Ćwiczenie laboratoryjne VLAN 2

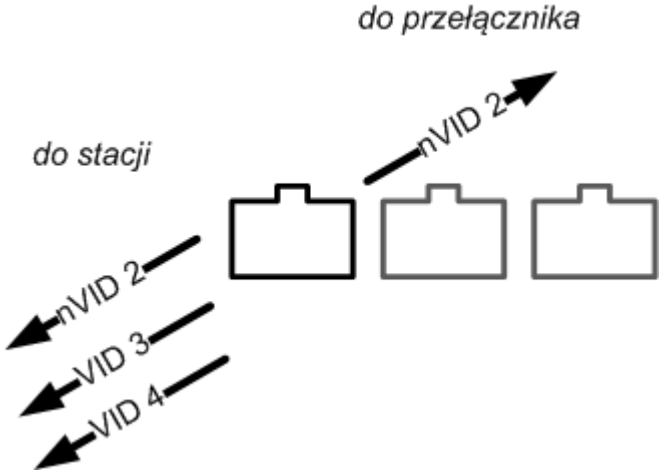
Wstęp

Ćwiczenie dotyczy konfiguracji wirtualnych sieci lokalnych w wariantach nowych w stosunku do ćwiczeń poprzednich. Podczas zajęć realizowane będą dwa warianty VLANów prywatnych (ang. private VLAN), nakładające się (ang. overlapping VLAN), filtrowanie ramek przychodzących (ang. ingress filtering) oraz VLANy konfigurowane automatycznie za pomocą serwera RADIUS.

Konfiguracja przełączników będzie mogła być realizowana za pomocą przeglądarki, konsoli zdalnej lub lokalnej – do wyboru. Praca będzie przebiegała w parach na zestawach składających się z dwóch komputerów i przełącznika Edge-Core 3526XA.

Nachodzące sieci wirtualne (overlapping VLANs)

Nachodzące sieci wirtualne nazywane są tak ponieważ jeden port należy do kilku sieci wirtualnych, w których wyłączone są znaczniki. Na tym porcie sieci te nachodzą na siebie – „pokrywają się” (ang. overlap). Nachodzenie sieci występuje tylko w sytuacji odbierania ramek na tym porcie, wysyłanie ramek nie powoduje rozsyłania ich do wszystkich skonfigurowanych sieci wirtualnych. Na tak skonfigurowanym porcie będzie można odebrać ramki rozgłoszeniowe i nieznanego przeznaczenia pochodzące z wszystkich wirtualnych sieci lokalnych oraz ramki adresowane do stacji znajdującej/znajdujących się na tym porcie. W przypadku gdy stacja wysyła ramkę, zostanie ona rozesłana tylko w obrębie sieci wirtualnej oznaczonej jako „natywna” – ang. native VLAN. Każdy port może posiadać skonfigurowaną tylko jedną sieć natywną.

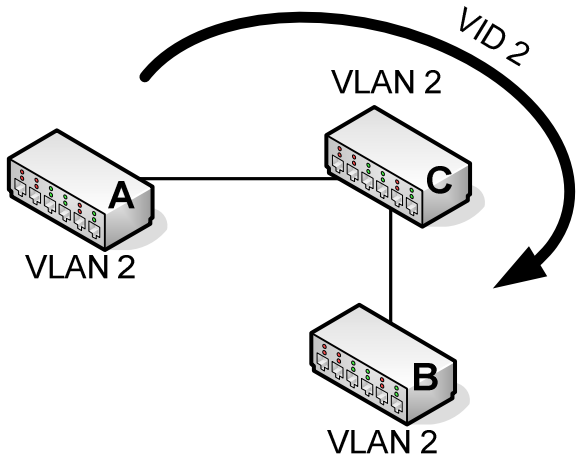


Rys. 1. Port należący do trzech sieci VLAN - 2, 3, 4, we wszystkich sieciach znaczniki są wyłączone; ruch z sieci 3 i 4 może być tylko obserwowany, komunikacja jest możliwa ze stacjami należącymi do VLAN 2 - native VLAN dla tego portu.

Protokół GVRP

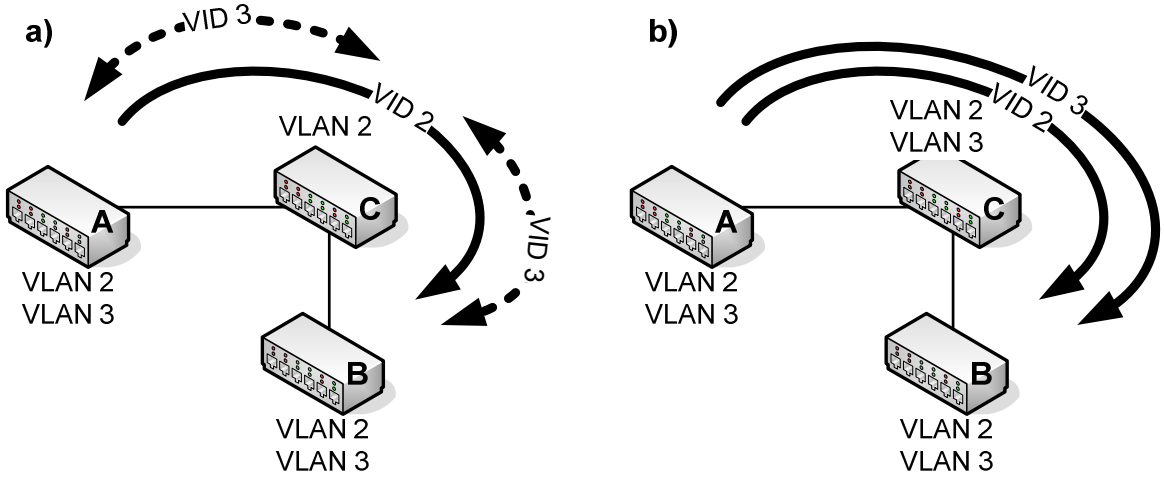
Protokół GVRP (GARP VLAN Registration Protocol) służy do automatycznej konfiguracji wirtualnych sieci lokalnych w przełącznikach. Pozwala uprościć administrację sieciami o złożonej strukturze, w których wykorzystywana jest duża liczba wirtualnych sieci lokalnych.

Wirtualne sieci lokalne często stosowane są w złożonych sieciach, w których pomiędzy przełącznikami do których bezpośrednio podłączone są stacje końcowe występują inne przełączniki. Przykład takiej sytuacji przedstawiony jest na Rys. 2, gdzie przełącznikiem pośredniczącym jest przełącznik C.



Rys. 2. Przykład hierarchicznej struktury przełączników posługujących się znacznikami 802.1Q.

Łącza pomiędzy przełącznikami A i C oraz B i C przenoszą ramki oznakowane VID 2. Aby obsługiwać taką sieć, porty przełącznika C, które prowadzą do przełączników A i B powinny także należeć do sieci VLAN 2 i obsługiwać ramki oznakowane takim VID. Protokół GVRP umożliwia wykonanie takiej konfiguracji automatycznie. Oznacza to, że w sytuacji z Rys. 2 po dodaniu na przełącznikach A i B sieci VLAN 3 (Rys. 3a), przełącznik C po opóźnieniu nieprzekraczającym kilku sekund zostanie skonfigurowany do obsługi sieci VLAN 3 (Rys. 3b).



Rys. 3. Brak konfiguracji sieci VLAN 3 na przełączniku C typowo uniemożliwia przesyłanie ramek należących do VLAN 3 pomiędzy przełącznikami A i B (a), włączenie protokołu GVRP na wszystkich portach łączących przełączniki pozwala automatycznie skonfigurować sieć VLAN 3 na przełączniku C (b).

Filtrowanie na wejściu (ingress filtering)

Filtrowanie na wejściu odpowiada za przekazywanie bądź nie ramek zawierających znacznik sieci wirtualnych, które nie są skonfigurowane na danym porcie przełącznika. Typowo ramki takie są przez przełącznik odrzucane. Odpowiada to sytuacji gdy ingress filtering jest włączone.

Rozważając konkretny przykład, port 1 przełącznika należy do sieci wirtualnych 1 (znaczniki wyłączone) oraz 2 (znaczniki włączone). Ponadto filtrowanie na wejściu jest włączone (ustawienie domyślne przełącznika).

a) Odebranie ramki ze znacznikiem 2 powoduje przesłanie jej na kolejne porty tej sieci.
b) Odebranie ramki bez znacznika odpowiada przesłanie jej na kolejne porty sieci 1.
c) Odebranie ramki ze znacznikiem sieci 3 (dowolnej oprócz 2, w szczególności także 1) powoduje odrzucenie tej ramki, ponieważ ingress filtering jest włączone. Jednak w sytuacji wyłączenia filtrowania na wejściu, ramka taka zostanie rozesłana na porty przełącznika, które należą do sieci 3.

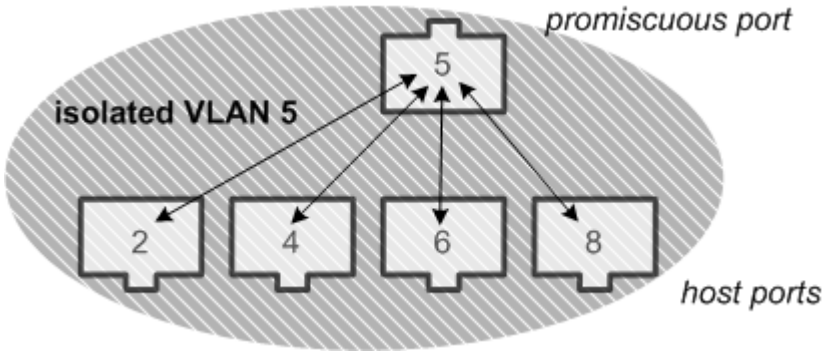
Jeżeli odebrana zostanie oznakowana ramka, ale sieć wirtualna o takim numerze nie została skonfigurowana w przełączniku, ramka zostanie odrzucona.

W ćwiczeniu laboratoryjnym rolę przełączników A i B będą spełniały komputery z systemem Linux skonfigurowane tak, żeby wysyłać i odbierać ramki zawierające znaczniki 802.1Q.

Sieci prywatne izolowane

Prywatne wirtualne sieci lokalne są rozwiązaniem upraszczającym zarządzanie sieciami, w których ruch pomiędzy stacjami końcowymi użytkowników końcowych jest ograniczony z jednoczesnym zapewnieniem wszystkim komunikacji z wybranym portem (np. bramą do Internetu). Typowym środowiskiem, w którym może być wykorzystane takie rozwiązanie jest sieć dostawcy Internetu, który zabrania komunikacji pomiędzy użytkownikami. Zastosowanie takiego rozwiązania pozwala wyeliminować dodatkowe urządzenie filtrujące ramki (np. firewall) pomiędzy portami użytkowników końcowych.

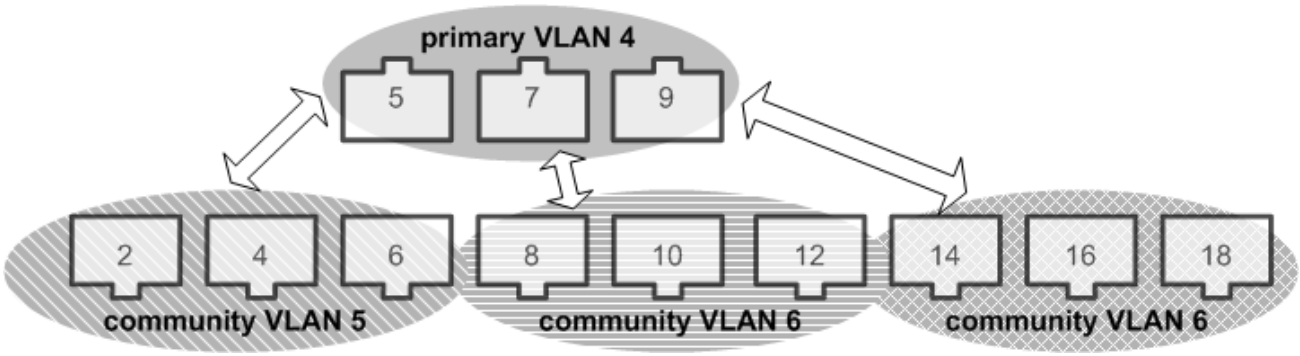
Przełączniki EC3526XA pozwalają na realizację dwóch wariantów prywatnych sieci wirtualnych. W tym punkcie omówiony zostanie pierwszy wariant. Polega on na utworzeniu sieci izolowanej (ang. isolated VLAN) z jednym portem wspólnym/uprzywilejowanym (ang. promiscuous port). Pozostałe porty nazywane są portami stacji (ang. host port). Stacje do nich podłączone nie mogą się komunikować pomiędzy sobą. Żadna ramka, nawet rozgłoszeniowa, nie zostanie przesłana pomiędzy jednym a drugim portem stacji. Natomiast ruch pomiędzy portem promiscuous a portami host może odbywać się bez ograniczeń. Przykładowa ilustracja przedstawiona jest na Rys. 4.



Rys. 4. Izolowana sieć wirtualna: pomiędzy portami o numerach parzystych komunikacja jest niemożliwa, wszystkie stacje mogą jednak przesyłać ramki do stacji na porcie 5 i stacja z portu 5 może wysyłać ramki do każdej stacji na portach parzystych.

Sieci prywatne – wspólnoty (communities)

Drugi wariant sieci prywatnych jest rozbudowaną wersją pierwszego – ruch izolowany jest nie pomiędzy pojedynczymi portami, ale pomiędzy grupami portów tworzących wspólnoty (ang. community VLAN). W obrębie jednej wspólnoty stacje mogą się komunikować, pomiędzy wspólnotami przesyłanie ramek jest niemożliwe, ale stacje ze wszystkich wspólnot mogą przesyłać dane do portów sieci podstawowej w obie strony. Jest to zilustrowane na Rys. 5.



Rys. 5. Community VLANs: stacje w każdej sieci wirtualnej mogą komunikować się ze sobą, pomiędzy sieciami wirtualnymi jest to możliwe jedynie jeżeli jedna sieć jest rodzaju primary, druga – community.

Ponieważ w tym wariancie, nietypowo w stosunku do klasycznych sieci VLAN, ramki mogą być przesyłane pomiędzy sieciami, konieczny jest proces asocjacji sieci typu community z siecią typu primary.

Konfiguracja VLANów z wykorzystaniem serwera RADIUS

Przełączniki EC3526XA umożliwiają automatyczną konfigurację wirtualnych sieci lokalnych na szereg sposobów. Jednym z nich jest przydział numerów wirtualnych sieci lokalnych, do których ma należeć stacja z serwera RADIUS. Serwer ten także uwierzytelnia stację, w tym przypadku na podstawie adresu MAC. Konfiguracja sieci wirtualnych na porcie, do którego podłączona jest stacja dokonywana jest dopiero po jej uwierzytelnieniu.

Proces uwierzytelniania oparty jest o stosunkowo prosty protokół PAP, serwer uwierzytelniający ma możliwość przesłania w odpowiedzi informacji, jak powinny zostać skonfigurowane VLANy na danym porcie. Istnieje możliwość skonfigurowania kilku sieci wirtualnych jednocześnie, a także opcja wskazania, które konfigurowane sieci mają mieć włączone znaczniki, a które nie. Wymogiem jest wcześniejsze stworzenie tych sieci na przełączniku (nawet bez przypisywania żadnych portów).

Rozwiązanie to posiada pewne ograniczenie. Jeżeli do jednego portu podłączonych jest więcej stacji, obowiązywała będzie konfiguracja sieci wirtualnych, przypisanych do pierwszej stacji, która się uwierzytelni.