

Ćwiczenie – Podstawowa konfiguracja routera z użyciem IOS

Część 1 Topologia



Część 2 Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Część 3 Do wykonania

Część 1: Konfiguracja połączeń i inicjacja urządzeń

- Okabluj urządzenia zgodnie z topologią sieci.
- Zainicjuj i zrestartuj router oraz przełącznik.

Część 2: Konfiguracja urządzeń i sprawdzenie łączności

- Statycznie skonfiguruj interfejsy PC-tów dla protokołu IPv4.
- Skonfiguruj podstawowe ustawienia routera.
- Sprawdź łączność w sieci.
- Skonfiguruj router do obsługi SSH.

Część 3: Wyświetl informacje o routerze

- Uzyskaj informacje o sprzęcie i oprogramowaniu routera.
- Zinterpretuj wyświetloną konfigurację początkową (startup configuration).
- Zinterpretuj wyświetloną tablicę wyboru trasy (routing table).
- Sprawdź stan interfejsów.

Część 4: Skonfiguruj IPv6 i sprawdź łączność

Część 4 Wprowadzenie / Scenariusz

Jest to kompleksowe ćwiczenie służące do powtórki wcześniej poznanych poleceń IOS routera. W części 1 i 2 będziesz okablowywać urządzenia i uzupełniać podstawową konfigurację oraz ustawienia interfejsu z protokołem IPv4 na routerze.

W części 3 będziesz używać SSH do połączenia zdalnego z routerem i skorzystasz z poleceń IOS do wyszukania informacji na urządzeniu tak aby odpowiedzieć na pytania dotyczące routera. W części 4 będziesz konfigurować IPv6 na routerze w taki sposób, aby umożliwić PC-B pozyskanie adresu i sprawdzenie łączności.

Na potrzeby powtórki niniejsza instrukcja zawiera polecenia niezbędne do konkretnej konfiguracji routera.

Uwaga: Niniejsza instrukcja zakłada użycie routerów Cisco 1941 Integrated Services Routers (ISRs) z oprogramowaniem Cisco IOS Release 15.2(4) M3 (universalk9 image). Można zastosować inne routery i wersje IOS. W zależności od modelu i wersji oprogramowania IOS Cisco dostępne polecenia i ich wyniki mogą się różnić od przedstawionych w tej instrukcji. Na końcu instrukcji znajduje się tabela zawierająca zestawienie interfejsów routerów, których można użyć na laboratorium. Ułatwi ona poprawną identyfikację interfejsów.

Uwaga: Sprawdź czy na routerach i przełącznikach została skasowana konfiguracja. Jeżeli tak nie jest w **dodatku A** znajdziesz opis procedury inicjacji i przeładowania routera.

Część 5 Wymagane zasoby

- 1 Router (Cisco 1941 z Cisco IOS Release 15.2(4)M3 universal image lub podobny)
- 1 Przełącznik (Cisco 2960 z Cisco IOS Release 15.0(2) lanbasek9 image lub podobny)
- 2 PC-ty (Windows 7, Vista, lub XP z zainstalowanymi programami emulatora terminala, takim jak Tera Term lub PuTTY oraz Wireshark)
- Kable konsolowe do konfiguracji urządzeń z IOS przez port konsoli
- Kable Ethernet tak jak pokazano na rysunku

Uwaga: Interfejs Gigabit Ethernet na Cisco 1941 ISR ma funkcję autosensing dzięki niej możesz użyć „prostego” kabla Ethernet (straight-through) pomiędzy routerem i PC-B. Jeżeli używasz innego modelu routera, może się okazać, że wymagane jest użycie kabla skrzyżowanego (crossover).

Część 1. Konfiguracja połączeń i inicjacja urządzeń

Krok 1. Okabluj urządzenia zgodnie z topologią sieci.

- a. Zgodnie z topologią pokazaną na rysunku wybierz urządzenie i wykonaj okablowanie.
- b. Włącz zasilanie wszystkich urządzeń pokazanych w topologii.

Krok 2. Zainicjuj i zrestartuj router oraz przełącznik.

Uwaga: W dodatku A opisano szczegółowo kroki prowadzące do inicjacji i przeładowania urządzeń.

Część 2. Konfiguracja urządzeń i sprawdzenie łączności

Krok 1. Konfiguracja interfejsów PC-tów.

- a. Skonfiguruj adres IP, maskę podsieci i bramę domyślną na PC-A.
- b. Skonfiguruj adres IP, maskę podsieci i bramę domyślną na PC-B.

Krok 2. Konfiguracja routera.

- a. Podłącz się do konsoli routera i przejdź na poziom uprzywilejowany (enable privileged EXEC mode).

```
Router> enable
Router#
```

- b. Wejdź do trybu konfiguracji globalnej (global configuration mode).

```
Router# config terminal
Router(config)#
```

- c. Przypisz nazwę urządzenia do routera.

```
Router(config)# hostname R1
```

- d. Zablokuj wyszukiwanie w DNS (DNS lookup) aby uniknąć sytuacji, w której router błędnie wpisane polecenia interpretuje jako nazwy i próbuje dokonać ich translacji na adres.

```
R1(config)# no ip domain-lookup
```

- e. Wymuś długość hasła na co najmniej 10 znaków dla wszystkich haseł.

```
R1(config)# security passwords min-length 10
```

Poza ustawieniem minimalnej długości hasła, podaj inne sposoby wzmocnienia haseł.

- f. Ustaw **cisco12345** jako zaszyfrowane hasło do poziomu uprzywilejowanego.

```
R1(config)# enable secret cisco12345
```

- g. Ustaw **ciscoconpass** jako hasło do konsoli, ustal timeout, włącz możliwość zalogowania (enable login), dodaj polecenie logging synchronous. Polecenie logging synchronous synchronizuje wyświetlanie komunikatów systemowych i oprogramowania Cisco IOS. Dzięki temu zapobiega przerywaniu tekstu wpisywanego z klawiatury przez komunikaty systemowe.

```
R1(config)# line con 0
R1(config-line)# password ciscoconpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
R1(config-line)# exit
R1(config)#
```

Co oznacza w poleceniu **exec-timeout** odpowiednio **5** i **0**?

- h. Ustaw **ciscovtypass** jako hasło do vty, ustal timeout, włącz możliwość zalogowania (enable login), dodaj polecenie logging synchronous.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
R1(config-line)# exit
R1(config)#
```

- i. Wymuś szyfrowanie haseł zapisanych jawnym tekstem.

```
R1(config)# service password-encryption
```

- j. Utwórz baner powitalny będący dla usiłujących uzyskać dostęp do urządzenia ostrzeżeniem, że zabroniony jest nieuprawniony dostęp.

```
R1(config)# banner motd #Zabrania sie nieuprawnionego dostepu!#
```

- k. Skonfiguruj adresy IP i opisy interfejsów (interface description). Aktywuj obydwa interfejsy na routerze.

```
R1(config)# int g0/0
R1(config-if)# description Connection to PC-B
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# int g0/1
R1(config-if)# description Connection to S1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# exit
R1#
```

- l. Ustaw zegar na routerze np.:

```
R1# clock set 15:00:00 13 Oct 2014
```

- m. Zapisz konfigurację (running configuration) do pliku startup configuration.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

R1#

Jaki będzie efekt przeładowania routera bez wykonania polecenia **copy running-config startup-config**?

- n. Z wiersza poleceń na PC-A wykonaj komendę ping do PC-B.

Uwaga: Może być konieczne wyłączenie na PC-tach funkcji firewall.

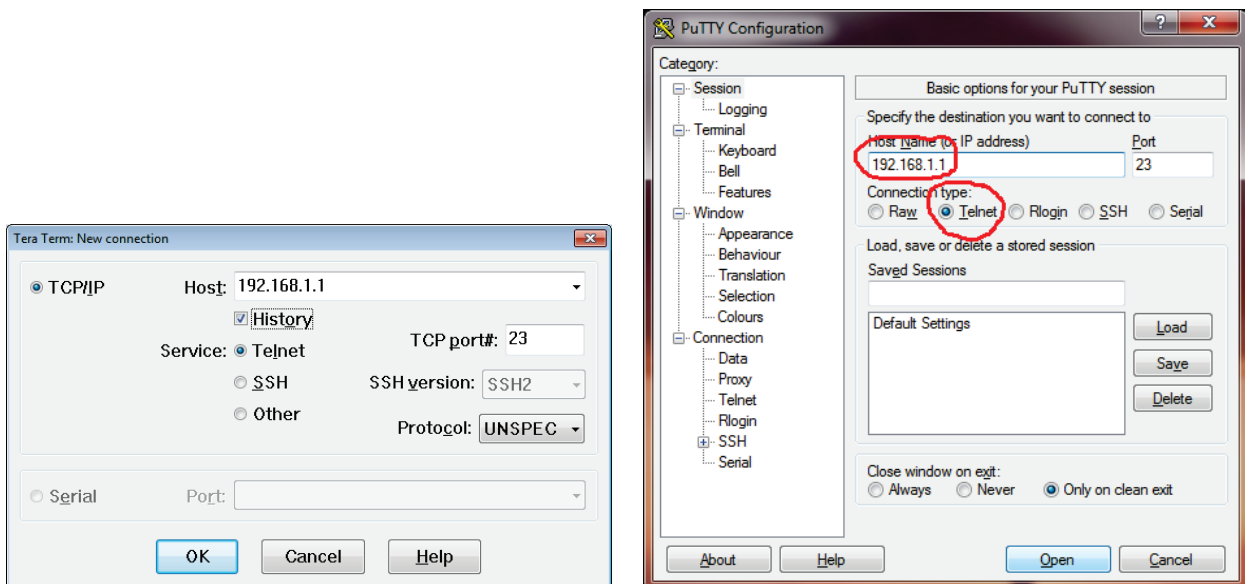
Czy ping zakończył się sukcesem? _____

Jaki rodzaj zdalnego dostępu może być użyty po ukończeniu powyższej konfiguracji aby uzyskać dostęp do R1?

- o. Zdalny dostęp z PC-A do R1 z użyciem klienta telnet w aplikacji Tera Term lub PuTTY.

Otwórz Tera Term lub PuTTY i wprowadź adres IP interfejsu G0/1 na R1

Tera Term: New Connection window -> adres IP w pole Host Service: **Telnet** I naciśnij **OK** PuTTY: w polu Host name wpisz adres IP, Connection type zaznacz **Telnet** i naciśnij **Open**



Czy próba zdalnego dostępu zakończyła się sukcesem? _____

Dlaczego protokół Telnet jest uważany za potencjalne zagrożenie?

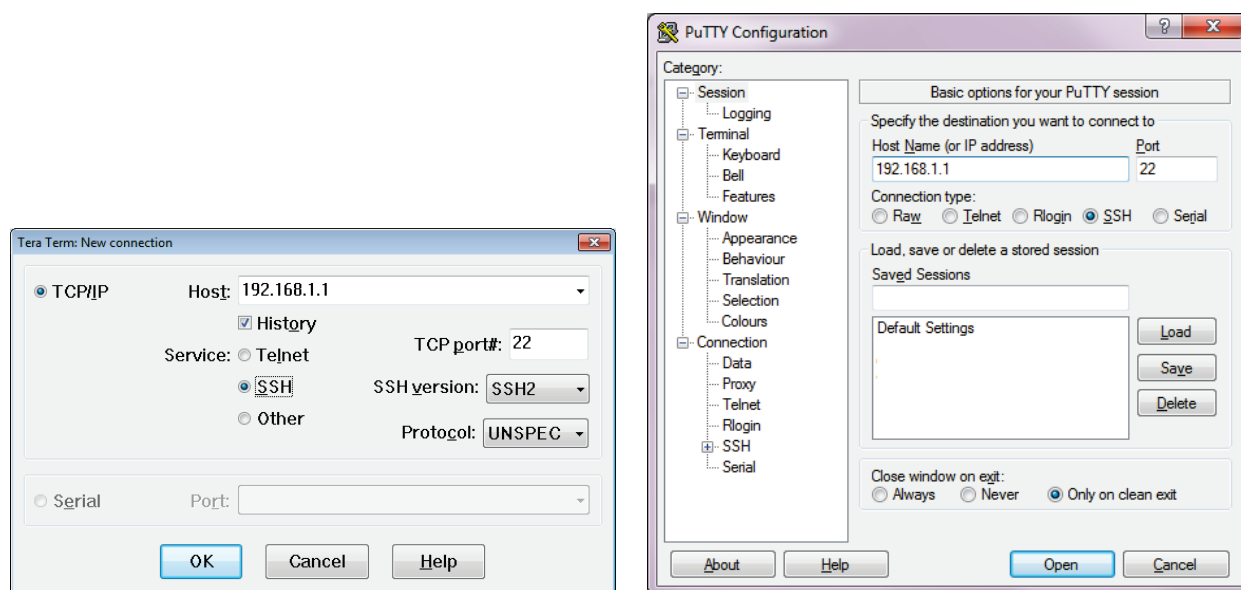
Krok 3. Konfiguracja routera dla dostępu przez SSH.

Zezwól na połączenia SSH i utwórz użytkownika w lokalnej bazie danych na routerze.

```
R1# configure terminal
R1(config)# ip domain-name CCNA-lab.com
R1(config)# username admin privilege 15 secret adminpass1
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
R1(config-line)# exit
R1(config)# crypto key generate rsa modulus 1024
R1(config)# exit
```

- a. Zdalny dostęp z PC-A do R1 z użyciem klienta **SSH** w aplikacji Tera Term lub PuTTY.
b. Otwórz Tera Term lub PuTTY i wprowadź adres IP interfejsu G0/1 na R1

Tera Term: New Connection window → wpisz adres IP w pole Host Service: **SSH** i naciśnij **OK**
PuTTY: w polu Host name → wpisz adres IP, Connection type → zaznacz **SSH** i naciśnij **Open**



Czy próba zdalnego dostępu zakończyła się sukcesem? _____

Część 3. Wyświetlenie informacji o routerze

W części 3, będziesz używać polecenia **show** podczas sesji SSH aby wydobyć informacje z routera.

Krok 1. Ustanowienie sesji SSH do R1.

Używając Tera Term lub PuTTY na PC-B, otwórz sesję SSH do R1 na adres IP 192.168.0.1 i zaloguj się jako **admin** z hasłem **adminpass1**.

Krok 2. Wydobycie ważnych informacji o sprzęcie i oprogramowaniu.

- a. Użyj polecenia **show version** aby odpowiedzieć na pytania dotyczące routera.

Jaka jest nazwa obrazu IOS działającego na routerze?

Ile pamięci nieulotnej typu NVRAM (non-volatile random-access memory) jest zainstalowane na routerze?

Ile jest pamięci typu Flash na routerze?

- b. Polecenie **show** zazwyczaj wyświetla wiele ekranów informacji. Filtrowanie informacji wyjściowej pozwala użytkownikowi wyświetlić tylko interesującą go sekcję. Aby włączyć filtrowanie należy po poleceniu **show**, wprowadzić pionową kreskę (pipe |) a po niej parameter filtru a następnie filtrowane wyrażenie. Możesz odfiltrować wyjście używając słowa kluczowego **include** do wyświetlenia wszystkich linii zawierających interesujące nas wyrażenie. Odfiltruj polecenie **show version**, używając **show version | include register** do odpowiedzi na następujące pytanie.

Jaki będzie proces boot podczas następnego przeładowania?

Krok 3. Wyświetlenie pliku startup configuration.

Użyj polecenia **show startup-config** na routerze do odpowiedzi na następujące pytania.

Jak są przedstawione hasła w pliku startup-config?

Użyj polecenia **show startup-config | begin vty**.

Jaki jest wynik użycia tego polecenia?

Krok 4. Wyświetlenie tablicy routingu

Użyj polecenia **show ip route** na routerze do odpowiedzi na następujące pytania.

Jaki kod jest używany w tablicy wyboru trasy (routing table) do wskazania bezpośrednio podłączonych sieci (directly connected network)?

Ile pozycji z kodem C jest w tablicy wyboru trasy? _____

Krok 5. Wyświetlenie listy z podsumowaniem interfejsów na routerze.

Użyj polecenia **show ip interface brief** na routerze do odpowiedzi na następujące pytanie.

Które polecenie zmienia stan portu Gigabit Ethernet z administratively down na up?

Część 4. Konfiguracja IPv6 i sprawdzenie łączności

Krok 1. Ustaw adres IPv6 na R1 G0/0 i włącz routing IPv6.

Uwaga: Przypisanie na interfejsie adresu IPv6 łącznie z adresem IPv4 jest znane jako podwójny stos (dual stacking), ponieważ zarówno stos protokołu IPv6 jak i IPv4 są aktywne. Po włączeniu routingu unicastowego IPv6 (IPv6 unicast routing) na R1, PC-B będzie odbierać z R1 G0/0 IPv6 prefiks sieci (network prefix) co pozwoli na autokonfigurację adresu IPv6 i bramy domyślnej.

- Przypisz do interfejsu G0/0 adres IPv6 typu global unicast address, przypisz też dodatkowo adres typu link-local address i włącz routing IPv6 (IPv6 routing).

```
R1# configure terminal
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:acad:a::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ipv6 unicast-routing
R1(config)# exit
```

- Użyj polecenia **show ipv6 int brief** do sprawdzenia ustawień IPv6 na R1.
Jeżeli adres IPv6 nie jest przypisany do G0/1, dlaczego jest wyświetlany, jako [up/up]?

- Przy pomocy polecenia **ipconfig** na PC-B sprawdź konfigurację IPv6.

Jaki adres IPv6 został przypisany do PC-B?

Jaki jest adres bramy domyślnej przypisanej do PC-B? _____

Wydadaj polecenie ping z PC-B do R1 na adres typu default gateway link local address. Czy polecenie zakończyło się sukcesem? _____

Wydaj polecenie ping z PC-B do R1 na adres IPv6 unicast address **2001:db8:acad:a::1**.

Czy polecenie zakończyło się sukcesem? _____

Do przemyślenia

1. Podczas badania przyczyn braku łączności w sieci technik zauważył, że interfejs nie jest włączony. Które polecenie **show** pomogło technikowi w rozwiązaniu tej kwestii?

2. Podczas badania przyczyn braku łączności w sieci technik zauważył, że na interfejsie jest przypisana niepoprawna maska podsieci. Które polecenie **show** pomogło technikowi w rozwiązaniu tej kwestii?

3. Po skonfigurowaniu IPv6 na R1 G0/0 w sieci LAN PC-B, jeżeli wydasz polecenie ping z PC-A do PC-B na adres IPv6, czy działanie ping zakończy się sukcesem? Dlaczego tak lub dlaczego nie?

Tabela z zestawieniem interfejsów routera

Zestawienie interfejsów routera				
Model routera	Interfejs Ethernet #1	Interfejs Ethernet #2	Interfejs Serial #1	Interfejs Serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Uwaga: Aby dowiedzieć się, jaka jest konfiguracja sprzętowa routera, obejrzyj interfejsy (lub z poziomu IOS użyj **show ip interface brief**), aby zidentyfikować typ routera oraz aby określić liczbę interfejsów routera. Nie ma sposobu na skuteczne opisanie wszystkich kombinacji konfiguracji dla wszystkich rodzajów routerów. Niniejsza tabela zawiera identyfikatory możliwych kombinacji interfejsów szeregowych i Ethernet w urządzeniu. Tabela nie zawiera żadnych innych rodzajów interfejsów, mimo iż mogą być na routerze zainstalowane. Przykładem może być interfejs ISDN BRI. Łańcuch w nawiasie jest skrótem, który może być stosowany w systemie operacyjnym Cisco IOS przy odwoływaniu się do interfejsu.

Dodatek A: Inicjacja i przeładowanie routera oraz przełącznika

1 Inicjacja i przeładowanie routera.

- a. Podłącz konsolę w routerze i przejdź na poziom uprzywilejowany (enable privileged EXEC mode).

```
Router> enable
Router#
```

- b. Wpisz polecenie **erase startup-config** aby usunąć plik startup configuration z NVRAM.

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

- c. Wykonaj polecenie **reload** aby usunąć starą konfigurację z pamięci (RAM). Gdy pojawi się monit o **Proceed with reload**, naciśnij Enter aby potwierdzić przeładowanie (reload). (Naciśnięcie innego klawisza przerwie proces przeładowania.)

```
Router# reload
Proceed with reload? [confirm]
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Uwaga: Może pojawić się monit o zachowanie running configuration przed przeładowaniem routera. Wpisz **no** i naciśnij Enter.

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

- d. Po przeładowaniu routera pojawi się monit o rozpoczęcie dialogu konfiguracji początkowej. Wpisz **no** i naciśnij Enter.

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

- e. Gdy pojawi się monit o zakończenie autoinstalacji. Wpisz **yes** i naciśnij Enter.

```
Would you like to terminate autoinstall? [yes]: yes
```

Krok 2. Inicjacja i przeładowanie przełącznika.

- a. Podłącz się do konsoli przełącznika i przejdź do trybu uprzywilejowanego (privileged EXEC mode).

```
Switch> enable
```

```
Switch#
```

- b. Użyj polecenia **show flash** do sprawdzenia czy na przełączniku były utworzone sieci VLAN

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

```
32514048 bytes total (20886528 bytes free)
```

```
Switch#
```

- c. Jeżeli plik **vlan.dat** zostanie znaleziony w pamięci flash należy go skasować.

```
Switch# delete vlan.dat
```

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

Pojawi się monit o potwierdzenie nazwy pliku. W tym miejscu możesz zmienić nazwę pliku lub po prostu nacisnąć Enter jeżeli wprowadzona nazwa jest poprawna.

Pojawi monit o potwierdzenie skasowania tego pliku. Naciśnij Enter aby potwierdzić kasowanie. (Naciśnij inny klawisz aby przerwać kasowanie.)

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

```
Switch#
```

- d. Użyj polecenia **erase startup-config** do skasowania pliku startup configuration z pamięci NVRAM. Pojawi się monit o potwierdzenie skasowania pliku z konfiguracją. Naciśnij Enter aby potwierdzić kasowanie. (Naciśnij inny klawisz aby przerwać kasowanie.)

```
Switch# erase startup-config
```

```
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
```

```
[OK]
```

```
Erase of nvram: complete
```

```
Switch#
```

- f. Wykonaj polecenie **reload** aby usunąć starą konfigurację z pamięci (RAM) przełącznika. Gdy pojawi się monit o **Proceed with reload**, naciśnij Enter aby potwierdzić przeładowanie (reload). (Naciśnięcie innego klawisza przerwie proces przeładowania.)

```
Switch# reload
```

```
Proceed with reload? [confirm]
```

Uwaga: Może pojawić się monit o zachowanie running configuration przed przeładowaniem routera. Wpisz **no** i naciśnij Enter.

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

- e. Po przeładowaniu przełącznika pojawi się monit o rozpoczęcie dialogu konfiguracji początkowej. Wpisz **no** i naciśnij Enter.

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

```
Switch>
```