

Sieci VLAN

1. Wprowadzenie

VLAN - (od ang. *virtual local area network*) w najbardziej ogólnym podejściu jest to wydzielony logicznie (wirtualnie) segment z fizycznej sieci LAN. Poszczególne LAN'y tworzone są na warstwie drugiej modelu OSI czyli na warstwie łącza danych czyli na switch'ach.

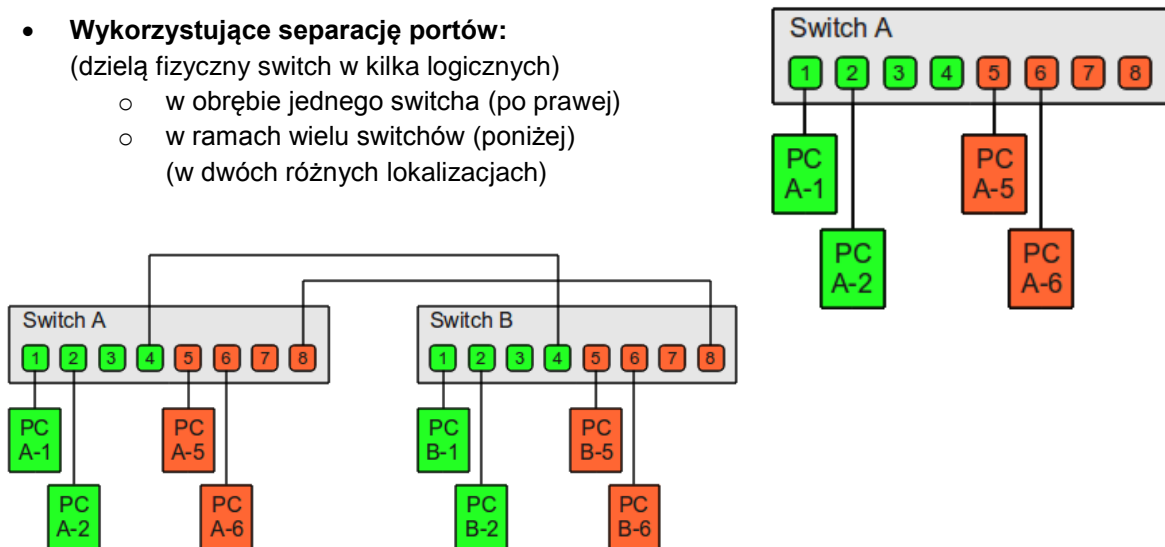
Urządzenia tworzące sieć VLAN, niezależnie od swojej fizycznej lokalizacji (przełącznika, do którego są podłączone), mogą się swobodnie komunikować ze sobą, a jednocześnie są odseparowane od innych sieci VLAN, co oznacza, że na poziomie przełącznika nie ma żadnej możliwości skomunikowania urządzeń należących do dwóch różnych sieci VLAN (dotyczy to także ramek rozgłoszeniowych).

Sieci VLAN konfiguruje się w przełącznikach programowalnych (zarządzalnych) – umożliwiających podział jednego fizycznego urządzenia na większą liczbę urządzeń logicznych. Jedna sieć VLAN może swym zasięgiem obejmować wiele przełączników, a w najprostszym przypadku tworzona jest w jednym przełączniku. Sieć VLAN identyfikowana jest poprzez liczbę całkowitą

2. Rodzaje sieci VLAN

W zależności od sposobu konstrukcji sieci można wyróżnić dwa rodzaje sieci VLAN:

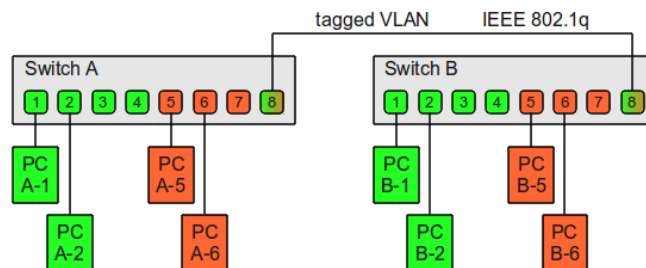
- **Wykorzystujące separację portów:**
(dzieli fizyczny switch w kilka logicznych)
 - w obrębie jednego switcha (po prawej)
 - w ramach wielu switchów (poniżej)
(w dwóch różnych lokalizacjach)



Komputery PC B-1 i PC B-2 mogą komunikować się z PC A-1 i PC A-2 z pierwszego pomieszczenia. Możliwa jest również komunikacja komputerów PC B-5 i PC B-6 z pomieszczenia 2 z komputerami PC A-5 i PC A-6 z pomieszczenia 1. W takiej konfiguracji w celu zapewnienia komunikacji pomiędzy switchami wymagane są dwa osobne połączenia kablowe pomiędzy obydwoma VLANami

- **Wykorzystujące tagowanie VLANów**

Dzięki tagowaniu VLANów komunikacja wielu VLANów może przebiegać przez jeden switch, jeden port. Każda pojedyncza ramka otrzymuje Tag, który określa przynależność ramki do VLAN-u. Gdy oba switche wspierają tagowanie to do podłączenia konieczny jest tylko jeden kabel.



Aby pomiędzy przełącznikami jednym łączem przesyłać ramki z różnych sieci VLAN, należy na tym łączu umożliwić przesyłanie ramek w ramach różnych sieci VLAN. Takie łącze określane jest mianem łącza trunk (ang. VLAN trunk).

Komunikację w ramach jednej sieci VLAN wykorzystującej łącza trunk (czyli sieci VLAN obejmującej więcej niż jeden przełącznik) umożliwia technika oznaczania ramek sieciowych identyfikatorem sieci VLAN (ang. VLAN ID). Technika ta polega na dodawaniu do ramki 12-bitowej liczby identyfikującej sieć VLAN nadawcy. Tak zmodyfikowana ramka przesyłana jest łączami trunk tak długo, aż dotrze do docelowego przełącznika. Ten zaś przed przekazaniem ramki na właściwy port usuwa z niej nadmiarową informację, wprowadzoną przez przełącznik źródłowy. Tagowanie ramek definiuje standard IEEE 802.1Q.

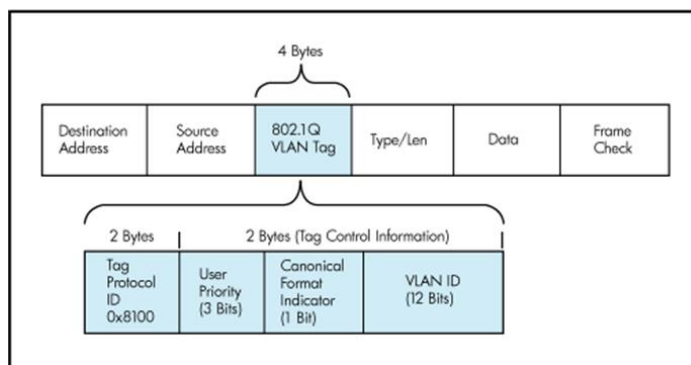
3. Ramka 802.1Q

802.1q jest to standard opisujący działanie wirtualnych sieci LAN (VLAN) implementowany w ramach standardu IEEE 802. Ma na celu umożliwić wielokrotne wykorzystanie jednego fizycznego łącza do przezroczystego przesyłania informacji pochodzących z różnych sieci VLAN. Podczas przesyłania danych z jednej sieci nie następuje ich wyciek do pozostałych, wykorzystujących to samo fizyczne łącze.

Urządzenia zarządzane (switche/routerzy) działające w standardzie 802.1Q, stosują tagowanie ramek.

4 bajtowy tag VLAN

- TPID (Tag Protocol Identifier) – 2 bajty (0x8100)
- Przydzielenie priorytetu dla ramki Ethernet (standard 802.1p) – 3 bity
- Obecność pola RIF - 1 bit (routing information field)
- VLAN ID - identyfikatora VLANu – 12 bitów

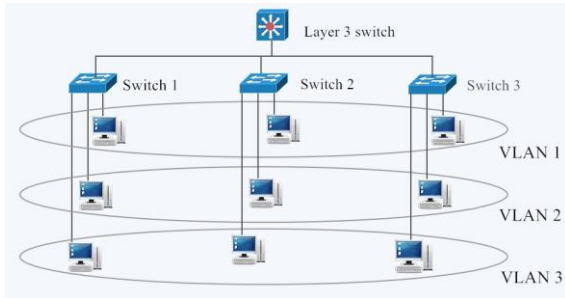


4. Zalety stosowania sieci VLAN

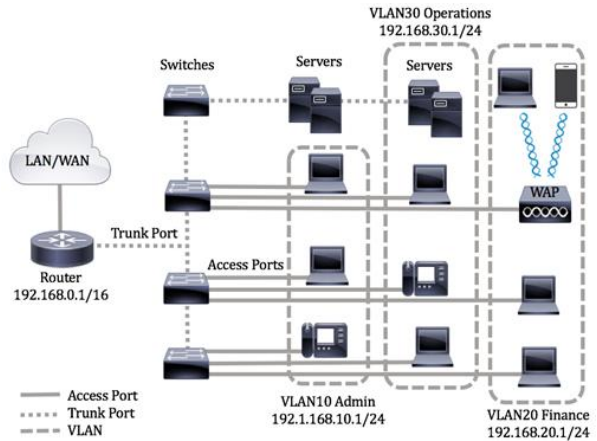
- Każda wirtualna sieć jest osobną domeną kolizyjną jak i rozgłoszeniową. Pozwalają one ograniczyć ruch rozgłoszeniowy, gdyż rozgłaszane ramki trafiają tylko do komputerów w obrębie danej sieci VLAN, nie „zalewają” całej sieci LAN.
- Konfigurowanie sieci VLAN odbywa się na drodze programowej. Dlatego nie wymaga ono fizycznego przenoszenia lub podłączania sprzętu sieciowego.
- Zapewniają zwiększone bezpieczeństwo sieci i grup roboczych

5. Komunikacja między VLAN'ami

Komunikacja między VLAN-ami jest możliwa, gdy w VLAN-ach tych partycypuje port należący do routera lub z wykorzystaniem przełączników warstwy trzeciej.



a) komunikacja w oparciu o przełącznik routujący

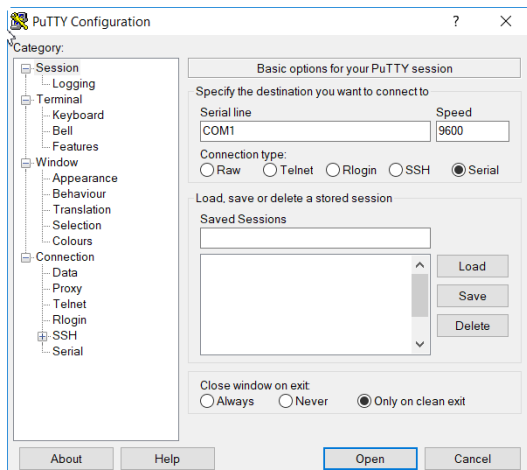


b) komunikacja VLANów oparta o router

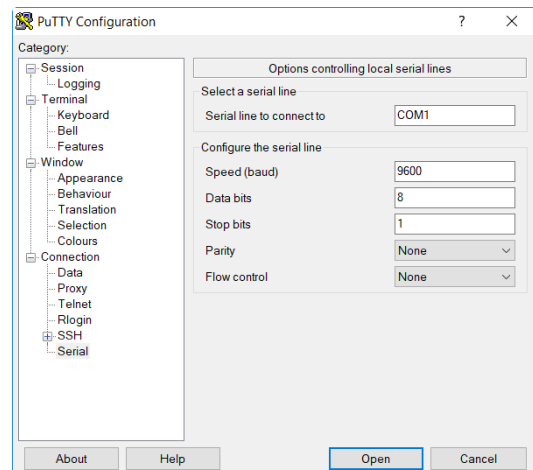
6. Instrukcje do użytego oprogramowania

a. PuTTY

Jest to emulator terminala tekstowego umożliwiający połączenie zarówno po fizycznych portach szeregowych (COM) jak i sieciowo z wykorzystaniem protokołów TELNET, rlogin, SSH-1 lub SSH-2.



Okno Programu



Do komunikacji z urządzeniami Cisco należy używać default'owych parametrów transmisji szeregowej

b. Obsługa switch'a CISCO Catalyst - przykładowe komendy

help - wyświetlanie pomocy
enable - przejście do trybu EXEC - uprzywilejowanego
disable - opuszczenie trybu EXEC - przejście do trybu użytkownika
show - wyświetlenie informacji o urządzeniu
show version - wyświetla informacje o wersji oprogramowania
Show configuration - wyświetlanie aktualnej konfiguracji
configure terminal - przejście do trybu konfiguracji
do ... - umożliwia uruchamianie poleceń trybu ogólnego w trybie konfiguracji
(np. Switch(config)#do show vlan brief)

Literatura / Bibliografia:

A.S. Tannenbaum, Sieci komputerowe, Helion 2004

<http://standards.ieee.org/getieee802/>

D.Dwornikowski, M.Kalewski, J.Kończak, Ł.Piątkowski, Politechnika Poznańska, Sieci VLAN

T.Krenn, „Podstawowe informacje o VLAN”

Scenariusz: Konfiguracja VLAN na przełączniku Cisco Catalyst

1. Oprogramowanie:

PuTTY

2. Przygotowanie do wykonania ćwiczenia

- Podłączyć **kabel konsoli** pomiędzy cienkim terminalem PC1 a switch'em
- Uruchomić program PuTTY na cienkim terminalu
Konfiguracja: Port szeregowy COM1 (9600 baud, 8 data bits, 1 stop bit, No parity)

3. Wariant scenariusza

Nr grupy:.....

Miesiąc (mc):

W wypadku kolizji adresów prowadzący wyznacza adresację alternatywną.

Utworzyć następujące sieci VLAN:

ID VLAN	nazwa VLAN	Numery portów



np.: vlan 11 z nazwą „biuro” dla interfejsów od

FaX/0/1 do FaX/0/4 i vlan 12 z nazwą „kadry” dla interfejsów FaX/0/5 do FaX/0/8

4. Realizacja ćwiczenia

- (a) Aktywować konsolę CLI przełącznika
komendą *enable*

```
Switch>enable  
Switch#
```

- (b) Przejść do trybu konfiguracji

```
Switch#configure terminal  
Switch(config)#
```

- (c) Skonfigurować adres IP domyślnego interfejsu VLAN1 (domyślnie wszystkie porty na switchu należą do VLAN1)

```
Switch(config)#interface vlan1  
Switch(config-if)#ip address 10.10.10.mc 255.255.255.0  
Switch(config-if)#no shutdown
```

INFO: W przełącznikach warstwy drugiej ISO OSI interfejs VLAN o numerze 1 (default) służy jedynie do komunikacji hosta ze switch'em z hostem w celach serwisowych poprzez wybrany VLAN za pomocą kabla Ethernet.

Aby takie połączenie było możliwe, adresy IP hosta oraz interfejsu VLAN1 switch'a muszą być w tej samej podsieci.

- (d) Sprawdzić listę interfejsów

```
Switch(config-if)#do show vlan brief
```

- (e) Za pomocą dwóch prostych kabli Ethernet podłączyć terminale PC1 i PC2 ze dwoma dowolnymi portami z pierwszego VLANu w switchu.

INFO: Co najmniej jeden z portów VLAN w przełączniku musi być w stanie Forwarding (musi być do niego podłączone jakiegokolwiek urządzenie sieciowe) aby konfiguracja VLAN była możliwa

- (f) Wyjść do trybu konfiguracji

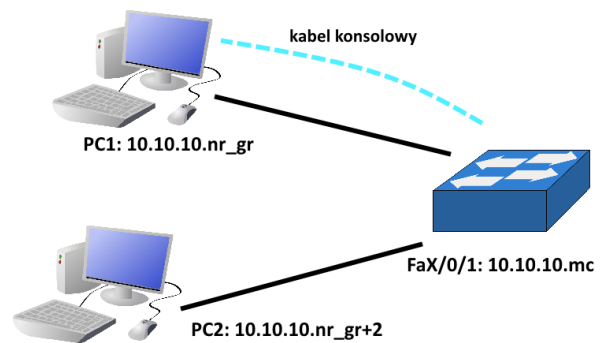
```
Switch(config-if)#exit
```

- (g) W oparciu o numer stacku (X), uzyskany za pomocą polecenia z punktu d) skonfiguruj tryb pracy portu przełącznika jako „access” (tryb komunikacji z urządzeniami DTE - stacjami roboczymi)

```
Switch(config)#interface fa X/0/1
```

gdzie, *fa X/0/1* to skrótowa oznaczenie portu przełącznika Fast Ethernet, gdzie X – oznacza numer urządzenia w stack'u (stack – połączenie wielu przełączników w jeden przełącznik logiczny), 0 – nr modułu przełącznika, 1 – numer portu w module,

```
Switch(config-if)#switchport mode access
```



- (d) Wyjść z trybu konfiguracji interfejsu do trybu ogólnego
`Switch(config-if)#exit`
`Switch(config)#exit`
`Switch#`
- (e) Sprawdzić ustawienia interfejsów IP przełącznika:
`Switch#show ip interface brief`
`Switch#show ip interface vlan 1`

5. Konfiguracje VLANów:

- a) Sprawdzić aktualny stan bazy VLAN w przełączniku:
`Switch#show vlan`
- b) Stwórz dwie nowe sieci VLAN o numerach ustalonych z prowadzącym (przykłady dla vlan 11 i vlan 12)
`Switch#conf t`
`Switch(config)#vlan 11`
`Switch(config-vlan)#name biuro`
`Switch(config-vlan)#exit`
`Switch(config)#vlan 12`
`Switch(config-vlan)#name kadry`
`Switch(config-vlan)#exit`
- c) Wybrać porty wyznaczone do przypisania do VLANów, pojedynczo:
`Switch(config)#interface fa x/0/1`
lub jako zakres
`Switch(config)#interface range fa x/0/1-4`
A później przypisać je do konkretnych VLANów
`Switch(config-if)#no shutdown`
`Switch(config-if)#switchport mode access`
`Switch(config-if)#switchport access vlan 11`
- d) W trybie ogólnym sprawdzić konfigurację vlanów
`Switch#show vlan brief`

6. Testy VLANów:

Skonfiguruj adresację IP obydwu terminali tak, aby znajdowały się one w tej samej sieci IP (zgodnie ze schematem)
Wykonaj ping (z linii poleceń) z jednego terminala do drugiego.

Sprawdź kolejno możliwość komunikowania się stacji PC (ping):

- między portami przełącznika należącymi do dwóch różnych VLAN
- między portami przełącznika w ramach jednej VLAN

W tym celu:

- podłączaj kolejno dwie stacje PC kablami prostymi do dwóch portów przełącznika
- wykonaj zrzut ekranu oraz zdjęcie kabli wpiętych do switcha

7. Oczyszczanie przełącznika:

Po skończonym ćwiczeniu wyczyść konfigurację VLAN dla całego zakresu portów i wybranych identyfikatorów VLANów

```
Switch#conf t
Switch(config)#interface range faX/0/1-24
Switch(config-if)#no vlan 11
Switch(config-if)#no vlan 12
```

8. Sprawozdanie:

Umieścić zrzuty ekranu oraz zdjęcia dokumentujące utworzenie poszczególnych sieci VLAN oraz komunikacje między urządzeniami wewnątrz VLAN i separacje pomiędzy VLAN'ami.