

Laboratorium - Konfiguracja zaawansowanych właściwości protokołu OSPFv2

Topologia

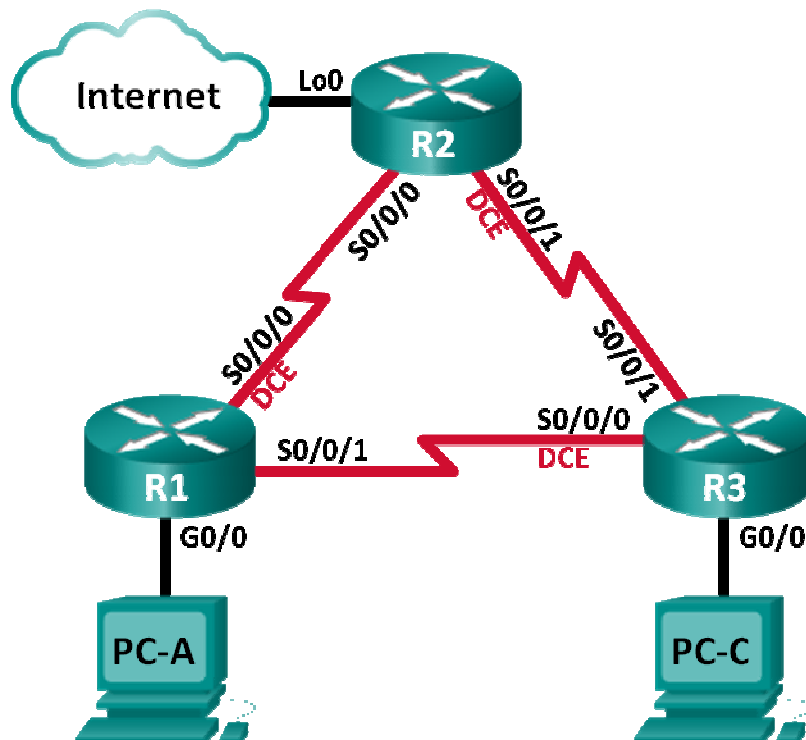


Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/0	192.168.1.1	255.255.255.0	nie dotyczy
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	nie dotyczy
	S0/0/1	192.168.13.1	255.255.255.252	nie dotyczy
R2	Lo0	209.165.200.225	255.255.255.252	nie dotyczy
	S0/0/0	192.168.12.2	255.255.255.252	nie dotyczy
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	nie dotyczy
R3	G0/0	192.168.3.1	255.255.255.0	nie dotyczy
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	nie dotyczy
	S0/0/1	192.168.23.2	255.255.255.252	nie dotyczy
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Cele

Część 1: Utworzenie sieci oraz skonfigurowanie podstawowych ustawień urządzenia

Część 2: Konfiguracja oraz weryfikacja routingu w oparciu o protokół OSPF

Część 3: Modyfikacja metryk OSPF

Część 4: Konfiguracja i rozsyłanie statycznych tras domyślnych.

Część 5: Konfiguracja uwierzytelniania OSPF

Tło / Scenariusz

Protokół OSPF posiada zaawansowane właściwości umożliwiające zmiany w kontroli metryk, propagacji trasy domyślnej oraz bezpieczeństwie.

W tym laboratorium będziesz dostosowywał metryki na interfejsach routera, konfigurował rozgłaszanie tras oraz użyjesz uwierzytelnienia MD5 w celu zabezpieczenia protokołu OSPF.

Uwaga: Routerami używanymi na laboratorium powinny być urządzenia Cisco 1941 z systemem Cisco IOS Release 15.2(4)M3. Inne routery i wersje systemu IOS również mogą być użyte. Zależnie od modelu urządzenia i wersji systemu IOS dostępne polecenia i wyniki ich działania mogą się różnić od prezentowanych w niniejszej instrukcji. Podczas laboratorium wykorzystaj identyfikatory interfejsów znajdujące się w tabeli interfejsów routerów umieszczonej na końcu tej instrukcji.

Uwaga: Sprawdź, czy konfiguracje routerów zostały skasowane i nie mają konfiguracji początkowych. Jeśli nie jesteś tego pewien, poproś o pomoc instruktora.

Wymagane wyposażenie

- 3 routery (Cisco 1941 z Cisco IOS Release 15.2(4)M3)
- 2 komputery PC (Windows 7, Vista, lub XP z emulatorem terminala takim jak Tera Term)
- Kable konsolowe do konfiguracji urządzeń Cisco przez port konsolowy
- Kable Ethernet i szeregowy powinny być zgodnie z topologia sieci.

Część 1: Budowanie sieci oraz konfiguracja podstawowych ustawień urządzeń

W części 1 zbudujesz topologię sieciową oraz skonfigurujesz podstawowe ustawienia komputerów i routerów.

Krok 1: Okabluj sieć zgodnie z topologią.

Krok 2: Zainicjuj i uruchom ponownie routery (jeśli jest to wymagane).

Krok 3: Skonfiguruj podstawowe ustawienia dla każdego routera.

- Wyłącz rozwiązywanie nazw domenowych.
- Przypisz nazwy urządzeniom zgodnie z topologią.
- Ustaw hasło dostępu do trybu uprzywilejowanego EXEC: **class**.
- Jako hasła dostępu do konsoli oraz VTY ustaw **cisco**.
- Zaszyfruj wszystkie hasła podane jako otwarty tekst.
- Skonfiguruj baner MOTD, aby ostrzec, że nieautoryzowany dostęp jest zabroniony.
- Skonfiguruj **logowanie synchroniczne (logging synchronous)** dla linii konsolowej.
- Skonfiguruj adresy IP, wypisane w tablicy adresacji, na wszystkich interfejsach.
- Ustaw taktowanie na wszystkich szeregowych interfejsach DCE jako 128000.
- Skopiuj bieżącą konfigurację do startowego pliku konfiguracyjnego.

Krok 4: Skonfiguruj komputery PC.

Skonfiguruj adresy IP na komputerach zgodnie z tabelą adresacji.

Krok 5: Test łączności.

W tym punkcie ćwiczenia komputery nie mają komunikacji z pozostałymi. Jednakże routery powinny łączyć się ze swoimi sąsiadami, a komputery powinny komunikować się ze swoimi bramami domyślnymi. Sprawdź łączność i rozwiąż ewentualne problemy z łącznością.

Część 2: Konfiguracja protokołu OSPF i weryfikacja konfiguracji

W części 2 skonfigurujesz routing OSPFv2 na wszystkich routerach w sieci, a następnie sprawdzisz, czy tablice routingu zostały poprawnie zaktualizowane.

Krok 1: Skonfiguruj ID na wszystkich routerach.

Przypisz 1 jako ID procesu. Każdy router powinien mieć ustawione następujące ID:

- ID routera R1: **1.1.1.1**
- ID routera R2: **2.2.2.2**
- ID routera R3: **3.3.3.3**

Krok 2: Skonfiguruj informacje sieciowe OSPF

Krok 3: Sprawdź routing OSPF

- Użyj polecenia **show ip ospf neighbor**, aby sprawdzić czy każdy router zna wszystkie pozostałe routery w sieci.
- Użyj polecenia **show ip route ospf**, aby sprawdzić, czy wszystkie sieci OSPF są obecne w tablicach routingu na wszystkich routerach.

Krok 4: Testowanie połączeń end-to-end.

Użyj polecenia ping na komputerze PC-A na adres komputera PC-C. Wykonanie polecenia powinno zakończyć się sukcesem. Jeżeli wystąpiło niepowodzenie, rozwiąż zaistniałe problemy.

Uwaga: Aby możliwa była komunikacja może wystąpić konieczność wyłączenia zapory sieciowej w komputerach.

Część 3: Zmiana metryk OSPF

W części 3 zmienisz metryki OSPF używając poleceń **bandwidth**, **auto-cost reference-bandwidth** oraz **ip ospf cost**. Wykonanie tych zmian zapewni bardziej precyzyjne metryki OSPF.

Uwaga: Wszystkie interfejsy szeregowo DCE powinny mieć ustawione taktowanie 128000, zgodnie z częścią 1 ćwiczenia.

Krok 1: Zmień szerokość pasma na wszystkich interfejsach szeregowych na 128kb/s.

- Użyj polecenia **show ip ospf interface brief**, aby wyświetlić domyślne ustawienia kosztu na interfejsach routera.

```
R1# show ip ospf interface brief
```

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Se0/0/1	1	0	192.168.13.1/30	64	P2P	1/1	
Se0/0/0	1	0	192.168.12.1/30	64	P2P	1/1	
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0	

- Użyj polecenia **bandwidth 128** na wszystkich interfejsach szeregowych.

- c. Użyj polecenia **show ip ospf interface brief**, aby sprawdzić nowe ustawienia kosztu.

R1# **show ip ospf interface brief**

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Se0/0/1	1	0	192.168.13.1/30	781	P2P	1/1	
Se0/0/0	1	0	192.168.12.1/30	781	P2P	1/1	
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0	

Krok 2: Zmień szerokość pasma odniesienia na routerach.

- a. Użyj polecenia **auto-cost reference-bandwidth 1000**, aby zmienić domyślną wartość szerokości pasma odniesienia na odpowiednią dla interfejsów Gigabit Ethernet.
- b. Użyj ponownie polecenia **show ip ospf interface brief**, aby zobaczyć, jak wykonanie tego polecenia zmieniło wartości kosztu.

R1# **show ip ospf interface brief**

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Se0/0/1	1	0	192.168.13.1/30	7812	P2P	0/0	
Se0/0/0	1	0	192.168.12.1/30	7812	P2P	0/0	
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0	

Uwaga: Jeżeli router ma interfejsy fastethernet zamiast gigabitowych, koszt na tych interfejsach powinien być równy 10.

Krok 3: Zmiana kosztu trasy

- a. Użyj polecenia **show ip route ospf**, aby wyświetlić aktualne trasy ospf na R1. Zauważ, że obecnie są dwie trasy w tablicy routingu, które używają interfejsu S0/0/1.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
 + - replicated route, % - next hop override

Gateway of last resort is not set

```
O 192.168.3.0/24 [110/7822] via 192.168.13.2, 00:00:12, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/15624] via 192.168.13.2, 00:00:12, Serial0/0/1
    [110/15624] via 192.168.12.2, 00:20:03, Serial0/0/0
```

- b. Użyj polecenia **ip ospf cost 16000** na interfejsie S0/0/1 routera R1. Koszt 16000 jest większy od skumulowanego kosztu na trasie przez R2, który wynosi 15624.
- c. Użyj polecenia **show ip interface brief**, aby sprawdzić koszt interfejsu S0/0/1.

R1# **show ip ospf interface brief**

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Se0/0/1	1	0	192.168.13.1/30	16000	P2P	1/1	
Se0/0/0	1	0	192.168.12.1/30	7812	P2P	1/1	
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0	

- d. Wykonaj ponownie polecenie **show ip route ospf** na routerze R1, aby wyświetlić efekt zmian, które zostały zrobione w tablicy routingu. Wszystkie trasy dla routera R1 prowadzą obecnie przez R2.

```
R1# show ip route ospf
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override
```

```
Gateway of last resort is not set
```

```
O      192.168.3.0/24 [110/15625] via 192.168.12.2, 00:05:31, Serial0/0/0
```

```
192.168.23.0/30 is subnetted, 1 subnets
```

```
O      192.168.23.0 [110/15624] via 192.168.12.2, 01:14:02, Serial0/0/0
```

Wyjaśnij, dlaczego trasa do sieci 192.168.3.0/24 na routerze R1 prowadzi obecnie przez R2.

Część 4: Konfiguracja i rozgłaszanie statycznej trasy domyślnej

W części 4 użyjesz interfejsu Loopback na R2 w celu zasymulowania połączenia routera ISP do sieci Internet. Stworzysz statyczną trasę domyślną na R2, a następnie OSPF rozgłosi ją do pozostałych routerów w sieci.

Krok 1: Skonfiguruj statyczną trasę domyślną na R2 na interfejs loopback 0.

Skonfiguruj trasę domyślną używając interfejsu loopback skonfigurowanego w części 1 w celu symulacji połączenia do ISP.

Krok 2: Wymuś rozgłaszanie statycznej trasy domyślnej.

Użyj polecenia **default-information originate**, aby umieścić statyczną trasę domyślną w aktualizacjach OSPF wysyłanych przez R2.

```
R2(config)# router ospf 1
```

```
R2(config-router)# default-information originate
```

Krok 3: Sprawdź rozgłaszanie statycznej trasy.

- a. Użyj polecenia **show ip route static** na R2.

```
R2# show ip route static
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override
```

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
```

```
S* 0.0.0.0/0 is directly connected, Loopback0
```

- b. Użyj polecenia **show ip route** na R1, aby sprawdzić czy otrzymano statyczną trasę z R2.

```
R1# show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```

```
Gateway of last resort is 192.168.12.2 to network 0.0.0.0
```

```
O*E2 0.0.0.0/0 [110/1] via 192.168.12.2, 00:02:57, Serial0/0/0
```

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, GigabitEthernet0/0
L      192.168.1.1/32 is directly connected, GigabitEthernet0/0
O      192.168.3.0/24 [110/15634] via 192.168.12.2, 00:03:35, Serial0/0/0
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.12.0/30 is directly connected, Serial0/0/0
L      192.168.12.1/32 is directly connected, Serial0/0/0
192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.13.0/30 is directly connected, Serial0/0/1
L      192.168.13.1/32 is directly connected, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O      192.168.23.0 [110/15624] via 192.168.12.2, 00:05:18, Serial0/0/0
```

- c. Sprawdź łączność w sieci poprzez użycie polecenie ping z komputera PC-A na adres ISP 209.165.200.225.

Czy wynik był pozytywny? _____

Część 5: Konfiguracja uwierzytelnienia OSPF

Uwierzytelnienie OSPF może zostać ustawione na poziomie łącza lub na poziomie obszaru. Istnieją trzy typy uwierzytelnienia dostępne w protokole OSPF: puste, tekst otwarty lub MD5. W części 5 użyjesz uwierzytelnienia MD5, które jest najsilniejsze z dostępnych.

Krok 1: Ustaw uwierzytelnienie MD5 na pojedynczym łączu.

- a. Użyj polecenia **debug ip ospf adj** na R2, aby wyświetlić wiadomości o przyległościach.

```
R2# debug ip ospf adj
```

```
OSPF adjacency debugging is on
```

- b. Przypisz klucz MD5 dla uwierzytelniania OSPF na interfejsie S0/0/0 routera R1.

```
R1(config)# interface s0/0/0
```

```
R1(config-if)# ip ospf message-digest-key 1 md5 MD5KEY
```

- c. Uaktywnij uwierzytelnienie MD5 na interfejsie S0/0/0 routera R1.

```
R1(config-if)# ip ospf authentication message-digest
```

Komunikaty debugowania poinformują na R2 o niepasującym typie uwierzytelniania.

```
*Mar 19 00:03:18.187: OSPF-1 ADJ Se0/0/0: Rcv pkt from 192.168.12.1 : Mismatched
Authentication type. Input packet specified type 2, we use type 0
```

- d. Na R2 użyj polecenia **u all**, która jest najkrótszą wersją polecenia **undebg all**, aby wyłączyć tryb debugowania.
- e. Skonfiguruj uwierzytelnienie na interfejsie S0/0/0 routera R2. Użyj tego samego hasła MD5, co dla R1.
- f. Użyj polecenia **show ip ospf interface s0/0/0** na R2. Polecenie wyświetla typ użytego uwierzytelniania.

```
R2# show ip ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.12.2/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 2.2.2.2, Network Type POINT_TO_POINT, Cost: 7812
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0                7812        no            no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
  Youngest key id is 1
```

Krok 2: Ustaw uwierzytelnienie na poziomie obszaru.

- a. Na R1 użyj polecenia **area 0 authentication**, aby ustawić uwierzytelnianie MD5 dla obszaru 0 protokołu OSPF.

```
R1(config)# router ospf 1
R1(config-router)# area 0 authentication message-digest
```

- b. Opcja ta wymaga jednak ustawienia hasła MD5 na poziomie interfejsu.

```
R1(config)# interface s0/0/1
R1(config-if)# ip ospf message-digest-key 1 md5 MD5KEY
```

- c. Na R3 użyj polecenia **show ip ospf neighbor**. R1 nie ma już przyległości z R3.

```
R3# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:31	192.168.23.1	Serial0/0/1

- d. Ustaw uwierzytelnianie na R3, używając tego samego hasła MD5 na interfejsie S0/0/0.

```
R3(config)# router ospf 1
R3(config-router)# area 0 authentication message-digest
R3(config-router)# interface s0/0/0
R3(config-if)# ip ospf message-digest-key 1 md5 MD5KEY
```

- e. Na R3 użyj polecenia **show ip ospf neighbor**. Zauważ, że R1 znajduje się na liście sąsiadów, ale brakuje R2.

R3# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	0	FULL/ -	00:00:38	192.168.13.1	Serial0/0/0

Dlaczego R2 nie jest już pokazywany jako sąsiad OSPF?

- f. Skonfiguruj uwierzytelnianie MD5 na poziomie obszaru na R2.

R2(config)# **router ospf 1**

R2(config-router)# **area 0 authentication message-digest**

- g. Przypisz **MD5KEY** jako hasło MD5 dla łącza pomiędzy R2 i R3.
- h. Użyj polecenia **show ip ospf neighbor** na wszystkich routerach, aby sprawdzić, że wszystkie przyległości znowu są obecne.

R1# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	0	FULL/ -	00:00:39	192.168.13.2	Serial0/0/1
2.2.2.2	0	FULL/ -	00:00:35	192.168.12.2	Serial0/0/0

R2# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	0	FULL/ -	00:00:36	192.168.23.2	Serial0/0/1
1.1.1.1	0	FULL/ -	00:00:32	192.168.12.1	Serial0/0/0

R3# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:33	192.168.23.1	Serial0/0/1
1.1.1.1	0	FULL/ -	00:00:39	192.168.13.1	Serial0/0/0

Do przemyślenia

1. Jaka jest najprostsza i preferowana metoda manipulowania kosztem trasy OSPF.

2. Co spowoduje użycie polecenia **default-information originate** w sieci, w której uruchomiony został protokół OSPF?

3. Dlaczego dobrym pomysłem jest używanie uwierzytelnienia OSPF?

Tabela zbiorcza interfejsów routera

Interfejsy routera podsumowanie				
Model routera	Interfejs Ethernet #1	Interfejs Ethernet #2	Interfejs Serial #1	Interfejs Serial #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)
<p>Uwaga: Aby poznać konfigurację routera, spójrz na jego interfejsy, określ ich liczbę oraz zidentyfikuj typ routera. Nie ma sposobu na skuteczne opisanie wszystkich kombinacji konfiguracji dla każdej klasy routera. Ta 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 może być interfejs ISDN BRI. Informacja w nawiasach jest dozwolonym skrótem, którego można używać w poleceniach IOS w celu odwołania się do interfejsu.</p>				