Część I - Badanie działania programu Ping

1. Wprowadzenie

Program **Ping** służy do testowania łączności między hostami w sieci, mierząc czas propagacji pakietów oraz wykrywając straty. W eksperymencie przeanalizowano wpływ wielkości pakietów na liczbę skoków (hopów), fragmentację i możliwość uzyskania odpowiedzi. Badania przeprowadzono dla dwóch serwerów:

- **ususweb.uw.edu.pl** (Warszawa, krótka trasa),
- **www.npu.ac.th**(Tajlandia, długa trasa).

2. Pełna tabela wyników

Adres	Lokalizacja	Wielkość pakietu	Skoki (tam)	Skoki (powrót)	Fragmentacja	Sygnał powrotny
ususweb.uw.edu.pl	Warszawa	56B	13	-	nie	nie
ususweb.uw.edu.pl	Warszawa	56B	13	-	tak	nie
ususweb.uw.edu.pl	Warszawa	56B	14	11	nie	tak
ususweb.uw.edu.pl	Warszawa	56B	14	11	tak	tak
ususweb.uw.edu.pl	Warszawa	1000B	14	11	nie	tak
ususweb.uw.edu.pl	Warszawa	1000B	14	11	tak	tak
ususweb.uw.edu.pl	Warszawa	1468B	14	11	nie	tak
ususweb.uw.edu.pl	Warszawa	1468B	14	11	tak	tak
ususweb.uw.edu.pl	Warszawa	1469B	14	-	nie	nie
ususweb.uw.edu.pl	Warszawa	1469B	14	11	tak	tak
ususweb.uw.edu.pl	Warszawa	1500B	14	11	tak	tak

ususweb.uw.edu.pl	Warszawa	1742B	14	11	tak	tak
ususweb.uw.edu.pl	Warszawa	1743B	14	-	tak	nie
www.npu.ac.th	Tajlandia	56B	18	-	nie	nie
www.npu.ac.th	Tajlandia	56B	18	-	tak	nie
www.npu.ac.th	Tajlandia	56B	19	18	nie	tak
www.npu.ac.th	Tajlandia	56B	19	18	tak	tak
www.npu.ac.th	Tajlandia	500B	19	18	nie	tak
www.npu.ac.th	Tajlandia	500B	19	18	tak	tak
www.npu.ac.th	Tajlandia	750B	19	18	nie	tak
www.npu.ac.th	Tajlandia	750B	19	18	tak	tak
www.npu.ac.th	Tajlandia	996B	19	18	nie	tak
www.npu.ac.th	Tajlandia	996B	19	18	tak	tak
www.npu.ac.th	Tajlandia	997B	19	-	nie	nie
www.npu.ac.th	Tajlandia	997B	19	-	tak	nie

3. Analiza wyników

A. Wpływ wielkości pakietu na odpowiedź

1. **Fragmentacja pakietów**:
    a. **Warszawa**:
        i. Pakiety **≤1468B** (np. 56B, 1000B) otrzymywały odpowiedź nawet przy fragmentacji.
        ii. Dla **1469B** i większych:
            1. **1469B bez fragmentacji**: Brak odpowiedzi (brak możliwości przesłania niefragmentowanego pakietu).

2. **1469B z fragmentacją**: Odpowiedź otrzymano, co sugeruje, że sieć toleruje fragmentację dla pakietów nieznacznie przekraczających MTU.

iii. **1743B**: Brak odpowiedzi nawet przy fragmentacji, co wskazuje na limit fizyczny lub konfiguracyjny.

b. **Tajlandia**:

i. Maksymalny niefragmentowany pakiet: **996B** (odpowiedź otrzymano).

ii. **997B**: Brak odpowiedzi niezależnie od fragmentacji, co potwierdza MTU ≈ 1500B, ale z ograniczeniami na trasie.

2. **MTU (Maximum Transmission Unit)**:
   a. **Warszawa**: 1468B (największy niefragmentowany pakiet z odpowiedzią).
   b. **Tajlandia**: 996B (ograniczenia wynikające z różnic w infrastrukturze).

B. Liczba skoków (hopów)

1. **Trasy krótkie (Warszawa)**:
   a. **Skoki "tam"**: 13–14 (różnice wynikają z dynamicznego routingu).
   b. **Skoki "powrót"**: 11 (stała dla większości testów).
   c. **Asymetria tras**: Potwierdzono różnice w ścieżkach "tam" i "z powrotem" (np. 14 skoków tam, 11 powrót).
2. **Trasy długie (Tajlandia)**:
   a. **Skoki "tam"**: 18–19 (najdłuższa zmierzona ścieżka).
   b. **Średnica internetu**: 19 skoków (najdłuższa trasa w eksperymencie).

C. Wpływ fragmentacji na komunikację

- **Pakiety niefragmentowane**:
  - Wysoka skuteczność dla rozmiarów ≤ MTU (np. 1468B w Warszawie, 996B w Tajlandii).
- **Pakiety fragmentowane**:
  - **Warszawa**: Odpowiedź otrzymywano nawet dla pakietów **1742B**, co sugeruje dobrą obsługę fragmentacji.
  - **Tajlandia**: Fragmentacja działała dla pakietów ≤996B, ale **997B** były odrzucane (możliwe blokowanie przez zapory sieciowe).

D. Trasy przez sieci wirtualne (cloud computing)

- **Pośrednie wskazówki**:
  - Większa liczba skoków w Tajlandii (19 vs. 14 w Warszawie) może wynikać z wykorzystania węzłów chmurowych (np. AWS, Azure).

- Różnice w MTU między lokalizacjami sugerują odmienną architekturę sieci (np. tunele VPN, overlay networks).

4. Wnioski

1. **Przydatność programu Ping**:
   a. **Zalety**: Skuteczny w ustalaniu MTU, wykrywaniu asymetrii tras i strat pakietów.
   b. **Ograniczenia**: Brak kontroli nad fragmentacją (niektóre sieci odrzucają fragmentowane pakiety).
2. **Kluczowe obserwacje**:
   a. **MTU zależy od trasy**: Różni się nawet dla tego samego hosta w zależności od lokalizacji.
   b. **Fragmentacja nie zawsze szkodliwa**: W Warszawie pakiety do 1742B były obsługiwane, ale w Tajlandii już 997B – blokowane.
   c. **Asymetria routingu**: Trasy "tam" i "powrót" często różnią się liczbą skoków.
3. **Rekomendacje**:
   a. Unikać pakietów przekraczających MTU (np. 1468B dla lokalnych połączeń).
   b. W przypadku braku odpowiedzi sprawdzać zarówno fragmentację, jak i konfigurację zapór sieciowych.

Podsumowanie: Program Ping jest nieoceniony w podstawowej diagnostyce sieci, ale jego interpretacja wymaga uwzględnienia czynników takich jak MTU, fragmentacja i dynamika routingu. Najdłuższa ścieżka w eksperymencie miała **19 skoków**, a maksymalne niefragmentowane pakiety różniły się znacząco między lokalizacjami (1468B vs. 996B).**

Część II - Ocena działania programów Traceroute i Wireshark w por

1. Wprowadzenie

Programy **Ping**, **Traceroute** i **Wireshark** są narzędziami diagnostycznymi służącymi do analizy sieci, ale różnią się funkcjonalnością i zakresem zastosowań. W raporcie porównano ich działanie, wskazano mocne i słabe strony oraz określono scenariusze, w których korzystanie z danego narzędzia jest najbardziej uzasadnione.

2. Opis programów

A. Ping

- **Cel**: Testowanie dostępności hosta, mierzenie czasu round-trip (RTT) oraz wykrywanie strat pakietów.
- **Działanie**: Wysyła pakiety ICMP (żądanie echo) i oczekuje na odpowiedź (echo reply).
- **Zalety**:
    - Prosty w użyciu (jednolinijkowe polecenie).
    - Szybka weryfikacja podstawowej łączności.
- **Ograniczenia**:
    - Nie pokazuje trasy pakietów.
    - Ograniczona informacja o przyczynach problemów.

B. Traceroute

- **Cel**: Śledzenie ścieżki pakietów od źródła do celu, identyfikacja węzłów (skoków) na trasie.
- **Działanie**: Wysyła serie pakietów z rosnącym TTL (Time To Live), analizując komunikaty ICMP "Time Exceeded" od routerów.
- **Zalety**:
    - Wykrywanie "wąskich gardeł" na trasie.
    - Identyfikacja asymetrii tras (tam vs. powrót).
- **Ograniczenia**:
    - Czasochłonne (wymaga analizy wielu skoków).
    - Niektóre sieci blokują pakiety Traceroute (np. przez zapory).

C. Wireshark

- **Cel**: Kompleksowa analiza ruchu sieciowego poprzez przechwytywanie i dekodowanie pakietów.
- **Działanie**: Przechwytuje pakiety w trybie promiscuous, umożliwiając filtrowanie i analizę protokołów (np. TCP, UDP, HTTP).
- **Zalety**:
    - Szczegółowa inspekcja zawartości pakietów.
    - Wsparcie dla setek protokołów.
- **Ograniczenia**:
    - Wymaga zaawansowanej wiedzy sieciowej.
    - Generuje duże ilości danych, co może przytłoczyć początkujących.

3. Porównanie funkcjonalności

Kryterium	Ping	Traceroute	Wireshark
Typ analizy	Podstawowa łączność	Ścieżka routingu	Głęboka inspekcja pakietów
Protokoły	ICMP	ICMP/UDP	Wszystkie warstwy (L2–L7)
Czas wykonania	Kilka sekund	Kilka–kilkanaście sekund	Ciągły monitoring
Poziom trudności	Początkujący	Średnio zaawansowany	Ekspert
Typowe zastosowania	Sprawdzenie "czy host żyje"	Diagnostyka opóźnień	Debugowanie protokołów, analiza bezpieczeństwa

4. Kiedy korzystać z danego programu?

A. Ping

- **Scenariusze**:
  - Szybkie sprawdzenie, czy host jest dostępny (np. ping google.com).
  - Pomiar podstawowych opóźnień i strat pakietów.
  - Testowanie MTU (np. ping -s 1500).
- **Przykład**: Gdy strona internetowa nie ładuje się, najpierw użyj Ping, aby potwierdzić łączność.

B. Traceroute

- **Scenariusze**:
  - Identyfikacja punktu awarii na trasie (np. traceroute npu.ac.th).
  - Analiza asymetrii routingu (różne ścieżki "tam" i "z powrotem").
  - Wykrywanie nadmiernych opóźnień na konkretnych skokach.
- **Przykład**: Gdy Ping wskazuje utratę pakietów, użyj Traceroute, aby zlokalizować problematyczny router.

C. Wireshark

- **Scenariusze**:

    - Diagnostyka błędów protokołów (np. analiza handshake TCP).
    - Wykrywanie ruchu malware (np. niespodziewane połączenia do podejrzanych adresów).
    - Optymalizacja wydajności aplikacji sieciowych (np. analiza opóźnień HTTP).
- **Przykład**: Gdy aplikacja wysyła nieoczekiwane dane, przechwyć ruch Wiresharkiem, aby zbadać pakiety.

5. Podsumowanie: Zalety i wady

Narzędzie	Zalety	Wady
Ping	Natychmiastowy wynik, prostota	Brak informacji o ścieżce lub przyczynach awarii
Traceroute	Mapowanie trasy, wykrywanie wąskich gardeł	Czasochłonne, wrażliwe na blokady zapór
Wireshark	Pełna kontrola nad analizą pakietów	Wysoki próg wejścia, przytłaczająca ilość danych

6. Wnioski końcowe

- **Ping** jest narzędziem "pierwszego kontaktu" – użyj go, gdy potrzebujesz szybkiej odpowiedzi na pytanie *"Czy host działa?"*.
- **Traceroute** sprawdza się w diagnostyce routingu – zastosuj go, gdy Ping wskazuje problem, ale nie wiesz, *gdzie* występuje.
- **Wireshark** to "mikroskop dla sieci" – sięgnij po niego, gdy potrzebujesz zrozumieć *dlaczego* coś nie działa (np. błędy protokołów, nieautoryzowany ruch).

Rekomendacje:

1. Zaczynaj od Ping, aby wykluczyć podstawowe problemy.
2. Jeśli Ping zawiedzie, przejdź do Traceroute, aby zlokalizować awarię.
3. Gdy problem jest złożony (np. błąd aplikacji), wykorzystaj Wireshark do analizy pakietów.

Podsumowanie: Każde z narzędzi ma unikalną rolę w diagnostyce sieci. Ping i Traceroute są niezbędne do szybkich testów, podczas gdy Wireshark dostarcza narzędzi do głębokiej analizy, wymagającej jednak eksperckiej wiedzy.

Authors: Karol Wziątek