Packet Tracer - Realizacja podstawowej łączności

# Tabela adresowania

|  |  |  |  |
| --- | --- | --- | --- |
| Urządzenie | Interfejs | Adres IP | Maska podsieci |
| S1 | VLAN 1 | 192.168.1.253 | 255.255.255.0 |
| S2 | VLAN 1 | 192.168.1.254 | 255.255.255.0 |
| PC1 | karta sieciowa | 192.168.1.1 | 255.255.255.0 |
| PC2 | karta sieciowa | 192.168.1.2 | 255.255.255.0 |

# Cele

**Część 1: Wykonanie podstawowej konfiguracji dla S1 i S2**

**Część 2: Konfiguracja komputerów**

**Część 3: Konfiguracja interfejsu zarządzania przełącznikiem**

# Wprowadzenie

W tym ćwiczeniu najpierw utworzysz podstawową konfigurację przełącznika. Następnie uruchomisz podstawową łączność poprzez skonfigurowanie adresów IP przełączników i komputerów. Po zakończeniu konfiguracji adresowania IP będziesz wykorzystywać różne opcje polecenia **show** w celu jej weryfikacji. Ostatecznie, aby sprawdzić poprawność podstawowego połączenia wykorzystasz komendę **ping**.

# Instrukcje

## Wykonanie podstawowej konfiguracji dla S1 i S2

Wykonaj następujące kroki na S1 i S2.

### Skonfiguruj nazwę (hostaname) na S1.

* + - 1. Kliknij na S1, a następnie przejdź do zakładki CLI .
      2. Użyj odpowiednich komend aby skonfigurować nazwę urządzenia jako S1.

### Skonfiguruj hasła konsoli oraz trybu uprzywilejowanego EXEC.

* + - 1. Użyj słowa **cisco** jako hasła dostępu do konsoli.
      2. Zastosuj słowo **class** jako hasło dostępu do trybu uprzywilejowanego EXEC.

### Sprawdź konfigurację haseł dla S1.

#### Pytanie:

W jaki sposób można sprawdzić, czy oba hasła zostały poprawnie skonfigurowane?

show running-config

Wprowadź swoją odpowiedź tutaj

### Konfiguracja banera MOTD.

Ustaw odpowiedni tekst banera, który będzie ostrzegał osoby przed nieautoryzowanym dostępem. W tym celu możesz np. wykorzystać poniższy tekst:

**Authorized access only. Violators will be prosecuted to the full extent of the law.**

### Zapisz plik konfiguracyjny do pamięci NVRAM.

#### Pytanie:

Jakie polecenie należy wydać, aby wykonać ten krok?

**copy running-config startup-config**

Wprowadź swoją odpowiedź tutaj

### Powtórz kroki od 1 do 5 dla S2.

## Skonfiguruj komputery PC.

Skonfiguruj PC1 i PC2 z odpowiednimi adresami IP.

### Skonfiguruj oba komputery z odpowiednimi adresami IP.

* + - 1. Kliknij na PC1, a następnie na zakładkę Desktop.
      2. Kliknij na IP Configuration. W zamieszczonej powyżej tablicy adresacji możesz przeczytać, że PC1 ma przydzielony adres IP 192.168.1.1 oraz maskę podsieci 255.255.255.0. Wykorzystaj te informacje aby skonfigurować PC1 przy pomocy opcji znajdujących się w oknie IP Configuration .
      3. Powtórz kroki 1a i 1b dla PC2.

### Przetestuj poprawność połączeń do przełączników.

* + - 1. Kliknij PC1. Zamknij okno IP Configuration , jeżeli pozostało ono nadal otwarte. W zakładce Desktop kliknij na opcji Command Prompt.
      2. Wpisz komendę **ping** z adresem IP przełącznika S1, a następnie wciśnij klawisz Enter.

Packet Tracer PC Command Line 1.0

PC> **ping 192.168.1.253**

#### Pytanie:

Udało ci się? Wyjaśnij.

Nie udało się gdyż, nie skonfigurowaliśmy adresu IP na przełączniku.

Wprowadź swoją odpowiedź tutaj.

## Konfiguracja interfejsu zarządzania przełącznikiem

Skonfiguruj S1 i S2 z odpowiednimi adresami IP.

### Skonfiguruj S1 z odpowiednim adresem IP.

Przełączniki mogą być używane jako urządzenia typu plug-and-play. Oznacza to, że nie trzeba ich konfigurować, aby działały. Przełączniki przesyłają informacje pomiędzy swoimi portami wykorzystując adresację MAC.

#### Pytanie:

Jeśli tak jest, to dlaczego mielibyśmy je konfigurować z adresem IP?

Aby tworzyć Vlany i kontrolować przesył pakietów pomiędzy poszczególnymi hostami oraz nie dopuszczać aby dostęp do pakietów miały osoby z poza danego vlanu.

Wprowadź swoją odpowiedź tutaj

Użyj następujących poleceń, aby skonfigurować S1 z adresem IP.

S1# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)# **interface vlan 1**

S1(config-if)# **ip address 192.168.1.253 255.255.255.0**

S1(config-if)# **no shutdown**

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1 (config-if) #

S1(config-if)# **exit**

S1#

#### Pytanie:

Dlaczego wprowadzasz polecenie **no shutdown**?

Aby włączyć interfejs.

Wprowadź swoją odpowiedź tutaj.

### Skonfiguruj adres IP na S2.

Użyj informacji w tabeli adresowania, aby skonfigurować S2 z adresem IP.

### Sprawdź konfigurację adresu IP na S1 i S2.

Wykorzystaj komendę **show ip interface brief**, aby wyświetlić adresy IP oraz status wszystkich interfejsów oraz portów dostępnych na przełączniku. Alternatywnie, można również użyć polecenia **show running-config**.

### Zapisz konfiguracje dla S1 i S2 w pamięci NVRAM.

#### Pytanie:

Które polecenie jest używane, aby zapisać plik konfiguracyjny z pamięci RAM do pamięci NVRAM?

**copy running-config startup-config**

Wprowadź swoją odpowiedź tutaj

### Sprawdzanie połączenia sieci.

Łączność w sieci może być sprawdzona za pomocą polecenia **ping**. Sprawdzenie poprawnej łączności w sieci jest bardzo ważnym elementem w procesie konfiguracji urządzeń. Jeśli wystąpią jakiekolwiek problemy z łącznością, należy podjąć odpowiednie czynności korygujące. Wykonaj ping S1 i S2 z PC1 i PC2.

* + - 1. Kliknij na PC1, a następnie na zakładkę Desktop.
      2. Kliknij na Command Prompt.
      3. Wykonaj ping na adres IP PC2.
      4. Wykonaj ping na adres IP S1.
      5. Wykonaj ping na adres IP S2.

**Uwaga**: Możesz również użyć tego samego polecenia **ping** w CLI przełącznika jak i PC2.

Wykonanie poleceń powinno zakończyć się sukcesem. Jeśli Twój pierwszy wynik ping wynosi 80%, spróbuj ponownie. Powinien wynosić 100%. Dowiesz się, dlaczego polecenie ping może czasami zakończyć się niepowodzeniem przy pierwszym testowaniu. Jeśli wykonanie ping kończy się niepowodzeniem dla któregoś urządzenia, sprawdź konfigurację czy nie ma w niej błędów.

W Cisco Packet Tracer „Check Results” pokazuje błąd przy „Enable Secrets” natomiast w treści zadania takie polecenie nie występuje!

Koniec dokumentu