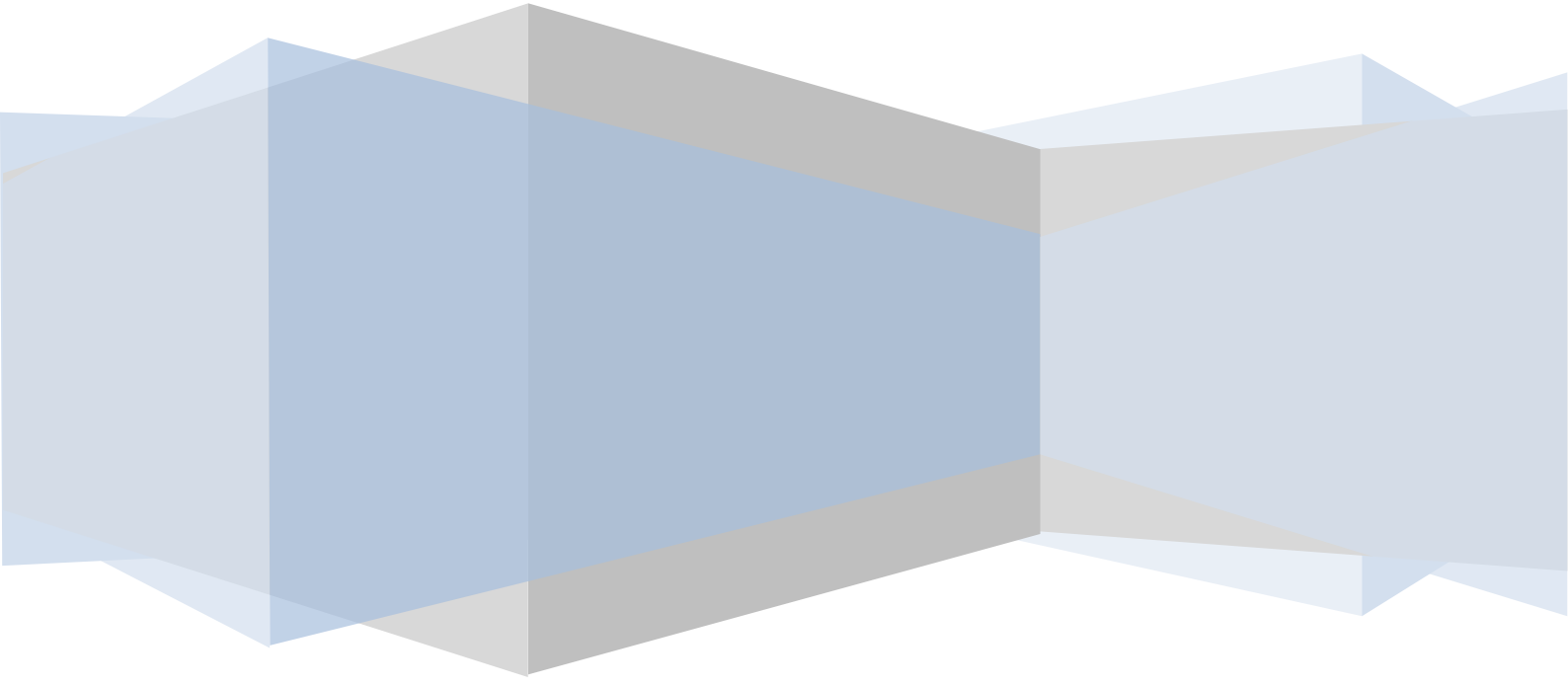
Katedra Inżynierii Komputerowej
Politechnika Częstochowska

Zastosowania protokołu ICMP

Laboratorium podstaw sieci komputerowych



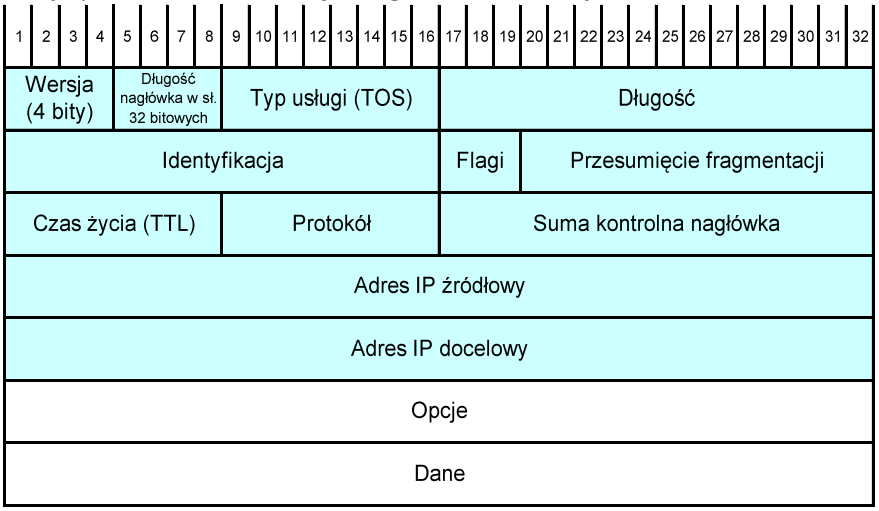
Cel ćwiczenia

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

Informacje wstępne

Protokół ICMP (ang. *Internet Control Message Protocol*) to protokół internetowych komunikatów sterujących. Jest nierozerwalnie związany z inkapsulującym go protokołem IP.

Poniższa ilustracja przedstawia budowę datagramu IP w wersji 4.



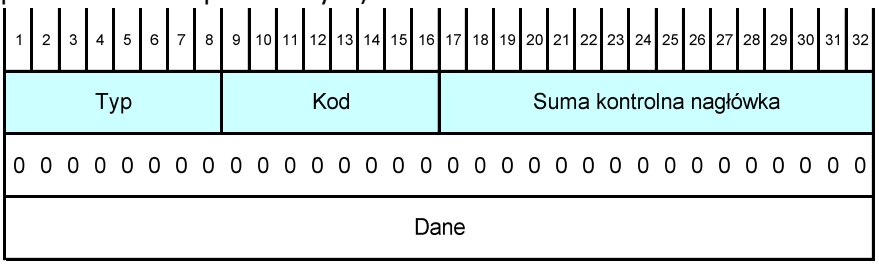
Z punktu widzenia planowanych eksperymentów interesujące są następujące pola nagłówka IP:

- **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.

  Obecnie wykorzystywany m.in. przez QoS.
- 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.

Sam protokół IP jest rozwiązaniem bardzo prostym. Nagłówek składa się z dwóch pól uzupełnionych sumą kontrolną (suma kontrolna nagłówka IP nie obejmuje danych, czyli też nagłówków protokołów enkapsulowanych):



- **Typ** – określa rodzaj komunikatu, wg poniższej tabeli.
- **Kod** – określa przyczynę wygenerowania komunikatu ICMP (tabela).

Typ	Kod	Opis
0	0	**Odpowiedź na żądanie echa**
3		**Cel nieosiągalny**
	0	sieć nieosiągalna
	1	host nieosiągalny
	2	nieobsługiwany protokół
	3	nieaktywny port
	4	konieczna lecz zabroniona fragmentacja
	5	niewłaściwa ścieżka trasowania
	6	nieznana sieć docelowa
	7	nieznany host docelowy
	8	odizolowany host źródłowy (przestażałe)
	9	dostęp do sieci docelowej zabroniony
	10	dostęp do hosta docelowego zabroniony
	11	sieć nieosiągalna przy danym TOS
	12	host nieosiągalny przy danym TOS
	13	komunikacja zabroniona
	14	złamanie zasad pierwszeństwa dla hosta
	15	rozpoczęty proces zamykania systemu
4	0	**Przepełnione bufory routera lub hosta**

Typ	Kod	Opis
5		**Żądanie przekierowania (zmiany trasy)**
	0	dla sieci
	1	dla hosta
	2	dla sieci z danym TOS
	3	dla hosta z danym TOS
8	0	**Żądanie echa**
9	0	**Rozgłoszenie routera**
10	0	**Oferowanie usług przez router**
11		**Przeterminowanie pakietu (TTL=0)**
	0	w trakcie przekazywania
	1	w trakcie defragmentacji
12		**Błędne dane**
	0	błędny nagłówek IP
	1	brak wymaganych opcji
13	0	**Żądanie czasu**
14	0	**Odpowiedź na żądanie czasu**
15	0	**Żądanie informacji**
16	0	**Odpowiedź na żądanie informacji**
17	0	**Żądanie maski adresu**
18	0	**Odpowiedź na żądanie maski adresu**

- **Dane** – zawiera początkowy fragment (nagłówki protokołów) ramki, która spowodowała wygenerowanie komunikatu ICMP.

Programy wykorzystujące 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:

```
ping /?

Sposób użycia: ping [-t] [-a] [-n liczba] [-l rozmiar] [-f] [-i TTL] [-v TOS]
               [-r liczba] [-s liczba] [[-j lista_hostów] | [-k lista_hostów]]
               [-w limit_czasu] [-R] [-S adres_źródłowy] [-4] [-6] nazwa_celu
Opcje:
    -t              Odpytuje określonego hosta do czasu zatrzymania.
                    Aby przejrzeć statystyki i kontynuować,
                    naciśnij klawisze Ctrl+Break.
                    Aby zakończyć, naciśnij klawisze Ctrl+C.
   -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 (tylko IPv4).
    -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 (podobnie jak **ping**) 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. 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. 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** moży być uzupełnione opcjonalnymi przełącznikami:

```
tracert /?

Sposób użycia: tracert [-d] [-h maks_przes] [-j lista_hostów] [-w limit_czasu]
               [-R] [-S adres_źródłowy] [-4] [-6] nazwa_celu

Opcje:
    -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.
```

VisualRoute

Program ten wykonuje zadanie programu **tracert** uzupełniając je wizualizacją wyników, m.in. na mapie świata. Na stronie producenta (http://www.visualroute.com/) znajduje się interaktywne demo. Można z niej również pobrać darmową wersję testową oraz darmową wersję **VisualRoute Lite**.

Zadania do wykonania

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

- Katedra Inżynierii Komputerowej,
- 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,
- …

Korzystając z przełączników programu **ping** zbadać dla dostępnych, ww. serwerów

- liczbę routerów pośredniczących,
- maksymalną wielkość ramki przekazywanej przez routery pośredniczące,
- wpływ wartości pola TOS nagłówka IP na komunikację.

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

Zasymulować działanie programu **tracert** za pomocą wielokrotnego wywołania programu **ping**.

Zadanie domowe

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

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?