Powtórka

VLAN

VLAN - zagadnienia

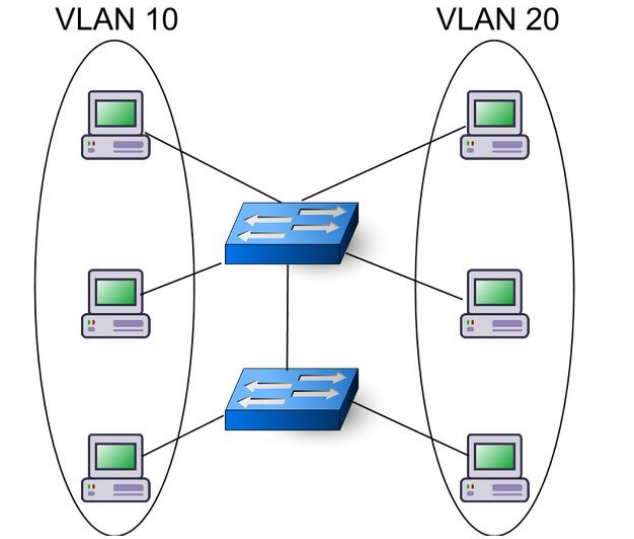
- Co to jest VLAN?
- Na czym polega konfiguracja VLAN na przełączniku?
- Co to jest łącze trunk, z jakiego standardu korzysta?
- Jakie urządzenia sieciowe mogą wspierać VLAN?
- Czym jest “router on a stick” / “one-armed router”? Na czym polega jego konfiguracja?

Definicja

VLAN - wydzielona (logicznie) sieć urządzeń z jednej domeny rozgłoszeniowej w drugiej warstwie ISO/OSI

Podstawowe działanie

Konfiguracja przełącznika: przypisanie portom wybranych identyfikatorów VLAN (dowolnych wybranych liczb naturalnych). Ruch dopuszczony tylko między portami oznaczonymi tym samym identyfikatorem VLAN.



Łącze trunk

Łącze trunk umożliwia przesyłanie pakietów z wielu sieci VLAN jednym łączem.

Jest wykorzystywane do łączenia przełączników z routerami i innymi przełącznikami.

Standard powiązany z tym pojęciem to 802.1Q. Działa dodając do pakietów etykiety z numerem VLAN dla którego pakiet jest przeznaczony.

Router on a stick

Router posiadający jedno fizyczne połączenie z siecią. Zazwyczaj używany do pośredniczenia między logicznie wydzielonymi fragmentami sieci lokalnej (VLANami).

Kluczowym etapem konfiguracji jest utworzenie podinterfejsów odpowiadającym poszczególnym sieciom VLAN.

WLAN

WLAN - zagadnienia

- Jak nazywają się standardy opisujące sieci bezprzewodowe?
- Czym są kanały?
- Co ma wpływ na prędkość przesyłu danych w sieci bezprzewodowej?
- Czym jest tryb ad-hoc?
- Jak działa CSMA/CA?
- Czym jest problem ukrytej stacji?
- Co to jest punkt dostępowy?
- Czym jest tryb infrastruktury?
- Co to jest BSSID/ESSID/SSID?
- Jakie są różnice między poszczególnymi standardami 802.11?
- Czym są WEP, WPA, WPA2, WPA2-EAP, WPA2-PSK, TKiP, CCMP?
- Jakie są typy ramek w sieciach wifi?

Tryb infrastruktury

Tryb infrastruktury - (lub też tryb stacjonarny) wykorzystuje punkty dostępowe (AP); wszystkie urządzenia komunikują się tylko z AP, który spełnia funkcję bramy (do sieci przewodowej) i pośredniczy w komunikacji pomiędzy urządzeniami sieci bezprzewodowej (STA).

- IBSS - Independent Basic Service Set = ad-hoc
- BSS - Basic Service Set (AP + STAs)
- BSSID - Basic Service Set identifier
- (E)SSID - Service Set identifier

Tryb ad-hoc

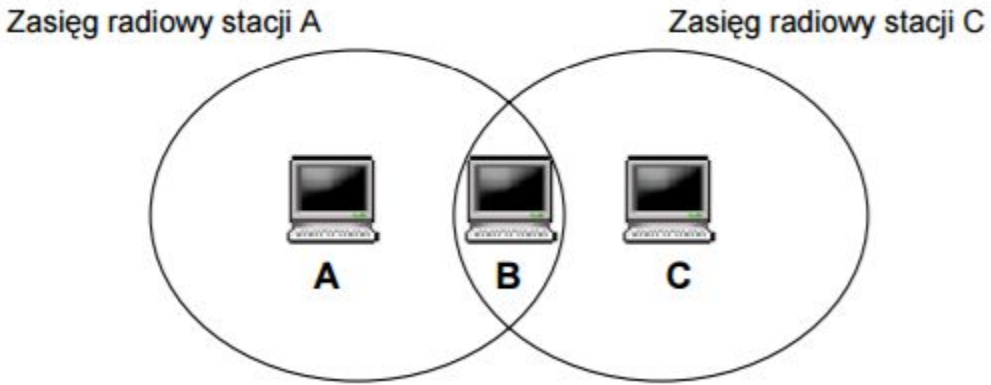
Tryb ad hoc - wszystkie urządzenia w sieci komunikują się ze sobą bezpośrednio (jeśli pozwala na to zasięg radiowy) – nie wykorzystuje się punktów dostępowych;

Dlaczego CSMA/CD jest nieodpowiednie dla WLAN

- Z reguły bezprzewodowe karty sieciowe nie są zdolne do jednoczesnego wysyłania i odbierania pakietów.
- Nawet jeśli posiadałyby taką zdolność, sygnał radiowy emitowany podczas transmisji zagłuszyłby transmisje innych węzłów.

Problem ukrytego węzła (hidden node/station)

Dwie stacje widzą Access Point, ale nie widzą siebie nawzajem



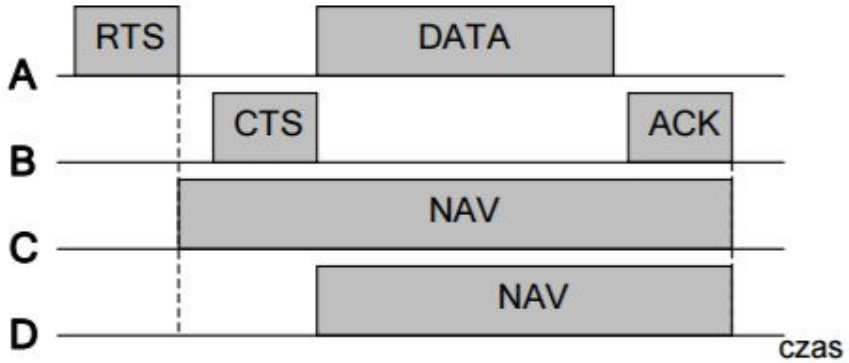
Kolizje pakietów - w sieciach WLAN

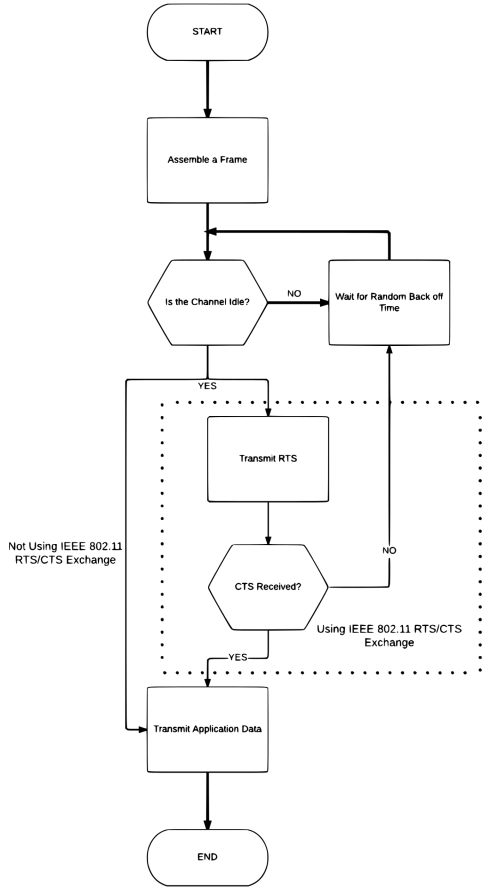
CSMA/CA - carrier sense multiple access with collision **avoidance**

- Carrier sense
  - przed wysłaniem sprawdzamy czy nośna jest wolna
- Multiple access
  - wiele urządzeń korzysta z tego samego medium
- **Avoidance**
  - Przed wysłaniem danych wysyłany jest pakiet “ostrzegawczy”
  - Odebranie pakietu ostrzegawczego jest potwierdzane
  - Odebranie pakietu ostrzegawczego powoduje wstrzymanie wysyłania swoich danych aż do odebrania danych od węzła, który wysłał pakiet ostrzegawczy
  - Jeżeli nadawca nie otrzymał ack od odbiorcy, to spróbuje ponownie po pewnym czasie

CSMA/CA dla 802.11.x

- RTS - request to send
  - nadawca do odbriocy - zazwyczaj AP
- CTS - clear to send
  - Odbiorca do wszystkich w jego zasięgu (którzy mogliby przeszkodzić w transmisji)





Źródło: https://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance#/media/File:Csma_ca.svg

WEP

- Pre-shared key o stałej długości 40(64) albo 104(128) bitów
- RC4 - strumieniowy algorytm szyfrujący
  - Konkatenacja wektora inicjalizującego (przesyłany jawnie) i klucza
  - Dziurawy
- Dopuszczalne powtórne wykorzystanie tego samego IV
- Brak uwierzytelnienia źródła danych

WPA

- Klucz do 256 bit (w praktyce 128 wystarczy)
- Tymczasowe rozwiązanie kompatybilne ze sprzętem wspierającym WEP
- Głównie TKIP - też RC4, ale:
  - Zamiast konkatenacji - połączenie => brak ścisłego ograniczenia na długość hasła
  - Częsta zmiana klucza
  - + inne ulepszenia
- Opcjonalnie CCMP (AES)
  - Nie RC4 - fundamentalnie różny
  - Do tej pory nie udowodniono słabości

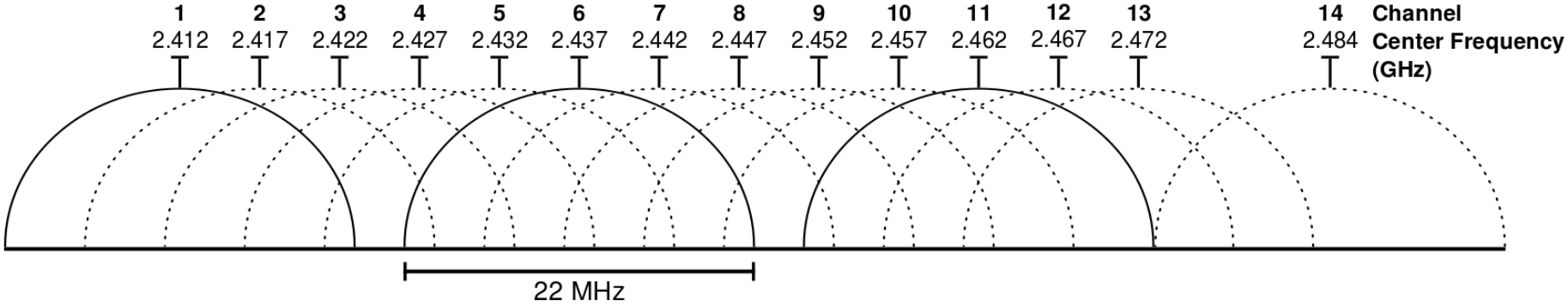
WPA2

- Opcjonalne TKIP (kompatybilność z WPA)
- Głównie CCMP (AES)
- Enterprise (EAP) - używa serwera uwierzytelniającego (RADIUS)
- Personal (PSK) - wykorzystuje klucz dzielony

BSSID

- Basic Service Set Identifier
- Służy do rozróżnienia sieci o tym samym SSID
- W ad-hoc losowa liczba
- W trybie infrastruktury adres MAC AP

Kanały - 2,4GHz

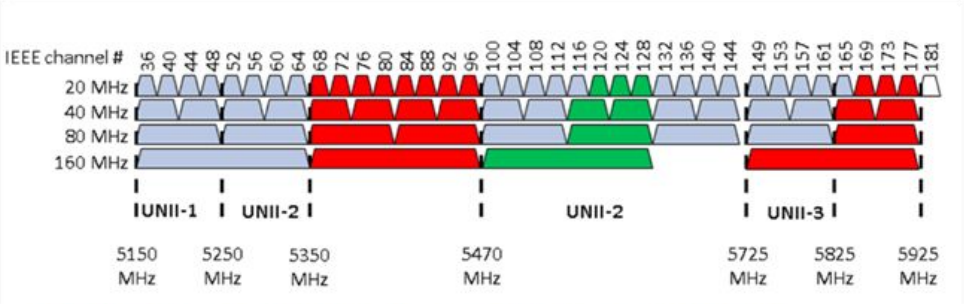


Dlaczego zdefiniowano nachodzące na siebie kanały?

Źródło: https://en.wikipedia.org/wiki/List_of_WLAN_channels#/media/File:2.4_GHz_Wi-Fi_channels_(802.11b,g_WLAN).svg

Kanały - 5GHz

FCC: 5 GHz Channel Plan – Snapshot as of January 2015



- Cisco's dedicated Regulatory Team continues to lobby for more wide, non-overlapping channels enabling for better 802.11ac experience
- Current UNII spectrum allows
  - **6x** 80 MHz channels (**Five** in Canada and Europe)
  - **2x** 160 MHz channels (**One** in Canada)
- Additional unlicensed use of 5.35-5.47 GHz and 5.85-5.925 GHz would allow
  - **Thirty seven** 20 MHz channels,
  - **Eighteen** 40 MHz channels
  - **Nine** 80 MHz channels
  - **Four** 160 MHz channels

New 5 GHz Channels totaling 60 MHz = ALL of available 2.4 GHz channels today

Źródło: http://blogs.cisco.com/wp-content/uploads/802.11ac-image3.png

Standardy 802.11 - podsumowanie

Standard	Częstotliwości	Maks. prędkość	Szerokość kanału
a	5GHz	54Mbit/s	20MHz
b	2,4GHz	11Mbit/s	20MHz
g	2,4GHz	54Mbit/s	20MHz
n	2,4GHz, 5GHz	600Mbit/s	20MHz, 40MHz
ac	5GHz	2Gbit/s	20MHz, 40MHz, 80MHz, 160MHz

Dla porównania:
FastEthernet (100Mbit/s); GigabitEthernet; 40GigabitEthernet; 100GigabitEthernet

Typy ramek w sieciach wifi

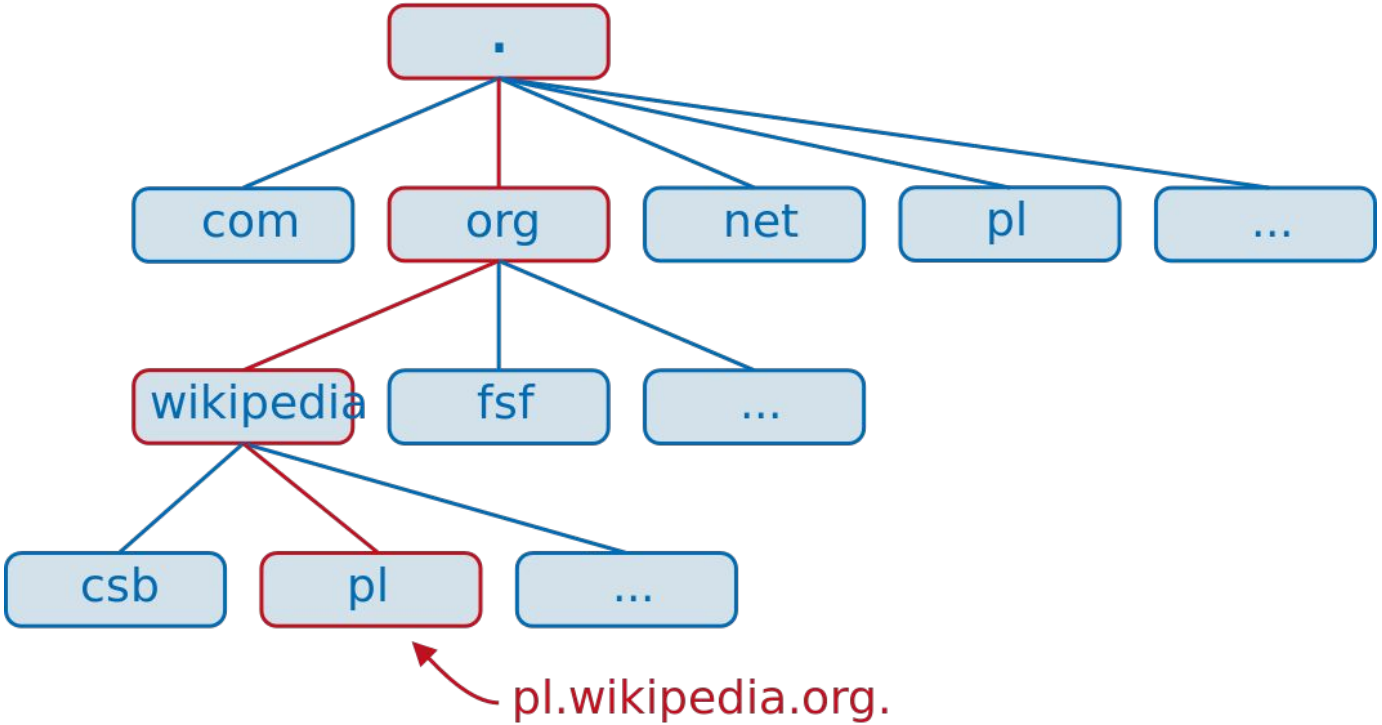
- Kontrolne (RTS/CTS/ACK)
- Zarządzające (beacon, probe, authentication etc.)
- Danych

DNS

DNS - zagadnienia

- Jakie są typy serwerów DNS?
- Jak działa odwzorowanie nazwy domenowej?
- Jakie są typy domen?
- Jak wygląda hierarchia domen?
- Co to jest FQDN, TLD, DNS zone?
- Jakie są typy rekordów DNS (o jakie informacje można zapytać operując rekordami DNS)?

Hierarchia domen



Źródło: https://pl.wikipedia.org/wiki/Domena_internetowa#/media/File:Dns-schemat.svg

Pojęcia

- Domain Name System
- Domain - domena
- Domain Name - nazwa domenowa np. cs.put.poznan.pl
- Top Level Domain - domeny o nazwach np. pl, com, org
  - Country Code Top Level Doman - pl, de
- Fully Qualified Domain Name - pełna nazwa domenowa (konkretnej maszyny). Np. sirius.cs.put.poznan.pl
- DNS zone - strefa DNS - (nieprzerwany) fragment przestrzeni domenowej pod kontrolą jednego zarządcy. Może zawierać więcej niż jedną domenę.

Typy serwerów DNS

- Serwery domeny głównej (root servers)
  - Obsługują TLD (top level domain)
  - Około 13tu na całym świecie
- Serwery autorytatywne (authoritative servers)
  - Posiada informacje o komputerach
- Caching name servers
  - Zbierają dane z powyższych, przeznaczone dla użytkowników końcowych (public DNS)

Rekordy zasobowe (Resource Records)

- **SOA** (ang. *Start Of Authority*) - wskazuje, że dany serwer jest najlepszym źródłem informacji o domenie oraz definiuje zachowanie serwerów głównych (ang. *primary DNS*) oraz zapasowych (ang. *secondary DNS*); rekord SOA jest obecny jako pierwszy rekord w każdym pliku strefowym (opisującym domenę)
- **A** - zawiera odwzorowanie nazwy domenowej w adres IP
- **NS** - określa nazwę komputera będącego serwerem DNS dla tej domeny.
- **CNAME** (ang. *canonical name*) - pozwala stworzyć “alias” dla już istniejącej nazwy domenowej
- **MX** (*mail exchange*) - określa nazwę komputera będącego serwerem poczty elektronicznej w danej domenie. Serwery SMTP odczytują jego wartość żeby wiedzieć, który komputer obsługuje pocztę dla domeny.
- **SRV** - zawiera dodatkowe informacje dotyczące lokalizacji usługi, którą wskazuje serwer DNS, rekord SRV używany jest np. przez usługi VoIP, protokół XMPP, LDAP, czy nawet grę Minecraft.
- **TXT** - rekord pozwala na wpisanie dowolnego tekstu, używany głównie przez usługę SPF do walki ze spamem (**host -t txt wp.pl**)
- **PTR** - definiuje odwzorowanie odwrotne (ang. *reverse DNS*) adresu IP na nazwę domenową
- **AAAA** - to samo co rekord A, ale dla adresów IPv6

IPv6

IPv6 - zagadnienia

- Dlaczego zostało zaproponowane, jakie oferuje ulepszenia względem IPv4?
- Jak wygląda adres IPv6?
- Jak można skracać zapis adresu IPv6?
- Jakie są typy adresów IPv6?
- Czym są adresy link local, a czym global routable?
- Jak wygląda adres loopback?
- Jak wygląda dowolny adres?
- Które nagłówki zostały usunięte (względem IPv4)?
- Na co pozwala protokół NDP - neighbor discovery protocol?
- Jak może być przypisany publiczny adres IPv6?
- Na czym polega tunelowanie i jak można je zastosować do IPv6?

Dlaczego?

- Mało adresów IPv4
  - NAT
  - CIDR
- Wprowadzenie ulepszeń względem IPv4
  - Większa pula adresów
  - Lepszy routing
  - Autokonfiguracja
  - Bezpieczeństwo
  - Lepsza organizacja nagłówków
  - Przywrócenie end-to-end connectivity
  - Rozszerzalność

Jak to wygląda?

- Każdy adres IPv6 ma 128 bitów
- Zapis blokami 16-to bitowymi oddzielonymi dwukropkami

- Przykład 1a: fe80:0000:0000:0000:0000:0000:0000:cafe
- Przykład 1b: fe80:0:0:0:0:0:0:cafe (kompresja zer w poszczególnych polach)
- Przykład 1c: fe80::cafe (kompresja sąsiadujących pól z zerami)

- Przykład 2a: fe80:0:0:0:beef:0:0:0
- Przykład 2b: fe80::beef:0:0:0

Typy adresów

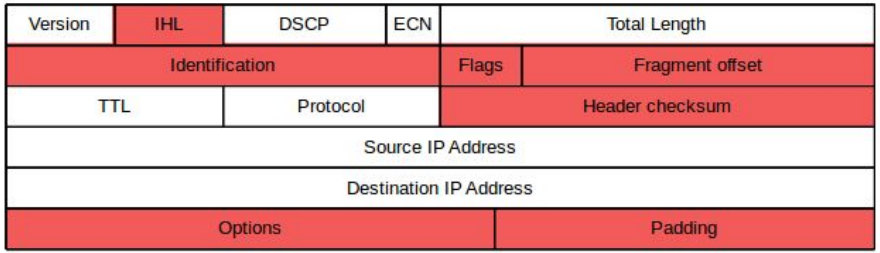
- Unicast
  - Odnosi się do jednego interfejsu w sieci
- Multicast
  - Pozwala na wysłanie wiadomości do wybranej grupy odbiorców (oszczędza przepustowość łączy)
  - Wiadomość wysłaną na adres multicast, mogą odebrać wszystkie interfejsy, które mają taki adres
  - Np.: transmisja video na żywo do wielu użytkowników jednocześnie
- Anycast
  - Do “kogokolwiek” - w praktyce do najbliższego odbiorcy

Konwencje

- fe80::/10 - adresy lokalne dla łącza (link local) (pozostałe - global routable)
- ::1 - loopback (odpowiednik 127.0.0.1 w IPv4)
- :: - dowolny adres (same zera)

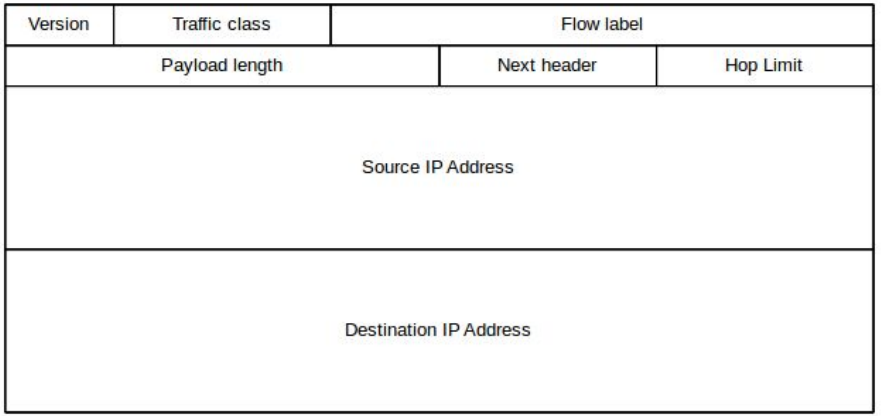
Nagłówki

Pakiet IPv4



Usunięte w IPv6

Pakiet IPv6

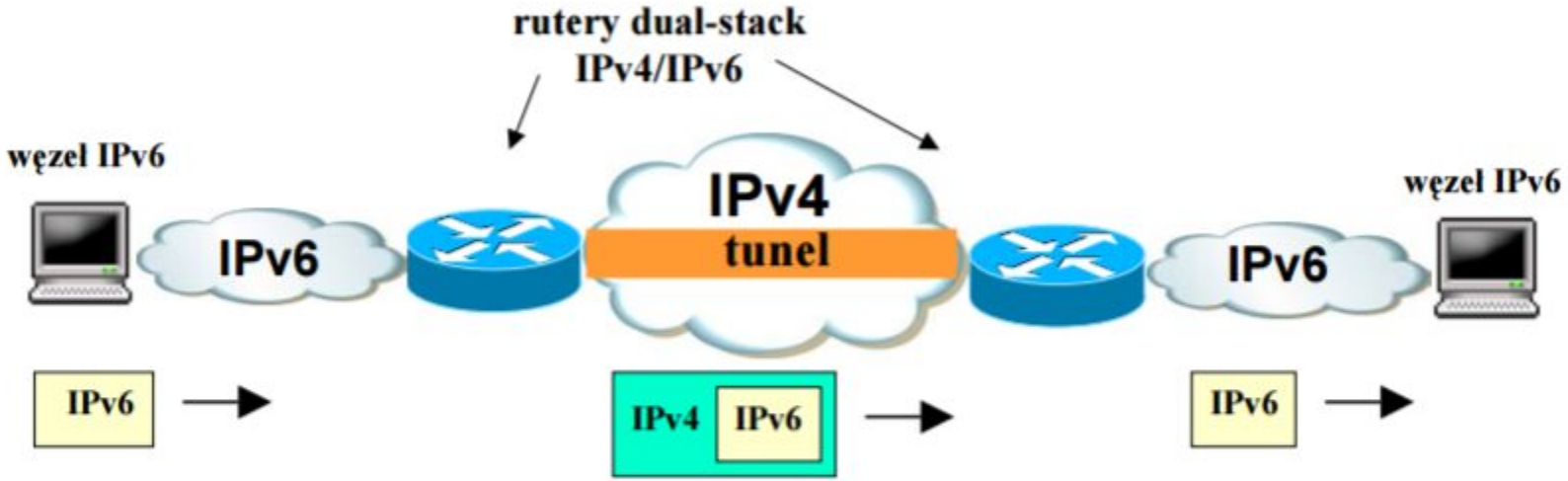


IHL - Internet Header Length
DSCP - Differentiated Services Code Point
ECN - Explicit Congestion Notification
ToS - Type of Service (kiedyś było na miejscu DSCP i ECN)
TTL - Time To Live

NDP (Neighbor Discovery Protocol)

- Autokonfiguracja
  - Router wysyła prefix łącza w cyklicznie wysyłanych wiadomościach
  - Pozostałą część maszyna może wygenerować na podstawie swojego adresu MAC
- Odnajdywanie dostępnych routerów
- Odnajdywanie dostępnych serwerów DNS
- Monitorowanie dostępności innych węzłów na tym samym łączu

Tunelowanie IPv6 w IPv4



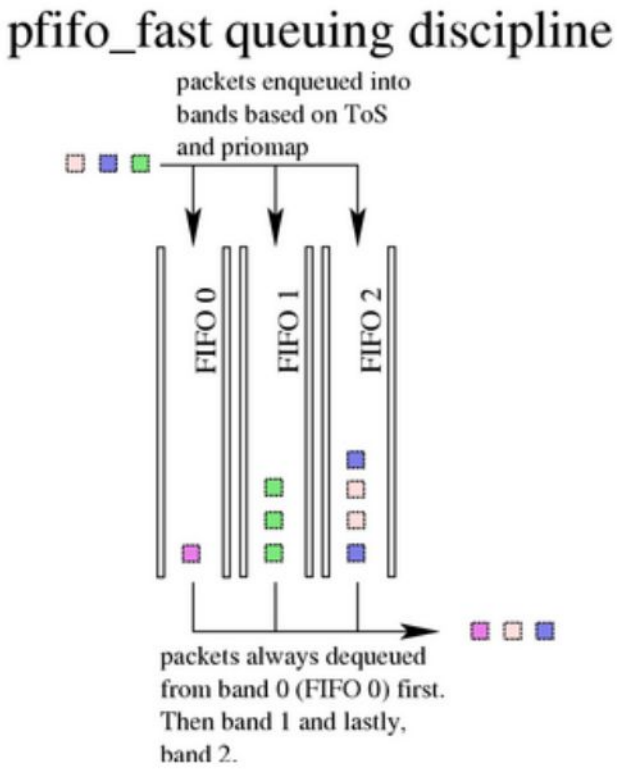
- Tunel sprawia, że choć rutery dzieli w ogólności wiele sieci IPv4, z perspektywy IPv6 dystans pomiędzy nimi jest równy jednemu skokowi

Kształtowanie ruchu

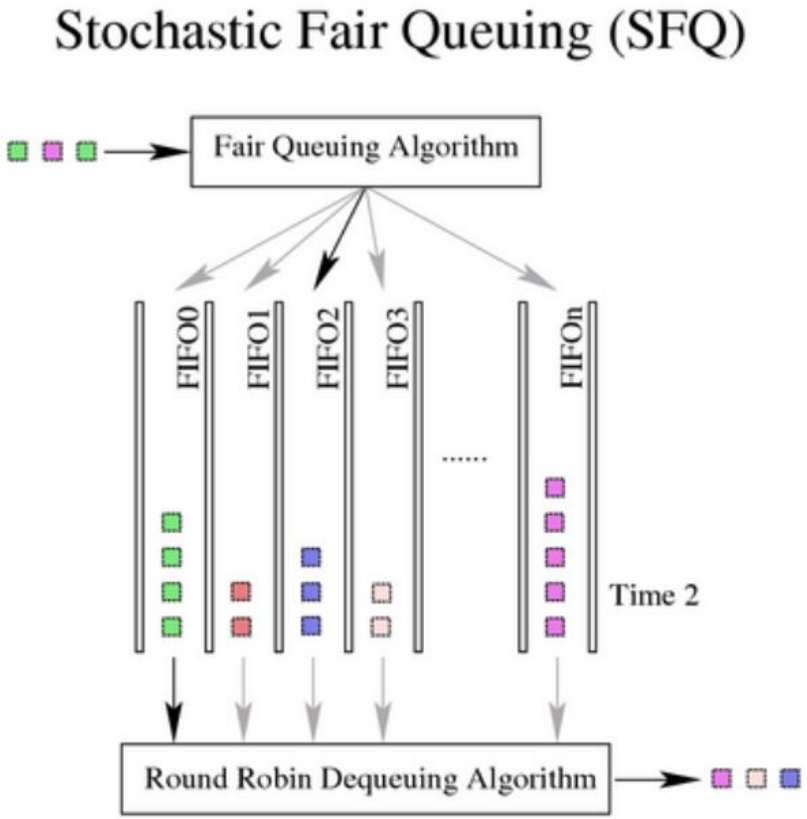
Kształtowanie ruchu - zagadnienia

- Jakie są dwie kategorie kolejek, czym się różnią?
- Jakie są kolejki, jak działają?
- Czym są filtry w kontekście kolejek?
- Jaka jest domyślna kolejka w systemie Linux?

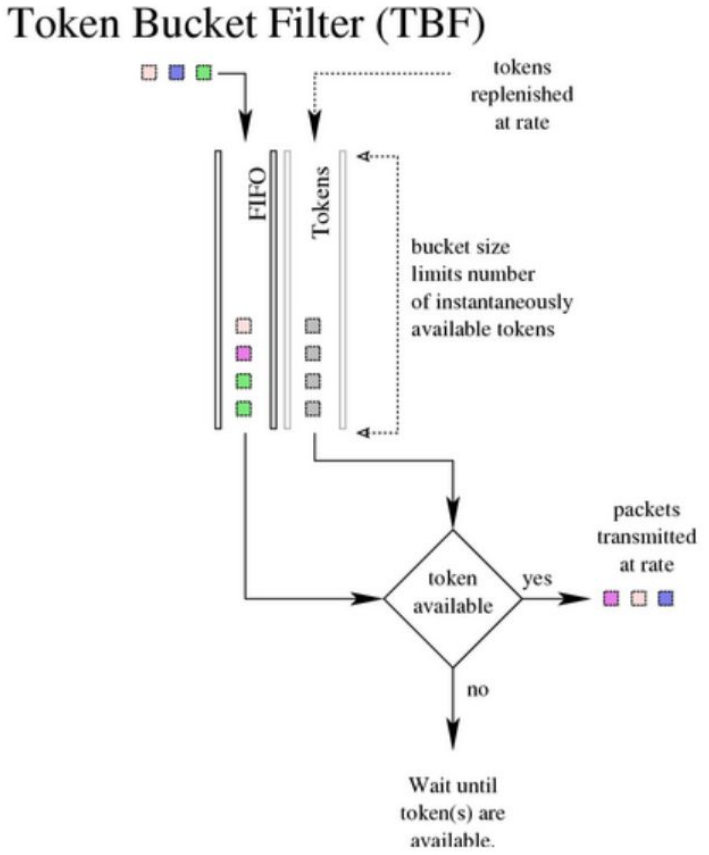
Kolejki bezklasowe - pfifo fast



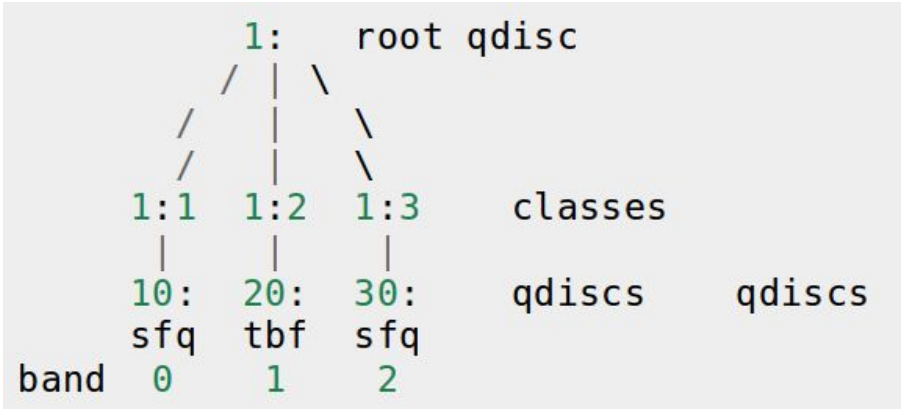
Kolejki bezklasowe - stochastic fair queuing



Kolejki bezklasowe - token bucket filter



Kolejki złożone - PRIO



Kolejki złożone - Hierarchical Token Bucket