Laboratorium - Stosowanie TFTP, Flash i USB do zarządzania plikami konfiguracyjnymi

Topologia

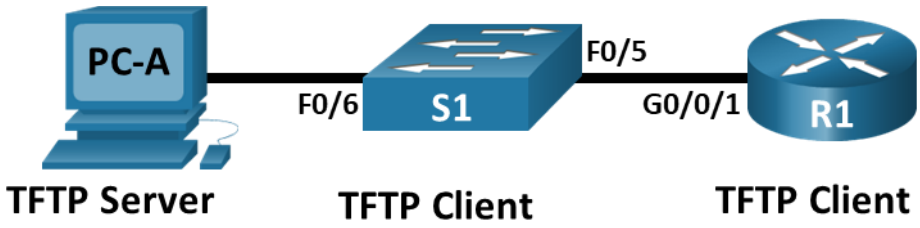

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/0/1	192.168.1.1	255.255.255.0	Brak danych
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: Utworzenie sieci oraz konfigurowanie podstawowych ustawień urządzenia

Część 2: Korzystanie z serwera TFTP do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych przełącznika

Część 3: Korzystanie z serwera TFTP do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych routera

Część 4: Tworzenie kopii zapasowych i przywracania plików konfiguracji routera przy użyciu pamięci flash

Część 5: (opcjonalna) Użycie dysku USB do tworzenia kopii zapasowych i przywracania plików konfiguracji bieżącej

Tło / scenariusz

Urządzenia sieciowe Cisco są często aktualizowane lub jest zmieniane oprogramowanie z wielu różnych powodów. Należy pamiętać, aby zapisywać kopie najnowszych konfiguracji urządzenia oraz historię zmian konfiguracyjnych. W sieciach produkcyjnych często używa się serwera TFTP do tworzenia kopii zapasowych plików konfiguracyjnych i obrazów IOS. Serwer TFTP zapewnia scentralizowane i bezpieczne metody używane do przechowywania kopii zapasowych plików i przywrócenia ich w razie potrzeby. Za pomocą scentralizowanego serwera TFTP, można wykonać kopię zapasową plików z wielu różnych urządzeń Cisco.

Większość obecnych routerów Cisco, prócz wykorzystania serwera TFTP, może wykonywać kopię zapasowe i przywracanie plików z lokalnych mediów jak np. pamięci CompactFlash (CF) lub dysku flash USB. Pamięć CF jest to wymienny moduł pamięci, który zastąpił ograniczoną wewnętrzną pamięć flash stosowaną we

wcześniejszych modelach routerów. Obraz IOS routera zapisany jest w pamięci CF, natomiast router używa tego obrazu IOS w procesie rozruchu systemu operacyjnego. W przypadku stosowania pamięci CF o większej pojemności, można w niej zapisywać dodatkowe pliki w celach archiwizacji. Wymienny dysk USB flash także może być wykorzystany do celów archiwizacji.

W tym laboratorium użyjesz oprogramowania serwera TFTP do wykonania kopii zapasowej uruchomionej konfiguracji urządzenia Cisco na serwerze TFTP. Edycję pliku możesz wykonać za pomocą edytora tekstu i skopiować nową konfigurację z powrotem do urządzenia Cisco. Instrukcje dotyczące konfiguracji i działania serwera TFTP mają charakter ogólny i mogą występować pewne różnice w terminologii z oprogramowaniem serwera TFTP.

Uwaga: Routery używane w praktycznych laboratoriach CCNA to Cisco 4221 z Cisco IOS XE wydanie 16.9.4 (obraz universalk9). Przełączniki używane w laboratoriach to Cisco Catalyst 2960 z Cisco IOS wydanie 15.2 (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 różnić od prezentowanych w niniejszej instrukcji. Przejrzyj tabelę podsumowującą interfejsy routera w celu określenia poprawnych identyfikatorów interfejsów.

Uwaga: Upewnij się, że konfiguracje startowe routerów i przełączników zostały wykasowane. Jeśli nie jesteś pewien, poproś o pomoc instruktora.

Wymagane zasoby

- 1 router (Cisco 4221 z uniwersalnym obrazem Cisco IOS XE Release 16.9.3 lub porównywalnym)
- 1 przełącznik (Cisco 2960 z systemem Cisco IOS wersja15.2 (2) obraz lanbasek9 lub porównywalny)
- 1 komputer PC (Windows z emulatorem terminala takim jak Tera Term)
- Kable konsolowe do konfiguracji urządzeń Cisco IOS za pośrednictwem portów konsoli
- Kable Ethernet zgodnie z przedstawioną topologią
- Dysk USB flash (opcjonalnie)

Instrukcje

Część 1: Utworzenie sieci oraz konfigurowanie podstawowych ustawień urządzeń

W części 1 będziesz konfigurować topologię sieci i skonfigurujesz podstawowe ustawienia, takie jak adresy IP dla routera R1, przełącznika S1 oraz komputera PC-A.

Krok 1: Zbuduj sieć zgodnie z topologią.

Połącz wymagane urządzenia oraz kable tak, jak pokazano na schemacie topologii.

Krok 2: Wykonaj podstawową konfigurację routera.

a. Przypisz routerowi nazwę.

b. Wyłącz wyszukiwanie DNS, aby router nie próbował tłumaczyć niepoprawnie wprowadzonych poleceń, tak jakby były one nazwami hostów.

c. Przypisz **class** jako zaszyfrowane hasło trybu uprzywilejowanego EXEC.

d. Przypisz **cisco** jako hasło konsoli i włącz logowanie.

e. Przypisz **cisco** jako hasło do VTY oraz włącz logowanie.

f. Zaszyfruj hasła zapisane jawnym tekstem.

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

h. Skonfiguruj interfejsy zgodnie z powyższą tabelą.

i. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

Uwaga: Użyj znaku zapytania (**?**) aby uzyskać informację pomocniczą o kolejności parametrów potrzebnych do wykonania tego polecenia.

Krok 3: Wykonaj podstawową konfigurację przełączników.

a. Przypisz nazwę urządzenia do przełącznika.

b. Wyłącz wyszukiwanie DNS, aby router nie próbował tłumaczyć niepoprawnie wprowadzonych poleceń, tak jakby były one nazwami hostów.

c. Przypisz **class** jako zaszyfrowane hasło trybu uprzywilejowanego EXEC.

d. Przypisz **cisco** jako hasło konsoli i włącz logowanie.

e. Przypisz **cisco** jako hasło do VTY oraz włącz logowanie.

f. Zaszyfruj hasła zapisane jawnym tekstem.

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

h. Wyłącz wszystkie nieużywane interfejsy.

i. Skonfiguruj interfejs VLAN 1 zgodnie z powyższą tabelą.

j. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

Uwaga: Użyj znaku zapytania (**?**) aby uzyskać informację pomocniczą o kolejności parametrów potrzebnych do wykonania tego polecenia.

Krok 4: Sprawdź połączenie z PC-A.

a. Wykonaj ping z PC-A do S1.

b. Wykonaj ping z PC-A do R1.

Jeżeli polecenia ping kończą się niepowodzeniem, to przed kontynuowaniem ćwiczenia należy rozwiązywać podstawowe problemy związane z konfiguracją urządzeń.

Część 2: Użyj protokołu TFTP do tworzenia kopii zapasowych i przywracania uruchomionej konfiguracji przełącznika

Krok 1: Sprawdź połączenie z komputera PC-A do przełącznika S1.

Aplikacja TFTP używa protokołu transportowego UDP (warstwa 4), który jest enkapsulowany w pakiecie IP. Aby przesyłanie plików TFTP działało, musi istnieć połączenie w warstwach 1 i 2 (w tym przypadku Ethernet) oraz warstwie 3 (IP) pomiędzy klientem TFTP i serwerem TFTP . Topologia sieci LAN w tym laboratorium używa tylko Ethernetu w warstwach 1 i 2. Przesyłanie plików TFTP można również realizować poprzez łącza WAN, które korzystają z innych protokołów warstwy 1 (warstwy fizycznej) i warstwy 2. Transfer TFTP może nastąpić gdy istnieje łączność IP między klientem a serwerem, co można sprawdzić poleceniem ping. Jeżeli polecenia ping kończą się niepowodzeniem, to przed kontynuowaniem ćwiczenia należy rozwiązywać podstawowe problemy związane z konfiguracją urządzeń.

Uwaga: Powszechnym błędnym przekonaniem jest to, że możesz przesłać plik za pośrednictwem TFTP podczas połączenia konsoli. Nie może się tak wydarzyć, ponieważ połączenie konsolowe nie używa protokołu

IP. Transfer TFTP może być zainicjowany przez urządzenie klienckie (router lub przełącznik) poprzez połączenie konsolowe, ale pomiędzy klientem a serwerem musi być połączenie IP aby transfer mógł być możliwy.

Krok 2: Uruchom serwer TFTP.

Uruchom program TFTP na PC-A. Upewnij się, że program TFTP używa katalogu, do którego masz uprawnienia ZAPISU, na przykład folderu na pulpicie.

Krok 3: Poznaj polecenie copy na urządzeniach Cisco.

a. Podłącz konsolę do przełącznika S1 i w uprzywilejowanym trybie EXEC wpisz **copy?** aby wyświetlić opcje źródła lub lokalizacji „z" oraz inne dostępne opcje kopiowania. Możesz określić **flash:** lub **flash0:** jako źródło. Jeśli jednak jako źródło podasz po prostu nazwę pliku, przyjmowane jest **flash0:** i jest to wartość domyślna. Zauważ, że **running-config** jest również opcją dla lokalizacji źródłowej.

```
S1# copy ?
  /erase Erase destination file system.
  /error Allow to copy error file.
  /noverify Don't verify image signature before reload.
  /verify Verify image signature before reload.
  bs: Copy from bs: file system
  cns: Copy from cns: file system
  flash: Copy from flash: file system
  ftp: Copy from ftp: file system
  http: Copy from http: file system
  https: Copy from https: file system
  logging Copy logging messages
  null: Copy from null: file system
  nvram: Copy from nvram: file system
  rcp: Copy from rcp: file system
  running-config Copy from current system configuration
  scp: Copy from scp: file system
  startup-config Copy from startup configuration
  system: Copy from system: file system
  tar: Copy from tar: file system
  tftp: Copy from tftp: file system
  tmpsys: Copy from tmpsys: file system
  vb: Copy from vb: file system
  xmodem: Copy from xmodem: file system
  ymodem: Copy from ymodem: file system
```

b. Użyj **?** aby wyświetlić opcje miejsca docelowego po wybraniu lokalizacji pliku źródłowego. W tym przykładzie system plików **flash:** dla S1 jest systemem plików źródłowych.

```
S1# copy flash: ?
  flash: Copy to flash: file system
  ftp: Copy to ftp: file system
  http: Copy to http: file system
  https: Copy to https: file system
  null: Copy to null: file system
  nvram: Copy to nvram: file system
  rcp: Copy to rcp: file system
```

```
  running-config Update (merge with) current system configuration
  scp: Copy to scp: file system
  startup-config Copy to startup configuration
  system: Copy to system: file system
  tftp: Copy to tftp: file system
  tmpsys: Copy to tmpsys: file system
  vb: Copy to vb: file systesystem
```

Krok 4: Prześlij plik running-config z przełącznika S1do serwera TFTP na PC-A.

a. W uprzywilejowanym trybie EXEC na przełączniku wprowadź polecenie **copy running-config tftp:** . Musisz zapewnić zdalny dostęp do adresu hosta serwera TFTP (PC-A) 192.168.1.3. Naciśnij klawisz Enter, aby zaakceptować domyślną nazwę pliku docelowego (**s1-confg**) lub podaj własną nazwę pliku. Wykrzykniki (**!!**) wskazują, że proces przesyłania jest w toku i zakończył się pomyślnie.

```
S1# copy running-config tftp:
Address or name of remote host []? 192.168.1.3
Destination filename [s1-confg]?
!!
1465 bytes copied in 0.663 secs (2210 bytes/sec)
S1#
```

Serwer TFTP może również wyświetlać postęp przesyłania.

Uwaga: jeśli nie masz uprawnień do zapisu w bieżącym katalogu używanym przez serwer TFTP, zostanie wyświetlony następujący komunikat o błędzie:

```
S1# copy running-config tftp:
Address or name of remote host []? 192.168.1.3
Destination filename [s1-confg]?
%Error opening tftp://192.168.1.3/s1-confg (Permission denied)
```

Uwaga: Inne problemy, takie jak zapora blokująca ruch TFTP, mogą uniemożliwić transfer TFTP. Proszę skontaktować się z instruktorem dla dalszej pomocy.

b. Sprawdź katalog na serwerze TFTP (zazwyczaj jest to katalog domyślny oprogramowania serwera TFTP), aby sprawdzić, czy plik został pomyślnie przeniesiony. Serwer TFTP może mieć w tym celu okno dialogowe lub można po prostu użyć Eksploratora plików dostarczonego przez system operacyjny.

Krok 5: Utwórz zmodyfikowany plik konfiguracji bieżącej dla przełącznika.

Zapisany działający plik konfiguracyjny, **s1-confg**, można również przywrócić do przełącznika za pomocą polecenia **copy** z przełącznika. Oryginalna lub zmodyfikowana wersja pliku może być kopiowana do systemu plików pamięci flash w przełączniku.

a. Przejdź do katalogu TFTP na komputerze PC-A, korzystając z systemu plików PC-A, a następnie znajdź plik **s1-confg**. Otwórz ten plik za pomocą edytora tekstu, np. WordPad.

b. Po otwarciu pliku znajdź wiersz **hostname S1** . Zamień **S1** na **Switch1**. W razie potrzeby usuń wszystkie generujące się automatycznie klucze kryptograficzne. Przykładowe klucze wyświetlono poniżej. Klucze te nie dają się eksportować i mogą powodować błędy podczas aktualizacji bieżącej konfiguracji.

```
crypto pki trustpoint TP-self-signed-1566151040
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1566151040
 revocation-check none
 rsakeypair TP-self-signed-1566151040
!
```

```
!
crypto pki certificate chain TP-self-signed-1566151040
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
<output omitted>
  E99574A6 D945014F B6FE22F3 642EE29A 767EABF7 403930CA D2C59E23 102EC12E
  02F9C933 B3296D9E 095EBDAF 343D17F6 AF2831C7 6DA6DFE3 35B38D90 E6F07CD4
  40D96970 A0D12080 07A1C169 30B9D889 A6E2189C 75B988B9 0AF27EDC 6D6FA0E5
  CCFA6B29 729C1E0B 9DADACD0 3D7381
       quit
```

c. Zapisz ten plik jako zwykły plik tekstowy z nową nazwą, **Switch1-confg.txt**, w tym przykładzie.

Uwaga: podczas zapisywania pliku rozszerzenie, takie jak **.txt**, może zostać automatycznie dodane do nazwy pliku.

d. Jeśli oprogramowanie TFTP ma taką opcję, użyj go do wyświetlenia zawartości katalogu w celu sprawdzenia, czy plik jest obecny.

Krok 6: Skopiuj zmodyfikowany bieżący plik konfiguracyjny z serwera TFTP, aby przełączyć S1.

a. W uprzywilejowanym trybie EXEC na przełączniku wprowadź polecenie **copy tftp running-config** . Użyj adres hosta zdalnego dla serwera TFTP: 192.168.1.3. Wprowadź nową nazwę pliku, **Switch1-confg.txt**. Wykrzyknik (!!) oznacza, że proces przesyłania przebiega pomyślnie.

```
S1# copy tftp: running-config
Address or name of remote host []? 192.168.1.3
Source filename []? Switch1-confg.txt
Destination filename [running-config]?
Accessing tftp://192.168.1.3/Switch1-confg.txt...
Loading Switch1-confg.txt from 192.168.1.3 (via Vlan1): !
[OK - 1580 bytes]
[OK]
1580 bytes copied in 9.118 secs (173 bytes/sec)
*Mar 1 00:21:16.242: %PKI-4-NOAUTOSAVE: Configuration was modified.  Issue "write
memory" to save new certificate
*Mar 1 00:21:16.251: %SYS-5-CONFIG_I: Configured from tftp://192.168.1.3/Switch1-
confg.txt by console
Switch1#
```

Po zakończeniu przesyłania znak zachęty zmienił się z S1 na Switch1, ponieważ bieżąca konfiguracja jest aktualizowana za pomocą polecenia **hostname Switch1** w zmodyfikowanej konfiguracji bieżącej.

b. Wpisz polecenie **show running-config**, aby sprawdzić działający plik konfiguracyjny.

```
Switch1# show running-config
Building configuration...

Current configuration : 3062 bytes
!
! Last configuration change at 00:09:34 UTC Mon Mar 1 1993
!
version 15.0
no service pad
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch1
!
boot-start-marker
boot-end-marker
<output omitted>
```

Uwaga: Ta procedura powoduje połączenie pliku running-config z serwera TFTP z bieżącym plikiem running-config w przełączniku lub routerze. Jeżeli dokonano zmian w aktualnym pliku running-config, to polecenia z kopii TFTP są dodawane. Ewentualnie, jeżeli to samo polecenie zostanie wydane, to aktualizuje się adekwatne polecenie w bieżącym pliku running-config przełącznika lub routera .

Jeżeli chcesz całkowicie wymienić obecny running-config na inny pobrany z serwera TFTP, to musisz usunąć startup-config z przełącznika i restartować urządzenie. Następnie musisz skonfigurować adres zarządzania VLAN 1, aby zaistniała łączność IP między serwerem TFTP i przełącznikem.

Część 3: Stosowanie TFTP do tworzenia kopii zapasowych i przywracania bieżącej konfiguracji routera

Procedury tworzenia kopii zapasowych i przywracania zawarte w części 3 można także wykonać na routerze. W części 4 zostanie utworzona kopia zapasowa pliku bieżącej konfiguracji i przywrócona bieżąca konfiguracja za pomocą serwera TFTP.

Krok 1: Sprawdź połączenie z komputera PC-A do routera R1.

Jeżeli polecenia ping kończą się niepowodzeniem, to przed kontynuowaniem ćwiczenia należy rozwiązywać podstawowe problemy związane z konfiguracją urządzeń.

Krok 2: Prześlij bieżącą konfigurację z routera R1 do serwera TFTP na komputerze PC-A.

a. W uprzywilejowanym trybie EXEC na R1 wprowadź polecenie **copy running-config tftp** . Użyj adres hosta zdalnego jako serwera TFTP, 192.168.1.3 i zaakceptuj domyślną nazwę pliku.

b. Sprawdź czy plik został przesłany na serwer TFTP.

Krok 3: Przywróć plik konfiguracji bieżącej routera.

a. Na routerze usuń plik startup-config.

b. Zrestartuj router.

c. Skonfiguruj interfejs G0/0/1 na routerze z adresem IP 192.168.1.1.

d. Sprawdź połączenie między routerem i PC-A.

e. Użyj polecenia **copy**, aby przesłać plik running-config z serwera TFTP do routera. Użyj **running-config** jako miejsca docelowego.

f. Sprawdź czy router zaktualizował running-config.

Część 4: Tworzenie kopii zapasowych i przywracanie plików konfiguracji przy użyciu wewnętrznej pamięci flash w routerze

Routery Cisco obecnej generacji nie mają wewnętrznej pamięci flash. Pamięcią flash dla tych routerów jest pamięć CompactFlash (CF). Pamięć CF jest bardziej pojemna of flash i umożliwia łatwiejszą zmianę wersji oprogramowania bez konieczności otwierania obudowy routera. Pamięć CF przechowuje niezbędne pliki,

takie jak obrazy IOS, ale może przechowywać inne pliki, takie jak kopia bieżącej konfiguracji. W części 5 utworzysz kopię zapasową uruchomionego pliku konfiguracyjnego i zapiszesz ją w pamięci USB routera.

Uwaga: Jeśli router nie korzysta z CF, router może nie mieć wystarczającej ilości pamięci flash do przechowywania kopii zapasowej uruchomionego pliku konfiguracyjnego. Należy jeszcze raz przeczytać instrukcję i zapoznać się z poleceniami.

Krok 1: Wyświetl systemy plików routera.

Polecenie **show file systems** wyświetla dostępne systemy plików na routerze. System plików **flash0:** jest domyślnym systemem plików na tym routerze, co wskazuje symbol gwiazdki (*) (na początku wiersza). Do systemu plików **flash0:** można się również odwoływać, używając nazwy **flash:**. Całkowity rozmiar **flash0:** wynosi około 7 GB z około 6 GB dostępnych. Obecnie **flash0:**: i **nvram:** są jedynymi dostępnymi systemami plików.

```
R1# show file systems
File Systems:

       Size(b)  Free(b)  Type  Flags  Prefixes
             -        -  opaque  rw  system:
             -        -  opaque  rw  tmpsys:
* 7194652672 6299918336  disk  rw  bootflash: flash:
    1804468224 1723789312  disk  ro  webui:
             -        -  opaque  rw  null:
             -        -  opaque  ro  tar:
             -        -  network  rw  tftp:
             -        -  opaque  wo  syslog:
      33554432 33543116  nvram  rw  nvram:
             -        -  network  rw  rcp:
             -        -  network  rw  ftp:
             -        -  network  rw  http:
             -        -  network  rw  scp:
             -        -  network  rw  sftp:
             -        -  network  rw  https:
             -        -  opaque  ro  cns:
```

Gdzie znajduje się plik startup-config ?

Uwaga: sprawdź, czy jest co najmniej 1 MB (1 048 576 bajtów) wolnego miejsca. Jeżeli w pamięci flash jest za mało miejsca, to należy skontaktować się z instruktorem aby uzyskać dalsze instrukcje. Możesz określić rozmiar pamięci flash i dostępnego miejsca za pomocą polecenia **show flash** lub **dir flash:** w uprzywilejowanym znaku zachęty EXEC.

Krok 2: Skopiuj bieżącą konfigurację routera do pamięci flash.

Plik można skopiować do pamięci flash, używając polecenia **copy** w uprzywilejowanym wierszu polecenia EXEC. W tym przykładzie plik jest kopiowany do **flash0:**, ponieważ dostępny jest tylko jeden dysk flash, jak pokazano w poprzednim kroku, i jest to również domyślny system plików. Plik **R1-running-config-backup** jest używany jako nazwa pliku kopii zapasowej uruchomionego pliku konfiguracyjnego.

Uwaga: Pamiętaj, że w nazwach plików w systemie plików IOS rozróżniana jest wielkość liter.

a. Skopiuj konfigurację bieżącą do pamięci flash.

```
R1# copy running-config flash:
```

```
Destination filename [running-config]? R1-running-config-backup
2169 bytes copied in 0.968 secs (2241 bytes/sec)
```

b. Użyj polecenia **dir**, aby sprawdzić, czy running-config został skopiowany do pamięci flash.

```
R1# dir flash:
Directory of bootflash:/

   11 drwx 16384 Aug 2 2019 04:15:13 +00:00 lost+found
370945 drwx 4096 Sep 25 2019 20:17:11 +00:00 .installer
338689 drwx 4096 Aug 2 2019 04:15:55 +00:00 .ssh
217729 drwx 4096 Aug 2 2019 04:17:59 +00:00 core
379009 drwx 4096 Sep 25 2019 20:19:13 +00:00 .prst_sync
80641 drwx 4096 Aug 2 2019 04:16:09 +00:00 .rollback_timer
161281 drwx 4096 Aug 2 2019 04:16:11 +00:00 gs_script
112897 drwx 77824 Sep 25 2019 20:23:03 +00:00 tracelogs
362881 drwx 4096 Aug 23 2019 17:19:54 +00:00 .dbpersist
298369 drwx 4096 Aug 2 2019 04:16:41 +00:00 virtual-instance
   12 -rw- 30 Sep 25 2019 20:19:13 +00:00 throughput_monitor_params
 8065 drwx 4096 Aug 2 2019 04:17:55 +00:00 onep
   13 -rw- 35 Sep 25 2019 20:20:19 +00:00 pnp-tech-time
249985 drwx 4096 Aug 20 2019 17:40:11 +00:00 Archives
   14 -rw- 64414 Sep 25 2019 20:20:28 +00:00 pnp-tech-discovery-summary
   15 -rw- 3509 Sep 25 2019 20:24:32 +00:00 R1-running-config-backup
   17 -rw- 5032908 Sep 19 2019 14:16:23 +00:00 isr4200_4300_rommon_1612_1r_SPA.pkg
   18 -rw- 517153193 Sep 21 2019 04:24:04 +00:00 isr4200-
universalk9_ias.16.09.04.SPA.bin

7194652672 bytes total (6299643904 bytes free)
```

c. Użyj polecenia **more** , aby wyświetlić plik running-config w pamięci flash. Sprawdź plik wyjściowy plik i przejdź do sekcji interfejsu. Zauważ, że polecenie**no shutdown** nie jest dołączone do GigabitEthernet0 / 1. Jeżeli plik ten jest używany w celu aktualizacji konfiguracji bieżącej na routerze, to interfejs jest wyłączony,

```
R1# more flash:R1-running-config-backup
<output omitted>
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
<output omitted>
```

Krok 3: Usuń konfigurację startową routera i zrestartuj go.

Krok 4: Przywróć konfigurację bieżącą z pamięci flash.

a. Upewnij się, że router ma domyślną konfigurację początkową.

b. Skopiuj zapisany plik running-config z pamięci flash w celu aktualizacji bieżącej konfiguracji.

```
Router# copy flash:R1-running-config-backup running-config
```

c. Użyj polecenia **show ip interface brief**, aby wyświetlić stan interfejsów. Interfejs GigabitEthernet0/1 nie został włączony podczas aktualizacji konfiguracji bieżącej, ponieważ jest on wyłączony administracyjnie.

```
R1# show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 unassigned YES unset administratively down down
GigabitEthernet0/0/1 192.168.1.1 YES TFTP administratively down down
Serial0/1/0 unassigned YES unset administratively down down
Serial0/1/1 unassigned YES unset administratively down down
```

Interfejs można włączyć za pomocą polecenia **no shutdown** w trybie konfiguracji interfejsu na routerze.

Inną opcją jest dodanie polecenia **no shutdown** dla interfejsu GigabitEthernet0/0/1 do zapisanego pliku przed aktualizacją uruchomionego pliku konfiguracyjnego routera. Zostanie to zrobione za pomocą zapisanego pliku na dysku USB flash w części 5.

Uwaga: ponieważ adres IP został skonfigurowany przy użyciu transferu plików, protokół TFTP jest wymieniony pod nagłówkiem Method w danych wyjściowych **show ip interface brief**.

Część 5: (Opcjonalnie) Użycie dysku USB do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych

Pamięć USB flash może być używana do tworzenia kopii zapasowych i przywracania plików na routerze wyposażonym w port USB. Jeden port USB jest dostępny na routerach 4221.

Uwaga: porty USB nie są dostępne we wszystkich routerach, ale nadal powinieneś zapoznać się z poleceniami.

Uwaga: Niektóre routery ISR G1 (1841, 2801 lub 2811) używają systemów plików FAT (File Allocation Table), co skutkuje ograniczeniem maksymalnego rozmiaru dysków flash USB, których można używać w tej części ćwiczenia. Zalecana maksymalna pojemność dla G1 ISR wynosi 4 GB. Jeśli pojawi się następujący komunikat, system plików na dysku flash USB może być niekompatybilny z routerem lub pojemność dysku flash USB może przekroczyć maksymalny rozmiar systemu plików FAT routera.

```
*Feb 8 13:51:34.831: %USBFLASH-4-FORMAT: usbflash0 contains unexpected values in
partition table or boot sector.  Device needs formatting before use!
```

Krok 1: Włóż dysk USB flash do portu USB w routerze.

Zwróć uwagę na komunikat w terminalu po włożeniu dysku USB flash.

```
*Sep 24 23:00:33.242: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usb0 added
```

Krok 2: Sprawdź, czy system plików w USB flash jest obsługiwany.

```
R1# show file systems
File Systems:

       Size(b)  Free(b)  Type  Flags  Prefixes
             -        -  opaque  rw  system:
             -        -  opaque  rw  tmpsys:
* 7194652672 6297677824  disk  rw  bootflash: flash:
     256589824 256577536  disk  rw  usb0:
    1804468224 1723789312  disk  ro  webui:
             -        -  opaque  rw  null:
             -        -  opaque  ro  tar:
             -        -  network  rw  tftp:
             -        -  opaque  wo  syslog:
      33554432 33543116  nvram  rw  nvram:
             -        -  network  rw  rcp:
```

```
- - network rw ftp:
- - network rw http:
- - network rw scp:
- - network rw sftp:
- - network rw https:
- - opaque ro cns:
```

Krok 3: Skopiuj plik konfiguracji bieżącej na dysk USB flash.

Użyj polecenia **copy**, aby skopiować bieżący plik konfiguracyjny na dysk flash USB.

```
R1# copy running-config usb0:
Destination filename [running-config]? R1-running-config-backup.txt
2198 bytes copied in 0.708 secs (3105 bytes/sec)
```

Krok 4: Wyświetl listę plików znajdujących się na dysku USB flash.

Użyj polecenia **dir** (lub polecenia **show**) na routerze, aby wyświetlić listę plików na dysku flash USB. W tym przykładzie napęd pamięci flash został włożony do portu USB 0 w routerze.

```
R1# dir usb0:
Directory of usb0:/

    6 -rwx 3539 Sep 25 2019 20:41:58 +00:00 R1-running-config-backup.txt
    3 drwx 4096 Sep 24 2019 13:32:26 +00:00 System Volume Information

256589824 bytes total (256573440 bytes free)
```

Krok 5: Usuń startup-config i zrestartuj router.

Krok 6: Zmodyfikuj zapisany plik.

a. Wyjmij dysk USB z routera.

```
Router#
*Sep 24 23:00:27.674: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usb0 removed
```

b. Włóż dysk USB do portu USB komputera PC.

c. Zmodyfikuj plik za pomocą edytora tekstu. Polecenie **no shutdown** zostało dodane do interfejsu GigabitEthernet0/0/1. Zapisz plik jako pliku tekstowy na dysku USB flash.

```
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 no shutdown
 duplex auto
 speed auto
```

d. Wyjmij bezpiecznie dysk USB flash z komputera PC.

Krok 7: Przywróć plik konfiguracji bieżącej routera.

a. Włóż pamięć USB flash do portu USB w routerze. Jeżeli jest więcej niż jeden port USB dostępny w routerze, to zwróć uwagę na numer portu w którym został włożony dysk USB.

```
*Sep 24 23:00:33.242: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usb0 added
```

b. Wyświetl listy plików na dysku USB flash.

```
R1# dir usb0:
```

```
Directory of usb0:/

    6 -rwx 3539 Sep 25 2019 20:41:58 +00:00 R1-running-config-backup.txt
    3 drwx 4096 Sep 24 2019 13:32:26 +00:00 System Volume Information

256589824 bytes total (256573440 bytes free)
```

c. Skopiuj plik konfiguracji bieżącej do routera.

```
Router# copy usb0:R1-running-config-backup.txt running-config
Destination filename [running-config]?
2344 bytes copied in 0.184 secs (12739 bytes/sec)
R1#
```

d. Sprawdź czy interfejs GigabitEthernet0/1 jest włączony.

```
R1# show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 unassigned YES unset administratively down down
GigabitEthernet0/0/1 192.168.1.1 YES TFTP up up
Serial0/1/0 unassigned YES unset administratively down down
Serial0/1/1 unassigned YES unset administratively down down
```

Interfejs G0 / 1 jest włączony, ponieważ zmodyfikowana konfiguracja bieżąca zawiera polecenie **no shutdown** .

Pytania do przemyślenia

1. Jakiego polecenia użyjesz aby skopiować plik z pamięci flash na dysk USB?

2. Jakiego polecenia użyjesz do skopiowania pliku z dysku USB flash do serwera TFTP?

Tabela zbiorcza interfejsów routerów

Model routera	Interfejs Ethernet #1	Interfejs Ethernet #2	Interfejs szeregowy #1	Interfejs szeregowy #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)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Model routera	Interfejs Ethernet #1	Interfejs Ethernet #2	Interfejs szeregowy #1	Interfejs szeregowy #2
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Uwaga: Aby stwierdzić jak router jest skonfigurowany, spójrz na interfejsy, aby zidentyfikować typ routera oraz liczbę jego interfejsów. Nie ma jednego sposobu na skuteczne opisanie wszystkich kombinacji konfiguracji dla każdego modelu routera. Tabela zawiera identyfikatory możliwych kombinacji interfejsów Ethernet i Serial w urządzeniu. W tabeli nie podano żadnych innych rodzajów interfejsów, pomimo iż dany router może być w nie wyposażony. Przykładem takiego interfejsu może być ISDN BRI. Informacje umieszczone w nawiasach są dozwolonym skrótem, którego można używać w poleceniach IOS w celu odwołania się do interfejsu.