

Metody przesyłania konfiguracji na nowoczesnych przełącznikach Cisco:

1. TFTP (Trivial File Transfer Protocol):

- **TFTP** jest wciąż powszechnie używany, zwłaszcza w prostych scenariuszach do przesyłania konfiguracji i plików obrazu systemu operacyjnego. Jest łatwy w konfiguracji, ale ma ograniczone funkcje, takie jak brak szyfrowania i uwierzytelniania.
- TFTP jest wciąż stosowany w środowiskach, gdzie prostota i łatwość konfiguracji mają większe znaczenie niż bezpieczeństwo.

2. FTP (File Transfer Protocol):

- **FTP** jest bardziej zaawansowaną alternatywą dla TFTP. Wspiera uwierzytelnianie i jest bardziej bezpieczny niż TFTP, choć nie zapewnia szyfrowania (chyba że używasz FTPS, co jest bezpieczniejszą wersją FTP z obsługą SSL/TLS).
- Możesz używać FTP do kopiowania konfiguracji na przełącznikach Cisco, szczególnie w bardziej złożonych środowiskach.

3. SFTP (Secure File Transfer Protocol):

- **SFTP** to rozszerzenie **SSH** (Secure Shell) i oferuje **bezpieczne przesyłanie plików**. Współczesne przełączniki Cisco obsługują SFTP, co zapewnia szyfrowanie podczas transferu plików, co jest szczególnie ważne w środowiskach produkcyjnych, gdzie bezpieczeństwo danych jest kluczowe.
- Jest to bezpieczniejsza opcja niż FTP i TFTP, ponieważ zapewnia zarówno uwierzytelnianie, jak i szyfrowanie.

4. SCP (Secure Copy Protocol):

- **SCP** to kolejna metoda oparta na SSH, która zapewnia bezpieczne przesyłanie plików. Jest to bardziej wydajny i bezpieczny sposób niż FTP lub TFTP.
- SCP jest szeroko używany w środowiskach, które korzystają z **SSH** do zarządzania urządzeniami, zapewniając szybki i bezpieczny transfer plików.

5. USB (Universal Serial Bus):

- **USB** jest również popularnym sposobem przesyłania plików konfiguracji na nowoczesnych przełącznikach Cisco. Można podłączyć nośnik USB do

przetącznika i używać komend takich jak `copy usb0:/config.txt running-config` do załadowania konfiguracji z pliku zapisane na USB.

- Ta metoda jest przydatna w przypadku, gdy urządzenia sieciowe znajdują się w miejscach, gdzie nie ma dostępu do sieci.

Przykłady komend dla różnych metod

TFTP:

```
Switch# copy running-config tftp:  
Address or name of remote host []? 192.168.1.100  
Destination filename [switch-config]?
```

FTP:

```
Switch(config)# ip ftp username cisco  
Switch(config)# ip ftp password P@ssw0rd123
```

```
Switch# copy running-config ftp:  
Address of remote host? 192.168.1.100  
Destination filename? switch-config
```

SFTP:

```
Switch# copy running-config sftp:  
Address or name of remote host? 192.168.1.100  
Username? cisco  
Password? ****  
Destination filename? switch-config
```

SCP:

```
Switch# copy running-config scp:  
Address of remote host? 192.168.1.100  
Username? cisco  
Password? ****  
Destination filename? switch-config
```

USB:

```
Switch# copy usb0:/config.txt running-config
```

Podsumowanie

Choć **TFTP** wciąż jest stosowane w wielu środowiskach, współczesne przetączniki Cisco oferują bardziej zaawansowane metody transferu plików, takie jak **SFTP**, **SCP** czy **FTP**. Wybór metody zależy głównie od wymagań bezpieczeństwa i wygody administracyjnej:

- **TFTP** jest prostsze, ale mniej bezpieczne.
- **FTP**, **SFTP** i **SCP** zapewniają lepsze bezpieczeństwo i szyfrowanie.
- **USB** to dobra opcja, gdy nie ma dostępu do sieci.

W dzisiejszych czasach w środowiskach produkcyjnych, gdzie bezpieczeństwo jest kluczowe, **SFTP** i **SCP** są preferowanymi metodami przesyłania plików konfiguracyjnych.