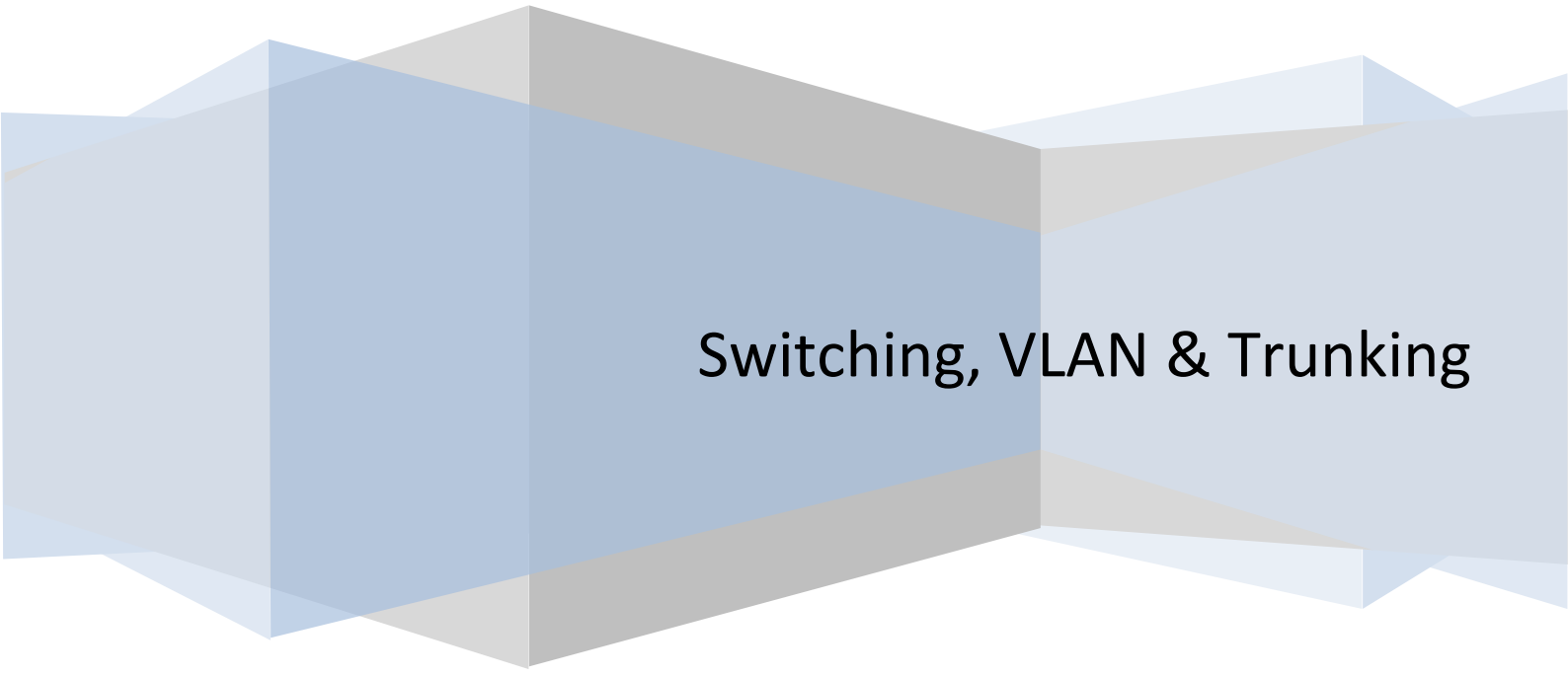
**Politechnika Krakowska**

Katedra Automatyki i Technik Informacyjnych

# Laboratorium Sieci Komputerowych

## 2015/2016



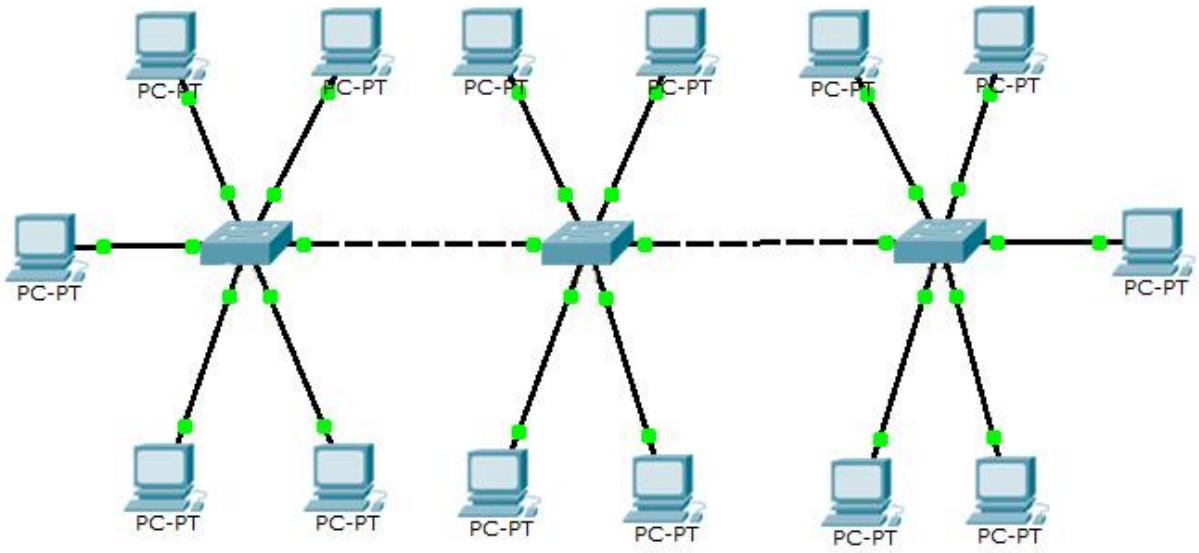
## Switching, VLAN & Trunking

## 1.1 Przełączanie w sieciach bez VLAN

W sieciach lokalnych przełączanie realizowane jest za pośrednictwem przełączników. W większości przypadków są to przełączniki warstwy 2. modelu ISO/OSI. Proces przełączania przebiega więc na podstawie adresów fizycznych (ang. physical address).

W przełączniku znajduje się **tablica przełączania** (ang. switching table), na podstawie której ramki kierowane są na odpowiedni port (interfejs) przełącznika. Przełączniki nie wysyłają ramek do wszystkich, jak miało to miejsce w koncentratorze, lecz tylko do określonego adresata. Wyjątkiem jest sytuacja, w której w tablicy przełączania nie ma wpisu na temat poszukiwanego adresu MAC. Wtedy przełącznik wysyła otrzymaną ramkę do wszystkich stacji roboczych podłączonych do przełącznika.

Tak więc pierwszą cechą przełączników jest to, że nie pomniejszają domeny rozgłoszeniowej, wręcz przeciwnie, powiększają ją poprzez przekazywanie rozgłoszeń. Spójrzmy na poniższy rysunek:




W tej sieci znajdują się trzy przełączniki. Ponieważ każdy interfejs przełącznika to osobna domena kolizji, w tej podsieci mamy szesnaście domen kolizji. Niewątpliwie jest to wielka zaleta tych urządzeń. Gdyby w tym przypadku zamiast przełączników znalazły się trzy koncentratory, w sieci funkcjonowałaby jedna domena kolizji, co skutkowałoby powstawaniem wielu kolizji. Bez wątpienia sieć stałaby się wolniejsza i mniej wydajna.

Zauważmy, że w przedstawionej na rysunku sieci znajduje się tylko jedna podsieć. Wszystkie urządzenia mogą więc komunikować się między sobą. Oczywiście, to nie wada, pod warunkiem że jest to zamierzona funkcjonalność. Jednak w sytuacji, w której stacje podłączone do jednego przełącznika przetwarzają dane finansowe lub inne „wrażliwe” z punktu widzenia działalności firmy dane, sytuacja staje się bardziej skomplikowana. Każdy użytkownik może bowiem takie dane przeglądać. Można

każdą z tych stacji roboczych odpowiednio zabezpieczyć, ale wymaga to dodatkowej pracy i często nie przynosi dobrych rezultatów.

Jeśli w takiej sieci jedna ze stacji nie będzie znajdowała się w tablicy przełączania przełącznika, wówczas rozgłoszenie będzie wysłane do wszystkich stacji w sieci. W tej sytuacji niepotrzebnie sieć staje się bardziej obciążona. Powyższy przykład dotyczy tylko szesnastu hostów, ale często w sieci występuje ich o wiele więcej. Co się stanie, jeśli w tym przypadku ilość hostów będzie przekraczała tysiąc? Za każdym razem, kiedy będzie wysyłane rozgłoszenie, sieć będzie narażona na dość duże obciążenie.

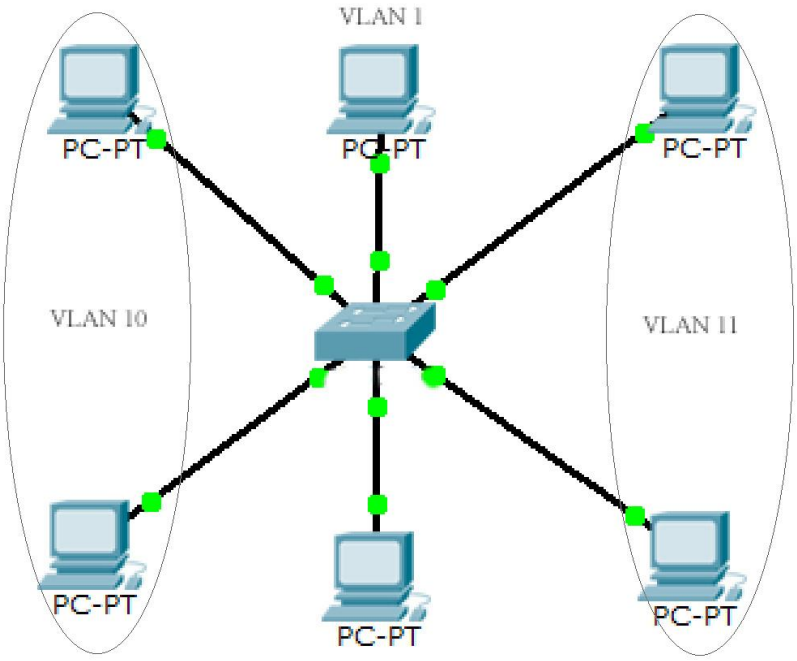
Innym aspektem jest zarządzanie określonymi hostami lub ich grupą. Sprawa związana z implementacją zabezpieczeń interfejsów staje się bardziej skomplikowana i trudna do realizacji. Niewątpliwie wymaga dość dużych nakładów czasowych i sporej wiedzy administratora sieci.

Patrząc więc na powyższy wywód, można dojść do wniosku, że brak sieci VLAN jest dość sporym problemem w dużych sieciach z wielką ilością hostów. Jeśli dodatkowo w przedsiębiorstwie występują działy, których dane powinny być dostępne tylko dla uprawnionych osób, zastosowanie sieci VLAN staje się koniecznością.

Spójrzmy zatem na charakterystykę sieci VLAN i spróbujmy przeanalizować sieć znajdującą się na powyższym rysunku pod kątem sieci VLAN.

## 1.2 Sieci VLAN

**Sieć VLAN** jest siecią specyficzną ponieważ wyodrębniona jest z sieci rzeczywistej. Wyodrębnienie polega na tym, że sieć dzielona jest na logiczne podsieci. Oznacza to, że hosty pracujące w jednej sieci VLAN, mimo iż znajdują się fizycznie w tej samej sieci, są od siebie odseparowane na poziomie logiki.

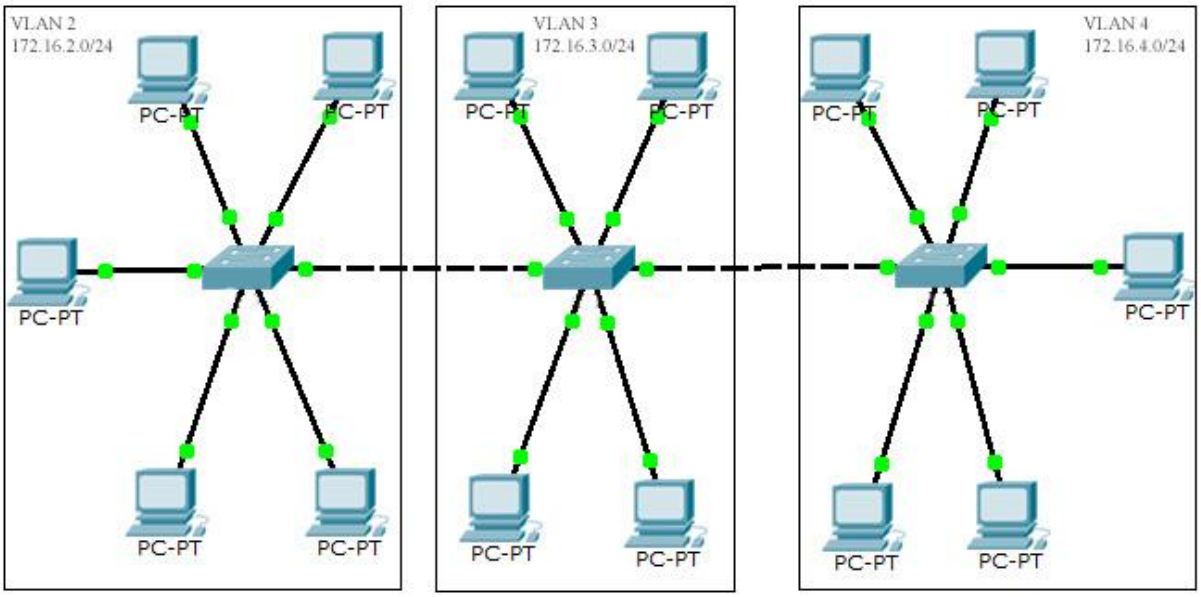


W tym przypadku wszystkie sześć hostów znajduje się w tej samej sieci, podłączonej w dodatku do tego samego przełącznika. Jednak nie wszystkie stacje mogą się ze sobą komunikować. Komunikacja przebiega tylko pomiędzy stacjami znajdującymi się w tej samej sieci VLAN. Dlatego w sieciach VLAN10, VLAN1 oraz VLAN11 komunikacja przebiega tylko pomiędzy dwoma hostami. Stosowanie sieci VLAN powoduje utworzenie osobnych grup hostów na poziomie logicznym (bo fizycznie znajdują się w tej samej sieci).

Wyodrębnione sieci są od siebie zupełnie niezależne. Oznacza to m.in., że może w nich pojawić się różna adresacja. Ponadto jedna sieć VLAN może realizować połączenia] pomiędzy hostami, inna sieć VLAN może realizować komunikację pomiędzy drukarkami, a w jeszcze inna komunikację głosową która wykorzystywana jest m.in. prze- telefonię IP.

Sieci wirtualne dokonują więc segmentacji sieci bez potrzeby korzystania z routerów

Spójrzmy jeszcze raz na sieć, która w tym przypadku została podzielona na odrębne sieci VLAN:

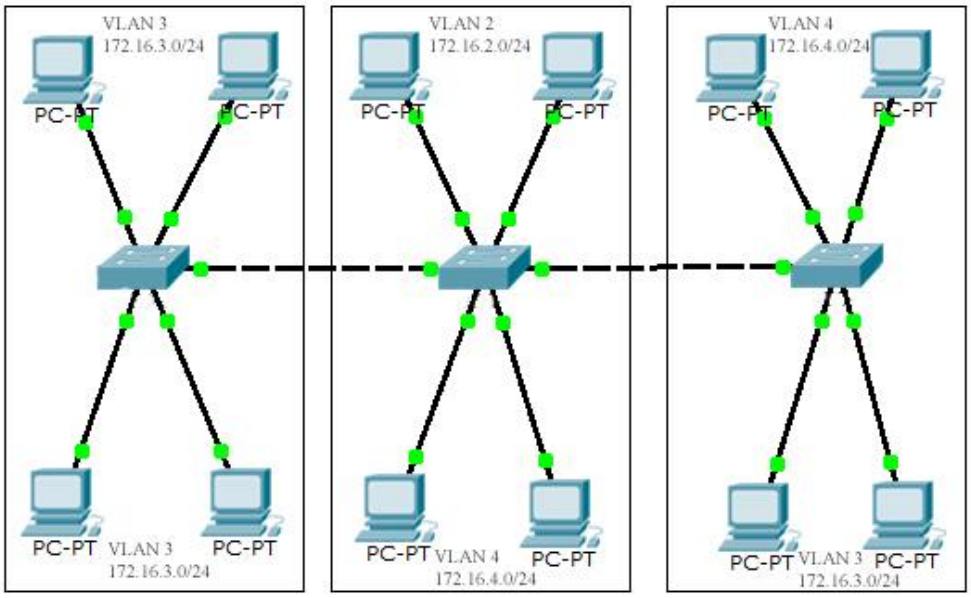



W tej sieci również występuje szesnaście hostów i wszystkie znajdują się w tej samej sieci lokalnej. Jednak tym razem są od siebie oddzielone przy wykorzystaniu sieci VLAN.

Jak widać, każda sieć VLAN reprezentowana jest przez inną podsieć. I tak podsieć 172.16.2.0/24 to sieć VLAN nr 2, podsieć 172.16.3.0/24 to sieć VLAN nr 3 i podsieć 172.16.4.0/24 to sieć VLAN nr 4.

Z powyższego rysunku może wynikać, że sieć VLAN jest przydzielona dla konkretnego przełącznika i tylko dany przełącznik może reprezentować jedną sieć VLAN. Nie jest to prawdą gdyż takie rozwiązanie powodowałoby dość duże ograniczenia.

Oczywiście, sieć VLAN jest przypisana do konkretnego interfejsu przełącznika i od ilości interfejsów w przełączniku zależy ilość utworzonych sieci VLAN. Spójrzmy na poniższy rysunek:




Na rysunku przedstawiono trzy sieci VLAN, jednak znajdujące się w różnych lokalizacjach. Widać również, że do interfejsów przełącznika nr 3 podłączono dwie sieci VLAN. Jedna sieć to VLAN 4, a druga VLAN 3. W przełączniku nr 1 również znajduje się sieć VLAN 3.

Zatem hosty podłączone do przełącznika nr 1 oraz do przełącznika nr 3 będą mogły i się komunikować. Pozostałe hosty znajdujące się w innych sieciach VLAN nie będą w stanie w tej komunikacji uczestniczyć.

W tym przypadku podział sieci na osobne sieci VLAN skutkować będzie większą ilością domen rozgłoszeniowych. Każda sieć VLAN tworzy bowiem odrębną domenę rozgłoszeniową. W naszym przykładzie cała sieć została podzielona na trzy odrębne domeny rozgłoszeniowe.

A więc jeśli stacja robocza podłączona do przełącznika nr 3 i znajdująca się w sieci VLAN 3 wyśle ramkę rozgłoszeniową nie będzie ona przesłana na wszystkie interfejsy przełącznika, ale tylko na te, które aktualnie znajdują się w sieci VLAN 3. Zostaną również przesłane do przełącznika nr 1 poprzez specjalny port zwany portem **trunk**, o którym będzie mowa w dalszej części.

Sieci VLAN dzielą sieć na odrębne sieci rozgłoszeniowe, podobnie jak routery. Co sprawia, że sieć jest wolna od niepotrzebnego ruchu, a tym samym wydajniejsza?

Sieci VLAN segmentują sieć na odrębne sieci logiczne; w ten sposób możemy odseparować ruch powodowany przesyłaniem danych od np. ruchu generowanego przez telefonię IP. Co więcej, posługując się metodami priorytetyzacji (ang. Quality of Service), możemy zarządzać wielkością pasma, jakie zostanie przeznaczone na konkretne usługi.

Kolejną dużą zaletą tworzenia sieci VLAN jest ułatwione zarządzanie uprawnieniami oraz dbanie o bezpieczeństwo sieci. Po utworzeniu sieci VLAN możemy ich członkom przypisywać określone uprawnienia. Ponadto możemy niezaufany ruch w sieci przyporządkować do odrębnej sieci VLAN, która w żaden sposób nie jest połączona z siecią firmy.

Pamiętajmy, że łatwiej zarządzać mniejszymi grupami komputerów niż całą ogromną siecią, w której znajduje się nawet kilka tysięcy hostów.

## 1.3 Domyślna sieć VLAN

Gdy kupimy nowy przełącznik po podłączeniu do sieci wszystkie jego interfejsy są aktywne i gotowe do pracy. Możemy więc podłączyć do nich hosty i sieć będzie pracować prawidłowo. Nie jest wymagana żadna konfiguracja. Dzieje się tak dlatego, że każdy z interfejsów przełącznika znajduje się w domyślnej sieci VLAN 1. VLAN 1 jest domyślnym (ang. default VLAN) rodzajem sieci i zawsze po usunięciu całej konfiguracji przełącznika wszystkie interfejsy zostaną do niej przypisane.

Domyślnej sieci VLAN nie można usunąć i nie można zmienić jej nazwy, co jest szczególną funkcjonalnością.

Obecnie zaleca się, aby VLAN 1 nie była używana do przekazywania ruchu. Ruch powinien zostać przekazany przez inne utworzone sieci VLAN. Ponadto należy zadbać, aby sieć VLAN 1 stała się tzw. **„czarną dziurą”** (ang. black hole VLAN).

Czarna dziura to miejsce w sieci, do którego będzie kierowane nierozpoznane urządzenie, które nagle zostało podpięte do sieci. Podczas zapewniania bezpieczeństwa w sieci i można wszystkie nieużywane interfejsy przełącznika wyłączyć i włączać je dopiero wtedy, kiedy trzeba. Innym rozwiązaniem jest właśnie utworzenie „czarnej dziury”, czyli sieci VLAN, która nie jest połączona z żadną inną siecią. Jeśli interfejs zostanie i w ten sposób skonfigurowany, po podłączeniu do niego urządzenia zostanie automatycznie odseparowany od reszty sieci. Pozornie będzie działał, lecz nie będzie stanowić zagrożenia. Można w ten sposób również łatwo namierzyć miejsce, do którego dane urządzenie zostało podłączone.

Podczas konfiguracji VLAN należy również zadbać o to, aby sieć VLAN 1 nie była siecią zarządzania przełącznika.

## 1.4 Identyfikatory sieci VLAN

Podczas konfiguracji sieci VLAN każdej sieci przypisywany jest identyfikator. Oznacza to, że podczas tworzenia nowych sieci VLAN zostaną im przypisane odpowiednie numery z przedziału od 1 do 4094.

Wyróżniamy dwa rodzaje identyfikatorów. Pierwsza grupa to identyfikatory normalne. Mieszczą się w przedziale od 1 do 1005. Identyfikatory od 1002 do 1005 są zarezerwowane dla sieci Token Ring oraz FDDI.

Natomiast identyfikatory 1. oraz od 1006 do 4094 to identyfikatory rozszerzone.

## 1.5 Natywny VLAN

Pierwotna sieć VLAN (natywna) służy do komunikacji i przypisania hostów niepodłączonych do żadnej sieci VLAN. Jeśli do przełącznika zostanie przekazana ramka nieoznakowana, domyślnie znajdzie się w pierwotnej sieci VLAN. Domyślnie siecią tą jest VLAN 1, jednak Cisco zaleca, aby numer ten został zmieniony na np. 99.

## 1.6 Konfiguracja sieci VLAN

### Tworzenie nowej sieci VLAN

Aby można było korzystać z sieci VLAN, konieczne jest ich utworzenie. Każdy przełącznik posiada już pięć sieci VLAN. Aby je zobaczyć, w trybie uprzywilejowanym wydajemy polecenie `show vlan`, np. tak:

```
Switch>en
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
Switch#
```

Zauważmy, że sieci VLAN1, 1002, 1003, 1004, 1005 są na stałe umieszczone w konfiguracji przełącznika i nie można ich usuwać. Sieć VLAN 1 jest domyślną siecią VLAN, do której należą wszystkie interfejsy przełącznika. Dlatego po zakupie nowego przełącznika nie jest konieczna jego konfiguracja, aby wszystkie komputery mogły się komunikować. Podczas próby usunięcia jednej z nich pojawi się komunikat informujący o tym, iż sieć nie może zostać usunięta:

```
Switch(config)#no vlan 1002
Default VLAN 1002 may not be deleted.
Switch(config)#
```

Aby utworzyć nową sieć VLAN, przejdźmy do konfiguracji globalnej przełącznika i wydajmy polecenie `vlan [numer_sieci_VLAN]:`

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#vlan 8
Switch(config-vlan)#
```

Po utworzeniu sieci VLAN ponownie wyświetlmy wszystkie poleceniem `show vlan`:

```
Switch#
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
8    VLAN0008                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
8    enet  100008     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
Switch#
```

Na powyższym listingu widać nowo utworzoną sieć VLAN 8 oraz jej status ustawiony na aktywna (ang. active).

Podczas konfiguracji nowych sieci VLAN nadawana jest im domyślna nazwa. Nazwa ta może zostać zmieniona na bardziej intuicyjną, kojarzącą sieć, w której będą pracować, np. administracja.

Aby zmienić nazwę sieci, przejdźmy do konfiguracji sieci VLAN, następnie wydajmy polecenie `name [nazwa]`:

```
Switch(config)#vlan 8
Switch(config-vlan)#name ADMINISTRACJA
Switch(config-vlan)#
```

Aby zobaczyć zmienioną nazwę, wyświetlmy utworzone sieci VLAN.

### Przypisanie interfejsów do utworzonej sieci VLAN

Aby można było wykorzystać utworzoną wcześniej sieć VLAN, konieczne jest przypisanie do niej konkretnych interfejsów przełącznika. Załóżmy, że w sieci VLAN 8 będą pracowały dwa komputery. Jeden z nich jest podłączony do interfejsu FastEthemet0/10, a drugi do interfejsu FastEthemet0/15. Interfejsy te należy przydzielić sieci VLAN 8.

Na początek konieczne jest określenie trybu pracy interfejsu. Każdy interfejs może pracować bowiem w trzech trybach. Przejdźmy do konfiguracji interfejsu FastEthemet0/10 i wydajmy polecenie `switchport mode ?`:

```
Switch(config-if)#switchport mode ?
  access    Set trunking mode to ACCESS unconditionally
  dynamic   Set trunking mode to dynamically negotiate access or trunk mode
  trunk     Set trunking mode to TRUNK unconditionally
Switch(config-if)#switchport mode
```

Pierwszym trybem jest **tryb dostępowy (ang. `access`).** Tryb ten używany jest wtedy, kiedy do interfejsu przełącznika będzie podłączone urządzenie końcowe, np. komputer, drukarka itd.

Jeśli planujemy podłączenie do konfigurowanego interfejsu drugiego przełącznika, należy wybrać **tryb `trunk`**. Port będzie umożliwiał przesyłanie pomiędzy przełącznikami oznaczonych ramek.

Trzecim trybem jest **tryb dynamiczny (ang. `dynamic`).** W trybie dynamicznym przełącznik sam zadecyduje, w jakim trybie będzie pracować interfejs. Jeśli zostanie wykryte podłączenie komputera, interfejs przejdzie w stan **`access`**, i na odwrót, jeżeli do interfejsu zostanie podłączony inny przełącznik, interfejs przejdzie w tryb **`trunk`**. W niektórych przypadkach może okazać się przydatny tryb **`dynamic`**, ale jego wykorzystywanie w dużych sieciach nie jest zalecane.

Kontynuując opisywany przypadek, zakładamy, że do interfejsu będą podłączone komputery, dlatego w konfiguracji interfejsów należy ustawić `tryb access` za pomocą polecenia `switchport mode access`:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet 0/10
Switch(config-if)#switchport mode access
Switch(config-if)#
```

Następnie w konfiguracji interfejsu wydajemy polecenie `switchport access [numer_sieci_vlan]`, aby przypisać do interfejsu konkretną sieć VLAN. Oto przykład:

```
Switch(config-if)#switchport access vlan 8
Switch(config-if)#
```

W ten sposób interfejs FastEthemet0/10 został przypisany do sieci VLAN 8. Aby sprawdzić przypisanie, wydajemy w trybie uprzywilejowanym polecenie `show vlan brief`:

```
Switch#
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24
8    ADMINISTRACJA                    active    Fa0/10
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Zauważmy, że z prawej strony w kolumnie Ports pojawił się symbol Fa0/10. Port ten nie jest widoczny w interfejsach przypisanych do sieci VLAN 1.

Pamiętajmy, że interfejs może znajdować się tylko w jednej sieci VLAN.

W ten sam sposób dokonajmy konfiguracji interfejsu FastEthemet0/15. Oto przykład:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastEthernet 0/15
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 8
Switch(config-if)#end
Switch#
```

Po przypisaniu interfejsu ponownie wyświetlmy podsumowanie wszystkich sieci VLAN. Tym razem w kolumnie Ports znajdą się dwa interfejsy - Fa0/10 oraz Fa0/15.

## Polecenia show związane z sieciami VLAN

Podczas konfiguracji sieci VLAN możemy użyć kilku poleceń `show` umożliwiających przeglądanie wprowadzonych zmian oraz weryfikację ich poprawności.

Aby wyświetlić właściwości konkretnej sieci VLAN, znając jej nazwę, użyjemy poleceni `show vlan name [nazwa_vlan]`. Jeśli znamy numer VLAN, którego właściwości chcemy przejrzeć, wpisujemy polecenie show `vlan id [numer_vlan]`. Oto przykład:

```
Switch#show vlan name ADMINISTRACJA

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
8    ADMINISTRACJA                    active    Fa0/10, Fa0/15

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
8    enet  100008     1500  -      -      -        -    -        0      0
```

Jak widać na powyższym listingu, polecenie wyświetla właściwości tylko określonej sieci VLAN, m.in. jej nazwę, numer, status oraz przypisane porty.

Kolejnym poleceniem jest `show interface [interfejs] switchport`. Po jego wydaniu pojawią się właściwości określonego interfejsu w kontekście sieci VLAN. Oto przykład:

```
Switch#show interfaces fastEthernet 0/10 switchport
Name: Fa0/10
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 8 (ADMINISTRACJA)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

Na powyższym listingu znajdują się m.in. informacje na temat nazwy interfejsu (ang. name) oraz trybu jego pracy (ang. mode) i sieci VLAN, do której jest podłączony (ang. Access Mode VLAN).

### Usuwanie sieci VLAN oraz przypisania z sieci VLAN

Usuwanie przypisania interfejsu do sieci VLAN zawsze rozpoczynamy od wyświetlenia wszystkich sieci VLAN, aby dokładnie określić, jaki port musi zostać wyłączony z danej sieci. Wydajmy więc polecenie `show vlan brief`:

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
8    ADMINISTRACJA                    active    Fa0/10, Fa0/15
23   VLAN0023                         active
34   VLAN0034                         active
56   VLAN0056                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Naszym zadaniem jest usunięcie przypisania wszystkich interfejsów z VLAN 8, a następnie usunięcie VLAN 23, VLAN 34 i VLAN 56.

W tym celu przejdźmy do konfiguracji globalnej, następnie użyjmy polecenia `interface rangę fastethernet 0/10 - 15`, które sprawi, że przejdziemy od razu do konfiguracji wszystkich tych interfejsów jednocześnie. Nie będzie więc konieczności wpisywania za każdym razem tych samych poleceń.

Następnie w trybie konfiguracji interfejsów wydajmy polecenie `no switchport access vlan 8`. Usuniemy w ten sposób przypisanie interfejsów do danej sieci VLAN. Oto przykład:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/10-15
Switch(config-if-range)#no switchport access vlan 8
Switch(config-if-range)#
```

Wydajmy polecenie `show vlan brief`, aby sprawdzić wynik:

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
8    ADMINISTRACJA                    active
23   VLAN0023                         active
34   VLAN0034                         active
56   VLAN0056                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Zauważmy, że interfejsy, które wcześniej były przypisane do sieci VLAN 8, zostały automatycznie przeniesione do domyślnej sieci VLAN 1. W sieci VLAN 8 nie ma już żadnych przypisanych interfejsów.

Kolejnym krokiem jest usunięcie niepotrzebnych sieci VLAN. W tym celu w trybie konfiguracji globalnej wydajemy polecenie `no vlan [numer_VLAN]`:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no vlan 23
Switch(config)#no vlan 34
Switch(config)#no vlan 56
```

Wydajmy polecenie `show vlan brief`, aby sprawdzić wynik. Podane sieci zostały usunięte.

Zauważmy, jak często wykorzystywane jest polecenie `show vlan brief`. Bardzo istotne jest, aby na każdym etapie konfiguracji VLAN było ono wykorzystywane. Zanim coś usuniemy lub zmodyfikujemy, zawsze upewnijmy się, że o to nam chodzi, szczególnie wtedy, jeśli sprawa dotyczy sieci VLAN.

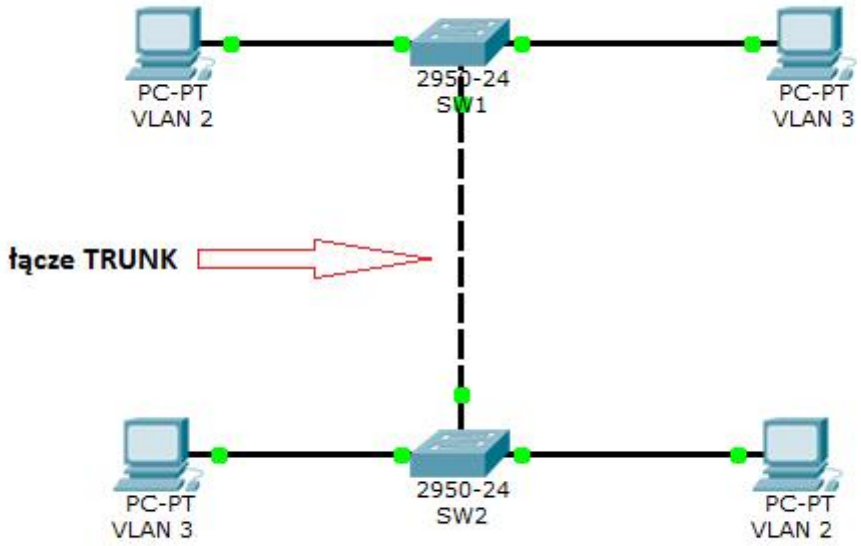
Zauważmy, że do jednej sieci VLAN można przypisać nawet kilkaset portów. Jeśli taką sieć usuniemy, kilkaset osób zostanie odłączonych od sieci, a to może wpłynąć na wydajność całej firmy.

## 1.7 Łączenie sieci VLAN – trunking

Podczas konfiguracji sieci VLAN będziemy również niejako zmuszeni do zapoznania się z pojęciem trzonu (magistrali) VLAN (ang. VLAN **`trunk`**). Jest to bezpośrednie połączenie między przełącznikami lub routerem, przenoszące dane przesyłane przez sieci VLAN.

Zauważmy, że tworzenie sieci VLAN ma zapewnić przede wszystkim połączenie pomiędzy różnymi lokalizacjami. Tak więc możliwe jest tworzenie na jednym przełączniku kilku sieci VLAN i podłączenie do innego przełącznika, na którym również utworzone są sieci VLAN. Przełączniki muszą jakoś wymieniać ze sobą informacje płynące z poszczególnych sieci VLAN, używają do tego celu połączeń **`trunk`**.

Na poniższym rysunku widać dwa przełączniki — s1 oraz s2.



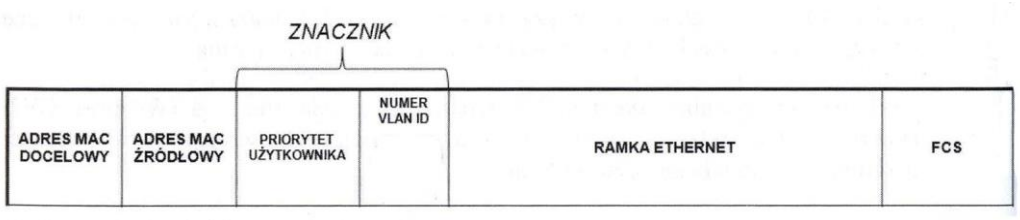

Jeśli w tym przypadku stacja robocza oznaczona jako VLAN 3 wyśle rozgłoszenie do przełącznika SW1, wówczas przełącznik, analizując przesłaną ramkę, stwierdzi, że do sieci VLAN 3 na przełączniku SW1 nie należą żadne porty i otrzymane dane trzeba przesłać przy użyciu połączenia **`trunk`** do przełącznika SW2 sieci VLAN3, w której się znajduje.

W tym przypadku rozgłoszenie nie będzie wysyłane do innych stacji roboczych znajdujących się w podanej sieci.

**W jaki sposób przełącznik „wie", do jakiej sieci VLAN przypisać przychodzącą ramkę?**

W sieciach, w których zastosowano technologię VLAN, wszystkie ramki należące do określonej sieci VLAN są znakowane (ang. tagging). Do każdego nagłówka ramki ethernetowej jest dodawana krótka informacja na temat tego, z jakiej sieci VLAN pochodzi. Pole określające (znakujące) ramkę posiada długość 1 bitu.

W uproszczeniu ramka przesyłana z przełącznika SW1 do SW2 przez połączenie `trunk` będzie wyglądać następująco:




Po otrzymaniu znakowanej ramki przełącznik usuwa znacznik i przekazuje ją do określonej sieci VLAN. Znakowanie ramek odbywa się w warstwie 2. ISO/OSI. Do nagłówka ramki ethernetowej dodawane jest pole znacznika, w którym znajduje się m.in. numer sieci VLAN. Przesyłaniem ramek przez połączenie `trunk` zajmuje się protokół 802.1Q (ang. trunking protocol).

## Konfiguracja połączeń trunk

Najpierw należy określić port lub porty, które będą umożliwiać przekazywanie ruchu pochodzącego z poszczególnych sieci VLAN. Załóżmy, że będzie to interfejs FastEthernet0/1. W praktyce należy więc interfejs FastEthernet0/1 połączyć z innym przełącznikiem. Na drugim urządzeniu konieczne jest wykonanie tych samych czynności.

Na początek należy przejść do konfiguracji interfejsu. Następnie wydać polecenie `switchport mode trunk`. W zasadzie podstawowa konfiguracja sprowadza się tylko do tych czynności. Oto przykład:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Switch(config-if)#exit
Switch(config)#
```

Aby sprawdzić stan interfejsu, wydaj polecenie:
`show interface FastEthernet 0/1 switchport:`

```
Switch#show interface FastEthernet 0/1 switchport
Name: Fa0/1
```

```
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
Switch#
```

Na powyższym listingu widać, że interfejs pracuje jako `trunk`. Następnie podano rodzaj enkapsulacji - `dotlq`.

Rodzaj enkapsulacji to metoda przesyłania danych przez połączenie `trunk`. Kilka lat temu firma Cisco udostępniała jeszcze inną metodę enkapsulacji wykorzystującą protokół ISL (ang. Inter-Switch Link). Tak więc wszystkie przełączniki umożliwiały zastosowanie protokołów ISL lub 802.1Q.

Przez lata protokół 802.1Q stał się jednak bardziej optymalny i coraz częściej używany | dlatego w nowych przełącznikach zrezygnowano z obsługi protokołu ISL i wykorzystywany jest jedynie 802.1Q. Stąd na przełączniku 2960, który został skonfigurowany! powyżej, dostępna jest enkapsulacja `dotlq`. W celu sprawdzenia, czy połączenie `trunk` działa, możesz posłużyć się jeszcze poleceniem: `show vlan brief`:

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24
8    ADMINISTRACJA                    active    Fa0/10, Fa0/15
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Zauważmy, że interfejs FastEthernet0/1 po konfiguracji na nim połączenia `trunk` nie jest dostępny na liście. Świadczy to o prawidłowej konfiguracji.

Ostatnim poleceniem, które może okazać się pomocne w celu weryfikacji utworzonych połączeń trunk, jest `show interfaces trunk`:

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,8

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,8
```

W pierwszej linii widać symbol interfejsu, na którym skonfigurowano `trunk`, następnie podana jest enkapsulacja. W trzecim wierszu wyliczono sieci VLAN, które są utworzone na przełączniku i dopuszczone do przesyłania danych przez utworzone połączenie `trunk`.

## Literatura


[1] „W drodze do CCNA” A. Józefiok

[2] http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg.pdf