Sieci komputerowe

Wykład 6
Warstwa transportu, protokoły UDP, ICMP

Zadania warstwy transportu

- Zapewnienie niezawodności
- Dostarczanie danych do odpowiedniej aplikacji w warstwie aplikacji (multipleksacja)
- Kontrola przepływu
- Przesyłanie strumienia bajtów

Numery portów

- Numer portu służy protokołom UDP i TCP do identyfikacji procesów w warstwie aplikacji
- Oprogramowanie warstwy aplikacji korzystające z UDP/TCP używa modelu klient-serwer
- Numer portu jest liczbą 16 bitową
- Numery portów poniżej 1024 są związane z aplikacjami i określone przez IANA dla każdej z aplikacji
  - http://www.iana.org/assignments/port-numbers
- Numery portów dla aplikacji klienckich są zazwyczaj przydzielane na krótko i z zakresu powyżej 1024

Charakterystyczne numery portów

- Lista numerów portów popularnych usług:
  - 20 FTP - dane
  - 21 FTP
  - 22 SSH
  - 23 Telnet
  - 25 SMTP
  - 53 DNS
  - 70 Gopher
  - 80 HTTP
  - 109 POP2
  - 110 POP3
  - 119 NNTP

Gniazda

- Gniazda umożliwiają wielu aplikacjom jednoczesną komunikację
- Gniazdo jest określone za pomocą pary adres IP i numer portu
  - Np. 193.0.96.15:80

/etc/services, netstat

- Dobrze znane numery portów znajdują się w pliku /etc/services
- Aby zobaczyć jakie aplikacje nasłuchują na portach należy użyć programu netstat

UDP, nagłówek protokołu

0	31
16 bit nr portu źródłowego	16 bit nr portu przeznaczenia
16 bit długość UDP	16 bit suma kontrolna UDP
dane	

- UDP (User Datagram Protocol) jest prostym protokołem warstwy transportu – nie zapewnia niezawodności
- Nagłówek UDP ma dużo prostszą budowę niż TCP

Pseudonagłówek UDP

0 31

32 bit adres źródłowy IP		
32 bit adres przeznaczenia IP		
zero	8 bit protokół	16 bit długość UDP
16 bit nr portu źródłowego		16 bit nr portu przeznaczenia
16 bit długość UDP		16 bit suma kontrolna UDP
dane		

- Pseudonagłówek jest wykorzystywany do obliczania sumy kontrolnej
- Jest stosowany po to, aby sprawdzić, czy dane dotarły do właściwego adresata (stąd konieczność uwzględnienia przy liczeniu sumy kontrolnej adresów IP)

Własności protokołu UDP

- Nie zapewnia niezawodności (w przeciwieństwie do TCP)
- Nie jest zorientowany strumieniowo (w przeciwieństwie do TCP)
- Jest protokołem bezpołączeniowym (odmiennie niż TCP)

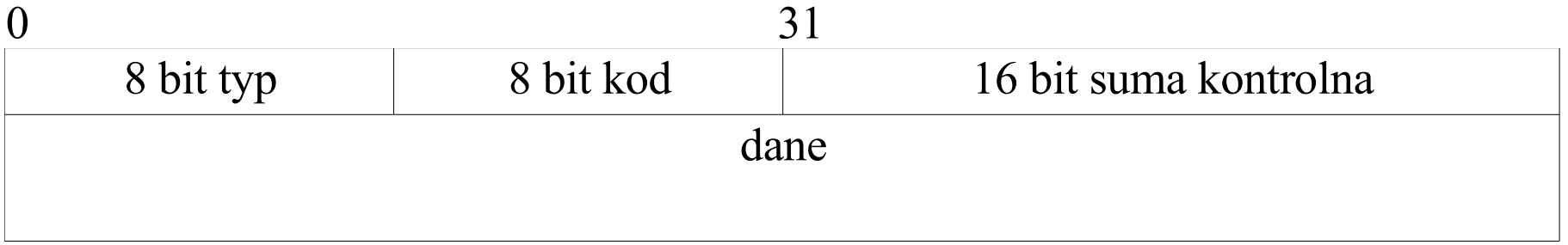
Zastosowanie UDP

- Przykłady zastosowania:
  - DNS
  - RIP
  - DHCP (broadcast)

Protokół ICMP

- ICMP (Internet Control Message Protocol) służy do wysyłania komunikatów o problemach związanych z komunikacją, np. z rutingiem
- Jest używany także w celach diagnostycznych

Nagłówek ICMP



- Komunikaty ICMP są przesyłane wewnątrz datagramów IP
- Komunikat ICMP o błędzie, w polu dane, zawiera nagłówek datagramu IP, który spowodował wygenerowanie komunikatu i 8 bajtów następujących po nim (może to być np. nagłówek UDP – wtedy znany jest numer portu źródłowego. Numer ten może być wtedy skojarzony przez system odbierający wiadomość z konkretnym procesem np. klientem ftp)

Komunikaty ICMP

Typy komunikatów ICMP:

Typ	***Kod***	***Opis***
0 (odpowiedź echo)	0	Odpowiedź echo
3 (przeznaczenie nieosiągalne)	0	Sieć nieosiągalna
3	1	Host nieosiągalny
3	2	Protokół nieosiągalny
3	3	Port nieosiągalny
3	4	Konieczna fragmentacja, lecz włączony bit „nie fragmentować”
3	5	Błąd trasy routowania
3	6	Nieznana sieć przeznaczenia
3	7	Nieznany host przeznaczenia
3	8	(Przestarzałe – nieużywane)
3	9	Dostęp do sieci przeznaczenia zabroniony
3	10	Dostęp do hosta przeznaczenia zabroniony
3	11	Sieć nieosiągalna dla usługi
3	12	Host nieosiągalny dla usługi
3	13	Komunikacja ograniczona za pomocą filtrowania
8 (zapytanie o echo)	0	Zapytanie o echo
11 (przekroczenie czasu)	0	Podczas przejścia czas życia równy 0

Komunikaty ICMP c.d.

Komunikat ICMP o nieosiągalności przeznaczenia:

8 bit typ (3)	8 bit kod (3)	16 bit suma kontrolna
Nie używane		
Dane (nagłówek datagramu IP, który spowodował wygenerowanie komunikatu oraz 8 bajtów następujących po nim – czyli może to być np. nagłówek UDP)		

Komuniktat ICMP żądanie echa i odpowiedź echo:

8 bit typ (3)	8 bit kod (3)	16 bit suma kontrolna
Identyfikator (nr procesu)		Numer sekwencyjny
dane		

Programy korzystające z ICMP

- ping
- traceroute
  - traceroute wysyła datagramy UDP o TTL zwiększanym o 1, pozwala to uzyskać obraz trasy do hosta przeznaczenia