SIECI KOMPUTEROWE I

Konfiguracja wirtualnych sieci LAN w przełączniku Ethernet

(na przykładzie przełącznika Ethernet HP ProCurve 2512/2524)

Struktura laboratorium

Celem ćwiczenia jest poznanie metod konfiguracji przełączników zarządzanych HP serii 2500.

Ćwiczenie jest wykonywane na komputerach wyposażonych w przewodowe interfejsy sieciowe, pracujących pod systemami MS Windows i GNU/Linux Xubuntu oraz z przełącznikami sieciowymi HP ProCurve 2512/2524..

Dla poprawnego wykonania poniższego ćwiczenia warto zapoznać się z dokumentacją „Management & Config guide".

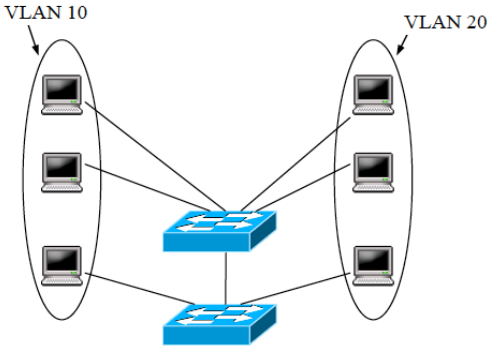
Wymagany zakres materiału

- zadania przełącznika warstwy 2 modelu OSI,
- adresacja IP, sprawdzanie poprawności połączenia i adresacji (test PING),
- parametry transmisji szeregowej RS232,
- obsługa programów: putty, minicom (linux), HyperTerminal (Windows),
- zestawianie połączeń dla protokołów: telnet, ssh, http.

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 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 rysunku 1.



Rys.1. Schemat ilustrujący koncepcję sieci wirtualnych.

Z zastosowaniem 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. Ponadto, podział sieci fizycznej na wiele sieci VLAN zwiększa bezpieczeństwo sieci komputerowej już z racji samej tylko separacji ruchu sieciowego w różnych sieciach VLAN.

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 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.

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).

Komunikacja między sieciami VLAN

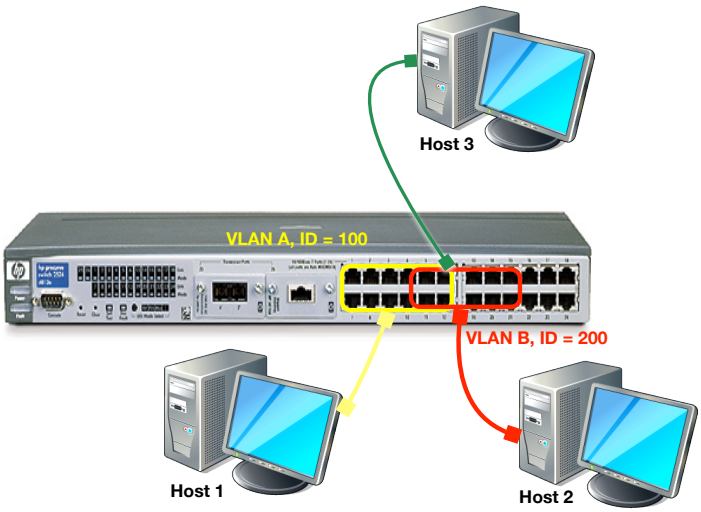
Przełączniki nie mogą przesyłać ramek między różnymi sieciami VLAN, gdyż naruszałoby to podstawową ideę tworzenia sieci VLAN - separację ruchu sieciowego. Do komunikacji między sieciami VLAN stosowane są więc urządzenia warstwy wyższej, sieciowej - rutery. Każda sieć VLAN na wyższym poziomie przekłada 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.

Przebieg ćwiczenia

Zadanie 1

Konfigurację sieci z wykorzystaniem VLAN omówiono na przykładzie sieci składającej się z trzech komputerów oraz przełącznika zarządzanego warstwy 2 modelu OSI. Modelową sieć przedstawia rysunek 2.



Rys. 2. Schemat sieci modelowej.

Host 1 należy do vlanu 100, host 2 należy do vlanu 200 a host 3 należy jednocześnie do vlanu 100 i 200.

Komputery podłączone są do portów przełącznika sieciowego (switcha): host 1 do portu **1**, host 2 do portu **5** a host 3 do portu **3**.

Wstępnie należy utworzyć odpowiednie vlany na przełączniku sieciowym oraz przydzielić do nich odpowiednie porty switcha. W ten sposób pojedyncza sieć fizyczna zostaje rozdzielona na dwie sieci logiczne.

VLAN w Linux-ie

W systemie Linux do tworzenia VLAN'ów wykorzystuje sie polecenie `vconfig`. Jest ono używane zarówno do tworzenia, jak i usuwania VLAN(ów) z systemu. Polecenie `vconfig` powoduje dodanie do systemu wirtualnego urządzenia ethernet, które reprezentuje VLAN w fizycznej sieci LAN. Poniżej zamieszczono opis wybranych opcji tego polecenia.

Polecenie	Uwagi / Opis
`add [interface-name] [vlan-id]`	tworzy urządzenie vlan na interfejsie o nazwie [interface-name]
`rem [vlan-device]`	usuwa urządzenie o podanej nazwie
`set_flag [vlan-device]`	ustawia flagę na urządzeniu o nazwie [vlan-device] możliwe ustawienia są następujące 0 (domyślnie) co oznacza ze pakiety są niezmienione przy przejściu przez interfejs lub 1 urządzenie [vlan-device] zachowuje się jak normalna karta NIC. Opcja ta ma znaczenie gdy ramki są tagowane.
`set_egress_map [vlan-device] [skb-priority] [vlan-qos]`	ustawia priorytet qos dla ramek wychodzących
`set_ingress_map [vlan-device] [skb-priority] [vlan-qos]`	ustawia priorytet qos dla ramek przychodzących
`set_ingress_map [vlan-device] [skb-priority] [vlan-qos]`	ustawia priorytet qos dla ramek przychodzących

Instalacja pakietu vconfig

Obecnie pakiet vconfig jest zwykle preinstalowany w systemie operacyjnym. W przeciwnym razie można go zainstalować używając polecenia:

```
root@studentN1# apt-get install vconfig
```

Po zainstalowaniu pakietu, umożliwiającego tworzenie VLANow na interfejsie sieciowym komputera, kolejnym krokiem który należy wykonać jest załadowanie modułu jadra o nazwie 8021q obsługującego vlany. Do weryfikacji czy moduł jest już załadowany wykorzystuje się polecenie:

```
root@studentN1# lsmod | grep 8021q
```

Jeśli w wyniku działania poleceń nie otrzyma się informacji lub komunikat o braku modułu, należy załadować moduł wykonując polecenie:

```
root@studentN1# modprobe 8021q
```

Poprawność załadowania modułu można stwierdzić powtarzając polecenia:

```
root@studentN1# lsmod | grep 8021q
```

Do tworzenia VLANów na istniejacych interfejsach sieciowych użyte zostanie polecenie vconfig.

Konfiguracja interfejsów na hostach

Do konfiguracji interfejsów służy polecenie *vconfig*. Na przykładzie hosta 3, przedstawiono konfigurację, zgodnie z którą powinien on mieć skonfigurowane na karcie dwa vlany.

Zostaną zatem użyte następujące polecenia:

```
root@studentN1#vconfig add eth0 100 – dodanie do systemu urządzenia wirtualnego eth0.100
root@studentN1#vconfig add eth0 200 - dodanie do systemu urządzenia wirtualnego eth0.200
```

W ten sposób utworzono w systemie dwa nowe, logiczne sieciowe interfejsy wirtualne, z których każdy przypisany jest do innego vlanu. W ich rezultacie, w systemie plików tworzone są następujące pliki:

```
/proc/net/vlan/vconfig – plik z konfiguracją vlanów na komputerze;
/proc/net/vlan/eth0.100
/proc/net/vlan/eth0.200 – pliki z ustawieniami priorytetów qos;
```

Ostatni etap konfiguracji interfejsów hosta to przypisanie im adresów IP. Można go wykonać na dwa sposoby:

- wykorzystując polecenie ifconfig – rozwiązanie które nie zapewni trwałości stworzonej konfiguracji,
- tworząc dla interfejsów pliki konfiguracyjne (pliki konfiguracyjne interfejsów sieciowych w dystrybucji xubuntu 14 znajdują się w /etc/sysconfig/network-scripts/.

W sprawozdaniu umieścić rezultaty / zrzuty ekranowe wyniku działania powyższych poleceń. Proszę opatrzyć je odpowiednim komentarzem.

UWAGA: Należy zwrócić uwagę iż dla urządzenia eth0 (urządzenia fizycznego na którym utworzone wirtualne interfejsy VLAN), nie należy przypisywać jakiegokolwiek adresu sieciowego, jednocześnie aktywując urządzenie w systemie. Odnośnie konfiguracji interfejsów wirtualnych należy zwrócić uwagę na opcję VLAN=yes. Brak tej opcji skutkuje nieutworzeniem interfejsu przy uruchamianiu systemu.

Konfiguracja przełącznika sieciowego

Przełączniki ProCurve z serii 2500 to niedrogie wieżowe przełączniki zarządzalne z 24 i 12 portami oraz automatycznym rozpoznawaniem szybkości 10/100 i 2 wolnymi gniazdami transceiverów na

łącza Gigabit lub 100Base-FX. Przełączniki ProCurve 2524 i 2512 udostępniają funkcję HP Auto-MDIX we wszystkich portach 10/100 i 100/1000 oraz funkcje wysokiej dostępności. Przełączniki ProCurve 2524 i 2512 umożliwiają niedrogą migrację do przełączników zarządzanych 10/100 z łączami nadrzędnymi. Oferują one:

1) Elastyczność i wysoką dostępność
    a. Protokół Link Aggregation Control Protocol (LACP) 802.3ad i trunking ProCurve: obsługuje jedno łącze agregowane obejmujące maks. 4 porty
    b. Spanning Tree Protocol (IEEE 802.1D): zapewnia połączenia nadmiarowe, zapobiegając jednocześnie powstawaniu pętli sieciowych
    c. Rapid Convergence Spanning Tree Protocol (802.1w): wydłuża czas pracy sieci bez przestojów przyspieszając odzyskiwanie sprawności po awarii łączy
2) Przełączanie w warstwie 2
    a. Obsługa i znakowanie (tagging) sieci VLAN: obsługa maksymalnie 30 sieci VLAN opartych na portach i dynamiczna konfiguracja znakowania (tagging) VLAN 802.1Q zapewniają bezpieczeństwo komunikacji między zespołami
    b. Protokół GVRP (Group VLAN Registration Protocol): umożliwia automatyczne rozpoznawanie sieci VLAN i ich dynamiczne przypisywanie
3) Bezpieczeństwo
    a. Ochrona portów: zapobiega nieautoryzowanemu dostępowi za pomocą MAC address lockdown
    b. 802.1x i serwery uwierzytelniania RADIUS: kontrola dostępu do portów zapewnia uwierzytelnianie i rozliczanie użytkowników
    c. TACACS+: dzięki serwerowi uwierzytelniania za pomocą haseł, ułatwia administrowanie bezpieczeństwem zarządzania przełącznikiem.

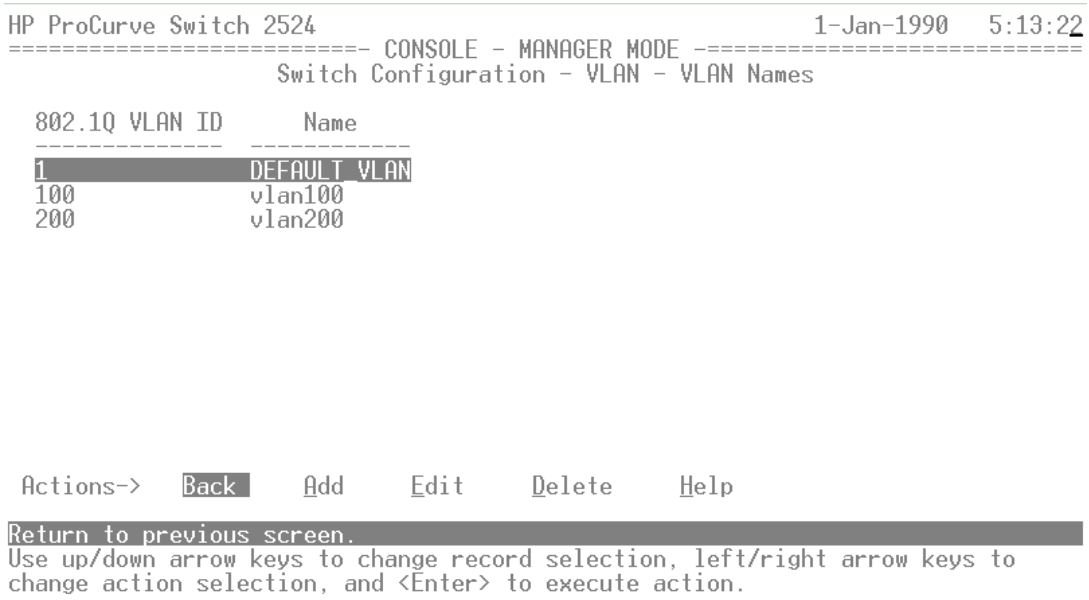
Przełączniki ProCurve 2524 i 2512 wspierają standard 802.1Q (obsługa i znakowanie sieci VLAN), a także posiadają zaimplementowany protokół GVRP. W ćwiczeniu nie korzysta się jednak z dobrodziejstw protokołu GVRP i zostanie wyłącznie przeprowadzona ręczna konfiguracja VLANów na portach.

1. Do połączenia ze switchem w celu jego konfiguracji należy wykorzystać konsolę podłączoną do portu RS komputera oraz program `putty`.
2. Po dokonaniu połączenia z konsolą switcha zostanie przeprowadzona konfiguracja urządzenia. Najprostszą metodą konfiguracji switchy HP procurve jest użycie zaimplementowanego interfejsu pseudograficznego - `menu`. W tym celu należy zalogować

się na urządzeniu jako manager a następnie użyć polecenia `menu` by uruchomić nakładkę umożliwiającą szybkie i sprawne skonfigurowanie switcha.

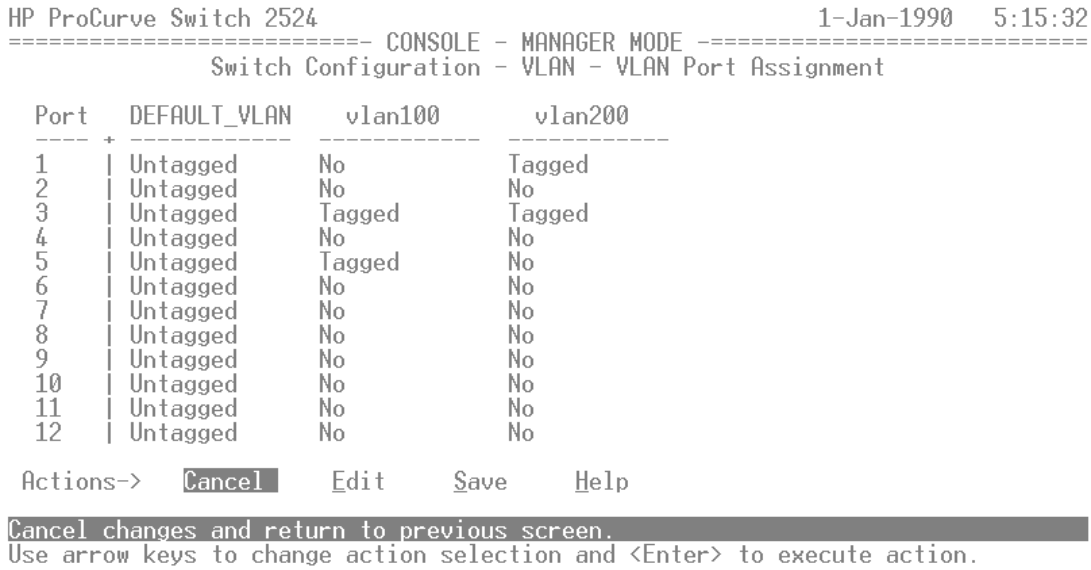
a. Następnie z listy `switch configuration` by przejść do opcji konfiguracji switcha, dalej VLAN menu. Wybrać `VLAN names` by sworzyć vlany zgodnie z założeniami ćwiczenia.

   Ten etap konfiguracji przedstawiono na rysunku 3:



Rys.3. Nadawanie nazw VLANom.

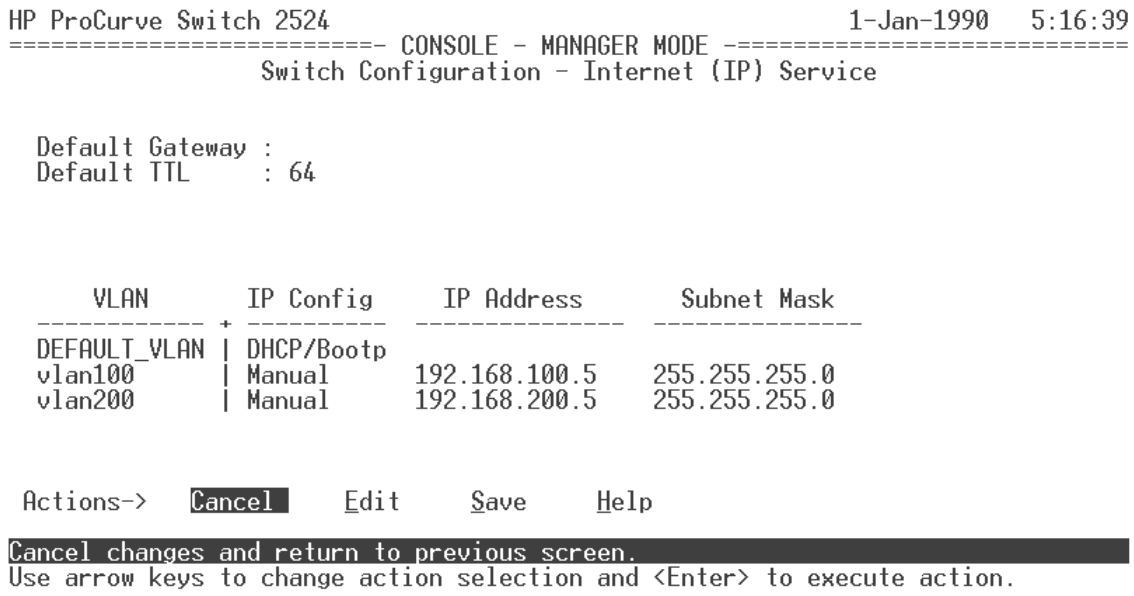
b. Po utworzeniu nazw pozostaje przypisać vlany do portów przełącznika. W oknie `VLAN menu` wybrać opcję `VLAN port assignment`. Dokonać konfiguracji analogicznie jak na rysunku 4.



Rys.4. Przypisywanie vlanów do portów switcha.

c. Przypisując vlany do portów switcha należy zwrócić uwagę na pewne obostrzenia:
   i. Jeśli nie zamierzamy do portu przypisać vlanu to pomimo tego do portu będzie przypisany vlan domyślny (DEFAULT VLAN ID=1).
   ii. Jeśli do jednego portu przypisywanych jest więcej niż jeden vlan, to tylko jeden vlan może być nietagowany.

d. Stosując się do powyższych zaleceń i przydzielając vlany do portów według rysunku switch jest skonfigurowany do pracy. Dodatkowo można do każdego vlanu przypisać adres IP (ułatwia diagnozowanie połączeń switch – host). W celu skonfigurowania adresów IP dla poszczególnych vlanów należy wykorzystując menu wejść w `Switch configuration`, a następnie `IP configration` i ustawić konfigurację IP podobnie jak na rysunku 5.



Rys.5. Konfiguracja IP vlanów.

3. Wszystko co do tej pory zostało wykonane na switchu możemy zobaczyć podglądając plik konfiguracyjny. W naszym przypadku ma on następująca postać:

```
; J4813A Configuration Editor; Created on release #F.05.09
hostname "HP ProCurve Switch 2524"
cdp run
snmp-server community "public" Unrestricted
vlan 1
name "DEFAULT_VLAN"
```

```
untagged 1-26
ip address dhcp-bootp
exit
vlan 100
name "vlan100"
ip address 192.168.100.5 255.255.255.0
tagged 3,5
exit
vlan 200
name "vlan200"
ip address 192.168.200.5 255.255.255.0
tagged 1,3
exit
no aaa port-access authenticator active
```

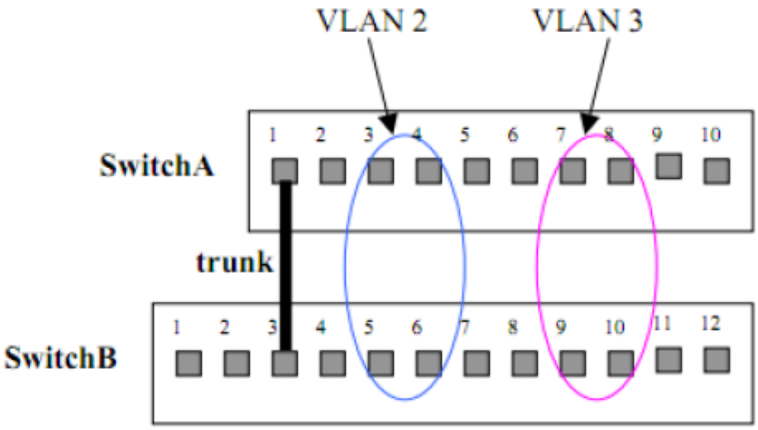
W ten sposób skonfigurowano przełącznik sieciowy do pracy z trzema vlanami, przy czym: vlan 1 jest vlanem domyślnym, występującym standardowo na urządzeniach tego typu.

W sprawozdaniu umieścić rezultaty / zrzuty ekranowe wyniku działania powyższych poleceń Przetestuj i odpowiedz na następujące pytania:

a. Czy urządzenia przypisane do vlanu 100 są widoczne wzajemnie w ramach utworzonej sieci?
b. Czy urządzenia przypisane do vlanu 200 „widzą się" wzajemnie w sieci?
c. Dlaczego nie ma możliwości połączenia pomiędzy hostem 1 i 2 ?
d. Czy host 3 ma dostęp do urządzeń znajdujących się zarówno w jednym jak i drugim vlanie? Jeżeli tak to dlaczego?
e. Czy przepięcie któregokolwiek hosta na inny port switcha powoduje, że traci on kontakt z urządzeniami należącymi do jego vlanu?

Zadanie 2 – Konfiguracja dwóch sieci VLAN w dwóch przełącznikach połączonych łączem trunk.

W opariu o schemat z rysunku 6, w dwóch przełącznikach HP ProCurve 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



Rys.6. Schemat przykładowej konfiguracji z łączem trunk.

W sprawozdaniu umieścić rezultaty / zrzuty ekranowe wyniku działania powyższych poleceń. Opatrz je odpowiednim komentarzem.

1. Konfigurację trybu ad-hoc przeprowadzić w konsoli, np:

```
sudo service wicd stop
sudo ip link set wlan1 down
sudo iwconfig wlan1 mode ad-hoc
sudo iwconfig wlan1 channel 4
sudo iwconfig wlan1 essid "STANDALONE"
sudo ip link set wlan1 up
sudo ip addr add 192.254.34.x/16 dev wlan1
```

2. Do konfiguracji w trybie graficznym, można posłużyć się materiałem, dostępnym pod linkiem: http://www.ubuntugeek.com/creating-an-adhoc-host-with-ubuntu.html

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?

!!

1. Sprawozdanie należy nazwać "Cw5-nazwisko" gdzie nazwisko, oznacza nazwisko wykonującego sprawozdanie i wgrać do katalogu na Dropbox (katalog Sprawozdania, podkatalog odpowiadający terminowi zajęć).
2. Na wstępie sprawozdania proszę podać imiona i nazwiska wszystkich członków grupy ćwiczeniowej, która uczestniczyła w wykonaniu ćwiczenia.
3. Format sprawozdania: PDF. !

!!