

## **Warstwa sieci**

### **Plan wykładu**

- Miejsce w modelu OSI/ISO
- Funkcje warstwy sieciowej
- Adresacja w warstwie sieciowej (IPv4)
- Protokół IPv4
- IPv6

## Warstwa sieci

- Warstwa sieci modelu OSI/ISO

warstwa aplikacji

warstwa prezentacji

warstwa sesji

warstwa transportowa

**warstwa sieci**

warstwa łącza danych

warstwa fizyczna

- Jej zadaniem jest **dostarczenie logicznej adresacji**. Warstwa ta odpowiada także za **znalezienie najlepszej drogi łączącej dwa hosty**, które mogą się znajdować w oddzielnych z punktu widzenia warstwy łączy danych sieciach.
- Jednym z protokołów pracujących w warstwie sieciowej jest **Internet Protocol (IP)** (inne: IPX, AppleTalk, NetBEUI).

## Po co adresacja w warstwie sieci ?

- Mamy adresy Ethernet — unikalne w skali światowej, ale:
  - Istnieją **różne** standardy komunikacji, nie tylko Ethernet
  - Adresy Ethernet mają **PŁASKĄ** przestrzeń adresową
    - nieskalowalne
    - brak powiązania z geograficznym rozmieszczeniem

### Adresacja IP

- Jest niezależna od warstwy łącza danych
- Jest **HIERARCHICZNA**
- Powiązana z położeniem geograficznym adresowanych urządzeń, dzięki temu można znaleźć łatwo drogę do odbiorcy
- Jest skalowalna
- Podobieństwo do numerów telefonicznych  
+48 12 617 3982 34

### Adresy IPv4

- Najbardziej popularna adresacja
- Adresy mają 32 bity podzielone na dwie części: sieci i hosta

10000110 10101100 00111110 01000011
-------------------------------------



- Mniejsza przestrzeń adresowa (ok. 4,3mld) niż w Ethernetie (140 737 488 355 326; ok. 140bln; ok. 65 tys. razy więcej) — kłopoty
  - Część niewykorzystana
  - Część zarezerwowana
  - Telefonia komórkowa (2.5G/3G/4G – GPRS/UMTS/LTE)

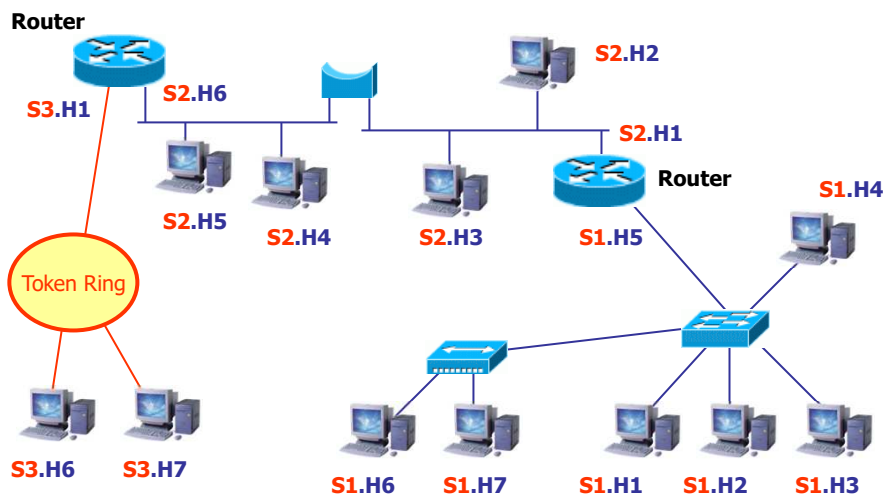
### Skąd można uzyskać adres IP?

- Ethernet
  - adres zaszyty na karcie sieciowej
- IP
  - W przypadku braku połączenia do sieci globalnej można nadawać dowolne adresy.
  - W przeciwnym przypadku:
    - numer sieci należy uzyskać od NIC (Network Information Center) lub od Internet Provider.
    - numery hostów przydzielane są według własnego uznania (lokalny administrator)

### Do czego przypisujemy adres IP?

- Adres IP nie jest powiązany z urządzeniem (komputer, drukarka itp.) **tylko z kartą sieciową (przyłączeniem do sieci)**. Host może mieć wiele kart sieciowych, a więc wiele adresów IP.
- Każda karta sieciowa komputera w sieci IP ma przypisany co najmniej 1 adres IP.
- Wszystkie hosty dołączone do tej samej, z punktu widzenia warstwy łącza danych, sieci mają **identyczny adres sieci**.
- Jeśli hosty są dołączone do różnych, z punktu widzenia warstwy łącza danych, sieci **muszą różnić się adresem sieci**.

## Adresy sieci i hosta



## Routery — podstawy



← Symbol

- Zadania:
  - Wyznaczają drogę pakietom
  - Pozwalają łączyć sieci o różnych standardach warstwy drugiej
  - Ograniczają domeny rozgłoszeniowe

### Notacja adresu

00000110 10000100 00000010 00000001

← 32 bity →

- Zapis binarny
  - 00000110 10000100 00000010 00000001
- Zapis szesnastkowy
  - 0x06840201
- Zapis dziesiętny
  - 109314561
- Zapis **kropkowo – dziesiętny**
  - 6.132.2.1 — dziesiętnie, każdy bajt oddzielnie -> każdy liczba z zakresu 0 – 255

### Zamiana liczb binarnych na dziesiętne — przypomnienie

- Zapis liczb dziesiętnych:

859235

$$\begin{array}{cccccc}
 8 & 5 & 9 & 2 & 3 & 5 \\
 8 \cdot 10^5 & + & 5 \cdot 10^4 & + & 9 \cdot 10^3 & + & 2 \cdot 10^2 & + & 3 \cdot 10^1 & + & 5 \cdot 10^0 \\
 800000 & + & 50000 & + & 9000 & + & 200 & + & 30 & + & 5 = 859235
 \end{array}$$

- Zapis liczb binarnych:

00101100

$$\begin{array}{cccccccc}
 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
 0 \cdot 2^7 & + & 0 \cdot 2^6 & + & 1 \cdot 2^5 & + & 0 \cdot 2^4 & + & 1 \cdot 2^3 & + & 1 \cdot 2^2 & + & 0 \cdot 2^1 & + & 0 \cdot 2^0 \\
 0 & + & 0 & + & 32 & + & 0 & + & 8 & + & 4 & + & 0 & + & 0 = 44
 \end{array}$$

## Zamiana liczb binarnych na dziesiętne – przypomnienie

- Zakres: bajt — 8 bitów:
  - 00000000 – 11111111 (binarnie)
  - 0 – 255 (dziesiętnie)

0	0	1	0	1	1	0	0									
$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$									
128	64	32	16	8	4	2	1									
0	+	0	+	32	+	0	+	8	+	4	+	0	+	0	=	44

## Zamiana liczb dziesiętnych na binarne – przypomnienie

	235	1	Zapisać liczbę 235
$(235-1) / 2 =$	117	1	w postaci binarnej
$(117-1) / 2 =$	58	0	
$(58-0) / 2 =$	29	1	
$(29-1) / 2 =$	14	0	Zapisujemy od dołu:
$(14-0) / 2 =$	7	1	
$(7-1) / 2 =$	3	1	235 = ...0011101011
$(3-1) / 2 =$	1	1	
$(1-1) / 2 =$	0	0	
$(0-0) / 2 =$	0	0	
	...		

### Zamiana liczb dziesiętnych na binarne — przypomnienie

			$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
			128	64	32	16	8	4	2	1
			x	x	x	x	x	x	x	x
235	$\geq$	128	1	x	x	x	x	x	x	x
235 - 128	(107)	$\geq$	1	1	x	x	x	x	x	x
107 - 64	(43)	$\geq$	1	1	1	x	x	x	x	x
43 - 32	(11)	$\geq$	1	1	1	0	x	x	x	x
11	$\geq$	8	1	1	1	0	1	x	x	x
11 - 8	(3)	$\geq$	1	1	1	0	1	0	x	x
3	$\geq$	2	1	1	1	0	1	0	1	x
3 - 2	(1)	$\geq$	1	1	1	0	1	0	1	1
235	$=$		1	1	1	0	1	0	1	1

### Zamiana liczb dziesiętnych na binarne — przypomnienie

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1
235	$\geq$	128					1xxxxxxx
235	$\geq$	128 + 64	(192)				11xxxxxx
235	$\geq$	192 + 32	(224)				111xxxxx
235	$\geq$	224 + 16	(240)				1110xxxx
235	$\geq$	224 + 8	(232)				11101xxx
235	$\geq$	232 + 4	(236)				111010xx
235	$\geq$	232 + 2	(234)				1110101x
235	$\geq$	234 + 1	(235)				11101011



## Przykłady

```

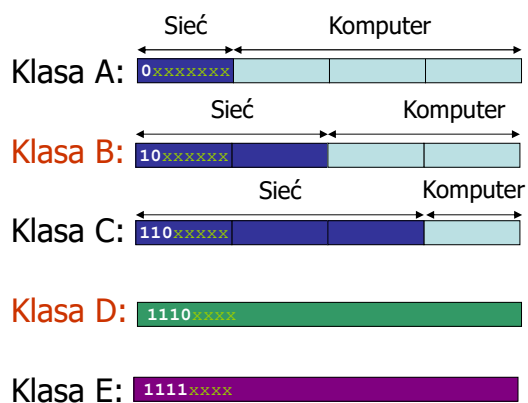
-----
-----
-----
-----
2 5.1 8 4.2 2 4. 5
1 0 0. 3 9.1 9 2. 8 4
2 0.2 3 4. 9 0.2 3 8
7 4.1 2 8. 6 5.2 0 0
-----

1 0 0 0 1 1 0 0 0 1 1 1 0 1 1 0 1 1 1 1 1 1 1 0 0 0 0 0 1 1 0
1 1 0 0 1 1 1 0 1 1 0 0 0 1 1 0 1 0 1 0 1 0 1 0 1 1 0 1 1 0 1
0 0 1 0 1 0 1 1 0 0 0 1 1 0 1 1 0 1 1 1 0 0 1 1 0 1 0 1 0 1 0 1
0 1 1 0 0 0 1 1 0 0 1 1 1 1 1 0 1 0 0 1 0 1 0 1 0 0 1 1 0 0 1 0
-----
-----
-----
0 0 0 1 1 0 0 1 1 0 1 1 1 0 0 0 0 1 1 1 0 0 0 0 0 0 0 0 0 1 0 1
0 1 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 0 0 0 0 0 1 0 1 0 1 0 0
0 0 0 1 0 1 0 0 0 1 1 1 0 1 0 1 0 0 1 0 1 1 0 1 0 1 1 1 0 1 1 0
0 1 0 0 1 0 1 0 1 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 1 1 0 0 1 0 0 0

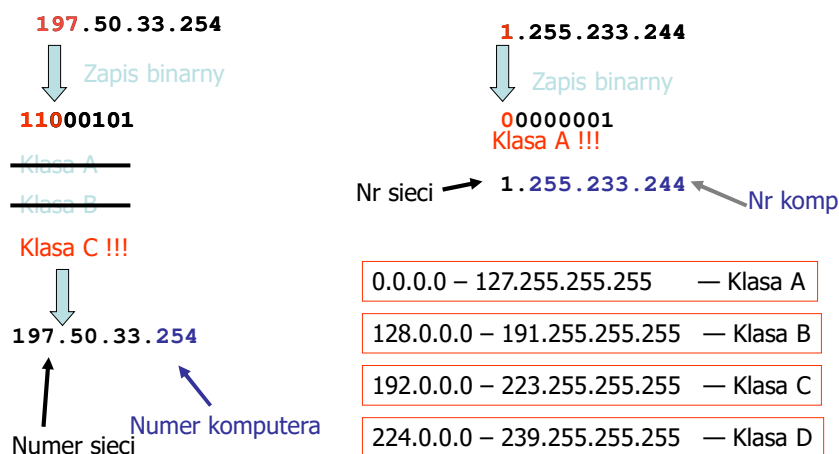
```

## Klasy adresowe

- Klasa A:  
126 sieci,  
ponad 16mln komp.
- Klasa B:  
ok. 16tys sieci,  
ok. 65tys komp
- Klasa C:  
ponad 2 mln sieci,  
254 komputery
- Klasa D:  
multicast
- Klasa E:  
zarezerwowana



## Wyznaczanie nr sieci i hosta



## Adresy specjalne

- **0.0.0.0** – ten komputer w tej sieci. Podawany jako adres źródłowy w trakcie uruchamiania komputera gdy nie zna on jeszcze swojego adresu IP.
- **0.x.y.z** – komputer x.y.z w tej sieci. Podawany w trakcie uruchamiania jako adres źródłowy w komputerze posiadającym niekompletne informacje.
- **x.0.0.0** – dowolny komputer w sieci x. Sieć x.
- **127.x.y.z** – adres 'loopback'. Pakiet wysłany na taki adres nie może zostać wysłany poza komputer. Pozwala aplikacjom pracującym na tym samym komputerze komunikować się poprzez stos TCP/IP.

### Adresy typu broadcast

- Mogą być podane tylko jako adres docelowy.
- Ograniczony broadcast
  - 255.255.255.255 – Oznacza wszystkie komputery w sieci lokalnej. Nigdy nie są przekazywane przez routery.
- Broadcast skierowany
  - Adres, w którym część adresu komputera składa się z samych jedynek, zaś część sieci jest określona. Oznacza wszystkie komputery w danej sieci. Np.: 130.1.255.255 – wszystkie komputery w sieci 130.1.0.0

### Adresy IP specjalnego przeznaczenia

Adres IP		Może się pojawić jako	
sieć	host	źródło?	przeznaczenie?
0	0	OK	nigdy
0	hostId	OK	nigdy
127	cokolwiek	OK	OK
-1	-1	nigdy	OK
netId	-1	nigdy	OK

## Tworzenie podsieci – cele

- Zbyt dużo komputerów w klasach A ( $2^{24} - 2$ ) i B ( $2^{16} - 2$ )
- Daje elastyczność administratorowi (+48 12 617 3982)
- Pozwala ukryć szczegóły budowy sieci przed routerami zewnętrznymi
- Zmniejszone są domeny rozgłoszeniowe
- Mogą istnieć różne rodzaje sieci lokalnych, które trzeba jakoś połączyć
- Liczba hostów w sieci może być ograniczona
- Lepsze podsieci w klasie B niż wiele sieci klasy C, ponieważ redukuje to rozmiar tablic rutowania

Przykład: Adres IP klasy B: 149.156.10.18

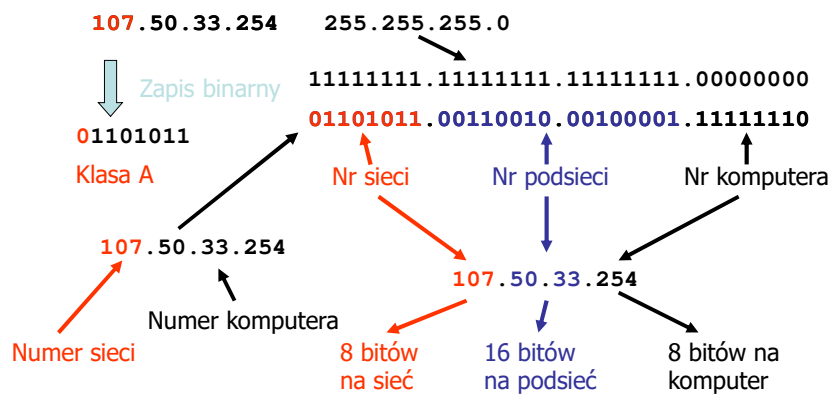
Adres sieci 149.156	Adres komputera 10.18	
Adres sieci 149.156	Adres podsieci 10	Adres komp. 18

## Maska podsieci

- Ma 4 bajty (32 bity) – identycznie jak adres IP
- Zawiera bity jedynek dla części będącej adresem sieci i bity zer dla części, która jest adresem komputera
- Musi być ciągła (jedyneki, później zera).
- Zapis: szesnastkowy, kropkowo-dziesiętny lub liczba bitów znaczących

	16 bitów	8 bitów	8 bitów	
Klasa B:	Adres sieci	Podsieć	Host	0xFFFFF00 lub 255.255.255.0 lub /24
Maska:	1111111111111111	11111111	00000000	
	16 bitów	10 bitów	6 bitów	
Klasa B:	Adres sieci	Podsieć	Host	0xFFFFFC0 lub 255.255.255.192 lub /26
Maska:	1111111111111111	1111111111	000000	

### Numer sieci, podsieci i hosta



### Adresy IP specjalnego przeznaczenia

- Broadcast skierowany do podsieci
  - Oznacza wszystkie komputery w danej podsieci.  
Np.: **10.20.30.255/24** — wszystkie komputery w sieci 10 i podsieci 20.30

### Zarezerwowane adresy IP

- Takie, które nie mogą być wykorzystywane do adresacji hostów
  - adresy broadcast np.
    - 10.255.255.255
    - 10.20.30.255/255.255.255.0
  - adresy sieci np.
    - 10.0.0.0
    - 10.20.30.0/255.255.255.0

} Liczba dopuszczalnych hostów zmniejszona o 1

} Liczba dopuszczalnych hostów zmniejszona o 1

### Prywatne adresy IP (v4)

- Mogą być wykorzystane tylko w sieciach lokalnych (nie działają w publicznej części Internetu).
  - **10.0.0.0 - 10.255.255.255** - dla sieci prywatnych klasy A (maska: 255.0.0.0)
  - **172.16.0.0 - 172.31.255.255** - dla sieci prywatnych klasy B (maska: 255.255.0.0)
  - **192.168.0.0 - 192.168.255.255** - dla sieci prywatnych klasy C (maska: 255.255.255.0)
- Technika NAT, PAT umożliwia połączenie z publiczną siecią Internet.

### **Możliwe i użyteczne adresy IP dla hostów**

- W sieci klasy C istnieje możliwość nadania 256 ( $2^8$ ) adresów IP
- Tylko 254 ( $2^8-2$ ) adresy są użyteczne
  - jeden zabiera nam numer 0 (00000000) — jest to adres całej sieci
  - jeden zabiera nam numer 255 (11111111) — jest to adres wszystkich komputerów w tej sieci

### **Minimalny i maksymalny rozmiar maski**

- Bity na podsieć 'pożyczają się' z części dla hosta
  - klasa A: N.H.H.H -> minimalna maska 255.0.0.0
  - klasa B: N.N.H.H -> minimalna maska 255.255.0.0
  - klasa C: N.N.N.H -> minimalna maska 255.255.255.0
  - maska minimalna nazywa się **maską domyślną**
- Adres hosta nie może składać się z samych zer (zarezerwowane dla 'cała sieć') oraz samych jedynek (zarezerwowane dla 'wszystkie hosty') -> maska musi zostawić co najmniej dwa bity dla hosta

## **Protokół IP**

### **Właściwości protokołu IP**

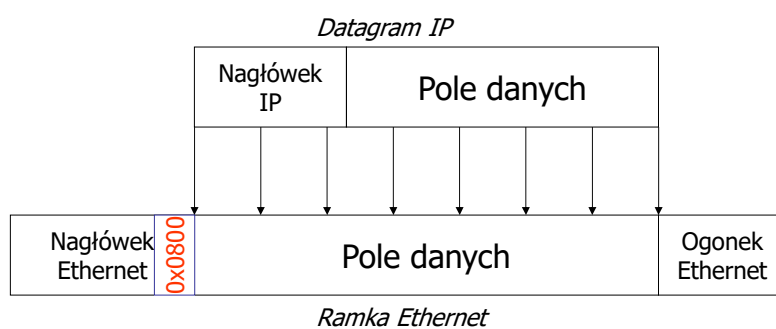
- Bezpołączeniowy — każdy pakiet przesyłany samodzielnie
- Brak potwierżeń dostarczenia pakietu
- Brak timeout-u i retransmisji
- Brak kontroli poprawności danych
- Brak kontroli przepływu
- Ograniczone wiadomości
- Brak wykrywania powtórzeń tych samych pakietów
- Brak zachowania kolejności pakietów



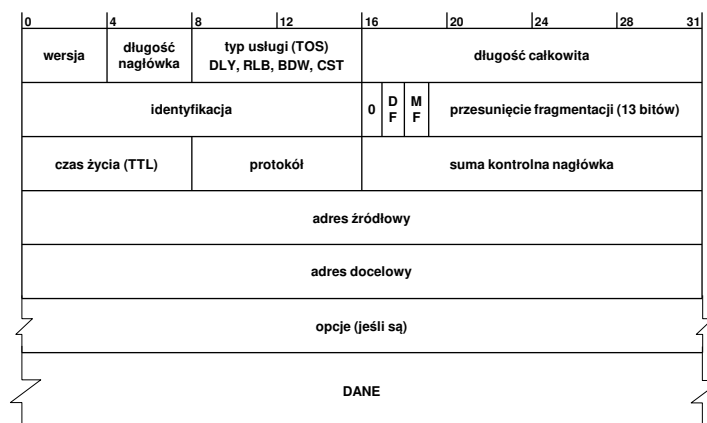
## Datagram IP

## Enkapsulacja

- Jednostka danych nazywa się **datagramem**



## Budowa datagramu IP



## Nagłówek IP

0	4	8	12	16	20	24	28	31
wersja	długość nagłówka	typ usługi (TOS) DLY, RLB, BDW, CST			długość całkowita			

- Wersja: 4
- Długość nagłówka: wyrażona w jednostkach 32bity. Maksymalny rozmiar —  $15 * 4\text{ bajty} = 60\text{ bajtów}$  — narzuca ograniczenia w stosowaniu niektórych opcji.

## Nagłówek IP

0	4	8	12	16	20	24	28	31
wersja	długość nagłówka	typ usługi (TOS) DLY, RLB, BDW, CST		długość całkowita				

- Typ usługi:
  - opóźnienie (np. telnet)
  - niezawodność (np. SNMP)
  - przepustowość (np. ftp)
  - koszt (np. news)
  - Priorytety
- Istnieje inna interpretacja pola TOS związana z klasyfikacją ruchu (diffserv)
- Długość całkowita: bajty. Max=64kB

## Nagłówek IP

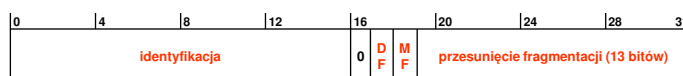
0	4	8	12	16	20	24	28	31
czas życia (TTL)				protokół		suma kontrolna nagłówka		

- Czas życia: liczba przeskoków; zapobiega krążeniu pakietów.
- Protokół: typ danych w polu dane.
- Suma kontrolna nagłówka — dotyczy tylko nagłówka. O poprawność danych muszą zabiegać protokoły wyższych warstw.

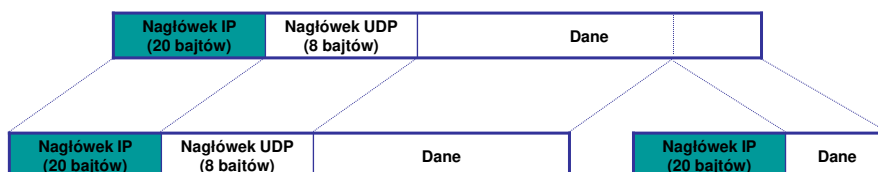
## Dzielenie datagramu IP

- Maksymalny rozmiar datagramu IP (65535 bajtów) może przekraczać maksymalny rozmiar pakietów warstwy niższej (np. Ethernet: 1500 bajtów)
- Jeżeli warstwa IP ma do wysłania datagram, to pyta interfejs przez który datagram ma zostać wysłany o jego MTU. Jeżeli MTU jest mniejsze niż rozmiar datagramu to następuje fragmentacja.
- Może dzielić komputer wysyłający i routery pośrednie.
- Składanie następuje TYLKO u odbiorcy — routery pośrednie nie wykonują tej czynności. Podzielony datagram dociera w takim stanie do odbiorcy.

## Nagłówek IP — fragmentacja



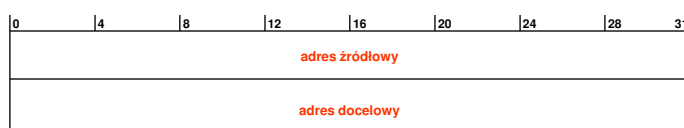
- Pola ważne przy fragmentacji:
  - Wszystkie fragmenty mają takie samo pole *identyfikacja*
  - **DF** - Don't Fragment; **MF** - More Fragments
  - **Przesunięcie fragmentacji** — numer pierwszego bajta danych w stosunku do oryginalnego datagramu (po 8 bajtów)



### Składanie pakietu IP

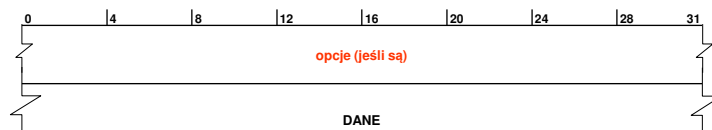
- Z każdym otrzymanym niekompletnym pakietem IP związany jest bufor, tablica znaczników i zegar.
- Na podstawie *przesunięcia* fragment wstawiany jest w odpowiednie miejsce w buforze.
- Wypełnianie trwa aż do otrzymania ostatniego fragmentu, tzn. najdalej przesunięty fragment posiada wyłączony bit MF i cały bufor jest wypełniony.
- Po każdym otrzymanym fragmencie uruchamiany jest zegar. Inicjalizowany jest wartością  $\max(\text{wart\_pocz}, \text{TTL})$ . Jeżeli zegar zliczy do zera bufor jest zwalniany i pakiet odrzucany.

### Nagłówek IP



- Adres źródłowy
  - ZAWSZE adres pojedynczego hosta
- Adres docelowy
  - adres pojedynczego hosta
  - adres grupowy
  - adres rozgłoszeniowy

## Nagłówek IP



- Opcje np.:
  - zapis trasy
  - definiowanie ścieżki po której pakiet ma przejść

## Protokół IPv6

### **Przyczyny zastąpienia IPv4**

- Przestrzeń adresowa na wyczerpaniu
- Słaba wydajność
- Braki w mechanizmach zabezpieczeń
- Złożona konfiguracja

### **Przestrzeń adresowa**

Ogromne zapotrzebowanie na adresy:

- dla milionów nowych użytkowników (Chiny, Indie, Japonia, ...)
- dla milionów nowych urządzeń (telefony komórkowe, smartphony, samochody, AGD, ...)
- dla aplikacji, które nie mogą pracować poprzez NAT (telefonia IP, serwery domowe, gry sieciowe, multimedia, ...)
- dla połączeń dzierżawionych (TV kablowa, xDSL, WLAN, Bluetooth, ...)

### Może częściej stosować NAT?

Nie, gdyż:

- NAT znacznie zwiększa stopień skomplikowania sieci i redukuje możliwości zarządzania nią
- NAT wymusza stosowanie modelu aplikacji 'klient-serwer'
  - blokowanie komunikacji 'każdy-z-każdym'
  - blokowanie usług, urządzeń wywoływanych przez innych (domowe serwisy, telefony IP)
  - ogranicza stosowanie niektórych aplikacji i serwisów

### Historia rozdziału adresów

**1981:** wprowadzanie protokołu IPv4

**1985:** wykorzystano  $\approx 1/16$  dostępnej przestrzeni

**1990:** wykorzystano  $\approx 1/8$  dostępnej przestrzeni

**1995:** wykorzystano  $\approx 1/4$  dostępnej przestrzeni

**2000:** wykorzystano  $\approx 1/2$  dostępnej przestrzeni

- możliwości oszczędzania na przydziale adresów
  - dzielenie puli adresów PPP / DHCP
  - Bezklasowy routing wewnątrzdomenowy CIDR (Classless Inter-Domain Routing)
  - translacja adresów NAT (Network Address Translation)
- teoretyczny limit 32-bitowej przestrzeni:  $\approx 4$  miliardy urządzeń
- praktyczny limit 32-bitowej przestrzeni:  $\approx 250$  milionów urządzeń



### **Mechanizmy zabezpieczeń**

- Protokół IPv4 nigdy nie był projektowany jako bezpieczny
  - stworzony dla odizolowanych sieci wojskowych
  - następnie zaadaptowany na potrzeby publicznych sieci akademickich i naukowych
- Wsparcie dla bezpieczeństwa zostało wprowadzone później
  - SSL, SHTTP, IPSECv4
  - brak JEDNEGO standardu
- Rozszerzenia o bezpieczeństwo są opcjonalne
  - nie można zakładać ich obecności

### **Podstawowe zmiany**

- Poszerzenie przestrzeni adresowej
- Uproszczenie budowy nagłówka
- Poprawiony mechanizm opcji i rozszerzeń
- Wprowadzenie etykietowania strumieni
- Wsparcie dla uwierzytelnienia i szyfrowania danych

Uproszczenie nagłówka

Zmienione

Usunięte

0 bitów	4	8	16	24	31
Wer.	IHL	Typ usługi	Całkowity rozmiar		
Identyfikator		Flagi		Offset fragmentacji	
Czas życia	Protokół		Suma kontrolna		
32 bitowy adres źródła					
32 bitowy adres celu					
Opcje i dopełnienie					

Nagłówek IPv6

0	4	12	16	24	31
Wersja	Klasa	Etykieta strumienia (Flow Label)			
Długość pola danych		Następny nagłówek		Limit przeskoków	
128 bitowy adres źródłowy					
128 bitowy adres docelowy					

### **Nagłówek IPv6**

- Wersja (4 bity) – definiuje wersję protokołu, dla IPv6 - 6 (bitowo 0110)
- Klasa ruchu (8 bitów) – określa sposób w jaki ma zostać potraktowany pakiet. W IPv4 podobno pole „Type of Service” jednak zmieniono mechanizmy priorytetowania.
- Etykieta strumienia (20 bitów) – pomaga odróżnić pakiety, które wymagają takiego samego traktowania (ta sama wartość pola klasy ruchu)
- Długość pola danych (16 bitów) – wielkość pakietu, bez długości podstawowego nagłówka (jednak wliczając nagłówki rozszerzające)

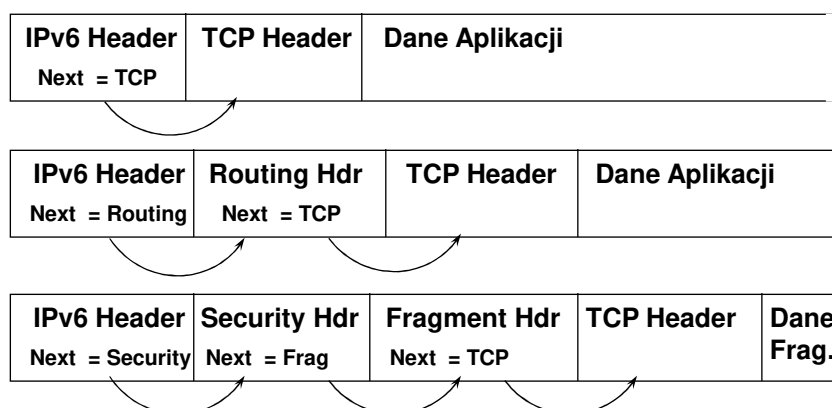
### **Nagłówek IPv6**

- Następny nagłówek (8 bitów) – identyfikuje typ następnego nagłówka (pozwala rozróżnić , nagłówek rozszerzający od nagłówka warstwy wyższej). W przypadku nagłówka warstwy wyższej wartość pola jest identyczna jak w IPv4
- Limit przeskoków (8 bitów) – określa ilość węzłów, po której pakiet zostaje skasowany (w IPv4 pole TTL).
- Adres źródłowy (128 bitów) – adres węzła, który wysłał pakiet danych
- Adres docelowy (128 bitów) – adres węzła do którego jest adresowany pakiet danych

### Dodatkowe opcje

- Pole Opcje IP zostało zastąpione zestawem opcjonalnych "Extension Headers"
- Dodatkowe nagłówki są ze sobą powiązane (lista dowiązań)
- Uproszczenie przetwarzania pakietów
  - routery analizują zawartość głównego nagłówka (wyjątek routing-header)
  - pozostałe są jedynie brane pod uwagę gdy router wspiera dane opcje
  - skrócenie czasu przetwarzania i przesyłania

### Dodatkowe nagłówki



### Zmiany w nagłówkach

- Nagłówek IPv4
  - 20 oktetów + opcje : 13 pól, w tym 3 bity flag
  - Zmienna długość
- Nagłówek IPv6
  - 40 oktetów, 8 pól
  - Stała długość
  - Opcje umieszczone w nagłówkach dodatkowych
- Pola zmodyfikowane
  - Adresy, zwiększona długość z 32 bitów -> 128 bitów
  - Zmiana Time to Live -> Hop Limit
  - Typ Protokołu (Protocol Type) -> Następny Nagłówek (Next Header)
  - Rodzaj usługi (Type of Service) -> Klasa ruchu (Traffic Class)

### Zmiany w nagłówkach

- Pola usunięte
  - Fragmentation field umieszczone poza podstawowym nagłówkiem
  - IP options umieszczone poza podstawowym nagłówkiem
  - Header Checksum usunięte
  - Header Length usunięte
  - Length field nie uwzględnia nagłówka
  - Wypełnienie zmienione z 32 do 64 bitów
- Pola dodane
  - Nowe pole Flow Label

### Jaka długość adresu?

- propozycja 64-bitowego adresu o stałej długości
  - wystarczający do obsługi  $10^{12}$  sieci i  $10^{15}$  węzłów, przy .0001 wydajności alokacji
  - minimalizuje rozmiar narzutu na dane przy pakietowaniu
  - efektywny przy przetwarzaniu przez oprogramowanie
- propozycja adresu o zmiennej długości maksymalnie do 160-bitów
  - schemat kompatybilny z planami adresacji OSI NSAP
  - wystarczająco duża przestrzeń dla mechanizmów auto-konfiguracji z użyciem adresów IEEE 802
  - można by było rozpocząć od adresów krótszych od 64 bitów zwiększanych w miarę zapotrzebowania
- wybrano 128-bitowy adres o stałej długości
  - **(340 282 366 920 938 463 463 374 607 431 768 211 456 wszystkich możliwych adresów)**

### Tekstowa reprezentacja adresów

- Dla IPv6 128 bitowy adres dzieli się na 16 bitowe fragmenty przedzielone dwukropkami. Każdy 16-bitowy fragment konwertowany jest do postaci szesnastkowej.
- "Preferowana" forma:  
1080:0000:00FF:0000:0008:0800:200C:417A
- Forma skrócona: FF01:0:0:0:0:0:0:43  
zastąpione przez: FF01::43
- Z adresem IPv4: 0:0:0:0:0:FFF:13.1.68.3  
lub ::FFFF:13.1.68.3

### Tekstowa reprezentacja adresów

- Prefiks adresu: 2002:43c:476b::/48  
**(uwaga: brak masek w IPv6!)**
- Prefiks („/48” ) jest częścią adresu wskazującą bity, które mają ustalone wartości lub są bitami identyfikatora sieci.
- Format w URLach:  
http://[3FFE::1:800:200C:417A]:8000

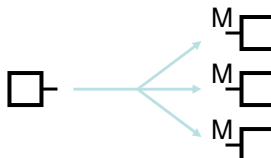
(konwersja z nawiasami prostokątnym używana jest zawsze gdy może wystąpić mylna interpretacja)

### Podstawowe typy adresów

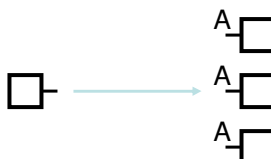
unicastowe:

komunikacja jeden- do-jeden 

multicastowe:

komunikacja jeden-do-wielu 

anycastowe:

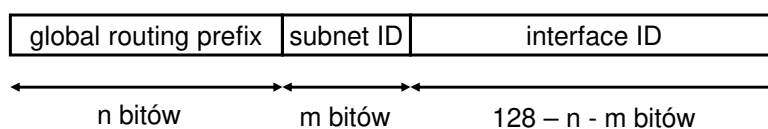
komunikacja jeden- do-  
najbliższego węzła 

### IPv6 – model adresacji

- adresy są powiązane z interfejsami
  - brak zmiany w stosunku do IPv4
- interfejs może posiadać kilka różnych adresów
- adresy unicast mają zasięg
  - Link-Local
  - Unique Local
  - Global
- adresy mają okres ważności
  - poprawny i preferowany czas



### Format adresu unicastowego



- adresy unicastowe są hierarchiczne, podobnie jak w IPv4
- 'global routing prefix' również ma strukturę hierarchiczną



### Zakresy adresów unicast

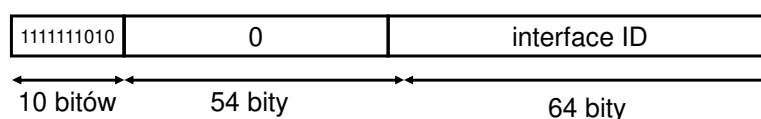
- Adresy lokalne dla łącza (Link-Local) mają prefiks FE80::/10 i są wykorzystywane tylko do komunikacji w jednym segmencie sieci lokalnej lub przy połączeniu typu punkt-punkt. Routery nie przekazują pakietów z takimi adresami. Każdy interfejs musi mieć przydzielony co najmniej jeden adres lokalny (nawet jeżeli posiada adres globalny lub unikatowy adres lokalny).
- Unikatowe adresy lokalne (Unique Local) mają prefiks FC00::/7 i są odpowiednikami adresów prywatnych w IPv4.
- Adresy globalne (Global Unicast) są widoczne w całej sieci Internet i są odpowiednikami adresów publicznych w IPv4 (np. prefiks 2001:0200::/23).

### Adresy unicastowe nie globalne

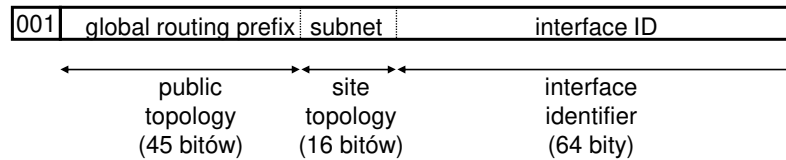
- Adres unicastowy unique local ma zastosowanie jedynie w pojedynczej sieci, może być powielany (odpowiednik adresów prywatnych IPv4)



- Adres unicastowy link-local ma zastosowanie jedynie w obszarze pojedynczego łącza, może być powielany



### Global Unicast Addresses



- Jedynie 1/8 całkowitej przestrzeni (binarny prefix 001) wstępnie zostało użyte
- Globalny prefiks routingu ma strukturę hierarchiczną, używanie alokacji i routingu typu CIDR
- Polityka agregacji przy przydziale adresów dla końcowych konsumentów
  - 48-bitowy prefix => 16 bitów na przestrzeń podsieci

### Adresy interfejsu

- Loopback - nadany jedynie dla jednego wirtualnego interfejsu w węźle (::1/128)
- Link-Local
- Unique-Local
- Kompatybilny z IPv4 (:::/96 - pierwsze 96 bitów stanowią 0, pozostają 32 bity adres IPv4).
- Automatycznie uzyskany 6to4 (jeżeli jest dostępny publiczny adres IPv4)
- ...

### Autokonfiguracja urządzeń

- Protokół IPv6 definiuje 2 typy automatycznej autokonfiguracji urządzeń (nie jest wymagana ręczna konfiguracja adresów IP):
- **Stateless Address Autoconfiguration** (bezstanowa autokonfiguracja adresu IPv6) to wymagany i podstawowy element systemu autokonfiguracji adresów IPv6. W prostszych konfiguracjach jest to jedyna metoda konfiguracji urządzenia.
- **Stateful Address Autoconfiguration** (stanowa autokonfiguracja adresu IPv6) stosowane w przypadkach, kiedy wymagana jest większa kontrola nad przydzielanymi adresami. Wykorzystywany jest protokół DHCPv6.

### Bezstanowa autokonfiguracja adresu IPv6

- Generacja adresów lokalnych łączy (Link-Local)
- Brak możliwości określania jakichkolwiek parametrów
- Komunikacja ograniczona do segmentu sieci (laboratorium, sala)
- Bez dodatkowych protokołów niewystarczająca do automatycznego podłączenia do sieci Internet
- Brama domyślna może zostać ustawiona na podstawie informacji przesłanych od routera
- Podstawa do dalszej automatycznej konfiguracji na wyższych poziomach

### **Stanowa autokonfiguracja adresu IPv6**

- Przyznawanie adresów z dowolnego zakresu (np. adresów globalnych)
- Konfiguracja serwerów DNS
- Konfiguracja strefy czasowej
- Konfiguracja bramy domyślnej
- Możliwość wykorzystania wielu opcji
- Możliwość wykorzystania Router Renumbering do określenia innej bramy domyślnej
- Konfiguracją stanową (statefull) zajmuje się protokół DHCPv6

### **Neighbor Discovery**

- |  |  |
|--|--|
| <ul style="list-style-type: none"> <li>• Typy komunikatów ICMPv6:             <ul style="list-style-type: none"> <li>– router solicitation</li> <li>– router advertisement</li> <li>– neighbor solicitation</li> <li>– neighbor advertisement</li> <li>– redirect</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>• Realizowane funkcje:             <ul style="list-style-type: none"> <li>– wykrywanie routerów</li> <li>– wykrywanie prefiksu</li> <li>– autokonfiguracja adresów i innych parametrów</li> <li>– wykrywanie duplikacji adresów (DAD)</li> <li>– odwzorowanie na adresy łączy danych</li> <li>– przekierowanie pierwszego-hopa</li> </ul> </li> </ul> |
|--|--|

### **Routing**

- Użycie tego samego schematu routingu "longest-prefix match" jak w CIDR IPv4
- Adaptacja istniejących w IPv4 protokołów routingu aby obsługiwały większe adresy
  - unicast: OSPF, RIP-II, IS-IS, BGP4+, ...
  - multicast: MOSPF, PIM, ...
- Możliwe użycie dodatkowego nagłówka (Routing Header) z adresami anycastowymi by routować pakiety poprzez wybrane regiony
  - np. wybór ISP, wydajność, itd.

### **Pozostałe cechy IPv6**

- Możliwe server-less plug-and-play
- Uwierzytelnianie end-to-end i szyfrowanie możliwe w warstwie IP
- Eliminacja tzw. "triangle routing" w mobile IP
- Inne ulepszenia ...

Wady:

- quality of service (te same możliwości jak w IPv4)
- routing (te same protokoły routingu jak w IPv4)
  - Z wyjątkiem przestrzeni adresowej i hierarchii adresacji

**Dokumentacja**

- Internet Protocol — RFC 971
- Internet Protocol, Version 6 (IPv6) — RFC 2460
- R.W. Stevens — „Biblia TCP/IP”, t.1