Piotr Jakubowski 148570
Seweryn Kraczyński 148702

Lokalne sieci komputerowe - laboratorium

Ćwiczenie 1
Diagnozowanie sieci z wykorzystaniem poleceń ping oraz traceroute

I. Wstęp, cel ćwiczenia

Polecenia ping oraz traceroute są najbardziej podstawowymi narzędziami służącymi do diagnostyki sieci. Pierwsze z nich umożliwia sprawdzenie połączenia z innym komputerem w sieci oraz zebrania podstawowych statystyk takich jak jakość połączenia wyrażona w % utraconych pakietów oraz opóźnienie dostarczenia pakietu.

Traceroute służy do wyznaczania trasy przebiegu pakietu w sieci, poprzez wysyłanie kolejnych pakietów z polem TTL ustawionym na coraz większe wartości (poczynając od 1) i analizowanie komunikatów “przekroczenie czasu transmisji” otrzymywanych ze stacji pośredniczących. Umożliwia to zlokalizowanie powolnego lub uszkodzonego łącza sieci na drodze do stacji docelowej.

Celem ćwiczenia jest zapoznanie się z zasadą działania obu narzędzi oraz praktyczne ich wykorzystanie.

Dodatkowym narzędziem wykorzystanym w ćwiczeniu był program nmap - do sprawdzania poprawności rozpoznania systemu operacyjnego.

II. Przebieg ćwiczenia

1. Wybranie dwóch węzłów sieci:
- bliskiego (Szwecja, 7 hop): www.ikea.se (IP 150.254.186.70)
- dalekiego (Australia, 22 hop): router strony visitcanberra.com.au (IP 203.10.110.193)

2. Śledzenie obu tras przy pomocy programu ping: zmieniając wartość początkowego TTL (przełącznikiem -i) udało się prześledzić całą trasę pakietu.

Przykład dla www.ikea.se:

```
Badanie a341.g.akamai.net [150.254.186.70] z użyciem 32 bajtów danych:

Odpowiedź z 156.17.43.62
Odpowiedź z 156.17.30.126
Odpowiedź z 156.17.18.222
Odpowiedź z 156.17.18.254
Odpowiedź z 156.17.255.154
Odpowiedź z 150.254.232.10
Odpowiedź z 150.254.186.70
```

Korzystając z narzędzia traceroute otrzymano taką samą trasę:

```
Trasa śledzenia do a341.g.akamai.net [150.254.186.70]

1 syriusz.kssk.pwr.wroc.pl [156.17.43.62]
2 elek.wask.wroc.pl [156.17.30.126]
3 156.17.18.222
4 156.17.18.254
5 karkonosz-do-g12centrum.wask.wroc.pl [156.17.255.154]
6 z-wroclawia-loc.poznan.pionier.net.pl [150.254.232.10]
7 a150-254-186-70.deploy.akamaitechnologies.com [150.254.186.70]
```

3. Zebranie statystyk opóźnień dla obu węzłów (przełącznik -t):

```
Statystyka badania ping dla 203.10.110.193:
    Pakiety: Wysłane = 689, Odebrane = 689, Utracone = 0 (0% straty),
    Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 376 ms, Maksimum = 614 ms, Czas średni = 399 ms

Statystyka badania ping dla 150.254.186.70:
    Pakiety: Wysłane = 702, Odebrane = 702, Utracone = 0 (0% straty),
    Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 6 ms, Maksimum = 106 ms, Czas średni = 9 ms
```

4. Sprawdzenie wpływu wartości pola TOS na trasę oraz opóźnienie pakietów.

Wykryto niewielkie różnice w trasach i opóźnieniu pakietów dla różnych wywołań polecenia ping/traceroute tylko w przypadku stacji dalekiej. Mimo licznych prób, nie udało się wykazać zależności pomiędzy wartością pola TOS a trasą lub opóźnieniem: dla jednakowych wartości TOS rozrzut wyników był taki sam jak dla wartości całkowicie różnych funkcjonalnie, np. 111 100, 111 010 i 111 001.

5. Sprawdzenie wpływu rozmiaru pakietów na opóźnienie:
W zakresie rozmiarów pakietów możliwych do przesłania (do około 5000 bajtów), nie znaleziono jakichkolwiek różnic w opóźnieniach które można by powiązać z rozmiarem pakietu. Wyniki przedstawiono w tabeli.

Rozmiar [B]	Australia [ms]	Szwecja [ms]
32	379	9
64	378	41
128	380	10
256	381	9
512	382	12
1024	404	24
2048	384	15
4096	384	10
5000	384	14

6. Określenie systemu operacyjnego na podstawie wartości pola TTL:

Jak wiadomo, różne systemy operacyjne ustawiają różne początkowe wartości pola TTL. Na tej podstawie można w dużym przybliżeniu ustalić rodzaj systemu zainstalowanego na zdalnym hoście. Należy pamiętać o powiększeniu wartości TTL o liczbę przeskoków na drodze do danego węzła.

Odebrano następujące wartości TTL:

- dla www.ikea.se (150.254.186.70): 57 (+7 hop = 64)
- dla visitcanberra.com.au (203.10.110.193): 233 (+22 hop = 255)

Na podstawie zestawienia znalezionego w Internecie należy przypuszczać że pierwszy system operacyjny to Linux, BSD lub Solaris 8, natomiast drugi to Cisco lub Solaris 2. Przypuszczenia te potwierdza program nmap:

- dla www.ikea.se: OS guesses: Linux 2.6.5 - 2.6.19 (99%)
- dla visitcanberra.com.au: OS details: Cisco Aironet 1200 WAP (IOS 12.3)

III. Analiza i wnioski

- Ping i traceroute używają tych samych tras - otrzymane wyniki są identyczne

- Pole typu usługi nie ma wpływu na trasę ani na opóźnienie pakietu - dla takich samych wartości pola wybierane są różne trasy, dla różnych wartości identyczne trasy. Analogiczna sytuacja występuje w przypadku opóźnień.

- Długość pakietu nie ma zauważalnego wpływu na jego opóźnienie - powyżej długości około 5000 bajtów rośnie jedynie gwałtownie procent utraty pakietów, a powyżej około 6000 bajtów wszystkie pakiety są tracone, w tych granicach zawiera się więc maksymalna długość pakietu.

- Długość trasy wyrażona w liczbie przeskoków ma zasadniczy wpływ na opóźnienie dostarczenia pakietu - w każdym węźle pakiet musi zostać odebrany, zdekodowany, zaklasyfikowany do odpowiedniego wyjścia, a następnie nadany. W rzeczywistej sieci opóźnienie do węzła oddalonego o 22 przeskoki okazało się znacznie większe od opóźnienia do węzła oddalonego tylko o 7 przeskoków - co potwierdza teoretyczne założenia.

- Geograficznej długości trasy zazwyczaj w przybliżeniu odpowiada liczba przeskoków, należy się więc spodziewać korelacji pomiędzy tymi dwoma wartościami. Należy również uwzględnić czas propagacji sygnału, który zaczyna mieć znaczenie przy odległościach liczonych w tysiącach kilometrów. Tak też jest w rzeczywistości - opóźnienia dla dalekiego węzła są kilkanaście razy większe niż dla węzła bliskiego.

- Przy pomocy analizy pola TTL można określić jaki system operacyjny pracuje w danym węźle, na podstawie analizy TTL znanych systemów operacyjnych. Odpowiednie zestawienia znanych systemów dostępne są w Internecie.

Wykres opóźnienia dla trasy do węzła dalekiego, w zależności od liczby przeskoków: