Packet Tracer - Konfiguracja ustawień początkowych przełączników

Cele

Część 1: Sprawdzenie domyślnej konfiguracji przełącznika

Część 2: Konfiguracja podstawowych ustawień przełącznika

Część 3: Konfigurowanie banneru MOTD

Część 4: Zapisanie plików konfiguracyjnych w pamięci NVRAM

Część 5: Konfiguracja S2

Wprowadzenie

W tym ćwiczeniu, będziesz wykonywać podstawową konfiguracje przełącznika. Będzie można zabezpieczyć dostęp do interfejsu wiersza poleceń (CLI) i portów konsoli przy użyciu zaszyfrowanych i jawnych 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.

Uwaga: W Packet Tracer przełącznik Catalyst 2960 domyślnie korzysta z IOS w wersji 12.2. W razie potrzeby wersję IOS można zaktualizować z serwera plików w topologii PT. Przełącznik można następnie skonfigurować do uruchamiania systemu IOS w wersji 15.0, jeśli ta wersja jest wymagana.

Instrukcje

Część 1: Sprawdzenie domyślnej konfiguracji przełącznika

Krok 1: Przejdź do uprzywilejowanego trybu EXEC.

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

Tryb poleceń uprzywilejowanych EXEC obejmuje komendy dostępne w trybie EXEC użytkownika, wiele dodatkowych komend oraz komendę **configure**, dzięki której uzyskuje się dostęp do trybów konfiguracji.

a. Kliknij na S1, a następnie na zakładkę CLI. Naciśnij klawisz Enter.

b. Wejdź do trybu uprzywilejowanego EXEC poprzez wprowadzenie komendy enable

```
Switch> enable
Switch#
```

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

Krok 2: Sprawdzenie bieżącej konfiguracji przełącznika.

Wpisz polecenie show running-config.

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

Odpowiedz na następujące pytania:

Ile interfejsów Fast Ethernet posiada przełącznik?

Ile interfejsów Gigabit Ethernet posiada przełącznik?

Jaki jest zakres wartości linii vty?

Które polecenie wyświetli bieżącą zawartość nieulotnej pamięci o dostępie swobodnym (NVRAM)?

Dlaczego przełącznik odpowiada “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 w szybki sposób poruszać się w przełączniku.

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

Krok 2: Zabezpieczenie dostępu z linii konsolowej.

Aby zabezpieczyć dostęp z linii konsoli, wybierz tryb config-line i ustaw hasło na **letmain**.

```
S1# configure terminal
Enter configuration commands, one per line. End with 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 wymagana jest komenda **login**?

Krok 3: Sprawdzanie czy dostęp przez konsolę jest zabezpieczony.

Wyjdź z trybu uprzywilejowanego, aby sprawdzić, czy hasło 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 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: Upewnij się, że dostęp do trybu uprzywilejowanego jest zabezpieczony.

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

b. Naciśnij **<Enter>**, a zostaniesz poproszony o podanie hasła:

```
User Access Verification
Password:
```

c. Pierwszym hasłem jest hasło konsoli, które zostało skonfigurowane dla **linie con 0**. Wpisz hasło i powróć do trybu user EXEC.

d. Przejdź do trybu uprzywilejowanego.

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

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

```
S1# show running-config
```

Zauważ, że oba hasła (konsoli i enable) są w postaci jawnego tekstu. Może to stanowić zagrożenie bezpieczeństwa, jeśli ktoś patrzy ci przez ramię lub uzyskuje dostęp do plików konfiguracyjnych przechowywanych w lokalizacji kopii zapasowej.

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 oba są skonfigurowane na przełączniku, musisz wprowadzić **enable secret**, aby wejść do trybu uprzywilejowanego EXEC**.**

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

Wpisz ponownie polecenie show running-config i sprawdź czy hasło enable secret jest skonfigurowane.

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

```
S1# show run
```

Co jest wyświetlane dla enable secret?

Dlaczego tajne hasło jest wyświetlane inaczej niż to, co skonfigurowaliśmy?

Krok 8: Szyfrowanie hasła enable i konsolowego.

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
```

Jeśli skonfigurujesz więcej haseł na przełączniku, czy będą one wyświetlane w pliku konfiguracyjnym jako zwykły tekst czy w postaci zaszyfrowanej? Wyjaśnij.

Część 3: Konfiguracja banera MOTD.

Krok 1: Skonfiguruj wiadomość dnia (MOTD) banner.

W zbiorze poleceń systemu Cisco IOS dostępne jest polecenie umożliwiające skonfigurowanie wiadomości, które będą wyświetlane każdej osobie logującej się do przełącznika. 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 będzie wyświetlany ten baner?

Dlaczego każdy przełącznik powinien mieć baner MOTD?

Część 4: Zapisanie plików konfiguracyjnych do pamięci NVRAM i weryfikacja

Krok 1: Upewnij się, że konfiguracja jest ustawiona za pomocą polecenia show run.

Zapisz konfigurację. 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 wersja polecenia **copy running-config startup-config**?

Sprawdź plik konfiguracji startowej.

Które polecenie wyświetli zawartość pamięci NVRAM?

Czy wszystkie wprowadzone zmiany są zarejestrowane wtym 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. Zabezpiecz konsolę używając hasła **letmein**.

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

d. Skonfiguruj odpowiednią wiadomość dla tych, którzy logują się do przełącznika.

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.