

**Politechnika Krakowska**

Katedra Automatyki i Technik Informatycznych

# **Laboratorium Sieci Komputerowych**

2015/2016



Routing pomiędzy sieciami VLAN

## 1.1 Routing pomiędzy sieciami VLAN

Wiemy już, jak tworzyć sieci VLAN, usuwać istniejące oraz konfigurować protokół VTP. Wiemy, że sieci VLAN umożliwiają odseparowanie ruchu sieciowego, np. pomiędzy dwoma działami. Pomimo wszystkich zalet, jakie niesie ze sobą wykorzystywanie sieci VLAN, często zdarza się, że odseparowane sieci muszą się w jakiś sposób komunikować. Niestety, jeśli komputery są podłączone do osobnych sieci VLAN, nie jest to możliwe.

Istnieją techniki, które umożliwiają komunikację między sieciami VLAN. Technologia ta nazywa się routingiem pomiędzy VLAN (ang. *Inter VLAN Routing*) i jest realizowana przez routery lub przełączniki 3. warstwy (ang. *Layer 3 Switching*).

W sieci bez VLAN jedynym urządzeniem, które tworzy odrębne domeny rozgłoszeniowe, jest router. Nierzadko router jest jeden, a stacji roboczych kilkaset. Wszystkie znajdują się w jednej domenie rozgłoszeniowej. Niewątpliwie wpływa to negatywnie na przepustowość sieci.

Utworzenie sieci VLAN logicznie podzielić na odrębne domeny rozgłoszeniowe. W konsekwencji znacznej redukcji ulegnie ilość rozsyłanych rozgłoszeń, komunikacja będzie jednak możliwa poprzez router, na którym uruchomiony jest routing między sieciami VLAN.

Drugą zaletą jest bezpieczeństwo i możliwość kontrolowania ruchu sieciowego. Kiedy wszystkie komputery należą do jednej sieci VLAN, filtrowanie ruchu jest - oczywiście - możliwe, jednak bardzo trudne do zrealizowania. Ponadto nie mają zastosowania listy kontroli dostępu (ang. *Access Lists*), a ich konfiguracja staje się bardzo skomplikowana.

Listy dostępu są to wprowadzone w urządzeniu sieciowym reguły, jakie muszą zostać spełnione, aby np. przesłać pakiet dalej lub zablokować jego przesłanie.

Wprowadzenie podziału na odrębne sieci VLAN i połączenie ich poprzez zastosowanie routingu pomiędzy sieciami VLAN, a następnie dodanie filtrowania ruchu pomagają w pełni zapanować nad rozsyłanymi informacjami. Dzięki temu sieć staje się bezpieczna i wydajniejsza.

## 1.2 Rodzaje routingu między sieciami VLAN

Pamiętajmy, że każda sieć VLAN powinna posiadać swoją odrębną adresację. Oznacza to, że sieć VLAN to odrębna podsieć

Najczęściej stosowanym schematem jest tworzenie podsieci w ten sposób, aby pokrywały się z numerem utworzonej sieci VLAN.

Jeśli utworzyliśmy sieć VLAN o numerze 10, dla niej podsieć w klasie C będzie np. 192.168.10.0. Dla sieci VLAN29 będzie to 192.168.29.0 itd. Oczywiście, nie jest to wymogiem, jednak podczas konfiguracji routingu taki schemat postępowania bardzo ułatwia konfigurację i rozeznanie w sieci.

Generalnie wyróżniamy trzy rodzaje routingu między sieciami VLAN:

- jeden interfejs routera —jedna sieć VLAN,
- „router na patyku”,
- zastosowanie przełączników warstwy 3.

**Jeden interfejs routera - jedna sieć VLAN** jest rozwiązaniem, które wymaga zastosowania routera z wieloma interfejsami. Dzieje się tak, ponieważ każda sieć VLAN musi zostać podłączona z interfejsu przełącznika do interfejsu routera osobnym przewodem.

W takim rozwiązaniu marnuje się dość dużą ilość interfejsów zarówno przełączniki jak i routera. W przypadku przełącznika na każdą sieć VLAN przypadają dwa interfejsy. Przełączniki posiadają dużą liczbę interfejsów, więc w praktyce nie jest to duże obciążenie, jednak w przypadku routerów utworzenie dziesięciu sieci VLAN pociąga za sobą konieczność posiadania na routerze co najmniej jedenastu interfejsów (jeden dodatkowy interfejs musi zostać przeznaczony do podłączenia innych sieci lub urządzeń).

Jak widzimy, powyższe rozwiązanie jest dobre, ale tylko wtedy, kiedy sieć nie jest duża, a liczba utworzonych sieci VLAN nie przekracza trzech. Obecnie w sieciach komputerowych jest rozwiązaniem niepraktycznym.

Kolejnym rozwiązaniem jest **zastosowanie przełączników warstwy 3**.

Przełączniki warstwy 3. pełnią funkcje typowe dla przełączników warstwy 2., lecz dodatkowo są wyposażone w mechanizmy umożliwiające przejęcie funkcji routingu. Pamiętajmy jednak, że przełącznik warstwy 3. nie jest routerem. Niektóre mechanizmy i funkcje są zaimplementowane tylko routerach i na razie nie zanoszą się na to, aby było inaczej.

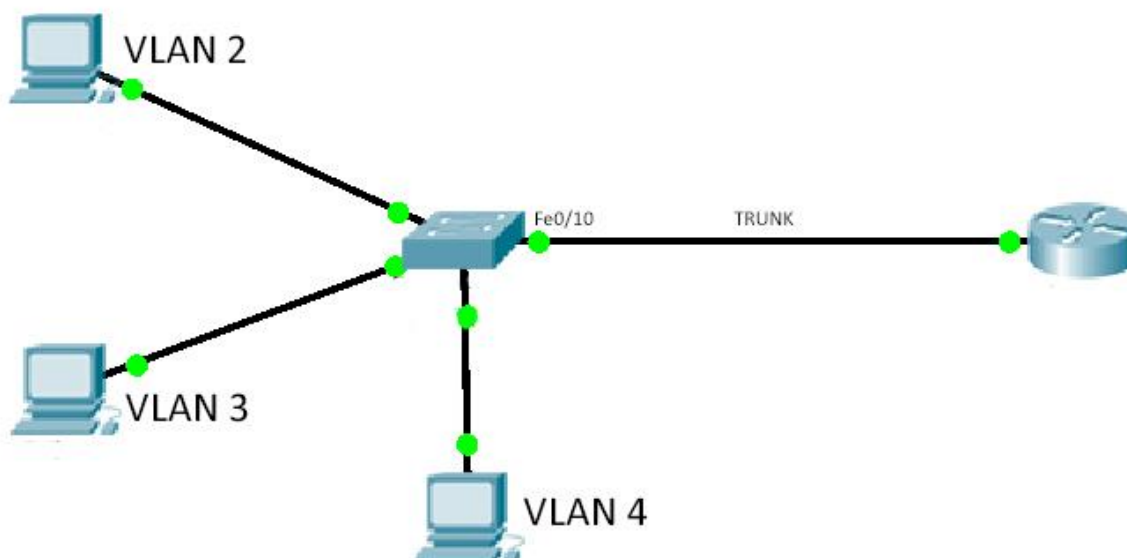
Na przełączniku warstwy 3. tworzone są wirtualne interfejsy. Interfejsy posiadają w większości przypadków te same nazwy, co tworzone sieci VLAN. Tak więc dla sieci VLAN2 interfejsem wirtualnym będzie interfejs VLAN2.

Po utworzeniu interfejsu należy przypisać mu adres IP z zakresu podsieci VLAN. Po zakończeniu konfiguracji interfejsu oraz routingu przełącznik zajmuje się przekazywaniem ruchu z jednej sieci VLAN do drugiej. Tej funkcji nie pełni już router, który bez wątpienia jest mniej obciążony. Niewątpliwie jest to zaleta tego typu rozwiązania.

Należy pamiętać, że przełączniki warstwy 3. są droższe od swoich odpowiedników z warstwy 2. i podczas zakupu należy liczyć się z większymi wydatkami. Jednak w parze z kosztami idzie znacznie większa wydajność, która osiągana jest poprzez ekspresowe przekazywanie ramek między różnymi sieciami VLAN. Metoda ta wbudowana jest w przełączniki warstwy 3. i zwana mechanizmem CEF (ang. Cisco Express Forwarding). Polega na bardzo szybkim przekazywaniu ramek pomiędzy sieciami VLAN na podstawie specjalnych tablic przypominających w działaniu tablice routingu.

Metodą która bez wątpienia jest kompromisem pomiędzy dwoma wcześniej opisanymi, jest **„router na patyku”**.

Spójrzmy na poniższy rysunek:



Metoda o nazwie „router na patyku” (*ang. router-on-a-stick*) polega na utworzeniu połączenia **trunk** do routera, na którym realizowany będzie routing pomiędzy sieciami VLAN.

Na rysunku widzimy trzy stacje robocze podłączone do przełącznika. Każda stacja znajduje się w innej sieci VLAN, a co za tym idzie, w różnej podsieci. Jeden interfejs przełącznika, w tym przypadku Fe0/10, skonfigurowany jest jako **trunk**, pozostałe natomiast w trybie **access**.

Metoda ta wymaga konfiguracji na routerze **podinterfejsów** (*ang. subinterfaces*). Zauważ, że jeden interfejs routera jest interfejsem głównym, do którego połączony jest trunk z przełącznika. Główny interfejs należy więc podzielić w tym konkretnym przypadku na trzy **podinterfejsy**. Robi się tak, ponieważ każda sieć VLAN (podsieć) musi posiadać swój interfejs. Tak więc na routerze utworzono trzy **podinterfejsy** — 0.2, 0.3, 0.4 — zgodnie z nazwami utworzonych na przełączniku sieci VLAN. Pierwszy człon nazwy **podinterfejsu** to cyfra 0, ponieważ interfejs główny również zaczyna się od 0.

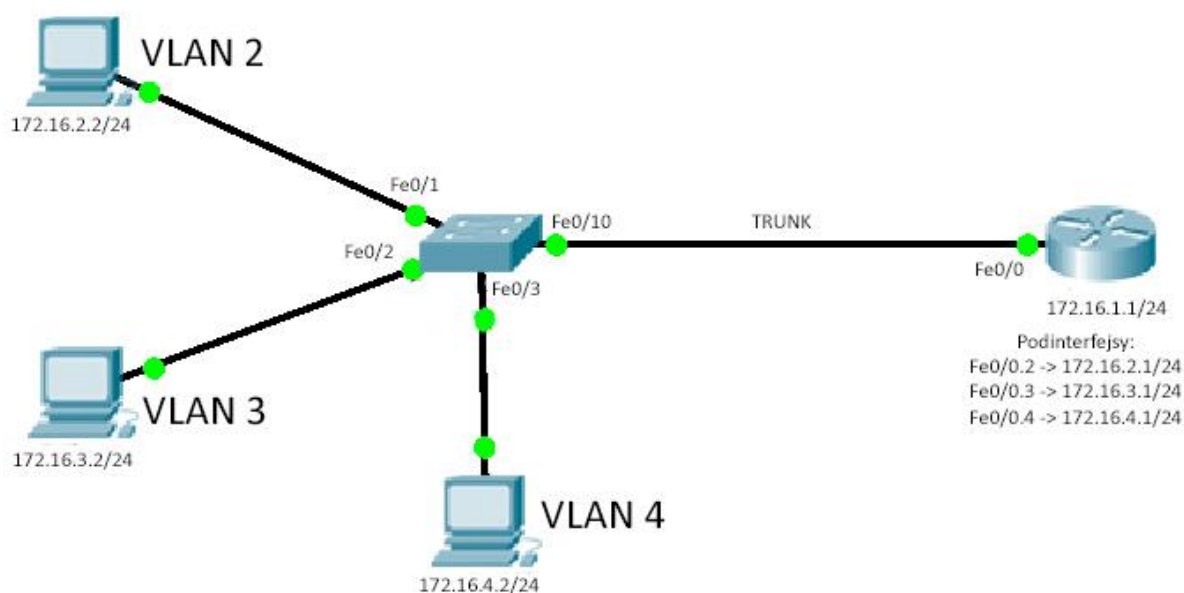
Każdy **podinterfejs** na routerze posiada swój adres IP, jest on adresem domyślną bramy dla stacji roboczych podłączonych do określonej sieci VLAN.

Dość istotną uwagą jest to, że połączenie **trunk** pomiędzy przełącznikiem a routerem musi posiadać szybkość co najmniej 100 Mb/s. Niestety, do tego celu nie można wykorzystać interfejsów 10 Mb/s.

W praktyce jest to bardzo często stosowane rozwiązanie. Nie marnuje bowiem dużej ilości interfejsów przełącznika, a co najważniejsze - routera. Wadą jest dodatkowi obciążenie procesora routera przez rozszerzenie jego tablic routingu oraz słaba wydajność, np. w porównaniu do przełączników warstwy 3.

#### **Przykładowa konfiguracja routingu pomiędzy sieciami VLAN — „router na patyku”**

Przed konfiguracją routingu nadajmy wszystkim stacjom roboczym odpowiednie adresy IP. Podłączmy je do odpowiednich interfejsów. Możemy posłużyć się poniższym rysunkiem i ustawić na początek te same adresy.



Najpierw zalogujemy się do przełącznika SW1. Utwórzmy trzy sieci VLAN. W tym celu w trybie konfiguracji globalnej użyjemy polecenia `vlan [numer]`, W kolejnym kroku przypiszmy do sieci VLAN określone interfejsy. Następnie ustawmy port FE0/10 jako `trunk`. Jest to port łączący przełącznik z routerem.

Oto przykład:

```
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config)#do sh vlan
-----
Switch(config-vlan)#exit
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit

Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit

Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
Switch(config-if)#exit
Switch(config)#do sh vlan
```

```
-----  
Switch(config)#interface fastEthernet 0/10  
Switch(config-if)#switchport mode trunk  
-----
```

W kolejnym kroku zalogujemy się do routera w celu ustawienia podinterfejsów. Po zalogowaniu się przejdźmy do kontekstu podinterfejsu, używając polecenia `interface FastEthernet [numer_podinterfejsu]`. Następnie wydajmy polecenie `encapsulation dot1Q [numer_sieci_vlan]`. Polecenie służy do przypisania podinterfejsu do konkretnej sieci VLAN. Pamiętajmy, że podinterfejs zawsze pracuje w kontekście konkretnej podsieci oraz sieci VLAN. Powyższe czynności wykonajmy do każdego z podinterfejsów. Oto przykład:

```
Router(config)#interface fastEthernet 0/0  
Router(config-if)#ip address 172.16.1.1 255.255.255.0  
Router(config-if)#no sh  
Router(config-if)#exit  
Router(config)#
```

```
Router(config)#interface fastEthernet 0/0.2  
Router(config-subif)#encapsulation dot1Q 2  
Router(config-subif)#ip address 172.16.2.1 255.255.255.0  
Router(config-subif)#exit
```

```
Router(config)#interface fastEthernet 0/0.3  
Router(config-subif)#encapsulation dot1Q 3  
Router(config-subif)#ip address 172.16.3.1 255.255.255.0  
Router(config-subif)#exit
```

```
Router(config)#interface fastEthernet 0/0.4  
Router(config-subif)#encapsulation dot1Q 4  
Router(config-subif)#ip address 172.16.4.1 255.255.255.0  
Router(config-subif)#exit  
Router(config)#exit
```

```
Router#sh ip int br
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	172.16.1.1	YES	manual	up	up
FastEthernet0/0.2	172.16.2.1	YES	manual	up	up
FastEthernet0/0.3	172.16.3.1	YES	manual	up	up
FastEthernet0/0.4	172.16.4.1	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

-----  
**Uwaga!!!!!!**

**Podinterfejsy dziedziczą status po interfejsie głównym.**

**Gdyby Fe0/0 był wyłączony również i podinterfejsy byłyby wyłączone.**

-----

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
      172.16.0.0/24 is subnetted, 4 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, FastEthernet0/0.2
C       172.16.3.0 is directly connected, FastEthernet0/0.3
C       172.16.4.0 is directly connected, FastEthernet0/0.4
```

Wszystkie wpisy są traktowane jako trasy bezpośrednio podłączone. I tak np. sieć 172.16.2.0 osiągnięta jest poprzez podinterfejs FastEthernet0/0.2.

Zakończyliśmy konfigurację routera i przełącznika. Teraz nadajmy adresy 1P poszczególnym, stacjom roboczym. Pamiętajmy, aby każdej stacji roboczej w naszym przykładzie nadać odpowiedni adres bramy domyślnej. Adresem bramy jest adres IP podinterfejsu na routerze.

Po konfiguracji stacji roboczych możemy sprawdzić, czy komunikują się ze sobą. Wykonajmy ping z dowolnie wybranej stacji roboczej na inną.

## Literatura

[1] „W drodze do CCNA” A. Józefiok