VLAN 2 – zadania

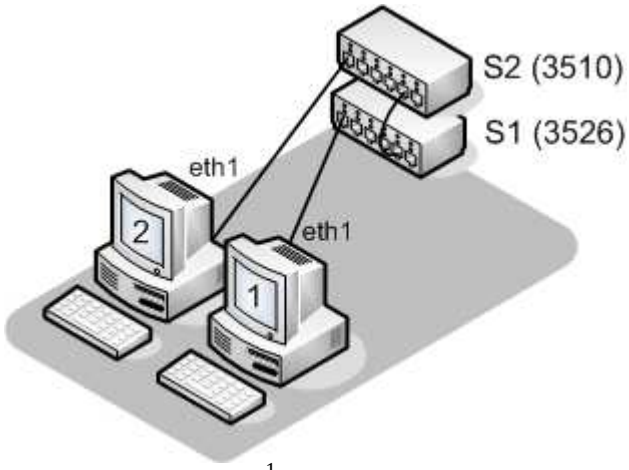
Uwagi

1. Zadanie jest realizowane w systemach Linux, bo wykorzystywane jest znacznikowanie realizowane przez komputery.
2. Przełączniki konfigurować można albo konsolą (małe liczby w potędze poleceń to numer strony WYSZUKANEJ w pliku PDF z instrukcją obsługi przełącznika 26-portowego ES3526), albo przez interfejs WWW (miejsce konfiguracji w nawiasach kwadratowych)
3. Treść komend i umiejscowienie w interfejsie webowym jest taki sam dla obu rodzajów przełączników.

Przygotowanie

1. Wyłączyć Rapid Spanning Tree na przełączniku[163].
   [Spanning Tree –> Configuration]
2. Wyłączyć interfejsy eth0 poleceniem *ifdown eth0*.
3. Zapamiętać wartości adresów IP i domyślnych bram na interfejsach eth1, wykonać polecenie *ifdown eth1*, przypisać adresy ręcznie, włączyć interfejsy i dodać domyślne bramy.

Zadanie 1 – Klasyczny VLAN, komputery obsługują znaczniki 802.1Q



1. Dodać interfejsy z dowolnie wybranym[1] znacznikiem sieci VLAN A do interfejsów eth1 obu komputerów.
   [ostatnia strona tego dokumentu]
2. Przypisać adresy IP z dowolnej sieci[2] nowym interfejsom na obu komputerach (nazwy w postaci eth1.A) i włączyć je.
3. Utworzyć w przełączniku sieć VLAN A[416-dół].
   [VLAN –> 802.1Q VLAN –> Static List]
4. Dodać porty 3 w S1 i S2 do sieci VLAN A z włączonymi znacznikami[421].
   [VLAN –> 802.1Q VLAN –> Static Table]
5. Podłączyć komputery do portów 3 i przesłać ping pomiędzy interfejsami eth1.A.

Zadanie 2 – Ingress filtering (cz. 2)

1. Usunąć z sieci VLAN A port komputera 1 [421].
   [VLAN –> 802.1Q VLAN –> Static Table]
2. Wyłączyć ingress filtering na porcie komputera 1 [419].

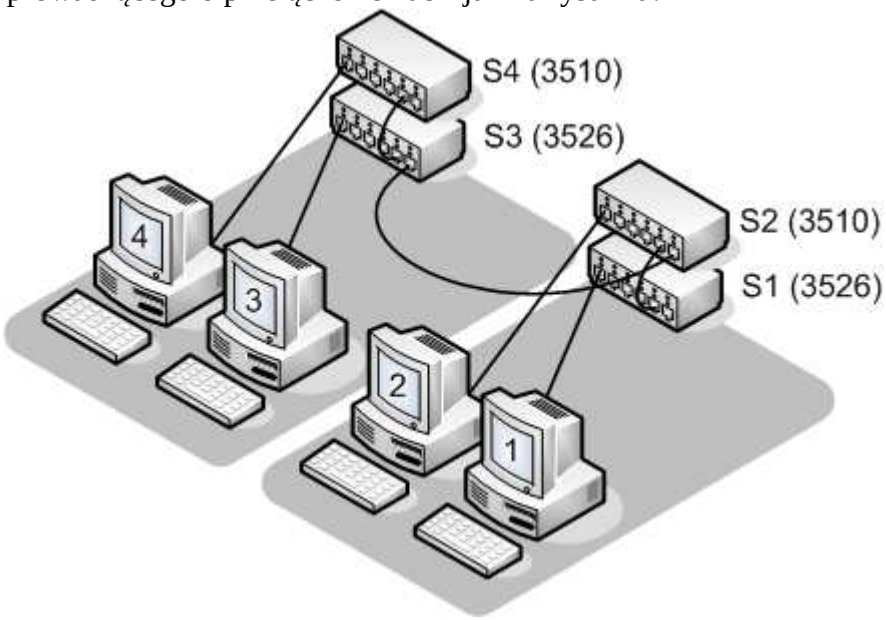
[1] różnym od VLAN1
[2] sieć powinna być inna niż na pozostałych interfejsach

[VLAN –> 802.1Q VLAN –> Port configuration]

3. Na komputerze 2 programem *tcpdump* zademonstrować dowolne ramki rozgłoszeniowe z komputera 1.

Zadanie 3 – GVRP

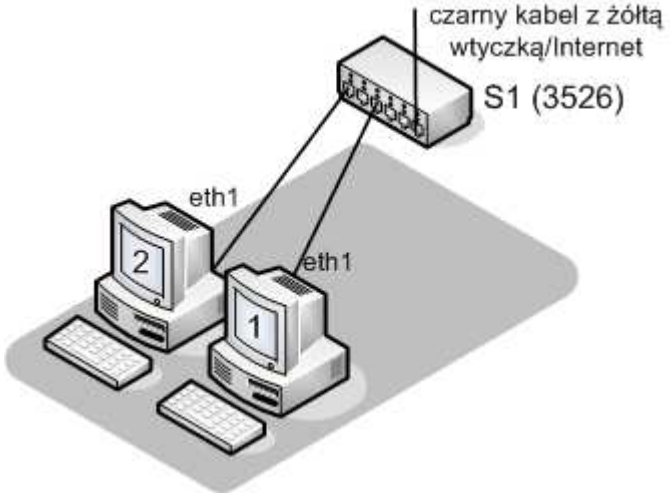
1. Usunąć sieci z poprzedniego zadania z przełączników (w `vlan database` polecenie `no vlan NR`) i interfejsy eth1.A z komputerów.
   [VLAN –> 802.1Q VLAN –> Static List]
   [ostatnia strona tego dokumentu]
2. Poprosić prowadzącego o przełączenie kabli jak na rysunku:



3. Włączyć GVRP na **wszystkich portach, na których kable łączą przełączniki** [431-dół].
   [VLAN –> 802.1Q VLAN –> Port configuration]
4. Utworzyć sieć VLAN o numerze 11 na przełącznikach A i D[416-dół], przypisać do niej porty prowadzące TYLKO do komputerów[421].
   [VLAN –> 802.1Q VLAN –> Static List]
   [VLAN –> 802.1Q VLAN –> Static Table]
5. Utworzyć na komputerach podłączonych do przełączników A i D interfejsy eth1.11, przypisać im adresy IP ze wspólnej sieci.
   [ostatnia strona tego dokumentu]
6. Włączyć instancję GVRP na wszystkich czterech przełącznikach[431-góra].
   [VLAN –> 802.1Q VLAN –> GVRP status]
7. Zademonstrować ping pomiędzy komputerami 1 i 4 w nowym VLANie.

Zadanie 4 – Isolated VLANs

1. Usunąć sieć wirtualną z poprzedniego zadania z komputerów i przełączników, wyłączyć GVRP na portach i przełącznikach.
   [VLAN –> 802.1Q VLAN –> GVRP status]
   [VLAN –> 802.1Q VLAN –> Port configuration]
   [VLAN –> 802.1Q VLAN –> Static List]
2. Przełączyć kable, aby odpowiadały rysunkowi:



3. Utworzyć w przełączniku sieć Private VLAN C typu **Isolated** (nie primary ani community)[426].
   [VLAN –> Private VLAN –> Configuration]
4. Zmienić tryb pracy portu z czarnym kablem na Promiscuous i dodać go do VLAN C[427].
   [VLAN –> Private VLAN –> Port Configuration]
5. Zmienić tryb pracy portów OBOK podłączonych komputerów na Host i dodać je do VLAN C[427].
   [VLAN –> Private VLAN –> Port Configuration]
6. Przełączyć kable prowadzące do komputerów do utworzonej sieci i przesłać ping z komputerów na bramę domyślną, a następnie między sobą. (w tym momencie nie można zarządzać przełącznikiem).

Zadanie 5 – Community VLANs

1. Usunąć sieci z zadania poprzedniego.
2. Utworzyć w przełączniku sieć Private VLAN D typu Primary[426].
   [VLAN –> Private VLAN –> Configuration]
3. Utworzyć w przełączniku sieci Private VLAN E i F typu Community[426].
   [VLAN –> Private VLAN –> Configuration]
4. Przypisać VLAN D VLANom E i F[426-dół].
   [VLAN –> Private VLAN –> Association]
5. Zmienić tryb pracy portów 7 i 9 na Promiscuous i dodać je do VLAN D[427].
   [VLAN –> Private VLAN –> Port Configuration]
6. Zmienić tryb pracy portów 3 i 5 na Host i dodać je do VLAN E[427,428].
   [VLAN –> Private VLAN –> Port Configuration]
7. Zmienić tryb pracy portów 19 i 21 na Host i dodać je do VLAN F[427,428].
   [VLAN –> Private VLAN –> Port Configuration]
8. Zademonstrować możliwość komunikowania w obrębie sieci VLAN E oraz VLAN F, a następnie brak komunikacji między VLAN E i VLAN F poprzez ping na adres rozgłoszeniowy.

Zadanie 6 – Network Access – protokół RADIUS

1. Usunąć sieci z zadania poprzedniego.
2. Skonfigurować serwer RADIUS numer 1 na przełączniku[313-314].
   [Security –> Authentication; uwaga: Authentication: LOCAL pozostaje BEZ ZMIAN]
3. Włączyć uwierzytelnianie adresami MAC (Network Access) na portach OBOK komputerów[329].
   [Security –> 802.1x –> Port configuration]
4. Włączyć dynamiczny przydział do VLANów na tych portach[331].

[Security –> 802.1x –> Port configuration]

5. Wymusić ponowne uwierzytelnianie na JEDNYM z portów (najprościej poprzez wyjęcie i włożenie kabla).
6. Zademonstrować z jednego komputera w jaki sposób został skonfigurowany port drugiego. Wysłać ping na domyślną bramę z komputera uwierzytelnianego po adresie MAC.

Zadanie 7 – overlapping VLANs

1. Utworzyć w przełączniku sieć VLAN B[416-dół].
2. Dodać porty 3 i 7 do VLAN B z wyłączonym znacznikowaniem (powinny one także należeć do sieci domyślnej VLAN 1 i mieć w niej wyłączone znaczniki)[421].
3. Dodać port 23 do VLAN B bez znaczników, usunąć go z sieci VLAN 1 i zmienić native VLAN (PVID) na VLAN B[421, 420-dół].
4. Programem tcpdump zademonstrować wysyłanie pakietów ping na adres rozgłoszeniowy interfejsu eth1 najpierw z jednego komputera, następnie z drugiego.

Polecenie vconfig

1. Dodanie sieci VLAN o numerze x do interfejsu eth1:

```
vconfig add eth1 x
```

   Nowy interfejs ma nazwę **eth1.x**, można sprawdzić jego stan pisząc `ip link show`.

2. Usunięcie sieci VLAN o numerze x z interfejsu eth1:

```
vconfig rem eth1.x
```

Polecenie tcpdump

1. Nasłuchiwanie na interfejsie eth1 bez rozwiązywania nazw:

```
tcpdump -ni eth1
```

2. J/w + pokazywanie adresów warstwy łącza danych (opcja *e*):

```
tcpdump -eni eth1
```

3. Odfiltrowanie tylko ruchu ICMP lub ARP:

```
tcpdump -ni eth1 icmp
tcpdump -ni eth1 arp
```

4. Odfiltrowanie ruchu na podstawie adresu MAC (na przykład broadcast):

```
tcpdump -ni eth1 ether host xx:xx:xx:xx:xx:xx
tcpdump -ni eth1 ether host ff:ff:ff:ff:ff:ff
```