Laboratorium - Testowanie połączeń sieciowych przy użyciu ping i traceroute

Topologia

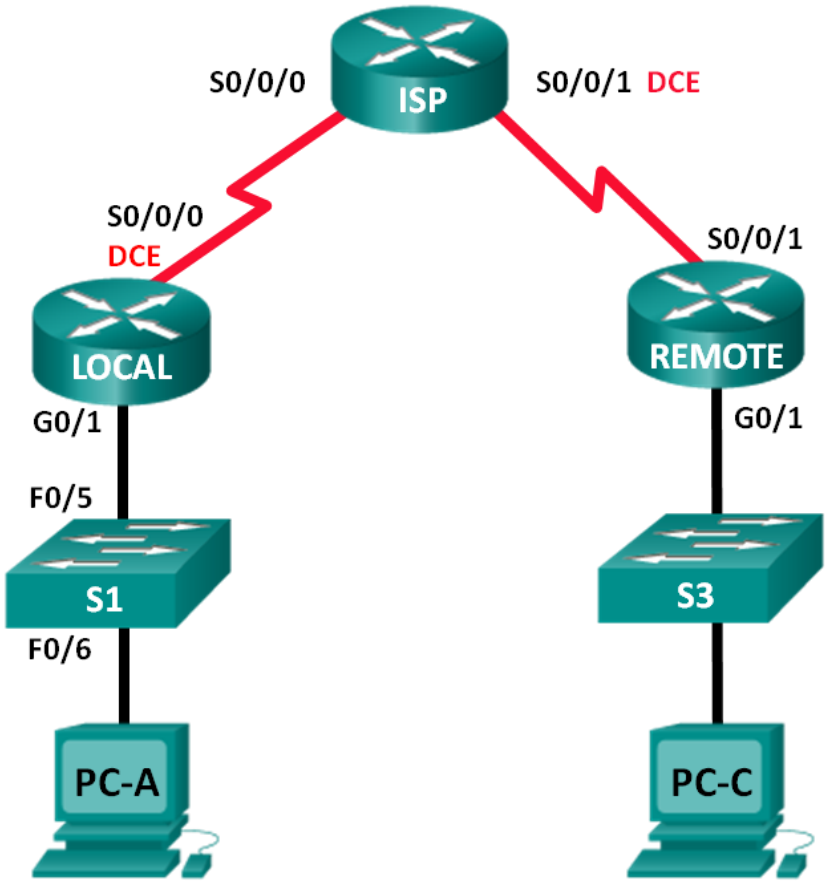

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
LOCAL	G0/1	192.168.1.1	255.255.255.0	Nie dotyczy
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Nie dotyczy
ISP	S0/0/0	10.1.1.2	255.255.255.252	Nie dotyczy
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Nie dotyczy
REMOTE	G0/1	192.168.3.1	255.255.255.0	Nie dotyczy
	S0/0/1	10.2.2.1	255.255.255.252	Nie dotyczy
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.3.11	255.255.255.0	192.168.3.1
PC-A	Karta sieciowa	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	Karta sieciowa	192.168.3.3	255.255.255.0	192.168.3.1

Cele

Część 1: Budowanie i konfiguracja sieci

- Połączenie okablowania sieci
- Konfiguracja komputerów PC
- Konfiguracja routerów
- Konfiguracja przełączników

Część 2: Użycie polecenia ping do podstawowego testowania sieci

- Użycie polecenia ping z PC
- Użycie polecenia ping z urządzeń Cisco

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

- Użycie tracert z PC
- Użycie traceroute z urządzeń Cisco

Część 4: Rozwiązanie problemu z topologią

Scenariusz

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. Routery Cisco będą używać protokołu EIGRP (Enhanced Interior Gateway Routing Protocol) do trasowania pakietów między sieciami. Wymagane konfiguracje urządzeń sieciowych Cisco są dostarczone z tym laboratorium.

Uwaga: Routery używane w laboratorium to Cisco 1941 ISR (Integrated Services Routers) z oprogramowaniem Cisco IOS 15.2(4)M3 (obraz universalk9). Przełączniki używane w laboratorium to Cisco Catalyst 2960s z oprogramowaniem Cisco IOS 15.0(2) (obraz lanbasek9). Inne routery, przełączniki i wersje systemu IOS również mogą być użyte. Zależnie od modelu urządzenia i wersji systemu IOS dostępne komendy i wyniki ich działania mogą się różnić od prezentowanych w niniejszej instrukcji. Identyfikatory interfejsów znajdują się w tabeli Interfejsów routerów na końcu tej instrukcji.

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

Wymagane wyposażenie

- 3 routery (Cisco 1941 z Cisco IOS Release 15.2(4)M3 obraz universal lub porównywalny)
- 2 przełączniki (Cisco 2960 z Cisco IOS Release 15.0(2) obraz lanbasek9 lub porównywalny)
- 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 Ethernetowe i szeregowe, zgodnie z topologią.

Część 1: Budowa i konfiguracja sieci

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 do przekazywania pakietów między sieciami używany jest protokół EIGRP.

Krok 1: Połącz okablowanie 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 LOCAL, ISP i REMOTE używając konfiguracji dostępnych poniżej.

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

Wstępna konfiguracja routera LOCAL:

```
hostname LOCAL
no ip domain-lookup
interface s0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 56000
 no shutdown
interface g0/1
 ip add 192.168.1.1 255.255.255.0
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
```

```
 network 192.168.1.0 0.0.0.255
 no auto-summary
```

Wstępna konfiguracja dla routera ISP:

```
hostname ISP
no ip domain-lookup
interface s0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
interface s0/0/1
 ip add 10.2.2.2 255.255.255.252
 clock rate 56000
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 no auto-summary
end
```

Wstępna konfiguracja dla routera REMOTE:

```
hostname REMOTE
no ip domain-lookup
interface s0/0/1
 ip address 10.2.2.1 255.255.255.252
 no shutdown
interface g0/1
 ip add 192.168.3.1 255.255.255.0
 no shutdown
router eigrp 1
 network 10.2.2.0 0.0.0.3
 network 192.168.3.0 0.0.0.255
 no auto-summary
end
```

Krok 5: Skonfiguruj wstępnie przełączniki S1 i S3.

Wstępna konfiguracja S1:

```
hostname S1
no ip domain-lookup
interface vlan 1
 ip add 192.168.1.11 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.1.1
end
```

Wstępna konfiguracja dla S3:

```
hostname S3
no ip domain-lookup
interface vlan 1
 ip add 192.168.3.11 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.3.1
end
```

Krok 6: Skonfiguruj tablicę IP hostów na routerze LOCAL.

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 LOCAL. Te konfiguracje pozwolą użyć nazw hostów dla polecenia **ping** i **traceroute** na routerze LOCAL.

```
ip host REMOTE 10.2.2.1 192.168.3.1
ip host ISP 10.1.1.2 10.2.2.2
ip host LOCAL 192.168.1.1 10.1.1.1
ip host PC-C 192.168.3.3
ip host PC-A 192.168.1.3
ip host S1 192.168.1.11
ip host S3 192.168.3.11
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) i zaginięcie któregokolwiek pakietu.

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 LOCAL 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 0/1 routera LOCAL).

```
C:\Users\User1> ping 192.168.1.1
Badanie 192.168.1.1 z 32 bajtami danych:
Odpowiedź z 192.168.1.1: bajtów=32 czas<1ms TTL=255
Odpowiedź z 192.168.1.1: bajtów=32 czas<1ms TTL=255
Odpowiedź z 192.168.1.1: bajtów=32 czas<1ms TTL=255
Odpowiedź z 192.168.1.1: bajtów=32 czas<1ms TTL=255

Statystyka badania ping dla 192.168.1.1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty)
Szacunkowy czas błądzenia pakietów w milisekundach:
    Minimum = 0ms, Maksimum = 0ms, Średnia = 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 ICMP zwiększa się wraz ze wzrostem liczby urządzeń pośredniczących w transmisji do i z urządzenia docelowego.

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).

Adres docelowy	Średni czas błądzenia (Round Trip Time) (ms)	TTL
192.168.1.1 (LOCAL)		
192.168.1.11 (S1)		
10.1.1.1 (LOCAL)		
10.1.1.2 (ISP)		
10.2.2.2 (ISP)		
10.2.2.1 (REMOTE)		
192.168.3.1 (REMOTE)		
192.168.3.11 (S3)		
192.168.3.3 (PC-C)		

Odnotuj średni czas przesłania w obie strony (Round Trip Time) do 192.168.3.3 (PC-C). Czas wzrósł ponieważ żądania ICMP były przetwarzane przez trzy routery zanim PC-A otrzymał odpowiedź od PC-C.

```
C:\Users\User1> ping 192.168.3.3
Badanie 192.168.3.3 z użyciem 32 bajtów danych:
Odpowiedź z 192.168.3.3: bajtów=32 czas=41ms TTL=125
Odpowiedź z 192.168.3.3: bajtów=32 czas=41ms TTL=125
Odpowiedź z 192.168.3.3: bajtów=32 czas=40ms TTL=125
Odpowiedź z 192.168.3.3: bajtów=32 czas=41ms TTL=125

Statystyka badania ping dla 192.168.3.3:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty)
Szacunkowy czas błądzenia pakietów w milisekundach:
    Minimum = 40ms, Maksimum = 41ms, Czas średni = 40ms
```

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:\Users\User1> ping
Sposób użycia: ping [-t] [-a] [-n liczba] [-l rozmiar] [-f] [-i TTL] [-v TOS]
            [-r liczba] [-s liczba] [[-j lista_hostów] | [-k lista_hostów]]
            [-w limit_czasu] [-R] [-S adres_zrodlowy] [-4] [-6] nazwa_celu

Opcje:
```

```
    -t             Odpytuje określonego hosta do czasu zatrzymania.
                   Aby przejrzeć statystyki i kontynuować, naciśnij klawisze
Control+Break.
                   Aby zakończyć naciśnij klawisze Control+C.
    -a             Tłumacz adresy na nazwy hostów.
    -n Liczba       Liczba wysłanych powtórzeń żądania.
    -l rozmiar      Rozmiar bufora wysyłania.
    -f  Ustawia w pakiecie flagę "Nie fragmentuj" (tylko IPv4).
    -i TTL         Czas wygaśnięcia.
    -v Typ usługi (tylko IPv4).  To ustawienie zostało zaniechane
                   i nie ma wpływu na wartość pola typu usługi w nagłówku IP.
    -r liczba Rejestruje trasę dla podanej liczby przeskoków (tylko IPv4).
    -s liczba Sygnatura czasowa dla podanej liczby przeskoków (tylko IPv4).
    -j lista_hostów Swobodna trasa źródłowa według listy lista_hostów (tylko IPv4).
    -k lista_hostów Ściśle określona trasa źródłowa według listy lista_hostów (tylko
IPv4).
    -w limit-czasu     Limit czasu oczekiwania na odpowiedź (w milisekundach).
    -R  Powoduje użycie nagłówka routingu w celu dodatkowego testowania trasy
wstecznej (tylko IPv6).
    -S adres_źródłowy Adres źródłowy do użycia.
    -4 Wymusza używanie IPv4.
    -6 Wymusza używanie IPv6.
```

b. Używając opcji **-t** wykonaj polecenie ping aby sprawdzić, czy PC-C jest osiągalny.

```
C:\Users\User1> ping –t 192.168.3.3
Odpowiedź z 192.168.3.3: bajtów=32 czas=41ms TTL=125
Odpowiedź z 192.168.3.3: bajtów=32 czas=40ms TTL=125
```

Aby zilustrować wynik w przypadku, kiedy host jest nieosiągalny, rozłącz kabel pomiędzy routerem REMOTE a przełącznikiem S3 lub wyłącz interfejs GigabitEthernet 0/1 na routerze REMOTE.

```
Odpowiedź z 192.168.3.3: bajtów=32 czas=41ms TTL=125
Odpowiedź z 192.168.1.3: Host docelowy jest nieosiągalny.
Odpowiedź z 192.168.1.3: Host docelowy jest nieosiągalny.
```

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 Ethernetowy lub włącz interfejs GigabitEthernet na routerze REMOTE (używając polecenia **no shutdown**) przed przejściem do kolejnego kroku. Po około 30 sekundach ping powinien kończyć się ponownie sukcesem.

```
Upłynął limit czasu żądania.
Upłynął limit czasu żądania.
Upłynął limit czasu żądania.
Upłynął limit czasu żądania.
Odpowiedź z 192.168.3.3: bajtów=32 czas=41ms TTL=125
Odpowiedź z 192.168.3.3: bajtów=32 czas=40ms TTL=125
```

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

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

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

e. Wykonaj polecenie ping do PC-C w sieci routera REMOTE używając adresu 192.168.3.3 z routera LOCAL.

```
LOCAL# ping 192.168.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/64/68 ms
```

Wykrzyknik (!) oznacza że ping z routera LOCAL do PC-C zakończył się sukcesem. Czas przesłania w obie strony (round trip time) wyniósł średnio 64 ms bez utraty pakietów, co jest wskazywane przez 100% współczynnik sukcesu.

f. Ponieważ na routerze LOCAL została skonfigurowana tablica lokalnych hostów, możesz użyć polecenia ping z sieci routera REMOTE do PC-C używając nazwy dla tego hosta.

```
LOCAL# ping PC-C
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/63/64 ms
```

g. Dla polecenia **ping** dostępnych jest więcej opcji. W CLI wpisz **ping** i naciśnij Enter. Wprowadź **192.168.3.3** lub **PC-C** w polu Target IP address. Naciśnij Enter aby zaakceptować domyślne wartości dla innych opcji.

```
LOCAL# ping
Protocol [ip]:
Target IP address: PC-C
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/63/64 ms
```

h. Możesz użyć rozszerzonej wersji polecenia ping do obserwacji problemów w sieci. Uruchom polecenie **ping** do 192.168.3.3 z ilością powtórzeń równą 500. Następnie rozłącz kabel pomiędzy routerem REMOTE i przełącznikiem S3 lub wyłącz interfejs GigabitEthernet 0/1 na routerze REMOTE.

Podłącz ponownie kabel Ethernetowy lub włącz interfejs GigabitEthernet na routerze REMOTE 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.

```
LOCAL# ping
Protocol [ip]:
Target IP address: 192.168.3.3
Repeat count [5]: 500
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
```

```
Type escape sequence to abort.
Sending 500, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!U.............
....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
Success rate is 95 percent (479/500), round-trip min/avg/max = 60/63/72 ms
```

Litera U oznacza, że urządzenie docelowe jest nieosiągalne. Jednostka danych protokołu (PDU) do obsługi błędu została otrzymana przez router LOCAL. Każda kropka (.) oznacza, że przekroczono limit czasowy podczas oczekiwania na odpowiedź z PC-C. W tym przykładzie 5% pakietów zostało utraconych podczas symulowanej niedostępności sieci.

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

```
LOCAL# ping 192.168.3.3 repeat 500
```

lub

```
LOCAL# ping PC-C repeat 500
```

i. Możesz również sprawdzić łączność w sieci używając przełącznika. W tym przykładzie przełącznik S1 wykonuje ping przełącznik S3 w sieci routera REMOTE.

```
S1# ping 192.168.3.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 67/67/68 ms
```

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 4: Użyj polecenia trecert z PC-A do PC-C.

a. W wierszu poleceń wpisz tracert **192.168.3.3**.

```
C:\Users\User1> tracert 192.168.3.3
Śledzenie trasy do PC-C [192.168.3.3]
z maksymalną liczbą 30 przeskoków:
```

```
  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2    24 ms    24 ms    24 ms    10.1.1.2
  3    48 ms    48 ms    48 ms    10.2.2.1
  4    59 ms    59 ms    59 ms    PC-C [192.168.3.3]

Śledzenie zakończone.
```

Wyniki polecenia tracert wskazują, że ścieżka od PC-A do PC-C prowadzi z PC-A do LOCAL przez ISP do REMOTE, a następnie do PC-C. Oznacza to trzy przeskoki do osiągnięcia PC-C.

Krok 5: Przejrzyj dodatkowe opcje polecenia tracert.

a. W wierszu poleceń wpisz **tracert** i naciśnij Enter.

```
C:\Users\User1> tracert

Sposób użycia: tracert [-d] [-h maks_przes] [-j lista_hostów] [-w limit_czasu]
               [-R] [-S adres_źródłowy] [-4] [-6] nazwa_celu

Opcje:
    -d Nie rozpoznawaj adresów jako nazw hostów.
    -h maks_przes Maksymalna liczba przeskoków w poszukiwaniu celu.
    -j lista_hostów Swobodna trasa źródłowa według listy lista_hostów (tylko IPv4).
    -w limit_czasu Limit czasu oczekiwania na odpowiedź w milisekundach.
    -R Śledź ścieżkę błądzenia (tylko IPv6).
    -S adres_źródłowy Adres źródłowy do użycia (tylko IPv6).
    -4 Wymuś używanie IPv4.
    -6 Wymuś używanie IPv6.
```

b. Użyj opcji **-d** . Zauważ, że adres IP 192.168.3.3 nie jest odwzorowany na nazwę PC-C.

```
C:\Users\User1> tracert –d 192.168.3.3
Śledzenie trasy do 192.168.3.3 z maksymalną liczbą 30 przeskoków:

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2    24 ms    24 ms    24 ms    10.1.1.2
  3    48 ms    48 ms    48 ms    10.2.2.1
  4    59 ms    59 ms    59 ms    192.168.3.3

Śledzenie zakończone
```

Krok 6: Użyj polecenia traceroute z routera LOCL do PC-C.

a. W wierszu poleceń routera LOCAL wpisz **traceroute 192.168.3.3** lub **traceroute PC-C**. Nazwy hostów są odwzorowane, ponieważ na routerze LOCAL została skonfigurowana tablica IP hostów.

```
LOCAL# traceroute 192.168.3.3
Type escape sequence to abort.
Tracing the route to PC-C (192.168.3.3)
VRF info: (vrf in name/id, vrf out name/id)
  1 ISP (10.1.1.2) 16 msec 16 msec 16 msec
  2 REMOTE (10.2.2.1) 28 msec 32 msec 28 msec
  3 PC-C (192.168.3.3) 32 msec 28 msec 32 msec
```

```
LOCAL# traceroute PC-C
Type escape sequence to abort.
Tracing the route to PC-C (192.168.3.3)
VRF info: (vrf in name/id, vrf out name/id)
  1 ISP (10.1.1.2) 16 msec 16 msec 16 msec
  2 REMOTE (10.2.2.1) 28 msec 32 msec 28 msec
  3  PC-C (192.168.3.3) 32 msec 32 msec 28 msec
```

Krok 7: Użyj polecenia traceroute z przełącznika S1 do PC-C.

a. Na przełączniku S1 wpisz **traceroute 192.168.3.3**. Nazwy hostów nie są wyświetlane w wynikach polecenia traceroute, ponieważ nie została na tym przełączniku skonfigurowana lokalna tablica IP hostów.

```
S1# traceroute 192.168.3.3
Type escape sequence to abort.
Tracing the route to 192.168.3.3
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.1.1 1007 msec 0 msec 0 msec
  2 10.1.1.2 17 msec 17 msec 16 msec
  3 10.2.2.1 34 msec 33 msec 26 msec
  4 192.168.3.3 33 msec 34 msec 33 msec
```

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 z topologią

Krok 1: Wykasuj konfigurację routera REMOTE.

Krok 2: Uruchom ponownie router REMOTE.

Krok 3: Skopiuj i wklej poniższą konfigurację na router REMOTE.

```
hostname REMOTE
no ip domain-lookup
interface s0/0/1
 ip address 10.2.2.1 255.255.255.252
 no shutdown
interface g0/1
 ip add 192.168.8.1 255.255.255.0
 no shutdown
router eigrp 1
 network 10.2.2.0 0.0.0.3
 network 192.168.3.0 0.0.0.255
 no auto-summary
end
```

Krok 4: Z sieci routera LOCAL użyj polecenia ping i tracert lub tracerote do rozwiązania problemu w sieci routera REMOTE.

b. 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-C.

```
C:\Users\User1>tracert 192.168.3.3

Śledzenie trasy do 192.168.3.3 z maksymalną liczbą 30 przeskoków:
  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2  192.168.1.1 zgłasza: Host docelowy jest nieosiągalny.

Śledzenie zakończone
```

Jedną z metod zlokalizowania problemu w sieci jest wykonanie ping do każdego z przeskoków w sieci na trasie do PC-C. Najpierw ustal, czy PC-A może osiągnąć interfejs Serial 0/0/1 routera ISP o adresie 10.2.2.2.

```
C:\Users\Utraser1> ping 10.2.2.2

Badanie 10.2.2.2 z użyciem 32 bajtów danych:
Odpowiedź z 10.2.2.2: bajtów=32 czas=41ms TTL=125
Odpowiedź z 10.2.2.2: bajtów=32 czas=41ms TTL=125
Odpowiedź z 10.2.2.2: bajtów=32 czas=41ms TTL=125
Odpowiedź z 10.2.2.2: bajtów=32 czas=41ms TTL=125

Statystyka polecenia ping dla adresu 10.2.2.2:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty)
Szacunkowy czas przesyłania pakietów w obie strony w milisekundach:
    Minimum = 20 ms, Maksimum = 21 ms, Przeciętnie = 20 ms
```

Ping do routera ISP zakończył się sukcesem. Następnym przeskokiem w sieci jest router REMOTE. Wykonaj polecenie ping do interfejsu Serial 0/0/1 o adresie IP 10.2.2.1 na routerze REMOTE.

```
C:\Users\User1> ping 10.2.2.1

Badanie 10.2.2.1 z użyciem 32 bajtów danych:
Odpowiedź z 10.2.2.1: bajtów=32 czas=41ms TTL=125
Odpowiedź z 10.2.2.1: bajtów=32 czas=41ms TTL=125
Odpowiedź z 10.2.2.1: bajtów=32 czas=41ms TTL=125
Odpowiedź z 10.2.2.1: bajtów=32 czas=41ms TTL=125

Statystyka badania ping dla 10.2.2.1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty)
Szacunkowy czas błądzenia pakietów w milisekundach:
    Minimum = 40ms, Maksimum = 41ms, Czas średni = 40ms
```

PC-A może osiągnąć router REMOTE. Bazując na pomyślnym wyniku polecenia ping z PC-A do routera REMOTE można stwierdzić, że występuje problem z połączeniem w sieci 192.168.3.0/24. Użyj polecenia ping do domyślnej bramy PC-C, którą jest interfejs GigabitEthernet 0/1 routera REMOTE.

```
C:\Users\User1> ping 192.168.3.1
```

```
Badanie 192.168.3.1 z 32 bajtami danych:
Odpowiedź z 192.168.1.1: Host docelowy jest nieosiągalny.
Odpowiedź z 192.168.1.1: Host docelowy jest nieosiągalny.
Odpowiedź z 192.168.1.1: Host docelowy jest nieosiągalny.
Odpowiedź z 192.168.1.1: Host docelowy jest nieosiągalny.

Statystyka badania ping dla 192.168.3.1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty)
```

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

Przełącznik S3 może być również testowany z PC-A - aby zweryfikować problem z łącznością, wydaj polecenie **ping 192.168.3.11** w wierszu poleceń. Ponieważ PC-A nie może osiągnąć interfejsu GigabitEthernet 0/1 routera REMOTE, nie będzie mógł prawdopodobnie również osiągnąć przełącznika S3, na co wskazują poniższe wyniki.

```
C:\Users\User1> ping 192.168.3.11

Badanie 192.168.3.11 z 32 bajtami danych:
Odpowiedź z 192.168.1.1: Host docelowy jest nieosiągalny.
Odpowiedź z 192.168.1.1: Host docelowy jest nieosiągalny.
Odpowiedź z 192.168.1.1: Host docelowy jest nieosiągalny.
Odpowiedź z 192.168.1.1: Host docelowy jest nieosiągalny.

Statystyka badania ping dla 192.168.3.11:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty)
```

Wyniki poleceń tracert i ping wskazują, że PC-A może osiągnąć routery LOCAL, ISP i REMOTE lecz nie PC-C czy przełącznik S3, jak również domyślną bramę PC-C.

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

```
REMOTE# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         192.168.8.1     YES manual up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                10.2.2.1        YES manual up                    up

REMOTE# show run
<fragment pominięto>
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.8.1 255.255.255.0
 duplex auto
```

```
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
<fragment pominięto>
```

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

d. Popraw adres IP interfejsu GigabitEthernet 0/1.

```
REMOTE# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
REMOTE(config)# interface GigabitEthernet 0/1
REMOTE(config-if)# ip address 192.168.3.1 255.255.255.0
```

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

```
C:\Users\User1> ping 192.168.3.3
Badanie 192.168.3.3 z użyciem 32 bajtów danych:
Odpowiedź z 192.168.3.3: bajtów=32 czas=44ms TTL=125
Odpowiedź z 192.168.3.3: bajtów=32 czas=41ms TTL=125
Odpowiedź z 192.168.3.3: bajtów=32 czas=40ms TTL=125
Odpowiedź z 192.168.3.3: bajtów=32 czas=41ms TTL=125

Statystyka badania ping dla 192.168.3.3:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty)
Szacunkowy czas błądzenia pakietów w milisekundach:
    Minimum = 40ms, Maksimum = 44ms, Czas średni = 41ms

C:\Users\User1> tracert 192.168.3.3

Śledzenie trasy do PC-C [192.168.3.3]
z maksymalną liczbą 30 przeskoków:

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2    24 ms    24 ms    24 ms    10.1.1.2
  3    48 ms    48 ms    48 ms    10.2.2.1
  4    59 ms    59 ms    59 ms    PC-C [192.168.3.3]

Śledzenie zakończone
```

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

Do przemyślenia

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

_____

_____

2. Gdy wykonujesz ping na nieistniejący adres w zdalnej sieci, taki jak 192.168.3.4, jaki komunikat wyświetla polecenie **ping**? Co on oznacza? Jeśli wykonujesz ping na prawidłowy adres hosta, czy otrzymujesz taki komunikat, co należy 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 on oznacza?

   _____

   _____

Tabela zbiorcza interfejsów routerów

Zestawienie interfejsów routerów				
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)

Uwaga: Aby stwierdzić jak router jest skonfigurowany, spójrz na interfejsy, aby zidentyfikować typ routera i ilość jego interfejsów. 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, mimo 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.