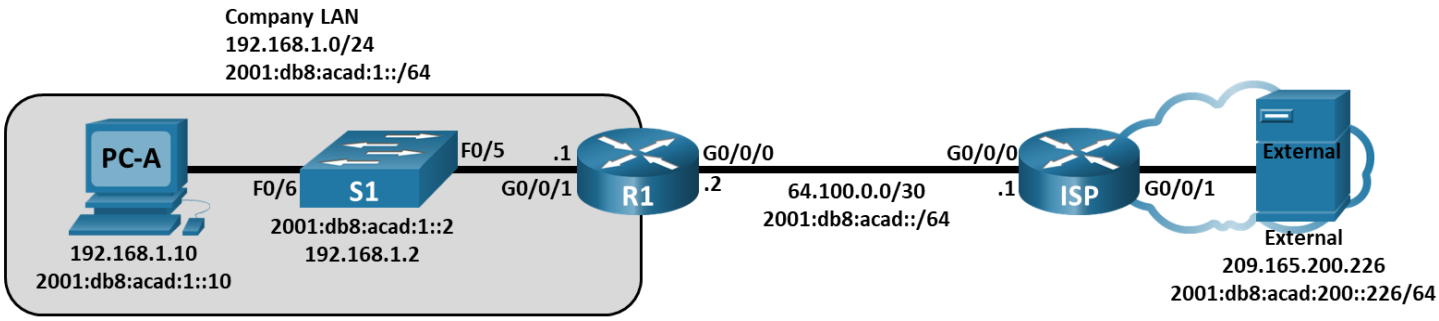
# Laboratorium - Stosowanie komendy ping oraz traceroute do testowania połączeń w sieci

## Topologia sieci




## Tabela adresowania

| Urządzenie | interfejs | Adres IP/Prefiks | Brama domyślna |
|---|---|---|---|
| R1 | G0/0/0 | 64.100.0.2 /30 | nd. |
| | | 2001:db8:acad::2 /64 | |
| | | fe80::2 | |
| R1 | G0/0/1 | 192.168.1.1/24 | nd. |
| | | 2001:db8:acad:1::1 /64 | |
| | | fe80::1 | |
| ISP | G0/0/0 | 64.100.0.1 /30 | nd. |
| | | 2001:db8:acad::1 /64 | |
| | | fe80::1 | |
| ISP | G0/0/1 | 209.165.200.225 /27 | nd. |
| | | 2001:db8:acad:200::225 /64 | |
| | | fe80::225 | |
| S1 | VLAN 1 | 192.168.1.2 /24 | 192.168.1.1 |
| | | 2001db8:acad:1::2 /64 | fe80::1 |
| | | fe80::10 | |
| PC-A | karta sieciowa | 2001:db8:acad:1::10 /64 | fe80::1 |
| | | 64.100.0.2 /30 | nd. |

| Urządzenie | interfejs | Adres IP/Prefiks | Brama domyślna |
|---|---|---|---|
| Zewnętrzny | karta sieciowa | 209.165.200.226 /27 | 209.165.200.225 |
| | | 2001:DB8:ACAD:200::226 /64 | FE80::225 |

## Cele

**Część 1: Budowanie i konfiguracja sieci**

**Część 2: Użycie polecenia ping do podstawowego testowania sieci**

**Część 3: Użycie poleceń tracert i traceroute do podstawowego testowania sieci.**

**Część 4: Rozwiązanie problemu z topologią**

## Wprowadzenie

Ping i traceroute to dwa narzędzia, które są nieodzowne w przypadku testowania łączności w sieciach TCP/IP. Ping jest programem użytkowym używanym do testowania osiągalności urządzenia w sieci IP. Program ten mierzy również tzw. round-trip time, czyli czas potrzebny na przesłanie wiadomości z hosta źródłowego do komputera docelowego i z powrotem. Ping jest dostępny w systemie Windows, systemach operacyjnych bazujących na UNIX oraz w systemie IOS (Internetwork Operating System) firmy Cisco.

Traceroute jest sieciowym narzędziem diagnostycznym służącym do wyświetlania trasy oraz pomiaru opóźnienia transmisji pakietów przesyłanych w sieci IP. Polecenie tracert jest dostępne w systemie Windows, a podobne narzędzie - traceroute - w systemach UNIX/Linux i Cisco IOS.

W tym laboratorium zostaną użyte polecenia **ping** i **traceroute** oraz ich różne opcje w celu zmodyfikowania zachowania tych poleceń. Do przeglądu poleceń zostaną użyte komputery PC i urządzenia Cisco. Wymagane konfiguracje urządzeń sieciowych Cisco są dostarczone z tym laboratorium.

**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 użyć również innych routerów i przełączników Cisco z różnymi wersjami 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, czy konfiguracje routerów oraz przełączników zostały wymazane i nie posiadają konfiguracji początkowej. Jeśli nie jesteś pewien, to poproś o pomoc instruktora.

**Domyślny, wbudowany** szablon używany przez Switch Database Manager (SDM) nie zapewnia możliwości adresowania IPv6.Upewnij się że SDM wykorzystuje szablon **dual-ipv4-and-ipv6** lub **lanbase-routing**. Nowy szablon będzie użyty po restarcie urządzenia nawet jeśli konfiguracja nie zostanie zapisana.

```
S1# show sdm prefer
```

Użyj następujących poleceń, aby przypisać szablon **dual-ipv4-i-ipv6** jako domyślny szablon SDM.

```
S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

## Wymagane zasoby

- 2 routery (Cisco 4221 z uniwersalnym obrazem Cisco IOS XE Release 16.9.4 lub porównywalnym)

- 1 przełącznik (Cisco 2960 z systemem Cisco IOS wersja15.2 (2) obraz lanbasek9 lub porównywalny)
- 2 komputery PC (Windows z emulatorem terminala takim jak Tera Term)
- Kable konsolowe do konfiguracji urządzeń Cisco przez porty konsolowe
- Kable Ethernet i szeregowe powinny być zgodnie z topologia sieci.

## Instrukcje

## Część 1: Wykonaj i skonfiguruj sieć

W Części 1 należy skonfigurować sieć zgodnie z topologią oraz skonfigurować komputery PC i urządzenia Cisco. Wstępna konfiguracja routerów i przełączników znajduje się niniejszej instrukcji. W tej topologii routing statyczny służy do kierowania pakietów między sieciami.

### Krok 1: Zbuduj sieć zgodnie z topologią.

### Krok 2: Wykasuj konfiguracje routerów i przełączników, ponownie uruchom urządzenia.

### Krok 3: Skonfiguruj adresy IP i domyślne bramy komputerów PC zgodnie z tabelą adresacji.

### Krok 4: Skonfiguruj routery R1 i ISP oraz przełącznik S1, korzystając z początkowych konfiguracji podanych poniżej.

W trybie konfiguracji globalnej routera lub przełącznika skopiuj i wklej konfiguracje dla każdego urządzenia. Zapisz bieżącą konfigurację do konfiguracji startowej.

**Wstępna konfiguracja routera R1:**

```
hostname R1
no ip domain lookup
ipv6 unicast-routing.
interface g0/0/0
ip address 64.100.0.2 255.255.255.252
ipv6 address 2001:db8:acad::2/64
ipv6 address fe80::2 link-local
ip nat outside
no shutdown
interface g0/0/1
ip add 192.168.1.1 255.255.255.0
ipv6 address 2001:db8:acad:1::1/64
ipv6 address fe80::1 link-local
ip nat inside
no shutdown
ip route 0.0.0.0 0.0.0.0 64.100.0.1
ipv6 route 0::/0 2001:db8:acad::1
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface g0/0/0 overload
```

**Wstępna konfiguracja dla routera ISP:**

```
hostname ISP
no ip domain lookup
```

```
ipv6 unicast-routing
interface g0/0/0
ip address 64.100.0.1 255.255.255.252
ipv6 adres 2001:db8:acad: :1/64
ipv6 address fe80::1 link-local
no shutdown
interface g0/0/1
ip add 209.165.200.225 255.255.255.224
ipv6 address 2001:db8:acad:200::225/64
ipv6 address fe80::225 link-local
no shutdown
ipv6 route ::/0 2001:db8:acad::2
```

**Wstępna konfiguracja S1:**

```
hostname S1
no ip domain-lookup
interface vlan 1
ip add 192.168.1.2 255.255.255.0
ipv6 address 2001:db8:acad:1::2/64
ipv6 address fe80::2 link-local
no shutdown
exit
ip default-gateway 192.168.1.1
end
```

### Krok 5: Skonfiguruj tablicę IP hostów na routerze R1.

Tablica IP hostów umożliwia używanie nazwy hosta zamiast adresu IP do połączenia ze zdalnym urządzeniem. Tablica hostów dostarcza nazw dla urządzeń zgodnie z poniższą konfiguracją. Skopiuj i wklej poniższą konfigurację dla routera R1.Te konfiguracje pozwolą użyć nazw hostów dla polecenia **ping** i **traceroute** na routerze R1.

```
ip host Externalv4 209.165.200.226
ip host Externalv6 2001:db8:acad:200::226
ip host ISPv4 64.100.0.1
ip host ISPv6 2001:db8:acad::1
ip host PC-Av4 192.168.1.10
ip host PC-Av6 2001:db8:acad:1::10
ip host R1v4 64.100.0.2
ip host R1v6 2001:db8:acad::2
ip host S1v4 192.168.1.2
ip host S1v6 2001:db8:acad:1::2
end
```

## Część 2: Użycie polecenia ping do podstawowego testowania sieci

W części 2 tego laboratorium użyj polecenia **ping** do weryfikacji łączności pomiędzy urządzeniami. Ping wysyła komunikat echo request protokołu ICMP do hosta docelowego i oczekuje na odpowiedz ICMP. Może

odnotowywać czas przesłania pakietu w obie strony (round trip time), zaginięcie któregokolwiek pakietu lub pętlę routingu.

Pakiety IP mają ograniczony czas życia w sieci. Pakiety IP używają 8-bitowej wartości pola nagłówka Time to Live (IPv4) lub Hop Limit (IPv6), która określa maksymalną liczbę przeskoków warstwy trzeciej, które mogą być przemierzane na ścieżce do miejsca docelowego. Hosty w sieci ustawią własną wartość 8-bitową z maksymalną wartością 255.

Tak więc za każdym razem, gdy pakiet IP dociera do urządzenia sieciowego warstwy trzeciej ta wartość jest zmniejszana o jeden, zanim zostanie przekazany do miejsca docelowego. Więc jeśli ta wartość ostatecznie osiągnie zero, pakiet IP zostanie odrzucony.

Zaobserwujesz wynik działania polecenia **ping** i dodatkowych opcji tego polecenia, które są dostępne w systemie Windows i na urządzeniach Cisco.

## Krok 1: Przetestuj łączność z sieci routera R1 używając PC-A.

Wszystkie testy ping z PC-A do innych urządzeń w topologii powinny zakończyć się sukcesem. Jeśli nie, sprawdź topologię i okablowanie, jak również konfigurację urządzeń Cisco i komputerów PC.

a. Wykonaj polecenie ping do domyślnej bramy PC-A (interfejsu GigabitEthernet 0/0/1 routera R1).

```
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

W tym przykładzie 4 żądania ICMP, każde po 32 bajty, zostały wysłane i odpowiedzi zostały odebrane w czasie poniżej jednej milisekundy, bez utraty żadnego pakietu. Czas transmisji i odpowiedzi może się wydłużyć, ponieważ żądania i odpowiedzi ICMP są przetwarzane przez więcej urządzeń podczas podróży do i z miejsca docelowego.

Można to również zrobić przy użyciu adresu IPv6 bramy domyślnej (interfejs GigaitEthernet 0/0/1 R1).

```
C:\> ping 2001:db8:acad:1::1
Pinging 2001:db8:acad:1::1 with 32 bytes of data:
Reply from 2001:db8:acad:1::1: time=5ms
Reply from 2001:db8:acad:1::1: time=1ms
Reply from 2001:db8:acad:1::1: time=1ms
Reply from 2001:db8:acad:1::1: time=1ms

Ping statistics for 2001:db8:acad:1::1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 5ms, Average = 2ms
```

b. Z PC-A wykonaj polecenie ping do adresów umieszczonych w poniższej tabeli i zapisz średni czas przesłania w obie strony (round-trip time) oraz TTL (Time To Live) lub Hop Limit. **Opcjonalnie**: Użyj WireShark, aby zobaczyć wartość limitu przeskoków IPv6.

| Odbiorca | Średni czas odpowiedzi (Round Trip Time) (ms) | TTL/Hop Limit |
|---|---|---|
| 192.168.1.10 | | |
| 2001:db8:acad:1::10 | | |
| 192.168.1.1 (R1) | | |
| 2001:db8:acad:1::1 (R1) | | |
| 192.168.1.2 (S1) | | |
| 2001:db8:acad:1::2(S1) | | |
| 64.100.0.2 (R1) | | |
| 2001:DB8:ACAD::2 (R1) | | |
| 64.100.0.1 (ISP) | | |
| 2001:DB8:ACAD::1 (ISP) | | |
| 209.165.200.225 (ISP G0/0/1) | | |
| 2001:DB8:ACAD:200::225 (ISP G0/0/1) | | |
| 209.165.200.226 (zewnętrzny) | | |
| 2001:DB8:ACAD:200::226 (zewnętrzny) | | |

## Krok 2: Użycie rozszerzonego polecenia ping na komputerze PC.

Domyślnie polecenie **ping** wysyła cztery żądania, po 32 bajty każde. Czeka 4000 milisekund (4 sekundy) na każdą odpowiedź, zanim wyświetli komunikat Upłyną limit żądania (Request timed out).Polecenie **ping** może być dodatkowo dostosowane w celu lepszego wykrywania błędów w sieci.

a. W linii poleceń wpisz **ping** i naciśnij Enter.

```
C:\>ping
```

b. Używając opcji **-t** wykonaj polecenie ping aby sprawdzić czy zewnętrzny jest osiągalny.

```
C:\Users\User1>ping -t 209.165.200.226
```

Aby zilustrować wyniki, gdy host jest nieosiągalny, odłącz kabel między routerem ISP a zewnętrznym lub wyłącz interfejs GigabitEthernet 0/0/1 na routerze ISP.

Gdy sieć funkcjonuje poprawnie, polecenie **ping** może określić czy urządzenie docelowe odpowiedziało i jak dużo czasu trwało odbieranie od niego odpowiedzi. Gdy w sieci występują problemy z połączeniem, polecenie **ping** wyświetla komunikat o błędzie.

c. Podłącz ponownie kabel Ethernet lub włącz interfejs GigabitEthernet 0/0/1 na routerze ISP (używając polecenia **no shutdown**) przed przejściem do następnego kroku. Po około 30 sekundach ping powinien kończyć się ponownie sukcesem.

d. Naciśnij **Ctrl** + **C** aby zatrzymać wykonywanie polecenia ping.

e. Powyższe kroki można powtórzyć dla adresu IPv6, aby uzyskać komunikat o błędzie ICMP.

Jakie komunikaty o błędach ICMP otrzymałeś?

f. Włącz interfejs GigabitEthernet 0/0/1 na routerze ISP (używając polecenia **no shutdown**) przed przejściem do następnego kroku. Po około 30 sekundach ping powinien kończyć się ponownie sukcesem.

## Krok 3: Przetestuj łączność z sieci routera R1 używając urządzeń Cisco.

Polecenie **ping** jest dostępne również na urządzeniach Cisco. W tym kroku polecenie **ping** jest sprawdzane przy użyciu routera R1 i przełącznika S1.

a. Wykonaj ping do hosta w sieci zewnętrznej przy użyciu adresu IP 209.165.200.226 z routera R1.

```
R1# ping 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Wykrzyknik (!) wskazuje, że ping zakończył się pomyślnie z routera R1 do zewnętrznego. Podróż w obie strony trwa średnio 1 ms bez utraty pakietów, o czym świadczy 100% wskaźnik sukcesu.

b. Ponieważ lokalna tablica hostów została skonfigurowana na routerze R1, możesz wykonywać ping na Externalv4 w sieci zewnętrznej za pomocą nazwy hosta skonfigurowanej z routera R1.

**Uwaga**: W nazwie hosta nie jest rozróżniana wielkość liter. Możesz zastąpić nazwę hosta adresem IP, jeśli chcesz na R1 w tym laboratorium.

```
R1# ping externalv4
```

Jaki adres IP został użyty?

c. Dla polecenia **ping** dostępnych jest więcej opcji. W CLI wpisz **ping** i naciśnij Enter. Użyj **ipv6** jako protokołu. Wprowadź **2001:DB8:ACAD:200::226** lub **zewnętrzny** dla docelowego adresu IPv6.Naciśnij Enter aby zaakceptować domyślne wartości dla innych opcji.

```
R1# ping
Protocol [ip]: ipv6
Target IPv6 address: 2001:db8:acad:200::226
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands?[no]:
Sweep range of sizes?[no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:200::226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

d. Możesz użyć rozszerzonej wersji polecenia ping do obserwacji problemów w sieci. Uruchom polecenie **ping** do 209.165.200.226 z liczbą powtarzań 50000.Następnie odłącz kabel między routerem ISP a EXTERNAL lub wyłącz interfejs GigabitEthernet 0/0/1 na routerze ISP.

Podłącz ponownie kabel Ethernetowy lub włącz interfejs GigabitEthernet na routerze ISP po tym jak wykrzyknik (!) zostanie zastąpiony literą U i kropkami (.).Po około 30 sekundach ping powinien kończyć się ponownie sukcesem. Naciśnij **Ctrl** + **Shift** + **6** aby zatrzymać wykonywanie polecenia **ping**, jeśli zachodzi taka potrzeba.

```
R1# ping
```

```
Protocol [ip]:
Target IP address: 209.165.200.226
Repeat count [5]: 10000
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Sending 500, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.U.U.U.U.U.
U.U.................!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
Success rate is 99 percent (9970/10000), round-trip min/avg/max = 1/1/10 ms
```

Litera U oznacza, że urządzenie docelowe jest nieosiągalne. Router R1 odebrał jednostkę danych protokołu błędu (PDU).Każdy kropka (.) w danych wyjściowych wskazuje, że upłynął limit czasu ping podczas oczekiwania na odpowiedź z Zewnętrznego. W tym przykładzie 1% pakietów zostało utraconych podczas symulowanej przerwy w sieci.

**Uwaga** : Możesz także użyć następującego polecenia aby uzyskać ten sam rezultat:

```
R1# ping 209.165.200.226 repeat 10000
```

lub

```
R1# ping 2001:db8:acad:200::226 repeat 10000
```

Komenda **ping** jest bardzo przydatna w usuwaniu problemów z łącznością w sieci. Jednakże ping nie może wskazać lokalizacji problemu w przypadku niepowodzenia. Polecenie **tracert** (lub **traceroute**) może wyświetlić opóźnienie sieci i informację o ścieżce.

## Część 3: Użycie poleceń tracert i traceroute do podstawowego testowania sieci.

Polecenia do śledzenia tras można znaleźć na komputerach PC i urządzeniach sieciowych. Dla komputerów PC wykorzystujących system Windows polecenie **tracert** używa komunikatów ICMP do śledzenia ścieżki do urządzenia docelowego. Polecenie **traceroute** używa protokołu UDP (User Datagram Protocol) do śledzenia tras do urządzeń docelowych w przypadku urządzeń Cisco i komputerów wykorzystujących system operacyjny bazujący na UNIX.

W części 3 zbadasz polecenie traceroute i określisz ścieżkę, którą pakiet podróżuje do urządzenia docelowego. Użyjesz polecenia **tracert** z komputera PC z systemem Windows oraz polecenia **traceroute** z urządzenia Cisco. Sprawdzisz również dostępne opcje polecenia traceroute

### Krok 1: Użyj polecenia trecert z PC-A do External.

a. W wierszu polecenia wpisz **tracert 209.165.200.226**.

```
C:\>tracert 209.165.200.226
```

Wyniki tracert wskazują, że ścieżka z PC-A do External prowadzi z PC-A do R1 do ISP do External. Ścieżka do External przeszła przez dwa przeskoki routera do ostatecznego miejsca docelowego External.

### Krok 2: Przejrzyj dodatkowe opcje polecenia tracert.

a. W wierszu polecenia wpisz polecenie **tracert** i naciśnij klawisz Enter, aby wyświetlić dostępne opcje.

```
C:\>tracert
```

b. Użyj opcji **-d** .Należy zauważyć, że adres IP z dnia 209.165.200.226 nie jest odwzorowany jako zewnętrzny.

```
C:\>tracert -d 209.165.200.226
```

### Krok 3: Użyj polecenia traceroute z routera R1 na External.

W wierszu polecenia wpisz **traceroute 209.165.200.226** lub **traceroute 2001:db8:acad:200::226** na routerze R1.Nazwy hostów są odwzorowane, ponieważ na routerze R1 została skonfigurowana tablica IP hostów.

```
R1# traceroute 209.165.200.226


R1# traceroute 2001:db8:acad:200::226
```

### Krok 4: Użyj polecenia traceroute z przełącznika S1 na External.

W wierszu polecenia wpisz **traceroute 209.165.200.226** lub **traceroute 2001:db8:acad:200::226** na przełączniku S1.Nazwy hostów nie są wyświetlane w wynikach polecenia traceroute ponieważ nie została na tym przełączniku skonfigurowana lokalna tablica IP hostów.

```
S1# traceroute 209.165.200.226


S1# traceroute 2001:db8:acad:200::226
```

Polecenie **traceroute** posiada dodatkowe opcje. Aby je zobaczyć możesz użyć znaku zapytania **?** lub po prostu nacisnąć Enter po wpisaniu **traceroute** w wierszu poleceń.

Poniższy odnośnik dostarcza więcej informacji odnośnie poleceń **ping** i **traceroute** dla urządzeń Cisco:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6057.shtml

## Część 4: Rozwiązywanie problemów topologii

### Krok 1: Skopiuj i wklej następującą konfigurację do routera ISP.

```
hostname ISP
interface g0/0/0
ip address 64.100.0.1 255.255.255.252
ipv6 address 2001:db8:acad::1/64
no shutdown
interface g0/0/1
ip address 192.168.8.1 255.255.255.0
no ipv6 address 2001:db8:acad:200::225/64
ipv6 address 2001:db8:acad:201::225/64
no shutdown
end
```

### Krok 2: Z sieci routera R1 użyj polecenia ping i tracert lub tracerote do rozwiązania problemu w sieci routera ISP.

a. Użyj poleceń **ping** i **tracert** z PC-A.

Możesz użyć polecenia **tracert** aby zweryfikować łączność w sieci. Poniższy wynik polecenia tracert wskazuje, że PC-A jest w stanie dotrzeć do swojej bramy domyślnej 192.168.1.1, ale nie ma połączenia sieciowego z PC-A.

Jednym ze sposobów zlokalizowania problemu z siecią jest pingowanie każdego skoku w sieci do zewnętrznego hosta. Najpierw ustal, czy PC-A może dotrzeć do interfejsu routera ISP g0/0/0 z adresem IP 64.100.0.1.

b. PC-A może osiągnąć router ISP. Na podstawie udanych wyników ping z PC-A do routera ISP, problem z łącznością sieciową dotyczy sieci 209.165.200.224/24.Wykonaj ping z domyślnej bramy na zewnętrzny host, który jest interfejsem GigabitEthernet 0/0/1 routera ISP.

PC-A nie może osiągnąć interfejsu GigabitEthernet 0/0/1 routera ISP, jak widać z rezultatów polecenia **ping**.

Wyniki tracert i ping wskazują, że PC-A może dotrzeć do routerów R1 i ISP, ale nie do zewnętrznej lub domyślnej bramy zewnętrznej.

c. Użyj polecenia **show** aby sprawdzić bieżącą konfigurację routera ISP.

Wynik poleceń **show run** i **sh ip interface brief** wskazują, że interfejs GigabitEthernet 0/0/1 działa (up/up), ale został skonfigurowany z niewłaściwym adresem IP.

d. Popraw znalezione problemy.

e. Zweryfikuj poleceniami ping i traceroute, że zewnętrzny host jest osiągalny z PC-A.

**Uwaga**: To samo może być wykonane używając poleceń **ping** i **traceroute** z CLI routera ISP i przełącznika S1 po weryfikacji, że nie ma problemów z połączeniem w sieci 192.168.1.0/24.

f. Teraz powtórz proces łączności IPv6.**Uwaga**: Jeśli znajdziesz niepoprawny adres IPv6, musisz go usunąć, ponieważ nie jest on zastąpiony przez nowe polecenie adresu IPv6.

## Pytania do przemyślenia

1. Co oprócz problemów z łącznością w sieci mogłoby zatrzymać odpowiedzi ping lub traceroute na drodze powrotnej do urządzenia źródłowego?

2. Jeśli testujesz nieistniejący adres w sieci zdalnej, taki jak 209.165.200.227, jaki jest komunikat wyświetlany przez polecenie **ping** ?Co to oznacza? Jeśli testujesz prawidłowy adres hosta i otrzymasz tę odpowiedź, co powinieneś sprawdzić?

3. Jeśli wykonujesz ping na adres, który nie istnieje w żadnej sieci w Twojej topologii, taki jak 192.168.5.3, z komputera PC z systemem Windows, to jaki komunikat jest wyświetlany przez polecenie **ping**? Co wskazuje ta wiadomość?

4. Jaka jest wartość IPv4 TTL ustawiona na hoście Windows? Jaka jest wartość IPv4 TTL ustawiona na urządzeniu Cisco?

5. Jaka jest wartość Hop Limit IPv6 ustawiona na hoście Windows? Jaka jest wartość Hop Limit IPv6 ustawiona na urządzeniu Cisco?

## Tabela zbiorcza interfejsów routerów

| Model routera | Interfejs Ethernet nr 1 | Interfejs Ethernet nr 2 | Interfejs szeregowy nr 1 | Interfejs szeregowy nr 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) |
| 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.