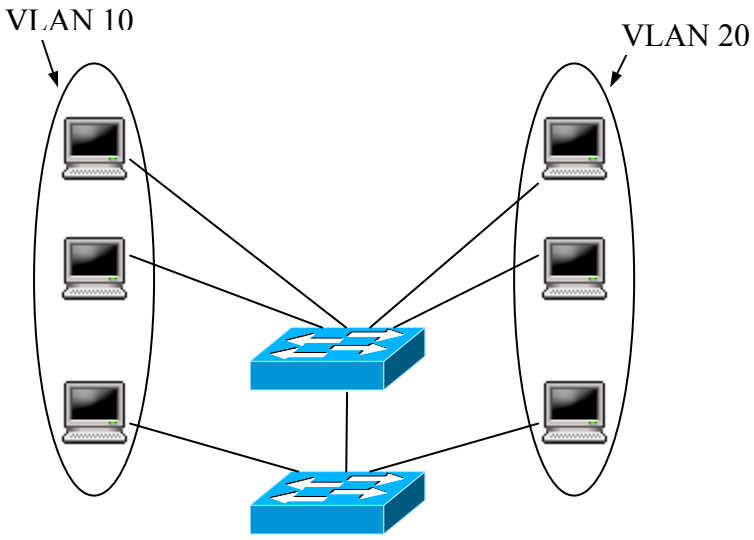
Konfigurowanie sieci VLAN

1 Wprowadzenie

Sieć VLAN (ang. Virtual LAN) to wydzielona logicznie sieć urządzeń w ramach innej, większej sieci fizycznej. 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, urządzeniach sieciowych warstwy 2 modelu ISO/OSI. 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. Ideę sieci VLAN zilustrowano na poniższym rysunku.



Ze stosowaniem sieci VLAN wiąże się kilka korzyści. Pozwalają one ograniczyć ruch rozgłoszeniowy, gdyż rozgłaszane ramki trafiają tylko do komputerów w obrębie danej sieci VLAN, nie „zalewają" całej sieci LAN. Ponadto, stosując sieci VLAN łatwo jest dostosować strukturę sieci do zmian w organizacji, ponieważ administrator może dokonać zmian topologii sieci programowo, a nie sprzętowo. Na przykład jeśli użytkownik należący do danej sieci VLAN zmienia stanowisko pracy, administrator po prostu konfiguruje przełącznik tak, by nowe stanowisko należało do odpowiedniej sieci VLAN. Do odzwierciedlenia zmiany administrator używa oprogramowania, a nie sprzętu (okablowania). Taka elastyczność jest szczególnie ceniona w dużych sieciach, w których często zachodzą zmiany w fizycznej topologii sieci. I wreszcie, podział sieci fizycznej na wiele sieci VLAN zwiększa bezpieczeństwo sieci komputerowej już z racji samej tylko separacji ruchu sieciowego w różnych sieciach VLAN.

1.1 Rodzaje sieci VLAN

Sieć VLAN tworzą porty jednego lub wielu przełączników. Wyróżnia się dwie odmiany sieci VLAN: *statyczne* i *dynamiczne*. W statycznych sieciach VLAN porty te konfigurowane są w przełącznikku 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.

1.2 Identyfikacja sieci VLAN

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.

Istnieje kilka sposobów oznaczania ramek, lecz jeden z nich, zgodny z powyższym opisem, objęto standardem **IEEE 802.1Q**. Podejście to nazywane jest etykietowaniem ramek (ang. *frame tagging*).

1.3 Komunikacja między sieciami VLAN

Przełączniki nie mogą przesyłać ramek między różnymi sieciami VLAN, gdyż naruszałoby to podstawową ideę tworzenia sieci VLAN - separację ruchu sieciowego. Do komunikacji między sieciami VLAN stosowane są więc urządzenia warstwy wyższej, sieciowej - rutery. Każda sieć VLAN na wyższym poziomie przekłada się na odrębną sieć IP. Zadaniem rutera zaś jest przenoszenie ruchu sieciowego między różnymi sieciami IP. W ten sposób uzyskuje się możliwość komunikowania różnych sieci VLAN.

Niniejsze ćwiczenie polega na utworzeniu kilku sieci VLAN w dwóch przełącznikach i połączniu ich za pomocą rutera.

2. Zadania

1. Na wzór punktu 1 Dodatku, w dwóch przełącznikach Cisco Catalyst 3550 skonfiguruj kilka statycznych sieci VLAN połączonych łączem trunk. Do każdej sieci VLAN powinny należeć przynajmniej 2 komputery, podłączone do różnych przełączników. Przed i po skonfigurowaniu sieci VLAN należy stwierdzić, czy możliwa jest komunikacja między komputerami w ramach jednej sieci VLAN i pomiędzy różnymi sieciami VLAN.
2. Na wzór punktu 2 Dodatku, skonfiguruj ruter Cisco 2800 tak, by komputery należące do różnych sieci VLAN mogły się komunikować. Użyj jednego interfejsu GigabitEthernet rutera i kilku jego podinterfejsów.

3. Pytania sprawdzające

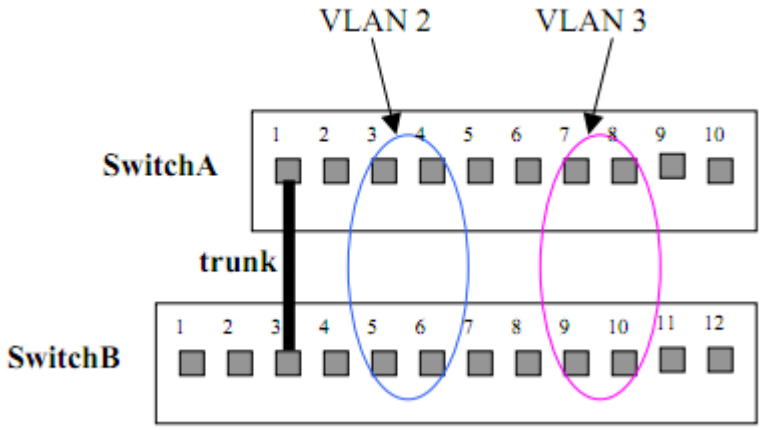
1. Co to jest sieć VLAN i jakie są korzyści ze stosowania tej technologii?
2. Jak przebiega identyfikacja ramek w sieciach VLAN?
3. Czy pojedynczy port przełącznika (port, który nie pracuje w trybie trunk) należy zawsze do dokładnie jednej sieci VLAN ?
4. Dlaczego do komunikowania różnych sieci VLAN potrzebna jest funkcjonalność rutera?
5. Jakie jest uzasadnienie dla separowania ruchu sieciowego poprzez tworzenie różnych sieci VLAN i późniejszego komunikowania tych sieci poprzez ruter? Czym takie działanie różni się od sytuacji, w której w ogóle nie zastosowano sieci VLAN ?
6. Jak stosując technologię sieci VLAN można podnieść bezpieczeństwo sieci przewodowej (np. sieć pracownicza), do której podłączony jest bezprzewodowy punkt dostępowy, tworzący sieć *hot-spot*?
7. Czy numer podinterfejsu (liczba poprzedzona kropką) w ruterze Cisco musi być równa numerowi sieci VLAN, do której ten podinterfejs należy? (patrz dodatek i literatura)

4. Literatura

1. Koncepcja sieci VLAN – książka A. S. Tanenbaum: Sieci komputerowe, Helion 2004.
2. Artykuł firmy 3Com wprowadzający do technologii VLAN: http://www.3com.com/other/pdfs/solutions/en_US/20037401.pdf
3. Standard IEEE 802.1Q: http://standards.ieee.org/getieee802/ .
4. Artykuł „Creating Ethernet VLANs on Catalyst Switches”: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_configuration_example09186a008009478e.shtml
5. Artykuł “Configuring InterVLAN Routing with Catalyst Switches”: http://www.cisco.com/en/US/tech/tk389/tk815/technologies_configuration_example09186a008015f17a.shtml

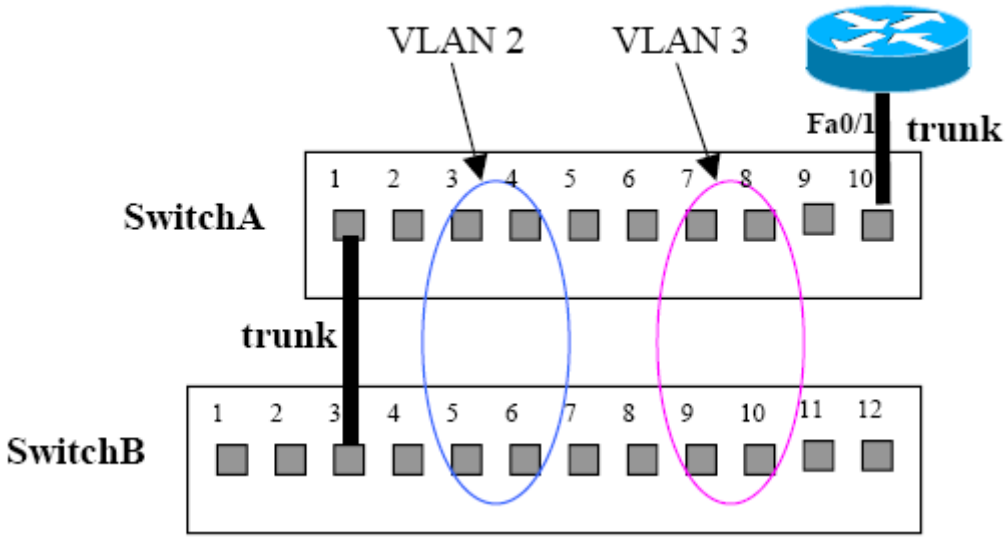
DODATEK

1. Przykładowa konfiguracja dwóch sieci VLAN w dwóch przełącznikach połączonych łączem trunk.




```
SwitchA> enable
SwitchA# configure terminal
SwitchA(config)# interface GigabitEthernet 0/3
SwitchA(config-if)# !przypisanie portow 3 i 4 do sieci VLAN 2
SwitchA(config-if)# switchport access vlan 2
SwitchA(config-if)# interface GigabitEthernet 0/4
SwitchA(config-if)# switchport access vlan 2
SwitchA(config-if)# !przypisanie portow 5 i 6 do sieci VLAN 3
SwitchA(config-if)# interface GigabitEthernet 0/7
SwitchA(config-if)# switchport access vlan 3
SwitchA(config-if)# interface GigabitEthernet 0/8
SwitchA(config-if)# switchport access vlan 3
SwitchA(config-if)# interface GigabitEthernet 0/1
SwitchA(config-if)#!utworzenie lacza VLAN trunk
SwitchA(config-if)# switchport trunk encapsulation dot1q
SwitchA(config-if)# switchport mode trunk
```

2. Przykładowa konfiguracja rutera łączącego dwie sieci VLAN.




```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/1
Router(config-if)# no shutdown
Router(config-if)# !utworzenie pierwszego podinterfejsu
Router(config-if)# interface GigabitEthernet 0/1.2
Router(config-if)# !umieszczenie podinterfejsu w sieci VLAN 2
Router(config-if)# encapsulation dot1q 2
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# !utworzenie drugiego podinterfejsu
Router(config-if)# interface GigabitEthernet 0/1.3
Router(config-if)# !umieszczenie podinterfejsu w sieci VLAN 3
Router(config-if)# encapsulation dot1q 3
Router(config-if)# ip address 192.168.2.1 255.255.255.0
```

Uwaga – port przełącznika, do którego podłączony jest ruter, musi również zostać skonfigurowany jako łącze trunk.