

Ćwiczenie – Konfiguracja VLAN i łącza trunk

Topologia

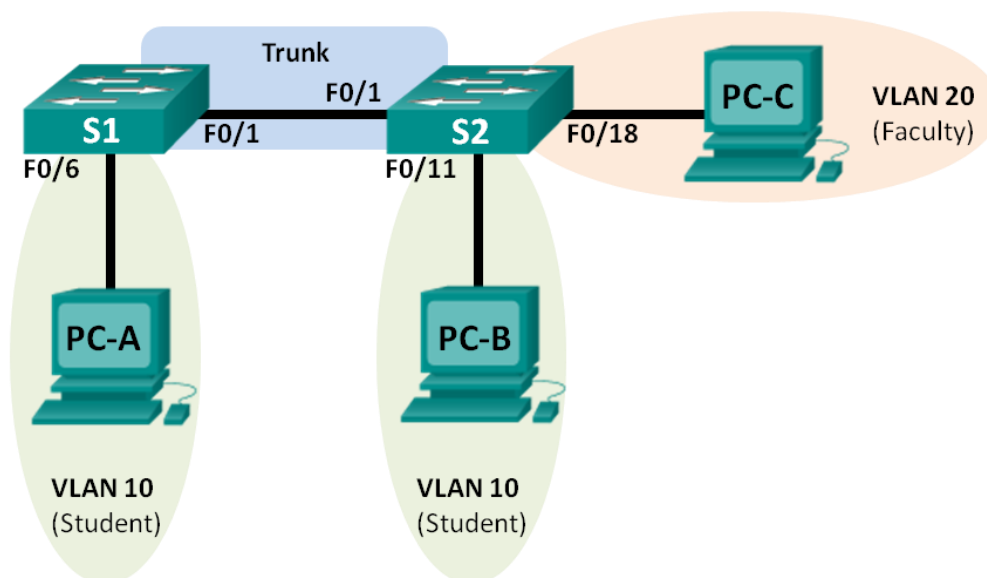


Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Cele

Część 1: Budowa sieci i konfiguracja podstawowych ustawień urządzenia.

Część 2: Tworzenie VLAN a przypisanie do nich interfejsów przełącznika.

Część 3: Obsługa przypisanych portów VLAN oraz bazy danych VLAN.

Część 4: Konfiguracja połączeń trunk 802.1Q pomiędzy przełącznikami.

Część 5: Kasowanie bazy danych VLAN.

Scenariusz

Nowoczesne przełączniki używają wirtualnych sieci lokalnych (VLAN) do poprawy wydajności sieci poprzez podział dużych obszarów rozgłoszeniowych warstwy drugiej na mniejsze. Sieci wirtualne (VLAN) mogą być również używane jako środek bezpieczeństwa do kontrolowania, który z hostów jest dopuszczony do komunikacji. Na ogół zastosowanie sieci VLAN ułatwia projektowanie sieci zgodnie z celami organizacji.

Łącza VLAN trunk wykorzystywane są do rozciągnięcia sieci VLAN przez wiele urządzeń. Umożliwiają one przesyłanie informacji pochodzących z wielu sieci VLAN poprzez pojedyncze łącze, utrzymując przy tym identyfikację danych z właściwą siecią VLAN.

Podczas laboratorium należy utworzyć sieci VLAN na obu urządzeniach zgodnie z topologią, przypisać porty do odpowiednich sieci VLAN oraz przeprowadzić weryfikację, czy VLAN działa zgodnie z oczekiwaniami. Następnie należy utworzyć łącze typu trunk pomiędzy dwoma przełącznikami, aby umożliwić hostom w tej samej sieci VLAN komunikowanie się za pośrednictwem łącza, bez względu na to, do którego urządzenia będą przypięte hosty.

Uwaga: Przełączniki użyte w instrukcji to Cisco Catalyst 2960s z obrazem systemu operacyjnego Cisco IOS Release 15.0(2) (lanbasek9). Do realizacji ćwiczenia mogą być użyte inne przełączniki lub wersje systemu IOS. W zależności od użytego modelu urządzenia oraz wersji IOS dostępne komendy oraz komunikaty na ekranie mogą się różnić od tych zamieszczonych w instrukcji.

Uwaga: Upewnij się, że przełączniki nie są skonfigurowane oraz nie przechowują pliku z konfiguracją startową. Jeśli nie jesteś tego pewien, skontaktuj się z instruktorem.

Wymagane zasoby:

- 2 przełączniki (Cisco 2960 z obrazem system Cisco IOS Release 15.0(2) lanbasek9 lub porównywalnym)
- 3 komputery PC (Windows 7, Vista, lub XP z zainstalowanym emulatorem terminala)
- kabel konsolowy do konfiguracji urządzeń CISCO poprzez port konsolowy
- kable ethernetowe, jak pokazano na rysunku topologii sieci.

Część 1: Budowa sieci i konfiguracja podstawowych ustawień urządzeń.

W części pierwszej należy zestawić sieć zgodnie z topologią i skonfigurować podstawowe ustawienia na komputerach PC oraz przełącznikach.

Krok 1: Połącz okablowanie zgodnie z topologią sieci.

Połącz urządzenia zgodnie z rysunkiem topologii sieci.

Krok 2: Zainicjuj przełączniki i przeładuj je, jeśli to konieczne.

Krok 3: Skonfiguruj podstawowe ustawienia na każdym przełączniku.

- Wyłącz automatyczne zapytania DNS (DNS lookup).
- Skonfiguruj nazwę urządzenia, jak to pokazano na schemacie.
- Przypisz **class** jako hasło do trybu uprzywilejowanego EXEC.
- Przypisz **cisco** jako hasło konsoli i VTY oraz włącz logowanie do konsoli i VTY.
- Skonfiguruj **logging synchronous** dla wejścia konsolowego.
- Skonfiguruj baner MOTD, aby ostrzegał użytkowników, że nieautoryzowany dostęp jest zabroniony.
- Skonfiguruj adresy IP wyszczególnione w tabeli adresacji dla VLAN 1 na obu przełącznikach.
- Administracyjnie zablokuj wszystkie nieużywane porty na przełączniku.
- Skopiuj konfigurację bieżącą do konfiguracji startowej.

Krok 4: Konfiguracja komputerów PC.

Dane do konfiguracji hostów są zamieszczone w tabeli adresacji.

Krok 5: Sprawdzanie połączeń.

Sprawdź, czy wszystkie komputery PC odpowiadają na polecenie ping z każdego komputera.

Uwaga: Może być konieczne wyłączenie ściany ogniowej (firewall) w celu przeprowadzenia pingowania pomiędzy komputerami PC.

Czy ping z PC-A do PC-B zakończył się sukcesem? _____

Czy ping z PC-A do PC-C zakończył się sukcesem? _____

Czy ping z PC-A do S1 zakończył się sukcesem? _____

Czy ping z PC-B do PC-C zakończył się sukcesem? _____

Czy ping z PC-B do S2 zakończył się sukcesem? _____

Czy ping z PC-C do S2 zakończył się sukcesem? _____

Czy ping z S1 do S2 zakończył się sukcesem? _____

Jeśli którakolwiek odpowiedź brzmi „nie”, napisz, dlaczego pingi się nie powiodły.

Część 2: Tworzenie sieci VLAN i przypisywanie do nich portów.

W części drugiej należy utworzyć na obu przełącznikach trzy sieci VLAN: „student”, „faculty” i „management”. Następnie trzeba odpowiednie interfejsy przypisać do odpowiednich sieci VLAN. Do weryfikacji konfiguracji sieci VLAN należy użyć komendy **show vlan**.

Krok 1: Utwórz sieci VLAN na przełączniku.

- a. Utwórz sieci VLAN na przełączniku S1.

```
S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# end
```

- b. Utwórz te same sieci VLAN na przełączniku S2.

- c. Wyдай komendę **show vlan**, aby wyświetlić listę sieci VLAN na przełączniku S1.

```
S1# 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 Gi0/1, Gi0/2
10	Student	active	
20	Faculty	active	
99	Management	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
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
99	enet	100099	1500	-	-	-	-	-	0	0

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
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

Jaki jest domyślny VLAN? _____

Jakie porty są dołączone do domyślnej sieci VLAN?

Krok 2: Przypisanie sieci VLAN do odpowiednich interfejsów przełącznika.

a. Przypisz sieci VLAN do interfejsów przełącznika S1.

1) Przypisz PC-A do sieci VLAN Student.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

2) Przenieś 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. Wyдай komendę **show vlan brief** i zweryfikuj, czy sieci VLAN są przyłączone do prawidłowych interfejsów.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, 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	Student	active	Fa0/6
20	Faculty	active	
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

c. Wydadz komendę **show ip interfaces brief**.

Jaki jest status VLAN 99? Dlaczego?

d. Wykorzystaj topologię sieci w celu podłączenia sieci VLAN do właściwych interfejsów przełącznika S2.

e. Usuń adres IP przełącznika S2 z VLAN 1.

f. Skonfiguruj adres IP dla VLAN 99 na przełączniku S2 zgodnie z tabelą adresacji.

g. Użyj komendy **show vlan brief** do sprawdzenia, czy sieci VLAN są przyłączone do prawidłowych interfejsów.

S2# **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, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
10	Student	active	Fa0/11
20	Faculty	active	Fa0/18
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Czy ping z PC-A do PC-B zakończył się sukcesem? Dlaczego?

Czy ping z S1 do S2 zakończył się sukcesem? Dlaczego?

Część 3: Zachowanie konfiguracji portów w sieci VLAN i bazy danych sieci VLAN.

W części trzeciej należy zmienić przypisanie VLAN do portów i usunąć sieci VLAN z bazy danych VLAN.

Krok 1: Przypisz VLAN do wielu interfejsów.

a. Na przełączniku S1 przypisz interfejsy F0/11 – 24 do VLAN 10.

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

```
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# end
```

- b. Wydadź komendę **show vlan brief** w celu weryfikacji przypisanych sieci VLAN.
- c. Ponownie przypisz interfejsy od F0/11 do F0/21 do VLAN 20.
- d. Sprawdź, czy sieci VLAN są prawidłowo przypisane.

Krok 2: Usuń przyporządkowanie sieci VLAN z interfejsu.

- a. Użyj komendy **no switchport access vlan** w celu usunięcia interfejsu F0/24 z VLAN 10.

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

- b. Sprawdź, czy nastąpiła zmiana przyporządkowaniu do sieci VLAN.

Do którego VLAN przyporządkowany jest teraz interfejs F0/24?

Krok 3: Usuń numer identyfikacyjny (ID) VLAN z bazy danych.

- a. Dodaj interfejs F0/24 do VLAN 30 bez wydawania komend konfiguracyjnych sieci VLAN.

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

Uwaga: Obecna technologia nie wymaga na przełącznikach wydania komendy **vlan** w celu dodania VLAN do bazy danych. Przypisując interfejs do nieznanej sieci VLAN, VLAN jest automatycznie tworzony i dodawany do bazy danych VLAN.

- b. Sprawdź, czy nowy VLAN jest wyświetlany w tabeli VLAN.

```
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, Gi0/1, Gi0/2
10	Student	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
30	VLAN0030	active	Fa0/24
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Jaka jest domyślna nazwa sieci VLAN 30? _____

- c. Aby usunąć VLAN 30 z bazy danych VLAN, użyj komendy **no vlan 30**.

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

- d. Wydadź komendę **show vlan brief**.

F0/24 był przypisany do sieci VLAN 30.

Do czego przypisany jest interfejs F0/24 po skasowaniu LAN 30?

Co się stało z ruchem kierowanym do hosta przypiętego do interfejsu F0/24?

```
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, Gi0/1, Gi0/2
10	Student	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

e. Wydadz komendę **no switchport access vlan** na interfejsie F0/24.

f. Wydadz komendę **show vlan brief** w celu określenia, do jakiej sieci VLAN przyporządkowany jest interfejs F0/24.

Do jakiej sieci VLAN przyporządkowany jest interfejs F0/24?

Uwaga: Przed usunięciem VLAN z bazy danych jest wskazane przeniesienie wszystkich interfejsów z usuwanego VLAN do innego.

Dlaczego należy ponownie przyporządkować interfejs do innego VLAN przed usunięciem VLAN z bazy danych?

Część 4: Konfiguracja 802.1Q trunk pomiędzy przełącznikami.

W części czwartej należy skonfigurować interfejs F0/1 do pracy z protokołem DTP (Dynamic Trunking Protocol), aby przełącznik mógł automatycznie negocjować tryb połączenia trunk na tym interfejsie. Po wykonaniu i zweryfikowaniu działania trybu DTP należy wyłączyć tryb DTP na interfejsie F0/1 i ręcznie skonfigurować na nim łącze typu trunk.

Krok 1: Użyj DTP do inicjalizacji łącza typu trunk na interfejsie F0/1.

W przełącznikach serii 2960 interfejsy mają domyślnie włączony tryb DTP. Umożliwi to automatyczne przekształcenie łącza na interfejsie w tryb trunk, jeśli tylko na interfejsie przełącznika po drugiej stronie łącza ustawiony będzie tryb trunk lub DTP auto.

a. Ustaw interfejs F0/1 na przełączniku S1 w tryb DTP.

```
S1(config)# interface f0/1
```

```
S1(config-if)# switchport mode dynamic desirable
```

```
*Mar 1 05:07:28.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,  
changed state to down
```

```
*Mar 1 05:07:29.744: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
S1(config-if)#
*Mar 1 05:07:32.772: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
S1(config-if)#
*Mar 1 05:08:01.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99,
changed state to up
*Mar 1 05:08:01.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to up
```

Również na przełączniku S2 powinien pojawić się komunikat o zmianie statusu łącza.

```
S2#
*Mar 1 05:07:29.794: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
S2#
*Mar 1 05:07:32.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
S2#
*Mar 1 05:08:01.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99,
changed state to up
*Mar 1 05:08:01.850: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to up
```

- b. Wyдай komendę **show vlan brief** na przełączniku S1 i S2. Interfejs F0/1 już nie jest przypisany do VLAN 1. Interfejsy w trybie trunk nie są od tego momentu wyświetlane w tabeli VLAN.

S1# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/24, Gi0/1, Gi0/2
10	Student	active	Fa0/6, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

- c. Wyдай komendę **show interfaces trunk**, aby wyświetlić interfejsy w trybie trunk. Zauważ, że na przełączniku S1 interfejs jest w trybie desirable, podczas gdy na przełączniku S2 w trybie auto.

S1# **show interfaces trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	desirable	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,99

```
Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1         1,10,20,99
```

```
S2# show interfaces trunk
```

```
Port          Mode          Encapsulation  Status        Native vlan
Fa0/1         auto          802.1q         trunking      1
```

```
Port          Vlans allowed on trunk
Fa0/1         1-4094
```

```
Port          Vlans allowed and active in management domain
Fa0/1         1,10,20,99
```

```
Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1         1,10,20,99
```

Uwaga: Domyślnie wszystkie sieci VLAN są przenoszone przez łącze typu trunk. Polecenie **switchport trunk** umożliwia ustawienie, które VLAN będą przenoszone przez łącze typu trunk. W tym ćwiczeniu zachowaj ustawienia domyślne, które umożliwiają przenoszenie wszystkich sieci VLAN przez F0/1.

- d. Upewnij się, że ruch na VLAN kierowany jest przez interfejs F0/1 z statusem trunking.

Czy ping z PC-A do PC-B zakończył się sukcesem? _____

Czy ping z PC-A do PC-C zakończył się sukcesem? _____

Czy ping z PC-A do S1 zakończył się sukcesem? _____

Czy ping z PC-B do PC-C zakończył się sukcesem? _____

Czy ping z PC-B do S2 zakończył się sukcesem? _____

Czy ping z PC-C do S2 zakończył się sukcesem? _____

Jeśli którakolwiek odpowiedź brzmi „nie”, wyjaśnij, dlaczego.

Krok 2: Ręcznie skonfiguruj łącze typu trunk na interfejsie F0/1.

Polecenie **switchport mode trunk** służy do ręcznej konfiguracji interfejsu jako łącza typu trunk. Komenda powinna być wydana na obu przełącznikach współdzielących łącze typu trunk.

- a. Zmień typ interfejsu F0/1 z przełączającego na trunk. Wykonaj operację na obu przełącznikach.

```
S1(config)# interface f0/1
```

```
S1(config-if)# switchport mode trunk
```

- b. Wydadz komendę **show interfaces trunk**, aby wyświetlić status interfejsów w trybie trunk. Zauważ, że tryb zmienił się z **desirable** na **on**.

```
S2# show interfaces trunk
```

```
Port          Mode          Encapsulation  Status        Native vlan
Fa0/1         on            802.1q         trunking      99
```

```
Port          Vlans allowed on trunk
Fa0/1         1-4094
```

```
Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,99
```

```
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,20,99
```

Dlaczego warto ręcznie skonfigurować interfejs w trybie trunk zamiast za pomocą DTP?

Część 5: Kasowanie bazy danych VLAN.

W części piątej należy skasować bazę danych VLAN na przełączniku. Jest to konieczna czynność przed przywróceniem na przełączniku ustawień domyślnych.

Krok 1: Ustalanie, czy baza danych VLAN istnieje na przełączniku.

Wydadź polecenie **show flash**, aby określić, czy na przełączniku istnieje plik **vlan.dat**.

```
S1# show flash
```

```
Directory of flash:/
```

```
 2  -rwx      1285   Mar 1 1993 00:01:24 +00:00  config.text
 3  -rwx     43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
 4  -rwx         5   Mar 1 1993 00:01:24 +00:00  private-config.text
 5  -rwx    11607161  Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-
2.SE.bin
 6  -rwx       736   Mar 1 1993 00:19:41 +00:00  vlan.dat
```

```
32514048 bytes total (20858880 bytes free)
```

Uwaga: Jeśli na przełączniku w pamięci flash istnieje plik: **vlan.dat**, to na pewno nie zawiera on wartości domyślnych.

Krok 2: Kasowanie bazy danych VLAN.

- a. Wydadź polecenie **delete vlan.dat**, aby skasować plik **vlan.dat** z pamięci flash przełącznika i zresetuj bazę danych VLAN do ustawień domyślnych. Przełącznik będzie dwa razy monitował o potwierdzenie, że plik **vlan.dat** ma być skasowany. Należy potwierdzić oba monity naciśnięciem klawisza ENTER.

```
S1# delete vlan.dat
```

```
Delete filename [vlan.dat]?
```

```
Delete flash:/vlan.dat? [confirm]
```

```
S1#
```

- b. Wydadź polecenie **show flash** aby zweryfikować usunięcie pliku **vlan.dat**.

```
S1# show flash
```

```
Directory of flash:/
```

```
 2  -rwx      1285   Mar 1 1993 00:01:24 +00:00  config.text
 3  -rwx     43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
 4  -rwx         5   Mar 1 1993 00:01:24 +00:00  private-config.text
 5  -rwx    11607161  Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-
2.SE.bin
```

32514048 bytes total (20859904 bytes free)

Jakie komendy należy jeszcze wydać, aby zainicjować przełącznik z jego ustawieniami fabrycznymi?

Do przemyślenia:

1. Co jest potrzebne, aby umożliwić komunikację pomiędzy hostami z VLAN 10 z hostami należącymi do VLAN 20?

2. Jakie są główne korzyści, które organizacja może uzyskać w wyniku efektywnego wykorzystania sieci VLAN?
