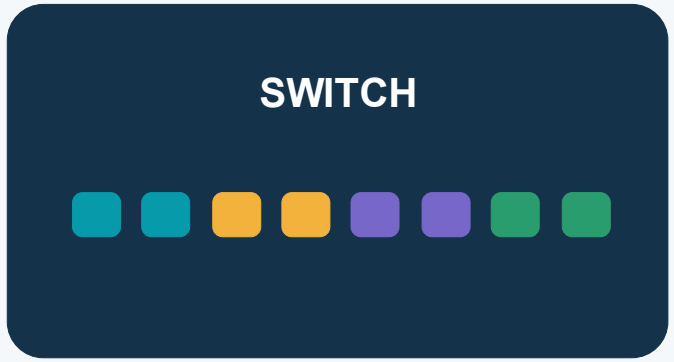
MBUM#11 · POZNAŃ · 1 PAŹDZIERNIKA 2026

VLAN

temat znany, ale czy każdy go zna?

Od ramki 802.1Q do bezpiecznej konfiguracji
Bridge VLAN Filtering w RouterOS



10 20 99

trzy VLAN-y
jeden przełącznik

Michał Filipek
MWTC

O PRELEGENCIE

Michał Filipek



MWTC

CZYM SIĘ ZAJMUJĘ

01 Sieci IP i RouterOS

projektowanie · routing · switching

02 Monitoring Zabbix

wdrożenia · integracje · observability

03 Linux i automatyzacja

administracja · skrypty · usługi

04 Wi-Fi, VoIP i HA

audyty · wdrożenia · wsparcie

szkolenia · wdrożenia · audyty · doradztwo

Jeden przełącznik, kilka domen warstwy drugiej

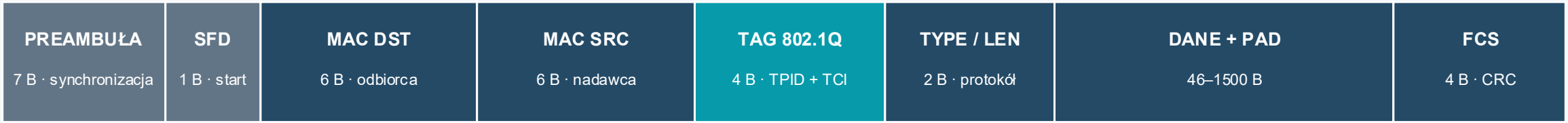
VLAN rozdziela ruch L2 według identyfikatora, mimo że urządzenia korzystają z tej samej infrastruktury fizycznej.



Komputery wysyłają ramki bez tagu. Switch przypisuje VLAN przez PVID; tag pojawia się dopiero na trunku do routera.

Ramka Ethernet z tagiem IEEE 802.1Q

Znacznik ma 4 bajty i jest wstawiany między adres źródłowy a pole EtherType/Length. Schemat nie jest w skali.



4 BAJTY ZNACZNIKA 802.1Q

TPID
16 bitów

0x8100 — informacja, że dalej znajduje się tag VLAN

PCP
3 bity

priorytet 802.1p: wartości 0–7

DEI
1 bit

ramkę można preferencyjnie odrzucić

VID
12 bitów

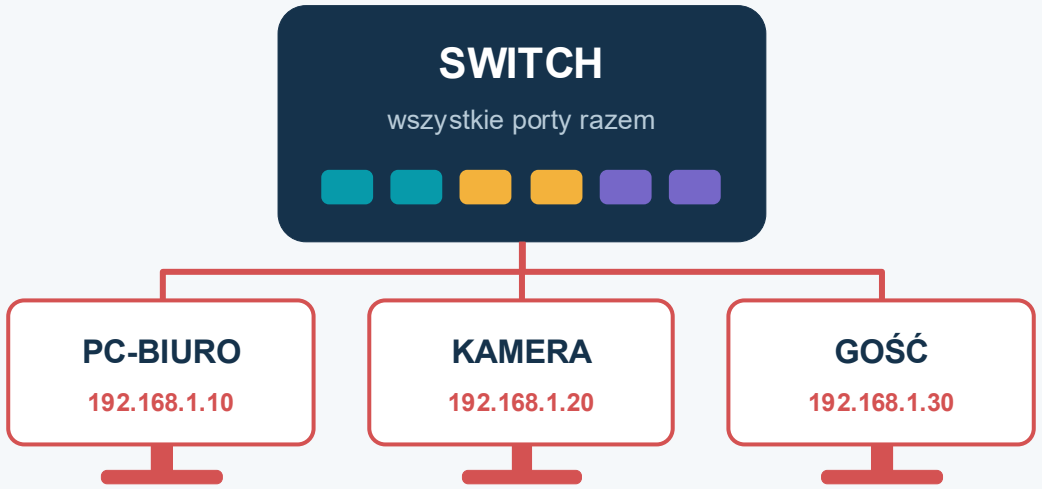
VLAN ID: 1–4094; 0 i 4095 mają znaczenie specjalne

Tag zwiększa ramkę o 4 B. Nie szyfruje danych i nie uwierzytelnia nadawcy — tylko niesie priorytet oraz identyfikator domeny VLAN.

Po co są VLAN-y? Segmentacja zamiast jednej płaskiej sieci

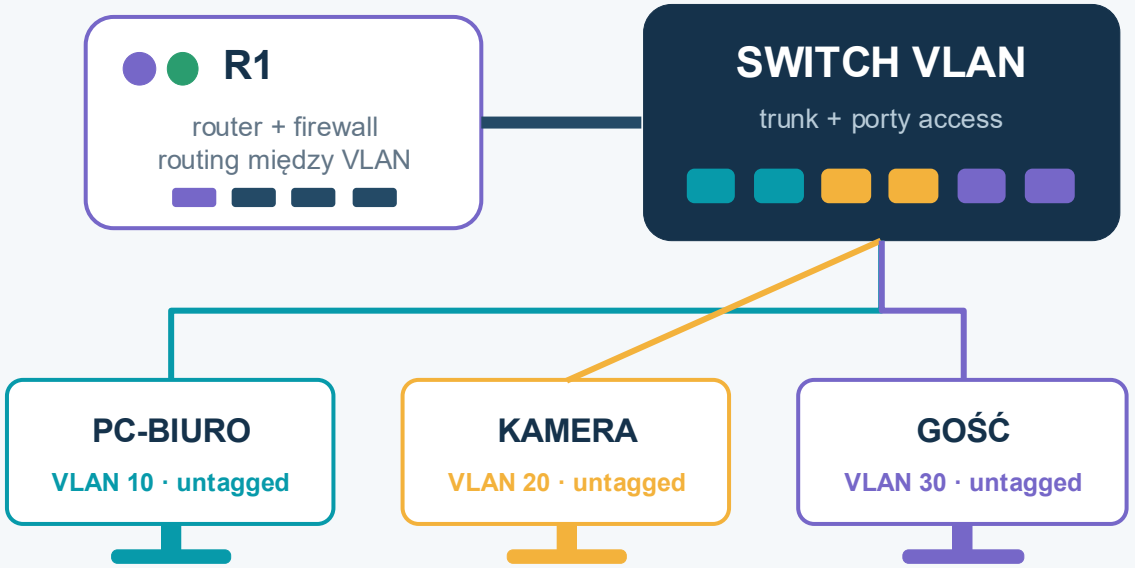
VLAN-y dzielą jedną infrastrukturę fizyczną na kontrolowane domeny rozgłoszeniowe i granice polityki.

BEZ VLAN-ÓW · JEDNA DOMENA L2



broadcast dociera wszędzie · urządzenia widzą się bez routingu · trudniej egzekwować politykę

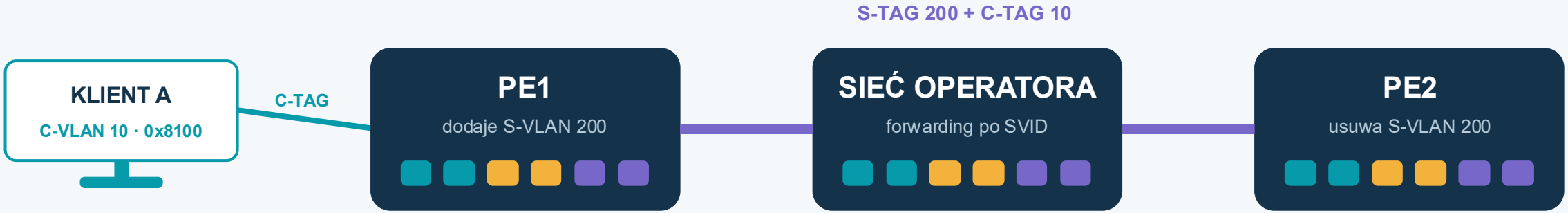
Z VLAN-AMI · SEGMENTACJA



mniej broadcastów · osobne podsieci · komunikacja między segmentami tylko przez router i firewall

QinQ oraz inne warianty VLAN

QinQ przenosi ramkę klienta z tagiem C-VLAN wewnątrz dodatkowego tagu operatorskiego S-VLAN.



802.1Q · C-VLAN

TPID 0x8100

Pojedynczy tag w sieci LAN; zwykłe access i trunk.

802.1ad · QinQ

S-TAG 0x88A8 + C-TAG

Operator rozdziela klientów po SVID, zachowując ich CVID.

CVID stacking

0x8100 nad 0x8100

Dwa tagi klienta; funkcja podobna do QinQ, lecz bez S-TAG.

Klasyfikacja VLAN

port / MAC / protokół

Sposób przypisania ramki do VID zależy od switch chipa.

RouterOS sprawdza zewnętrzny tag. Dla 802.1ad ustaw ether-type=0x88A8; sprzętowy offload S-TAG zależy od układu.

PRZYKŁAD OPERATORA

Po co stosuje się QinQ?

Operator może przenieść wiele VLAN-ów klienta między lokalizacjami, dodając jeden własny identyfikator S-VLAN.



01 Łączenie lokalizacji

Ta sama domena L2 może działać w oddziałach A i B.

02 Powtarzalne CVID

Różni klienci mogą używać u siebie tych samych VLAN ID.

03 Izolacja klientów

Operator przełącza po własnym SVID, a tagi klienta pozostają wewnątrz.

04 Prostszy rdzeń

Sieć operatorska nie musi znać każdego VLAN-u używanego przez klienta.

Koszt: dodatkowe 4 B, wymagana odpowiednia MTU i zgodność sprzętu z 0x88A8 / hardware offload.

Access, trunk i hybrid opisują zachowanie portu

ACCESS

WEJŚCIE

ramka bez tagu

DECYZJA

PVID nadaje VLAN

WYJŚCIE

bez tagu

TRUNK

WEJŚCIE

ramka z tagiem

DECYZJA

VID na liście portu

WYJŚCIE

z tagiem

HYBRID

WEJŚCIE

tagowana lub bez tagu

DECYZJA

PVID + dozwolone VID

WYJŚCIE

według tabeli

Nazwy pomagają w rozmowie. Konfigurację określają PVID, frame-types oraz członkostwo tagged / untagged.

MODEL PRZEPŁYWU

Ramka przechodzi przez trzy decyzje

1 WEJŚCIE

Czy typ ramki jest dozwolony?
Czy port należy do danego VLAN-u?

frame-types + ingress-filtering

2 PRZEŁĄCZANIE

Nauka MAC odbywa się osobno dla VLAN-u.
Decyzja dotyczy konkretnego VID.

bridge host table + VID

3 WYJŚCIE

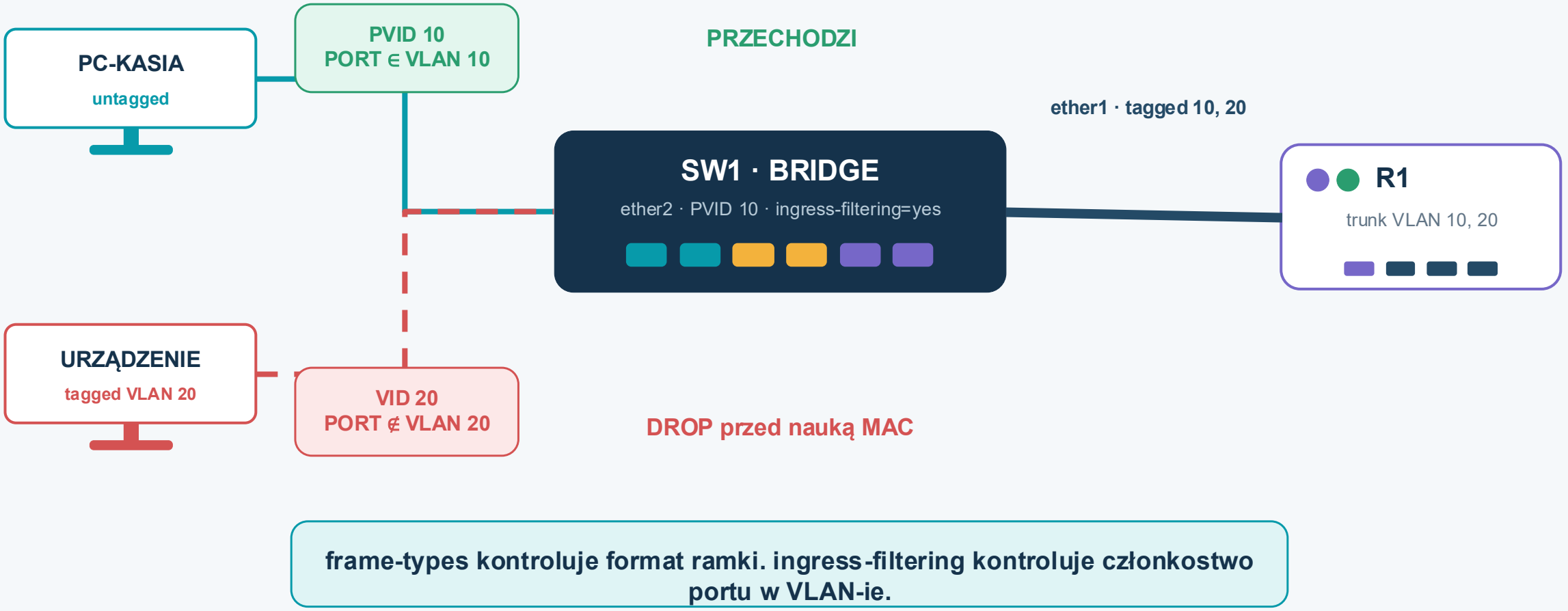
Czy port może przenieść ten VLAN?
Tag zostaje albo znika.

bridge VLAN table

PVID nadaje VLAN ramce bez tagu na wejściu. Nie jest listą VLAN-ów dozwolonych na porcie.

Ingress filtering: kontrola VLAN-u na wejściu

Port przyjmuje ramkę tylko wtedy, gdy po klasyfikacji należy do wskazanego VLAN-u.



frame-types kontroluje format ramki. ingress-filtering kontroluje członkostwo portu w VLAN-ie.

Ingress filtering: konfiguracja i konsekwencje

ROUTEROS CLI

```
/interface bridge port
set [find interface=ether1] \
   frame-types=admit-only-vlan-tagged \
   ingress-filtering=yes

set [find interface=ether2] pvid=10 \
   frame-types=admit-only-untagged-and-priority-tagged \
   ingress-filtering=yes

/interface bridge vlan
add bridge=bridge1 vlan-ids=10 \
   tagged=ether1 untagged=ether2
```

INGRESS-FILTERING=YES

- obcy VID jest odrzucany na wejściu
- trunk działa jak jawna lista dozwolonych VLAN-ów
- błąd w tabeli VLAN może odciąć poprawny ruch

INGRESS-FILTERING=NO

- port może wprowadzić tagged VLAN, którego nie ma na liście
- egress filtering nadal ogranicza port wyjściowy
- łatwo o niezamierzony dostęp i ruch asymetryczny

DWIE ROLE

VLAN na switchu i VLAN na routerze

Ta sama liczba VLAN oznacza inną pracę w warstwie drugiej i inną w warstwie trzeciej.

SWITCH L2

WEJŚCIE
tag lub PVID

SWITCH CHIP
MAC + VID

WYJŚCIE
tagged / untagged

bez zmiany adresów IP i bez decyzji firewalla

ROUTER L3

VLAN IF
brama IP

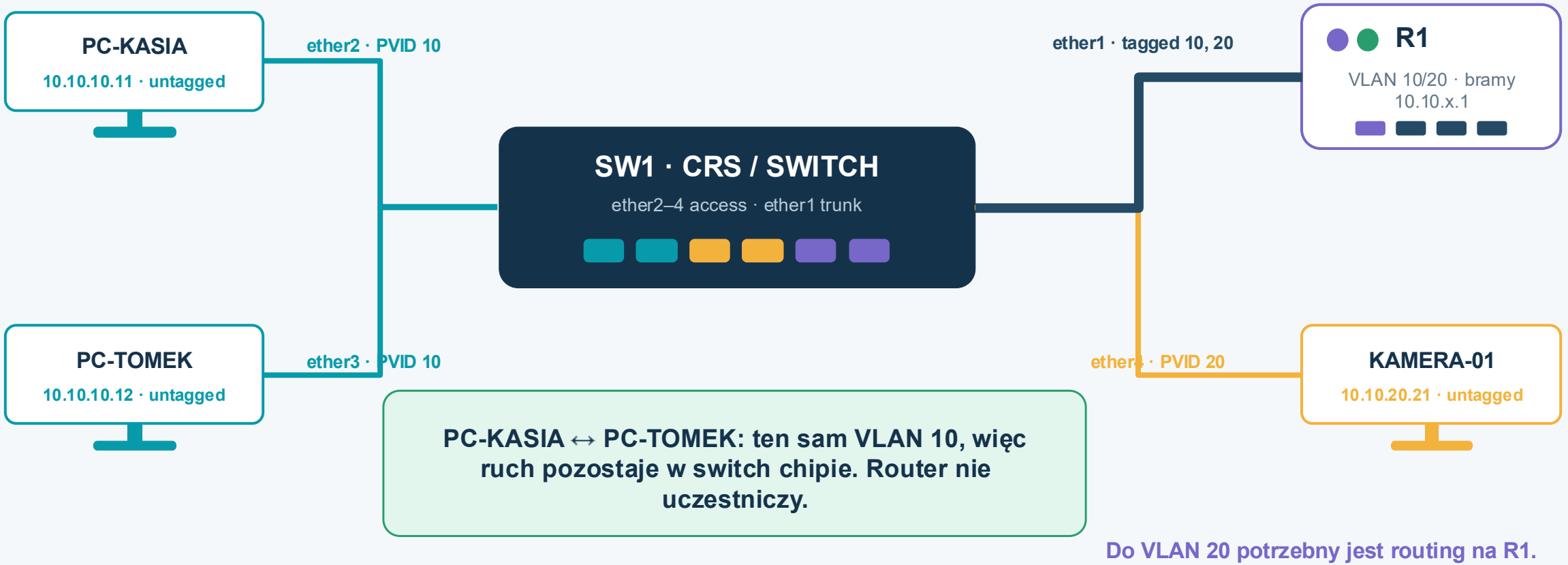
ROUTING
tablica tras + firewall

WYJŚCIE L3
inny VLAN lub WAN

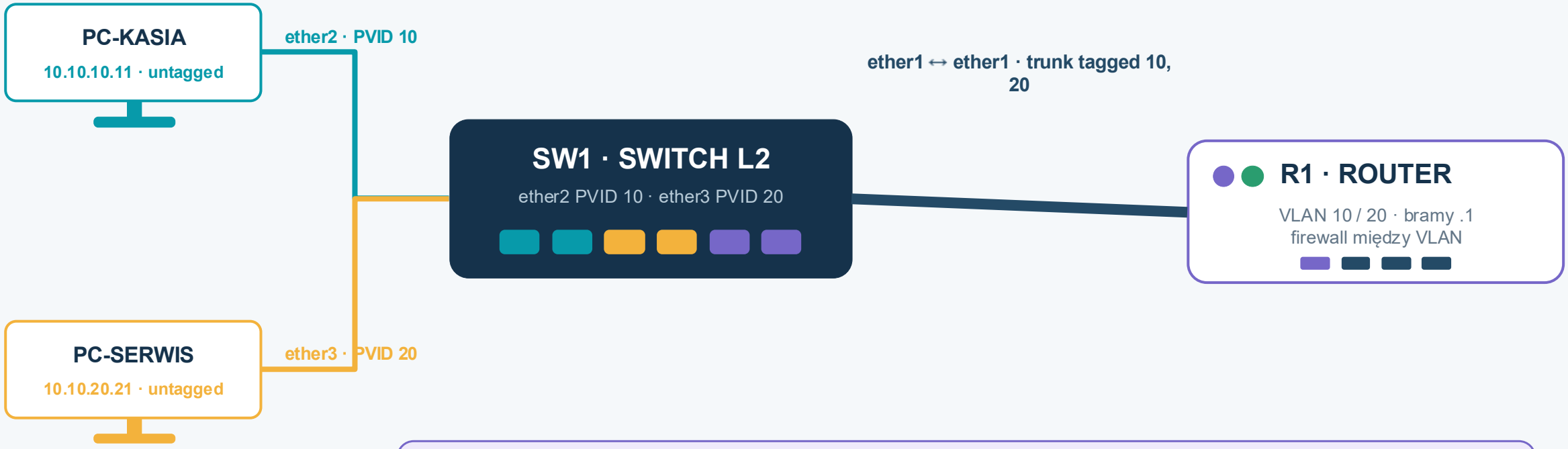
Pytanie kontrolne

Czy ramka ma tylko przejść przez urządzenie, czy urządzenie ma być jej bramą IP?

VLAN na switchu: ruch pozostaje w warstwie drugiej



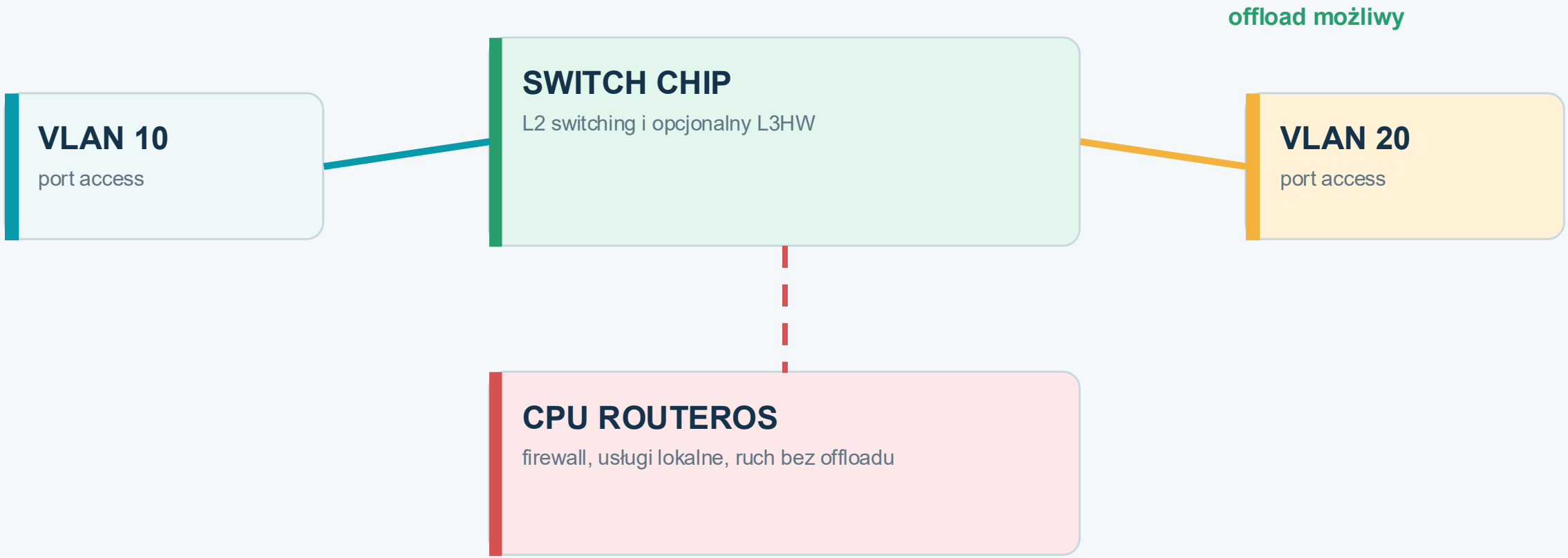
Router-on-a-stick: tag kończy się na interfejsie VLAN



PC-KASIA wysyła untagged → SW1 nadaje VID 10 → trunk niesie tag 10 → R1 routuje → ramka wraca z tagiem 20 → SW1 usuwa tag na ether3.

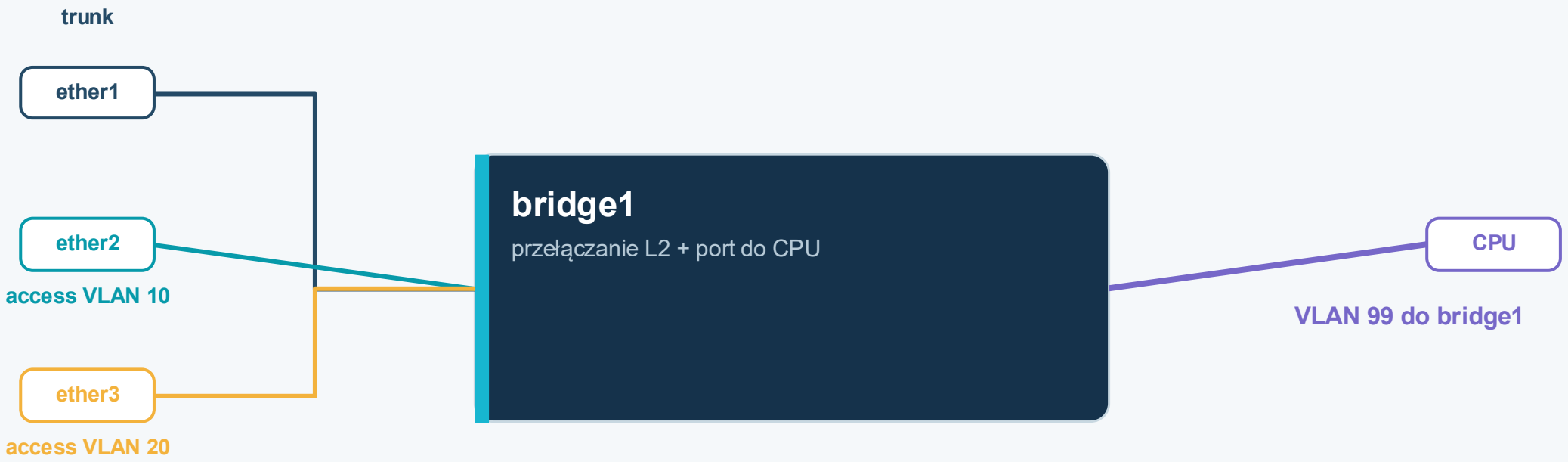
CRS może przełączać L2 i routować L3

Jedna obudowa nie oznacza jednej ścieżki przetwarzania.



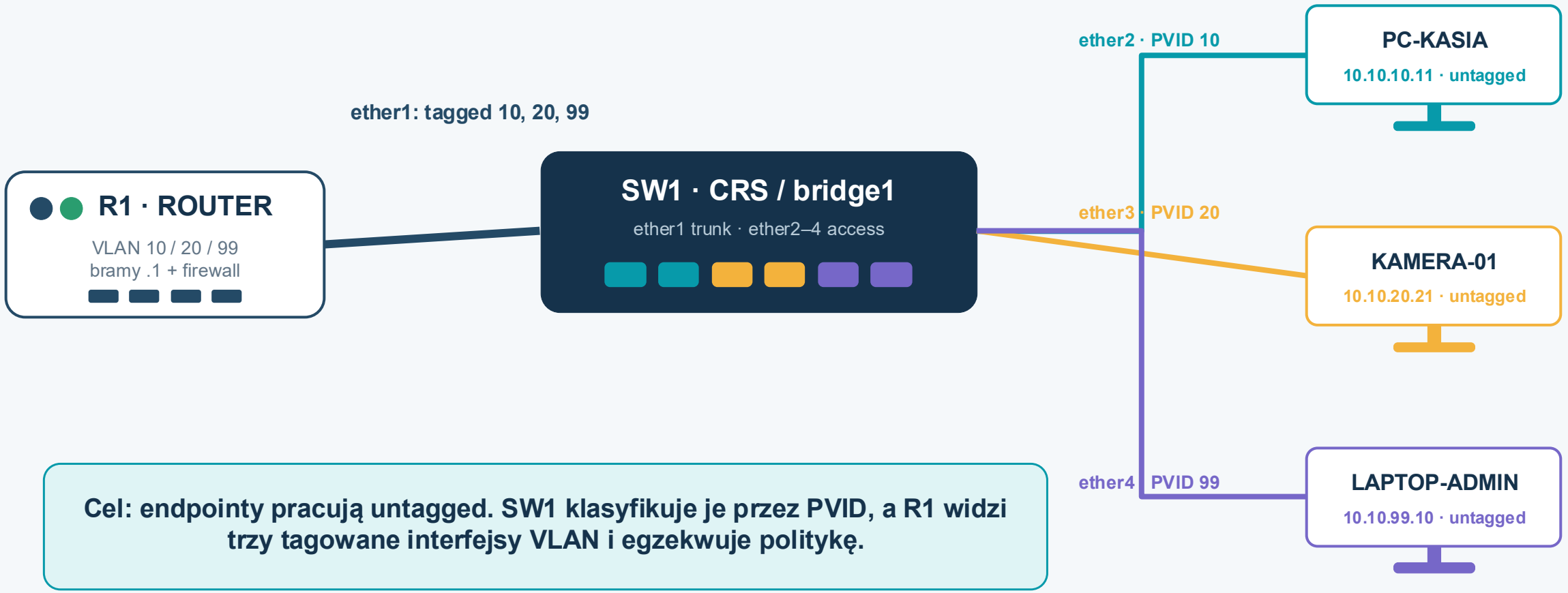
ruch do CPU tylko wtedy, gdy funkcja lub polityka tego wymaga

Bridge jest także portem do CPU



Jeżeli router ma terminować VLAN, zapewniać management przełącznika albo routować między VLAN-ami, bridge musi mieć dostęp do właściwego VID.

Topologia demonstracyjna



Cel: endpointy pracują untagged. SW1 klasyfikuje je przez PVID, a R1 widzi trzy tagowane interfejsy VLAN i egzekwuje politykę.

Najpierw bridge i role portów

ROUTEROS CLI

```
/interface bridge
add name=bridge1 vlan-filtering=no

/interface bridge port
add bridge=bridge1 interface=ether1 \
    frame-types=admit-only-vlan-tagged
add bridge=bridge1 interface=ether2 pvid=10 \
    frame-types=admit-only-untagged-and-priority-tagged
add bridge=bridge1 interface=ether3 pvid=20 \
    frame-types=admit-only-untagged-and-priority-tagged
add bridge=bridge1 interface=ether4 pvid=99 \
    frame-types=admit-only-untagged-and-priority-tagged
```

DLACZEGO W TEJ KOLEJNOŚCI

1. **Filtrowanie pozostaje wyłączone podczas budowy tabeli.**
2. **PVID opisuje VLAN dla ruchu bez tagu na wejściu.**
3. **frame-types ogranicza format ramek przyjmowanych przez port.**

PVID zacznie działać dopiero po włączeniu vlan-filtering.

Tabela VLAN i tag na wyjściu

ROUTEROS CLI

```
/interface bridge vlan
add bridge=bridge1 vlan-ids=10 \
   tagged=ether1 untagged=ether2
add bridge=bridge1 vlan-ids=20 \
   tagged=ether1 untagged=ether3
add bridge=bridge1 vlan-ids=99 \
   tagged=bridge1,ether1 untagged=ether4
```

VID	TAGGED	UNTAGGED
10	ether1	ether2
20	ether1	ether3
99	bridge1, ether1	ether4

Nie łącz wielu VLAN ID w jednym wpisie z portami access. Możesz niechcący dopuścić oba VLAN-y na obu portach.

MVRP automatyzuje członkostwo VLAN na trunkach

Switche deklarują potrzebne VLAN-y, a sąsiedzi dynamicznie rejestrują porty tagged na właściwej ścieżce.



AUTOMATYCZNIE

członkostwo tagged na portach trunk

STATYCZNIE

PVID i porty access pozostają konfiguracją administratora

WARUNEK

vlan-filtering=yes i port w stanie forwarding

MVRP nie tworzy interfejsów VLAN, adresów IP ani routingu.

MVRP: konfiguracja, monitoring i granica zaufania

ROUTEROS CLI

```
/interface bridge
set bridge1 vlan-filtering=yes mvrp=yes

/interface bridge port
set [find interface=ether1] \
    mvrp-applicant-state=normal-participant \
    mvrp-registrar-state=normal

# port do niezaufanej sieci
set [find interface=ether5] \
    mvrp-applicant-state=non-participant \
    mvrp-registrar-state=fixed

/interface bridge vlan
set [find vlan-ids=20] mvrp-forbidden=ether5

/interface bridge port monitor [find]
```

REGISTRAR

IN	VLAN zarejestrowany
LV	rejestracja wygasa
MT	VLAN niezarejestrowany

Dostęp management przed włączeniem filtrowania

ROUTEROS CLI

```
/interface vlan
add name=vlan99-mgmt interface=bridge1 vlan-id=99

/ip address
add address=10.10.99.2/24 interface=vlan99-mgmt

# sprawdź tabelę, porty i drogę awaryjną
/interface bridge vlan print
/interface bridge port print

/interface bridge
set bridge1 vlan-filtering=yes
```

PRZED OSTATNIĄ KOMENDĄ

1. bridge1 należy do VLAN 99 jako tagged
2. trunk przenosi VLAN management
3. adres i firewall pozwalają wejść z właściwej sieci
4. masz konsolę, port ratunkowy albo Safe Mode

Po zmianie sprawdź management i ruch VLAN-ów.

PORÓWNANIE

CRS3xx, CRS1xx/2xx i pozostałe urządzenia

Najważniejsza różnica to miejsce konfiguracji VLAN i możliwość zachowania sprzętowego przełączania.

Cecha	CRS3xx / CRS4xx / CRS5xx	CRS1xx / CRS2xx	Inne RouterBOARD
Konfiguracja VLAN	Bridge VLAN Filtering	/interface ethernet switch	Zależnie od switch chipa
L2 HW offload	Tak, z Bridge VLAN Filtering	Tak, przez /interface ethernet switch	Zależnie od switch chipa i użytych funkcji
Bridge vlan-filtering	Działa w sprzęcie na wspieranych CRS	Działa programowo; wire speed wymaga switch chip	Działa programowo; HW tylko na wspieranych chipach
Routing między VLAN	CPU lub L3HW na wybranych modelach	CPU	Zwykle CPU
Typowa pułapka	Brak H lub zły dostęp do CPU	Konfiguracja jak CRS3xx	Założenie, że każdy chip działa tak samo

Najpierw sprawdź model i switch chip. Dopiero potem wybierz składnię.

CRS3xx: jeden bridge i Bridge VLAN Filtering

ROUTEROS CLI

```
/interface bridge
add name=bridge1 vlan-filtering=no

/interface bridge port
add bridge=bridge1 interface=ether1 \
   frame-types=admit-only-vlan-tagged
add bridge=bridge1 interface=ether2 pvid=10 \
   frame-types=admit-only-untagged-and-priority-tagged
add bridge=bridge1 interface=ether3 pvid=20 \
   frame-types=admit-only-untagged-and-priority-tagged

/interface bridge vlan
add bridge=bridge1 tagged=ether1 untagged=ether2 vlan-ids=10
add bridge=bridge1 tagged=ether1 untagged=ether3 vlan-ids=20

/interface bridge set bridge1 vlan-filtering=yes
```

CZEGO OCZEKUJESZ

H	na portach bridge
1	jeden bridge korzystający z HW
L2	ruch 10 i 20 pozostaje w SWITCH CHIP
CPU	tylko management lub routing

Dodaj bridge1 do tagged tylko dla VLAN-ów, które mają trafić do CPU.

CRS1xx/2xx: VLAN-y w switch chip

ROUTEROS CLI

```
/interface ethernet switch ingress-vlan-translation
add ports=ether2 customer-vid=0 new-customer-vid=10
add ports=ether3 customer-vid=0 new-customer-vid=20
add ports=ether4 customer-vid=0 new-customer-vid=99

/interface ethernet switch egress-vlan-tag
add tagged-ports=ether1 vlan-id=10
add tagged-ports=ether1 vlan-id=20
add tagged-ports=ether1,switch1-cpu vlan-id=99

/interface ethernet switch vlan
add ports=ether1,ether2 vlan-id=10
add ports=ether1,ether3 vlan-id=20
add ports=ether1,ether4,switch1-cpu vlan-id=99

/interface ethernet switch
set drop-if-invalid-or-src-port-not-member-of-vlan-on-ports=    ether1,ether2,ether3,ether4
```

KOLEJNOŚĆ MA ZNACZENIE

Porty są wcześniej dodane do jednego bridge z hw=yes.

1 · INGRESS

Untagged z portu access otrzymuje VID.

2 · EGRESS

Trunk oraz CPU dla VLAN 99 wysyłają tag.

3 · MEMBERSHIP

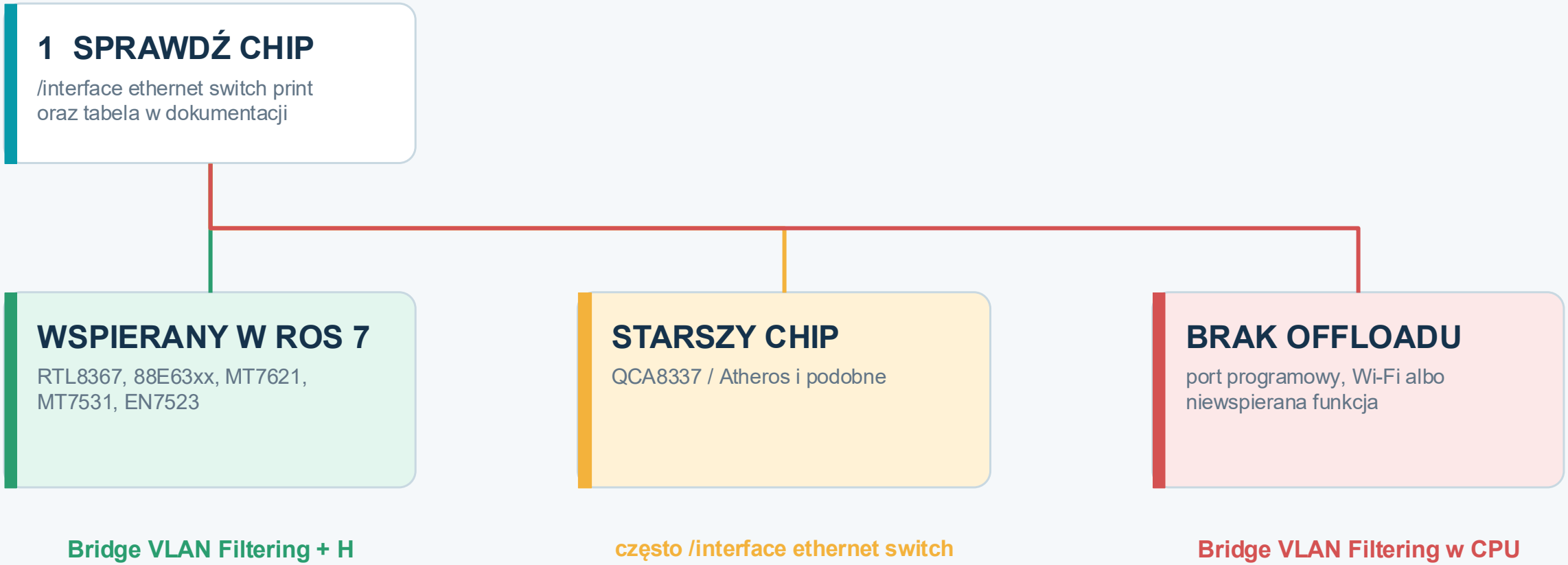
Tabela VLAN określa dozwolone porty.

4 · FILTERING

Odrzucanie nieprawidłowych VLAN-ów włącz na końcu.

Dobór konfiguracji według switch chipa

RouterBOARD nie jest jedną rodziną przełączników. Ten sam RouterOS może prowadzić do innej ścieżki sprzętowej.



Pięć pułapek, które wyglądają niewinnie

01	**PVID traktowany jak allowlist**	PVID klasyfikuje ruch bez tagu. Członkostwo portu określa tabela VLAN.
02	**Kilka VID przy portach access**	Jedna skrócona reguła może dopuścić VLAN-y do niewłaściwych portów.
03	**VLAN management trafia do CPU bez kontroli**	Dopuszczenie bridge1 wymaga później ograniczenia usług przez firewall.
04	**Native VLAN nie zgadza się po obu stronach trunku**	Ramka bez tagu wpada do innej domeny niż zakłada operator.
05	**Brak H przy porcie**	Ruch może przejść przez CPU, obniżając przepustowość i zwiększając użycie procesora.

Diagnostyka

SPRAWDŹ NA URZĄDZENIU

```
/interface bridge vlan print detail
/interface bridge port print detail
/interface bridge host print where !local
/interface bridge port monitor [find]

/tool torch interface=ether1
/tool sniffer quick interface=ether1
```

PYTANIA DO KAŻDEJ RAMKI

- **A** Z którego portu weszła i czy miała tag?
- **B** Jaki VID widzi bridge po klasyfikacji?
- **C** Na których portach ten VID jest dozwolony?
- **D** Czy na wyjściu tag ma zostać czy zniknąć?

Sukces to zgodność stanu z intencją: port, VID, tag i oczekiwany kierunek ruchu.

Ścieżka sprzętowa i CPU

HARDWARE OFFLOAD

port ma flagę H
ruch przełącza switch chip

wire speed

SOFTWARE FORWARDING

brak H
ruch może obciążać CPU

wysokie CPU · niższa przepustowość

Sprawdź model urządzenia, switch chip i tabelę zgodności. Nie zakładaj, że każdy RouterBOARD zachowa się jak CRS3xx.

Test akceptacyjny dla małej sieci

Sprawdzaj dozwolone i zabronione ścieżki. Sam ping w jednym VLAN-ie nie wystarczy.

01	PC → brama VLAN 10	MA DZIAŁAĆ
02	Kamera → brama VLAN 20	MA DZIAŁAĆ
03	PC → kamera	TYLKO ZGODNIE Z FIREWALLEM
04	PC → management SW1	MA BYĆ ZABLOKOWANE
05	Admin → management SW1	MA DZIAŁAĆ
06	Nieznany VID na trunku	MA BYĆ ODRZUCONY

Po teście zapisz wynik i konfigurację. Następna zmiana powinna zaczynać się od znanego punktu odniesienia.

Dobry VLAN zaczyna się od dobrej mapy ramek

01 PVID klasyfikuje ruch bez tagu na wejściu.

02 Tabela VLAN określa członkostwo portów i tag na wyjściu.

03 bridge1 jest także portem do CPU.

04 ingress-filtering i frame-types ograniczają niepożądany ruch.

05 Wydajność zależy od sprzętu i obecności flagi H.

Pytania?

MWTC

mwtc.pl

SZKOLENIA MIKROTIK

mwtc.pl/szkolenia-mikrotik.php