Laboratorium — Konfiguracja NAT dla IPv4

Topologia

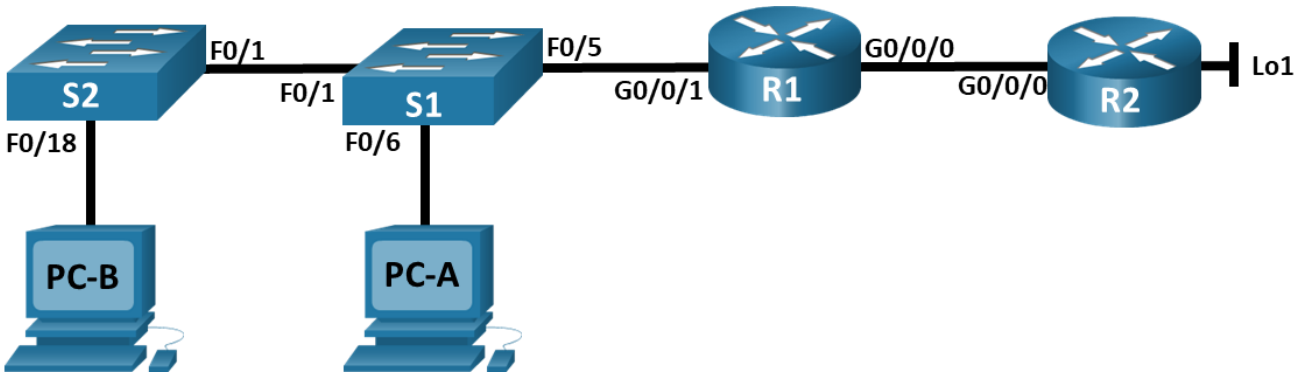

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci
R1	G0/0/0	209.165.200.230	255.255.255.248
	G0/0/1	192.168.1.1	255.255.255.0
R2	G0/0/0	209.165.200.225	255.255.255.248
	Lo1	209.165.200.1	255.255.255.224
S1	VLAN 1	192.168.1.11	255.255.255.0
S2	VLAN 1	192.168.1.12	255.255.255.0
PC-A	Karta sieciowa	192.168.1.2	255.255.255.0
PC-B	Karta sieciowa	192.168.1.3	255.255.255.0

Cele

Część 1: Utworzenie sieci oraz konfigurowanie podstawowych ustawień urządzenia

Cześć 2: Konfigurowanie i weryfikacja NAT dla IPv4

Cześć 2: Konfigurowanie i weryfikacja PAT dla IPv4

Część 4: Konfigurowanie i weryfikacja statycznego NAT dla IPv4

Wprowadzenie / Scenariusz

Translacja Adresów Sieciowych (NAT) jest procesem, w którym urządzenie sieciowe, takie jak router Cisco, przypisuje adresy publiczne urządzeniom w sieci prywatnej. Głównym powodem użycia NAT jest zredukowanie liczby wykorzystywanych przez organizację publicznych adresów, z uwagi na ograniczoną ich liczbę.

Dostawca usług internetowych przydzielił firmie publiczną przestrzeń adresową 209.165.200.224/29. Sieć ta służy do adresowania połączenia między routerem ISP (R2) a bramą firmową (R1). Pierwszy adres (209.165.200.225) jest przypisany do interfejsu g0/0/0 na R2, a ostatni adres (209.165.200.230) jest przypisany do interfejsu g0/0/0 na R1. Pozostałe adresy (209.165.200.226-209.165.200.229) zostaną wykorzystane do zapewnienia dostępu do Internetu hostom firmy. Domyślna trasa jest używana od R1 do R2. Internet jest symulowany przez adres loopback na R2.

W tym ćwiczeniu zostaną skonfigurowane różne typy NAT. Należy przetestować, podejrzeć i sprawdzić, czy translacje się odbywają. W tym celu należy dokonać interpretacji statystyk NAT/PAT służących do monitorowania procesu.

Uwaga: Routery używane w laboratoriach CCNA to Cisco 4221 z Cisco IOS XE wydanie 16.9.3 (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

- 2 routery (Cisco 4221 z uniwersalnym obrazem Cisco IOS XE Release 16.9.4 lub porównywalny)
- 2 przełączniki (Cisco 2960 z Cisco IOS Release 15.2(2) obraz lanbasek9 lub porównywalny)
- 2 komputery 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

Instrukcje

Część 1: Utworzenie sieci oraz konfigurowanie podstawowych ustawień urządzeń

W części 1 utworzysz topologię sieciową i skonfigurujesz podstawowe ustawienia komputerów i przełączników.

Krok 1: Zbuduj sieć zgodnie z topologią.

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

Krok 2: Skonfiguruj podstawowe ustawienia dla każdego 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 adresowanie IP interfejsu zgodnie z powyższą tabelą.

i. Skonfiguruj domyślną trasę do R2 z R1.

j. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

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. Zamknij wszystkie interfejsy, które nie będą używane.

i. Skonfiguruj adresowanie IP interfejsu zgodnie z powyższą tabelą.

j. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

Część 2: Konfigurowanie i weryfikacja NAT dla IPv4

W części 2 skonfigurujesz i zweryfikujesz NAT dla IPv4.

Krok 1: Skonfiguruj NAT na R1 przy użyciu puli trzech adresów: 209.165.200.226-209.165.200.228.

a. Skonfiguruj prostą listę dostępu, która określa, jakie hosty będą dopuszczone do tłumaczenia. W takim przypadku wszystkie urządzenia w sieci LAN R1 kwalifikują się do tłumaczenia.

```
R1(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

b. Utwórz pulę translacji adresów sieciowych i nadaj jej nazwę i zakres adresów do użycia.

```
R1(config)# ip nat pool PUBLIC_ACCESS 209.165.200.226 209.165.200.228 netmask
255.255.255.248
```

Uwaga: Parametr netmask nie jest ogranicznikiem adresów IP. Powinna to być właściwa maska podsieci dla przypisanych adresów, nawet jeśli nie używasz wszystkich adresów podsieci w puli.

c. Skonfiguruj translację, kojarząc listy ACL i pulę z procesem tłumaczenia.

```
R1(config)# ip nat inside source list 1 pool PUBLIC_ACCESS
```

Uwaga: Trzy bardzo ważne punkty. Po pierwsze, słowo „inside” ma kluczowe znaczenie dla działania tego rodzaju NAT. Jeśli go pominiesz, NAT nie będzie działać. Po drugie, numer listy to numer ACL skonfigurowany w poprzednim kroku. Po trzecie, w nazwie puli rozróżniana jest wielkość liter.

d. Określ interfejs wewnętrzny.

```
R1(config)# interface g0/0/1
R1(config-if)# ip nat inside
```

e. Zdefiniuj interfejs zewnętrzny.

```
R1(config)# interface g0/0/0
R1(config-if)# ip nat outside
```

Krok 2: Wykonaj testy i zweryfikuj konfigurację.

a. Z poziomu komputera PC-B, wykonaj ping do interfejsu Lo1 (209.165.200.1) na R2. Jeżeli ping się nie powiedzie, znajdź błąd i popraw go. Na R1 wyświetl tablicę NAT za pomocą polecenia **show ip nat translations**.

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.226 192.168.1.3 --- ---
icmp 209.165.200.226:1 192.168.1.3:1 209.165.200.1:1 209.165.200.1:1
Total number of translations: 2
```

Na jaki adres wewnętrzny lokalny został przetłumaczony adres PC-B?

Jakim typem adresu NAT jest przetłumaczony adres?

b. Z poziomu komputera PC-A, wykonaj ping do interfejsu Lo1 (**209.165.200.1**) na R2. Jeżeli ping się nie powiedzie, znajdź błąd i popraw go. Na R1 wyświetl tablicę NAT za pomocą polecenia **show ip nat translations**.

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.227 192.168.1.2 --- ---
--- 209.165.200.226 192.168.1.3 --- ---
icmp 209.165.200.227:1 192.168.1.2:1 209.165.200.1:1 209.165.200.1:1
icmp 209.165.200.226:1 192.168.1.3:1 209.165.200.1:1 209.165.200.1:1
Total number of translations: 4
```

c. Zauważ, że poprzednie tłumaczenie dla PC-B nadal znajduje się w tablicy. Z S1, wykonaj ping do interfejsu Lo1 (**209.165.200.1**) na R2. Jeżeli ping się nie powiedzie, znajdź błąd i popraw go. Na R1 wyświetl tablicę NAT za pomocą polecenia **show ip nat translations**.

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.227 192.168.1.2 --- ---
--- 209.165.200.226 192.168.1.3 --- ---
--- 209.165.200.228 192.168.1.11 --- ---
icmp 209.165.200.226:1 192.168.1.3:1 209.165.200.1:1 209.165.200.1:1
icmp 209.165.200.228:0 192.168.1.11:0 209.165.200.1:0 209.165.200.1:0
Total number of translations: 5
```

d. Teraz spróbuj wykonać ping do R2 Lo1 z S2. Tym razem tłumaczenia nie powiodą się, a te komunikaty są wyświetlane (lub podobne) na konsoli R1:

```
Sep 23 15:43:55.562: %IOSXE-6-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000
TS:00000001473688385900 %NAT-6-ADDR_ALLOC_FAILURE: Address allocation failed; pool 1
may be exhausted [2]
```

e. Jest to oczekiwany wynik, ponieważ przydzielane są tylko 3 adresy, a my próbowaliśmy wysłać ping Lo1 z czterech urządzeń. Przypomnijmy, że NAT jest tłumaczeniem jeden do jednego. Jak długo są

przydzielane tłumaczenia? Wydaj polecenie **show ip nat translations verbose**, a zobaczysz, że jest to na 24 godziny.

```
R1# show ip nat translations verbose
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.226 192.168.1.3 --- ---
  create: 09/23/19 15:35:27, use: 09/23/19 15:35:27, timeout: 23:56:42
  Map-Id(In): 1
<output omitted>
```

f. Biorąc pod uwagę, że pula jest ograniczona do trzech adresów, translacja NAT do puli adresów nie jest odpowiednia w naszej sytuacji. Wyczyść tłumaczenia NAT i statystyki, i przejdziemy do PAT.

```
R1# clear ip nat translations *
R1# clear ip nat statistics
```

Część 3: Konfigurowanie i weryfikacja PAT dla IPv4

W części 3 skonfigurujesz zamianę NAT na PAT z pulą adresów, a następnie na PAT z interfejsem.

Krok 1: Usuń polecenie tłumaczenia na R1.

Składniki konfiguracji tłumaczenia adresów są zasadniczo takie same; coś (lista dostępu) do identyfikowania adresów kwalifikujących się do przetłumaczenia, opcjonalnie skonfigurowana pula adresów do tłumaczenia oraz polecenia niezbędne do identyfikacji wewnętrznych i zewnętrznych interfejsów. Z części 1 nasza lista dostępu (ACL 1) jest nadal poprawna dla scenariusza sieciowego, więc nie ma potrzeby jej odtworzenia. Będziemy używać tej samej puli adresów, więc nie ma też potrzeby ponownego tworzenia tej konfiguracji. Ponadto interfejsy wewnętrzne i zewnętrzne nie ulegają zmianie. Aby rozpocząć pracę w części 3, usuń polecenie, które łączy listy ACL i pulę.

```
R1(config)# no ip nat inside source list 1 pool PUBLIC_ACCESS
```

Krok 2: Dodaj polecenie PAT na R1.

Teraz skonfiguruj translację PAT z pulą adresów (pamiętaj, że ACL i pula są już skonfigurowane, więc jest to jedyne polecenie, które musimy zmienić z NAT na PAT).

```
R1(config)# ip nat inside source list 1 pool PUBLIC_ACCESS overload
```

Krok 3: Wykonaj testy i zweryfikuj konfigurację.

a. Sprawdźmy, czy PAT działa. Z poziomu komputera PC-B, wykonaj ping do interfejsu Lo1 (209.165.200.1) na R2. Jeżeli ping się nie powiedzie, znajdź błąd i popraw go. Na R1 wyświetl tablicę NAT za pomocą polecenia **show ip nat translations**.

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.226:1 192.168.1.3:1 209.165.200.1:1 209.165.200.1:1
Total number of translations: 1#
```

Na jaki adres wewnętrzny lokalny został przetłumaczony adres PC-B?

Jakim typem adresu NAT jest przetłumaczony adres?

Czym różni się wynik polecenia **show ip nat translations** od tego z ćwiczenia NAT?

b. Z poziomu komputera PC-A, wykonaj ping do interfejsu Lo1 (209.165.200.1) na R2. Jeżeli ping się nie powiedzie, znajdź błąd i popraw go. Na R1 wyświetl tablicę NAT za pomocą polecenia **show ip nat translations**.

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.226:1 192.168.1.2:1 209.165.200.1:1 209.165.200.1:1
Total number of translations: 1
```

Zwróć uwagę, że jest ponownie tylko jedno tłumaczenie. Wykonaj ping jeszcze raz i szybko wróć do routera i wydaj polecenie **show ip nat translations verbose** , a zobaczysz, co się stało.

```
R1# show ip nat translations verbose
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.226:1 192.168.1.2:1 209.165.200.1:1 209.165.200.1:1
  create: 09/23/19 16:57:22, use: 09/23/19 16:57:25, timeout: 00:01:00
<output omitted>
```

Jak widać, limit czasu tłumaczenia został zmniejszony z 24 godzin do 1 minuty.

c. Generuj ruch z wielu urządzeń, aby obserwować PAT. W przypadku PC-A i PC-B użyj parametru -t z poleceniem ping, aby wykonywać nieprzerwanie ping do interfejsu Lo1 R2 (**ping -t 209.165.200.1**), a następnie wróć do R1 i wydaj polecenie **show ip nat translations**:

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.226:1 192.168.1.2:1 209.165.200.1:1 209.165.200.1:1
icmp 209.165.200.226:2 192.168.1.3:1 209.165.200.1:1 209.165.200.1:2
Total number of translations: 2
```

Zauważ, że wewnętrzny adres globalny jest taki sam dla obu sesji.

W jaki sposób router śledzi powracające odpowiedzi?

d. PAT z pulą jest bardzo skutecznym rozwiązaniem dla małych i średnich organizacji. Jednak istnieją nieużywane adresy IPv4 zaangażowane w tym scenariuszu. Przejdziemy do PAT z przeciążeniem interfejsu, aby wyeliminować to marnowanie adresów IPv4. Zatrzymaj ping na PC-A i PC-B za pomocą kombinacji klawiszy Control-C, a następnie wyczyść tłumaczenia i statystyki tłumaczenia:

```
R1# clear ip nat translations *
R1# clear ip nat statistics
```

Krok 4: Na R1 usuń polecenia translacji nat pool.

Znowu, nasza lista dostępu (ACL 1) jest nadal poprawna dla scenariusza sieciowego, więc nie ma potrzeby jej odtworzenia. Ponadto interfejsy wewnętrzne i zewnętrzne nie ulegają zmianie. Aby rozpocząć korzystanie z protokołu PAT z interfejsem, wyczyść konfigurację, usuwając pulę NAT i polecenie, które łączy ze sobą ACL i pulę.

```
R1(config)# no ip nat inside source list 1 pool PUBLIC_ACCESS overload
R1(config)# no ip nat pool PUBLIC_ACCESS
```

Krok 5: Dodaj polecenie przeciążenia PAT, określając interfejs zewnętrzny.

Dodaj polecenie PAT, które spowoduje przeciążenie interfejsu zewnętrznego.

```
R1(config)# ip nat inside source list 1 interface g0/0/0 overload
```

Krok 6: Wykonaj testy i zweryfikuj konfigurację.

a. Sprawdźmy, czy działa PAT z interfejsem. Z poziomu komputera PC-B, wykonaj ping do interfejsu Lo1 (209.165.200.1) na R2. Jeżeli ping się nie powiedzie, znajdź błąd i popraw go. Na R1 wyświetl tablicę NAT za pomocą polecenia **show ip nat translations**.

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.230:1 192.168.1.3:1 209.165.200.1:1 209.165.200.1:1
Total number of translations: 1
```

b. Generuj ruch z wielu urządzeń, aby obserwować PAT. W przypadku PC-A i PC-B użyj parametru -t z poleceniem ping, aby wysłać non-stop ping do interfejsu Lo1 R2 **(ping -t 209.165.200.1**). W przypadku S1 i S2 wydaj polecenie trybu uprzywilejowanego ping 209.165.200.1 repeat 2000. Następnie wróć do R1 i wydaj polecenie **show ip nat translations**.

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.230:3 192.168.1.11:1 209.165.200.1:1 209.165.200.1:3
icmp 209.165.200.230:2 192.168.1.2:1 209.165.200.1:1 209.165.200.1:2
icmp 209.165.200.230:4 192.168.1.3:1 209.165.200.1:1 209.165.200.1:4
icmp 209.165.200.230:1 192.168.1.12:1 209.165.200.1:1 209.165.200.1:1
Total number of translations: 4
```

Teraz wszystkie wewnętrzne adresy globalne są mapowane na adres IP interfejsu g0/0/0.

Zatrzymaj wszystkie pingi. W przypadku PC-A i PC-B za pomocą kombinacji klawiszy CTRL-C.

Część 4: Konfigurowanie i weryfikacja statycznego NAT dla IPv4

W części 4 skonfigurujesz statyczny NAT tak, aby połączenie PC-A było bezpośrednio dostępne z Internetu. PC-A będzie osiągalny z R2 pod adresem 209.165.200.229.

Uwaga: Konfiguracja, którą chcesz ukończyć, nie jest zgodna z zalecanymi praktykami dla bram połączonych z Internetem. To ćwiczenie całkowicie pomija standardowe praktyki zabezpieczeń, aby skupić się na pomyślnej konfiguracji statycznej translacji NAT. W środowisku produkcyjnym zasadnicze znaczenie ma staranna koordynacja między infrastrukturą sieciową a zespołami bezpieczeństwa.

Krok 1: Na R1 wyczyść aktualne tłumaczenia i statystyki.

```
R1# clear ip nat translations *
R1# clear ip nat statistics
```

Krok 2: Na R1 skonfiguruj polecenie NAT wymagane do statycznego mapowania adresu wewnętrznego na adres zewnętrzny.

W tym kroku skonfiguruj mapowanie statyczne między 192.168.1.11 a 209.165.200.1 za pomocą następującego polecenia:

```
R1(config)# ip nat inside source static 192.168.1.2 209.165.200.229
```

Krok 3: Wykonaj testy i zweryfikuj konfigurację.

a. Sprawdźmy, czy statyczny NAT działa. Na R1 wyświetl tablicę NAT na R1 za pomocą polecenia **show ip nat translations**, i powinno zostać wyświetlone odwzorowanie statyczne.

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.229 192.168.1.2 --- ---
```

```
Total number of translations: 1
```

b. Tablica tłumaczeń pokazuje, że działa tłumaczenie statyczne. Sprawdź to, wykonując ping z R2 do 209.165.200.229. Test ping powinien zakończyć się pomyślnie.

Uwaga: Aby ping zakończył się pomyślnie, może być konieczne wyłączenie zapory ogniowej komputera.

c. Na R1 wyświetl tablicę NAT za pomocą polecenia **show ip nat translations** i powinieneś zobaczyć statyczne mapowanie i translację na poziomie portu dla przychodzących pingów.

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.229 192.168.1.2 --- ---
icmp 209.165.200.229:3 192.168.1.2:3 209.165.200.225:3 209.165.200.225:3
Total number of translations: 2
```

To potwierdza, że działa statyczny NAT.

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)	Seryjny 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)	Seryjny 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Seryjny 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.