



2	Podstawy konfiguracji przełącznika i urządzenia końcowego	^
2.4	urządzeń	^
2.4.1	Nazwy urządzeń	
2.4.2	Wytyczne dotyczące haseł	
2.4.3	Konfiguracja haseł	
2.4.4	Szyfrowanie haseł	
2.4.5	Baner - komunikaty	
2.4.6	Wideo - Zabezpieczanie dostępu administratora do przełącznika	
2.4.7	Weryfikator składni - Podstawowa konfiguracja urządzenia	
2.4.8	Sprawdź, czy zrozumiałeś - Podstawowa konfiguracja urządzenia	
2.5	Zapisywanie konfiguracji	✓
2.6	Porty i adresy	✓
2.7	Konfiguracja adresacji IP	✓
2.8	Weryfikacja łączności	✓

# Podstawowa konfiguracja urządzeń

2.4.1

## Nazwy urządzeń



Dowiedziałeś się wiele o Cisco IOS, nawigacji w IOS i strukturze poleceń. Teraz jesteś gotowy do konfiguracji urządzeń! Pierwszym poleceniem konfiguracji na dowolnym urządzeniu powinno być nadanie mu unikalnej nazwy urządzenia czyli hostname. Domyślnie wszystkie urządzenia mają przypisaną domyślną nazwę fabryczną. Na przykład przełącznik Cisco IOS ma nazwę Switch.

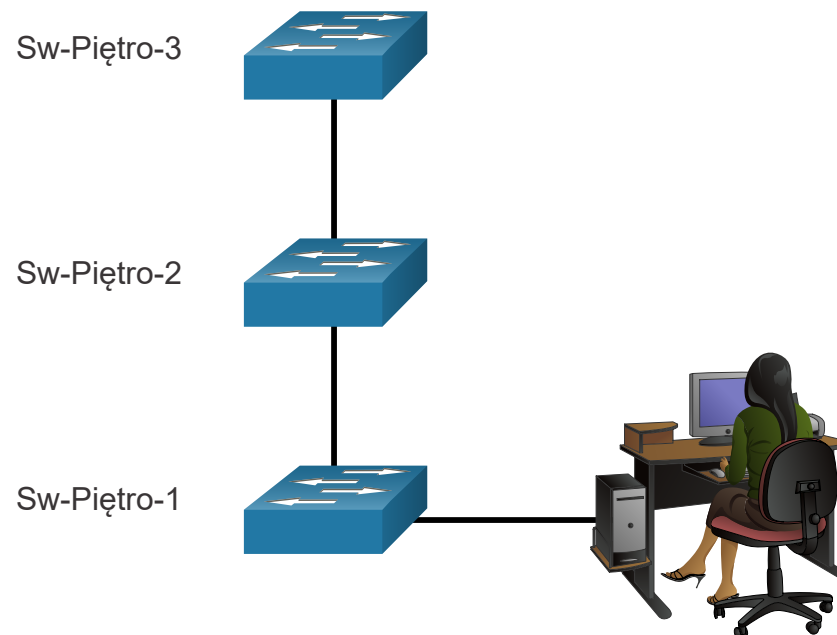
Problem polega na tym, że jeśli wszystkie przełączniki w sieci zostały pozostawione z domyślnymi nazwami, trudno byłoby zidentyfikować określone urządzenie. Na przykład, skąd możesz wiedzieć, że jesteś podłączony do odpowiedniego urządzenia podczas uzyskiwania dostępu do niego zdalnie za pomocą SSH? Nazwa hosta potwierdza połączenie z właściwym urządzeniem.

Domyślna nazwa powinna zostać zmieniona na coś bardziej opisowego. Poprzez przemyślany wybór łatwiej będzie pamiętać, dokumentować i identyfikować urządzenia sieciowe. Oto kilka ważnych wytycznych nazewnictwa dla hostów:

- Nazwa musi zaczynać się od litery.
- Nie powinny zawierać spacji
- Kończyć się literą lub cyfrą
- Używać tylko liter, cyfr i znaków podkreślenia.
- Nazwa nie powinna zawierać więcej niż 64 znaki.

Organizacja musi wybrać konwencję nazewnictwa, która ułatwia intuicyjną identyfikację określonego urządzenia. Nazwy hostów używane w urządzeniach IOS rozróżniają wielkość liter. Na przykład rysunek pokazuje, że trzy przełączniki, znajdujące się na trzech różnych piętrach, są ze sobą połączone w sieć. Konwencja nazewnictwa, która została użyta, zawierała lokalizację i przeznaczenie każdego urządzenia. Dokumentacja sieciowa powinna wyjaśniać, w jaki sposób wybrano te nazwy, tak aby dodatkowe urządzenia mogły być odpowiednio nazwane.

2.9	Moduł ćwiczeń i quizu	▼
3	Protokoły i modele	▼
2	Podstawy konfiguracji	▲
2.4	przełącznika i urządzenia	▲
2.4	końcowego	▲
2.4	urządzeń	▲
2.4.1	Nazwy urządzeń	
2.4.2	Wytyczne dotyczące haseł	
2.4.3	Konfiguracja haseł	
2.4.4	Szyfrowanie haseł	
2.4.5	Baner - komunikaty	
2.4.6	Wideo - Zabezpieczanie dostępu	
	administratora do przełącznika	
2.4.7	Weryfikator składni - Podstawowa	
	konfiguracja urządzenia	
2.4.8	Sprawdź, czy zrozumiałeś -	
	Podstawowa konfiguracja	
	urządzenia	
2.5	Zapisywanie konfiguracji	▼
2.6	Porty i adresy	▼
2.7	Konfiguracja adresacji IP	▼
2.8	Weryfikacja łączności	▼



Nazwane urządzenia sieciowe można łatwo zidentyfikować do celów konfiguracji.

Po ustaleniu konwencji nazewnictwa, korzystając z wiersza poleceń, nadajemy nazwy urządzeniom. Jak pokazano w przykładzie, będąc w uprzywilejowanym trybie EXEC przejdź do trybu konfiguracji globalnej, wprowadzając polecenie **configure terminal**. Zwróć uwagę, jak zmienił się symbol zachęty.

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

W trybie konfiguracji globalnej wprowadź polecenie **hostname** a następnie nazwę przełącznika i naciśnij **Enter**. Zwróć uwagę na zmianę znaków zachęty.

**Uwaga:** Aby przywrócić przełącznik do domyślnego znaku zachęty, użyj polecenia **no hostname** w trybie konfiguracji globalnej.

2.9	Moduł ćwiczeń i quizu	▼
3	Protokoły i modele	▼
2	Podstawy konfiguracji	
2	przełącznika i urządzenia	▲
2.4	końcowego	
2.4	urządzeń	▲
2.4.1	Nazwy urządzeń	
2.4.2	Wytyczne dotyczące haseł	
2.4.3	Konfiguracja haseł	
2.4.4	Szyfrowanie haseł	
2.4.5	Baner – komunikaty	
2.4.6	Wideo – Zabezpieczanie dostępu administratora do przełącznika	
2.4.7	Weryfikator składni – Podstawowa konfiguracja urządzenia	
2.4.8	Sprawdź, czy zrozumiałeś – Podstawowa konfiguracja urządzenia	
2.5	Zapisywanie konfiguracji	▼
2.6	Porty i adresy	▼
2.7	Konfiguracja adresacji IP	▼
2.8	Weryfikacja łączności	▼

Po dodaniu lub modyfikacji konfiguracji urządzenia należy uaktualnić dokumentację. Urządzenia w dokumentacji opisujemy poprzez wskazanie ich lokalizacji, celu oraz adresu.

#### 2.4.2

## Wytyczne dotyczące haseł



Używanie słabych lub łatwych do odgadnięcia haseł nadal jest największym problemem bezpieczeństwa organizacji. Urządzenia sieciowe, w tym domowe routery bezprzewodowe, powinny zawsze mieć hasła skonfigurowane w celu ograniczenia dostępu administracyjnego.

System Cisco IOS można skonfigurować do używania haseł w trybie hierarchicznym, aby nadać różne uprawnienia dostępu do urządzenia sieciowego.

Wszystkie urządzenia sieciowe powinny ograniczać dostęp administracyjny poprzez zabezpieczenie uprzywilejowanego trybu EXEC, trybu użytkownika EXEC i zdalnego dostępu Telnet hasłami. Ponadto wszystkie hasła powinny być szyfrowane, a powiadomienia prawne muszą być wyświetlane.

Wybierając hasła, używaj silnych, których nie można łatwo odgadnąć. Wybierając hasła, należy wziąć pod uwagę kilka kluczowych punktów:

- korzystaj z haseł o długości większej niż 8 znaków,
- używaj z kombinacji dużych i małych liter, liczb, znaków specjalnych i/lub sekwencji cyfr,
- unikaj stosowania tych samych haseł do wszystkich urządzeń,
- nie używaj popularnych słów, ponieważ łatwo się je domyślić.

Użyj wyszukiwarki internetowej, aby znaleźć generator haseł. Wiele z nich pozwala ustawić długość, zestaw znaków i inne parametry.

**Uwaga:** Większość laboratoriów tego kursu używa prostych haseł, takich jak **cisco** lub **class**. Hasła te są uznawane za słabe i łatwe do odgadnięcia. Należy ich unikać w środowiskach produkcyjnych. Hasła tych używamy dla ułatwienia tylko w salach szkoleniowych albo do zilustrowania przykładów konfiguracji.

2.9	Moduł ćwiczeń i quizu	▼
3	Protokoły i modele	▼
2	Podstawy konfiguracji	▼
2	przełącznika i urządzenia	▲
2.4	końcowego	▲
2.4	urządzeń	▲
2.4.1	Nazwy urządzeń	
2.4.2	Wytyczne dotyczące haseł	
2.4.3	Konfiguracja haseł	
2.4.4	Szyfrowanie haseł	
2.4.5	Baner - komunikaty	
2.4.6	Wideo - Zabezpieczanie dostępu	
2.4.7	Weryfikator składni - Podstawowa	
2.4.8	konfiguracja urządzenia	
2.5	Sprawdź, czy zrozumiałeś -	
2.5	Podstawowa konfiguracja	
2.5	urządzenia	
2.5	Zapisywanie konfiguracji	▼
2.6	Porty i adresy	▼
2.7	Konfiguracja adresacji IP	▼
2.8	Weryfikacja łączności	▼

## 2.4.3

## Konfiguracja haseł



Kiedy początkowo łączysz się z urządzeniem, jesteś w trybie EXEC użytkownika. Ten tryb jest zabezpieczony za pomocą konsoli.

Aby zabezpieczyć dostęp do trybu EXEC użytkownika, należy wejść w tryb konfiguracji linii konsoli przy użyciu polecenia **line console 0** w trybie konfiguracji globalnej, jak pokazano w przykładzie. Zero reprezentuje pierwszy (i w większości przypadków jedyny) interfejs konsoli routera. Następnie nadaj hasło trybu użytkownika EXEC za pomocą polecenia **password password**. Na koniec włącz dostęp użytkownika EXEC za pomocą polecenia **login**.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Połączenie z konsolą będzie teraz wymagało hasła przed uzyskaniem dostępu do trybu EXEC użytkownika.

Aby mieć dostęp administratora do wszystkich poleceń IOS, w tym do konfigurowania urządzenia, musisz uzyskać dostęp do trybu uprzywilejowanego EXEC. Jest to najważniejsza metoda dostępu, ponieważ zapewnia pełny dostęp do urządzenia.

Aby zabezpieczyć uprzywilejowany tryb EXEC, użyj polecenia **enable secret password** w trybie konfiguracji globalnej, jak pokazano w przykładzie.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Linie terminala wirtualnego (VTY) umożliwiają zdalny dostęp za pomocą Telnet lub SSH do urządzenia. Wiele przełączników Cisco wspiera do 16 linii VTY, które są ponumerowane od 0 do 15.

Aby zabezpieczyć linie VTY, wejdź w tryb linii VTY za pomocą polecenia **line vty 0 15** trybu konfiguracji globalnej. Następnie określ hasło VTY za pomocą polecenia **password password**. Na koniec włącz dostęp VTY za pomocą polecenia **login**.

- 2.9 Moduł ćwiczeń i quizu
- 3 Protokoły i modele
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego
- 2.4 urządzenia
- 2.4.1 Nazwy urządzeń
- 2.4.2 Wytyczne dotyczące haseł
- 2.4.3 Konfiguracja haseł
- 2.4.4 Szyfrowanie haseł
- 2.4.5 Baner – komunikaty
- 2.4.6 Wideo – Zabezpieczanie dostępu administratora do przełącznika
- 2.4.7 Weryfikator składni – Podstawowa konfiguracja urządzenia
- 2.4.8 Sprawdź, czy zrozumiałeś – Podstawowa konfiguracja urządzenia
- 2.5 Zapisywanie konfiguracji
- 2.6 Porty i adresy
- 2.7 Konfiguracja adresacji IP
- 2.8 Weryfikacja łączności

Przykład zabezpieczenia linii VTY na przełączniku.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

2.4.4

## Szyfrowanie haseł



Pliki start-config i running-config wyświetlają większość haseł w postaci zwykłego tekstu. Jest to zagrożenie bezpieczeństwa, ponieważ każdy może odkryć hasła, jeśli ma dostęp do tych plików.

Aby zaszyfrować wszystkie hasła trzymane jako zwykły tekst, użyj polecenia **service password-encryption** w trybie konfiguracji globalnej, jak pokazano w przykładzie.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)#
```

Polecenie stosuje słabe szyfrowanie do wszystkich niezaszyfrowanych haseł. To szyfrowanie dotyczy tylko haseł zapisanych w pliku konfiguracyjnym, a nie haseł, które są przesyłane przez sieć. Celem tej komendy jest uniemożliwienie nieautoryzowanym użytkownikom zapoznanie się z hasłami zapisanymi w pliku konfiguracyjnym.

Użyj polecenia **show running-config**, aby sprawdzić, czy hasła są teraz szyfrowane.

```
Sw-Floor-1(config)# end
Sw-Floor-1# show running-config
!
!
line con 0
```

- 2.9 Moduł ćwiczeń i quizu
- 3 Protokoły i modele
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego
- 2.4 urządzeń
- 2.4.1 Nazwy urządzeń
- 2.4.2 Wytyczne dotyczące haseł
- 2.4.3 Konfiguracja haseł
- 2.4.4 Szyfrowanie haseł
- 2.4.5 Baner - komunikaty
- 2.4.6 Wideo - Zabezpieczanie dostępu administratora do przełącznika
- 2.4.7 Weryfikator składni - Podstawowa konfiguracja urządzenia
- 2.4.8 Sprawdź, czy zrozumiałeś - Podstawowa konfiguracja urządzenia
- 2.5 Zapisywanie konfiguracji
- 2.6 Porty i adresy
- 2.7 Konfiguracja adresacji IP
- 2.8 Weryfikacja łączności

```
hasło 7 094F471A1A0A
login
!
line vty 0 4
hasło 7 03095A0F034F38435B49150A1819
login
!
!
end
```

2.4.5

## Baner - komunikaty











Chociaż wymaganie haseł jest jedną z metod trzymania nieautoryzowanych osób z dala od urządzeń sieciowych, istotne jest również dostarczenie metody informowania o tym, kto może uzyskać dostęp do urządzenia. Aby to zrobić, do konfiguracji urządzenia należy dodać baner. Banery mogą być istotnym elementem procesu prawnego w sytuacji, gdy ktoś jest ścigany za włamanie do urządzenia. Niektóre systemy prawne nie pozwalają na ściganie, a nawet monitoring użytkowników, bez wcześniejszej widocznej informacji o tym fakcie.

Aby utworzyć wiadomość banera dnia na urządzeniu sieciowym, użyj polecenia **banner motd # the message of day #** w trybie konfiguracji globalnej. Znak „#” w składni poleceń nazywa się znakiem ograniczającym. Jest on wprowadzany przed i po wiadomości. Znak ograniczający może być dowolnym znakiem, o ile nie występuje w wiadomości. Dlatego jako separatora często używa się symbolu #. Po wydaniu polecenia, baner będzie wyświetlany podczas wszystkich prób dostępu do urządzenia - aż do czasu jego usunięcia.

Poniższy przykład pokazuje kroki, aby skonfigurować baner na Sw-Floor-1.

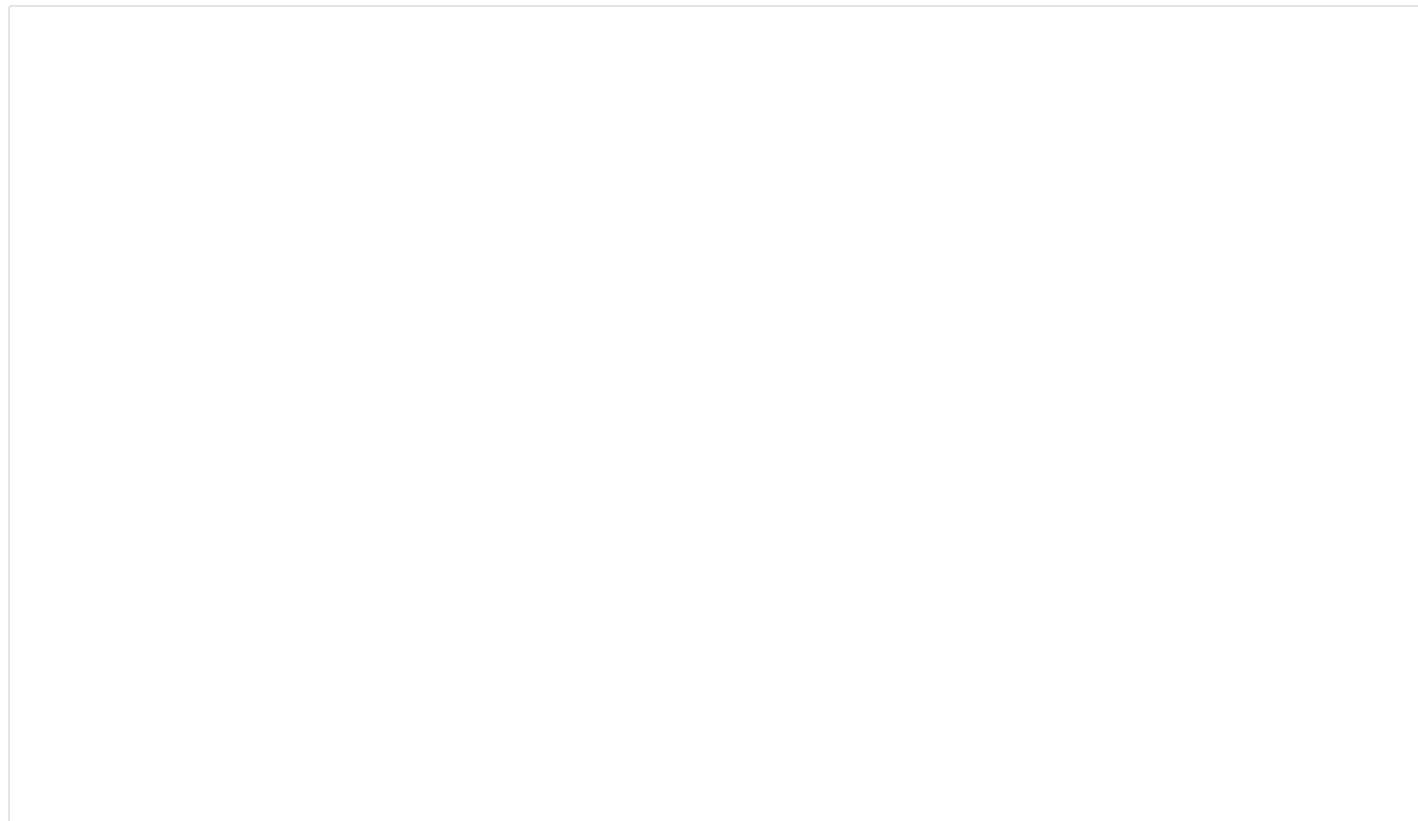
```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only#
```

2.4.6

- 2.9 Moduł ćwiczeń i quizu 
- 3 Protokoły i modele 
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego 
- 2.4 urządzeń 
- 2.4.1 Nazwy urządzeń
- 2.4.2 Wytyczne dotyczące haseł
- 2.4.3 Konfiguracja haseł
- 2.4.4 Szyfrowanie haseł
- 2.4.5 Baner – komunikaty
- 2.4.6 Wideo – Zabezpieczanie dostępu administratora do przełącznika
- 2.4.7 Weryfikator składni – Podstawowa konfiguracja urządzenia
- 2.4.8 Sprawdź, czy zrozumiałeś – Podstawowa konfiguracja urządzenia
- 2.5 Zapisywanie konfiguracji 
- 2.6 Porty i adresy 
- 2.7 Konfiguracja adresacji IP 
- 2.8 Weryfikacja łączności 

## Wideo - Zabezpieczanie dostępu administratora do przełącznika

Kliknij przycisk Odtwórz na rysunku, aby wyświetlić demonstrację wideo, jak zabezpieczyć administracyjny dostęp do przełącznika.



2.4.7

## Weryfikator składni - Podstawowa konfiguracja

2.9	Moduł ćwiczeń i quizu	▼
3	Protokoły i modele	▼
2	Podstawy konfiguracji	▼
2	przełącznika i urządzenia	▲
2.4	końcowego	▲
2.4	urządzeń	▲
2.4.1	Nazwy urządzeń	
2.4.2	Wytyczne dotyczące haseł	
2.4.3	Konfiguracja haseł	
2.4.4	Szyfrowanie haseł	
2.4.5	Baner - komunikaty	
2.4.6	Wideo - Zabezpieczanie dostępu	
2.4.7	administratora do przełącznika	
2.4.7	Weryfikator składni - Podstawowa	
2.4.8	konfiguracja urządzenia	
2.4.8	Sprawdź, czy zrozumiałeś -	
2.4.8	Podstawowa konfiguracja	
2.4.8	urządzenia	
2.5	Zapisywanie konfiguracji	▼
2.6	Porty i adresy	▼
2.7	Konfiguracja adresacji IP	▼
2.8	Weryfikacja łączności	▼

## urządzenia

Zabezpiecz dostęp do zarządzania do przełącznika.

- Przypisz routerowi nazwę
- Zabezpiecz dostęp do trybu EXEC użytkownika
- Zabezpiecz dostęp do trybu uprzywilejowanego EXEC.
- Zabezpiecz dostęp do VTY.
- Zasyfruj hasła zapisane jawnym tekstem.
- Wyświetla baner logowania.

Przejdź do trybu konfiguracji globalnej.

Switch#

Resetuj

Rozwiązanie









Pokaż całość

2.4.8

## Sprawdź, czy zrozumiałeś - Podstawowa konfiguracja





- 2.9 Moduł ćwiczeń i quizu 
- 3 Protokoły i modele 
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego 
- 2.4 urządzeń 
- 2.4.1 **Nazwy urządzeń**
- 2.4.2 Wytyczne dotyczące haseł
- 2.4.3 Konfiguracja haseł
- 2.4.4 Szyfrowanie haseł
- 2.4.5 Baner - komunikaty
- 2.4.6 Wideo - Zabezpieczanie dostępu administratora do przełącznika
- 2.4.7 Weryfikator składni - Podstawowa konfiguracja urządzenia
- 2.4.8 Sprawdź, czy zrozumiałeś - Podstawowa konfiguracja urządzenia
- 2.5 Zapisywanie konfiguracji 
- 2.6 Porty i adresy 
- 2.7 Konfiguracja adresacji IP 
- 2.8 Weryfikacja łączności 

## urządzenia



Sprawdź swoją wiedzę na temat podstawowej konfiguracji urządzenia, wybierając NAJLEPSZĄ odpowiedź na poniższe pytania.

2.9	Moduł ćwiczeń i quizu	▼
3	Protokoły i modele	▼
2	Podstawy konfiguracji	▼
2	przełącznika i urządzenia	▲
2.4	końcowego	▲
2.4	urządzeń	▲
2.4.1	Nazwy urządzeń	
2.4.2	Wytyczne dotyczące haseł	
2.4.3	Konfiguracja haseł	
2.4.4	Szyfrowanie haseł	
2.4.5	Baner - komunikaty	
2.4.6	Wideo - Zabezpieczanie dostępu	
2.4.7	administratora do przełącznika	
2.4.7	Weryfikator składni - Podstawowa	
2.4.8	konfiguracja urządzenia	
2.4.8	Sprawdź, czy zrozumiałeś -	
2.4.8	Podstawowa konfiguracja	
2.4.8	urządzenia	
2.5	Zapisywanie konfiguracji	▼
2.6	Porty i adresy	▼
2.7	Konfiguracja adresacji IP	▼
2.8	Weryfikacja łączności	▼

1. Jakie jest polecenie nadające nazwę „Sw-Floor-2” do przełącznikowi?

- ☐ **hostname** Sw-Floor-2
- ☐ **host name** Sw-Floor-2
- ☐ **name** Sw-Floor-2

2. W jaki sposób dostęp do uprzywilejowanego trybu EXEC jest zabezpieczony na przełączniku?

- ☐ **enable class**
- ☐ **secret class**
- ☐ **enable secret class**
- ☐ **service password-encryption**

3. Które polecenie umożliwia uwierzytelnianie hasła w celu uzyskania dostępu do trybu EXEC użytkownika na przełączniku?

- ☐ **enable secret**
- ☐ **login**
- ☐ **secret**
- ☐ **service password-encryption**

4. Które polecenie szyfruje dostęp do wszystkich haseł w postaci zwykłego tekstu na przełączniku?

- ☐ **enable secret**
- ☐ **login**
- ☐ **secret**
- ☐ **service password-encryption**

5. Jakie jest polecenie konfiguruje baner, który ma być wyświetlany podczas łączenia się z przełącznikiem?

- ☐ **banner \$ Keep out \$**

Sprawdź

- 2.9 Moduł ćwiczeń i quizu ▾
- 3 Protokoły i modele ▾
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego ▲
- 2.4 urządzeń ▲
- 2.4.1 Nazwy urządzeń
- 2.4.2 Wytyczne dotyczące haseł
- 2.4.3 Konfiguracja haseł
- 2.4.4 Szyfrowanie haseł
- 2.4.5 Baner - komunikaty
- 2.4.6 Wideo - Zabezpieczanie dostępu administratora do przełącznika
- 2.4.7 Weryfikator składni - Podstawowa konfiguracja urządzenia
- 2.4.8 Sprawdź, czy zrozumiałeś - Podstawowa konfiguracja urządzenia
- 2.5 Zapisywanie konfiguracji ▾
- 2.6 Porty i adresy ▾
- 2.7 Konfiguracja adresacji IP ▾
- 2.8 Weryfikacja łączności ▾

- ☐ banner motd \$ Keep out \$
- ☐ display \$ Keep out \$
- ☐ login banner \$ Keep out \$

Rozwiązanie

Resetuj

[2.3  
Struktura poleceń](#)[Zapisywanie konfiguracji](#)

2.5

