Sieci 021

wtorek, 8 marca 2022 15:44

A

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.

1. Podłączyć PC ze switchem Cisco Catalyst 2950/2960/3550/3560/3750 przy użyciu skrętki
2. Podłączyć kabel Console do Switcha
3. Wejść do CLI Switcha i uruchomić tryb uprzywilejowany poleceniem enable
4. Wejść do trybu configuracji poleceniem configure terminal
5. Adresy IP nie mogą być przypisane do portów fizycznych Switcha. Aby Switch mógł mieć IP to należy skonfigurować wirtualny interfejs w sieci VLAN. Przed konfigurowaniem interfejsu należy sprawdzić czy adres nie jest już zajęty (np. przez ping).
6. Należy skonfigurować adres IP interfejsu VLAN1 przełącznika oraz włączyć ten interfejs.
   Switch> enable
   Switch# configure terminal
   Switch(config)# interface vlan1
   Switch(config-if)# ip address 200.200.200.1 255.255.255.0
   Switch(config-if)# no shutdown
7. Skonfigurować adres IP stacji roboczej (np. 200.200.200.2)
8. 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 (domyślny)

   // Przykład zmiany trybu pracy portu
   Switch(config)# interface fa 0/5
   Switch(config-if)# switchport mode access

   Dynamic na podstawie tego co jest po drugiej stronie kabla (wybierane przez protokół DTP). DTP puszczane jest zawsze, nawet jeżeli tryb pracy jest inny niż dynamic (na wypadek jeśli administrator nagle by włączył dynamic). Nie może być po dwóch stronach dynamic. DTP nie działa, jeżeli po drugiej stronie kabla jest więcej niż jeden przełącznik Cisco (np. gdy ruch przechodzi przez przełącznik innego producenta, który nie wspiera DTP). Żeby definitywnie wyłączyć DTP, trzeba w interfejsie wpisać
   Switch(config)# interface fa 0/5
   Switch(config-if)# switchport nonegotiate
9. Sprawdzić ustawienia interfejsów IP przełącznika (należy zwrócić uwagę na stan aktywności danych interfejsów (up/down/administratively down).
   Switch#show ip interface brief
   Switch#show ip interface vlan 1

B

10. Sprawdzić aktualny stan bazy VLAN
    Switch# show vlan
11. Stworzyć dwie nowe sieci VLAN o wybranych numerach
    Switch# conf t
    Switch(config)# vlan20
    Switch(config-vlan)# exit
    Switch(config)# vlan21
    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
12. 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

13. 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

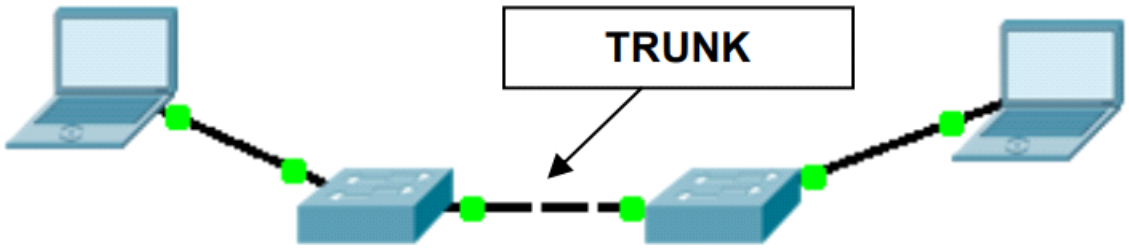
Uwaga: W treści przykładowego wyrażenia "15 - 17" muszą być zastosowane spacje.

14. Sprawdzenie klasycznego (używanego dawniej) trybu modyfikowania VLAN (tryb ten może być niedostępny już w niektórych przełącznikach):
Switch# vlan database
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
15. 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)

C

- 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.
- 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.

16. Przygotuj dwie stacje PC i dwa przełączniki. Połącz urządzenia zgodnie ze schematem



17. 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

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

18. 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.
Aby usunąć zezwolenie na komunikację między VLAN można użyć polecenia:
Switch(config-if)# switchport trunk allowed vlan remove 10

19. 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

20. Sprawdź otrzymaną konfigurację kontrolując, czy port został usunięty ze wszystkich VLAN (teraz pełni funkcję specjalną: trunk zamiast access):
    Switch# show vlan
21. 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.
22. Native VLAN w VLAN Trunks:
    - Port przełącznika skonfigurowany jako trunk stosuje dla przekazywanego przez łącze ruchu enkapsulację IEEE 802.1Q. Jednak jednocześnie dla jednej wyróŜnionej sieci VLAN nadal moŜliwe 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). Możemy to sprawdzić poleceniami
Switch# show interface fa 0/1 trunk // lub Switch# show interface fa 0/1 switchport
D
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 — konfigurowany przez admina, przesyła informację do Clientów
- transparent — jedynie przekazuje komunikaty VTP, nie aktualizuje swojej bazy VLAN
- client — 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

  Switch# 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 pracujący w trybie VTP Server i posiadający taką sama 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 przemigrowały 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. Przestaw 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 i sprawdź, czy baza VLAN została zaktualizowana.
   Switch(config)# vtp mode client
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.