

## Sieci VLAN

**VLAN** (ang. *Virtual Local Area Network*) to wirtualna (logiczna) sieć komputerowa wydzielona z sieci fizycznej. Technologia ta działa w warstwie drugiej modelu OSI, tak więc konfigurowana i wdrażana jest na przełącznikach sieciowych. Obecnie praktycznie każdy, zarządzalny przełącznik pozwala na tworzenie takich wirtualnych sieci LAN. Te wirtualne sieci są od siebie odseparowane, bez routera nie jest możliwa pomiędzy nimi komunikacja, doskonale zatem nadają się w sytuacji kiedy chcemy odizolować od siebie urządzenia, które nie powinny się ze sobą komunikować.

Każdy VLAN ma swój adres sieciowy i określoną liczbę adresów do wykorzystania. Wszystkie urządzenia w obrębie jednego VLANu muszą mieć adres IP i maskę zgodną z danym VLANem, aby mogły komunikować się ze sobą.

Technologia VLAN oferuje znacznie więcej możliwości niż tylko separacja portów. Jej wdrożenie, nawet w stosunkowo niewielkiej sieci, przynieść może wiele korzyści, do najważniejszych z nich należy zaliczyć:

- **ograniczony ruch rozgłoszeniowy** – każda sieć VLAN tworzy oddzielną domenę rozgłoszeniową;
- **łatwiejsze nadawanie uprawnień** – dla różnych sieci VLAN można tworzyć osobne Listy Kontroli Dostępu;
- **łatwiejsze wdrażanie "Quality of Service"** (priorytety dla usług sieciowych) – osobna sieć VLAN może transportować np. ruch tylko z telefonii VoIP;
- **bezpieczeństwo** – użytkownicy o różnych uprawnieniach mogą być odseparowani od siebie, ale także od sieci zarządzania (sieć zarządzania to VLAN utworzony na potrzeby konfiguracji urządzeń sieciowych);
- **logiczny podział sieci** – komputery, które powinny znajdować się w logicznych sieciach mogą być podłączone do różnych przełączników.

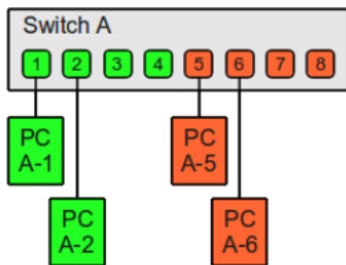
### Typy sieci VLAN:

Sieć VLAN tworzą porty jednego lub wielu przełączników. Wyróżnia się dwa typy sieci VLAN: *statyczne i dynamiczne*. W statycznych sieciach VLAN porty te konfigurowane są w przełączniku statycznie przez administratora. Przynależność danego portu do sieci VLAN nie może ulec zmianie, dopóki administrator nie zmieni konfiguracji. W sieciach dynamicznych natomiast przełącznik, odpytując specjalny serwer, automatycznie ustala, do jakiej sieci VLAN przypisać dany port, na przykład na podstawie adresu MAC maszyny, która rejestruje się w sieci komputerowej.

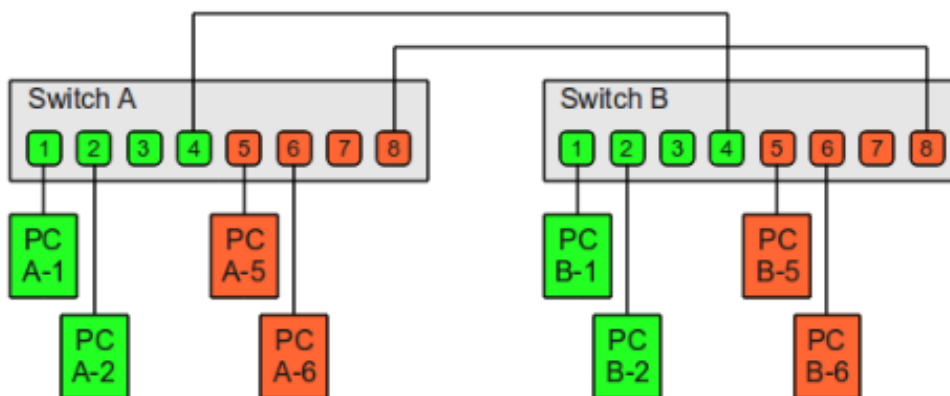
## Rodzaje sieci VLAN:

### Sieci VLAN wykorzystujące separację portów

w obrębie jednego switcha

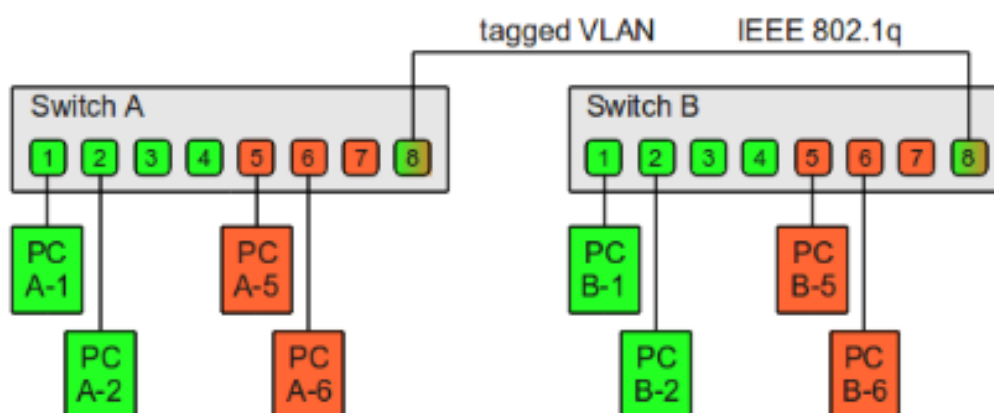


w obrębie wielu switchów



W przypadku takiej konfiguracji, w celu zapewnienia komunikacji pomiędzy switchami wymagane są dwa osobne połączenia kablowe pomiędzy obydwojema VLANami

### Sieci VLAN 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 VLANu. 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 różnych sieci VLAN. Takie łącze określane jest mianem łącza trunk.

### **Rodzaje VLANów:**

- Domyślny VLAN – VLAN 1, po starcie switcha wszystkie porty do niego należą, wszyscy mogą się ze sobą komunikować, należąc do jednej domeny broadcastowej, dopóki nie zostaną przydzielone do innych VLANów
- Natywny VLAN – dzięki niemu ramki nieotagowane, nie pochodzące od żadnego VLANu, są przesyłane przez porty typu trunk
- Data VLAN – często używane określenie logiczne VLANu przesyłającego dane użytkowników
- Voice VLAN – określenie logiczne - VLAN stworzony specjalnie dla VoIP

### **Tryby portów na switchu:**

- *switchport mode access* - tryb na urządzeń końcowych podłączonych do switcha
- *switchport mode trunk* - tryb do połączeń pomiędzy switchami lub połączeń switch-router

### **Konfigurowanie sieci VLAN**

Statyczna konfiguracja sieci VLAN polega na ręcznym przypisywaniu portów przełącznika do sieci VLAN (tzw. access-porty). Można to skonfigurować bezpośrednio w przełączniku za pomocą interfejsu CLI. Porty te zachowują przypisaną im konfigurację sieci VLAN do momentu ręcznej jej zmiany.

Każdy VLAN ma swój numer, dla łatwości zarządzania można nadać też nazwę. Są dwa rodzaje VLANów: podstawowe i rozszerzone.

#### **Podstawowe:**

- VLAN ID od 1 do 1005
- ID od 1002 do 1005 zarezerwowane są dla Token Ringa i VLANów FDDI
- VLANy o numerze 1 i od 1002 do 1005 są tworzone automatycznie i nie da się ich usunąć

- do automatycznego zarządzania VLANami służy protokół VTP

#### Rozszerzone:

- VLAN ID od 1006 do 4094
- informacje zapisywane są w pliku działającej konfiguracji
- VTP nie działa w zakresie rozszerzonych VLANów

VLANy można konfigurować w trybie globalnej i VLANowej konfiguracji. Dotyczy to switchy będących w trybie serwera bądź transparentnym.

Przypisywanie portów do danego VLANu oraz określanie jego trybu odbywa się w konfiguracji danego portu.

```
Switch#configure terminal
Switch(config)#vlan vlan id
Switch(config-vlan)#name nazwa VLANu
Switch(config-vlan)#exit
```

Do usunięcia VLANa wystarczy wpisać no przed komendą vlan

Następnym krokiem jest przypisanie sieci VLAN do jednego lub wielu interfejsów, np.:

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan VLAN id
```

#### Sprawdzanie konfiguracji.

Zalecaną zasadą jest sprawdzanie konfiguracji sieci VLAN. Korzystamy z poleceń:

```
show vlan
```

```
show vlan brief - skrócona tabelka z VLANami
```

### **Konfiguracja łącza trunkingowego**

Konfiguracja portu jako łącza trunkingowego dla wszystkich VLANów;

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
```

