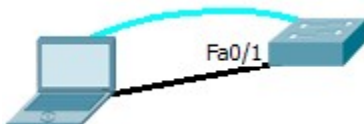


Tematyka:

Konfigurowanie przełączników nie routujących Cisco Catalyst:
Dynamic Trunking Protocol. Trunks, konfigurowanie sieci VLAN, VLAN Tunneling Protocol

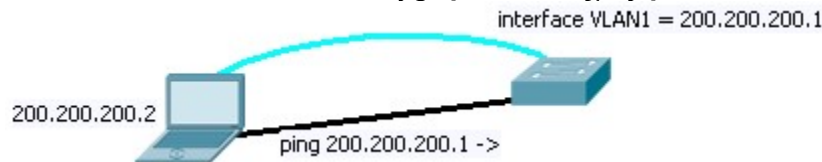
Zadanie A: Podstawowa konfiguracja ustawień przełącznika Cisco Catalyst

1. Połącz stację PC z przełącznikiem Ethernet Cisco Catalyst 2950, 2960, 3550, 3560 lub 3750 przy użyciu kabla *Twisted Pair* i wykorzystując wybrane gniazda Ethernet. Zamontuj kabel konsoli pomiędzy tymi urządzeniami.



2. Po nawiązaniu połączenia konsoli pomiędzy przełącznikiem i stacją PC zaktywuj tryb uprzywilejowany (exec) CLI przełącznika - komendą *enable* (skrót: *en*). Poprawne przejście do tego trybu zasygnalizuje symbol '#'.
3. Następnie przejdź do trybu konfiguracji przełącznika z wykorzystaniem terminala:
Switch#configure terminal
Switch(config)#
4. Przełącznik nie routujący (tzw. "warstwy drugiej ISO OSI") może posiadać swoją tożsamość w sieci IP, a co za tym idzie - interfejsy IP. Ta funkcjonalność wykorzystywana jest tu jednak tylko w celach administracyjnych (na przykład za pośrednictwem połączeń telnet, HTTP czy SSH z przełącznikiem możliwe jest jego konfigurowanie). Adresy IP nie mogą być przypisywane do portów fizycznych przełączników jak w przypadku stacji PC czy routera IP). Aby przełącznik mógł posiadać adres IP - adresację IP otrzymują specjalne wirtualne interfejsy związane z sieciami VLAN budowanymi w przełączniku. Sieć VLAN w przełączniku Ethernet to zbiór wybranych przez administratora portów przełącznika. Poszczególne sieci VLAN mogą być od siebie izolowane - dzieląc tym samym przełącznik Ethernet na kilka wyizolowanych sekcji (komunikacja pomiędzy portami Ethernet należącymi do różnych VLAN nie będzie możliwa). Sieci VLAN są numerowane. Domyślnie - wszystkie porty przełącznika zakwalifikowane są do VLAN1.
5. Należy skonfigurować adres IP interfejsu VLAN1 przełącznika oraz włączyć (zaktywować) ten interfejs.
Switch(config)#interface vlan1
Switch (config-if)#ip address 200.200.200.1 255.255.255.0
Switch (config-if)#no shutdown
Interfejs VLAN w przełącznikach warstwy drugiej ISO OSI służy jedynie do

komunikowania się z hostem IP przełącznika w celach konfiguracyjnych i kontrolnych (poprzez wybrany VLAN). Należy skonfigurować adres IP stacji PC podłączonej do przełącznika. Adresacja IP dla wszystkich interfejsów używanych w danym segmencie sieci IP musi spełniać ogólnie znane reguły. Przykładowo przy masce 255.255.255.0 może ona wyglądać następująco:



Uwaga: Gdy żaden z portów fizycznych Ethernet zakwalifikowanych do danego VLAN (w przykładzie do VLAN1) nie znajduje się w stanie *Forwarding* - uruchomienie VLAN nie będzie możliwe. Konieczne jest zatem podłączenie przynajmniej jednego urządzenia (np. stacji PC) do portów przełącznika zakwalifikowanych do przedmiotowego VLAN.

6. Konfigurowanie trybu pracy portu przełącznika.

Każdy z portów przełącznika może pracować w jednym z trzech narzuconych przez administratora trybów: *access* (port prowadzący do DTE), *trunk* (port prowadzący do DCE), *dynamic* (tryb pracy negocjowany automatycznie - zależnie od typu urządzenia po drugiej stronie podłączonego kabla). Od wybranego trybu zależy rodzaj ramkowania Ethernet, jakie jest stosowane w łączy (IEEE 802.3 lub IEEE 802.1Q). Tryb (poniżej przykład dla trybu *access*) można ustalać komendą:

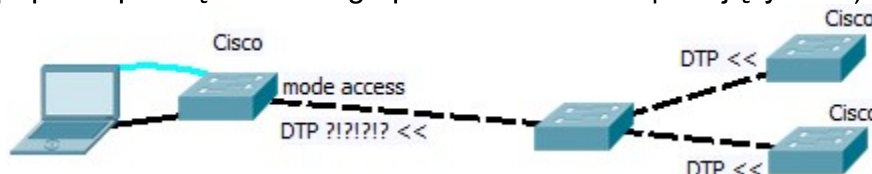
```
Switch(config)#interface fa 0/5
```

```
Switch(config-if)#switchport mode access
```

gdzie fa 0/5 to skrócony identyfikator portu typu *Fast Ethernet* o numerze 5 znajdującego się bezpośrednio z obudowie przełącznika (co sygnalizuje liczba 0 w tym identyfikatorze). Identyfikatory portów w przypadku przełączników Catalyst to przeważnie fa 0/1..0/n dla Fast Ethernet, czy gig 1/0/1..gig 1/0/n lub gig 0/1..gig 0/n dla portów Gigabit Ethernet

Tryb *dynamic* portu jest wybierany domyślnie. Przełącznik Cisco do identyfikacji rodzaju portu po drugiej stronie kabla używa protokołu DTP (*Dynamic Trunking Protocol*). Czyni to także wtedy, gdy wybrano inny niż *dynamic* tryb pracy portu (na wypadek włączenia trybu *dynamic* przez administratora).

Uwaga! - nie jest możliwe stosowanie protokołu DTP w trybie innym niż *dynamic* gdy kabel prowadzi do wielu innych przełączników Cisco jednocześnie (na przykład poprzez przełącznik innego producenta nie wspierający DTP):



Napływające (sprzeczne) komunikaty DTP uniemożliwią wtedy ustalenie trybu pracy dla portu, a przełącznik sam nie może go negocjować (brak aktywnego trybu *dynamic*). Gdy dodatkowo konfiguracja tzw. domeny VTP (*VLAN Trunking Protocol*) przełącznika będzie kolidowała z innym przełącznikiem (co może zdarzyć się w Laboratorium) - port zostanie wyłączony i zobaczymy komunikat: *%DTP-5-DOMAINMISMATCH: Unable to perform trunk negotiation on port Fa0/5 because of VTP domain mismatch.*

Aby definitywnie wyłączyć DTP dla danego portu i w takiej sytuacji usunąć problem, należy posłużyć się komendami:

```
Switch(config)#interface fa 0/5
Switch(config-if)#switchport nonegotiate
```

7. Należy sprawdzić ustawienia interfejsów IP przełącznika:

```
Switch#show ip interface brief
Switch#show ip interface vlan 1
```

lub z trybu konfiguracji:

```
Switch(config)#do show ip interface brief
Switch(config)#do show ip interface vlan 1
```

Należy zwrócić uwagę na stan aktywności danych interfejsów (up/down/administratively down).

Zadanie B: Konfigurowanie VLAN przełącznika Cisco Catalyst

1. Sprawdź aktualny stan bazy VLAN w przełączniku:

```
Switch#show vlan
```

2. Stwórz dwie nowe sieci VLAN o wybranych numerach:

```
Switch#conf t
Switch(config)#vlan 20
Switch(config-vlan)#exit
Switch(config)#vlan 21
```

Uwaga: ręczna modyfikacja puli sieci VLAN nie jest możliwa w trybie *CLIENT* VTP (*VLAN Trunking Protocol*) przełącznika. W przypadku odmowy założenia VLAN z takiego powodu, należy zmienić tryb VTP:

```
Switch(config)#vtp mode transparent
```

3. Przypisz pojedyncze porty do nowych VLAN, przykładowo:

```
Switch(config)#interface fa0/2
Switch(config-if)#no shutdown
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
```

W momencie dokonania takiego przypisania porty zostaną przesunięte z VLAN1 do VLAN20. W przypadku wystąpienia problemów negocjacji typu portu powodowanych przez protokół DTP - wyłącz działanie tego protokołu dla odpowiedniego portu Ethernet:

```
Switch(config)#interface fa 0/2
Switch(config-if)#switchport nonegotiate
```

4. Przypisz porty do nowych VLAN inną metodą – poprzez aktywowanie i konfigurowanie całego zakresu portów jednocześnie:

```
Switch(config)#interface range fa0/15 - 17
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
```

Uwaga: w treści przykładowego wyrażenia "15 - 17" muszą być zastosowane spacje.

5. Sprawdzenie klasycznego (używanego dawniej) trybu modyfikowania VLAN (tryb ten może być niedostępny już w niektórych przełącznikach):

Wprowadź komendę (w trybie exec):

```
Switch#vlan database
```

i sprawdź opcje dostępne w trybie edycji bazy VLAN (ten tryb zarządzania bazą VLAN pochodzi z przełączników pracujących pod kontrolą systemu CatalystOS).

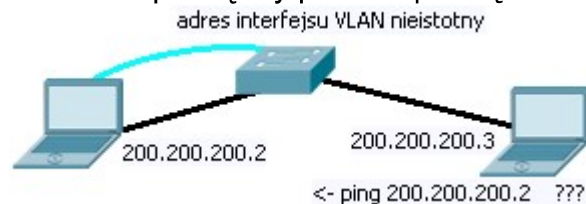
Wyjście z trybu edycji VLAN:

`Switch(vlan)#exit`

6. Sprawdź kolejno (ping) możliwość komunikowania się stacji PC:
 - pomiędzy portami przełącznika należącymi do dwóch różnych VLAN
 - pomiędzy portami przełącznika w ramach jednej VLAN

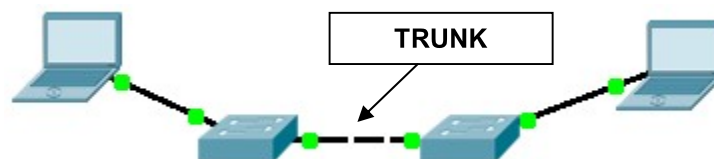
W tym celu:

- podłączaj kolejno dwie stacje PC kablami TP (*Twisted Pair*) do dwóch wybranych portów przełącznika (podlegających sprawdzeniu komunikacji)
- skonfiguruj adresację IP obydwu stacji PC tak, aby znajdowały się one w tej samej sieci IP (zgodnie z ogólnie znanymi zasadami)
- wykonaj *ping* z jednej stacji PC do drugiej (sprawdzając tym samym możliwość komunikowania pomiędzy portami przełącznika)



Zadanie C: Tworzenie VLAN trunks i tagowanych VLAN w przełącznikach Cisco Catalyst

1. VLAN trunks (z użyciem IEEE 802.1Q) umożliwia tworzenie systemu sieci VLAN obejmujących wiele przełączników. Każdy VLAN może być budowany z portów rozproszonych po przełącznikach znajdujących się w różnych lokalizacjach. Dodatkowo - system tagowania ramek IEEE 802.1Q pozwala na użycie jednego połączenia fizycznego między portami przełączników (trunk) - pomimo konieczności przekazania izolowanych od siebie ramek wielu różnych VLAN.
2. Należy przygotować dwie stacje PC i dwa przełączniki. Przełączniki należy połączyć ze sobą kablem TP RJ45 – ten kabel będzie służył do komunikowania kilku VLAN jednocześnie pomiędzy przełącznikami (trunk). Stacje PC należy podłączyć po jednej do każdego przełącznika.



3. W obydwu przełącznikach należy określić jako trunk port, do którego podłączony jest kabel komunikujący przełączniki (w przykładzie jest to fa0/1):

`Switch(config)#interface fa0/1`

`Switch(config-if)#no shutdown`

`Switch(config-if)#switchport mode trunk`

gdzie *switchport mode trunk* zmienia przeznaczenie portu - na trunk.

Standardowo każdy port przełącznika znajduje się w stanie *dynamic*, czyli adaptuje się automatycznie do trybu pracy portu po przeciwległej stronie kabla, korzystając z protokołu DTP (*Dynamic Trunking Protocol*).

Uwaga: W niektórych wersjach przełączników (np. Catalyst 3550) konieczne jest jawne wytypowanie rodzaju enkapsulacji stosowanej przez port - jako IEEE 802.1Q (zanim będzie możliwe uruchomienie trybu trunk dla portu):

```
Switch(config-if)#switchport trunk encapsulation dot1q
```

4. W kolejnym kroku należy zezwolić na komunikowanie wybranych VLAN poprzez trunk:

```
Switch(config-if)#switchport trunk allowed vlan 1-100
```

Uwaga: Powyższa komenda działa z kilkunastosekundowym opóźnieniem.

Usuwanie zezwolenia, np.:

```
Switch(config-if)#switchport trunk allowed vlan remove 10
```

5. Sprawdź otrzymaną konfigurację kontrolując, czy port został zakwalifikowany jako trunk:

```
Switch#show running-config
```

```
Switch#show interface trunk
```

```
Switch#show interface fa 0/1 switchport
```

```
Switch#show interface fa 0/1 status
```

6. Sprawdź otrzymaną konfigurację kontrolując, czy port został usunięty ze wszystkich VLAN (teraz pełni funkcję specjalną: *trunk* zamiast *access*):

```
Switch#show vlan
```

7. Po skonfigurowaniu obydwu przełączników sprawdź przy użyciu stacji PC funkcjonowanie rozproszonych pomiędzy przełącznikami VLAN oraz izolowanie portów należących do różnych VLAN. W tym celu podłączaj stacje kolejno do różnych VLAN w dwóch przełącznikach - sprawdzając, kiedy stacje będą mogły się kontaktować.

8. Native VLAN w VLAN Trunks:

Port przełącznika skonfigurowany jako *trunk* stosuje dla przekazywanego przez łączy ruchu enkapsulację IEEE 802.1Q. Jednak jednocześnie dla jednej wyróżnionej sieci VLAN nadal możliwe jest przekazywanie ruchu w trybie native (bez enkapsulacji IEEE 802.1Q). Sieć VLAN, dla której w *trunk* taki ruch jest dopuszczony (domyślnie jest to VLAN 1) określamy mianem *native VLAN*. Wyboru numeru tej sieci VLAN dla określonego portu przełącznika należy dokonać poprzez zastosowanie instrukcji:

```
Switch(config)#int fa 0/1
```

```
Switch(config-if)#switchport trunk native vlan 10
```

Uwaga: W obydwu połączonych ze sobą przełącznikach konfiguracja *native VLAN* musi być zgodna (czyli wybrany został ten sam numer *native VLAN*)

Weryfikacja, np.:

```
Switch#show interface fa 0/1 trunk
```

lub

```
Switch#show interface fa 0/1 switchport
```

Zadanie D: VLAN i protokół VTP (Virtual LAN Trunking Protocol)

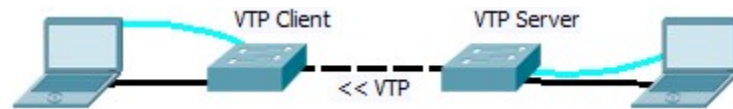
VLAN Trunking Protocol umożliwia automatyczną propagację informacji o VLAN pomiędzy przełącznikami. Tworzone są tzw. domeny VTP, a informacja jest przekazywana w ramach tej samej domeny (domena VTP identyfikowana jest poprzez nazwę konfigurowaną w przełącznikach). Każdy z przełączników jest przypisywany do domeny jako pełniący jedną z trzech możliwych funkcji:

- *server* (który jest konfigurowany przez użytkownika i serwuje informację do przełączników VTP *client*),
- *transparent* (który jedynie przekazuje komunikaty VTP dalej, lecz nie aktualizuje swojej bazy VLAN),
- *client* (który konfiguruje własne VLAN na podstawie komunikatów serwera VTP).

Uwagi:

- aby VTP funkcjonował poprawnie na trasie łącza fizycznego pomiędzy przełącznikami nie może być innych przełączników (innych firm lub w innej domenie VTP)
- gdy przełącznik dołącza do domeny VTP, pobiera automatycznie bazę VLAN od już istniejących przełączników w domenie (nawet gdy będzie tam serwerem, a w domenie wcześniej jest tylko klient). Jego poprzednia baza zostanie utracona!
- łącze (porty przełącznika) wykorzystywane do przekazywania informacji w ramach VTP należy skonfigurować jako *trunk*:
`Switch(config-if)#switchport mode trunk`
 Sprawdzenia można dokonać np. w raporcie generowanym przez, np.:
`Switch(config)#show int fa 0/1 switchport`
 Należy usunąć z konfiguracji tych portów inne wpisy ograniczające pracę w trybie *trunk* (mogące pozostać po realizacji innych zadań).
- W obydwu przełącznikach należy skonfigurować identyczną nazwę domeny VTP, np.:
`Switch(config)#vtp domain domena`
 Uwaga!: Nazwa domeny VTP stosowana w doświadczeniu musi być unikatowa! (więc w Laboratorium nie należy używać powyższej, przykładowej). Jeżeli w sieci pojawi się inny przełącznik w trybie *vtp server* i posiadający taką samą nazwę domeny VTP - system ten nie zadziała poprawnie.
- Urządzenia uczestniczące w VTP można zabezpieczać hasłem:
`Switch(config)#vtp password haslo`
 Uwaga: Gdy hasła w kliencie i serwerze VTP są niezgodne, w przełącznikach pojawi się niezgodność *hash-kodów MD5* (obliczanych na podstawie haseł i potrzebnych później do zakodowania/rozkodowania komunikatów VTP). W konsekwencji VTP nie zadziała. Należy wtedy ujednolicić hasła VTP w przełącznikach lub je usunąć.
- W przypadku dalszych błędów niezgodności *hash-kodów MD5 VTP* należy przeprowadzić klienta VTP do trybu *transparent*, po czym ponownie do trybu *client* (odpowiednie komendy podano niżej)
- W przypadku błędów *niezgodności VTP revision number* i braku możliwości kasowania *revision number* komendami VTP należy zmienić nazwę tzw. domeny VTP na inną i następnie ponownie na poprzednią (odpowiednie komendy podano niżej)
- Sprawdzenie statusu VTP:
`Switch#show vtp status`
- Diagnostyka VTP (należy włączyć do doświadczeń w przełączniku klienta VTP), oraz gdy VTP nie zadziałało:
`Switch#debug sw-vlan vtp events`

1. Należy przygotować dwa przełączniki Cisco (modele 2950, 2960, 3550, 3560, 3750) łącząc je kablem TP (*Twisted Pair*) lub światłowodem. Jeden z nich będzie konfigurowany jako serwer VTP, drugi - jako klient VTP.



W przełączniku wytypowanym do roli serwera VTP należy skonfigurować tryb pracy VTP: serwer (jest to ustawienie domyślne, jednak należy je zweryfikować):
`Switch(config)#vtp mode server`

2. W przełączniku klienta VTP należy skonfigurować domenę VTP o identycznej nazwie jak w serwerze VTP, a tryb VTP jako *klient*:

`Switch(config)#vtp domain domena`

`Switch(config)#vtp mode client`

3. Następnie w przełączniku-serwerze VTP należy zdefiniować kilka VLAN, np.:

`Switch(config)#vlan 20`

`Switch(config-vlan)#exit`

`Switch(config)#vlan 21`

`Switch(config-vlan)#exit`

`Switch(config)#vlan 22`

`Switch(config-vlan)#exit`

Uwaga: Propagacja komunikatu VTP o nowym VLAN następuje dopiero po wydaniu komendy `exit`.

Uwaga: Konieczne jest zdefiniowanie VLAN, a nie utworzenie/skonfigurowanie interfejsów IP VLAN. To drugie realizowałoby się komendą:

`Switch(config)#interface vlan 3`

Gdy utworzono błędnie interfejs IP VLAN, można skasować komendą:

`Switch(config)#no int vlan 3`

4. Po dokonaniu ustawień należy sprawdzić, czy zdefiniowane w serwerze VTP sieci VLAN przemiegrowały do drugiego przełącznika (do *vtp client*):

`Switch#show vlan`

W przełączniku klienta VTP pozycja *Number of existing VLANs* powinna zostać zwiększona z bazowej ilości (5) o ilość sieci VLAN, jakie skonfigurowano za pośrednictwem VTP. Teraz możliwe jest przydzielanie portów do VLAN otrzymanych od serwera VTP.

5. Przetaw przełącznik klienta VTP w tryb *transparent*:

`Switch(config)#vtp mode transparent`

Przełącznik powinien teraz przestać aktualizować swoją bazę VLAN, przekazując jednak komunikaty VTP do ewentualnych dalszych przełączników. Dokonaj zmian w bazie w serwerze VTP i sprawdź, czy faktycznie nie doszło do aktualizacji VLAN. Następnie przywróć w przełączniku rolę klienta VTP

`Switch(config)#vtp mode client`

i sprawdź, czy baza VLAN została zaktualizowana.

6. Metoda wymuszenia aktualizacji VTP - należy chwilowo założyć i usunąć VLAN w serwerze VTP (innej niestety nie ma)..

7. Sprawdzenie stanu i diagnostyka:

`Switch#show vtp status`

`Switch#debug sw-vlan vtp events`

Podczas eksperymentów należy obserwować rosnącą wartość *Revision number* w raporcie osiągalnym komendą *show vtp status* i wskazującą na kolejną aktualizację listy VLAN, zaczynając od 0.