TIN
Techniki Internetowe

zima 2019

Grzegorz Blinowski

Instytut Informatyki

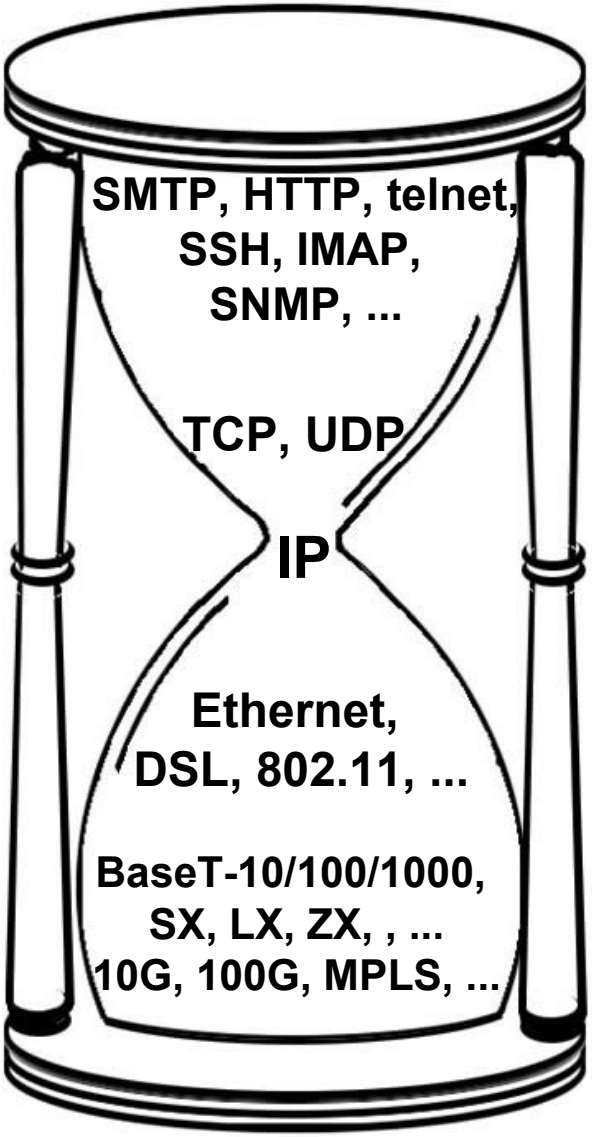
Politechniki Warszawskiej

Plan wykładów

2	Intersieć, ISO/OSI, protokoły sieciowe, IP
3	Protokół IP i prot. transportowe: UDP, TCP
4	Model klient-serwer, techniki progr. serwisów
5	Protokoły aplikacyjne: telnet, ftp, smtp, nntp, inne
6	HTTP
7, 8	HTML, XML
9, 10, 11	Aplikacje WWW, CGI, sesje, serwery aplikacji serwlety, integracja z backended SQL
12	Aspekty zaawansowane: wydajność, przenośność, skalowalność; klastering
13	Inne: P2P, SOAP, RDF, WSDL, ontologie
14	Wstęp do zagadnień bezpieczeństwa (IPSec, VPN, systemy firewall) oraz aspekty kryptograficzne (DES, AES, RSA, PGP, S/MIME), tokeny i akceleracja sprzętowa

Protokół IP

“Klepsydra” protokołów



Podstawowe własności rodziny protokołów TCP/IP

- Otwartość (nie zależą od producentów sprzętu lub oprogramowania)
- Dostępne dla praktycznie każdej platformy, od smartfonów i komputerów wbudowanych po superkomputery
- Mogą być stosowane w sieciach LAN jak i WAN

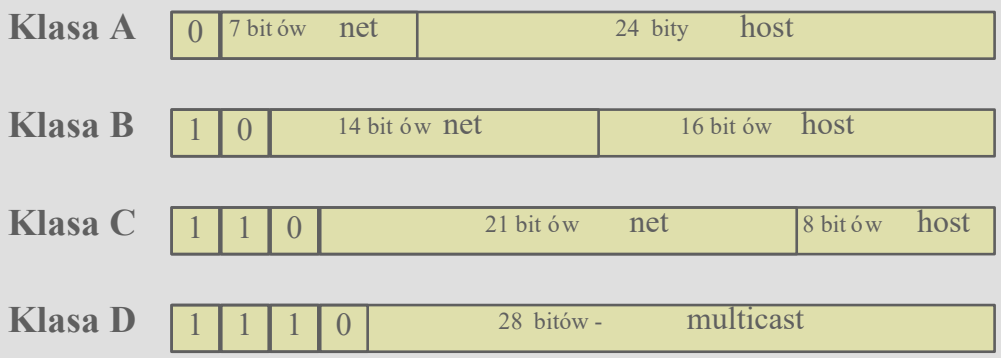
Podstawowe cechy protokołu IP

- Protokół warstwy 3 (sieciowej) - odpowiada za dostarczenie danych od hosta do hosta
- Cechy:
  - Datagramowy
  - Nie gwarantuje sekwencyjności, nie gwarantuje poprawności, może nastąpić: uszkodzenie, gubienie i zwielokrotnienie pakietów
- Ruting - wyłącznie na podstawie adresu docelowego
- Przygotowany do przenoszenia protokołów warstwy 4
- Przygotowany do przenoszenia pakietów przez sieci o różnym MTU (fragmentacja – zob. dalej)
- Dupleksowy

Adresowanie IPv4

- Adres liczba 32-u bitowa, konwencja “big-endian” (network order), zwyczajowo zapisuje się jako 4 bajty (oktety)
  - Dygresja dot. API: **`htonl(), ntohl()`**
- W celu uproszczenia rutingu adres dzieli się na część określajacą sieć oraz pozostałą - określajacą hosta
- Mechanizm “subnettingu” pozwala na dalsze dzielenie części hosta na pod-sieć i hosta (wielokrotnie)
- Adresy prywatne {RFC 1918}, Network Address Translation (NAT) {RFC 1631}:
  - `10.0.0.0 - 10.255.255.255 jedna klasa A`
  - `172.16.0.0 - 172.31.255.255 16 klas B`
  - `192.168.0.0 - 192.168.255.255 256 klas C`

Adresowanie IP - przypomnienie



Prefiks wyznacza jednoznacznie klasę adresu

host = 0..0 oraz 1…1 ma znaczenie specjalne (sieć, broadcast)

Klasa D - Multicast RFC 1112

Klasa **A**: wiele hostów, mało sieci

0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh

7 bitów sieci (126 - 0 i 127 zarezerw.), 24 bitów hosta (> 16M hostów/sieć)

Pierwszy bajt: 1-127

Klasa **B**: zrównoważona liczba hostów i sieci

10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh

16,384 sieci klasy B, 65,534 hostów/sieć

Pierwszy bajt: 128-191

Klasa **C**: dużo małych sieci

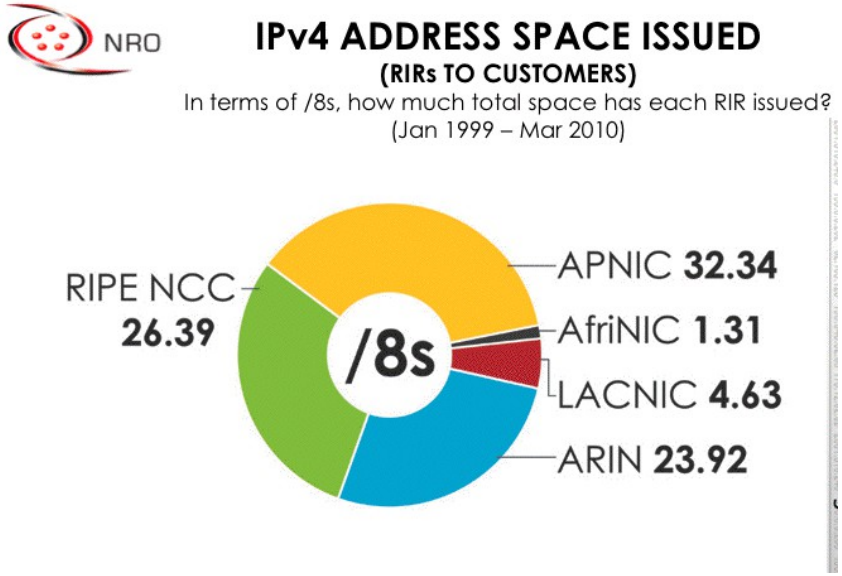
110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh

2,097,152 sieci klasy C, 254 hostów/sieć

Pierwszy bajt: 192-223 (decimal)

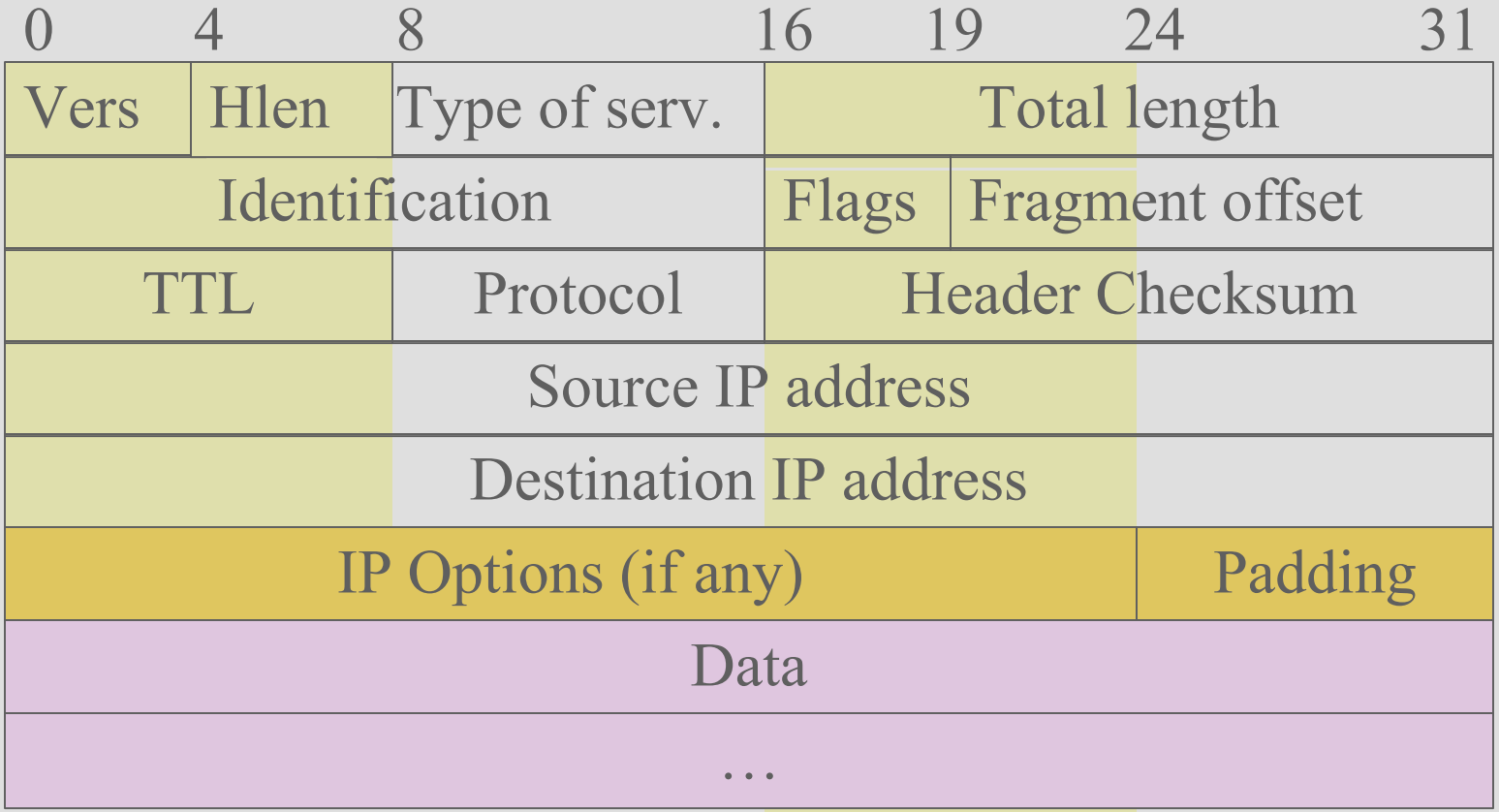
Klasa D: 224-247(*RFC 1112*); Klasa E: 248-255

Zarządzanie adresami IP



- APNIC – Australia, Azja centralna, pd.-wsch. i Pacyfik *www.apnic.net*
- AfriNIC - Afryka
- ARIN – Ameryka Pn. (USA i Kanada) *www.arin.net*
- LACNIC – Ameryka Pd. i Środkowa
- RIPE –Europa, Rosja, Bliski i Śr Wschód *www.ripe.net*

Nagłówek protokołu IP - przypomnienie



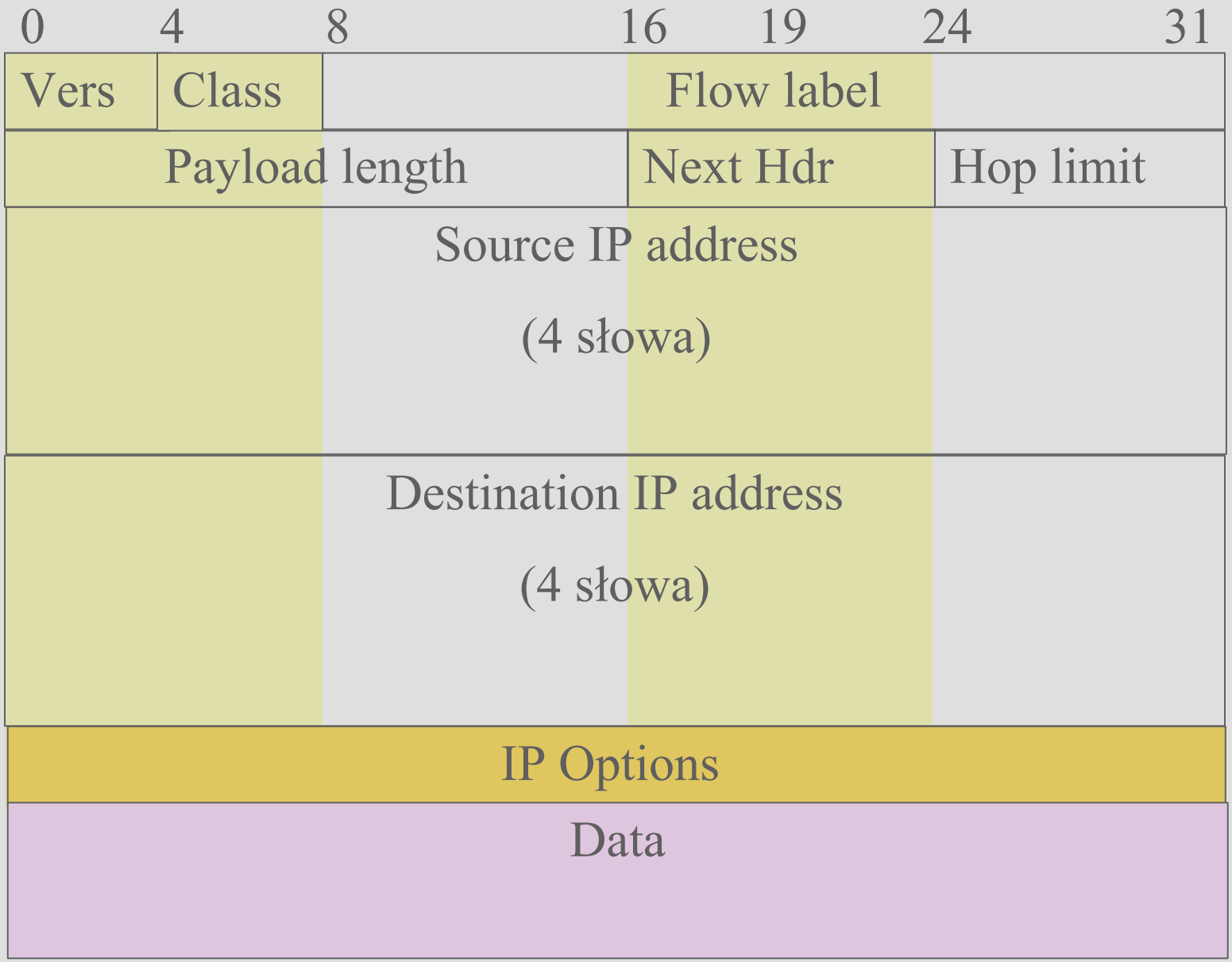
IPv6

- Ogólne założenia takie jak dla IPv4: warstwa 3, datagram, niezależny ruting pakietów
- Adres 128 bitów (3.4*10^38 adresów)
- Integracja IPsec w standardzie
- IPv6 funkcjonuje “równolegle” do sieci IPv4, dopuszczone jest tunelowanie, są to jednak niezależne protokoły
- **Inne cechy IPV6:**
  - Prostsza struktura nagłówka
  - Brak fragmentacji (zazwyczaj)
  - “jumbogramy”, do 4294967295 (2^32 - 1) oktetów
  - Typy transmisji:
    - Unicast : 1-do-1
    - Anycast : 1-do-sąsiednich
    - Multicast : 1-do-wielu

IPv6

- Adres IPv6:
  - adres: `2001:0db8:85a3:0000:0000:8a2e:0370:7334`
  - 64 bity adres sieci; 64 bity adres interfejsu
  - skracanie: `fe80:0000:0000:0000:0202:b3ff:fe1e:8329 ->`
    `fe80:0:0:0:202:b3ff:fe1e:8329`
    `fe80:0:0:0:202:b3ff:fe1e:8329 ->`
    `fe80::202:b3ff:fe1e:8329`
- Praktyka:
  - IPv6 zaimplementowany w większości systemów operacyjnych desktop/server,
  - wiele urządzeń, np. sprzęt do użytku domowego do tej pory jednak nie obsługuje IPv6,
  - Nie wszędzie odpowiednio skonfigurowana infrastruktura transmisyjna.

IPV6 - nagłówek



Fragmentacja IP

- Maksymalny rozmiar datagramu IPv4 – w teorii (c.a. 64 kB), w praktyce ...
- Fragmentacja (podział datagramu IP) ważna z punktu widzenia aplikacji.
- Za duży (co to zn. “za duży?) datagram jest dzielony przez ruter na mniejsze datagramy - “fragmenty”, i ...
  - proces ten może się powtarzać.
- Fragmenty identyfikowane są poprzez identyczną wartość pola “identification” nagłówka IP.
- Fragmenty przesyłane są oddzielnie.
- Fragmenty są łączone dopiero przez odbiorcę.
- Zgubienie fragmentu = zgubienie datagramu.
- Konkluzja: uwaga na rozmiar datagramu w prot. datagramowych! (UDP, <=576B gwarantuje brak fragmentacji; maks. ~1500B - Ethernet); dla TCP dobór rozmiaru odbywa się automatycznie.

Warstwa Transportowa

Warstwa transportowa

- Warstwa transportowa odpowiada za dostarczenie danych pomiędzy programami działającymi na różnych hostach (od procesu do procesu)
- Dwa protokoły warstwy 4:
  - UDP - User Datagram Protocol
  - TCP - Transmission Control Protocol
- UDP, przykladowe zastosowanie: **TFTP** (prosty transfer plików, np. bootowanie systemu lub upload firmware-u); **DNS**, **RPC, SNMP** (zarządzanie hostami i sieciami), media streaming
- TCP - większość protokołów aplikacyjnych wymagających zestawienia sesji lub transmisji większej ilości danych: **HTTP, ESMTP, POP3, IMAP4, FTP, SSH, wiele innych**

Protokół UDP

- Minimalna “nadbudowa” nad IP, *RFC 768*
- Nagłówek:

`Source Port`	`16 bit`
`Destination Port`	`16 bit`
`Length`	`16 bit` w bajtach
`UDP hdr. checksum`	`16 bit` udp hdr + IP addr, length

- **Port** - identyfikuje zdalną i lokalną aplikację
- Dzięki portom nadawca i odbiorca są identyfikowani jednoznacznie
- Jak wynika z samej konstrukcji nagłówka UDP nie oferuje nic w stosunku do IP prócz dostarczenia danych do aplikacji

Porty

Wykorzystywane w UDP i TCP

Liczba 16-o bitowa, network order (big endian)

Zakres:

0	nielegalny
1 - 1023	zarezerwowane dla procesów usługowych: “*well known ports*” ("*system ports"*), przypisane przez IANA
>= 1024	“efemeryczne” i serwery testowe
ale:	
1024 – 49151	“*Registered ports*” (usługi znane, opcjonalnie dostępne)

API: **`ntohs(), htons()`**

http://www.iana.org/assignments/port-numbers

Asocjacje

- Asocjacja jednoznacznie określa dwa komunikujące się procesy:

  $\{prot, Adres_{lokalny}, Port_{lokalny}, Adres_{zdalny}, Port_{zdalny}\}$

- Asocjacja jest unikalna w skali Internetu
- Półasocjacja:
  - $\{prot, Adres, Port\}$
  - określa punkt końcowy komunikacji gotowy do przyjecia lub wysłania danych (gniazdo)

- Przy omawianiu TCP zobaczymy jak przekształcanie pół-asocjacji w asocjację zapewnia unikalność powstałej asocjacji
- Asocjacja nie musi być związana z trwałym połączeniem TCP

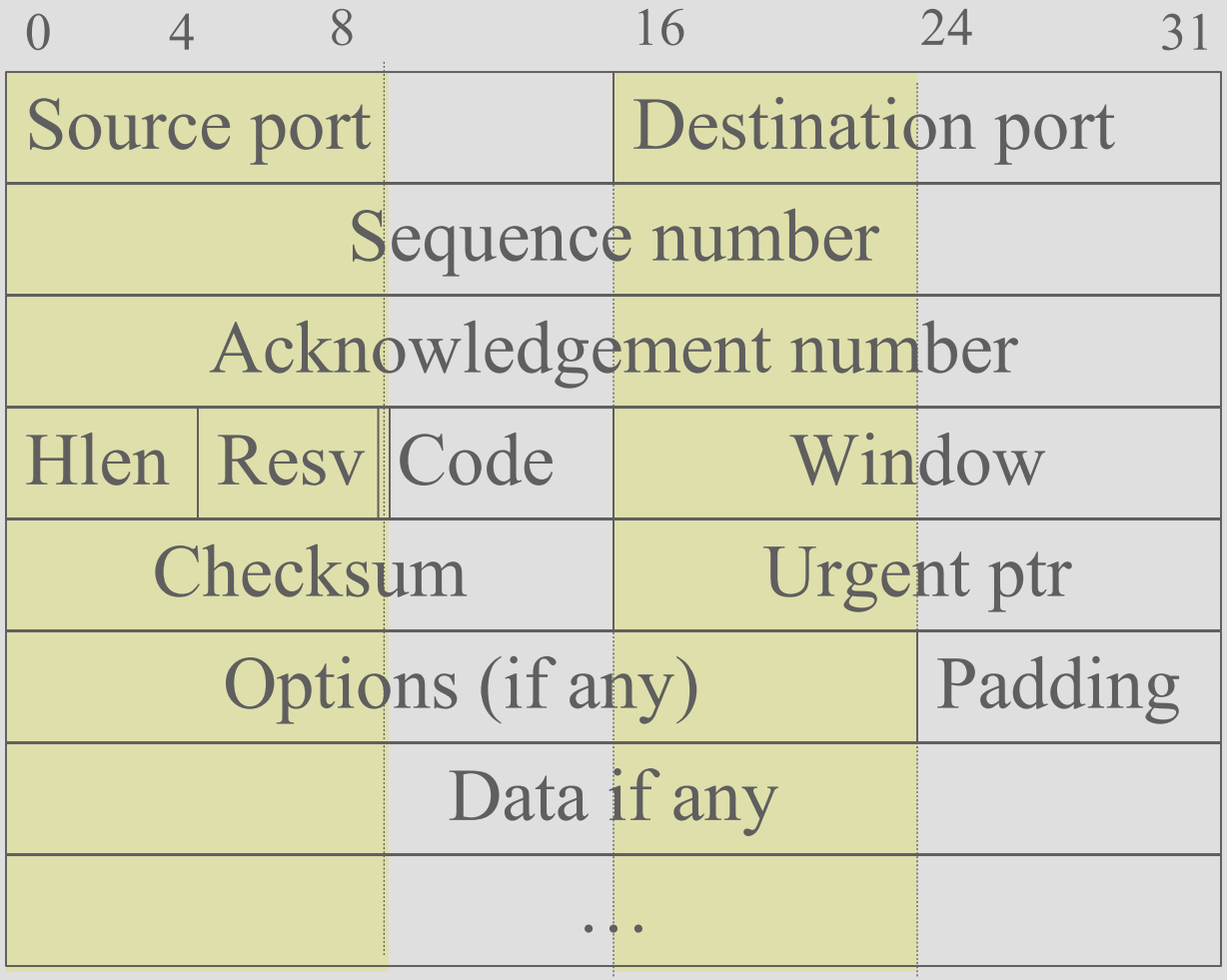
Protokół transportowy TCP

- Protokół sekwencyjny, niezawodny, dupleksowy. Transmitowany jest strumień bajtów - użytkownik nie ma dostępu do abstrakcji “pakietu”, ***RFC 768, 1122***
- Nawiązanie połączenia jest asymetryczne (model klient - serwer) - **Uwaga**: sama transmisja danych odbywa się w pełni symetrycznie - nie ma strony wyróżnionej
- Podobnie jak UDP identyfikuje proces poprzez 16-o bitowy numer portu
- Zapewnia sterowanie przepływem, tj. dopasowanie szybkości transmisji źródla i odbiorcy danych
- Zapewnia dodatkowo transmisję danych wysokopriorytetowych (OOB)
- Uwaga: Przestrzenie portów UDP i TCP są oddzielne - patrz asocjacja

Protokół transportowy TCP

- TCP zbudowany jest na warstwie IP
- Protokół określa dokładnie nawiązania połączenia “3 way handshake” oraz kilka trybów jego zamknięcia
- TCP należy do rodziny protokołów “z przesuwnym oknem”:
    - Stosowane jest obustronne potwierdzanie bajtów w strumieniu (nie pakietów)
    - Brak potwierdzenia skutkuje retransmisją ***segmentu*** (do skutku)
    - Dla każdego wysłanego i niepotwierdzonego segmentu musi być utrzymany licznik czasu
    - Dostarczenie n-tego bajtu oznacza, że wszystkie poprzednie zostały dostarczone i są poprawne

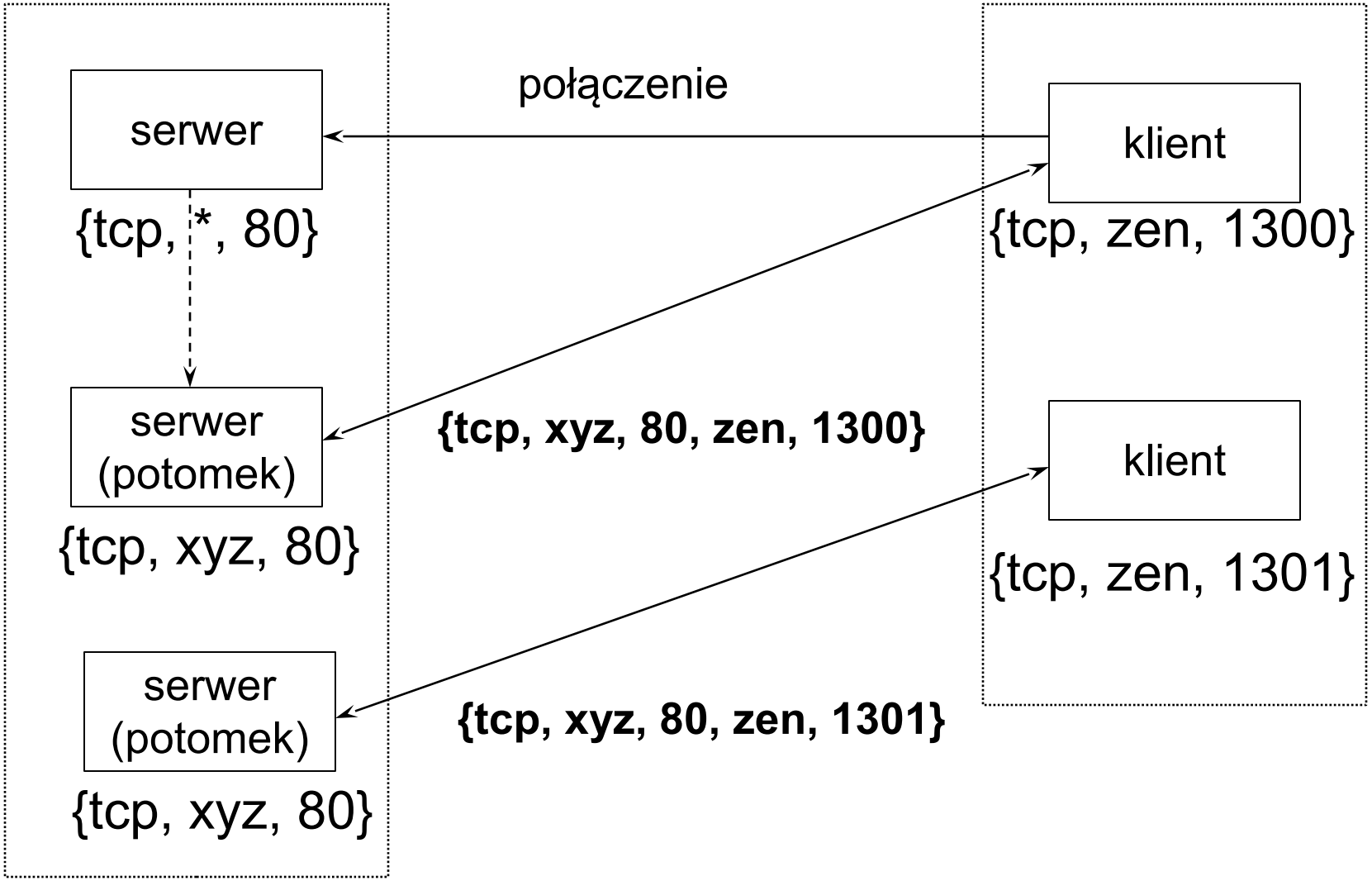
Nagłówek TCP - przypomnienie



Model klient - serwer

- Serwer - otwarcie pasywne gniazda - oczekiwanie na połączenie
- Klient - otwarcie aktywne - połączenie z serwerem
- W jaki sposób serwer obsługuje wielu klientów?
  - Unikalność asocjacji (połączonego gniazda)
  - Porty efemeryczne klienta przyznawane automatycznie w czasie nawiązywania połączenia
  - Serwery współbieżne i iteracyjne

Model klient - serwer



Typy serwerów

	Iteracyjny	Współbieżny
UDP	Typowe: np.DNS	Rzadkie: np. TFTP
TCP	Rzadkie: głównie prot. testowe	Typowe: np. FTP. HTTP (WWW), SMTP (e-mail), telnet, ...

Serwis DNS

- Tłumaczenie adresów symbolicznych: takich jak: “www.ii.pw.edu.pl” na adresy IP
- Hierarchiczna struktura adresowania w DNS
- Odpowiadająca jej hierarchia serwerów
- Pojęcie strefy
- Pojęcie "root serwera"
- Biblioteka resolver-a

DNS - prehistoria

- do 1970 - używano adresów numerycznych
- 1971-72 wprowadzono adresy symboliczne:
  - jeden plik “hosts” na wszystkich komputerach
  - propagowany na wszystkie maszyny
- 1980 - to rozwiązanie przestało się sprawdzać
- 1981 - początek prac nad DNS (David Mills)
- Rozwój standardu DNS - *RFC 882, 883* (*1034, 1035*), podstawowe pojęcia:
  - ***“authority”***
  - ***“delegation”***

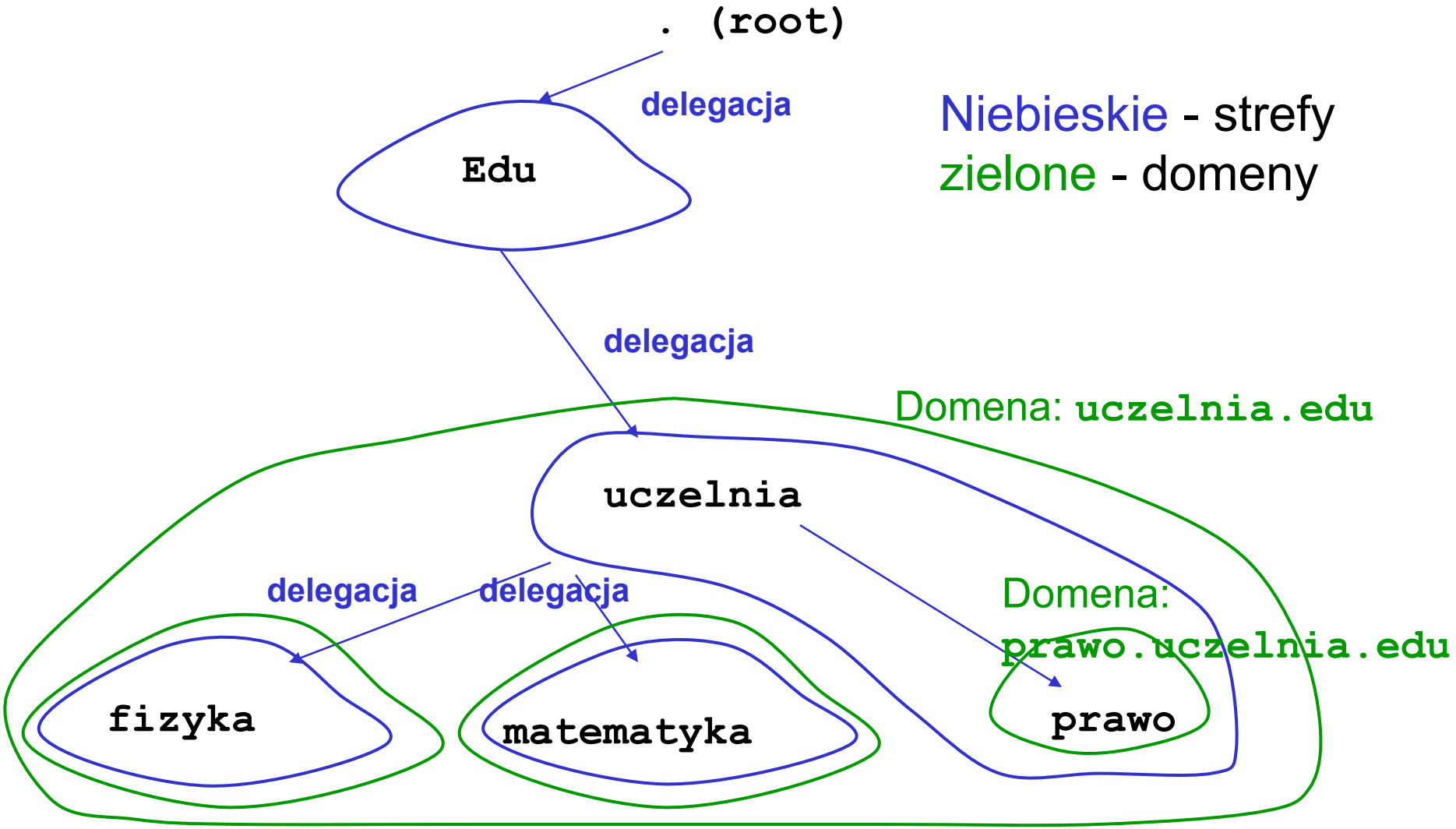
DNS Authority

- Baza danych DNS ma postać drzewa
- Każde poddrzewo to ***poddomena (subdomain)***
- Nazwy w (pod)domenie muszą być różne, co zapewnia unikalność (nie może być więcej niż jednej poddomeny lub hosta o tej samej nazwie)
- Wewnętrzny węzeł domeny obsługiwany przez niezależny serwer DNS to ***strefa****, "zone"*
    - *host:* bolek.ii.pw.edu.pl*:*
    - strefy: *pl*, . *edu.pl*, and .*pw.edu.pl*
- Każda strefa jest upoważniona (authority) do udzielania autorytatywnych odpowiedzi dotyczących jej zawartości
- **Uwaga**: hosty należące do domeny nie muszą być w jakikolwiek sposób powiązane w zakresie adresów IP (każdy może być w innej sieci)

Delegacja strefy DNS

- Administratorzy strefy edu.*pl* nie chcą i nie mogą przechowywać adresów wszystkich hostów z tej strefy
- *delegują* uprawnienia dla podstref do serwerów je obsługujących, np.: dla pw.edu.pl serwerowi obsługującemu PW.
- Podobnie, w ramach pw.edu.pl istnieją delegacje, np. dla strefy ii.pw.edu.pl
- Domena a strefa:
  - domenę łatwo zidentyfikować patrząc na drzewo nazw
  - aby zidentyfikować strefę musimy znać strukturę delegacji

Domeny i strefy



Niebieskie - strefy
zielone - domeny

Rekordy DNS

- Nazwy domen:
  - –FQDN: sklejenie kolejnych nazw, w kierunku "od liścia do korzenia", separator - “.”.
  - –Nazwa domeny zawsze odnosi się do niej samej i całej zawartości domeny
  - –Niezależne od wielkości znaków
  - –Składnik może mieć do 63 znaków
  - –Pełna nazwa domenowa - do 255 znaków
  - –Dozwolone znaki: a-z,A-Z,0-9, -

Serwery DNS

- Serwer udziela odpowiedzi dot. translacji nazw - "name resolution"
- Serwer może:
  - "Znać" bezpośrednią odpowiedź na pytanie - w przypadku gdy żądany adres znajduje się w jego strefie
  - "Znać" pośrednią odpowiedź na pytanie - tj. delegować zapytanie do innego serwera
- Zapytania:
  - rekurencyjne (prosty resolver) - serwer odpowie lub odpyta pod-serwery i zwrócić ostateczną odpowiedź, być może odpytywanie będzie odbywać się rekurencyjnie (zostanie zaangażowanych kilka kolejnych serwerów)
  - iteracyjne (złożony resolver) - serwer odpowie lub odeśle klienta do "najbliższego" pod serwera
  - **Uwaga:** krytyczna rola serwerów obsługujących domenę"." (root)

Rekordy DNS

Rekord **SOA** (Start of Authority) - zawiera atrybuty strefy

```
movie.edu. IN SOA terminator.movie.edu.
al.robocop.movie.edu. (...)
```

Rekord **NS** - opisuje serwery nazw

```
movie.edu. IN NS terminator.movie.edu
```

Rekord **A** - mapuje nazwę na adres IP

```
misery.movie.edu. IN A 192.253.253.2
```

Rekord **PTR** - mapuje adres IP na nazwę

```
2.253.253.192.in-addr.arpa. IN PTR misery.movie.edu.
```

Rekord **CNAME** - nazwy kanoniczne (aliasy)

```
king.movie.edu, IN CNAME misery.movie.edu
```

Serwery DNS, Resolver

- Tematy (prawie) nieomawiane, warto zwrócić uwagę (patrz też SKOM):
  - Translacja odwrotna
  - Opis strefy
  - Typy serwerów DNS i transfery stref
  - Konfiguracja Serwerów – bind, named
  - Serwis Whois
  - nslookup
  - Zaawansowane: root serwery, obsługa wielu sieci, bezpieczeństwo i kontrola dostępu, automatyczna aktualizacja
- Resolver - omawiany przy okazji BSD socket API