Sprawozdanie z analizy programów sieciowych `ping`, `traceroute` i `Wireshark`

1. Opis programów

Ping

Program `ping` służy do diagnozowania połączeń sieciowych poprzez wysyłanie pakietów ICMP Echo Request do zadanego hosta i oczekiwanie na odpowiedź ICMP Echo Reply. Pozwala na pomiar czasu podróży pakietu (RTT) oraz wykrycie strat pakietów.

Najważniejsze opcje:

- `-c` - określa liczbę wysyłanych pakietów,
- `-t` - ustawia TTL (Time To Live),
- `-s` - określa rozmiar pakietu,
- `-p` - pozwala na wysyłanie pakietów z określonym wzorcem w systemie szesnastkowym,
- `-M do` - blokuje fragmentację pakietów.

Traceroute

Program `traceroute` pozwala na śledzenie trasy pakietów w sieci, identyfikując kolejne routery po drodze do hosta docelowego.

Wireshark

`Wireshark` to zaawansowane narzędzie do analizy ruchu sieciowego. Umożliwia przechwytywanie i szczegółową inspekcję pakietów przesyłanych w sieci, co pozwala na diagnozowanie problemów oraz analizę komunikacji między urządzeniami.

Najważniejsze funkcje:

- Monitorowanie i analiza pakietów w czasie rzeczywistym,
- Identyfikacja protokołów i struktur pakietów,
- Wyszukiwanie i filtrowanie określonych typów ruchu,
- Analiza opóźnień i problemów z połączeniami.

2. Wykonane testy i analiza wyników

Testy `ping`
Przeprowadzono testy pingowania do różnych adresów:

Adres	Średni czas RTT (ms)	Liczba skoków do	Liczba skoków od	Średni czas na skok (ms)	RTT przy obciążeniu (ms)	Średni czas na skok z obciążeniem (ms)
192.168.1.1	8,59	1?(0)	1?(0)	8,59	9,57	9,57
84.38.214.38	31,73	8	7	2,11	40,63	2,70
uwr.edu.pl	31,47	16	14	1,05	37,47	1,25
telefonica.de	30,33	8	12	1,51	33,27	1,66
stratford.org	25,81	8	8	1,61	29,25	1,84
hermannsburg.com.au	391,66	23	18	9,54	459,98	11,22

Z wyników widać, że odległość geograficzna ma kluczowy wpływ na RTT. Najdłuższe czasy odpowiedzi zaobserwowano dla serwera w Australii (hermannsburg.com.au), co jest zgodne z oczekiwaniami.

Test fragmentacji pakietów
Przy próbie wysłania pakietów bez fragmentacji (`ping -M do -s 1500`) system zwracał komunikat:

```
ping: local error: Message too long
```

Oznacza to, że domyślny MTU dla połączenia był niższy niż 1500 bajtów, co wymuszało fragmentację pakietów.

Analiza kapsułkowania komunikatów
Podczas komunikacji sieciowej dane są kapsułkowane w warstwach modelu OSI:

- Warstwa aplikacji (np. HTTP, DNS) przesyła dane, rozmiar rozny
- Warstwa transportowa (TCP/UDP) dodaje nagłówek z numerem portu, TCP 20 bajtow, UDP 8 bajtow

- Warstwa sieciowa (IP) dołącza adresy IP, IPv4 20 bajtow, IPv6 40 bajtow
- Warstwa łącza danych (Ethernet, Wi-Fi) dodaje nagłówek ramki, Header 14 bajtow i Footer 4 bajty
- Warstwa fizyczna przesyła dane jako sygnały elektryczne lub radiowe.

Przykład kapsułkowania

Pakiet ICMP widziany w `Wireshark`:

```
0000   9c 24 72 6f dd 6f 90 65 84 7c 56 c3 08 00 45 00  .$ro.o.e.|V...E.
0010   00 54 ab 68 40 00 40 01 0b 1f c0 a8 01 d0 c0 a8  .T.h@.@.........
0020   01 01 08 00 11 d4 00 61 00 01 e6 d0 d5 67 00 00  .......a.....g..
0030   00 00 4b 64 0a 00 00 00 00 00 6a 65 73 74 20 74  ..Kd......jest t
0040   65 73 74 0a 54 6f 20 6a 65 73 74 20 74 65 73 74  est.To jest test
0050   0a 54 6f 20 6a 65 73 74 20 74 65 73 74 0a 54 6f  .To jest test.To
0060   20 6a                                            j
```

Analiza:

- Adresy MAC (warstwa łącza danych)
- Nagłówek IP (warstwa sieciowa) z adresem źródłowym i docelowym
- Nagłówek ICMP (warstwa transportowa)
- Dane (warstwa aplikacji)

3. Wnioski

- `ping` jest bardzo przydatnym narzędziem do testowania podstawowej komunikacji sieciowej i analizy opóźnień.
- `traceroute` pozwala określić trasę pakietu i wykryć potencjalne punkty spowolnień w sieci.
- `Wireshark` pozwala na szczegółową inspekcję pakietów i analizę struktury protokołów.
- Testy RTT pokazują, że im większa odległość geograficzna, tym większe opóźnienia.
- Większe pakiety są bardziej podatne na opóźnienia i utratę danych.
- Fragmentacja może być problemem, jeśli MTU jest mniejsze niż rozmiar pakietu ICMP.
- Analiza w Wireshark pozwala na głębszą diagnostykę protokołu ICMP i kapsułkowania pakietów.

Narzędzia `ping`, `traceroute` i `Wireshark` są nieocenione w diagnostyce sieci, pozwalając na szybkie wykrywanie problemów z opóźnieniami i połączeniami.