Protokoły wspomagające

Mikołaj Leszczuk

Spis treści wykładu

- **Współpraca z warstwą łącza danych:**
  - **Protokół odwzorowania adresów (ARP)**
  - **Odwrotny protokół odwzorowania adresów (RARP)**
- **ICMP**
  - **Opis protokołu**
  - **Przykład zastosowania – ping**

Protokół odwzorowania adresów – ARP (1/2)

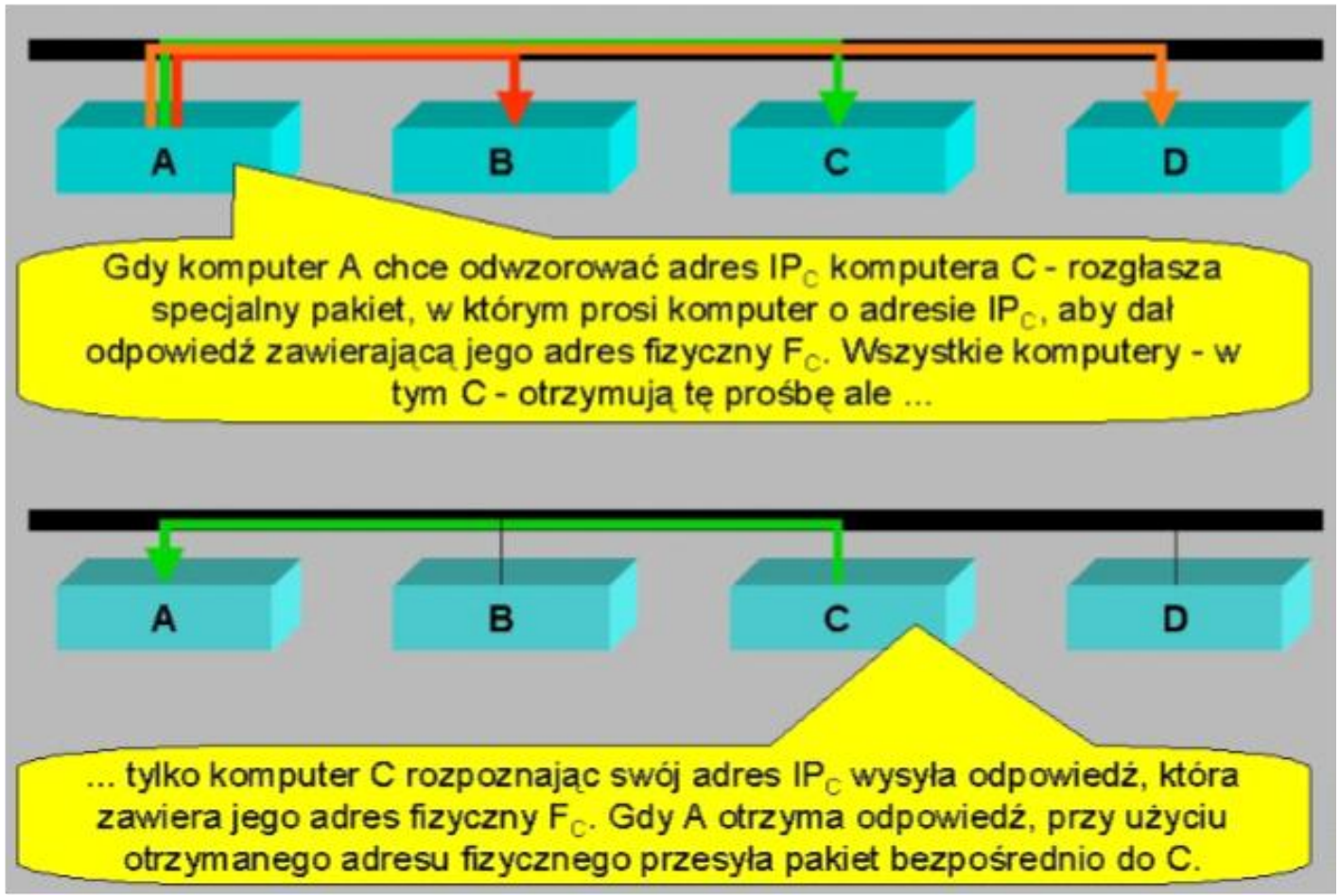
- W schemacie adresowania IP, każdy komputer to 32-bitowy adres jednoznacznie identyfikujący go w sieci
- Jednak komunikacja dwóch maszyn – tylko wtedy kiedy znane są nawzajem adresy fizyczne

Protokół odwzorowania adresów – ARP (2/2)

- Potrzeba przekształcenia adresu IP na adres fizyczny tak aby informacja poprawnie przesyłana
- Przykład sieci Ethernet, długi 48-bitowy adres fizyczny przypisany w trakcie procesu produkcyjnego urządzeń sieciowych
- W efekcie podczas wymiany karty sieciowej w komputerze, zmiana adresu fizycznego maszyny

Zasada działania ARP

Źródło: "Protokół ARP i RARP "



Protokół odwrotnego odwzorowania – RARP (1/2)

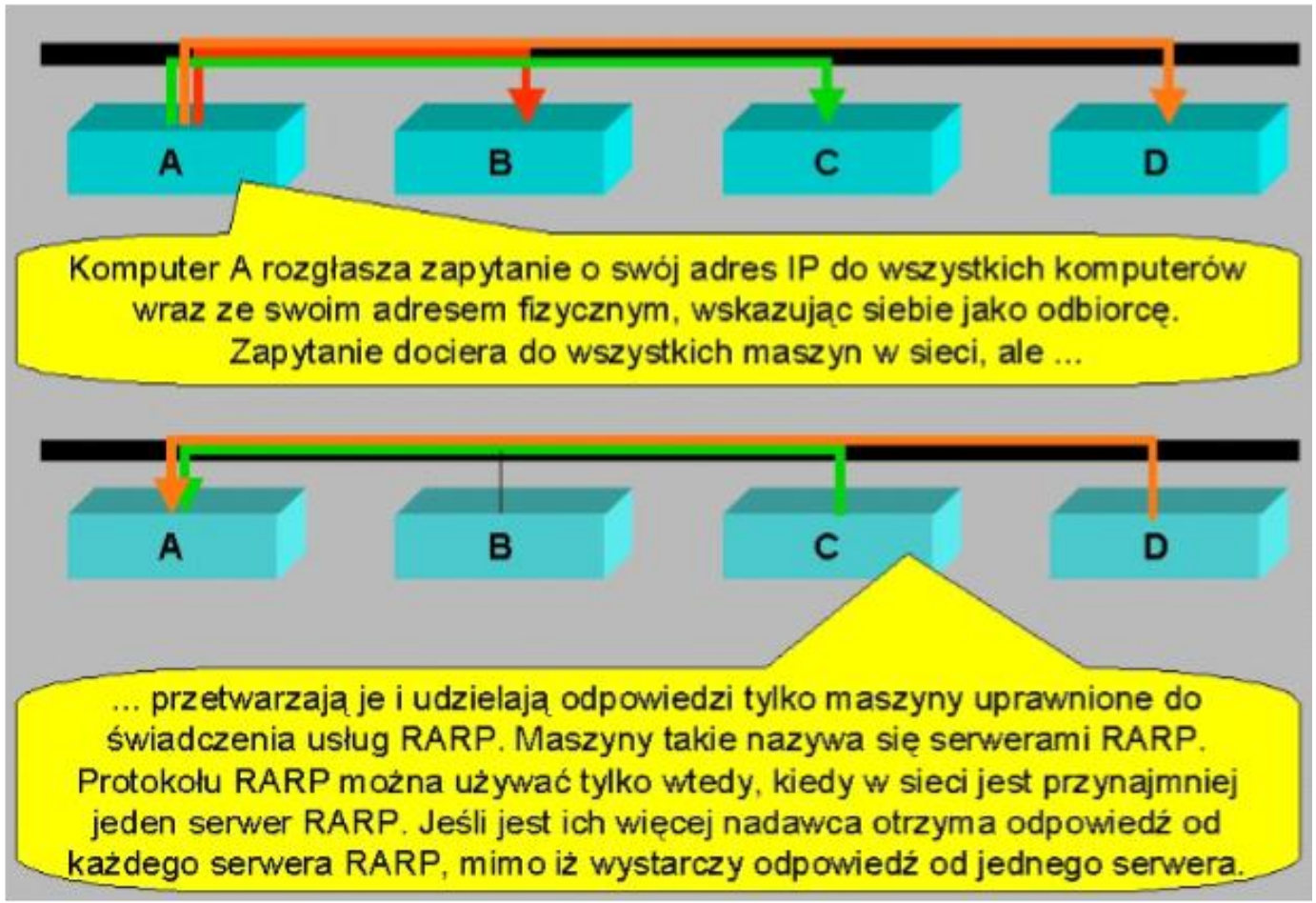
- Wiadomo już jak można uzyskać adres fizyczny innego komputera, znając jego adres IP
- Adres IP zwykle przechowywany w pamięci zewnętrznej komputera, skąd pobierany w trakcie ładowania systemu operacyjnego

Protokół odwrotnego odwzorowania – RARP (2/2)

- Pytanie: jak maszyna nie wyposażona w dysk twardy określa swój adres IP?
- Odpowiedź: w sposób przypominający uzyskiwanie adresu fizycznego
- Protokół odwrotnego odwzorowania adresów RARP (*Reverse Address Resolution Protocol*) – uzyskiwanie adresu IP na podstawie adresu fizycznego

Zasada działania RARP

Źródło: "Protokół ARP i RARP "



Protokół ICMP
Wprowadzenie (1/4)

- Przypomnienie cech protokołu IP:
  - Zawodne przenoszenie pakietów
  - Niezawodne przenoszenie treści
  - Wędrówka pakietów “end-to-end”

Protokół ICMP
Wprowadzenie (2/4)

- Sytuacje awaryjne:
  - Brak możliwości wyznaczenia trasy
  - Brak możliwości dostarczenia datagramu:
    - Przeciążenie sieci
    - Wyłączenie maszyny docelowej
    - Wyczerpanie się licznika czasu życia datagramu

Protokół ICMP
Wprowadzenie (3/4)

- Konieczność poinformowania nadawcy, aby podjął działania w celu uniknięcia skutków tej sytuacji
- Protokół komunikatów kontrolnych Internetu ICMP (ang. “Internet control message protocol”):
  - Umożliwienie ruterow oznajmiania błędów
  - Udostepnianie informacji o niespodziewanych sytuacjach

Protokół ICMP
Wprowadzenie (4/4)

- Wymagana część IP (konieczność realizacji przez każdą implementację IP)
- Enkapsulacja komunikatów ICMP w częściach datagramów IP przeznaczonych na dane

Protokół ICMP
Komunikacja

- IP: użytkownik <-> użytkownik
- ICMP (w teorii): ruter <-> ruter
- ICMP (w praktyce): dow. urządzenie <-> dow. urządzenie (obsługa komunikatów błędów ICMP przez moduł oprogramowania ICMP)
- W niektórych przypadkach, możliwość współpracy z protokołami wyższych warstw

Protokół ICMP
Reakcja na błędy (1/2)

- Standard protokołu ICMP:
  - Opis wszystkich komunikatów błędów
  - Opis niektórych sposobów reakcji na nie

Protokół ICMP
Reakcja na błędy (2/2)

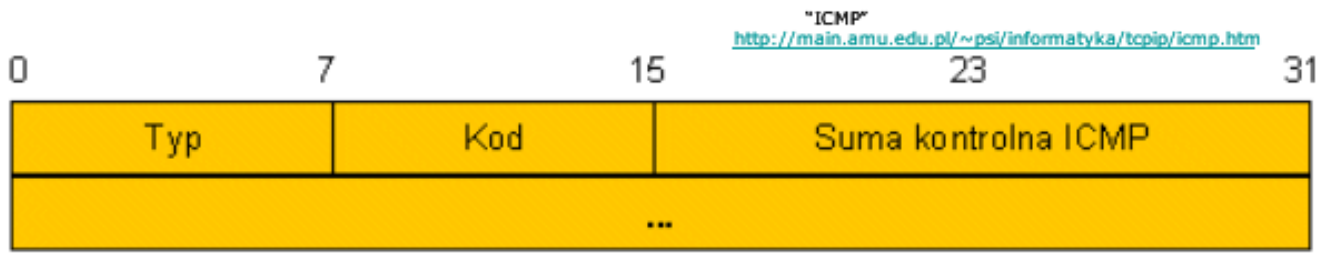
- W przypadku błędu:
  - Odbiorca: powiadomienie nadawcy
  - Nadawca:
    - Przekazanie informacji użytkownikowi
    - Samodzielne podjęcie działań mających na celu uporanie się z tym problemem

Protokół ICMP
Formaty komunikatów (1/2)

Każdy komunikat ICMP to inny format, część wspólna to trzy pola:

- 8-bitowe pole **TYP** komunikatu – identyfikacja komunikatu
- 8-bitowe pole **KOD** – dalsze informacje na temat rodzaju komunikatu
- 16-bitowe pole **SUMA KONTROLNA** – obliczane podobne jak suma IP, ale odnoszące się tylko do komunikatu ICMP

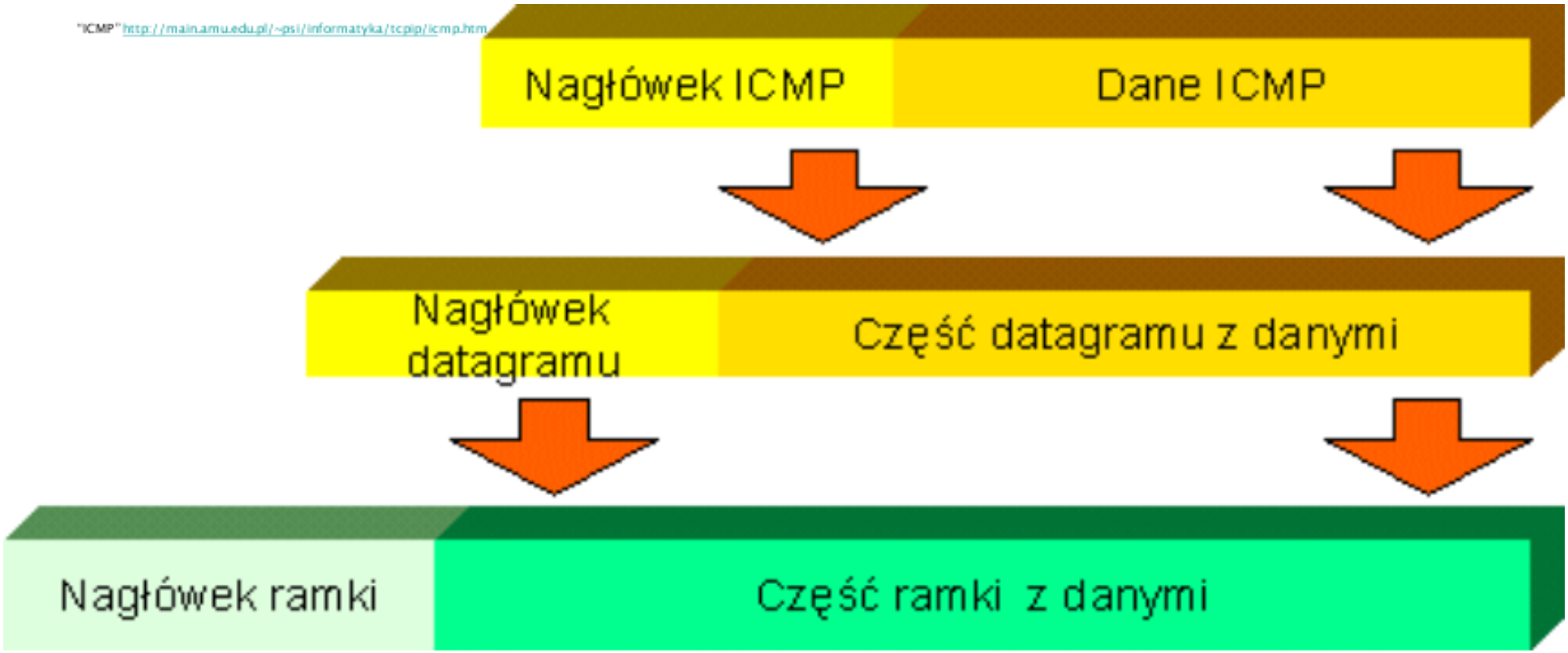
Protokół ICMP
Formaty komunikatów (2/2)



Protokół ICMP
Enkapsulacja (1/2)

- Oprócz tego, w przypadku oznajmiania błędu – nagłówek i pierwsze 64 bity danych datagramu z którym były problemy
- Dwa poziomy enkapsulacji komunikatów ICMP:
  - Enkapsulacja komunikatu ICMP w części datagramu IP przeznaczonej na dane
  - Enkapsulacja datagramu IP w części danych ramki

Protokół ICMP
Enkapsulacja (2/2)



Protokół ICMP
Przenoszenie datagramów (1/2)

- Trasy datagramów przenoszących komunikaty ICMP – wyznaczane dokładnie tak jak dla datagramów przenoszących informacje użytkowników
- Brak dodatkowych:
  - Priorytetów
  - Zabezpieczeń

Protokół ICMP
Przenoszenie datagramów (2/2)

- Efekt – możliwość zagubienia samych komunikatów o błędzie
- Co więcej w przeciążonej sieci komunikat o błędzie to dodaktowe przeciążenie

Protokół ICMP
Uwagi końcowe

- Wyjątek w procedurach obsługi błędów: nie ma tworzenia komunikatów o błędach jeśli błąd spowodowany przez datagram IP niosący komunikat ICMP
- **ICMP to nie protokół wyższego rzędu lecz wymagana część IP, mimo enkapsulacji i przenoszenia przez IP**

Przykład użycia ICMP – ping – Wprowadzenie (1/2)

- Wysyłanie pakietu informacji żądającej odesłania jej do wysyłającego
- Badanie:
  - Istnienia połączenia między komputerami
  - Czasu potrzebnego na przejście pakietu
  - Tego czy załączono drugi komputer

Przykład użycia ICMP – ping – Wprowadzenie (1/2)

- Zastosowania:
  - Testowanie sieci
  - Pomiary obciążenia sieci
  - Zarządzanie siecią
- Pomiar aktywny
- “Zaśmiecanie” sieci przy nadużywaniu, zwłaszcza niebezpieczne w przypadku użycia w skryptach

ping – Opis ogólny

- Wersje:
  - ping – wersja dla IPv4
  - ping6 – wersja dla IPv6
- Wysłanie zapytania – użycie komunikatu ICMP „ECHO_REQUEST” do zdalnego:
  - Hosta
  - Rutera
- Wysłanie odpowiedzi – komunikat ICMP „ECHO_RESPONSE”

ping – Zawartość datagramu ICMP „ECHO_REQUEST”

- Nagłówek IP
- Nagłówek ICMP
- Czas
- Padding

ping
Niektóre opcje (1/2)

- -c count
  Zatrzymaj po wysłaniu count pakietów ECHO_REQUEST. Użyty wraz z opcją deadline, ping czeka na odebranie count pakietów ECHO_REPLY, do czasu timeout.
- -p pattern
  Można wyspecyfikować do 16 bajtów “paddingu” wypełniających wysyłany pakiet.

ping
Niektóre opcje (2/2)

- -s packetsize
  Określa liczbę danych do wysłania.
- -w deadline
  Określa timeout, w sekundach, po którym ping kończy pracę, nie zważając na liczbę pakietów.

ping
Gdy brak sieci (1/4)

- Pierwsze użycie dla localhost, celem sprawdzenia czy prawidłowo pracuje lokalny interfejs
- Następnie – pingowanie hostów i ruterów położonych coraz dalej

Ping – Wyniki działania

- Obliczanie:
  - RTT (ang. “Round-Trip Time”)
  - Statystyk strat pakietów
- W przypadku odebrania podwójnych pakietów, duplikaty:
  - Nie wliczane do obliczeń strat/uszkodzeń pakietów
  - Wliczane do ustalenia minimalnych/średnich/maksymalnych wartości RTT

ping
Gdy brak sieci (3/4)

- Wyświetlenie krótkiego podsumowania po:
  - Osiągnięciu licznika pakietów:
    - Wysłanych
    - Odebranych
  - Zakończeniu programu sygnałem SIGINT

ping
Gdy brak sieci (4/4)

- Krótsze, bieżące statystyki są możliwe do wyświetlenia bez zakańczania programu, po otrzymaniu sygnału SIGQUIT

ping
Kody powrotu

- W przypadku braku jakichkolwiek odpowiedzi – kod powrotu **1**
- Gdy ustalono count i deadline, ale odebrano mniej pakietów niż count do czasu deadline – kod powrotu 1
- W przypadku innych błędów – kod powrotu 2
- W przeciwnym przypadku – kod powrotu 0
- Możliwość użycia kodów powrotu w celu sprawdzenia czy dany host jest aktywny

ping – Pakiet ICMP (1/2)

- Nagłówek IP bez opcji (20 bajtów)
- Pakiet ICMP ECHO_REQUEST:
  - Dodatkowych 8 bajtów nagłówka ICMP
  - Pole danych

ping – Pakiet ICMP (2/2)

- Kiedy podano packetsize, to równe temu polu danych (standardowo 56)
- Dlatego ilość danych odebranych wewnątrz pakietu IP typu ICMP ECHO_REQUEST zawsze większa o 8 niż żądane (przez nagłówek ICMP) pole danych

ping – wstawianie znacznika czasu

- Wstawianie w początkowe bajty danych znacznika czasu – jeśli rozmiar pola danych wystarczający
- Znacznik używany do obliczania RTT
- Przy krótszych polach danych – brak podawania RTT

ping – duplikowane pakiety (1/2)

- Raportowanie zduplikowanych pakietów przez ping
- Duplikaty nie powinny się nigdy pojawiać!
- Powód pojawiania się: niepoprawne retransmisje w warstwie łącza danych

ping – duplikowane pakiety (2/2)

- Istnieje wiele powodów niepoprawnych retransmisji
- Duplikaty = raczej niepokojący sygnał dla administratora
- Niewielka liczba zduplikowanych pakietów to jednak jeszcze nie powód do alarmu

ping – uszkodzone pakiety

- Raportowanie uszkodzonych pakietów
- Uszkodzone pakiety = poważny problem
- Zwykle uszkodzenie sprzętowe gdzieś na trasie pakietów, w:
  - Hostach
  - Ruterach

ping
Różne wzorce danych (1/4)

- W teorii: równoprawne traktowanie przez warstwę sieciową pakietów o różnych zawartościach pola danych
- W praktyce:
  - Niestety – w sieci znane przypadki nierównego traktowania pakietów
  - Długo nie wykryte

ping
Różne wzorce danych (2/4)

- Wzorce pakietów o niestandardowym rozkładzie bitów:
  - Same zera
  - Same jedynki
  - Prawie same zera/jedynki
- Zwykle np.: same zera – to nie same zera w LLC

ping
Różne wzorce danych (3/4)

- Skomplikowane relacje pomiędzy zadanym ciągiem, a sekwencją wysyłaną przez kontroler
- Problemy z zależnością od danych = długotrwałe testowanie

ping
Różne wzorce danych (4/4)

- Gdy się ma szczęście, można trafić na plik:
  - Niemożliwy do przesłania przez sieć
  - Przesyłany znacznie dłużej niż inne pliki o podobnej długości
- Wtedy można użyć polecenia ping z opcją -p pobierając sekwencje z pliku

Literatura (1/2)

- “RFC 792 (rfc792) - Internet Control Message Protocol” http://www.faqs.org/rfcs/rfc792.html
- “ICMP” http://main.amu.edu.pl/~psi/informatyka/tcpip/icmp.htm
- “The Story of the PING Program” http://ftp.arl.mil/~mike/ping.html
- “Manpage of PING” http://www.fifi.org/cgi-bin/man2html/usr/share/man/man8/ping6.8.gz
- “ping” http://www.immt.pwr.wroc.pl/export_hp/tool/node13.html
- “Gery.pl - Pliki > Internet / Połączenia / Monitoring” http://pliki.gery.pl/p/0,23,2.html

Literatura (2/2)

- “IFCONFIG(8) Podręcznik programisty linuxowego”
- “NETSTAT(8) Podręcznik programisty linuxowego”
- “TCP / IP protocols: ICMP UDP FTP HTTP reference page” http://www.protocols.com/pbook/tcpip1.htm
- “Protokół ARP i RARP” http://www.man.rzeszow.pl/docs/ip/xarp.htm