Laboratorium – Użycie wiersza poleceń w celu zebrania informacji na temat urządzeń sieciowych

Topologia

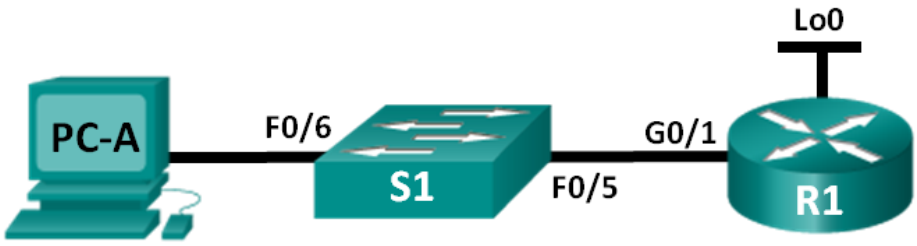


Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/1	192.168.1.1	255.255.255.0	Nie dotyczy
	Lo0	209.165.200.225	255.255.255.224	Nie dotyczy
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	Karta sieciowa	192.168.1.3	255.255.255.0	192.168.1.1

Cele

Część 1: Skonfigurowanie topologii i inicjalizacja urządzeń

- Połącz urządzenia zgodnie z topologią sieciową.
- Uruchom i zrestartuj router i przełącznik.

Część 2: Konfiguracja urządzeń i weryfikacja połączeń

- Przypisz statyczny adres IP do karty sieciowej komputera PC-A.
- Skonfiguruj podstawowe ustawienia na R1.
- Skonfiguruj podstawowe ustawienia na S1.
- Zweryfikuj połączenie sieciowe.

Część 3: Zebranie informacji na temat urządzenia sieciowego

- Wykorzystanie poleceń IOS CLI w celu zebrania informacji o R1.
- Wykorzystanie poleceń IOS CLI w celu zebrania informacji o S1.
- Wykorzystanie poleceń CLI w celu zebrania informacji o PC-A.

Scenariusz

Dokumentowanie pracy sieci jest jednym z najważniejszych zadań wykonywanych przez technika sieciowego. Odpowiednia dokumentacja zawierająca adresy IP, numery modeli urządzeń, wersje IOS, numery używanych portów oraz testy bezpieczeństwa może być bardzo pomocna w rozwiązywaniu problemów z siecią.

W tym laboratorium utworzysz małą sieć, skonfigurujesz urządzenia, ustawisz podstawowe zabezpieczenia oraz udokumentujesz konfiguracje, uzyskując informacje za pomocą wykonywania różnych poleceń na routerze, przełączniku i komputerze PC.

Uwaga: Routery używane w laboratorium to Cisco 1941 ISR (Integrated Services Routers) z oprogramowaniem Cisco IOS 15.2(4)M3 (obraz universalk9). Przełączniki używane w laboratorium to Cisco Catalyst 2960 z oprogramowaniem Cisco IOS 15.0(2) (obraz lanbasek9). Można używać innych routerów lub przełączników oraz wersji Cisco IOS. Zależnie od modelu urządzenia i wersji systemu IOS dostępne polecenia i wyniki ich działania mogą się różnic od prezentowanych w niniejszej instrukcji. Identyfikatory interfejsów znajdują się w tabeli interfejsów routerów na końcu tej instrukcji.

Uwaga: Upewnij się, że konfiguracje routerów i przełączników zostały usunięte i nie mają konfiguracji startowej. Jeśli nie jesteś pewien, poproś o pomoc instruktora.

Wymagane wyposażenie

- 1 router (Cisco 1941 z oprogramowaniem Cisco IOS, wersja 15.2(4)M3 obraz uniwersalny lub porównywalny)
- 1 przełącznik (Cisco 2960 Cisco IOS wersja15.0(2) obraz lanbasek9 lub porównywalny)
- 1 komputer PC (z systemem Windows 7, Vista, lub XP z emulatorem terminala takim jak Tera Term)
- Kable konsolowe do konfiguracji urządzeń Cisco przez port konsolowy
- Kable Ethernet zgodnie z pokazaną topologią

Część 1: Zestawienie topologii i zainicjowanie urządzeń

W części 1 będziesz skonfigurować topologię sieci, w razie potrzeby zerować konfigurację oraz konfigurować podstawowe ustawienia routera i przełącznika.

Krok 1: Połącz okablowanie zgodnie z topologią.

a. Dodaj urządzenia oraz kable wymagane, stosownie do przedstawionej topologii.

b. Włącz zasilanie wszystkich urządzeń przedstawionych w topologii.

Krok 2: Uruchom i zrestartuj router oraz przełącznik.

Część 2: Konfiguracja urządzeń i weryfikacja połączeń

W części 2 będziesz konfigurować topologię sieci oraz konfigurować podstawowe ustawienia routera i przełącznika. Nazwy urządzeń i ich adresy sprawdź w topologii i tabeli adresacji znajdujących się na początku tego laboratorium.

Uwaga: Dodatek A zawiera szczegóły konfiguracyjne poszczególnych kroków z części 2. Powinieneś spróbować zrealizować część 2 przed przejrzeniem tego dodatku.

Krok 1: Skonfiguruj adres IPv4 dla komputera PC.

Na podstawie tabeli adresacji skonfiguruj adres IPv4, maskę podsieci i adres bramy domyślnej dla komputera PC-A.

Krok 2: Skonfiguruj router.

Jeśli w kroku 2 potrzebujesz pomocy, to znajdziesz ją w załączniku A.

a. Za pomocą konsoli połącz się z routerem i przejdź do trybu uprzywilejowanego.

b. Ustaw właściwy czas na routerze.

c. Przejdź do trybu konfiguracji globalnej.
   1) W oparciu o topologię i tabelę adresacji przypisz nazwę urządzenia do routera.
   2) Wyłącz wyszukiwanie nazw domenowych (DNS lookup).
   3) Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony.
   4) Jako zaszyfrowane hasło trybu uprzywilejowanego ustaw **class**.
   5) Jako hasło dostępu do konsoli ustaw **cisco** oraz włącz logowanie.
   6) Zaszyfruj wszystkie hasła podane otwartym tekstem.
   7) Utwórz nazwę domeny **cisco.com** dla dostępu poprzez SSH.
   8) Utwórz użytkownika o nazwie **admin** z tajnym hasłem **cisco** dla dostępu poprzez SSH.
   9) Wygeneruj klucz RSA. Użyj **512** bitów.

d. Skonfiguruj linie VTY.
   1) Skorzystaj z lokalnej bazy danych do uwierzytelniania SSH.
   2) Włącz SSH tylko dla dostępu poprzez logowanie.

e. Powróć do trybu konfiguracji globalnej.
   1) Utwórz interfejs Loopback 0 i przypisz mu adres IP na podstawie tabeli adresacji.
   2) Skonfiguruj i włącz interfejs G0/1 na routerze.
   3) Skonfiguruj opisy dla interfejsu G0/1 oraz interfejsu L0.
   4) Zapisz plik konfiguracji bieżącej do pliku konfiguracji startowej.

Krok 3: Skonfiguruj przełącznik.

Jeśli w kroku 3 potrzebujesz pomocy, to znajdziesz ją w załączniku A.

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

b. Ustaw właściwy czas na przełączniku.

c. Przejdź do trybu konfiguracji globalnej.
   1) W oparciu o topologię i tabelę adresacji przypisz nazwę urządzenia do przełącznika.
   2) Wyłącz wyszukiwanie nazw domenowych (DNS lookup).
   3) Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony.
   4) Jako zaszyfrowane hasło trybu uprzywilejowanego ustaw **class**.
   5) Zaszyfruj wszystkie hasła podane otwartym tekstem.
   6) Utwórz nazwę domeny **cisco.com** dla dostępu poprzez SSH.
   7) Utwórz użytkownika o nazwie **admin** z tajnym hasłem **cisco** dla dostępu poprzez SSH.
   8) Wygeneruj klucz RSA. Użyj **512** bitów.
   9) Utwórz i aktywuj adres IP przełącznika w oparciu o topologię i tabelę adresacji.
   10) Ustaw na przełączniku bramę domyślną.
   11) Jako hasło dostępu do konsoli ustaw **cisco** oraz włącz logowanie dla konsoli.

d. Skonfiguruj linie VTY.

1) Skorzystaj z lokalnej bazy danych do uwierzytelniania SSH.
2) Włącz SSH tylko dla dostępu poprzez logowanie.
3) Wejdź do właściwego trybu aby skonfigurować opisy dla interfejsu dla F0/5 i interfejsu F0/6.
4) Zapisz plik konfiguracji bieżącej do pliku konfiguracji startowej.

Krok 4: Zweryfikuj połączenia sieciowe.

a. Z poziomu wiersza poleceń komputera PC-B wykonaj polecenie ping na adres VLAN 1 przełącznika S1. Jeżeli testy ping nie powiodły się, to rozwiąż problemy związane z konfiguracją logiczną i fizyczną.

b. Z poziomu wiersza poleceń komputera PC-B wykonaj polecenie ping do adresu IP bramy domyślnej w R1. Jeżeli testy ping nie powiodły się, to rozwiąż problemy związane z konfiguracją logiczną i fizyczną.

c. Z wiersza poleceń komputera PC-A wykonaj polecenie ping do interfejsu pętli zwrotnej w R1. Jeżeli testy ping nie powiodły się, to rozwiąż problemy związane z konfiguracją logiczną i fizyczną.

d. Przyłącz kabel konsolowy z powrotem do przełącznika i wykonaj polecenie ping do adresu IP dla G0/1 w R1. Jeżeli testy ping nie powiodły się, to rozwiąż problemy związane z konfiguracją logiczną i fizyczną.

Część 3: Zebranie informacji na temat urządzeń sieciowych

W części 3 będziesz używał różnych poleceń w celu zebrania informacji o urządzeniach w sieci oraz o ich niektórych parametrach. Dokumentacja sieci jest bardzo istotnym elementem zarządzania siecią. Dokumentacja obu topologii fizycznych i logicznych jest ważna w procesie weryfikacji modeli i wersji IOS dla urządzeń sieciowych. Posiadanie wiedzy o odpowiednich poleceniach służących do zbierania tej informacji jest podstawą pracy technika sieciowego.

Krok 1: Zbierz informacje o routerze R1 przy użyciu poleceń IOS.

Jednym z najbardziej podstawowych działań jest zbieranie informacji o urządzeniu fizycznym oraz o zainstalowanym systemie operacyjnym.

a. Wykonaj odpowiednie polecenie, aby uzyskać następujące informacje:

Model routera: _____

Wersja IOS: _____

Całkowita pojemność RAM: _____

Całkowita pojemność NVRAM: _____

Całkowita pojemność pamięci Flash: _____

Plik zawierający obraz IOS: _____

Rejestr konfiguracji: _____

Technology Package: _____

Jakiego polecenia użyłeś aby uzyskać te informacje?

_____

b. Wykonaj odpowiednie polecenie, aby wyświetlić podsumowanie ważnych informacji o interfejsach routera. Zanotuj polecenie oraz wyniki swoich badań:

Uwaga: Zapisuj tylko informacje dotyczące interfejsów posiadających adresy IP.

_____

_____

_____

_____

c. Wykonaj odpowiednie polecenie aby wyświetlić tablicę routingu. Zanotuj polecenie oraz wyniki swoich badań:

_____

_____

_____

_____

_____

_____

_____

_____

d. Jakiego polecenia należy użyć, aby wyświetlić przyporządkowanie adresów warstwy 2 do adresów warstwy 3 na routerze? Zapisz polecenie oraz swoje wyniki w poniższych rubrykach.

_____

_____

_____

_____

_____

e. Jakiego polecenia należy użyć, aby wyświetlić szczegółowe informacje na temat wszystkich interfejsów na routerze lub o określonym interfejsie? Zapisz w poniższej rubryce to polecenie.

_____

f. Cisco ma bardzo wydajny protokół, który działa na poziomie warstwy 2 modelu OSI. Protokół ten może pomóc w określaniu jak urządzenia Cisco są połączone fizycznie oraz ustalić mumery modeli, a nawet wersji IOS i adresowania IP. Jakiego polecenia lub poleceń należy użyć na routerze R1, aby wyświetlić informację o przełączniku S1 w celu wypełnienia poniższej tabeli?

ID urządzenia	interfejs lokalny	funkcjonalność	Nr modelu	ID zdalnego portu	Adres IP	Wersja systemu IOS

g. Bardzo elementarnym testem urządzeń sieciowych jest wypróbowanie, czy można się do nich podłączyć za pomocą usługi Telnet. Pamiętaj, że Telnet nie jest bezpiecznym protokołem. W większości przypadków nie powinien być aktywny. Wypróbuj usługę Telnet, aby uzyskać dostęp do R1 przy użyciu adresu IP bramy domyślnej (możesz użyć klienta Telnet w programach takich jak Tera Term lub PuTTY), Zapisz swoje wyniki w poniższej rubryce.

_____

h. Z komputera PC-A wykonaj test, aby zobaczyć, czy SSH działa prawidłowo. Używając klienta SSH (Tera Term lub PuTTY), z komputera PC-A zaloguj się poprzez SSH do R1. Jeżeli otrzymasz komunikat ostrzegający o innym kluczu, to kliknij **Continue**. Zaloguj się za pomocą odpowiedniej nazwy użytkownika i hasła utworzonego w części 2. Udało ci się?

_____

Hasła skonfigurowane na routerze powinny być silne oraz chronione przed osobami nieupoważnionymi.

Uwaga: Stosowane w naszym laboratorium hasła (**cisco** oraz **class**) nie spełniają wymogów najlepszych praktyk dla haseł silnych. Hasła te są używane wyłącznie w celu ułatwienia wykonywania ćwiczeń w laboratorium. Domyślnie skonfigurowane hasło konsoli oraz haseł VTY będzie wyświetlane w pliku konfiguracyjnym w postaci zwykłego tekstu.

i. Upewnij się, czy wszystkie hasła w pliku konfiguracyjnym zostały zaszyfrowane. Zanotuj polecenie oraz wyniki swoich badań:

Polecenie: _____

Czy hasło do konsoli jest zaszyfrowane? _____

Czy hasło do SSH jest zaszyfrowane? _____

Krok 2: Zbierz informacje o S1 przy użyciu poleceń IOS.

Wiele poleceń, których używałeś na R1 może być także stosowane na przełączniku. W przypadku niektórych poleceń są jednak pewne różnice.

a. Wydaj odpowiednie polecenie, aby uzyskać następujące informacje:

Model przełącznika: _____

Wersja IOS: _____

Całkowita pojemność pamięci NVRAM: _____

Plik obrazu IOS: _____

Jakiego polecenia użyłeś aby uzyskać te informacje?

_____

b. Wykonaj odpowiednie polecenie wyświetlające podsumowanie ważnych informacji o interfejsach przełącznika. Zanotuj polecenie oraz wyniki swoich badań.

Uwaga: Zapisuj tylko aktywne interfejsy.

_____

_____

_____

_____

_____

c. Wydaj odpowiednie polecenie, aby wyświetlić tabelę adresów MAC przełącznika. W poniższych rubrykach zapisz tylko dynamiczne adresy MAC.

_____

_____

_____

_____

d. Upewnij się, czy dostęp poprzez Telnet VTY jest wyłączony w S1. Spróbuj zalogować się za pomocą telnet 192.168.1.11 do przełącznika S1 (użyj klienta Telnet np. Tera Term lub PuTTY). Zapisz swoje wyniki w poniższej rubryce.

_____

e. Z komputera PC-A wykonaj test, aby zobaczyć, czy SSH działa prawidłowo. Używając klienta SSH (Tera Term lub PuTTY), z komputera PC-A zaloguj się poprzez SSH do S1. Jeżeli otrzymasz komunikat

ostrzegający o innym kluczu, to kliknij **Continue**. Zaloguj się z odpowiednią nazwą użytkownika i hasłem. Udało ci się?

_____

f. Uzupełnij poniższą tabelę informacjami na temat routera R1 używając odpowiedniego polecenia lub poleceń dla przełącznika S1.

ID urządzenia	interfejs lokalny	funkcjonalność	Nr modelu	ID zdalnego portu	Adres IP	Wersja systemu IOS

g. Upewnij się, czy wszystkie hasła w pliku konfiguracyjnym zostały zaszyfrowane. W poniższych rubrykach zanotuj polecenie oraz wyniki swoich badań:

Polecenie: _____

Czy hasło do konsoli jest zaszyfrowane? _____

Krok 3: Zbierz informacje na temat komputera PC-A.

Wykorzystując różne polecenia systemu Windows CLI uzyskaj informacje o komputerze PC-A.

a. W wierszu poleceń komputera PC-A wykonaj polecenie **ipconfig /all** a wyniki wpisz do poniższych rubryk.

Jaki jest adres IP komputera PC-A?

_____

Jaka jest maska podsieci komputera PC-A?

_____

Jaki jest adres bramy domyślnej dla komputera PC-A?

_____

Jaki jest adres MAC komputera PC-A?

_____

b. Wykonaj odpowiednie polecenie, aby sprawdzić stan stosu protokołów TCP/IP karty sieciowej. Jaka komenda została użyta?

_____

c. Z wiersza poleceń komputera PC-A wykonaj polecenie ping do interfejsu pętli zwrotnej w R1. Czy test ping zakończył się sukcesem?

_____

d. Wykonaj odpowiednie polecenie w PC-A aby prześledzić trasę dla pakietów wychodzących z PC-A do interfejsu pętli zwrotnej w R1. Zapisz polecenie i wyniki w poniższych rubrykach: Jakie polecenie zostało użyte?

_____

_____

e. Wykonaj odpowiednie polecenie w komputerze PC-A, aby znaleźć przypisanie adresów warstwy 2 do warstwy 3 przechowywane w twojej karcie sieciowej. Zanotuj swoje odpowiedzi w poniższych rubrykach. W poniższych rubrykach wpisz odpowiedzi tylko dla sieci 192.168.1.0/24. Jakie polecenie zostało użyte?

_____

_____

_____

_____

Do przemyślenia

Dlaczego tak ważne jest, aby dokumentować swoje urządzenia sieciowe?

_____

_____

_____

_____

_____

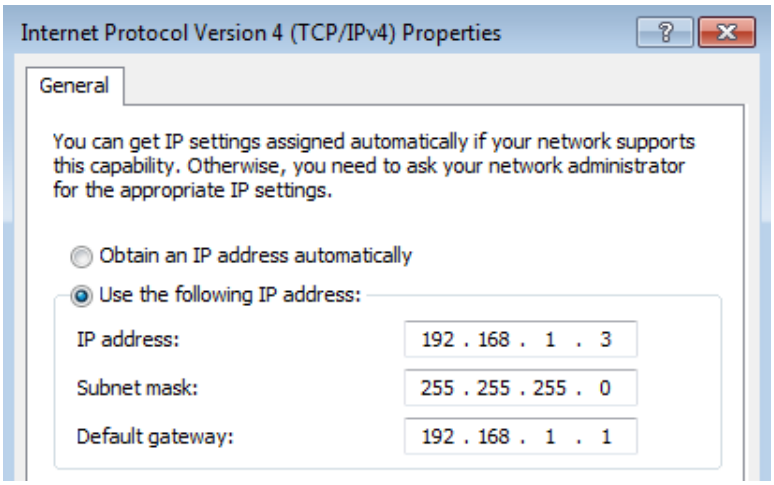
Tabela zbiorcza interfejsów routera

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 stwierdzić jak router jest skonfigurowany, spójrz na interfejsy aby zidentyfikować typ routera oraz liczbę jego interfejsów. Nie ma sposobu na skuteczne opisanie wszystkich kombinacji konfiguracji dla każdej klasy routera. Ta tabela zawiera identyfikatory możliwych kombinacji interfejsów Ethernet i Serial w urządzeniu. W tabeli nie podano żadnych innych rodzajów interfejsów, mimo iż dany router może być w nie wyposażony. Przykładem takiej sytuacji może być interfejs ISDN BRI. Informacja w nawiasach jest dozwolonym skrótem, którego można używać w poleceniach IOS w celu odwołania się do interfejsu.				

Dodatek A: Szczegółowa konfiguracja dla kroków w części 2

Krok 1: Skonfiguruj adres IPv4 dla komputera PC.

Na podstawie tabeli adresacji znajdującej się na początku tego laboratorium, skonfiguruj adres IPv4, maskę podsieci oraz adres bramy domyślnej dla komputera PC-A.



Krok 2: Skonfiguruj router.

a. Za pomocą konsoli połącz się z routerem i przejdź do trybu uprzywilejowanego.

```
Router> enable
Router#
```

b. Ustaw właściwy czas na routerze.

```
Router# clock set 10:40:30 6 February 2013
Router#
```

c. Przejdź do trybu konfiguracji globalnej.

```
Router# config t
Router(config)#
```

1) Przypisz nazwę do routera. Użyj topologii i tabeli adresacji.

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

2) Wyłącz wyszukiwanie nazw domenowych (DNS lookup).

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

3) Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony.

```
R1(config)# banner motd #Warning! Unauthorized Access is prohibited.#
```

4) Jako zaszyfrowane hasło trybu uprzywilejowanego ustaw **class**.

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

5) Jako hasło dostępu do konsoli ustaw **cisco** oraz włącz logowanie dla konsoli.

```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
```

6) Zaszyfruj wszystkie hasła podane otwartym tekstem.

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

7) Utwórz nazwę domeny **cisco.com** dla dostępu poprzez SSH.

```
R1(config)# ip domain-name cisco.com
```

8) Utwórz użytkownika o nazwie **admin** z tajnym hasłem **cisco** dla dostępu poprzez SSH.

```
R1(config)# username admin secret cisco
```

9) Wygeneruj klucz RSA. Użyj **512** bitów.

```
R1(config)# crypto key generate rsa modulus 512
```

d. Skonfiguruj dostęp do linii VTY.

1) Użyj lokalnej bazy danych do uwierzytelniania SSH.

```
R1(config)# line vty 0 4
R1(config-line)# login local
```

2) Włącz SSH tylko dla dostępu poprzez logowanie.

```
R1(config-line)# transport input ssh
```

e. Powróć do trybu konfiguracji globalnej.

```
R1(config-line)# exit
```

1) Utwórz interfejs Loopback 0 i przypisz jej adres IP na podstawie tabeli adresacji.

```
R1(config)# interface loopback 0
R1(config-if)# ip address 209.165.200.225 255.255.255.224
```

2) Skonfiguruj i włącz interfejs G0/1 na routerze.

```
R1(config-if)# int g0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shut
```

3) Skonfiguruj opisy dla interfejsu G0/1 oraz interfejsu L0.

```
R1(config-if)# description Connected to LAN
R1(config-if)# int lo0
R1(config-if)# description Emulate ISP Connection
```

4) Zapisz plik konfiguracji bieżącej do pliku konfiguracji startowej.

```
R1(config-if)# end
R1# copy run start
```

Krok 3: Skonfiguruj przełącznik.

a. W linii poleceń konsoli przełącznika przejdź do trybu uprzywilejowanego EXEC.

```
Switch> enable
Switch#
```

b. Ustaw właściwy czas na przełączniku.

```
Switch# clock set 10:52:30 6 February 2013
```

c. Przejdź do trybu konfiguracji globalnej.

```
Switch# config t
```

1) W oparciu o topologię i tabelę adresacji przypisz nazwę urządzenia do przełącznika.

```
Switch(config)# hostname S1
```

2) Wyłącz wyszukiwanie nazw domenowych (DNS lookup).

```
S1(config)# no ip domain-lookup
```

3) Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony.

```
S1(config)# banner motd #Warning! Unauthorized access is prohibited.#
```

4) Jako zaszyfrowane hasło trybu uprzywilejowanego ustaw **class**.

```
S1(config)# enable secret class
```

5) Zaszyfruj wszystkie hasła podane otwartym tekstem.

```
S1(config)# service password-encryption
```

6) Utwórz nazwę domeny **cisco.com** dla dostępu poprzez SSH.

```
S1(config)# ip domain-name cisco.com
```

7) Utwórz użytkownika o nazwie **admin** z tajnym hasłem **cisco** dla dostępu poprzez SSH.

```
S1(config)# username admin secret cisco
```

8) Wygeneruj klucz RSA. Użyj **512** bitów.

```
S1(config)# crypto key generate rsa modulus 512
```

9) Utwórz i aktywuj adres IP przełącznika w oparciu o topologię i tabelę adresacji.

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

10) Ustaw na przełączniku bramę domyślną.

```
S1(config)# ip default-gateway 192.168.1.1
```

11) Jako hasło dostępu do konsoli ustaw **cisco** oraz włącz logowanie dla konsoli.

```
S1(config-if)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
```

d. Skonfiguruj dostęp do linii VTY.

1) Skorzystaj z lokalnej bazy danych do uwierzytelniania SSH.

```
S1(config-line)# line vty 0 15
S1(config-line)# login local
```

2) Włącz SSH tylko dla dostępu poprzez logowanie.

```
S1(config-line)# transport input ssh
```

3) Wejdź do właściwego trybu, aby skonfigurować opisy dla interfejsu F0/5 i dla interfejsu F0/6.

```
S1(config-line)# int f0/5
S1(config-if)# description Connected to R1
S1(config-if)# int f0/6
S1(config-if)# description Connected to PC-A
```

4) Zapisz plik konfiguracji bieżącej do pliku konfiguracji startowej.

```
S1(config-if)# end
S1# copy run start
```