

P O L I T E C H N I K A W R O C Ł A W S K A

W Y D Z I A Ł E L E K T R O N I K I

Katedra Systemów i Sieci

Komputerowych

T E C H N O L O G I E S I E C I O W E 2

Konfigurowanie sieci VLAN

CEL ĆWICZENIA

Celem ćwiczenia jest opanowanie umiejętności konfiguracji sieci VLAN oraz łącza typu trunk w oparciu o protokół IEEE 802.1q na przełącznikach Cisco 2900.

WPROWADZENIE

VLAN

Jednym z najpopularniejszych urządzeń sieciowych, stosowanych powszechnie w biurach, jak i w domach, są przełączniki (ang. switch). Działają one w warstwie łącza danych (druga) modelu ISO/OSI. Głównym zadaniem switcha w sieci Ethernet jest przełączanie ramek na podstawie adresu MAC urządzeń.

W przypadku dużych sieci stosowany jest podział funkcjonalny urządzeń podpiętych do sieci, np. sieć administracyjna i sieć pracownicza. Innym przykładem może być podział sieci komputerowej na kampusie na sieć studencką i pracowniczą. Wskazane jest fizycznie rozdzielanie wspomnianych sieci, ze względu na minimalizację obciążenia oraz bezpieczeństwo. W klasycznym podejściu, rozwiązaniem tego problemu byłoby stworzenie dwóch rozłącznych infrastruktur sieciowych osobno dla sieci studenckiej i sieci pracowniczej. Powoduje to znaczne podniesienie kosztów budowy takiej sieci, wymaga więcej miejsca do instalacji sprzętu, większych nakładów finansowych na utrzymanie i zarządzanie taką siecią. W przypadku stosowania tylko dwóch sieci koszty rosną znacząco, a w przypadku zapotrzebowania np. na pięć sieci, są już najprawdopodobniej nie do zaakceptowania od strony ekonomicznej. Z tego powodu wprowadzono technologię wirtualnych sieci lokalnych (ang. Virtual Local Area Network, VLAN). Dzięki tej technologii istnieje możliwość fizycznego wydzielenia kilku sieci lokalnych w ramach jednego urządzenia klasy switch. Dla każdej sieci definiowany jest oddzielny VLAN, a następnie poszczególne porty przełącznika przydzielane są do odpowiednich VLAN'ów wg zapotrzebowania. Widać wyraźnie, że przydział do VLAN'ów jest dokonywany w oparciu o fizyczne przyłącze hosta do switch. Takie podejście pozwala w przyszłości całkowicie zmodernizować infrastrukturę sieciową, ponieważ VLAN'y można dowolnie modyfikować i ustawiać, zatem jedno stanowisko komputerowe w pierw może należeć do sieci pracowniczej, a potem zostać przełączone do sieci studenckiej. Taka zmiana nie będzie wymagała fizycznej ingerencji w infrastrukturę sieciową, wystarczy zmienić przynależność danego portu do odpowiedniego VLAN'u.

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).

Ze względu na oddzielenie komunikacji pomiędzy VLAN'ami, wymiana informacji pomiędzy nimi jest możliwa tylko w warstwie sieciowej (trzeciej) modelu ISO/OSI. Zatem przy pomocy klasycznego switcha z obsługą VLAN'ów nie da się tego zrobić. Wymagany jest do tego router lub tzw. switch warstwy trzeciej, czyli przełącznik posiadający także funkcje routera.

Trunk

Najczęściej zastosowanie VLAN'ów nie ogranicza się do pojedynczego przełącznika. Sieć komputerowa pokrywa kilka pięter i na każdym z nich są niezbędne te same VLAN'y, np. studencki i pracowniczy. W tej sytuacji istnieje kilka przełączników na których skonfigurowane zostały takie same VLAN'y. Pożądane jest aby użytkownicy należący do tej samej grupy roboczej (np. studenci lub pracownicy) mogli się komunikować bez problemu, tak jakby byli ze sobą bezpośrednio połączeni. Aby umożliwić taką komunikację należałoby pomiędzy switchami ustanowić łącza uplink dla każdego VLAN'u. Powoduje to, że rośnie zapotrzebowanie na porty i może prowadzić do tego że wymagane są kolejne drogie urządzenia. Rozwiązaniem tego problemu są łącza typu trunk. Taki łączę pomiędzy dwoma przełącznikami, nie należy do żadnego VLAN'u i przenosi ruch z grupy VLAN'ów na jednym przełączniku do analogicznej grupy VLAN'ów na drugim przełączniku. Ważne jest to, że taki ruch nie jest mieszany i nadal poszczególne VLAN'y są od siebie wydzielone. Natomiast komunikacja pomiędzy odpowiadającymi sobie VLAN'ami w obu switchach jest możliwa bez potrzeby zastosowania routera.

Istnieją dwa podejścia do realizacji takiego podejścia: enkapsulacja lub tagowanie ramek. Przykładami protokołów umożliwiających działanie łącza typu trunk są ISL (enkapsulacja) i IEEE 802.1q (tagowanie). ISL jest starszym protokołem, należącym do Cisco i obsługiwanym tylko przez urządzenia tej firmy. 802.1q jest rozwiązaniem ogólnodostępnym jako międzynarodowy standard i obecnie najbardziej popularnym.

Komunikacja w ramach jednej sieci VLAN wykorzystującej łącza trunk (czyli sieci VLAN obejmującej więcej niż jeden przełącznik) jest możliwa dzięki technice 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.

Konfiguracja VLAN na przełącznikach Cisco

Wyświetlanie informacji o skonfigurowanych sieciach VLAN

```
Switch>show vlan
```

Definiowanie sieci VLAN

```
Switch(config)#vlan 10 // '10' to unikalny identyfikator tworzonej sieci VLAN
Switch(config-vlan)#name studenci // 'studenci' to unikalna nazwa VLAN'u
```

Dołączanie portu przełącznika do sieci VLAN

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access // konf. portu w trybie dostępu
Switch(config-if)#switchport access vlan 10 // dołączenie portu do vlan'u nr 10
```

Konfiguracja wielu portów jednocześnie

```
Switch(config)#interface range fa0/1-8
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
```

Konfiguracja interfejsu jako trunk

```
Switch(config)#int fa0/2
Switch(config-if)#switchport mode trunk
```

Konfiguracja sieci VLAN przechowywana jest w pliku *vlan.dat*. Usuwanie całej konfiguracji VLAN z przełącznika:

Uwaga: Zachowujemy szczególną ostrożność, dokładnie czytamy komunikaty. Częste przypadki usunięcia całej zawartości pamięci flash !!!.

```
Switch#delete flash:vlan.dat
```

Spanning Tree Protocol

W przełączanych lokalnych sieciach komputerowych nie mogą istnieć pętle, niemożliwe jest również utworzenie wielu fizycznych tras pomiędzy urządzeniami znajdującymi się w jednej domenie rozgłoszeniowej. Sytuacja taka powoduje, iż w przypadku awarii łącza lub przełącznika komunikacja staje się niemożliwa. Rozwiązaniem opisanego problemu niezawodności są protokoły, które umożliwiają skonfigurowanie dodatkowych, zapasowych łączy pomiędzy przełącznikami i 'wyłączenie' ich tak aby nie były wykorzystywane do przesyłania ramek. W razie awarii łącza podstawowego zapasowe łącze jest automatycznie uruchamiane, bez ingerencji administratora sieci.

Jednym z najpopularniejszych protokołów tego typu jest Spanning Tree Protocol, dostępny m. in. na przełącznikach Cisco. Protokół buduje tzw. drzewo opinające, obejmujące wszystkie przełączniki i część łączy w sieci. Łącza nie wykorzystane do budowy drzewa są 'wyłączane'. W przypadku awarii którejś z 'gałęzi' drzewa budowane jest nowe drzewo, z wykorzystaniem któregoś z dotychczas wyłączonych łączy. Budowę drzewa rozpoczyna się od wyboru przełącznika, który będzie korzeniem drzewa. Właściwy wybór korzenia jest istotny ze względu na optymalne działanie sieci.

W celu równomiernego rozłożenia ruchu w sieci, protokół STP potrafi konstruować osobne drzewa dla każdego z vlan'ów istniejących w sieci lokalnej.

Konfiguracja STP na przełącznikach Cisco

Protokół jest uruchamiany automatycznie i nie wymaga konfiguracji wstępnej.

Wyświetlanie informacji o drzewach i konfiguracji STP (dla wszystkich vlan'ów):

```
Switch#show spanning-tree
```

Wyświetlanie informacji o drzewie dla vlan'u nr 10:

```
Switch#show spanning-tree vlan 10
```

Zmiana priorytetu STP dla vlan'u nr 10 (korzeniem drzewa zostaje przełącznik o najniższym priorytecie):

```
Switch(config)# spanning-tree vlan 10 priority 8192 // priorytet jest wielokrotnością  
4096, z przedziału 0-61440
```

Dodatkowe informacje

Kurs Cisco CCNA semestr 2 i 3

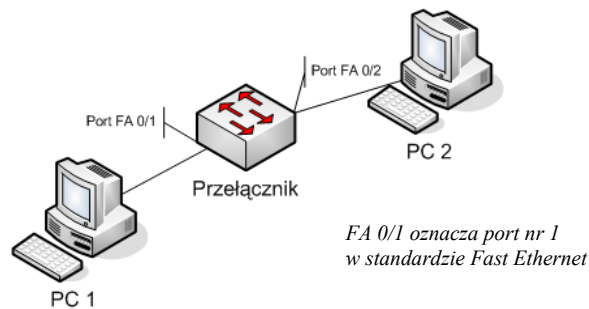
PRZYGOTOWANIE DO ĆWICZENIA

Przed przystąpieniem do wykonania ćwiczenia student powinien:

1. Przetestować działanie konfiguracji za pomocą symulatora *Packet Tracer*;
2. Wyjaśnić różnice pomiędzy kablem typu skrętka
 - straight-through (bez przeplotu)
 - crossover (z przeplotem)
 - rollover (konsolowy)
 - UTP, STP
3. Spośród kabli typu skrętka potrafi prawidłowo określić rodzaj kabla;
4. Wyjaśnić, którym kablem z powyższych należy bezpośrednio łączyć następujące pary urządzeń:
 - komputer – komputer
 - komputer – router
 - komputer – przełącznik
 - przełącznik – przełącznik
 - router – przełącznik
 - router – router
5. Wyjaśnić następujące pojęcia:
 - adres IP, maska, brama
 - adres fizyczny MAC
 - tablica routingu
 - tablica ARP
 - domena kolizyjna, domena rozgłoszeniowa
 - LAN, WAN
6. Wymienić w prawidłowej kolejności wszystkie warstwy modelu ISO/OSI;
7. Znać różnice między routerem, przełącznikiem, koncentratorem;
8. Znać różnice między LAN, VLAN i WLAN;
9. Biegłe używać polecenia `ping`;
10. Odczytać i zinterpretować konfigurację protokołu TCP/IP stacji roboczej;
11. Na podstawie adresu IP hosta i maski podsieci obliczyć adres IP podsieci;
12. Wskazać port szeregowy DB-9 w komputerze.
13. Umieć połączyć się z CLI przełącznika i konfigurować przełącznik w podstawowym zakresie.
14. Znać i rozumieć zasadę działania protokołu STP oraz algorytmu budowy drzewa opinającego
15. Odpowiedzieć na pytania
 - W jakim celu nadajemy przełącznikowi adres IP?
 - Jak przebiega identyfikacja ramek w sieciach VLAN?
 - Czy pojedynczy port przełącznika (port, który nie pracuje w trybie trunk) należy zawsze do dokładnie jednej sieci VLAN ?
 - W oparciu o jaką funkcjonalność odbywa się komunikowanie różnych sieci VLAN?
 - Jakie jest uzasadnienie dla separowania ruchu sieciowego poprzez tworzenie różnych sieci VLAN? Czym takie działanie różni się od sytuacji, w której nie zastosowano sieci VLAN ?
 - Jak VLAN wpływa na bezpieczeństwo sieci przewodowej (np. do której podłączony jest bezprzewodowy punkt dostępowy)?

ZADANIA DO WYKONANIA

1. Zestaw sieć tak, jak pokazano na schemacie. Zakres adresów przydzielany jest przez prowadzącego z puli dostępnej na końcu instrukcji.



- 1.1. Jakiego zestawu kabli należy użyć?
- 1.2. Zweryfikować połączenie pomiędzy hostami (podać sposób i wynik weryfikacji).
- 1.3. Zweryfikować połączenie PC1 z Internetem (podać sposób i wynik weryfikacji).
2. Podłączenie portu konsolowego
Połączyć się z przełącznikiem za pomocą portu konsolowego. Sprawdzić, czy na przełączniku obowiązuje konfiguracja domyślna. Jeśli nie, usunąć pliki *startup-config* oraz *vlan.dat*. Nadać przełącznikowi nazwę S1.
Zapisać i przeanalizować wyniki poleceń:

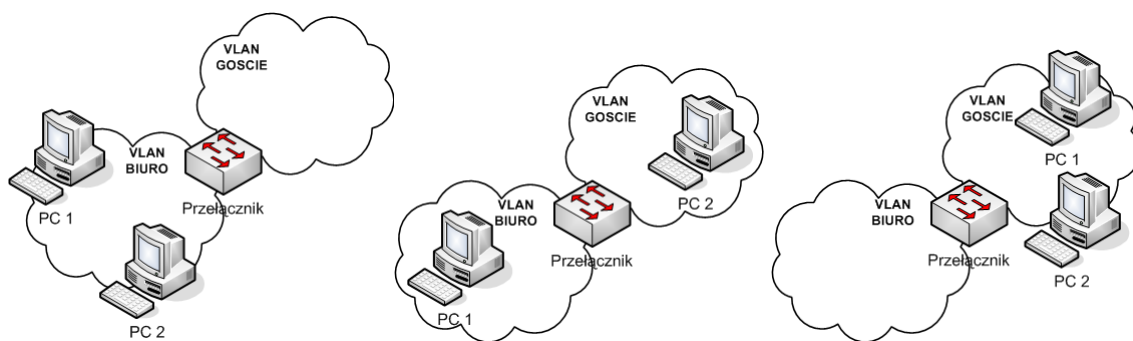
```
Switch>show version
```

```
Switch>show vlan
```
3. Tworzenie sieci VLAN
 - 3.1. Stworzyć dwie sieci VLAN dla pracowników biura (identyfikator 2) oraz gości (identyfikator 3). Jako nazwy sieci wpisać nazwiska członków grupy (bez polskich znaków)
 - 3.2. Zapisać i przeanalizować wynik polecenia:

```
Switch>show vlan
```
 - 3.3. Przypisać odpowiednie porty przełącznika S1 do VLAN 2 oraz VLAN 3 (zakresy portów przydzielane przez prowadzącego z puli dostępnej na końcu instrukcji)
 - 3.4. Zapisać i przeanalizować wyniki poleceń:

```
Switch#show vlan
```

```
Switch#show running-config
```
4. Weryfikacja połączenia
 - 4.1. Zweryfikować połączenie między hostami PC1 i PC2 w trzech następujących konfiguracjach (do których portów należy podłączyć hosty?)

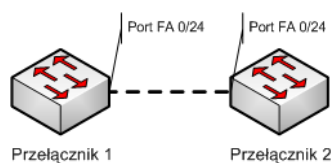


5. Konfiguracja dodatkowego przełącznika

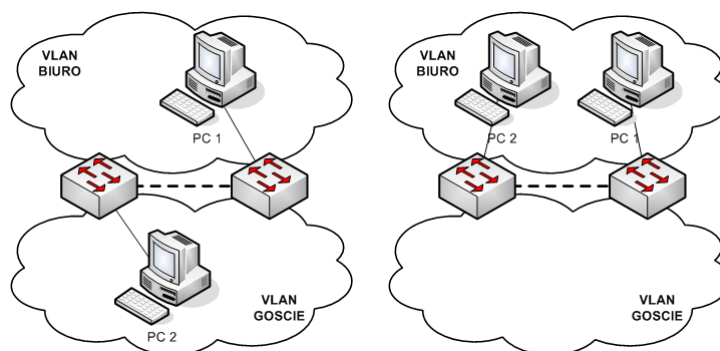
5.1. Skonfigurować kolejny przełącznik Cisco, przypisać odpowiednie porty do vlan'ów (zakresy portów przydzielane przez prowadzącego z puli dostępnej na końcu instrukcji). Nadać przełącznikowi nazwę S2.

6. Konfiguracja łącza trunkowego pomiędzy dwoma przełącznikami

6.1. Połączyć przełączniki tak, jak pokazano na schemacie:



6.2. Zweryfikować połączenie między hostami PC1 i PC2 w następujących konfiguracjach:



6.3. Pomiedzy przełącznikami skonfigurować łącze typu *trunk* w oparciu o protokół IEEE 802.1q

6.4. Zweryfikować połączenie między hostami PC1 i PC2 (tak jak w punkcie 6.2.).

6.5. Zapisać i przeanalizować wynik następujących poleceń

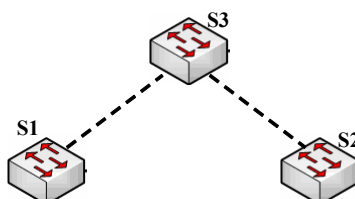
```
Switch#show vlan
```



```
Switch#show int fa 0/1 switchport
Switch#show int fa 0/24 switchport
Switch#show run
```

7. Konfiguracja z trzema przełącznikami

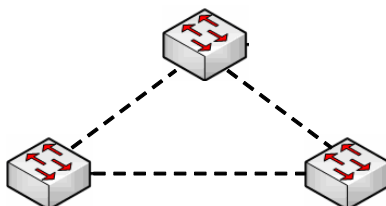
Rozłączyć *trunk* skonfigurowany w pkt. 6. Połączyć przełączniki S1 i S2 za pośrednictwem trzeciego przełącznika (o nazwie S3) – jak na rysunku poniżej.



Na trzecim przełączniku nie konfigurować żadnych portów w trybie dostępu (nie będą do niego podłączane żadne stacje robocze). Skonfigurować S3 tak, aby możliwa była komunikacja pomiędzy członkami vlan'ów podłączonymi przełączników S1 i S2.

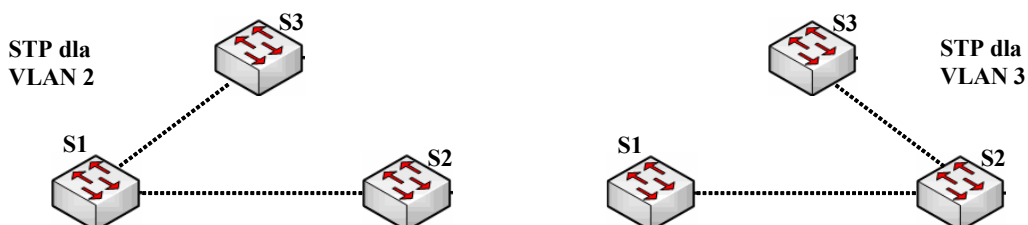
8. Analiza i konfiguracja protokołu STP

Połączyć przełączniki jak na rysunku.



8.1. Wyświetlić i przeanalizować budowę drzew STP dla obu sieci vlan.

8.2. Skonfigurować przełączniki w taki sposób, aby drzewa STP dla vlan'ów były takie jak na rysunku poniżej.



8.3. Wyświetlić i przeanalizować konfigurację STP dla obu sieci vlan.

9. Porządkowanie stanowiska

Przywrócić pierwotną konfigurację komputerów i przełączników.

KONFIGURACJE

Pula adresów:

- | | |
|----------------------|----------------------|
| 1. 10.0.0.64 /27 | 2. 10.0.1.32 /27 |
| 3. 10.10.0.96 /27 | 4. 10.4.0.64 /27 |
| 5. 10.100.0.192 /27 | 6. 10.0.0.16 /28 |
| 7. 10.0.10.32 /27 | 8. 10.1.1.96 /28 |
| 9. 10.1.1.160 /27 | 10. 10.2.2.64 /26 |
| 11. 10.11.12.128 /27 | 12. 10.3.3.128 /26 |
| 13. 10.9.8.32 /27 | 14. 10.20.30.192 /26 |
| 15. 10.0.0.96 /27 | 16. 10.10.10.0 /26 |
| 17. 10.1.1.224 /27 | 18. 10.11.12.192 /26 |
| 19. 10.0.10.64 /27 | 20. 10.0.5.176 /28 |

Pula portów dla VLAN:

	S1		S2	
	VLAN 2	VLAN 3	VLAN 2	VLAN 3
1.	1-4	6,11,13	4,7,9	12-21
2.	1,4,7	12-17	1,5,8	9-17
3.	3,19,21	8-15	3,6,21	8-16
4.	4,7,11	14-22	9-21	1,4,7
5.	5,6,9	10-18	1,2,6	7-18
6.	1-6	7,9,12	3-14	15,19,23
7.	4-11	1,3,15	2,4,8	12-17
8.	12-20	3,7,22	14-21	3,7,22
9.	2-9	1,16,20	8-12	1,7,19
10.	4,7,11	13,14,15,16	3-17	1,20,21
11.	3-11	2,16,22	2-7	1,16,22
12.	17-23	5,9,15	6,8,13	14-20
13.	8-13	1,6,21	2,5,9	10-21
14.	5,9,11	16-22	2-16	1, 17,20
15.	3-14	19,21,23	11-17	7,10,19
16.	5,7,12	13-21	2-20	1,21,23

OCENA ĆWICZENIA

Podczas oceniania ćwiczenia studenci powinni być przygotowani do przedstawienia wyników pracy wg następującego planu:

1. Szczegółowy opis zrealizowanych zadań
2. Opis i analiza otrzymanych wyników
3. Wnioski

Dodatkowo studenci powinni być w stanie udzielić prawidłowej odpowiedzi na wszystkie pytania postawione w zadaniach (odpowiedzi poprzez odpowiednie wydrukami z konsoli przełącznika, w szczególności polecenia grupy **show** oraz sposób i wynik weryfikacji połączeń w poszczególnych krokach).