

## Sieci komputerowe IPv6

dr inż. Piotr Kowalski

Katedra Automatyki  
i Techniki Informatycznych

## Plan i problematyka wykładu

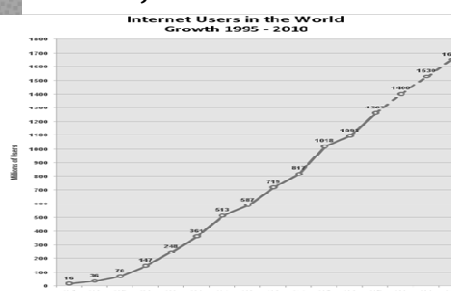
1. Uzasadnienie dla rozwoju protokołu IPv6 i próby „ratowania” idei IPv6
2. Główne aspekty funkcjonowania IPv6 i jego współdziałania ze starszymi protokołami
  - Adresowanie węzłów (z wszystkimi aspektami – typami adresów, autokonfiguracją itp.)
  - Datagram IPv6 (a w szczególności jego nagłówki)
  - Współpraca węzłów IPv4 i IPv6

Sieci komputerowe

## Dlaczego IPv6?

- ✦ Wykładniczy wzrost liczby węzłów sieci Internet jest ograniczany przez 32-bitową przestrzeń adresową protokołu IP w wersji 4.
- ✦ Zarządzanie przestrzenią adresową IPv4 staje się obecnie trudnym zadaniem.
- ✦ IPv4 nie implementuje skutecznych metod priorytetowego przesyłania informacji jak i multicastingu które we współczesnej sieci Internet – pełnej uwspólnionych strumieni audio-video – są wręcz niezbędne
- ✦ Bo IPv4 został opracowany w czasach gdy bezpieczeństwo przesyłu informacji i sieci bezprzewodowe były przedmiotem rozważań jedynie teoretycznych. Routing w sieci Internet stał się także bardziej złożony niż kiedyś.

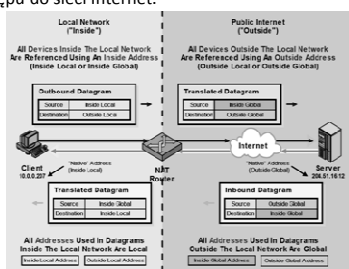
## Rozwój sieci Internet



W Polsce w 2009 – 20mln użytkowników.  
To ponad 6 razy więcej niż w roku 2000 (!)

## Przykład zatykania „dziur” w funkcjonalności IPv4 - NAT

NAT (ang. Network Address Translation) to technika pozwalająca na tworzenie wewnętrznych sieci prywatnych i zapewnienie węzłom tej sieci dostępu do sieci Internet.



## IPv6 – wprowadzenie

- ✦ IPv6 inaczej IPng (ang. IP Next Generation) jest wciąż rozwijanym protokołem intersieci którego zręby definiują dokumenty RFC z lat 1998-2003.
- ✦ Główne cechy
  - 128-bitowe adresy, z hierarchicznym podziałem ich przestrzeni
  - Rozwinięte mechanizmy transmisji grupowej
  - Sprawna autokonfiguracja hostów
  - Nowy format datagramów, z rozszerzalnymi nagłówkami dla różnych typów informacji
  - Rozwinięte mechanizmy QoS (ang. quality of service) i bezpieczeństwa danych
  - Zmodernizowane techniki fragmentacji i routingu
  - Zgodność (współdziałanie) z sieciami pracującymi z IPv4.

## Adresowanie – typy adresów

IP w wersji 6 definiuje następujące typy adresów:

- ✚ **Adres jednostkowy** (ang. unicast address) – taki adres odpowiada pojedynczemu węzłowi sieci
- ✚ **Adres rozsyłania grupowego** (ang. multicast address) – taki adres odpowiada zbiorowi węzłów znajdujących się być może w różnych miejscach (członkostwo można zmieniać), datagram przesyłany pod ten adres jest dostarczany do każdego członka grupy
- ✚ **Adres grona** (ang. anycast address) – taki adres odpowiada zbiorowi komputerów o wspólnym prefiksie adresu (zwykle w jednej lokalizacji). Datagram dostarczany jest do jednego węzła, do którego np. ścieżka jest najkrótsza.

## Zapis adresu - możliwości

Binary	1000000001011011001011011001101110111011100001010000000000000000															
	000000000000000000001111110001010111101010011001100100000111111111111															
Dotted Decimal	128	91	45	157	220	40	0	0	0	0	252	87	212	200	31	255
Hexadecimal	0	32	64	96	128											
Straight Hex	805B	2D9D	DC28	0000	0000	FC57	D4C8	1FFF								
Leading-Zero Suppressed	805B	2D9D	DC28	0	0	FC57	D4C8	1FFF								
Zero-Compressed	805B	2D9D	DC28	::		FC57	D4C8	1FFF								
Mixed Notation	805B	2D9D	DC28	::		FC57	212	200	31	255						

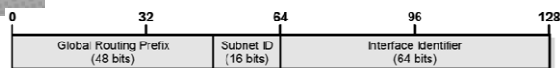
## Zapis adresu w praktyce

- ✚ Adresy IPv6 zapisywane są w notacji szesnastkowej  
805B:2D9D:DC28:0000:0000:FC57:D4C8:1FFF
  - ✚ Zera można pominać:  
805B:2D9D:DC28::0000:FC57:D4C8:1FFF  
(symbol :: może występować tylko raz i zastępuje zerowe pola o odpowiedniej długości – wylczanej na podstawie łącznej długości adresu IP)
- Przykłady:
- 0:0:0:0:0:0:1 → ::1
  - 0:0:0:0:0:0:0 → ::
  - 0:0:0:0:212:200:31:255 (notacja mieszana) → ::212:200:31:255 (to nie jest adres IPv4)

## Podział przestrzeni adresów

- ✚ Paradoksalnie w IPv6 powrócono do koncepcji podziału przestrzeni adresów podobnej do klas zIPv4.
- ✚ W IPv6 występują prefiksy adresów o zmiennej długości (pierwotnie od 3 do 10 bitów, zmienne) które określają grupę adresów, przykładowo:
  - 0000 0000 to prefiks adresów specjalnego przeznaczenia takich jak: adres pętli zwrotnej, adres nieokreślony, adres IPv4
  - 1111 1111 to prefiks adresów rozsyłania grupowego, zatem każdy adres zaczynający się od FF jest adresem typu multicast
  - 001 to prefiks adresów jednostkowych – czyli tych najbardziej nas interesujących

## Format adresu jednostkowego



Pierwsze 48 bitów adresu to prefiks sieci pozwalający na efektywne trasowanie datagramu w sieci IP.

Druga część adresu to identyfikator podsieci – pozwala on na podzielenie sieci o danym prefiksie na maksymalnie 65 536 podsieci.

Trzecia część adresu to 64 bitowy identyfikator interfejsu sieciowego danego węzła. Adres ten jest unikalny (!) dla interfejsu. Zatem to tożsamościowe mapowanie adresu fizycznego na część adresu IP. Format używanego w tym celu 64-bitowego adresu sprzętowego to zmodyfikowany EUI-64 (24 bity – producent, 40 bitów – ID interfejsu, 7 bit na 1).

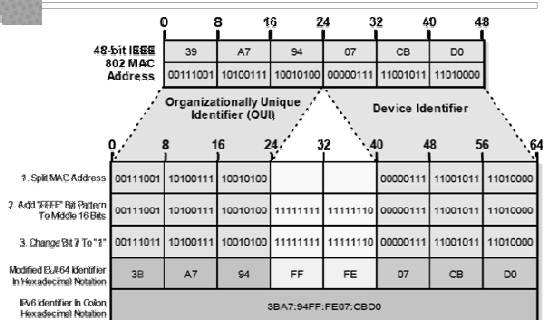
## Konwersja MAC → EUI-64

Większość urządzeń sieciowych używa w dalszym ciągu adresu fizycznego MAC. W celu konwersji takiego adresu do postaci adresu 64-bitowego należy przedsięwziąć następujące kroki:

- Pierwsze 24 bity adresu MAC przyjąć jako pierwsze 24 bity adresu EUI-64,
- Ostatnie 24 bity adresu MAC przyjąć jako ostatnie 24 bity adresu EUI-64,
- Pozostałe 16 środkowych bitów należy ustalić jako 11111111 11111110 (FFFEh)

Uzyskujemy wtedy adres EUI-64. Adres ten po ustaleniu 7 bitu na 1 stanowi zmodyfikowany EUI-64 czyli identyfikator interfejsu sieciowego (ostatnie 64 bity adresu IPv6).

## Przykład konwersji



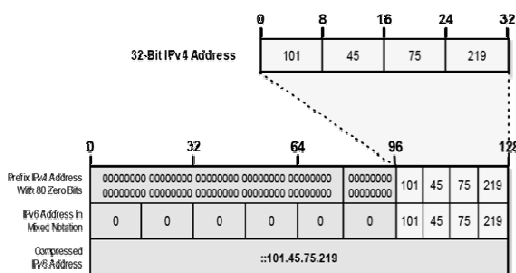
## Adresy specjalnego przeznaczenia

- Grupa adresów zarezerwowanych – prefiks 0000 0000 (00h)
- Adresy prywatne (używane do komunikacji w sieci lokalnej) – prefiks 1111 1110 1 (FE [8-F]h)
- Adres pętli zwrotnej – 0:0:0:0:0:1
- Adres nieokreślony – używany przez urządzenia które adresu IP przypisanego nie mają i chcą go otrzymać od odpowiedniego węzła w sieci – 0:0:0:0:0:0:1

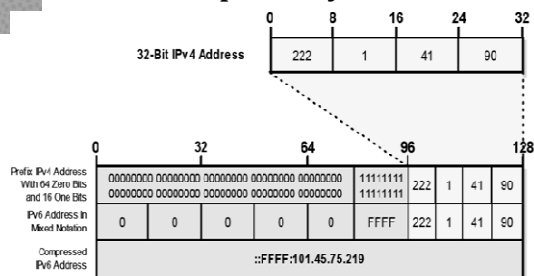
## Zgodność adresowania IPv6 a IPv4

- Współczesny Internet jest rozproszonym systemem składającym się z węzłów wspierających jedynie protokół IP w wersji 4, a także tych, które poza tym protokołem umożliwiają także komunikację z użyciem IPv6.
- Istnieje zatem potrzeba zapisu adresu IPv4 w postaci 128-bitowego adresu IPv6.
- Zapis ten przyjmuje różną postać:
  - dla węzłów z obsługą IPv6 stosujemy adres wbudowany (ang. IPv4-Compatible Embedded Address)
  - węzłów bez obsługi IPv6 stosujemy adres zmapowany (ang. IPv4-Mapped Address)

## Adres wbudowany



## Adres zmapowany



Sieci komputerowe

## Adresy rozsyłania grupowego

- Adresy rozsyłania grupowego cechuje prefiks 1111 1111
- Po prefiksie:
  - 4-bitowe pole flag
  - 4-bitowe pole zakresu (ang. scope) np. 1 dziesiętnie to adres używany w zakresie węzła, 2 – łącza, 5 – sieci, 8 – organizacji, 14 – całej sieci Internet
  - 112 bitów identyfikujących grupę
- W protokole zdefiniowano także typowe adresy rozsyłania grupowego:
  - FF:0x:0:0:0:0:0:1 – wszystkie węzły
  - FF:0x:0:0:0:0:0:2 – wszystkie routery
- IPv6 definiuje także specjalne dodatkowe adresy rozsyłania grupowego w sieci lokalnej (ang. solicited node address)

## Autokonfiguracja węzłów IPv6

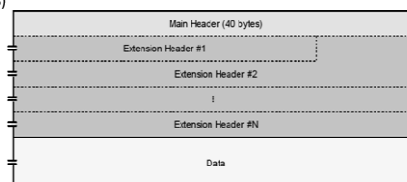
IPv6 używa tzw. bezstanowej autokonfiguracji węzła (tj. przypisania mu adresu IP), kolejne kroki tej procedury to:

- Przypisanie węzłowi adresu prywatnego (odpowiedni prefiks tj. 1111 1110 10 + 54 zera + zmodyfikowany EUI-64)
- Test jednoznaczności adresu (tj. czy któryś z węzłów w sieci nie używa identycznego adresu) z użyciem protokołu wykrywania sąsiadów (ang. IPv6 Neighbour Discovery), gdy jest konflikt generujemy nowy adres, gdy nie ma – możemy go używać do komunikacji w sieci lokalnej
- Kontakt z najbliższym routerem który informuje czy węzeł może użyć bezstanowej konfiguracji tj. do prefiksu sieci dodać swój identyfikator czy też użyć DHCP dla konfiguracji adresu

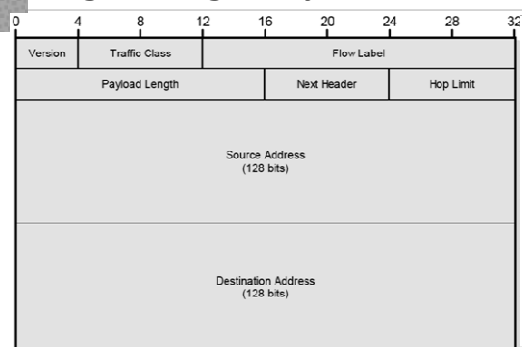
## Datagram IPv6

Datagram protokołu IPv6 w sposób oczywisty różni się od datagramu IP w wersji 4. Podstawowe jego cechy w zestawieniu z IPv4 to:

- „wielonagłówkowość” (nagłówek główny + nagłówki dodatkowe)
- zmniejszenie ilości pól (np. brak długości nagłówka – stała wartość i sumy kontrolnej), zmiana nazw itp.
- lepsze wsparcie dla mechanizmów priorytetowego przesyłania danych (QoS)



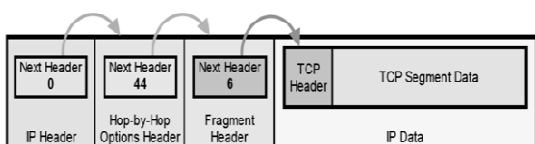
## Nagłówek główny



## Nagłówek główny – pola

- ⚡ Wersja [4 bity] – binarnie 0110, czyli że 6
- ⚡ Priorytet [8 bitów] – pole klasy priorytetu usług w formacie DS (ang. Differentiated Services)
- ⚡ Etykieta potoku [20 bitów] – pole wykorzystywane również w ramach zapewnienia QoS
- ⚡ Długość zawartości [16 bitów] – w bajtach, nie wliczając nagłówka głównego
- ⚡ Następny nagłówek [8 bitów] – określa etykietę dla danych następujących po nagłówku, to pole podobne do TYP w IPv4, przy czym może być tu albo od razu typ przesyłanego protokołu (gdy nie ma dodatkowego nagłówka albo identyfikator nagłówka następującego po głównym)
- ⚡ Liczba etapów [8 bitów] – czyli TTL z IPv4

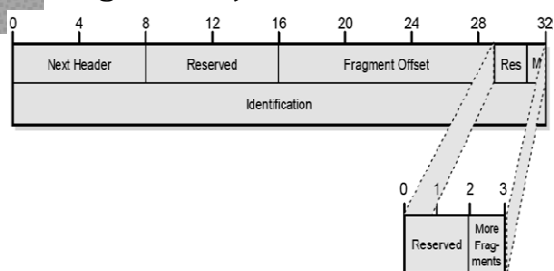
## Dodatkowe nagłówki w IPv6 – jak to działa?



## Dodatkowe nagłówki - typy

Nast. Nagł.	Nazwa	Długość	Opis
0	Hop-by-hop options	Zmienna	Opcje do użytku wszystkich węzłów na trasie
43	Routing	Zmienna	Możliwość zdefiniowania trasy dla pakietu
44	Fragment	8 bajtów	Gdy datagram stanowi fragment większej porcji danych
50	Encapsulating Security Payload	Zmienna	Dane zaszyfrowane (IPSEC)
51	Authentication Header	Zmienna	Uwierzytelnienie danych (IPSEC)
60	Destination Options	Zmienna	Opcje dla użytku adresata

## Przykład: nagłówek fragmentacji



## Płynne przejście z IPv4 do IPv6

Aby zapewnić w miarę płynne przejście do nowej wersji protokołu IP i współpracę węzłów IPv6 z tymi wspierającymi jedynie IPv4 (komunikacja w drugą stronę nie jest formalnie możliwa) stosuje się następujące mechanizmy:

- ✦ Wsparcie dla dwóch warstw IP w różnych wersjach
- ✦ Translacja adresów poprzez w/w urządzenia
- ✦ Kapsułkowanie pakietów IPv6 w pakietach IP w wersji 4 wędrujących przez sieć nie wspierającą nowej wersji protokołu

## Czego nie omawiamy...

- ✦ Protokołu ICMP w wersji 6
- ✦ Protokołu wykrywania sąsiadów
- ✦ Szczegółów funkcjonowania mechanizmu QoS
- ✦ Implementacji bezpieczeństwa przesyłania danych w IPv6 (IPSEC)
- ✦ Zmian w routingu

...

Ale: pamiętajmy także o tym że protokół IPv6 ulega wciąż ciągłym zmianom...

**DZIĘKUJĘ ZA UWAGĘ!**