Przełączniki: L2 i L3, tablica MAC, VLAN, LACP i STP

Poziom: średnio

Dotyczy: przełączniki zarządzalne L2 i L3, IEEE 802.1Q, 802.1AX, 802.1D i 802.1w, LLDP, FortiGate fw01

Czas: ~70 min

Przełącznik przekazuje ramki Ethernetu tylko do portu, za którym siedzi odbiorca, a sieci VLAN pozwalają zbudować kilka osobnych sieci na tym samym sprzęcie. Wyjaśniamy tablicę adresów MAC, trunki 802.1Q, agregację LACP, drzewo rozpinające i zarządzanie przełącznikiem w sieci VLAN 98. Proponujemy też podział na przełączniki sw01 do sw04 i sw-mag01 dla Zielonej, do zatwierdzenia przez autora bazy.

ZAŁOŻENIA SCENARIUSZA

magazyn w Swarzędzu jest podłączony do sieci centrali: `sw-mag01` należy do tych samych VLAN-ów (30 i 98), a trasuje je wyłącznie pojedynczy `fw01` (brama 10.20.30.1), bez osobnego routera. Zapora łączy się z rdzeniem `sw01` i `sw02` agregacją dwóch łączy. Wariant z osobną lokalizacją i routerem `rtr-mag01`: IPsec site-to-site: Pamiątkowo i Swarzędz między FortiGate a routerem innej firmy.

Skróty użyte na tej stronie (28)

Skrót	Co znaczy
BMC	Baseboard Management Controller: osobny malutki komputer na płycie serwera, który działa nawet przy wyłączonym serwerze i odczytuje m.in. temperatury czujników
BPDU	Bridge Protocol Data Unit: komunikat, który przełączniki wymieniają w protokole drzewa rozpinającego, żeby wybrać most główny i zablokować zbędne połączenia; ochrona BPDU wyłącza port brzegowy, na którym taki komunikat się pojawi
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
DEI	Drop Eligible Indicator: jeden bit w znaczniku 802.1Q, którym oznaczamy ramki, które można odrzucić przy przeciążeniu
EPEL	Extra Packages for Enterprise Linux: dodatkowe repozytorium pakietów dla RHEL i klonów

Skrót	Co znaczy
HTTP	Hypertext Transfer Protocol: protokół stron WWW
IEEE	Institute of Electrical and Electronics Engineers: międzynarodowa organizacja inżynierów, która m.in. wydaje normy i przyznaje kamienie milowe w historii techniki
IP	Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)
LACP	Link Aggregation Control Protocol: protokół z normy IEEE 802.1AX, w którym dwa urządzenia uzgadniają łączenie kilku kabli w jedno łącze logiczne; jedna sesja zostaje zawsze na jednym kablu
LBFO	Load Balancing and Failover: starszy zespół kart sieciowych Windows, który zastępuje w Hyper-V zespół SET, a w odróżnieniu od SET obsługuje LACP
LLDP	Link Layer Discovery Protocol: protokół, którym sąsiednie urządzenia sieciowe opowiadają sobie o sobie
MAC	Media Access Control: unikalny adres fizyczny karty sieciowej, przypisany fabrycznie
MC-LAG	Multi-Chassis Link Aggregation Group: agregacja łączy do dwóch osobnych przełączników, która działa jak jeden przełącznik dla serwera
PCP	Priority Code Point: trzy bity priorytetu w znaczniku 802.1Q, według których przełącznik może szybciej przepuszczać ważniejsze ramki
PN-EN	Polska Norma będąca wersją normy europejskiej, np. PN-EN 54 dla elementów systemów sygnalizacji pożaru
PoE	Power over Ethernet: zasilanie urządzenia tym samym kablem sieciowym, którym płyną dane
RADIUS	Remote Authentication Dial-In User Service: standardowy protokół pytania serwera, czy podane konto i hasło są poprawne
RSTP	Rapid Spanning Tree Protocol: szybka wersja drzewa rozpinającego z normy IEEE 802.1w, która po awarii łącza przebudowuje drzewo w kilka sekund zamiast 30 do 50 sekund w klasycznym STP
SET	Switch Embedded Teaming: zespół kart sieciowych zbudowany w przełączniku wirtualnym Hyper-V; łączy dwie karty w jedno łącze bez ustawień po stronie przełącznika fizycznego, więc bez LACP
SNMP	Simple Network Management Protocol: protokół odczytu stanu urządzeń sieciowych
SSH	Secure Shell: szyfrowane zdalne logowanie do serwera
SSID	Service Set Identifier: nazwa sieci Wi-Fi, którą widzą użytkownicy, na przykład Zielona-Biuro; jeden punkt dostępowy może rozgłaszać kilka SSID, każdy w innym VLAN-ie
STP	Spanning Tree Protocol: protokół drzewa rozpinającego, który wyłącza zbędne połączenia między przełącznikami, żeby ramki nie krążyły w pętli
TCP	Transmission Control Protocol: protokół sieciowy z potwierdzaniem dostarczenia
UDP	User Datagram Protocol: szybki protokół sieciowy bez potwierdzeń

Skrót	Co znaczy
UniFi	linia sprzętu Ubiquiti do sieci firmowych i domowych: punkty dostępowe Wi-Fi, przełączniki i bramy, zarządzana z aplikacji UniFi Network
VLAN	Virtual LAN: wydzielona logicznie sieć na tym samym sprzęcie
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej

Fiszka

Komendy przełączników różnią się między producentami. Zapora w Zielonej to FortiGate, więc pierwsze przykłady pochodzą ze składni FortiSwitch i FortiOS, a pozostałe z Linuksa i Windowsa. Jeśli kupimy przełączniki innego producenta, te same dane znajdziemy pod innymi nazwami poleceń, które sprawdzamy w jego dokumentacji.

□□ TYLKO ODCZYT

Odczyt tablicy MAC przełącznika: diagnose switch mac-address list

```
diagnose switch mac-address list
diagnose switch mac-address list | grep AdresMac
```

> (gdzie `AdresMac` to fragment szukanego adresu w zapisie przełącznika; polecenie działa na samodzielnym FortiSwitch, a według forum Fortinet opcja `grep` zależy od wersji oprogramowania [9])

Wynik zawiera adres MAC, numer VLAN i port, na którym przełącznik go nauczył. Brak wpisu oznacza, że urządzenie milczy albo stoi za innym portem, niż sądzimy. Układ kolumn sprawdzamy w dokumentacji naszej wersji, bo nie podajemy go z pamięci.

□□ **MAC** = Media Access Control: unikalny adres fizyczny karty sieciowej, przypisany fabrycznie · **VLAN** = Virtual LAN: wydzielona logicznie sieć na tym samym sprzęcie

□□ TYLKO ODCZYT

Odczyt sąsiadów LLDP przełącznika zarządzanego z FortiGate: switch-info lldp

```
diagnose switch-controller switch-info lldp neighbors-summary NumerSeryjnySwitcha
diagnose switch-controller switch-info lldp neighbors-detail NumerSeryjnySwitcha
NumerPortu
```

> (gdzie `NumerSeryjnySwitcha` to numer seryjny przełącznika zarządzanego przez zaporę, a `NumerPortu` to port, o którego sąsiada pytamy [8])

LLDP = Link Layer Discovery Protocol: protokół, którym sąsiednie urządzenia sieciowe opowiadają sobie o sobie

TYLKO ODCZYT

Odczyt stanu agregacji i drzewa rozpinającego: switch-info trunk i stp

```
diagnose switch-controller switch-info trunk status NumerSeryjnySwitcha
diagnose switch-controller switch-info stp NumerSeryjnySwitcha NumerInstancji
```

> (gdzie `NumerInstancji` to numer instancji drzewa, zwykle 0; pierwsze polecenie pokazuje porty aktywne i nieaktywne oraz tryb LACP, drugie priorytet mostu, most główny i stan każdego portu [8])

LACP = Link Aggregation Control Protocol: protokół z normy IEEE 802.1AX, w którym dwa urządzenia uzgadniają łączenie kilku kabli w jedno łącze logiczne; jedna sesja zostaje zawsze na jednym kablu

TYLKO ODCZYT

Odczyt sąsiadów LLDP w Linuksie: lldpcli show neighbors

```
sudo lldpcli show neighbors ports NazwaKarty details
```

> (gdzie `NazwaKarty` to nazwa interfejsu, na przykład `eno1`; demon `lldpd` musi działać, a pakiet na Rocky Linux 9 pochodzi prawdopodobnie z repozytorium EPEL, co do potwierdzenia [10])

Przykład (poglądowy, hana01 w szafie R4):

```
-------------------------------------------------------------------------------
LLDP neighbors:
-------------------------------------------------------------------------------
Interface:    eno1, via: LLDP, RID: 1, Time: 0 day, 02:10:43
  Chassis:
    ChassisID:    mac aa:bb:cc:dd:ee:03
    SysName:      sw02
    MgmtIP:       10.20.98.3
  Port:
    PortID:       ifname port12
    PortDescr:    hana01-eno1
```

Z takiego wyniku odczytujemy, w który port którego przełącznika wpięta jest karta, bez chodzenia do szafy.

LLDP = Link Layer Discovery Protocol: protokół, którym sąsiednie urządzenia sieciowe opowiadają sobie o sobie · **EPEL** = Extra Packages for Enterprise Linux: dodatkowe repozytorium pakietów dla RHEL i klonów · **lldpcli** = lldpcli: klient demona lldpd, polecenie lldpcli show neighbors pokazuje, z jakim portem którego przełącznika jest połączona karta sieciowa

TYLKO ODCZYT

Odczyt stanu agregacji w Linuksie: /proc/net/bonding

```
cat /proc/net/bonding/NazwaBondu
```

> (gdzie `NazwaBondu` to nazwa interfejsu agregującego, na przykład `bond0`)

Przykład (poglądowy, ora01):

```
Bonding Mode: IEEE 802.3ad Dynamic link aggregation
MII Status: up
Slave Interface: eno1
MII Status: up
Speed: 10000 Mbps
Slave Interface: eno2
MII Status: up
Speed: 10000 Mbps
```

Dwa interfejsy w stanie `up` i ten sam tryb 802.3ad po obu stronach oznaczają, że agregacja działa.

cat = concatenate: sklej i wypisz pliki

TYLKO ODCZYT

Odczyt kart i zespołu przełącznika Hyper-V: Get-NetAdapter i Get-VMSwitchTeam

```
Get-NetAdapter | Format-Table Name, InterfaceDescription, Status, LinkSpeed
Get-VMSwitchTeam -Name NazwaPrzelacznika | Format-List Name, TeamingMode,
LoadBalancingAlgorithm
```

> (gdzie `NazwaPrzelacznika` to nazwa przełącznika wirtualnego Hyper-V utworzonego z zespołem kart SET)

Przykład (poglądowy, hv01):

```
Name       InterfaceDescription          Status LinkSpeed
----       --------------------          ------ ---------
SFP-A      Karta 10G, port 1  Up     10 Gbps
SFP-B      Karta 10G, port 2  Up     10 Gbps
```

W Windowsie `Get-NetLldpAgent -NetAdapterName NazwaKarty` istnieje (moduł NetLldpAgent), ale pokazuje tylko ustawienia lokalnego agenta LLDP: nazwę interfejsu, zakres i adres MAC, a nie sąsiadów [11]. Sąsiadów dla hostów z Windowsem odczytujemy więc po stronie przełącznika.

SET = Switch Embedded Teaming: zespół kart sieciowych zbudowany w przełączniku wirtualnym Hyper-V; łączy dwie karty w jedno łącze bez ustawień po stronie przełącznika fizycznego, więc bez LACP · **LLDP** = Link Layer Discovery Protocol: protokół, którym sąsiednie urządzenia sieciowe opowiadają sobie o sobie · **MAC** = Media Access Control: unikalny adres fizyczny karty sieciowej, przypisany fabrycznie

Z życia wzięte

□□ Z ŻYCIA WZIĘTE

Czwartek, 19:15. Przełącznik w szafie ściennej w Swarzędzu zdechł po burzy, więc Tomek jedzie do magazynu z nowym, wyjętym z pudełka. Wpina kable w te same porty co poprzednio, a skanery nie dostają adresów IP i Marek dzwoni co kilka minut. Po godzinie okazuje się, że port łączący z szafą R1 w ustawieniach fabrycznych jest zwykłym portem w VLAN 1, więc VLAN 30 nigdzie nie dociera. Po wpisaniu portu jako trunku z VLAN 30 i 98 skanery dostają adresy, a Tomek dopisuje do NetBoksa, które porty są trunkami.

Skąd się wzięło

Początki przełącznika opisuje Sieć fizyczna: skąd się wzięły przełączniki, Wi-Fi i zasilanie przez kabel: koncentrator powtarzał ramkę na wszystkie porty, a przełącznik uczy się adresów i wysyła ramkę tylko tam, gdzie siedzi odbiorca. Sieci VLAN pojawiły się w standardzie IEEE 802.1Q z 1998 roku, który dodał do ramki cztery bajty z numerem sieci [1]. Agregację łączy opisało 802.3ad w marcu 2000 roku, dziś jest to norma 802.1AX, w wydaniu 2020 [2]. Pierwszy przełącznik pokazała około 1990 roku firma Kalpana [6][7].

Drzewo rozpinające wymyśliła Radia Perlman w 1985 roku, a w 1990 roku weszło ono do IEEE 802.1D [3]. Szybszą wersję, RSTP, opisało 802.1w w 2001 roku i włączono ją do 802.1D-2004 [3].

Przełącznik Juniper QFX5100.

□□ *Przełącznik Juniper QFX5100. Źródło: Wikimedia Commons (autor i wolna licencja podane na stronie pliku).*

Rodzaje i zasada działania

Jak przełącznik uczy się adresów

Pojęcie: tablica MAC (CAM). Pamięć przełącznika, w której zapisane są pary: adres MAC i port, za którym ten adres został widziany. Przełącznik wpisuje do niej adres nadawcy każdej ramki, która wpadnie na port.

Kiedy ramka ma adres odbiorcy, który jest w tablicy, przełącznik wysyła ją tylko na ten jeden port. Kiedy adresu nie zna, wysyła ramkę na wszystkie porty tego samego VLAN-u poza tym, z którego przyszła, i takie rozsyłanie nazywamy zalewaniem (flooding) [4]. Wpisy starzeją się, jeśli nic z danego adresu nie przychodzi, a czas starzenia zwykle wynosi kilka minut, co w naszym modelu sprawdzamy w dokumentacji.

Tablica ma skończoną pojemność, którą producent podaje w karcie katalogowej. Sieć Zielonej ma kilkaset urządzeń, więc pojemność sprawdzamy przy zakupie przełączników rdzeniowych, do których dojdzie wiele maszyn wirtualnych.

Przełącznik warstwy 2 i warstwy 3

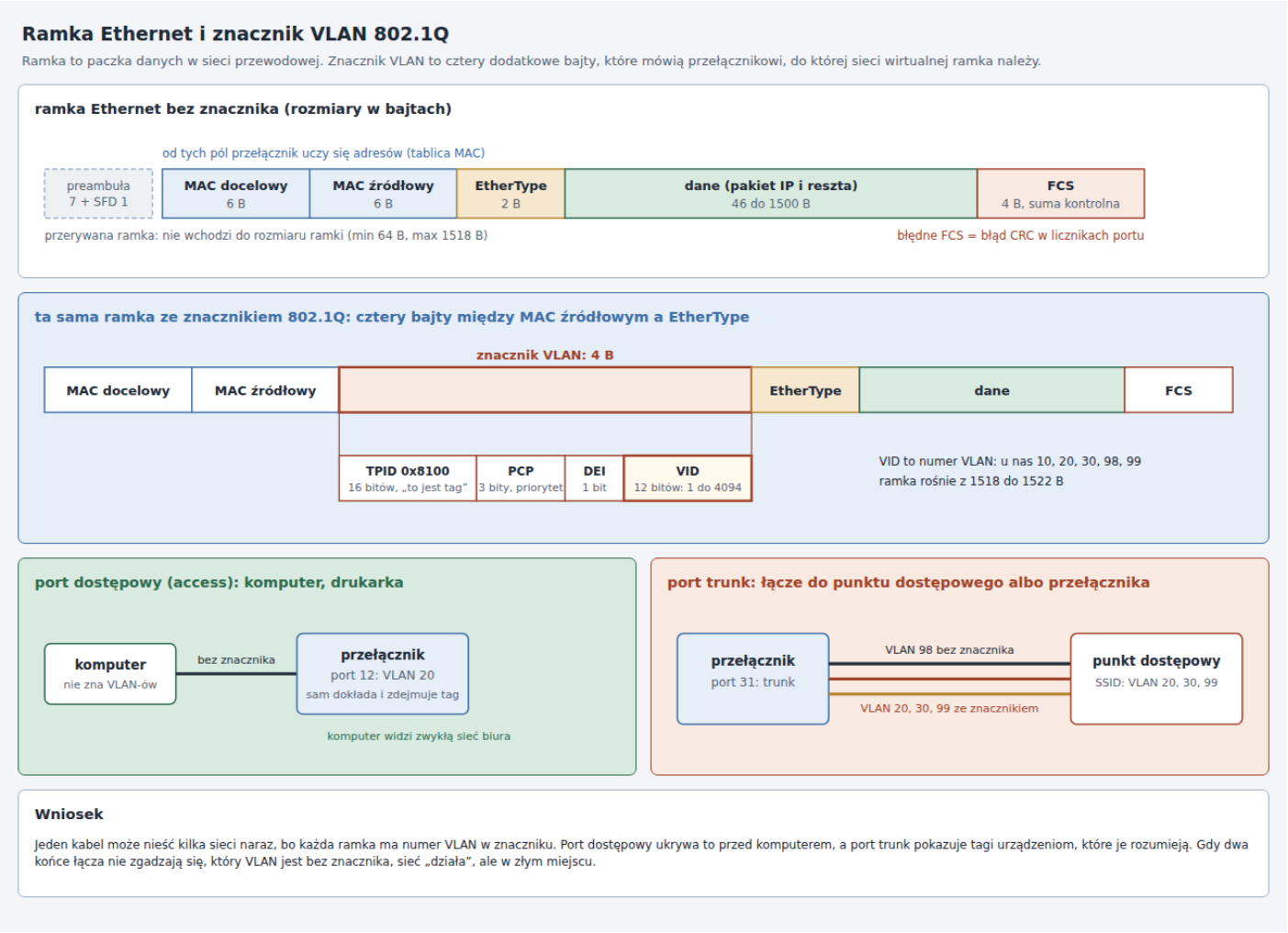
> **Pojęcie: przełącznik L2 i L3.** Przełącznik L2 przekazuje ramki według adresów MAC i nie zna adresów IP, a przełącznik L3 potrafi dodatkowo trasować pakiety IP między sieciami VLAN.

Przełącznik L3 jest szybki, bo trasuje sprzętowo, ale wtedy ruch między sieciami przechodzi przez niego, a nie przez zaporę. W Zielonej proponujemy przełączniki wyłącznie w roli L2, a trasowanie i filtrowanie między VLAN-ami zostawiamy na `fw01`, który jest bramą każdej sieci. Dzięki temu żaden pakiet z VLAN 20 do VLAN 10 nie ominie reguł zapory.

VLAN i trunk 802.1Q fizycznie

> **Pojęcie: VLAN.** Wirtualna sieć lokalna: przełącznik dzieli swoje porty na osobne sieci rozgłoszeniowe, tak jakby były na osobnych urządzeniach. Numer VLAN-u to liczba od 1 do 4094 [1].

Port dostępowy (access) należy do jednego VLAN-u, a ramki na nim chodzą bez znacznika. Port trunkowy niesie wiele VLAN-ów na jednym kablu, a ramki dostają czterobajtowy znacznik 802.1Q z numerem sieci. Znacznik składa się z identyfikatora protokołu 0x8100, trzech bitów priorytetu (PCP), jednego bitu DEI i 12 bitów numeru VLAN, co zwiększa maksymalną ramkę z 1518 do 1522 bajtów [1][5].



Rysunek 1. Ramka Ethernetu bez znacznika i z znacznikiem 802.1Q oraz port dostępowy i trunk w Zielonej: VLAN 98 bez znacznika, a VLAN 20, 30 i 99 ze znacznikiem. Warto zauważyć, że znacznik wchodzi między adres nadawcy a typ ramki. (kliknięcie otwiera pełny rozmiar)

Jeden VLAN na trunku może przechodzić bez znacznika i nazywamy go natywnym (native) albo nieznakowanym (untagged). Dla punktów dostępowych Zielonej proponujemy VLAN 98 jako nieznakowany, żeby punkt dostał adres zarządzania, i VLAN-y 20, 30 i 99 znakowane, które punkt przypisuje do identyfikatorów SSID. Różna konfiguracja natywnego VLAN-u na dwóch końcach trunku to klasyczna przyczyna dziwnych objawów, więc zapisujemy ją w NetBoksie dla każdego trunku.

Agregacja łączy LACP

> **Pojęcie: LACP.** Protokół z normy 802.1AX, w którym dwa urządzenia uzgadniają łączenie kilku kabli w jedno łącze logiczne. Obie strony wymieniają ramki na adres 01:80:C2:00:00:02, więc zła konfiguracja jednej strony jest widoczna po drugiej [2].

Agregacja daje i większą przepustowość, i odporność na awarię jednego kabla, ale nie rozkłada ruchu równo. Przełącznik wylicza z adresów i portów skrót ramki i według niego wybiera kabel, więc

jedna sesja pozostaje zawsze na jednym kablu. Dwa łącza po 10 Gb/s nie dadzą jednej kopii pliku 20 Gb/s, ale dwie kopie od różnych klientów mogą pójść różnymi kablami.

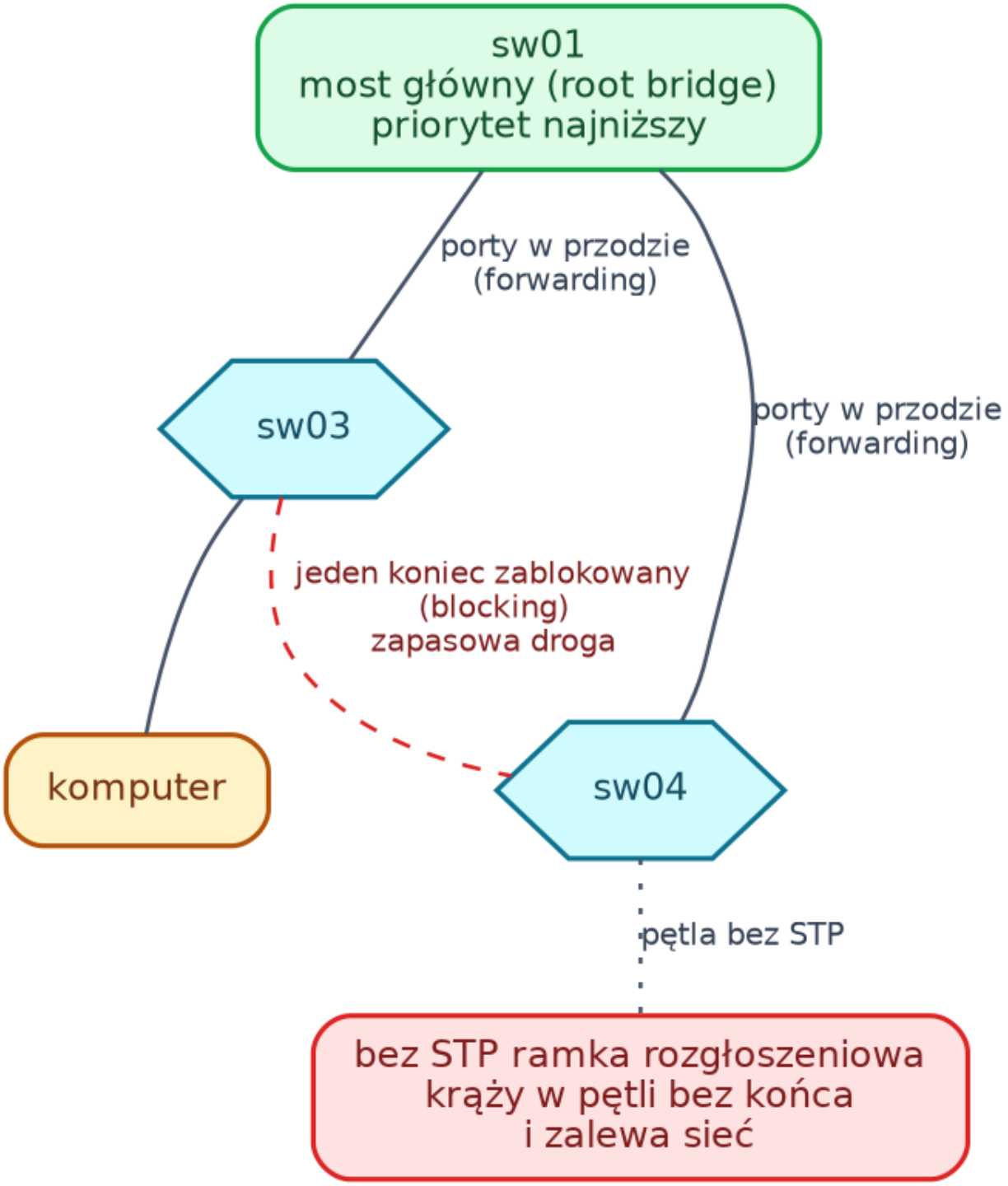
Połączone porty muszą mieć tę samą prędkość i dupleks [2].

Hyper-V w Windows Server ma wyjątek. Zespół SET (Switch Embedded Teaming), z którego korzystają hosty `hv01` i `hv02`, nie obsługuje LACP ani łączenia po stronie przełącznika i pracuje w trybie niezależnym od przełącznika [12]. Dlatego porty przełączników dla hostów Hyper-V konfigurujemy jako zwykłe trunki albo porty dostępowe, a nie jako grupę LACP. LACP planujemy dla zapory `fw01`, dla hostów z Linuksem i dla łączy między przełącznikami.

Pętle, STP i RSTP

> **Pojęcie: pętla w sieci L2.** Sytuacja, w której między dwoma przełącznikami prowadzą dwie ścieżki, więc ramka rozgłoszeniowa wraca do nadawcy i krąży bez końca. Ramka Ethernetu nie ma licznika przeskoków jak pakiet IP, więc nic jej nie zatrzyma.

> **Pojęcie: STP i RSTP.** Protokół drzewa rozpinającego wybiera jeden most główny i blokuje porty tak, aby między dwoma punktami została jedna ścieżka. Wersja klasyczna 802.1D potrzebuje 30 do 50 sekund na przebudowę po awarii, a RSTP z 802.1w robi to w czasie do kilku sekund [3].



Rysunek 2. Trzy przełączniki w trójkącie: sw01 jako most główny, dwa porty w przodzie i jeden koniec zablokowany na zapasowej drodze. Warto zauważyć, że zablokowany port nie wyłącza kabla, tylko czeka, aż główna droga padnie. (kliknięcie otwiera pełny rozmiar)

Przełączniki wymieniają się komunikatami BPDU i wybierają most główny po najniższym priorytecie, a przy remisie po najniższym adresie MAC. Dlatego priorytet ustawiamy ręcznie na `sw01` (rdzeń), a nie zostawiamy losowi: inaczej mostem głównym może zostać najstarszy przełącznik na hali. Na

portach, do których wpinamy komputery, skanery i punkty dostępowe, włączamy tryb portu brzegowego (edge) z ochroną BPDU, która wyłącza port, gdy zjawi się na nim BPDU. Takie ustawienie zatrzymałoby niedzielną pętlę z opowieści, bo własne BPDU przełącznika wróciłoby drugim kablem na port brzegowy i port zostałby wyłączony.

Stos i MC-LAG

> **Pojęcie: stos przełączników.** Dwa lub więcej przełączników połączonych specjalnym łączem, które działają jak jedno urządzenie z jedną konfiguracją i jednym adresem zarządzania.

Stos pozwala poprowadzić agregację LACP do dwóch fizycznych przełączników naraz, więc awaria jednego nie zatrzymuje łącza. Inne rozwiązanie to MC-LAG, w którym dwa niezależne przełączniki udają jedno dla partnera LACP. Obie metody zależą od producenta, więc przy zakupie sprawdzamy, którą oferuje wybrany model, i czy dla `fw01` (FortiGate 100F) agregacja do dwóch przełączników jest obsługiwana.

Zarządzanie przełącznikiem

Przełącznik ma własny adres IP do zarządzania i ten adres umieszczamy w sieci VLAN 98, w której stoją też BMC serwerów, jak opisuje strona Zdalne zarządzanie: BMC, IPMI i Redfish w osobnej sieci. Do przełącznika wchodzimy przez SSH z VPN, HTTP wyłączamy, a hasła fabryczne zmieniamy przy pierwszym uruchomieniu. SNMP i LLDP pozwalają `mon01` (Zabbix) i NetBoksowi zbierać dane o portach i sąsiadach.

Zapora przepuszcza w VLAN 98 tylko to, co potrzebne. Do reguł z strony o BMC dochodzą: `mon01` na przełączniki po UDP 161 (SNMP), punkty dostępowe do kontrolera UniFi Network (TCP 8080, UDP 3478; strona UISP i UniFi: dwa systemy zarządzania sprzętem Ubiquiti i czym się różnią) i punkty dostępowe do kontrolera domeny `dc02` po UDP 1812 i 1813 (RADIUS). Każdą z tych reguł zatwierdza autor bazy, bo rozszerza zbiór ustalony w sw2-01.

Wszystkie rodzaje w jednej tabeli

Rodzaj	Zarządzanie	VLAN, LACP, STP	Trasowanie	Do czego u nas
Niezarządzalny (unmanaged)	brak	brak	brak	nigdzie w szafach, zwłaszcza pod regałem w magazynie

Rodzaj	Zarządzanie	VLAN, LACP, STP	Trasowanie	Do czego u nas
Zarządzalny uproszczony (smart, web managed)	strona WWW	podstawowe VLAN, czasem LACP	brak	małe biuro, jeśli sprawdzimy RSTP
Zarządzalny L2	SSH, SNMP, WWW	pełne VLAN, LACP, RSTP i LLDP	brak	sw03, sw04, sw-mag01
Przełącznik L3	jak wyżej	jak wyżej	trasowanie sprzętowe między VLAN	rdzeń dużych sieci, w Zielonej zbędny
Stos lub para MC-LAG	jedna konfiguracja	jak wyżej	zależnie od modelu	sw01 i sw02 (propozycja)

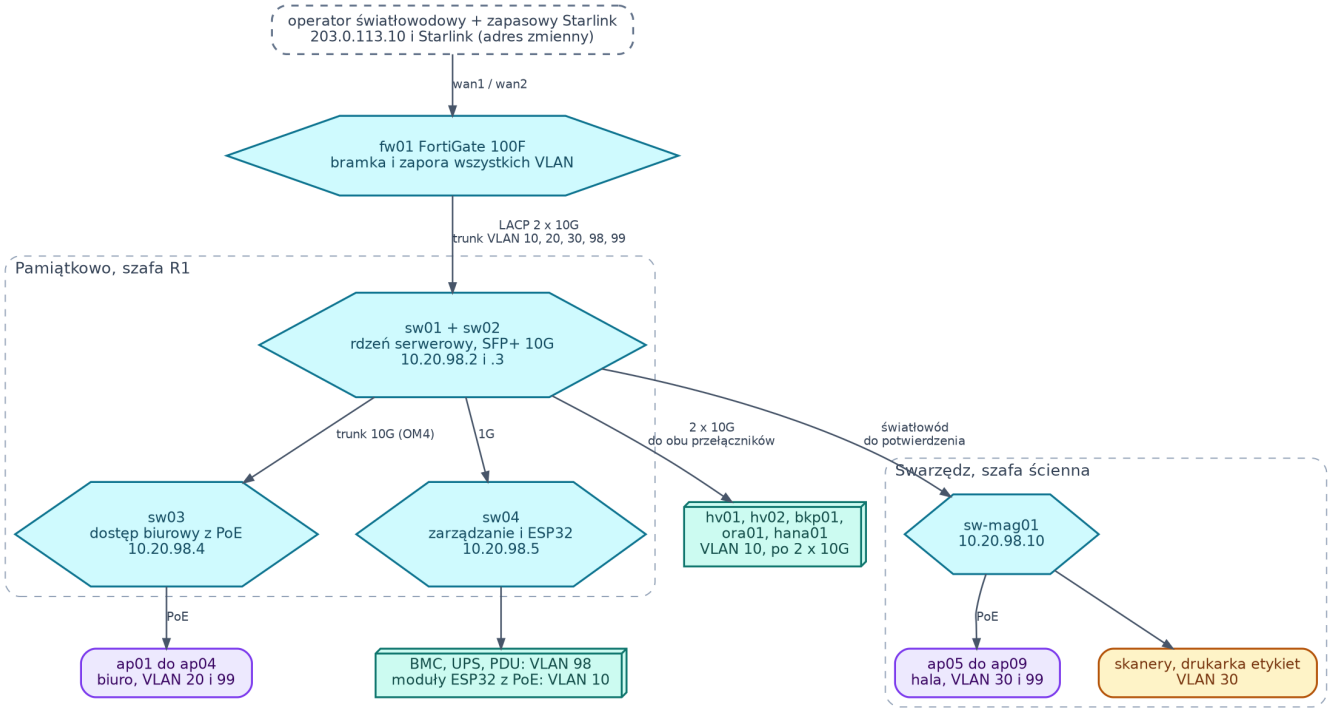
W serwerowni

Proponujemy cztery przełączniki w szafie R1 i jeden w szafie ściennej w Swarzędzu. Adres zarządzania przełącznika to 10.20.98.(1 + numer), więc sw01 ma .2, a sw04 ma .5, a punkty dostępowe mają 10.20.98.(10 + numer). Sprawdziliśmy po całej bazie, że adresy od .2 do .20 w VLAN 98 są wolne, bo zajęte są tylko .1 (`fw01`) i adresy BMC od .21 w górę.

Nazwa	Rola	Gdzie	Adres w VLAN 98
sw01	rdzeń serwerowy 10G SFP+, most główny STP	R1	10.20.98.2
sw02	rdzeń serwerowy 10G SFP+, w stosie lub parze z sw01	R1	10.20.98.3
sw03	dostęp biurowy z PoE (punkty dostępowe, kamery)	R1	10.20.98.4
sw04	zarządzanie: BMC, UPS, PDU i moduły ESP32 z PoE	R1	10.20.98.5
rezerwa	dodatkowe przełączniki	R1 lub R5	od 10.20.98.6 do .9
sw-mag01	magazyn, szafa ścienna	Swarzędz	10.20.98.10
ap01 do ap09	punkty dostępowe: ap01 do ap04 w biurze, ap05 do ap09 w hali	sufity	od 10.20.98.11 do .19
rezerwa	punkt dostępowy ap10		10.20.98.20

Hosty `hv01`, `hv02`, `bkp01`, `ora01` i `hana01` dostają po dwa łącza 10G do obu przełączników rdzeniowych, żeby awaria jednego przełącznika nie zatrzymała serwerów. Zapora `fw01` łączy się z rdzeniem przez agregację dwóch łączy, a trunk niesie VLAN-y 10, 20, 30, 98 i 99. Nazwy `sw01` do `sw04` zastępują w NetBoksie przykładową nazwę `sw3-r1` ze strony Porządek i dokumentacja:

patchpanele, etykiety, kolory i NetBox, która była tam tylko ilustracją formatu.



Rysunek 3. Proponowana topologia Zielonej: operator, zapora fw01, rdzeń sw01 i sw02, przełączniki sw03 i sw04, szafa sw-mag01 w Swarzędzu oraz punkty dostępowe. Warto zauważyć, że wszystkie linie do VLAN-ów przechodzą przez fw01, a przełączniki nigdzie nie trasują ruchu. (kliknięcie otwiera pełny rozmiar)

Kolory kabli zostają według konwencji ze strony o dokumentacji: pomarańczowe łącza między przełącznikami, zielone zarządzanie, żółte urządzenia PoE.

Co sprawdzamy u wykonawcy

- Wersję i model przełączników zgodną z zamówieniem, razem z numerami seryjnymi zapisanymi w NetBoksie.
- Konfigurację portów według tabeli: access, trunk, VLAN natywny, LACP, port brzegowy z ochroną BPDU.
- Priorytet STP na rdzeniu ustawiony ręcznie i zapisany.
- Adres zarządzania w VLAN 98, hasło zmienione, SSH włączone, HTTP wyłączone.
- Kopię konfiguracji przekazaną na piśmie, a nie tylko wykonaną w szafie.
- Opisy portów zgodne z etykietami panelu i kablami.
- Test odłączenia jednego łącza agregacji i jednego przełącznika rdzeniowego z podglądem, że ruch nie ustaje.

Mity i sprostowania

Obiegowa wersja	Jak jest naprawdę
Przełącznik zawsze wysyła ramkę tylko do właściwego portu	Dopóki nie zna adresu odbiorcy, zalewa wszystkie porty VLAN-u
Dwa łącza 10G dają 20 Gb/s dla każdej sesji	Jedna sesja zostaje na jednym łączu, bo skrót ramki wybiera kabel
Sieć VLAN to inna sieć fizyczna, więc jest bezpieczna sama z siebie	VLAN rozdziela ruch, ale o tym, co przepuścić między VLAN-ami, decyduje zapora
STP jest przestarzały, więc go wyłączamy	Bez niego jedna pętla zatrzymuje sieć, a nowoczesny RSTP przebudowuje się w sekundy
Przełącznik niezarządzalny wystarczy do magazynu	Nie ma STP, więc jeden dodatkowy kabel kończy się przestojem zmiany

Oś czasu

Data	Wydarzenie
1985	Radia Perlman wymyśla drzewo rozpinające
około 1990	Kalpana pokazuje pierwszy przełącznik Ethernet
1990	STP w standardzie IEEE 802.1D
1998	IEEE 802.1Q: sieci VLAN i znacznik w ramce
marzec 2000	802.3ad: agregacja łączy
2001	802.1w: szybkie drzewo rozpinające (RSTP)
2008	agregację przenosi norma 802.1AX, w 2020 roku wydanie 802.1AX-2020

Wątek polski

Nie znaleźliśmy udokumentowanego polskiego wkładu w historię przełączników ani w standardy 802.1. W Polsce o przełącznikach stojących w budynkach decydują wymagania producentów i zasady okablowania z PN-EN 50173-1, które opisuje księga Szafy i okablowanie.

Częste błędy

Objaw	Przyczyna	Co robimy
Nowy przełącznik nie widzi sieci, a kable są dobre	port trunk ustawiony fabrycznie jako access w VLAN 1	ustawiamy port jako trunk z właściwymi VLAN-ami
Ruch na jednym VLAN-ie nie przechodzi, inne działają	VLAN nie jest dozwolony po jednej stronie trunku	porównujemy listy dozwolonych VLAN-ów po obu stronach
Sieć staje po wpięciu kabla "dla wygody"	pętla w sieci i brak ochrony BPDU lub STP	wyjmujemy kabel, włączamy RSTP i ochronę BPDU na portach brzegowych
LACP nie podnosi się	różna prędkość lub tryb LACP po dwóch stronach	zgadzamy prędkość i tryb (active lub passive)
Nie udaje się włączyć LACP dla hosta Hyper-V	zespół SET nie obsługuje LACP	zostawiamy porty hostów jako zwykłe trunki bez agregacji
Natywny VLAN różni się po obu stronach	niezgodność ustawień untagged	ujednolicamy i zapisujemy w NetBoksie

□□ Ćwiczenia

1. Ile bajtów ma największa ramka Ethernetu ze znacznikiem 802.1Q i skąd ta liczba?

Odpowiedź

1522 bajty. Ramka bez znacznika ma najwyżej 1518 bajtów, a znacznik dodaje cztery bajty [1][5].

1. Który adres zarządzania dostanie piąty przełącznik, jeśli stosujemy regułę 10.20.98.(1 + numer), i który punkt dostępowy dostanie .17?

Odpowiedź

Piąty przełącznik, sw05, dostałby 10.20.98.6, czyli adres z rezerwy. Adres .17 to ap07, bo punkty dostępowe mają 10.20.98.(10 + numer).

1. Dlaczego porty przełączników dla hostów Hyper-V z zespołem SET nie dostają grupy LACP?

Odpowiedź

Zespół SET nie obsługuje LACP i działa w trybie niezależnym od przełącznika [12]. Porty konfigurujemy jak zwykłe trunki.

Powiązane: Wkładki SFP i kable DAC: rodziny, zgodność i pomiar mocy optycznej, PoE: klasy mocy, budżet przełącznika i długość kabla, Wi-Fi od strony fizycznej: pasma, kanały i rozmieszczenie punktów, Zdalne zarządzanie: BMC, IPMI i Redfish w osobnej sieci, Porządek i dokumentacja: patchpanele, etykiety, kolory i NetBox, Planowanie okablowania: porty, zapas, trasy i zamówienie

Źródła:

1. Wikipedia, „IEEE 802.1Q”: en.wikipedia.org/wiki/IEEE_802.1Q
2. Wikipedia, „Link aggregation”: en.wikipedia.org/wiki/Link_aggregation
3. Wikipedia, „Spanning Tree Protocol”: en.wikipedia.org/wiki/Spanning_Tree_Protocol
4. Wikipedia, „Network switch”: en.wikipedia.org/wiki/Network_switch
5. Wikipedia, „Ethernet frame”: en.wikipedia.org/wiki/Ethernet_frame
6. Wikipedia, „Kalpana (company)”: en.wikipedia.org/wiki/Kalpana_(company))
7. Wikipedia, „Ethernet”: en.wikipedia.org/wiki/Ethernet
8. Fortinet Community, „How to display LLDP, trunk and STP information of a managed FortiSwitch from FortiGate CLI”: community.fortinet.com
9. Fortinet Community, „Port details on which MAC address is learned”: community.fortinet.com
10. lldpd, dokumentacja: lldpd.github.io
11. Microsoft Learn, „Get-NetLldpAgent”: learn.microsoft.com
12. Microsoft, „Tip of the Day: Why You Should Recommend SET over LBFO”: learn.microsoft.com

---

Revision #12
Created 2026-10-03 17:41:11 UTC by Tomasz Konieczny
Updated 2026-10-26 14:23:26 UTC by Tomasz Konieczny