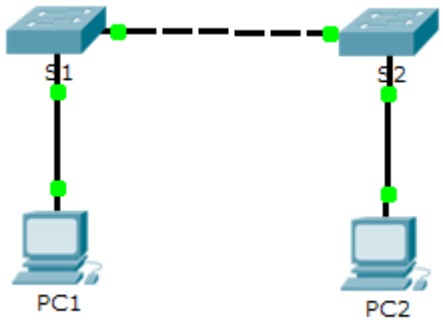
Packet Tracer - Konfiguracja ustawień początkowych przełącznika

Topologia



Cele

Część 1: Sprawdzenie domyślnej konfiguracji przełącznika.

Część 2: Konfiguracja podstawowych ustawień przełącznika.

Część 3: Konfiguracja wiadomości MOTD.

Część 4: Zapisanie plików konfiguracyjnych w pamięci NVRAM.

Część 5: Konfiguracja S2.

Wprowadzenie

W tym ćwiczeniu, będziesz wykonywać podstawową konfiguracje przełącznika. Można zabezpieczyć dostęp do interfejsu wiersza poleceń (CLI) i portów konsoli przy użyciu zaszyfrowanych i nieszyfrowanych haseł. Dowiesz się również, jak skonfigurować wiadomości dla użytkowników logujących się do przełącznika. Te wiadomości są również używane, aby ostrzec, że dostęp nieuprawnionych użytkowników jest zabroniony.

Część 1: Sprawdzenie domyślnej konfiguracji przełącznika

Krok 1: Przechodzenie do trybu uprzywilejowanego.

W tym trybie masz dostęp do wszystkich komend przełącznika. Ze względu na fakt, iż wiele komend dostępnych w trybie uprzywilejowanym dotyczy konfiguracji przełącznika, tryb ten powinien być zabezpieczony hasłem dostępowym.

W zestawie poleceń trybu użytkownika uprzywilejowanego dostępne jest między innymi polecenie **configure** umożliwiające uzyskanie dostępu do pozostałych trybów poleceń.

a. Kliknij na **S1**, a następnie na zakładkę **CLI**. Wciśnij **<Enter>**.

b. Wejdź do trybu uprzywilejowanego EXEC poprzez wprowadzenie komendy **enable**

```
Switch>enable
Switch#
```

Należy zwrócić uwagę na zmianę symbolu zachęty (z > na #) odzwierciedlającą przejście do uprzywilejowanego trybu EXEC.

Krok 2: Sprawdzenie bieżącej konfiguracji przełącznika.

a. Wpisz polecenie **show running-config**.

```
Switch# show running-config
```

b. Odpowiedz na następujące pytania:

Ile interfejsów FastEthernet ma przełącznik? _____

Ile interfejsów Gigabit Ethernet posiada przełącznik? _____

Jaki jest zakres wartości linii VTY? _____

Jakie polecenie wyświetla bieżącą zawartość pamięci NVRAM?

_____

Dlaczego przełącznik zwraca `startup-config is not present` ?

_____

_____

Część 2: Stworzenie podstawowej konfiguracji przełącznika

Krok 1: Przypisanie nazwy do przełącznika.

Aby skonfigurować parametry przełącznika, może zaistnieć konieczność poruszania się pomiędzy różnymi trybami konfiguracyjnymi. Zobacz, jak zmienia się znak zachęty, podczas gdy poruszasz się po systemie w przełączniku.

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# exit
S1#
```

Krok 2: Zabezpieczenie dostępu z linii konsolowej.

Aby zabezpieczyć dostęp do linii konsoli, wybierz tryb config-line i ustaw hasło na **letmein**

```
S1# configure terminal
Wprowadź polecenia konfiguracyjne, podając w każdym wierszu tylko jedno polecenie. Zakończ za pomocą CNTL/Z.
S1(config)# line console 0
S1(config-line)# password letmein
S1(config-line)# login
S1(config-line)# exit
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Dlaczego jest wymagane polecenie **login**?

_____

Krok 3: Sprawdzanie czy dostęp przez port konsolowy jest zabezpieczony.

Wyjdź z trybu uprzywilejowanego, aby sprawdzić, czy hasło na port konsoli jest nałożone.

```
S1# exit
Switch con0 is now available
```

```
Press RETURN to get started.

User Access Verification
Password:
S1>
```

Uwaga: Jeśli przełącznik nie poprosi o hasło, to nie skonfigurowałeś parametru **login** w kroku 2.

Krok 4: Zabezpieczenie dostępu do trybu uprzywilejowanego.

Ustaw **enable password** jako **c1$c0**. To hasło chroni dostępu do trybu uprzywilejowanego.

Uwaga: Znak **0** w **c1$c0** jest cyfrą, a nie dużą literą O. To hasło może nie być ocenione przez Packet Tracer jako poprawne dopóki nie zaszyfrujesz go w kroku 8.

```
S1> enable
S1# configure terminal
S1(config)# enable password c1$c0
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Krok 5: Upewnienie się, że dostęp do trybu uprzywilejowanego jest zabezpieczony.

a. Wpisz **exit** ponownie i wyloguj się z przełącznika.

b. Wciśnij**<Enter>** i teraz powinieneś ponownie zostać zapytany o hasło:

```
User Access Verification
Password:
```

c. Pierwsze hasło to hasło do konsoli, które zostało skonfigurowane dla **line con 0**. Wpisz to hasło, a znajdziesz się w trybie użytkownika EXEC.

d. Przejdź do trybu uprzywilejowanego EXEC.

e. Wprowadź drugie hasło skonfigurowane do ochrony trybu uprzywilejowanego EXEC.

f. Sprawdź swoje konfiguracje analizując zawartość pliku running-config:

```
S1# show running-configuration
```

Zauważ, że oba hasła (konsoli i trybu uprzywilejowanego) wyświetlane są w postaci jawnego tekstu. Może to stanowić zagrożenie dla bezpieczeństwa, jeśli ktoś spogląda Ci przez ramię.

Krok 6: Konfiguracja zaszyfrowanego hasła w celu zabezpieczenia dostępu do trybu uprzywilejowanego.

Polecenie **enable password** należy zastąpić nowszym zaszyfrowanym tajnym hasłem używając polecenia **enable secret** . Ustaw hasło jako **itsasecret**.

```
S1# config t
S1(config)# enable secret itsasecret
S1(config)# exit
S1#
```

Uwaga: Polecenie **enable secret** zastępuje polecenie **enable password**. Jeżeli obie są skonfigurowane na przełączniku, aby wejść do trybu uprzywilejowanego musisz wprowadzić hasło podane dla polecenia **enable secret**.

Krok 7: Sprawdzenie czy hasło jest dodane do pliku konfiguracyjnego.

a. Wpisz ponownie polecenie **show running-configuration** i sprawdź czy hasło **enable secret** jest skonfigurowane.

Uwaga: Możesz skrócić polecenie **show running-configuration** do

```
S1# show run
```

b. Jak jest wyświetlane hasło **enable secret** ? _____

Dlaczego hasło **enable secret** jest inaczej wyświetlane niż to poprzednie?

_____

Krok 8: Szyfrowanie hasła do konsoli i skonfigurowanego poleceniem enable password.

Jak mogłeś zauważyć w kroku 7, hasło **enable secret** jest szyfrowane, ale hasła **enable** i **console** są nadal zapisane jawnym tekstem. Można szyfrować te hasła używając polecenia **service password-encryption.**

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

Czy w przypadku konfigurowania kolejnych haseł na przełączniku, zostaną one wyświetlone w pliku konfiguracyjnym jako jawny tekst lub w formie zaszyfrowanej? Wyjaśnij, dlaczego?

_____

Część 3: Konfiguracja wiadomości MOTD

Krok 1: Konfiguracja wiadomości dnia (MOTD banner).

W zestawie poleceń systemu Cisco IOS dostępne jest polecenie umożliwiające skonfigurowanie wiadomości, które będą wyświetlane każdej logującej się osobie. Wiadomości te są określane terminem banerów logowania lub banerów MOTD (message of the day – wiadomość dnia). Tekst stanowiący treść banera należy ująć w cudzysłów lub otoczyć znakami innymi niż jakikolwiek ze znaków występujących w treści banera.

```
S1# config t
S1(config)# banner motd "This is a secure system. Authorized Access Only!"
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Kiedy zostanie wyświetlony ten baner?

_____

Dlaczego każdy przełącznik powinien mieć baner MOTD?

_____

_____

_____

Część 4: Zapisanie plików konfiguracyjnych do pamięci NVRAM

Krok 1: Upewnienie się za pomocą polecenia "show run", że konfiguracja została wykonana.

Krok 2: Zapisanie konfiguracji.

Właśnie ukończyłeś podstawową konfigurację przełącznika. Teraz utwórz kopię zapasową pliku konfiguracyjnego do pamięci NVRAM, aby zapewnić, że wprowadzone zmiany nie zostaną utracone w przypadku restartu systemu lub braku prądu.

```
S1# copy running-config startup-config
Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
```

Jaka jest najkrótsza postać polecenia **copy running-config startup-config**?

_____

Krok 3: Sprawdzenie pliku konfiguracji startowej.

Które polecenie wyświetli zawartość pamięci NVRAM? _____

Czy wszystkie wprowadzone zmiany są zarejestrowane w tym pliku? _____

Część 5: Konfiguracja S2

Zakończyłeś konfigurację przełącznika S1. Teraz rozpoczniesz konfigurację przełącznika S2. Jeśli nie pamiętasz poleceń, spójrz do część 1 - 4 w celu uzyskania pomocy.

Skonfiguruj S2 według następujących parametrów:

a. Nazwa urządzenia: **S2**

b. Zabezpieczenie konsoli używając hasła **letmein** .

c. Skonfiguruj enable password jako **c1$c0** oraz enable secret password jako **itsasecret**.

d. Skonfiguruj wiadomość do tych, którzy logują się do przełącznika z następującym komunikatem:

```
Authorized access only. Unauthorized access is prohibited and violators
will be prosecuted to the full extent of the law.
```

e. Zaszyfruj wszystkie hasła.

f. Upewnij się, że konfiguracja jest poprawna.

g. Zapisz plik konfiguracyjny, aby uniknąć utraty nie zapisanych danych w przypadku wyłączenia przełącznika.

Rubryka sugerowanej punktacji

Sekcja ćwiczenia	Położenie pytań	Maksymalna liczba punktów do uzyskania	Uzyskana liczba punktów
Część 1: Sprawdzenie domyślnej konfiguracji przełącznika	Krok 2b, q1	2	
	Krok 2b, q2	2	
	Krok 2b, q3	2	
	Krok 2b, q4	2	
	Krok 2b, q5	2	
Część 1 łącznie		**10**	
Część 2: Stworzenie podstawowej konfiguracji przełącznika	Krok 2	2	
	Step 7b	2	
	Krok 7c	2	
	Krok 8	2	
Część 2 łącznie		**8**	
Część 3: Konfigurowanie baneru MOTD	Krok 1, q1	2	
	Krok 1, q2	2	
Część 3 łącznie		**4**	
Część 4: Zapisanie plików konfiguracyjnych w pamięci NVRAM	Krok 2	2	
	Krok 3, q1	2	
	Krok 3, q2	2	
Część 4 łącznie		**6**	
Punktacja Packet Tracer		**72**	
Wynik łączny		**100**	