Laboratorium - Tworzenie mapy Internetu

Cele

Część 1: Testowanie połączenia z siecią za pomocą polecenia ping

Część 2: Śledzenie trasy do odległego serwera za pomocą Windows tracert

Część 3: Śledzenie trasy do zdalnego serwera za pomocą narzędzi dostępnych na stronach internetowych

Część 4: Porównanie wyników śledzenia tras

Wprowadzenie

Komputerowe programy śledzące trasy to narzędzia, które potrafią poznać i wskazać sieci, przez które dane muszą przechodzić podczas transmisji od urządzenia końcowego użytkownika do odległej sieci przeznaczenia.

To narzędzie sieciowe jest zwykle używane z poziomu wiersza poleceń w następujący sposób:

tracert <nazwa sieci docelowej albo adres urządzenia końcowego>

(Systemy Microsoft Windows)

lub

traceroute <nazwa sieci docelowej albo adres urządzenia końcowego>

(Unix i podobne systemy)

Narzędzia do śledzenia trasy pozwalają użytkownikowi na określenie ścieżki lub tras oraz pomiar opóźnień podczas przesyłania danych przez sieci IP. Istnieje szereg narzędzi do wykonywania tej funkcji.

Narzędzie **traceroute** (lub **tracert**) jest często wykorzystywane do diagnozowania błędów w sieci. Wyświetlenie listy routerów pozwala użytkownikowi określić ścieżkę wykorzystaną przez pakiet podczas docierania do konkretnego miejsca przeznaczenia w sieci lub przejścia przez sieci. Każdy router oznacza punkt, w którym jedna sieć łączy się z kolejną, przez którą przesłany został pakiet danych. Liczba przebytych routerów jest znana jako liczba skoków, przez które dane wędrują od źródła do miejsca przeznaczenia.

Wyświetlona lista pomaga zidentyfikować problemy związane z przepływem danych podczas korzystania z usług takich jak strony www. Może ona również być pomocna podczas wykonywania zadań takich jak pobieranie danych. Jeśli ten sam plik jest dostępny na wielu stronach (będących lustrzanymi kopiami), można przeprowadzić śledzenie trasy do każdej z nich, aby określić, która zapewni najszybszy dostęp do danych.

Dwa wyniki śledzenia trasy pomiędzy źródłem a miejscem przeznaczenia otrzymane w różnym czasie mogą dać różne rezultaty. Jest to spowodowane tym, iż Internet składa się z gęstej sieci połączeń pomiędzy sieciami, a protokoły internetowe są zdolne do wyboru różnych ścieżek, którymi będą przesyłane pakiety.

Narzędzia do śledzenia trasy używane z poziomu wiersza poleceń są zazwyczaj wbudowane w systemy operacyjne urządzeń końcowych.

Scenariusz

Wykorzystując połączenie internetowe, użyj trzech narzędzi śledzących trasy do określenia tras do miejsca przeznaczenia. Ćwiczenie powinno być wykonane na komputerze posiadającym dostęp do Internetu oraz linii komend. Jako pierwsze wykorzystasz narzędzie tracert, wbudowane w system Windows. Następnie do śledzenia trasy wykorzystasz narzędzie dostępne przez stronę internetową (http://www.subnetonline.com/pages/network-tools/online-traceroute.php).

Wymagane wyposażenie

1 PC (Windows 7, Vista albo XP z dostępem do Internetu)

Część 1. Testowanie połączenia z siecią za pomocą polecenia ping

Krok 1. Określ, czy zdalny serwer jest osiągalny.

Aby prześledzić trasę do odległej sieci, używany komputer musi mieć sprawne połączenie z Internetem.

a. Jako pierwsze wykorzystamy narzędzie ping. Ping jest narzędziem wykorzystywanym do sprawdzania łączności ze zdalnym hostem. Pakiety informacji są wysyłane do zdalnego hosta wraz z żądaniem odpowiedzi. Twój lokalny komputer sprawdza, czy otrzymał odpowiedź na każdy pakiet oraz mierzy czas, jaki był potrzebny tym pakietom na przejście przez sieć. Nazwa ping pochodzi od technologii sonaru aktywnego, w którym impuls dźwiękowy wysyłany pod wodą odbija się od terenu lub innych statków.

b. Na Twoim komputerze kliknij przycisk **Start**, wpisz **cmd** w oknie **Wyszukaj programy i pliki**, a następnie wciśnij klawisz **Enter**.

c. W wierszu poleceń wpisz: **ping www.cisco.com**.

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

d. Pierwszy wiersz wyniku działania polecenia zawiera pełną nazwę domenową (Fully Qualified Domain Name, FQDN) e144.dscb.akamaiedge.net. Następnie podany jest adres IP 23.1.48.170. Cisco utrzymuje tą samą zawartość strony internetowej na różnych serwerach rozmieszczonych na całym świecie (znanych jako mirrory). Oznacza to, że, w zależności od twojej lokalizacji geograficznej, FQDN i adres IP będą inne.

e. Z tej części rezultatu:

```
Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

Cztery żądania zostały wysłane i otrzymano odpowiedź na każde z nich. Ponieważ na każde żądanie udzielono odpowiedzi, utracono 0 pakietów, co stanowi 0% straty. Średnio pakiety potrzebowały 54ms (54 milisekundy) na przejście całej sieci. Jedna milisekunda to 1/1000 sekundy.

Strumieniowanie wideo i gry sieciowe są dwoma zastosowaniami, na które negatywny wpływ ma utrata pakietów lub wolne połączenie sieciowe. Szybkość połączenia sieciowego można ocenić dokładniej wysyłając 100 żądań ping, zamiast domyślnych 4. Oto jak to zrobić:

```
C:\>ping -n 100 www.cisco.com
```

A tak wygląda rezultat wykonania tego polecenia:

```
Ping statistics for 23.45.0.170:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 53ms, Average = 49ms
```

f. Teraz wyślij żądanie ping do Regionalnych Rejestrów Internetowych (RIR) zlokalizowanych w różnych częściach świata:

W Afryce:

C:\> **ping www.afrinic.net**

```
C:\>ping www.afrinic.net

Pinging www.afrinic.net [196.216.2.136] with 32 bytes of data:
Reply from 196.216.2.136: bytes=32 time=314ms TTL=111
Reply from 196.216.2.136: bytes=32 time=312ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111

Ping statistics for 196.216.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 312ms, Maximum = 314ms, Average = 313ms
```

W Australii:

C:\> **ping www.apnic.net**

```
C:\>ping www.apnic.net

Pinging www.apnic.net [202.12.29.194] with 32 bytes of data:
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=287ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49

Ping statistics for 202.12.29.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 286ms, Maximum = 287ms, Average = 286ms
```

W Europie:

C:\> **ping www.ripe.net**

```
C:\>ping www.ripe.net

Pinging www.ripe.net [193.0.6.139] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 193.0.6.139:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

W Ameryce Południowej:

`C:\>` **`ping lacnic.net`**

```
C:\>ping www.lacnic.net

Pinging www.lacnic.net [200.3.14.147] with 32 bytes of data:
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=157ms TTL=51

Ping statistics for 200.3.14.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 157ms, Maximum = 158ms, Average = 157ms
```

Wszystkie żądania wysłano z komputera znajdującego się w Stanach Zjednoczonych. Co dzieje się ze średnim czasem odpowiedzi w milisekundach, gdy dane przemierzają ten sam kontynent (Amerykę Północną) w porównaniu do danych biegnących z Ameryki Północnej do innych kontynentów?

_____

Co jest interesującego w żądaniach ping wysłanych do strony w Europie?

_____

Część 2. Wyznaczanie trasy do odległego serwera przy wykorzystaniu tracert

Krok 1. Wyznacz trasę, jaką pokonuje ruch internetowy, aby dotrzeć do odległego serwera.

Po wykonaniu prostych testów osiągalności przy pomocy narzędzia ping, warto przyjrzeć się bliżej każdemu uczestniczącemu w transmisji segmentowi sieci. Do wykonania tego zadania wykorzystane zostanie narzędzie **tracert**.

a. Z poziomu linii komend, wpisz **tracert www.cisco.com**.

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

b. Zapisz wynik działania polecenia tracert do pliku tekstowego, jak następuje:

1) Kliknij prawym klawiszem myszy na pasku tytułu okna wiersza poleceń i wybierz **Edytuj** > **Zaznacz wszystko**.

2) Kliknij ponownie prawym klawiszem myszy na pasku tytułu okna wiersza poleceń i wybierz **Edytuj** > **Kopiuj**.

3) Otwórz program **Notatnik Windows**: **Start** > **Wszystkie programy** > **Akcesoria** > **Notatnik**.

4) Aby wkleić dane do Notatnika, wybierz **Edycja** > **Wklej**.

5) Wybierz **Plik** > **Zapisz jako...** aby zapisać plik na swoim pulpicie pod nazwą **tracert1.txt**.

c. Uruchom **tracert** dla każdej lokalizacji docelowej i zapisz wyniki w plikach tekstowych z kolejnymi numerami.

```
C:\> tracert www.afrinic.net
C:\> tracert www.lacnic.net
```

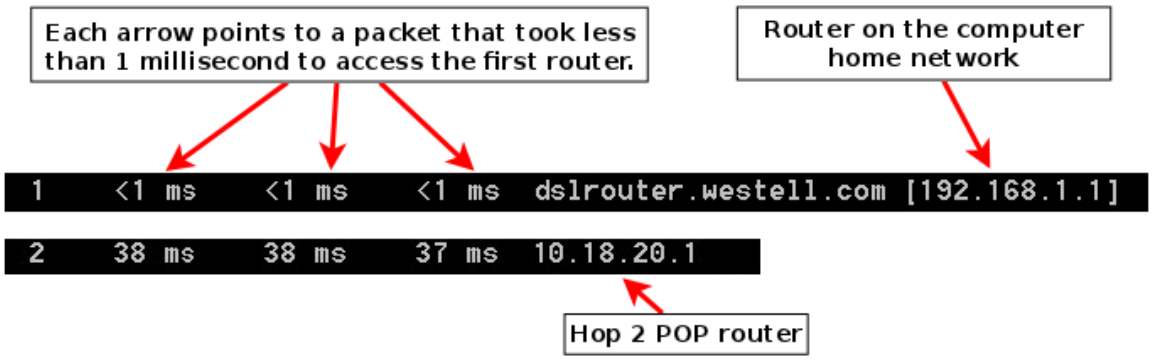
d. Zinterpretuj wyniki polecenia **tracert**.

Śledzone trasy mogą prowadzić przez wiele przeskoków oraz wielu różnych dostawców usług internetowych w zależności od tego, jak duża jest sieć twojego dostawcy oraz jaka jest odległość pomiędzy hostem źródłowym i docelowym. Każdy "przeskok" reprezentuje router. Router to specjalistyczny komputer wykorzystywany do kierowania ruchem w Internecie. Wyobraź sobie wycieczkę samochodową prowadzącą przez szereg autostrad w kilku krajach. W różnych punktach trasy docierasz do rozwidlenia dróg, gdzie masz możliwość wyboru spośród kilku różnych autostrad. A teraz wyobraź sobie, że przy każdym takim rozwidleniu stoi urządzenie, które kieruje na właściwą autostradę prowadzącą do celu Twojej podróży. Zadanie to, dla pakietów w sieci wykonuje router.

Ponieważ komputery komunikują się przy pomocy liczb a nie słów, routery identyfikowane są przy pomocy adresów IP (liczb w formacie x.x.x.x). Narzędzie **tracert** pokazuje jaką ścieżką przez sieć podążał pakiet z informacjami, aby dotrzeć do miejsca przeznaczenia. Narzędzie **tracert** podaje ponadto informację, jak szybko ruch przechodzi przez poszczególne segmenty sieci. Do każdego routera na trasie wysyłane są trzy pakiety. Czas odpowiedzi na nie mierzony jest w milisekundach. Teraz wykorzystaj tą informację do analizy rezultatów działania polecenia **tracert** dla www.cisco.com. Poniżej znajduje się rezultat śledzenia trasy:

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

Poniżej znajduje się wyjaśnienie najważniejszych elementów:



W przykładowym wyniku działania polecenia tracert pokazanym poniżej, pakiety podróżują ze źródłowego komputera PC do lokalnego routera będącego domyślną bramą (przeskok 1: 192.168.1.1) wykorzystywanego do połączenia z routerem dostawcy usług internetowych (przeskok 2: 10.18.20.1) w punkcie przyłączeniowym (ang. Point of Presence, POP). Każdy dostawca usług internetowych posiada wiele routerów POP. Te routery POP znajdują się na granicy sieci dostawcy usług internetowych i pozwalają klientom na podłączenie się do Internetu. Pakiety podróżują w sieci firmy Verizon przez dwa przeskoki a następnie przeskakują do routera należącego do alter.net. To może oznaczać, że pakiety przeszły do kolejnego dostawcy usług internetowych. Jest to istotne, gdyż czasami następuje utrata pakietów podczas przejścia pomiędzy dostawcami. Zdarza się też, że jeden dostawca jest wolniejszy od innego. W jaki sposób można określić czy alter.net to ten sam bądź inny dostawca?

e. Do tego celu służy narzędzie internetowe whois. Pozwala ono na określenie, kto jest właścicielem danej domeny internetowej. Dostęp do narzędzia whois poprzez stronę internetową można uzyskać pod adresem

http://whois.domaintools.com/ Zgodnie z informacją uzyskaną przy użyciu narzędzia dostępnego z poziomu strony internetowej, ta domena również należy do firmy Verizon.

Podsumowując, ruch internetowy rozpoczyna się od domowego komputera i przechodzi przez domowy router (przeskok 1). Następnie przechodzi do dostawcy usług internetowych i podróżuje przez jego sieć (przeskoki 2-7), aż dotrze do odległego serwera (przeskok 8). Ten przykład jest dość wyjątkowy, gdyż tutaj pakiety wykorzystują wyłącznie sieć jednego dostawcy usług internetowych. Bardziej typowe jest wykorzystanie sieci dwóch lub więcej dostawców, co demonstrują kolejne przykłady.

f. Teraz prześledźmy przykład, w którym ruch internetowy przechodzi przez sieci wielu dostawców. Poniżej znajduje się rezultat polecenia tracert dla www.afrinic.net:

```
C:\>tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    39 ms    38 ms    37 ms  10.18.20.1
  3    40 ms    38 ms    39 ms  G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.197.182]
  4    44 ms    43 ms    43 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    42 ms  0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6    43 ms    71 ms    43 ms  0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7    47 ms    47 ms    47 ms  te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137
]
  8    43 ms    55 ms    43 ms  vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9    52 ms    51 ms    51 ms  ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

 10   130 ms   132 ms   132 ms  ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
 11   139 ms   145 ms   140 ms  ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.13
7]
 12   148 ms   140 ms   152 ms  ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14
]
 13   144 ms   144 ms   146 ms  ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29
]
 14   151 ms   150 ms   150 ms  ae-23-23.ebr2.London1.Level3.net [4.69.148.193]

 15   150 ms   150 ms   150 ms  ae-58-223.csw2.London1.Level3.net [4.69.153.138]

 16   156 ms   156 ms   156 ms  ae-227-3603.edge3.London1.Level3.net [4.69.166.1
54]
 17   157 ms   159 ms   160 ms  195.50.124.34
 18   353 ms   340 ms   341 ms  168.209.201.74
 19   333 ms   333 ms   332 ms  csw4-pkl-gi1-1.ip.isnet.net [196.26.0.101]
 20   331 ms   331 ms   331 ms  196.37.155.180
 21   318 ms   316 ms   318 ms  fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
 22   332 ms   334 ms   332 ms  196.216.2.136

Trace complete.
```

Co dzieje się w przeskoku 7? Czy level3.net to ten sam dostawca usług internetowych, co w przeskokach 2-6, czy może jest to inna firma? Wykorzystaj narzędzie whois aby odpowiedzieć na to pytanie.

_____

Co dzieje się w przeskoku 10 z ilością czasu, jakiej potrzebuje pakiet na przejście pomiędzy Waszyngtonem D.C. a Paryżem, w porównaniu do wcześniejszych przeskoków 1-9?

_____

Co dzieje się podczas przeskoku 18? Wykonaj zapytanie whois dla adresu 168.209.201.74 przy pomocy narzędzia whois.

_____

g. Wpisz **tracert www.lacnic.net**.

```
C:\>tracert www.lacnic.net

Tracing route to www.lacnic.net [200.3.14.147]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    38 ms    38 ms    39 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    42 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    82 ms    47 ms    47 ms  0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  6    46 ms    47 ms    56 ms  204.255.168.194
  7   157 ms   158 ms   157 ms  ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  8   156 ms   157 ms   157 ms  xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]

  9   161 ms   161 ms   161 ms  xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]

 10   158 ms   157 ms   157 ms  ae0-0.ar3.nu.registro.br [200.160.0.249]
 11   176 ms   176 ms   170 ms  gw02.lacnic.registro.br [200.160.0.213]
 12   158 ms   158 ms   158 ms  200.3.12.36
 13   157 ms   158 ms   157 ms  200.3.14.147

Trace complete.
```

Co dzieje się podczas przeskoku 7?

_____

Część 3. Śledzenie trasy do zdalnego serwera za pomocą stron internetowych i oprogramowania narzędziowego

Krok 1. Użycie narzędzia traceroute poprzez stronę internetową.

a. Przy pomocy http://www.subnetonline.com/pages/network-tools/online-tracepath.php wyznacz trasę do następujących stron:

www.cisco.com

www.afrinic.net

Skopiuj i zapisz wyniki do Notatnika.

W jaki sposób różnią się rezultaty śledzenia trasy do www.cisco.com, jeśli zostanie ono wykonane z poziomu wiersza poleceń (część 1 ćwiczenia) zamiast z poziomu strony internetowej?

_____

_____

Porównaj rezultaty śledzenia trasy do Afryki z części 1 z tym wykonanym z poziomu strony internetowej. Jakie widzisz różnice?

_____

_____