

Laboratorium - Podstawowa konfiguracja przełącznika

Topologia sieci



Tabela adresowania

Urządzenie	Interfejs	Adres IP/prefiks
S1	VLAN 99	192.168.1.2 /24
		2001:db8:acad::2 /64
		fe80::2
PC-A	karta sieciowa	192.168.1.10 /24
		2001:db8:acad:3 /64
		fe80::3

Zadania

Część 1: Okablowanie sieciowe i weryfikacja domyślnej konfiguracji przełącznika.

Część 2: Konfiguracja podstawowych ustawień urządzeń sieciowych.

- Skonfiguruj podstawowe ustawienia przełącznika.
- Skonfiguruj hosty PC używając odpowiedniej adresacji IP.

Część 3: Weryfikacja i test połączeń sieciowych

- Wyświetl konfigurację urządzenia.
- Użyj polecenia ping do sprawdzenia połączenia punkt-punkt.
- Przetestuj możliwość zdalnego zarządzania za pomocą usługi Telnet.

Część 4: Zarządzanie tabelą adresów MAC

- Zapisz adresy MAC hostów.
- Określ adresy MAC uzyskane przez przełącznik.
- Wyświetl opcje polecenia show mac adress-table.
- Skonfiguruj statyczny adres MAC.

Wprowadzenie

Przełączniki Cisco mogą być skonfigurowane za pomocą specjalnego adresu IP znanego jako wirtualny interfejs przełącznika (SVI). SVI, czyli interfejs zarządzania, może służyć do zdalnego dostępu do przełącznika w celu wyświetlenia lub skonfigurowania ustawień. Jeśli VLAN 1 SVI ma przypisany adres IP, domyślnie wszystkie porty w sieci VLAN 1 mają dostęp do adresu IP SVI.

W tym laboratorium będziesz tworzyć prostą topologię z wykorzystaniem okablowania Ethernet LAN oraz uzyskasz dostęp do przełącznika Cisco przy użyciu konsoli i dostępu zdalnego. Przed skonfigurowaniem podstawowych ustawień przełącznika należy sprawdzić domyślne konfiguracje przełączników. Te podstawowe ustawienia przełączników obejmują nazwę urządzenia, opis interfejsu, lokalne hasła, baner wiadomości dnia (MOTD), adresowanie IP i statyczny adres MAC. Zademonstrujesz również użycie adresu IP zarządzania do zdalnego zarządzania przełącznikiem. Topologia składa się z jednego przełącznika i jednego hosta używających tylko portów Ethernet oraz konsoli.

Uwaga: W laboratorium zastosowano przełączniki Cisco Catalyst 2960 z systemem Cisco IOS wersji 15.2(2) (obraz lanbasek9). Można również używać innych przełączników i wersji systemu IOS. Zależnie od modelu urządzenia i wersji systemu IOS, dostępne polecenia i wyniki ich działania mogą się różnić od prezentowanych w niniejszej instrukcji.

Uwaga: Upewnij się, że konfiguracje przełączników zostały zresetowane oraz nie mają konfiguracji startowych. Jeśli nie jesteś pewien, to poproś o pomoc instruktora. W załączniku A znajdują się procedury inicjalizacji i restartu przełącznika.

Domyślny, wbudowany szablon używany przez Switch Database Manager (SDM) nie zapewnia możliwości adresowania IPv6. Upewnij się że SDM wykorzystuje szablon **dual-ipv4-and-ipv6** lub **lanbase-routing**. Nowy szablon będzie użyty po restarcie urządzenia nawet jeśli konfiguracja nie zostanie zapisana.

S1# show sdm prefer

Użyj następujących poleceń, aby przypisać szablon dual-ipv4-i-ipv6 jako domyślny szablon SDM.

```
S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

Wymagane zasoby

- 1 przełącznik (Cisco 2960 z systemem Cisco IOS wersja15.2 (2) obraz lanbasek9 lub porównywalny)
- 1 komputer PC (Windows z emulatorem terminala takim jak Tera Term)
- 1 kabel konsolowy do konfiguracji urządzeń Cisco przez port konsoli
- 1 kabel Ethernet pokazany jest na rysunku topologii

Część 1: Okablowanie sieciowe i weryfikacja domyślnej konfiguracji przełącznika

W części 1 uczestnicy kursu zbudują topologię sieci i skonfigurują podstawowe ustawienia na przełącznikach.

Krok 1: Zbuduj sieć zgodnie z topologią.

- a. Podłącz kabel konsoli, jak pokazano w topologii. W tej chwili nie podłączaj kabla Ethernet PC-A.
 Uwaga: Jeśli korzystasz z Netlab, zamknij F0/6 na S1. Ma to taki sam efekt, jak brak podłączania PC-A do S1.
- b. Podłącz się do przełącznika z PC-A za pomocą Tera Term lub innego programu emulacji terminala.

Dlaczego musisz używać połączenia konsoli, aby wstępnie skonfigurować przełącznik? Dlaczego nie można połączyć z przełącznikiem za pomocą Telnet lub SSH?

Krok 2: Sprawdź domyślną konfigurację przełącznika.

W tym kroku zbadasz domyślne ustawienia przełącznika, takie jak bieżąca konfiguracja przełącznika, informacje IOS, właściwości interfejsu, informacje o sieci VLAN i pamięć flash.

W uprzywilejowanym trybie EXEC, możesz uzyskać dostęp do wszystkich poleceń IOS przełącznika. Dostęp do uprzywilejowanego trybu EXEC powinien być ograniczony przez ochronę hasłem, aby zapobiec nieautoryzowanemu użyciu, ponieważ zapewnia bezpośredni dostęp do globalnego trybu konfiguracji i poleceń używanych do konfigurowania parametrów operacyjnych. Hasła ustawisz później w tym laboratorium.

W zestawie poleceń trybu użytkownika uprzywilejowanego dostępne jest między innymi polecenie **configure** umożliwiające uzyskanie dostępu do pozostałych trybów poleceń. Aby przejść do uprzywilejowanego trybu EXEC, użyj polecenia **enable**.

a. Zakładając, że przełącznik nie ma pliku konfiguracyjnego przechowywanego w nieulotnej pamięci NVRAM, połączenie konsoli za pomocą Tera Term lub innego programu emulującego terminal spowoduje wyświetlenie znaku zachęty trybu EXEC użytkownika na przełączniku w postaci Switch>. Aby przejść do uprzywilejowanego trybu EXEC, użyj polecenia **enable**.

Należy zwrócić uwagę na zmianę symbolu zachęty odzwierciedlającą przejście do uprzywilejowanego trybu EXEC.

Sprawdź, czy na przełączniku znajduje się czysty, domyślny plik konfiguracyjny, wydając polecenie **show running-config** uprzywilejowanego trybu EXEC. Jeśli plik konfiguracyjny został uprzednio zapisany, musi zostać usunięty. W zależności od modelu przełącznika i wersji IOS, zawartość pliku konfiguracyjnego może trochę się różnić. Zwróć uwagę na to, żeby w konfiguracji routera, którego używasz, nie było zapisanych haseł ani adresu IP. Jeśli przełącznik nie ma domyślnej konfiguracji, usuń i ponownie załaduj przełącznik.

Uwaga: Załącznik A szczegółowo opisuje kroki, aby zainicjować i przeładować przełącznik.

b. Zbadaj bieżący plik konfiguracyjny.

Ile interfejsów FastEthernet ma przełącznik 2960?

Ile interfejsów Gigabit Ethernet posiada przełącznik 2960?

Jaki jest zakres wartości linii vty?

c. Sprawdź plik konfiguracji startowej w NVRAM.

Dlaczego pojawia się ten komunikat?

d. Zbadaj właściwości SVI dla VLAN 1.

Czy istnieje adres IP przypisany do sieci VLAN 1?

Jaki jest adres MAC tego SVI? Odpowiedzi mogą być różne.

Czy interfejs ten jest aktywny (up)?

e. Sprawdź właściwości IP dla SVI VLAN 1.

Co widzisz po użyciu tej komendy?

f. Podłącz kabel Ethernet z PC-A do portu 6 na przełączniku i sprawdź właściwości IP dla SVI VLAN 1. Poczekaj, aż przełącznik i komputer PC wynegocjują parametry dupleksu i szybkości.

Uwaga: Jeśli używasz Netlab, włącz interfejs F0/6 na S1.

Co widzisz po użyciu tej komendy?

g. Zbadaj informacje o wersji Cisco IOS przełącznika.

Jaka wersja systemu Cisco IOS jest wykorzystywana w przełączniku?

Jaka jest nazwa pliku obrazu systemu?

Jaki jest podstawowy adres MAC przełącznika?

 h. Sprawdź domyślne właściwości interfejsu FastEthernet używanego przez PC-A. Switch# show interface f0/6
 Czy interfejs jest włączony, czy wyłączony?

Jakie zdarzenie mogłoby spowodować włączenie interfejsu?

Jaki jest adres MAC interfejsu?

Jakie są ustawienia dotyczące szybkości i trybu dupleksu na interfejsie?

Sprawdź domyślne ustawienia sieci VLAN przełącznika.
 Jaka jest nazwa sieci VLAN 1?

Które porty znajdują się w sieci VLAN 1?

Czy sieć VLAN 1 jest aktywna?

Jaki jest typ domyślnej sieci VLAN?

j. Sprawdź zawartość pamięci flash.

Użyj jednego następującego polecenia, aby zbadać zawartość katalogu pamięci flash:

Switch# show flash

Switch# dir flash:

Pliki posiadają rozszerzenia takie jak np. .bin, na końcu nazwy. Wyświetlane katalogi nie posiadają rozszerzeń.

Jaka jest nazwa pliku obrazu Cisco IOS?

Część 2: Konfiguracja podstawowych ustawień urządzeń sieciowych

W części 2 skonfigurujesz podstawowe ustawienia przełącznika i komputera.

Krok 1: Skonfiguruj podstawowe ustawienia przełącznika.

a. Skopiuj następującą podstawową konfigurację i wklej go do S1 w trybie konfiguracji globalnej.

```
no ip domain-lookup
hostname S1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
```

b. Ustaw adres IP na SVI przełącznika. Umożliwia to zdalne zarządzanie przełącznikiem.

Zanim będziesz mógł zdalnie zarządzać S1 z PC-A, musisz przypisać przełącznikowi adres IP. Domyślnie przełącznik jest skonfigurowany tak, aby zarządzanie nim odbywało się za pośrednictwem sieci VLAN 1. Jednak zgodnie z najlepszymi praktykami w zakresie podstawowej konfiguracji przełącznika zaleca się zmienić sieć VLAN zarządzania na inną niż VLAN 1.

Do celów zarządzania użyj VLAN 99. Wybór VLAN 99 jest arbitralny i w żaden sposób nie oznacza, że zawsze powinieneś używać VLAN 99.

Najpierw utwórz nową VLAN 99 na przełączniku. Następnie nadaj adres IP przełącznika 192.168.1.2 z maską podsieci 255.255.255.0 na wewnętrznym wirtualnym interfejsie VLAN 99. Można również skonfigurować na interfejsie SVI adres IPv6. Użyj adresów IPv6 wymienionych w tabeli adresacji.

Zauważ, że interfejs VLAN 99 jest w stanie wyłączonym, mimo że wprowadzono polecenie **no shutdown**. Interfejs jest obecnie wyłączony, ponieważ żadne porty przełączników nie są przypisane do sieci VLAN 99.

c. Przypisz wszystkie porty użytkownika do sieci VLAN 99.

Aby ustanowić łączność między hostem a przełącznikiem, porty używane przez hosta muszą znajdować się w tej samej sieci VLAN, co przełącznik. Zauważ w powyższym wyjściu, że interfejs VLAN 1 zmienił stan na down, ponieważ żaden z portów nie jest przypisany do VLAN 1. Po kilku sekundach VLAN 99 zmienia stan na up, ponieważ co najmniej jeden aktywny port (F0/6 z podłączonym PC-A) jest teraz przypisany do VLAN 99.

d. Wydaj polecenie show vlan brief, aby sprawdzić, czy wszystkie porty są w sieci VLAN 99.

- e. Skonfiguruj bramę domyślną dla S1. Jeśli nie jest ustawiona brama domyślna, przełącznik nie może być zarządzany z sieci zdalnej, która znajduje się w odległości więcej niż jednego routera. Chociaż to laboratorium nie obejmuje zewnętrznej bramy IP, załóżmy, że w końcu połączysz sieć LAN z routerem w celu uzyskania dostępu zewnętrznego. Zakładając, że interfejs routera ma adres IP 192.168.1.1, ustaw go jako bramę na przełączniku.
- f. Dostęp do portu konsoli powinien być również ograniczony hasłem. Użyj cisco jako hasła logowania konsoli w tym laboratorium. Domyślna konfiguracja pozwala na dostęp poprzez wszystkie połączenia konsoli bez hasła. Aby zapobiec przerywaniu poleceń przez komunikaty konsoli, użyj opcji logging synchronous.

```
S1(config)# line con 0
```

```
S1(config-line) # logging synchronous
```

g. Skonfiguruj terminal wirtualny (VTY) w przełączniku, tak aby umożliwić dostęp do niego poprzez Telnet. Jeśli nie skonfigurujesz hasła dla VTY, to nie będziesz mógł używać usługi Telnet aby mieć dostęp do przełącznika.

Dlaczego wymagana jest komenda login?

Krok 2: Skonfiguruj adres IP na komputerze PC-A.

Przypisz adres IP i maskę podsieci do komputera PC zgodnie z Tabelą adresacji. Skrócona wersja procedury jest opisana tutaj. Domyślna brama nie jest wymagana dla tej topologii; można jednak wprowadzić **192.168.1.1** i **fe80::1**, aby symulować router dołączony do S1.

- 1) Przejdź do okna Panel sterowania.
- 2) W widoku kategorii wybierz pozycję Wyświetl stan sieci i zadania.
- 3) Kliknij Zmień ustawienia adaptera w lewym okienku.
- 4) Kliknij prawym przyciskiem interfejs Ethernet i wybierz Właściwości.
- 5) Wybierz protokół internetowy w wersji 4 (TCP/IPv4) i kliknij Właściwości.
- 6) Kliknij przycisk opcji **Użyj następującego adresu IP** i wprowadź adres IP oraz maskę podsieci, a następnie kliknij przycisk **OK**.
- 7) Wybierz Protokół internetowy w wersji 6 (TCP/IPv6) i kliknij Właściwości.
- 8) Kliknij przycisk opcji **Użyj następującego adresu IPv6** i wprowadź adres IPv6 oraz prefiks, a następnie kliknij przycisk **OK**, aby kontynuować
- 9) Kliknij OK, aby zamknąć okno właściwości.

Część 3: Weryfikacja i testowanie komunikacji w sieci

W części 3 zweryfikujesz i udokumentujesz konfigurację przełącznika, przetestujesz łączność typu end-to-end między PC-A i S1 oraz przetestujesz możliwość zdalnego zarządzania przełącznikiem.

Krok 1: Wyświetl konfigurację przełącznika.

Użyj połączenia konsoli na PC-A, aby wyświetlić i zweryfikować konfigurację przełącznika. Użycie polecenia **show running-config** spowoduje wyświetlenie bieżącej konfiguracji z uwzględnieniem podziału na strony. Użyj spacji, aby przejść na kolejną stronę.

a. Tutaj pokazano przykładową konfigurację. Skonfigurowane ustawienia są podświetlone na żółto. Pozostałe ustawienia konfiguracyjne są domyślnymi ustawieniami systemu IOS.

```
S1# show run
Building configuration...
```

```
Current configuration : 2206 bytes
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
1
<mark>hostname S1</mark>
1
boot-start-marker
boot-end-marker
1
enable secret 5 $1$mtvC$6NC.1VKr3p6bj7YGE.jNg0
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
1
<output omitted>
1
interface FastEthernet0/24
switchport access vlan 99
!
interface GigabitEthernet0/1
switchport access vlan 99
!
interface GigabitEthernet0/2
switchport access vlan 99
1
interface Vlan1
no ip address
no ip route-cache
1
<mark>interface Vlan99</mark>
ip address 192.168.1.2 255.255.255.0
ipv6 address FE80::2 link-local
ipv6 address 2001:DB8:ACAD::2/64
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
```

```
password 7 00071A150754
logging synchronous
login
line vty 0 4
password 7 121A0C041104
login
line vty 5 15
password 7 121A0C041104
login
!
```

b. Sprawdź ustawienia VLAN 99 do zarządzania.

S1# show interface vlan 99

Jaka jest szerokość pasma tego interfejsu?

Jaki jest stan VLAN 99?

Jaki jest stan protokołu linii?

Krok 2: Użyj polecenia ping do sprawdzenia połączenia punkt-punkt.

- a. Z wiersza poleceń na PC-A, najpierw wyślij ping na adres PC-A.
 - C:\> ping 192.168.1.10
- b. Z wiersza poleceń na PC-A, wyślij ping na adres zarządzania SVI S1.

C:\> ping 192.168.1.2

Ponieważ PC-A musi odwzorować adres MAC od S1 używając ARP, pierwszy pakiet może przekroczyć limit czasu. Jeśli wyniki polecenia ping nadal kończą się niepowodzeniem, rozwiąż problemy z podstawową konfiguracją urządzeń. Sprawdź zarówno fizyczne okablowanie, jak i adresowanie logiczne.

Krok 3: Przetestuj i zweryfikuj zdalne zarządzanie S1.

Będziesz teraz używać Telnet, aby zdalnie uzyskać dostęp do przełącznika. W tym laboratorium PC-A i S1 znajdują się obok siebie. W sieci produkcyjnej przełącznik może znajdować się w szafie na najwyższym piętrze, podczas gdy komputer zarządzający znajduje się na parterze. W tym kroku, można użyć Telnet, aby zdalnie uzyskać dostęp do przełącznika S1 przy użyciu jego adresu zarządzania SVI. Telnet nie jest bezpiecznym protokołem; jednak użyjesz go do testowania zdalnego dostępu. Z Telnet wszystkie informacje, w tym hasła i polecenia, są wysyłane w sesji zwykłym tekstem. W kolejnych laboratoriach będziesz używać SSH do zdalnego dostępu do urządzeń sieciowych.

- a. Otwórz Tera Term lub inny program do emulacji terminala z funkcją Telnet.
- b. Wybierz serwer Telnet i podaj adres zarządzania SVI, aby połączyć się z S1. Hasło dostępu do routera to cisco.
- c. Po wprowadzeniu hasła **cisco**, pojawi się znak zachęty trybu użytkownika EXEC. Uzyskaj dostęp do uprzywilejowanego trybu EXEC za pomocą polecenia **enable** i podając tajne hasło **class**.
- d. Zapisz konfigurację.
- e. Wpisz polecenie exit, aby zakończyć sesję Telnet.

Część 4: Zarządzanie tablicą adresów MAC.

W części 4 określisz adresy MAC, których nauczył się przełącznik, ustawisz statyczny adres MAC na jednym z interfejsów przełącznika, a następnie usuniesz statyczny adres MAC z tego interfejsu.

Krok 1: Zapisz adresy MAC hostów.

Otwórz wiersz polecenia na PC-A i wyślij polecenie **ipconfig /all**, aby określić i zarejestrować adresy warstwy 2 (fizyczne) karty sieciowej.

Krok 2: Określ adresy MAC uzyskane przez przełącznik.

Wyświetl adresy MAC za pomocą komendy show mac-address-table.

S1# show mac address-table

Ile adresów dynamicznych zawiera tablica?

Ile łącznie adresów MAC zawiera tablica?

Czy dynamiczny adres MAC pasuje do adresu MAC PC-A?

Krok 3: Wyświetl opcje polecenia show mac adress-table.

a. Pokaż opcje polecenia show mac adress-table.

S1# show mac address-table ?

Ile opcji jest dostępnych dla polecenia show mac address-table?

b. Wydaj polecenie **show mac address-table dynamic**, aby wyświetlić tylko adresy MAC, które zostały zapamiętane dynamicznie.

S1# show mac address-table dynamic

Ile adresów dynamicznych zawiera tablica?

c. Wyświetl wpis adresu MAC dla PC-A. Formatowanie adresu MAC dla polecenia jest następujące xxxx.xxxx.xxxx.

S1# show mac address-table address <tutaj PC-A MAC>

Krok 4: Skonfiguruj statyczny adres MAC.

a. Wyczyść tablicę adresów MAC.

Aby usunąć istniejące adresy MAC, użyj polecenia **clear mac address-table dynamic** w uprzywilejowanym trybie EXEC.

S1# clear mac address-table dynamic

b. Sprawdź czy została wyczyszczona tablica adresów MAC.

S1# show mac address-table

Ile jest statycznych adresów MAC?

Ile adresów dynamicznych zawiera tablica?

c. Sprawdź ponownie tablicę adresów MAC.

Najprawdopodobniej aplikacja działająca na twoim komputerze wysłała już ramkę z karty sieciowej do S1. Spójrz ponownie na tablicę adresów MAC w uprzywilejowanym trybie EXEC, aby sprawdzić, czy S1 ponownie nauczył się adresu MAC komputera PC-A.

S1# show mac address-table

Ile adresów dynamicznych zawiera tablica?

Dlaczego wyświetlone dane różnią się od danych wyświetlonych uprzednio?

Jeśli S1 jeszcze nie nauczył się ponownie adresu MAC dla PC-A, wykonaj polecenie ping na adres IP VLAN 99 przełącznika z komputera PC-A, a następnie powtórz polecenie **show mac address-table**.

d. Skonfiguruj statyczny adres MAC.

Aby określić, z którymi portami host może się łączyć, jedną z opcji jest utworzenie statycznego mapowania adresu MAC hosta na port.

Skonfiguruj statyczny adres MAC na F0/6 przy użyciu adresu zarejestrowanego dla PC-A w części 4, krok 1. Adres MAC 0050.56BE.6C89 jest używany tylko jako przykład. Należy użyć adresu MAC PC-A, który jest inny niż podany tutaj jako przykład.

S1(config)# mac address-table static 0050.56BE.6C89 vlan 99 interface
fastethernet 0/6

e. Sprawdź wpisy w tabeli adresów MAC.

S1# show mac address-table

Ile łącznie adresów MAC zawiera tablica?

Ile adresów statycznych zawiera tablica?

f. Usuń statyczny wpis w tablicy MAC. Przejdź do trybu konfiguracji globalnej i usuń polecenie, umieszczając **no** przed słowami polecenia.

Uwaga: Adres MAC 0050.56BE.6C89 jest używany tylko jako przykład. Użyj adresu MAC dla PC-A.

S1(config)# no mac address-table static 0050.56BE.6C89 vlan 99 interface
fastethernet 0/6

g. Sprawdź, czy statyczny adres MAC został wyczyszczony.

S1# show mac address-table

Ile znajduje się wniej obecnie wszystkich adresów MAC?

Pytania refleksyjne

- 1. Dlaczego warto skonfigurować hasło vty dla przełącznika?
- 2. Dlaczego zmienić domyślną VLAN 1 na inny numer VLAN?
- 3. Jak można zapobiec wyświetlaniu haseł jako jawny tekst?
- 4. Dlaczego skonfigurować statyczny adres MAC na interfejsie portu?

Dodatek A: Inicjalizacja i restartowanie przełącznika

a. W linii poleceń konsoli przełącznika wejdź do trybu uprzywilejowanego.

```
Switch> enable
Switch#
```

b. Należy użyć polecenia show flash do ustalenia, czy nie zostały stworzone sieci VLAN w przełączniku.

```
Switch# show flash
Directory of flash:/
```

```
2 -rwx 1919 Mar 1 1993 00:06:33 +00:00 private-config.text
3 -rwx 1632 Mar 1 1993 00:06:33 +00:00 config.text
4 -rwx 13336 Mar 1 1993 00:06:33 +00:00 multiple-fs
5 -rwx 11607161 Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-2.SE.bin
```

32514048 bytes total (20886528 bytes free)

c. Jeżeli plik vlan.dat został znaleziony w pamięci flash, to należy usunąć ten plik.

6 -rwx 616 Mar 1 1993 00:07:13 +00:00 vlan.dat

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

d. Zostanie wyświetlony monit o sprawdzenie nazwy pliku. Jeśli poprawnie wpisałeś nazwę, naciśnij Enter; w przeciwnym razie możesz zmienić nazwę pliku.

Zostanie wyświetlony monit o potwierdzenie usunięcia tego pliku. Naciśnij klawisz Enter, aby potwierdzić.

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

 Użyj polecenia erase startup-config, aby usunąć plik konfiguracji startowej z pamięci NVRAM. Zostanie wyświetlony monit o usunięcie pliku konfiguracyjnego. Naciśnij klawisz Enter, aby potwierdzić.

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

f. Przeładuj przełącznik, aby usunąć stare dane konfiguracyjne z pamięci. Następnie otrzymasz monit o potwierdzenie przeładowania przełącznika. Naciśnij Enter, aby kontynuować.

Switch# **reload** Proceed with reload? [confirm]

Uwaga: Może pojawić się pytanie o zapisanie aktualnej konfiguracji przed przeładowaniem przełącznika. Należy wpisać **no**, a potem nacisnąć Enter.

System configuration has been modified. Save? [yes/no]: no

g. Po zrestartowaniu przełącznika zostanie wyświetlone pytanie o wejście w tryb dialogu konfiguracyjnego. Należy wpisać **no**, a potem nacisnąć Enter.

Would you like to enter the initial configuration dialog? [yes/no]: **no** Switch>