Instrukcja 5 - Zastosowania protokołu ICMP

5.1 Wstęp

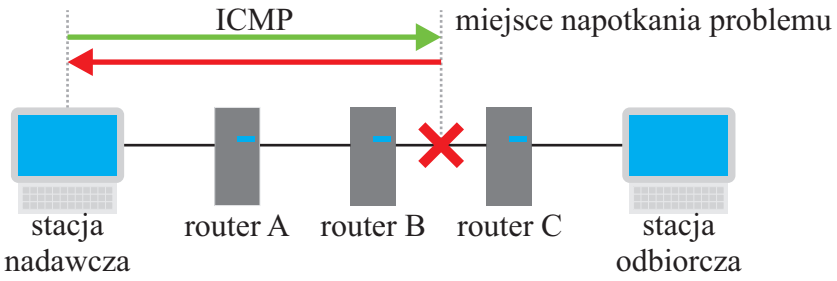
Protokół **ICMP** (ang. Internet Control Message Protocol) to protokół internetowych komunikatów sterujących. Jest nierozerwalnie związany z inkapsulującym go protokołem IP. Można także stwierdzić, że protokół ICMP jest **zestawem komunikatów**, przesyłanych w datagramach IP i zdolnych do zgłaszania błędów w dostarczaniu innych datagramów IP.

Tabela 5.1: Datagram IP w wersji 4

1 2 3 4	5 6 7 8	9 10 11 12 13 14 15 16	17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
wersja	dł. nagł.	typ usługi (TOS)	długość
identyfikacja		flagi	przesunięcie fragmentacji
czas życia (TTL)		protokół	suma kontrolna nagłówka
adres IP (źródłowy)			
adres IP (docelowy)			
opcje			
dane			

Z punktu widzenia planowanych eksperymentów interesujące są następujące pola nagłówka IP:

- **TOS** – Pole określa typ usługi. Pierwotnie poszczególne bity wyrażały „życznie" odnośnie traktowania datagramu:
  - 0-2 – określenie priorytetu,
  - 3 – wykorzystanie łącz o najmniejszym opóźnieniu,
  - 4 – wykorzystanie łącz o największej przepustowości,
  - 5 – wykorzystanie łącz o zwiększonej niezawodności,
  - 6-7 – zarezerwowane.
- **Flagi**
  - zarezerwowana,
  - nie fragmentować – ustawienie tej flagi zabrania dokonywania fragmentacji danych przez routery pośredniczące w jego przekazywaniu. W takim przypadku jeśli rozmiar datagramu przekracza wielkość ustaloną przez administratora routera lub wynikającą z ograniczeń stosowanych technologii, data gram jest porzucany, a router powinien przesłać do nadawcy komunikat ICMP informujący, że fragmentacja jest koniczna ale zabroniona,
  - więcej fragmentów – flaga jest ustawiona gdy datagram jest nieostatnim fragmentem datagramu, który uległ fragmentacji.
- **Czas życia TTL** – Pierwotnie każdy router przekazujący datagram IP był zobowiązany zmniejszyć wartość tego pola o liczbę sekund jaką przetrzymał datagram. Obecnie czas Przetwarzania datagramu przez routery jest mniejszy niż jedna sekunda i każdy router przekazujący datagram powinien zmniejszyć wartość pola TTL o 1. Datagram, którego pole TTL osiągnęło wartość 0 jest porzucany, a router powinien przesłać do nadawcy komunikat ICMP informujący o przeterminowaniu datagramu.
- **Adres IP źródłowy** – 32 bity (4 bajty) określające adres urządzeni, które wysłało datagram.
- **Adres IP docelowy** - 32 bity (4 bajty) określające adres urządzenia docelowgo. W trakcie interpretacji jest on dzielony na dwie części, określające adres sieci i adres urządzenia w danej sieci.



Rysunek 5.1: Przykładowe działanie protokołu ICMP

Sam protokół **ICMP** jest rozwiązaniem prostym. Nagłówek składa się z dwóch pól uzupełnionych sumą kontrolną (suma kontrolna nagłówka **ICMP** nie obejmuje danych):

- **Typ** – określa typ komunikatu (Tabela 5.3).
- **Kod** – określa przyczynę wygenerowania komunikatu ICMP.
- **Dane** – zawiera początkowy fragment (nagłówki protokołów) ramki, która spowodowała wygenerowanie komunikatu ICMP.

Tabela 5.2: Nagłówek protokołu IP w wersji 4

1 2 3 4 5 6 7 8	9 10 11 12 13 14 15 16	17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
typ	kod	suma kontrolna nagłówka
dane		

Tabela 5.3: Lista wybranych typów komunikatów

typ	znaczenie	nazwa angielska
0	zwrot echa – "odpowiedź na ping"	Echo Reply
3	nieosiągalność miejsca przeznaczenia (różne błędy według kodu)	Destination Unreachable
4	tłumienie nadawcy	Source Quench
5	zmiana trasowania	Redirect Message
6	alternatywny adres hosta	Alternate Host Address
8	**żądanie echa**	Echo Request
9	ogłoszenie routera	Router Advertisement
10	wybór routera	Router Solicitation
11	**przekroczenie limitu czasu**	Time Exceeded
12	problem z parametrem	Parameter Problem
13	żądanie sygnatury czasowej	Timestamp
14	zwrot sygnatury czasowej	Timestamp Reply
15	żądanie informacji	Information Request
16	zwrot informacji	Information Reply
17	żądanie maski adresowej	Address Mask Request
18	zwrot maski adresowej	Address Mask Reply
30	**śledzenie trasy**	Traceroute
31	błąd konwersji datagramu	Datagram Conversion Error
32	zmiana adresu ruchomego węzła	Mobile Host Redirect

5.1.1 Przykłady wykorzystania protokołu ICMP

- Zwolnienie napływania datagramów do routera w przypadku gdy router lub host jest **zbyt obciążony**.
- Powiadomienie o znalezieniu (przez router lub host) **lepszej trasy** do miejsca przeznaczenia.
- Powiadomienie o **nieosiągalności** miejsca przeznaczenia.
- **Przetestowanie** łączności sieciowej (np. program ping).

5.1.2 Programy wykorzystujące protokół ICMP

PING

Zadaniem programu jest zbadanie dostępności urządzenia sieciowego o podanym adresie. Program wysyła do niego komunikat ICMP typu 8 (żądanie echa). Urządzenie docelowe powinno w odpowiedzi przesłać do nadawcy komunikat ICMP typu 0 (odpowiedź na żądanie echa). Standardowo program wysyła cztery komunikaty z 32 bajtami danych. Tę i inne wielkości można zmienić stosując opcjonalne przełączniki (Tabela 5.4).

Tabela 5.4: Wybrane przełączniki programu ping

przełącznik	parametr	opis
-t		odpytuje określonego hosta do czasu zatrzymania
-a		tłumacz adresy na nazwy hostów.
-n	liczba	liczba wysyłanych powtórzeń żądania.
-l	rozmiar	rozmiar buforu transmisji.
-f		ustaw w pakiecie flagę "nie fragmentuj" (tylko IPv4).
-i	TTL	czas wygaśnięcia.
-v	TOS	typ usługi (nieaktualne).
-r	liczba	rejestruj trasę dla przeskoków (tylko IPv4).
-s	liczba	sygnatura czasowa dla przeskoków (tylko IPv4).
-j	lista_hostów	swobodna trasa źródłowa wg listy lista_hostów (tylko IPv4).
-k	lista_hostów	ściśle określona trasa źródłowa wg listy lista_hostów (tylko IPv4).
-w	limit_czasu	limit czasu oczekiwania na odpowiedź (w milisekundach).
-R		użyj nagłówka routingu, aby testować także trasę wsteczną (tylko IPv6).
-S	adres_źródłowy	adres źródłowy do użycia.
-4		wymuś używanie IPv4.
-6		wymuś używanie IPv6.

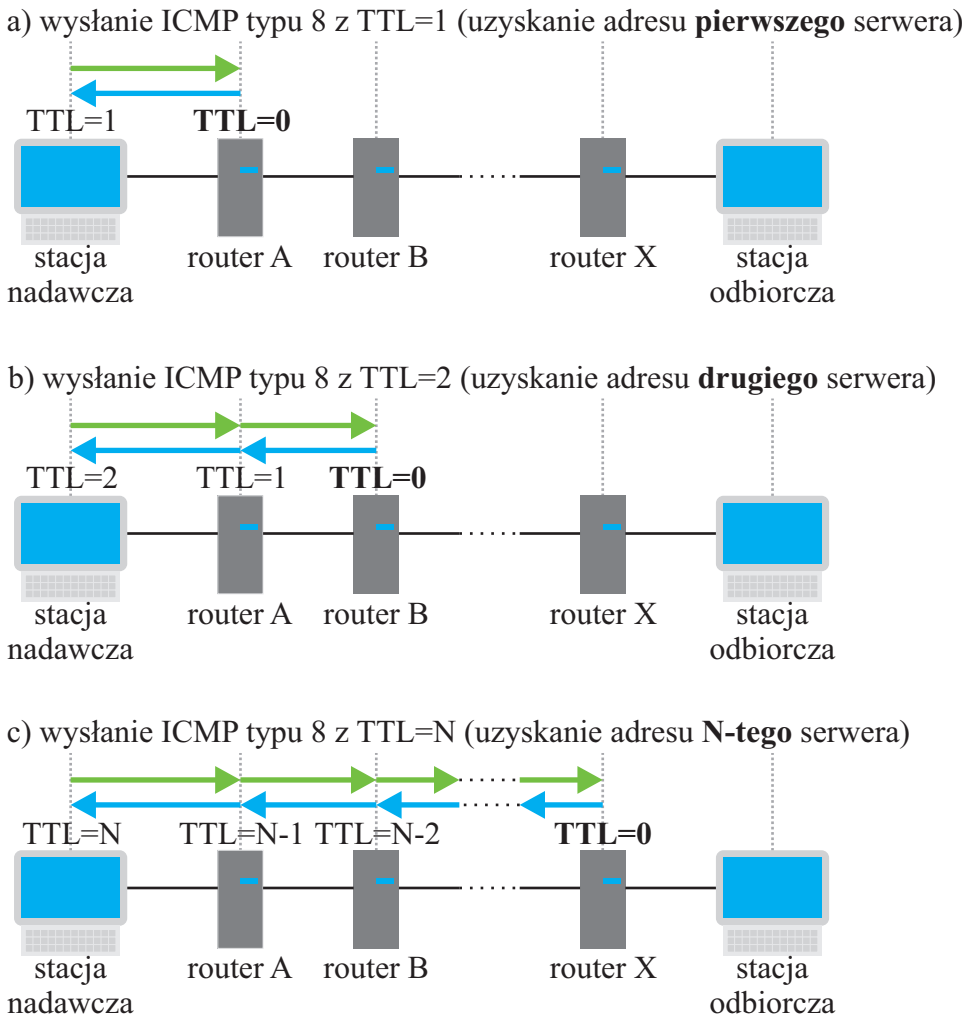
TRACERT

Zadaniem programu przedstawienie listy routerów pośredniczących w komunikacji pomiędzy dwoma urządzeniami sieciowymi. Program wysyła do urządzenia o wskazanym adresie komunikaty ICMP **typu 8 (żądanie echa)**. Program tracert wykorzystuje dodatkowo pole TTL w nagłówku protokołu IP. Pierwszy komunikat ICMP typu 8 jest wysyłany z wartością TTL=1. Pierwszy router, który pośredniczy w komunikacji z urządzeniem docelowym zmienia wartość TTL na 0 i porzuca pakiet (Rysunek 5.2.a)). Jeśli administrator routera nie zdecydował inaczej powinien on wysłać do nadawcy komunikat ICMP typu 11 (przeterminowany datagram IP). Program tracert odbierając ten komunikat uzyskuje informację o adresie IP pierwszego routera na ścieżce. Następnie wysyłane są komunikaty ICMP typu 8 z kolejnymi wartościami pola TTL=2,3,4..., co pozwala na uzyskanie adresów IP kolejnych routerów (Rysunek 5.2). Działanie programu kończy się gdy wartość TTL jest wystarczająca by żądanie echa dotarło do urządzenia docelowego i ten odpowie komunikatem ICMP typu 0 (odpowiedź na żądanie echa) lub gdy początkowa wartość pola TTL (maksymalna liczba przeskoków) osiągnie

określoną wartość maksymalną (zwykle 30). Jeśli program tracert uzyska od usługi DNS nazwy odpowiadające uzyskanym adresom IP routerów wyświetli je obok adresów IP. Wywołanie programu tracert może być uzupełnione opcjonalnymi przełącznikami (Tabela 5.5).

Tabela 5.5: Wybrane przełączniki programu tracert

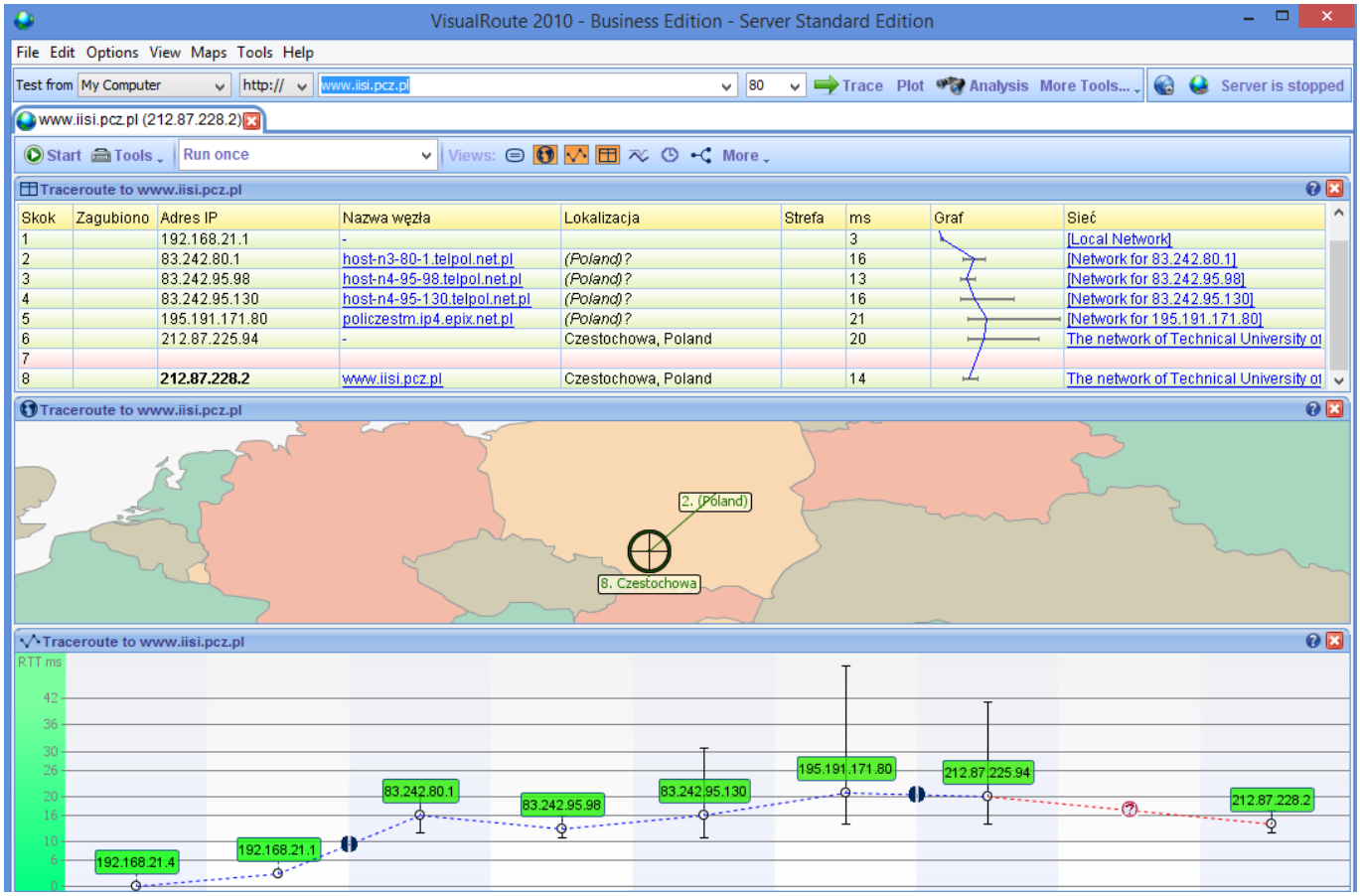
przełącznik	parametr	opis
-d		nie rozpoznawaj adresów jako nazw hostów.
-h	maks_przes	maksymalna liczba przeskoków w poszukiwaniu celu.
-j	lista_hostów	swobodna trasa źródłowa według listy lista_hostów (tylko IPv4).
-w	limit_czasu	limit czasu oczekiwania na odpowiedź w milisekundach.
-R		śledź ścieżkę błądzenia (tylko IPv6).
-S	adres_źródłowy	adres źródłowy do użycia (tylko IPv6).
-4		wymuś używanie IPv4.
-6		wymuś używanie IPv6.



Rysunek 5.2: Reprezentacja graficzna działania programu tracert

VisualRoute Lite

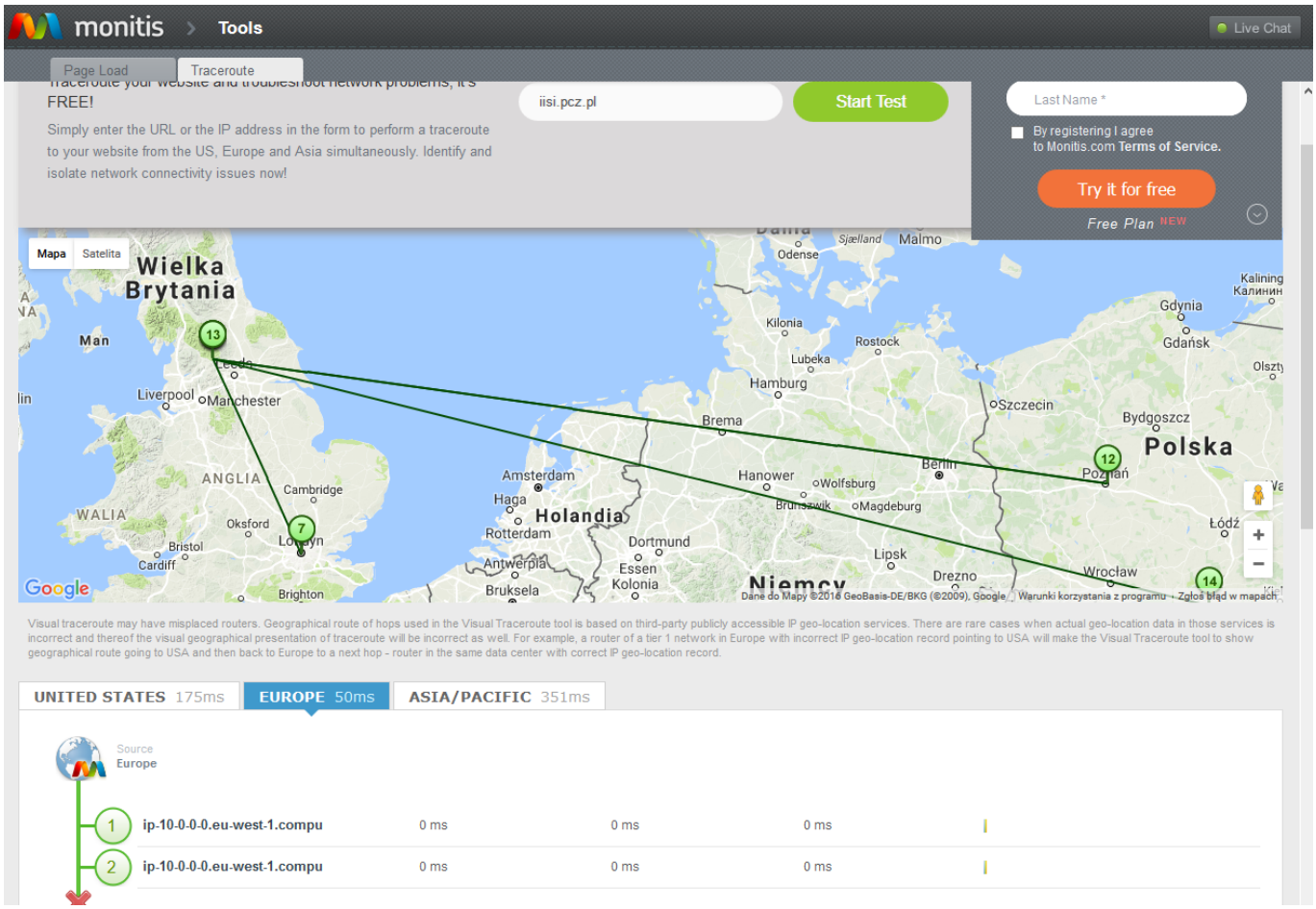
Program ten wykonuje zadanie programu tracert uzupełniając je wizualizacją wyników, m.in. na mapie świata. Na stronie producenta (http://www.visualroute.com/) znajduje się darmowa wersja testowa oraz darmowa wersja VisualRoute Lite.



Rysunek 5.3: Przykładowe działanie programu VisualRoute

Monitis Visual Trace Route Tool

Narzędzie to umożliwia wykonanie **zdalnie** programu tracert z trzech dowolnych lokalizacji (stany zjednoczone, europa, azja/pacyfik) uzupełniając wyniki wizualizacją na mapie świata. W sieci znajduje się wersja on-line (http://www.monitis.com/traceroute/).



Rysunek 5.4: Przykładowe działanie programu Monitis Visual Trace Route Tool

5.2 Cel ćwiczenia

Celem ćwiczenia jest zapoznanie się z przykładami zastosowania protokołu ICMP (ang. Internet Control Message Protocol).

5.3 Zadania do samodzielnego wykonania

5.3.1 Zadanie 1

Korzystając z programu **ping** należy sprawdzić dostępność serwerów znajdujących się w różnych lokalizacjach, np.:

- Instytut Inteligentnych Systemów Informatycznych,
- inne jednostki Wydziału Inżynierii Mechanicznej i Informatyki,
- inne jednostki Politechniki Częstochowskiej,
- Częstochowa, poza Politechniką Częstochowską,
- instytucje w Polsce, poza Częstochową,
- instytucje w Europie poza Polską,
- instytucje na poszczególnych kontynentach,
- ...

5.3.2 Zadanie 2

Korzystając z przełączników programu **ping** zbadać maksymalną wielkość ramki przekazywanej przez routery pośredniczące.

5.3.3 Zadanie 3

Korzystając z programu **tracert** należy uzyskać listę routerów pośredniczących w komunikacji z serwerami z Zadania 1. Zinterpretować różnorodność postaci uzyskanych wyników dla poszczególnych routerów.

5.3.4 Zadanie 4

Zasymulować działanie programu **tracert** za pomocą wielokrotnego wywołania programu **ping** (dla wszystkich serwerów z listy routerów pośredniczących) dla dowolnego serwera z Zadania 1.

5.3.5 Zadanie 5

Wykorzystując narzędzie **Monitis Visual Trace Route Tool** znaleźć serwer o jak największej liczbie zaznaczonych na mapie przeskoków. Czy pokonywana droga jest optymalna?

5.3.6 Zadanie domowe

W miarę możliwości należy wykonać zadanie także z użyciem programu VisualRoute Lite.

5.4 Sprawozdanie

Studenci przygotowują samodzielne sprawozdanie (ew. w zespołach pracujących przy wspólnym stanowisku komputerowym), w którym umieszczają uzyskane wyniki oraz komentarze i wnioski. Na podstawie uzyskanych nazw routerów, należy spróbować określić trasę pokonywaną przez datagramy na przybliżonej mapie Europy i Świata. Czy pokonywana droga jest optymalna?