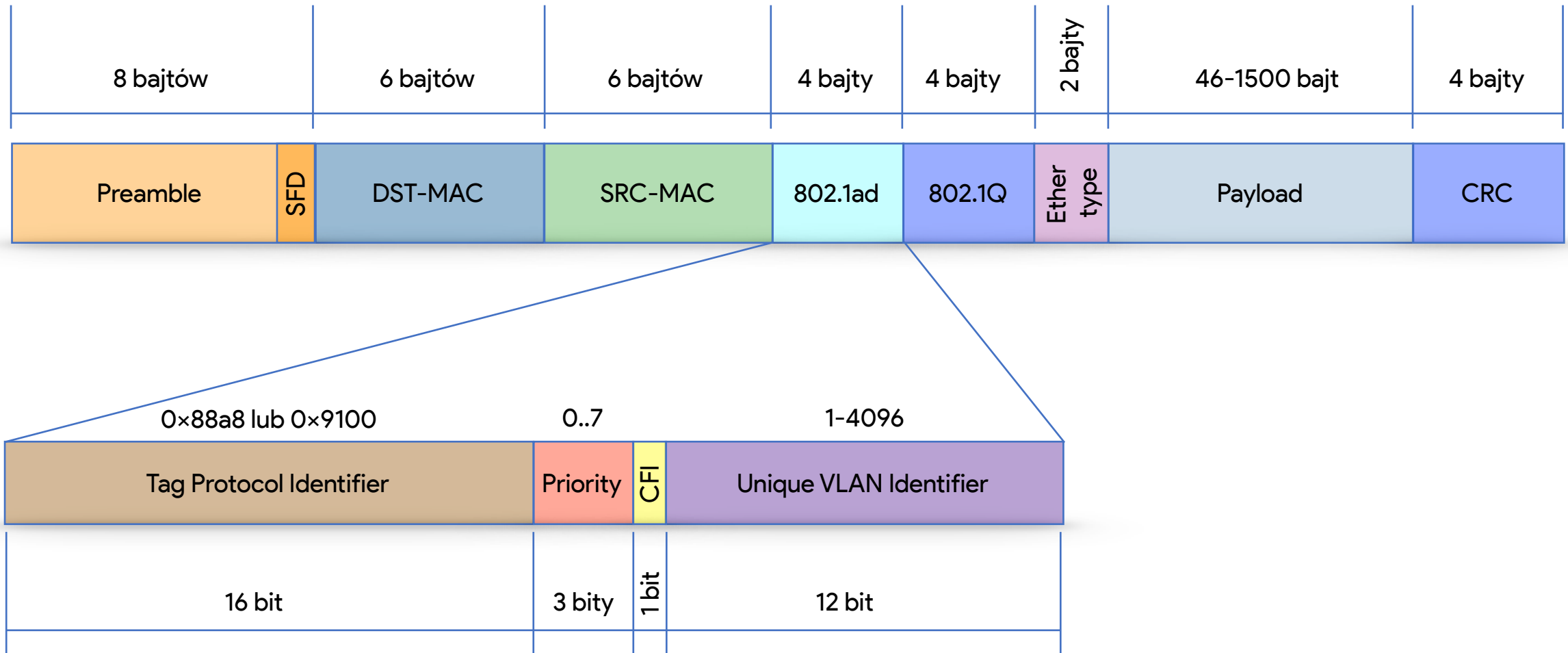
Czym jest vlan?

Ethernet frame 802.1Q / Ramka ethernetowa 802.1Q



Czym jest vlan?

Ethernet frame 802.1ad / Ramka ethernetowa 802.1ad



Czym jest vlan?

Ethernet frame 802.1ad / Ramka ethernetowa 802.1ad

- ▶ Frame 287: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
- ▼ Ethernet II, Src: Private_66:68:08 (00:50:79:66:68:08), Dst: Private_66:68:07 (00:50:79:66:68:07)
 - ▶ Destination: Private_66:68:07 (00:50:79:66:68:07)
 - ▶ Source: Private_66:68:08 (00:50:79:66:68:08)
 - Type: 802.1ad Provider Bridge (Q-in-Q) (0x88a8)
- ▼ IEEE 802.1ad, ID: 200
 - 000. = Priority: 0
 - ...0 = DEI: 0
 - 0000 1100 1000 = ID: 200
 - Type: 802.1Q Virtual LAN (0x8100)
- ▼ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 20
 - 000. = Priority: Best Effort (default) (0)
 - ...0 = DEI: Ineligible
 - 0000 0001 0100 = ID: 20
 - Type: IPv4 (0x0800)
- ▶ Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1
- ▶ Internet Control Message Protocol

Niemodyfikowany nagłówek

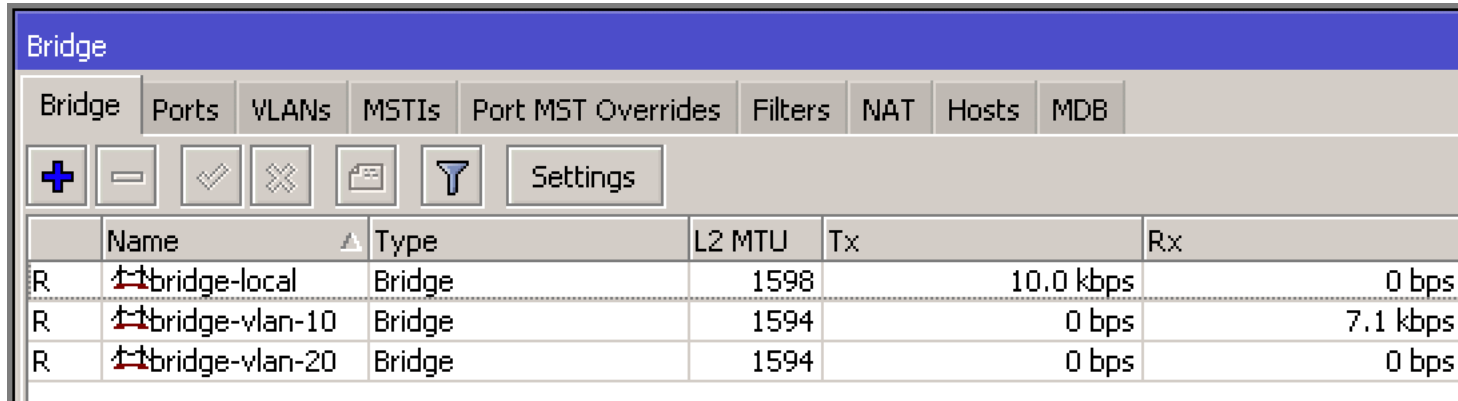
802.1Q - CVID tag

802.1ad - SVID tag

Metody konfigurowania «po staremu»

Metody konfigurowania «po staremu»

«Bridge'owanie» vlanów

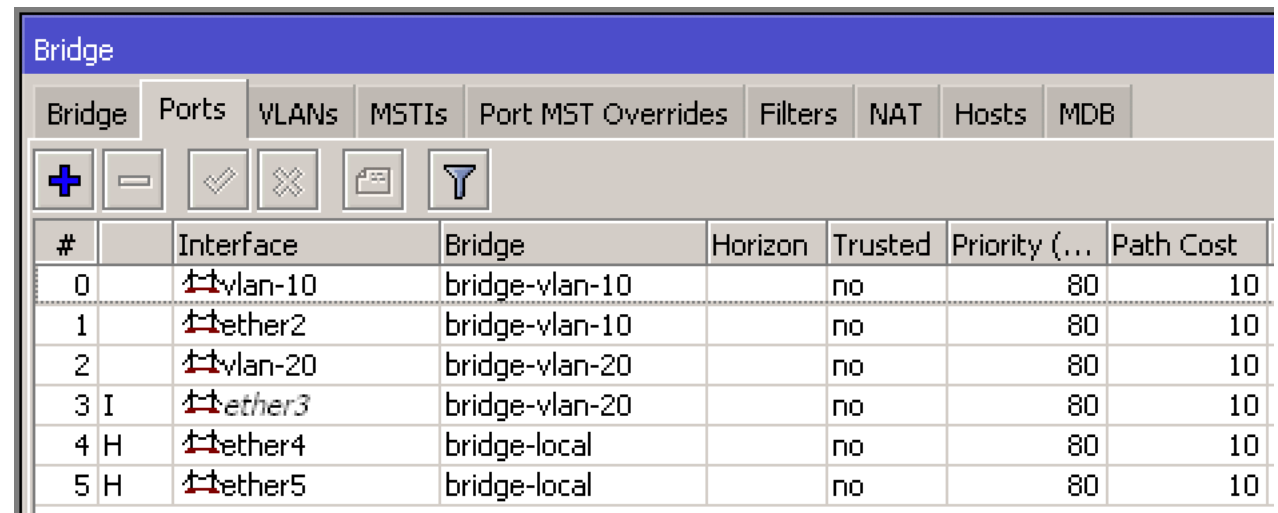


Bridge

	Name	Type	L2 MTU	Tx	Rx
R	bridge-local	Bridge	1598	10.0 kbps	0 bps
R	bridge-vlan-10	Bridge	1594	0 bps	7.1 kbps
R	bridge-vlan-20	Bridge	1594	0 bps	0 bps

Dodajemy bridge dla każdego VLAN-u oraz bridge dla tagowanych interfejsów (z nazwą **bridge-local**)

Dodajemy interfejsy typu VLAN oraz fizyczne do bridge-a, który ma być dostępowym lub do **bridge-local** interfejsy tagowane

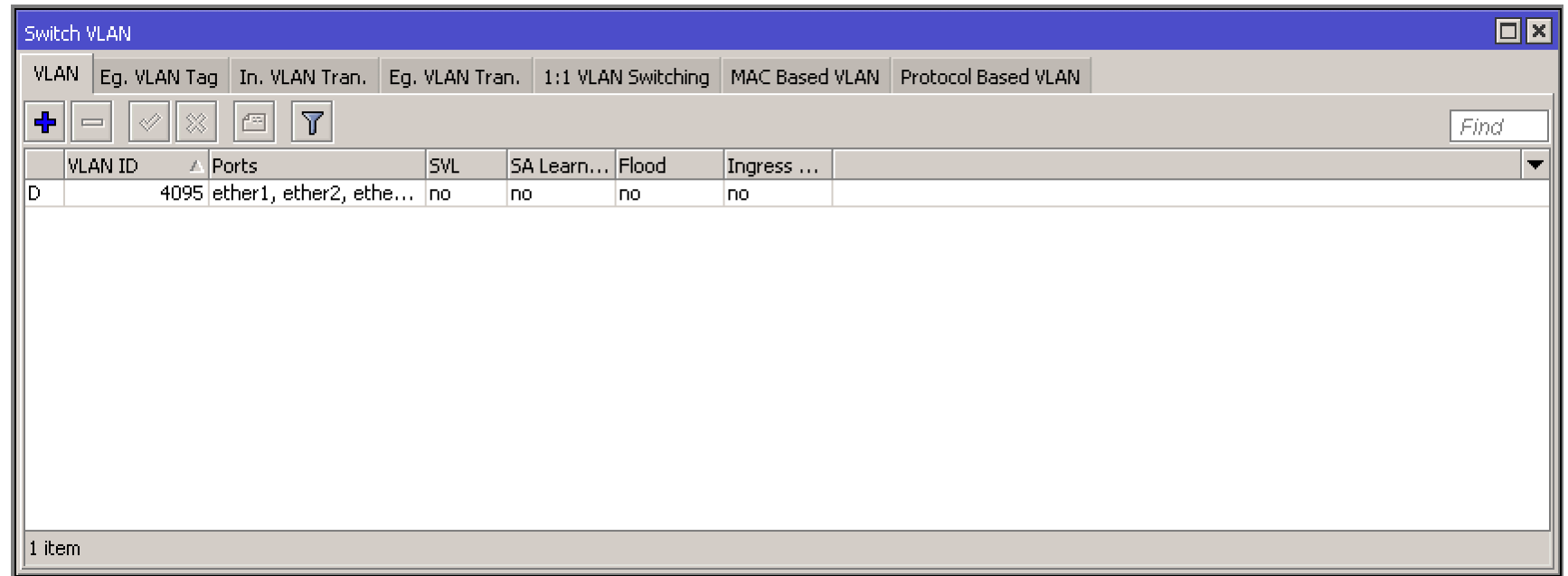
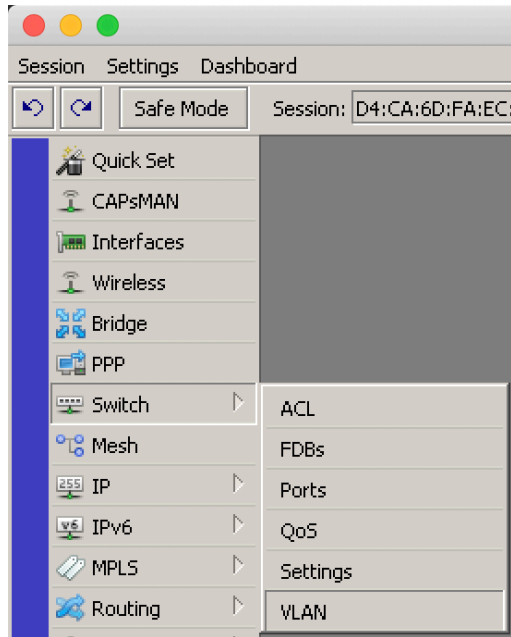


Bridge

#	Interface	Bridge	Horizon	Trusted	Priority (...)	Path Cost
0	vlan-10	bridge-vlan-10		no	80	10
1	ether2	bridge-vlan-10		no	80	10
2	vlan-20	bridge-vlan-20		no	80	10
3 I	ether3	bridge-vlan-20		no	80	10
4 H	ether4	bridge-local		no	80	10
5 H	ether5	bridge-local		no	80	10

Metody konfigurowania «po staremu»

CRS1xx/CRS2xx



W zakładce menu **Switch->VLAN** dodajemy VLAN-y, który mogą się pojawić na naszym urządzeniu

Metody konfigurowania «po staremu»

CRS1xx/CRS2xx

New Switch VLAN

VLAN ID: 10

Ports:

- ether1
- ether2
- ether3
- ether4
- ether5
- ether6
- ether7
- ether8
- ether9
- ether10
- ether11
- ether12
- ether13
- ether14
- ether15
- ether16
- switch1-cpu

OK

Cancel

Apply

Disable

Comment

Copy

Remove

☐ SVL

☒ SA Learning

☐ Flood

☐ Ingress Mirror

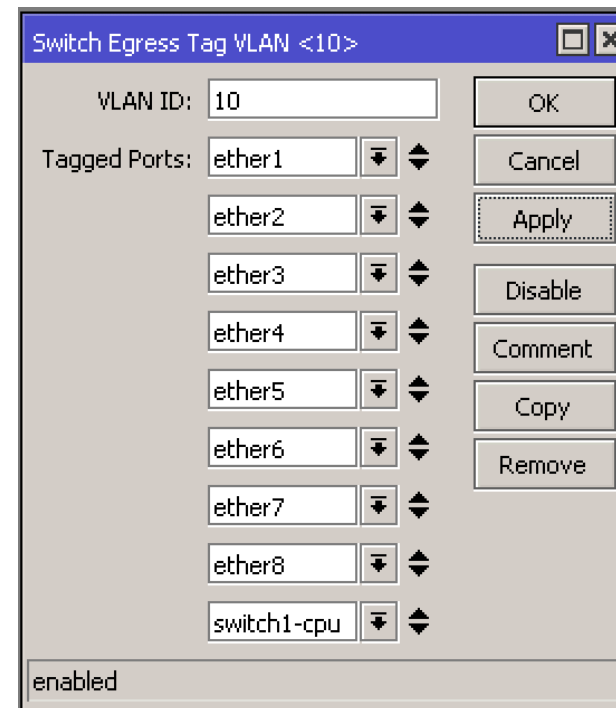
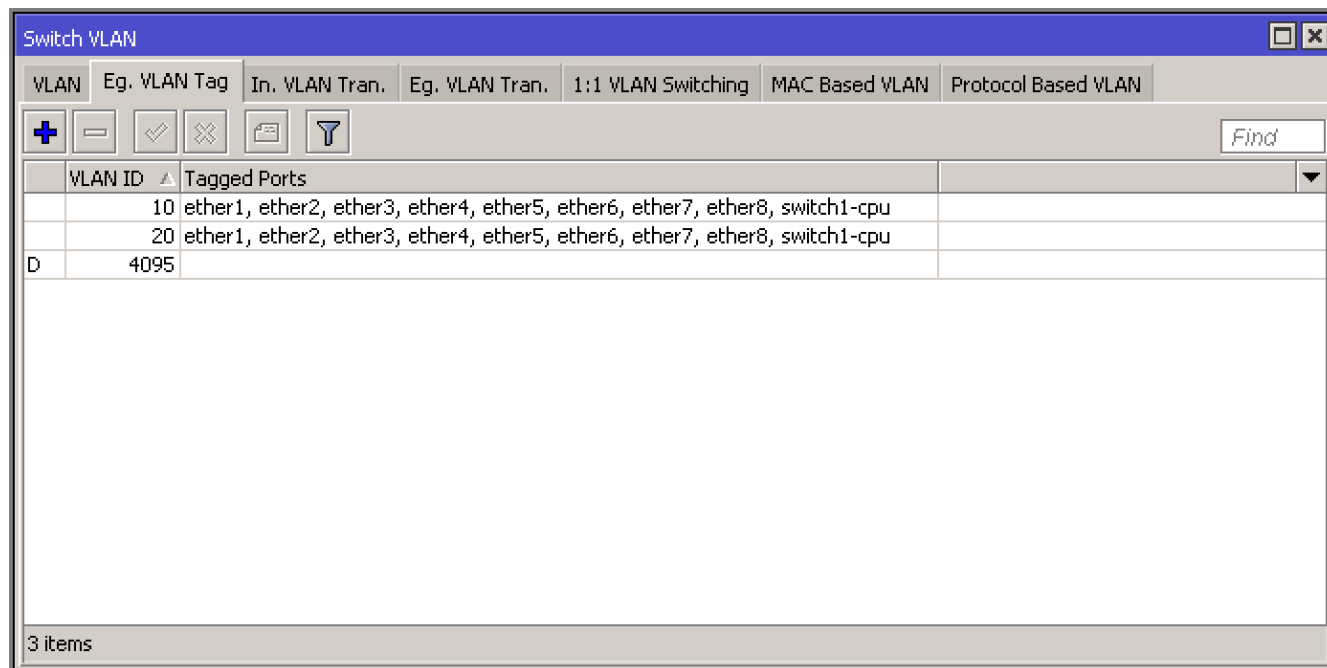
QoS Group: none

enabled

Określamy interfejsy na których mogą być VLAN-y z zaznaczonym VLAN ID

Metody konfigurowania «po staremu»

CRS1xx/CRS2xx



Na zakładce **Eg. VLAN Tag** wskazujemy tagowane (trunk) interfejsy

Metody konfigurowania «po staremu»

CRS1xx/CRS2xx

Ingress VLAN Translation <ether9, ether10, ether11, ether12, ether...>

Ports: ether9, ether10, ether11, ether12, ether13, ether14, ether15, ether16

Protocol:

Service VLAN Lookup For: any

Service VID:

Service PCP:

Service DEI:

Customer VLAN Lookup For: any

Customer VID: 0

Customer PCP:

Customer DEI:

New Service VID:

New Customer VID: 10

☐ PCP Propagation

☒ SA Learning

enabled

Switch VLAN

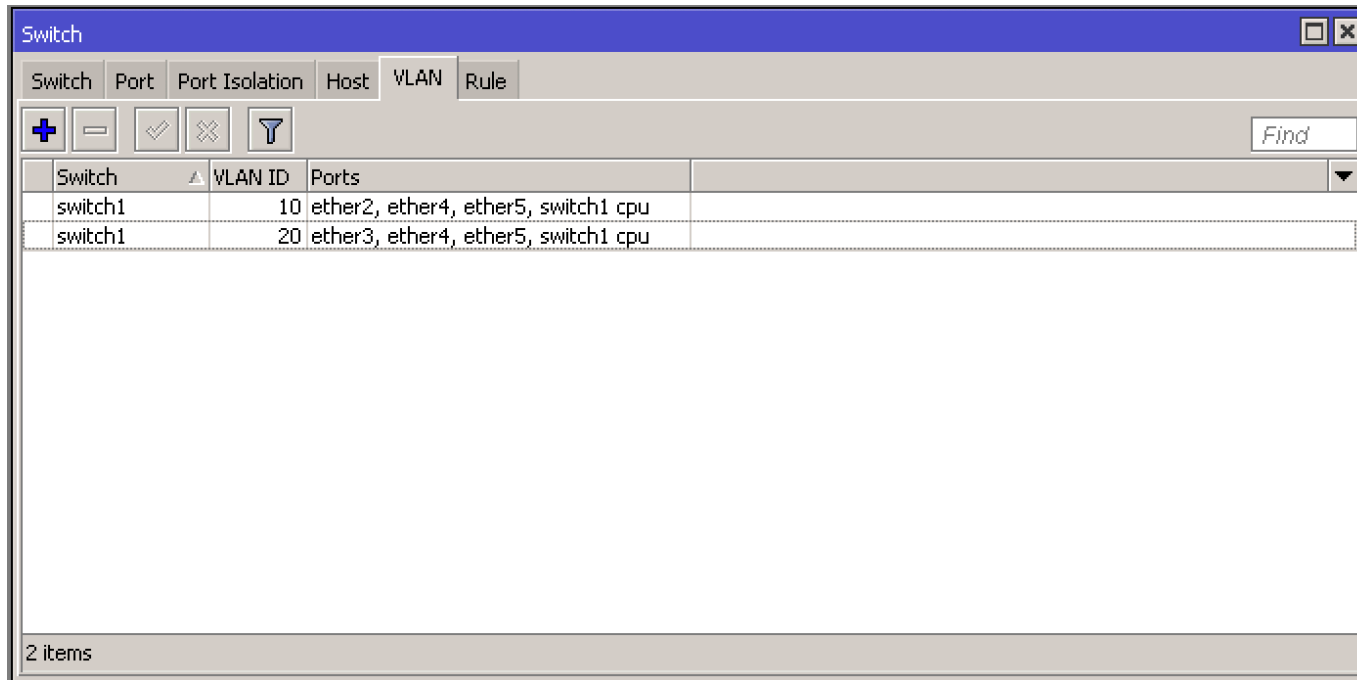
VLAN	Eg. VLAN Tag	In. VLAN Tran.	Eg. VLAN Tran.	1:1 VLAN Switching	MAC Based VLAN	Protocol Based VLAN
D	ether1, ether2, ether3, ether4, ether5, ...	any				
	ether9, ether10, ether11, ether12, ethe...	any				
	ether17, ether18, ether19, ether20, eth...	any				

3 items

Na zakładce **Ig. VLAN Tran.** wskazujemy
dostępowy (access) interfejsy

Metody konfigurowania «po staremu»

Na «małych» urządzeniach typu hAP AC Lite z SwitchChip



W zakładce menu **Switch->VLAN**
dodajemy VLAN-y, który mogą się pojawić
na naszym urządzeniu

Metody konfigurowania «po staremu»

Na «małych» urządzeniach typu hAP AC Lite z SwitchChip

Określamy interfejsy na których mogą być VLAN-y z zaznaczonym VLAN ID

Switch VLAN <10>

Switch: switch1

VLAN ID: 10

Ports: ether2, ether4, ether5, switch1 cpu

☐ Independent Learning

enabled

Metody konfigurowania «po staremu»

Na «małych» urządzeniach typu hAP AC Lite z SwitchChip

Switch Port <ether5>

Name: ether5

Switch: switch1

VLAN Mode: secure

VLAN Header: add if missing

Default VLAN ID: 0

Ingress Rate:

Egress Rate:

☒ Limit Broadcasts

☐ Limit Unknown Unicasts

☐ Limit Unknown Multicasts

OK

Cancel

Apply

Switch Port <ether3>

Name: ether3

Switch: switch1

VLAN Mode: secure

VLAN Header: always strip

Default VLAN ID: 20

Ingress Rate:

Egress Rate:

☒ Limit Broadcasts

☐ Limit Unknown Unicasts

☐ Limit Unknown Multicasts

OK

Cancel

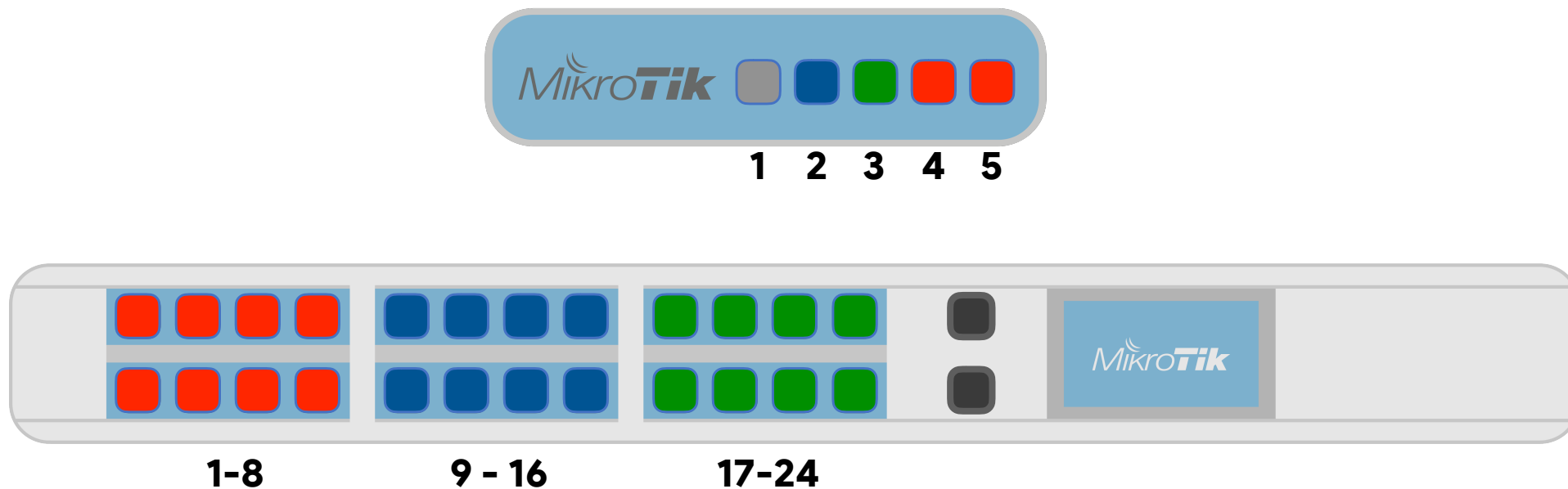
Apply

Zadajemy tryb pracy **VLAN Mode** w zakładce **Switch->Port** «**secure**», oraz dla interfejsów tagowanych wskazujemy **VLAN Header: add if missing**, dla interfejsów typu access - **VLAN Header: always strip**

DEMO

VLAN

Wstępne założenia do konfiguracji



Tagowane

VLAN ID 10

VLAN ID 20

192.168.10.0/24

10.20.20.0/24

VLAN

Bridge / dodawanie nowego

Dodajemy bridge
(z nazwą **bridge-local**)

Interface <bridge-local>

General STP VLAN Status Traffic

Name: bridge-local

Type: Bridge

MTU:

Actual MTU: 1500

L2 MTU: 1592

MAC Address: CC:2D:E0:D8:1C:7E

ARP: enabled

ARP Timeout:

Admin. MAC Address:

Ageing Time: 00:05:00

☐ IGMP Snooping

☐ DHCP Snooping

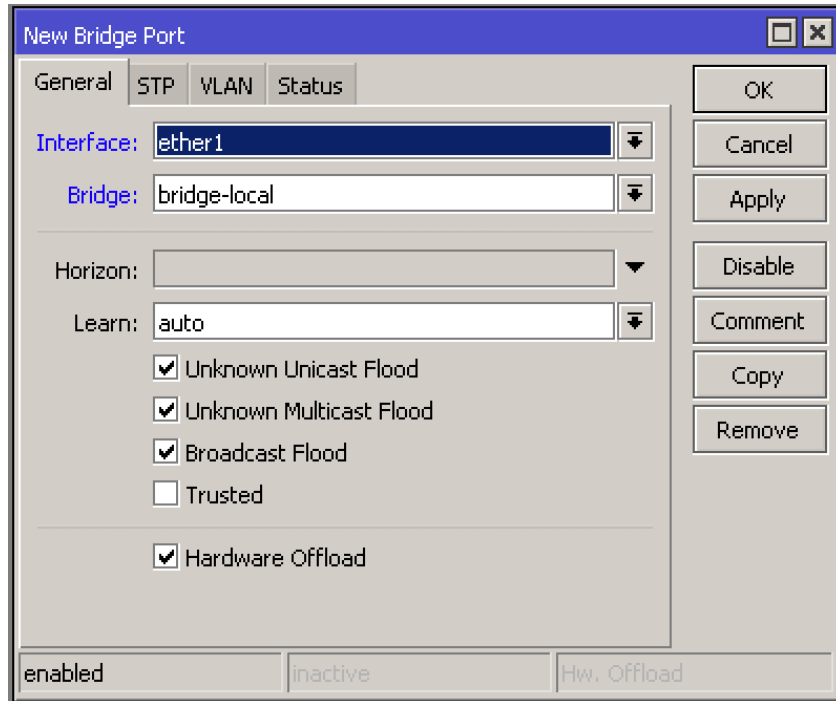
☒ Fast Forward

OK Cancel Apply Disable Comment Copy Remove Torch

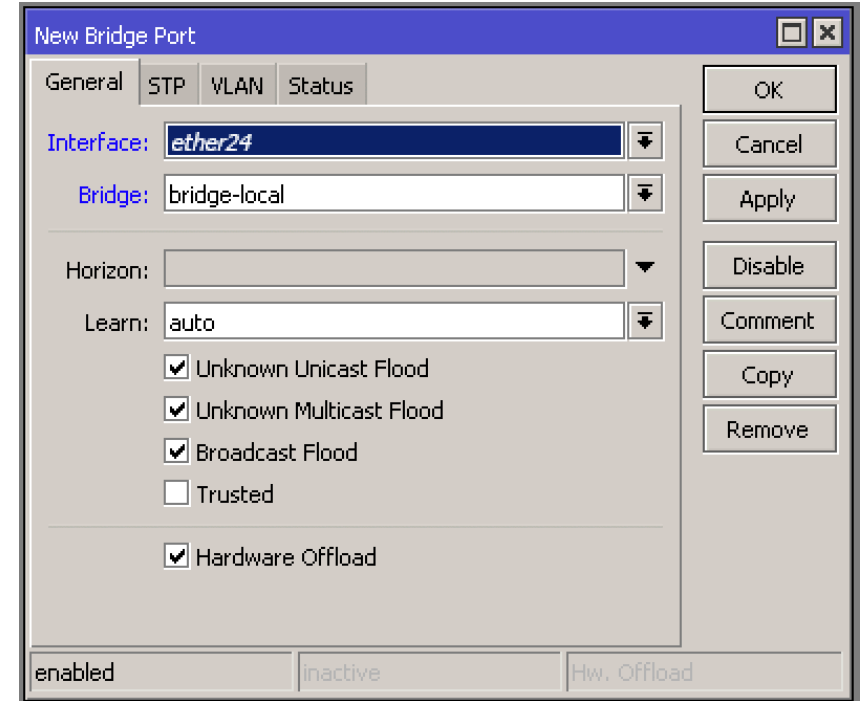
enabled running slave

VLAN

Bridge / dodawanie interfejsów do bridge



Dodajemy
wszystkie interfejsy
od **ether1** do
ether24 ręcznie



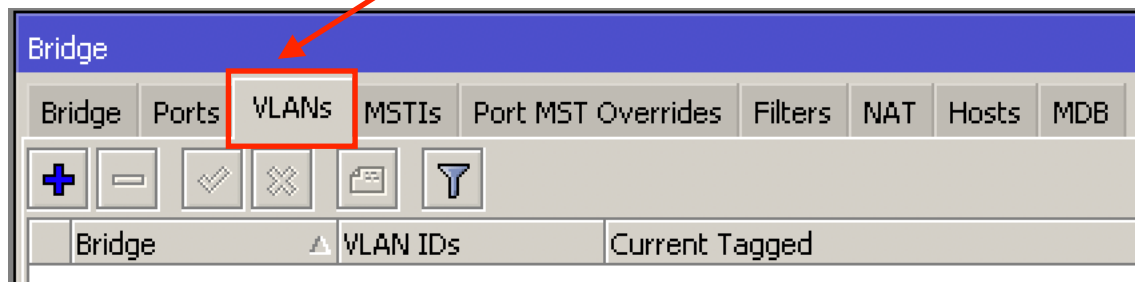
lub używając polecenia z linii komend

```
:for i from=1 to=24 do={/interface bridge port add \  
  bridge=bridge-local interface=( "ether" . $i) }
```

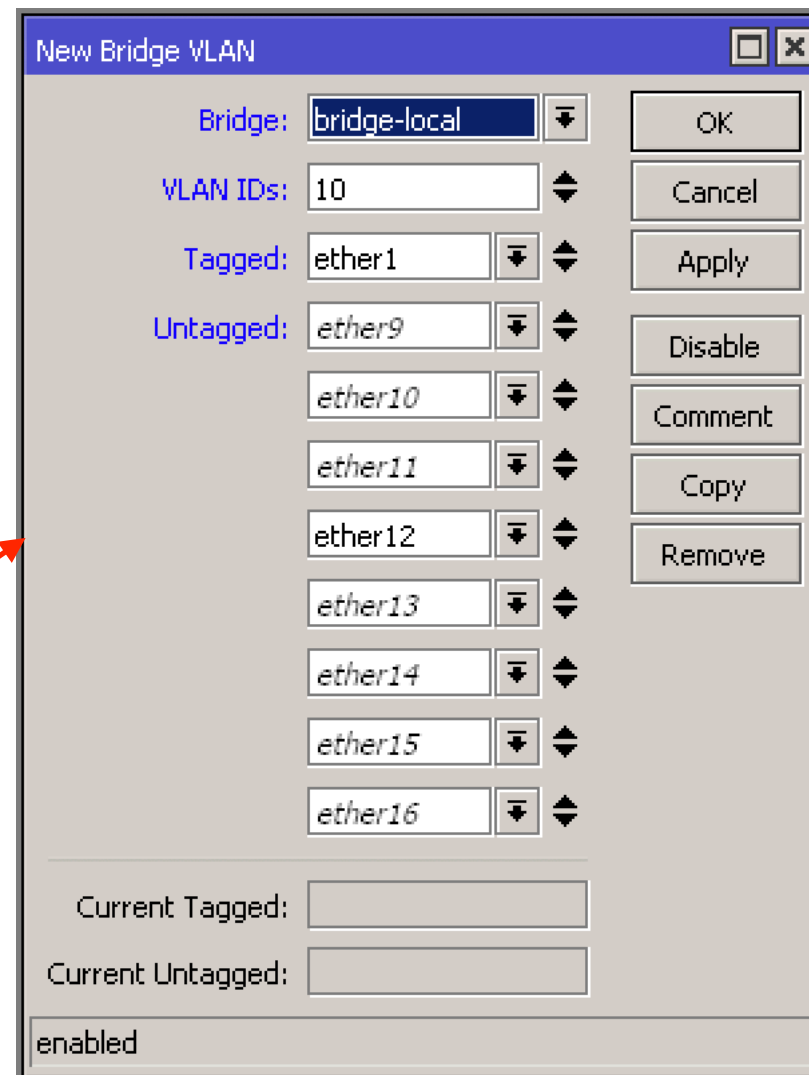
VLAN

Bridge / dodawanie VLAN do bridge-a

Na zakładce VLANs menu Bridge dodajemy znane VLAN-y



W przykładzie dodajemy nowy VLAN z VLAN ID 10, oraz określamy funkcje interfejsów:
ether1 - tagowany (trunk)
ether9-ether16 - nietagowane (access)



VLAN

Bridge / dodawanie VLAN do bridge-a

W taki sam sposób dodamy VLAN z VLAN ID 20,
z następującymi funkcjami interfejsów:

ether1 - tagowany (trunk)

ether17-ether24 - nietagowane (access)

```
/interface bridge vlan  
add bridge=bridge-local tagged=ether1 \  
untagged="ether17,ether18,ether19,ether20,\  
ether21,ether22,ether23,ether24" vlan-ids=20
```

Bridge VLAN <20>

Bridge: **bridge-local**

VLAN IDs: **20**

Tagged: **ether1**

Untagged: **ether17**, **ether18**, **ether19**, **ether20**, **ether21**, **ether22**, **ether23**, **ether24**

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

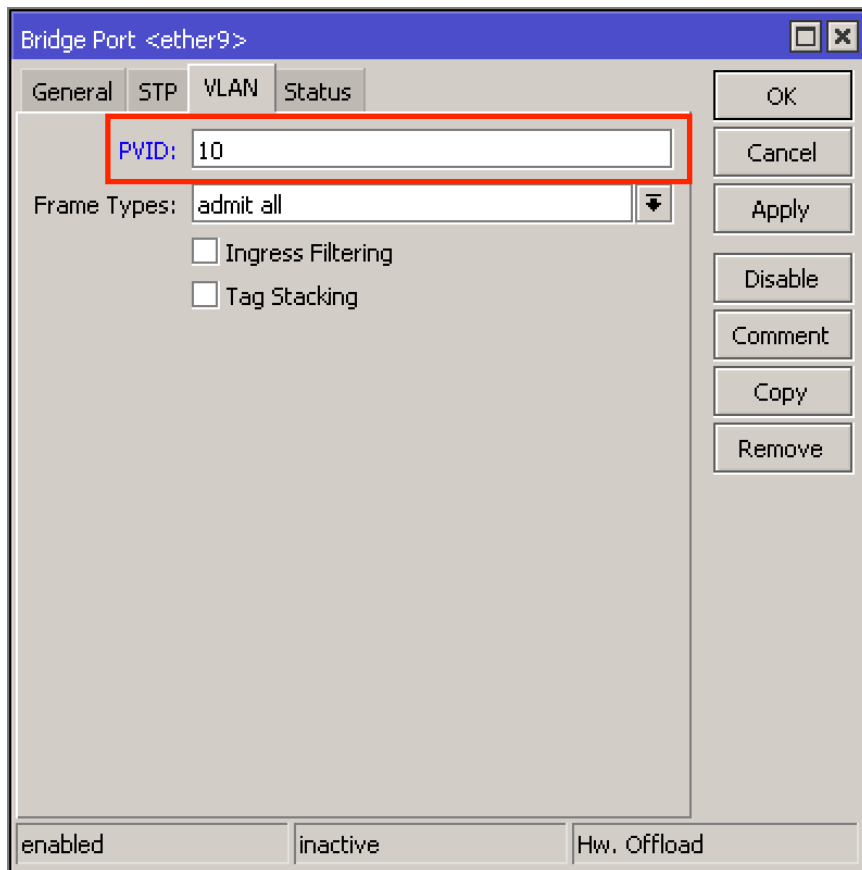
Current Tagged:

Current Untagged:

enabled

VLAN

Bridge / określenie PVID na interfejsach



W zakładce **Ports** menu **Bridge** określamy jaki VLAN ID ma być zdejmowany na przełączniku dla interfejsów, które pełnią funkcje dostępu (access)

Dla interfejsów tagowanych znacznik PVID zostawiamy bez zmian.

Takie określenie można było oznaczyć przy dodawaniu interfejsu do bridge-a.

VLAN

Bridge / określenie PVID na interfejsach

Bridge											
Bridge Ports VLANs MSTIs Port MST Overrides Filters NAT Hosts MDB											
#		Interface	Bridge	Horizon	Trusted	Priority (...)	Path Cost	PVID	Role	Root Path Cost	
0	H	ether1	bridge-local		no	80	10		1 root port	10	
1	IH	ether2	bridge-local		no	80	10		1 disabled port		
2	IH	ether3	bridge-local		no	80	10		1 disabled port		
3	IH	ether4	bridge-local		no	80	10		1 disabled port		
4	IH	ether5	bridge-local		no	80	10		1 disabled port		
5	IH	ether6	bridge-local		no	80	10		1 disabled port		
6	IH	ether7	bridge-local		no	80	10		1 disabled port		
7	IH	ether8	bridge-local		no	80	10		1 disabled port		
8	IH	ether9	bridge-local		no	80	10		10 disabled port		
9	IH	ether10	bridge-local		no	80	10		10 disabled port		
10	IH	ether11	bridge-local		no	80	10		10 disabled port		
11	H	ether12	bridge-local		no	80	10		10 designated port		
12	IH	ether13	bridge-local		no	80	10		10 disabled port		
13	IH	ether14	bridge-local		no	80	10		10 disabled port		
14	IH	ether15	bridge-local		no	80	10		10 disabled port		
15	IH	ether16	bridge-local		no	80	10		10 disabled port		
16	IH	ether17	bridge-local		no	80	10		20 disabled port		
17	IH	ether18	bridge-local		no	80	10		20 disabled port		
18	IH	ether19	bridge-local		no	80	10		20 disabled port		
19	IH	ether20	bridge-local		no	80	10		20 disabled port		
20	IH	ether21	bridge-local		no	80	10		20 disabled port		
21	IH	ether22	bridge-local		no	80	10		20 disabled port		
22	IH	ether23	bridge-local		no	80	10		20 disabled port		
23	IH	ether24	bridge-local		no	80	10		20 disabled port		

24 items

Zgodnie z wcześniejszymi założeniami, widzimy że interfejsy typu access mają dodany znacznik PVID (Port VLAN ID) który mają obowiązek zdjąć dla urządzeń klienckich.

Tagowane

VLAN ID 10

VLAN ID 20

VLAN

Bridge / włączamy filtrowanie VLAN na bridge-u

Włączając filtrowanie VLAN na bridge-u po klikaniu *OK* lub *Apply* nasz przełącznik zacznie filtrować VLAN-y na interfejsach który dodane do tego bridge-a.

Interface <bridge-local>

General STP **VLAN** Status Traffic

☒ VLAN Filtering

EtherType: 0x8100

PVID: 1

Frame Types: admit all

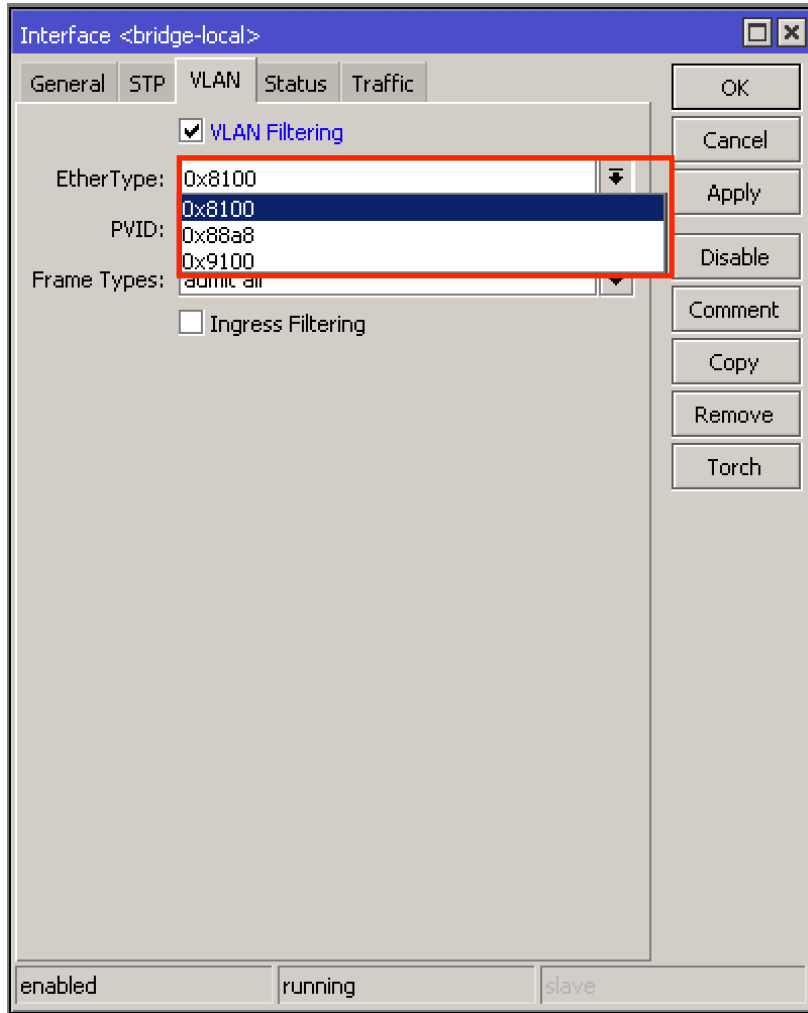
☐ Ingress Filtering

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave

VLAN

Bridge / EtherType dla ramek ethernetowych



W polu EtherType mamy możliwość wyboru typu nagłówka ramki ethernetowej, która będzie wysyłana za pomocą interfejsów naszego bridge-a.

EtherType mogą być następującymi:

0x8100 - 802.1Q - VLAN-tagged frame

0x88a8 - 802.1ad - Provider Bridging

0x9100 - 802.1ad - VLAN-tagged (802.1Q) frame with double tagging

**I co się stało po tych
wszystkich działaniach???**

**Stracony dostęp do naszego
urządzenia!!!**



Management VLAN

Management VLAN

Jak odzyskać dostęp do urządzenia?



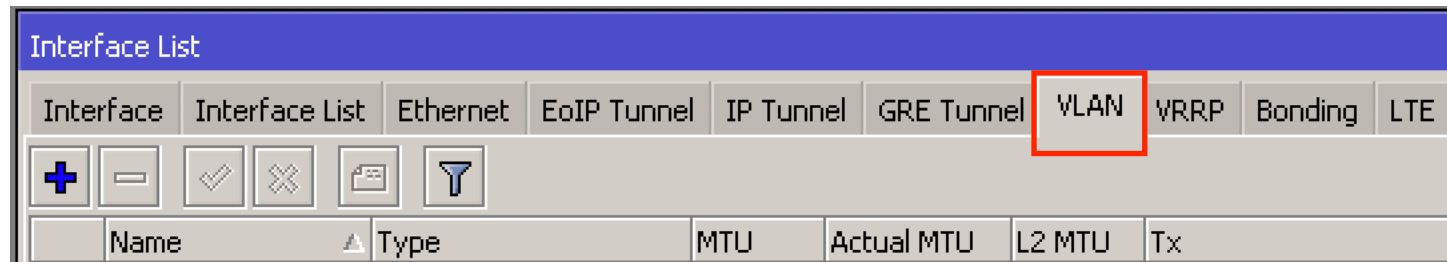
MikroTik Woobm-USB



Kabel konsolowy

Management VLAN

Konfiguracja



Na zakładce *VLAN* menu *Interfaces* dodajmy nowy interfejs typu VLAN z VLAN ID, który będzie używany do zarządzania naszym urządzeniem.

Management VLAN

Konfiguracja

W przykładzie będziemy używać ten VLAN który był stworzony na początku tworzenia naszej konfiguracji, czyli VLAN 10.

Tworzymy taki interfejs na interfejsie bridge.

Interface <vlan-10>

General Loop Protect Status Traffic

Name: vlan-10

Type: VLAN

MTU: 1500

Actual MTU: 1500

L2 MTU: 1588

MAC Address: CC:2D:E0:D8:1C:7E

ARP: enabled

ARP Timeout:

VLAN ID: 10

Interface: bridge-local

☐ Use Service Tag

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave

Management VLAN

Konfiguracja

Bridge VLAN <10>

Bridge: bridge-local

VLAN IDs: 10

Tagged: ether1

Untagged: ether9, ether10, ether11, ether12, ether13, ether14, ether15, ether16

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

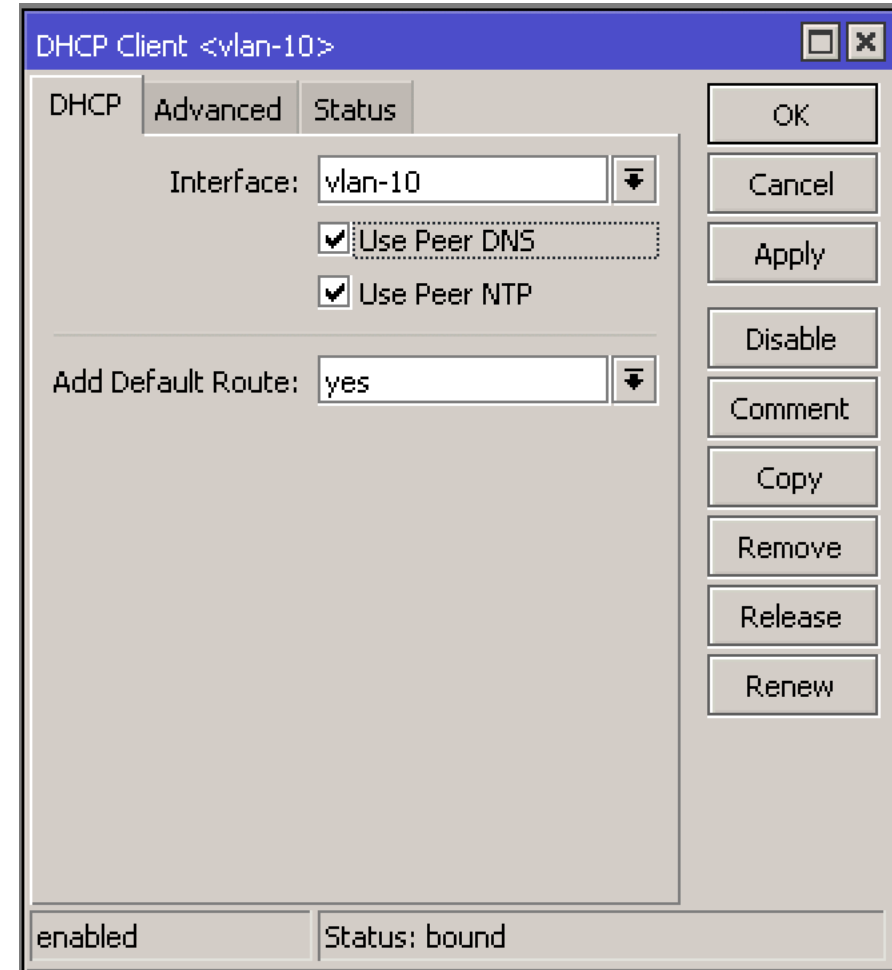
Do określenia VLAN na naszym bridge-u dodajemy **bridge-local**, jako tagowany interfejs (trunk)

Dodawanie **bridge-local** do interfejsów tagowanych pozwala odzyskać dostęp do management-u RouterOS, który się znajduje na CPU

Management VLAN

Konfiguracja

Teraz możemy uruchomić DHCP-Client lub nadać stały IP adres na interfejsie typu VLAN dla dostępu na nasze urządzenie.



The screenshot shows a window titled "DHCP Client <vlan-10>". It has three tabs: "DHCP", "Advanced", and "Status". The "DHCP" tab is selected. Inside the tab, there is a section for "Interface:" with a dropdown menu showing "vlan-10". Below this, there are two checked checkboxes: "Use Peer DNS" and "Use Peer NTP". Further down, there is a section for "Add Default Route:" with a dropdown menu showing "yes". On the right side of the window, there is a vertical stack of buttons: "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", "Remove", "Release", and "Renew". At the bottom of the window, there are two status indicators: "enabled" and "Status: bound".

VLAN

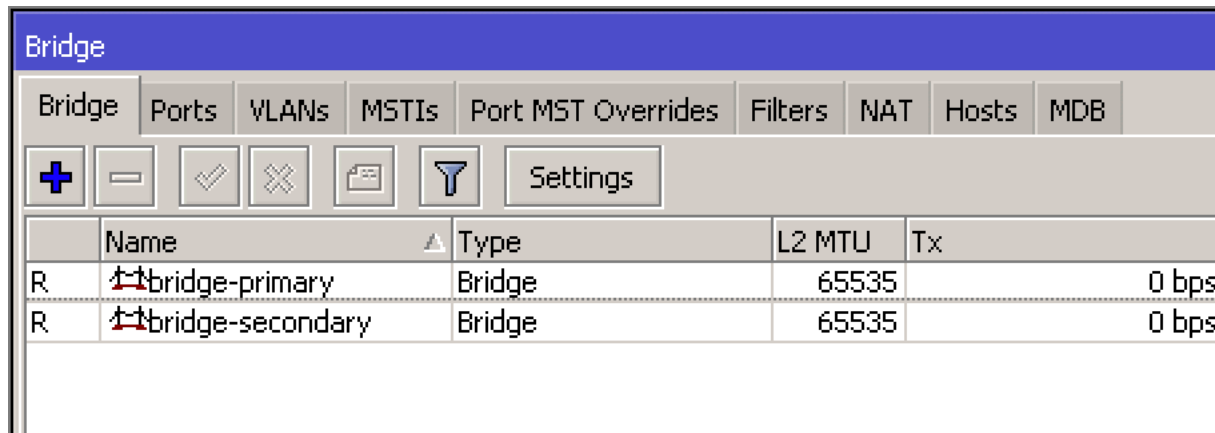
Sprzętowe wsparcie na bridge-u

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]	+	-	-	-	-	-	-

https://wiki.mikrotik.com/wiki/Manual:Interface/Bridge#Bridge_Hardware_Offloading

VLAN

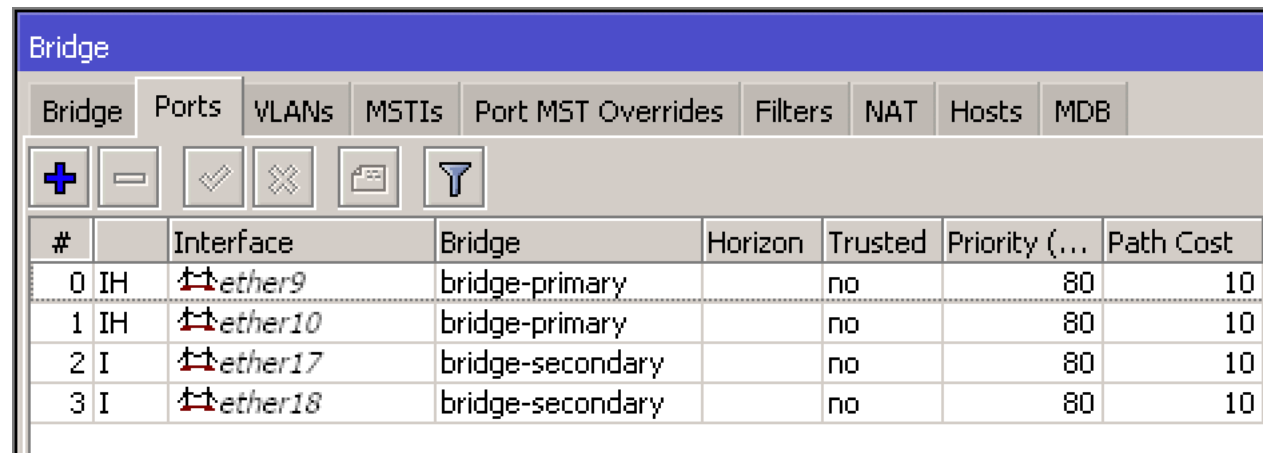
Wiele bridge-ów na jednym urządzeniu serii 3xx



	Name	Type	L2 MTU	Tx
R	bridge-primary	Bridge	65535	0 bps
R	bridge-secondary	Bridge	65535	0 bps

Stworzymy dwa bridge-a:
bridge-primary
bridge-secondary

Wsparcie sprzętowe jest
wyłącznie dla pierwszego stworzonego
bridge-a !!! *bridge-primary*



#	Interface	Bridge	Horizon	Trusted	Priority (...)	Path Cost
0 IH	ether9	bridge-primary		no	80	10
1 IH	ether10	bridge-primary		no	80	10
2 I	ether17	bridge-secondary		no	80	10
3 I	ether18	bridge-secondary		no	80	10

Koniec

Konfiguracje oraz prezentacja dostępne tu:

<https://ua.mwtc.pl/mbum/>



Kontakt do mnie:
e-mail: ihor@mwtc.pl