# **CISCO** Academy

# Laboratorium - Konfiguracja sieci VLAN i łączy trunk

# Topologia sieci



# Tabela adresowania

| Urządzenie | Interfejs      | Adres IP     | Maska podsieci | Brama domyślna |
|------------|----------------|--------------|----------------|----------------|
| S1         | VLAN 1         | 192.168.1.11 | 255.255.255.0  | nd.            |
| S2         | VLAN 1         | 192.168.1.12 | 255.255.255.0  | nd.            |
| PC-A       | karta sieciowa | 192.168.10.3 | 255.255.255.0  | 192.168.10.1   |
| PC-B       | karta sieciowa | 192.168.10.4 | 255.255.255.0  | 192.168.10.1   |

## Cele

Część 1: Utworzenie sieci oraz konfigurowanie podstawowych ustawień urządzenia

Część 2: Utworzenie sieci VLAN i przypisanie do nich portów

Część 3: Zarządzanie przypisywaniem portów do sieci VLAN i bazą sieci VLAN

Część 4: Konfiguracja magistrali 802.1Q pomiędzy przełącznikami

Część 5: Usunięcie bazy sieci VLAN

# Wprowadzenie

Nowoczesne przełączniki wykorzystują wirtualne sieci lokalne (VLAN) w celu poprawy wydajności sieci poprzez rozdzielenie dużych domen rozgłoszeniowych warstwy 2 na mniejsze. Sieci VLAN mogą być również wykorzystywane jako środek bezpieczeństwa poprzez kontrolowanie, które hosty mogą się komunikować. Ogólnie rzecz biorąc, sieci VLAN ułatwiają projektowanie sieci w celu wspierania celów organizacji.

Magistrale VLAN są używane do rozciągnięcia sieci VLAN na wiele urządzń. Łącza trunk umożliwiają przesyłanie ruchu z wielu sieci VLAN jednym łączem, zachowując jednocześnie identyfikację i segmentację sieci VLAN.

W tym laboratorium utworzysz sieci VLAN na obu przełącznikach w topologii, przypiszesz sieci VLAN do portów dostępowych, zweryfikujesz, czy sieci VLAN działają zgodnie z oczekiwaniami, a następnie utworzysz magistralę VLAN między dwoma przełącznikami, aby umożliwić hostom w tej samej sieci VLAN komunikację przez łącze trunk, niezależnie z którego przełącznika jest faktycznie podłączony host.

**Uwaga**: Przełączniki używane w laboratoriach CCNA to Cisco Catalyst 2960 z Cisco IOS w wersji 15.2 (2) (obraz lanbasek9). Można użyć również innych routerów i przełączników Cisco z różnymi wersjami Cisco IOS. Zależnie od modelu urządzenia i wersji systemu IOS, dostępne polecenia i wyniki ich działania mogą się różnić od prezentowanych w niniejszej instrukcji. Przejrzyj tabelę podsumowującą interfejsy routera w celu określenia poprawnych identyfikatorów interfejsów.

**Uwaga**: Upewnij się, że konfiguracje startowe routerów i przełączników zostały wykasowane. Jeśli nie jesteś pewien, poproś o pomoc instruktora.

# Wymagane zasoby

- 2 przełączniki (Cisco 2960 z Cisco IOS Release 15.2(2) obraz lanbasek9 lub porównywalny)
- 2 komputery PC (Windows z emulatorem terminala takim jak Tera Term)
- Kable konsolowe do konfiguracji urządzeń Cisco przez porty konsolowe
- Kable Ethernet zgodnie z przedstawioną topologią

#### Instrukcje

# Część 1: Utworzenie sieci oraz konfigurowanie podstawowych ustawień urządzeń

W części 1 utworzysz topologię sieciową i skonfigurujesz podstawowe ustawienia komputerów i przełączników.

#### Krok 1: Zbuduj sieć zgodnie z topologią.

Połącz wymagane urządzenia oraz kable tak, jak pokazano na schemacie topologii.

#### Krok 2: Wykonaj podstawową konfigurację przełączników.

- a. Połącz się do konsoli przełącznika i przejdź do trybu uprzywilejowanego.
- b. Wejdź do trybu konfiguracji globalnej.
- c. Przypisz nazwę urządzenia do przełącznika.
- d. Wyłącz DNS lookup, aby zapobiec próbom tłumaczenia przez router i przełącznik niepoprawnie wprowadzonych komend, jako nazw hostów.
- e. Przypisz class jako zaszyfrowane hasło trybu uprzywilejowanego EXEC.
- f. Przypisz cisco jako hasło konsoli i włącz logowanie.
- g. Przypisz cisco jako hasło do VTY oraz włącz logowanie.
- h. Zaszyfruj hasła zapisane jawnym tekstem.
- Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony.
- j. Skonfiguruj adres IP, wyświetlony w tabeli adresowania dla sieci VLAN 1, na przełączniku.
- k. Wyłącz wszystkie interfejsy, które nie będą używane.
- I. Ustaw zegar na przełączniku.
- m. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

#### Krok 3: Skonfiguruj hosty PC.

Skonfiguruj adresy IP na komputerach zgodnie z tabelą adresacji.

#### Krok 4: Sprawdź łączność.

Sprawdź, czy ping pomiedzy hostami PC kończą się powodzeniem.

**Uwaga**: W celu umożliwienia wykonania poleceń ping pomiędzy komputerami konieczne może być wyłączenie zapory sieciowej w komputerach.

Czy ping z PC-A osiągną PC-B?

Czy ping z PC-A osiągną S1?

Czy ping z PC-B osiągną S2?

Czy ping z S1 osiągną S2?

Jeśli odpowiedziałeś "nie" na którekolwiek z powyższych pytań, dlaczego testy ping nie powiodły się?

#### Część 2: Utworzenie sieci VLAN i przypisanie portów przełącznika

W części 2 utworzysz sieci VLAN o nazwach Management, Operations, Parking\_Lot i Native na obu przełącznikach. Następnie przypiszesz sieci VLAN do odpowiedniego interfejsu. Polecenie **show vlan** służy do weryfikacji ustawień konfiguracyjnych.

#### Krok 1: Utwórz sieci VLAN na przełączniku.

```
a. Utwórz sieci VLAN na S1.
```

```
S1(config)# vlan 10
S1(config-vlan)# name Operations
S1(config-vlan)# vlan 20
S1(config-vlan)# vlan 99
S1(config-vlan)# vlan 99
S1(config-vlan)# vlan 1000
S1(config-vlan)# vlan 1000
S1(config-vlan)# name Native
S1(config-vlan)# end
```

- b. Utwórz te same sieci VLAN na S2.
- c. Wydaj polecenie show vlan brief, aby wyświetlić listę sieci VLAN na S1.
  - S1# 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

Gi0/1, Gi0/2

| 10 Opera              | <mark>tions active</mark> |
|-----------------------|---------------------------|
| <mark>20 Parki</mark> | ng_Lot active             |
| 99 Manage             | ement active              |
| 1000 Nat:             | <mark>ive active</mark>   |
| 1002 fdd:             | i-default act/unsup       |
| 1003 tok              | en-ring-default act/unsup |
| 1004 fdd:             | inet-default act/unsup    |
| 1005 trne             | et-default act/unsup      |
| Która to de           | omyślna sieć VLAN?        |

Jakie porty są przypisane do domyślnej sieci VLAN?

#### Krok 2: Przypisz sieci VLAN do odpowiednich interfejsów przełącznika.

- a. Przypisz sieci VLAN do interfejsów na S1.
  - 1) Przypisz PC-A do Operation VLAN.
    - S1(config)# interface f0/6
    - S1(config-if) # switchport mode access
    - S1(config-if) # switchport access vlan 10
  - 2) Przenieś adres IP przełącznika do sieci VLAN 99.

```
S1(config)# interface vlan 1
S1(config-if)# no ip address
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# end
```

- b. Wydaj polecenie show vlan brief i sprawdź, czy sieci VLAN są przypisane do odpowiednich interfejsów.
- c. Wykonaj komendę show ip interface brief.

Jaki jest status VLAN 99? Wyjaśnij.

- d. Przypisz PC-B do Operations VLAN na S2.
- e. Usuń adres IP dla VLAN 1 na S2.
- f. Skonfiguruj adres IP dla sieci VLAN 99 na S2 zgodnie z tabelą adresowania.
- g. Użyj polecenia **show vlan brief**, aby sprawdzić, czy sieci VLAN są przypisane do odpowiednich interfejsów.

Czy ping z S1 osiągnie S2? Wyjaśnij.

Czy ping z PC-A osiągnie PC-B? Wyjaśnij.

## Część 3: Zarządzanie przypisywaniem portów do sieci VLAN i bazą sieci VLAN

W części 3 zmienisz przypisania VLAN do portów i usuniesz sieci VLAN z bazy danych VLAN.

#### Krok 1: Przypisz sieć VLAN do wielu interfejsów.

a. Na S1 przypisz interfejsy F0/11 - 24 do VLAN99.

```
S1(config) # interface range f0/11-24
```

```
S1(config-if-range)# switchport mode access
```

S1(config-if-range) # switchport access vlan 99

```
S1(config-if-range) # end
```

- b. Wydaj polecenie show vlan brief aby sprawdzić przypisanie sieci VLAN.
- c. Zmień przypisanie F0/11 i F0/21 do VLAN 10.
- d. Sprawdź, czy przypisania sieci VLAN są poprawne.

#### Krok 2: Usuń przypisanie sieci VLAN z interfejsu.

a. Użyj polecenia no switchport access vlan, aby usunąć przypisanie VLAN 99 z F0/24.

```
S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end
```

b. Sprawdź, czy została dokonana zmiana sieci VLAN.

Z którym VLAN jest teraz powiązany F0/24?

#### Krok 3: Usuń identyfikator sieci VLAN z bazy danych VLAN.

a. Dodaj VLAN 30 do interfejsu F0/24 bez wydawania globalnego polecenia VLAN.

```
S1(config)# interface f0/24
S1(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

**Uwaga**: Obecna technologia przełączników nie wymaga już wydawania polecenia **vlan** w celu dodania sieci VLAN do bazy danych. Przypisując nieznaną sieć VLAN do portu, sieć VLAN zostanie utworzona i dodana do bazy danych VLAN.

b. Sprawdź, czy nowa sieć VLAN jest wyświetlana w tabeli VLAN.

Jaka jest domyślna nazwa sieci VLAN 30?

c. Użyj polecenia no vlan 30, aby usunąć VLAN 30 z bazy danych VLAN.

```
S1(config)# no vlan 30
S1(config)# end
```

d. Wydaj polecenie show vlan brief. F0/24 został przypisany do VLAN 30.

Po usunięciu VLAN 30 z bazy danych VLAN, do jakiego VLAN jest przypisany port F0/24? Co dzieje się z ruchem przeznaczonym do hosta dołączonego do F0/24?

- e. Wydaj polecenie no switchport access vlan na interfejsie F0/24.
- f. Wydaj polecenie show vlan brief, aby określić przypisanie sieci VLAN dla F0/24.

Do której VLAN jest przypisany F0/24?

**Uwaga**: Przed usunięciem sieci VLAN z bazy danych zaleca się ponowne przypisanie wszystkich portów przypisanych do tej sieci VLAN.

Dlaczego warto przypisać port do innej sieci VLAN przed usunięciem sieci VLAN z bazy danych VLAN?

#### Część 4: Konfiguracja magistrali 802.1Q pomiędzy przełącznikami

W części 4 zostanie skonfigurowany interfejs F0/1 do korzystania z Dtnamic Trunking Protocol (DTP), aby umożliwić mu negocjowanie trybu trunk. Po wykonaniu tego i zweryfikowaniu, wyłączysz DTP na interfejsie F0/1 i ręcznie skonfigurujesz go jako łącze trunk.

#### Krok 1: Użyj DTP, aby zainicjować trunk na F0/1.

Trybem domyślnym na przełączniku 2960 jest tryb dynamic auto. Pozwala to interfejsowi na konwersję łącza na łącze trunk, jeśli sąsiedni interfejs jest ustawiony w trybie trunk lub desirable.

a. Ustaw F0/1 na S1, aby negocjować tryb trunk.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
Sep 19 02:51:47.257: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
Sep 19 02:51:47.291: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
```

Powinieneś również otrzymywać wiadomości o stanie łącza na S2.

```
S2#
Sep 19 02:42:19.424: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Sep 19 02:42:21.454: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
Sep 19 02:42:22.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

- b. Wydaj polecenie **show vlan brief** na S1 i S2. Interfejs F0/1 nie jest już przypisany do sieci VLAN 1. Interfejsy trunk nie są wymienione w tabeli sieci VLAN.
- c. Wydaj polecenie **show interfaces trunk**, aby wyświetlić interfejsy trunk. Zauważ, że tryb na S1 jest ustawiony na desirable, a tryb na S2 jest ustawiony na auto.

S1# show interfaces trunk

#### S2# show interfaces trunk

**Uwaga**: Domyślnie wszystkie sieci VLAN są dozwolone przez łącze trunk. Polecenie **switchport trunk** pozwala kontrolować, które sieci VLAN mają dostęp do łącza trunk. W tym laboratorium zachowaj domyślne ustawienia, które umożliwiają przechodzenie wszystkiem sieciom VLAN przez F0/1.

d. Sprawdź, czy ruch VLAN przechodzi przez interfejs trunk F0/1.

Czy ping z S1 osiągną S2?

Czy ping z PC-A osiągną PC-B?

Czy ping z PC-A osiągną S1?

Czy ping z PC-B osiągną S2?

Jeśli odpowiedziałeś "nie" na którekolwiek z powyższych pytań, wyjaśnij poniżej.

#### Krok 2: Ręcznie skonfiguruj interfejs trunk F0/1.

Polecenie **switchport mode trunk** służy do ręcznego konfigurowania portu jako łącza trunk. To polecenie powinno być wydane na obu końcach łącza.

a. Zmień tryb przełączania na interfejsie F0/1, aby wymusić trunking. Pamiętaj, aby to zrobić na obu przełącznikach.

S1(config)# interface f0/1
S1(config-if)# switchport mode trunk

b. Wydaj polecenie **show interfaces trunk**, aby wyświetlić tryby trunk. Zauważ, że tryb zmienił się z **desirable** na **on**.

S2# show interfaces trunk

c. Modyfikuj konfigurację trunk na obu przełącznikach, zmieniając natywną sieć VLAN z VLAN 1 na VLAN 1000.

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 1000
```

d. Wydaj polecenie show interfaces trunk, aby wyświetlić trunk. Zwróć uwagę, że informacje o natywnej sieci VLAN zostały zaktualizowane.

S2# show interfaces trunk

Dlaczego chcesz ręcznie skonfigurować interfejs do trybu trunk zamiast używać DTP?

Dlaczego chcesz zmienić natywną sieć VLAN na bagażniku?

# Część 5: Usunięcie bazy sieci VLAN

W części 5 usuniesz bazę danych VLAN z przełącznika. Należy to zrobić podczas inicjowania przełącznika aby powrócić do ustawień domyślnych.

#### Krok 1: Określ, czy baza danych sieci VLAN istnieje.

Wydaj polecenie show flash, aby określić, czy plik vlan.dat istnieje w pamięci flash.

S1# show flash:

**Uwaga**: Jeśli w pamięci flash znajduje się plik **vlan.dat**, oznacza to, że baza danych VLAN nie zawiera domyślnych ustawień.

#### Krok 2: Usuń bazę danych VLAN.

a. Wydaj polecenie **delete vlan.dat**, aby usunąć plik vlan.dat z pamięci flash i zresetować bazę danych VLAN z powrotem do ustawień domyślnych. Zostaniesz dwukrotnie poproszony o potwierdzenie, że chcesz usunąć plik vlan.dat. Naciśnij klawisz Enter dwukrotnie.

S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]

b. Wydaj polecenie show flash, aby sprawdzić, czy plik vlan.dat został usunięty.

S1# show flash:

Aby zainicjować przełącznik z powrotem do ustawień domyślnych, jakie inne polecenia są potrzebne?

# Pytania refleksyjne

- 1. Co jest potrzebne, aby umożliwić hostom w VLAN 10 komunikowanie się z hostami w sieci VLAN 99?
- 2. Jakie są podstawowe korzyści, które organizacja może otrzymać poprzez efektywne wykorzystanie sieci VLAN?