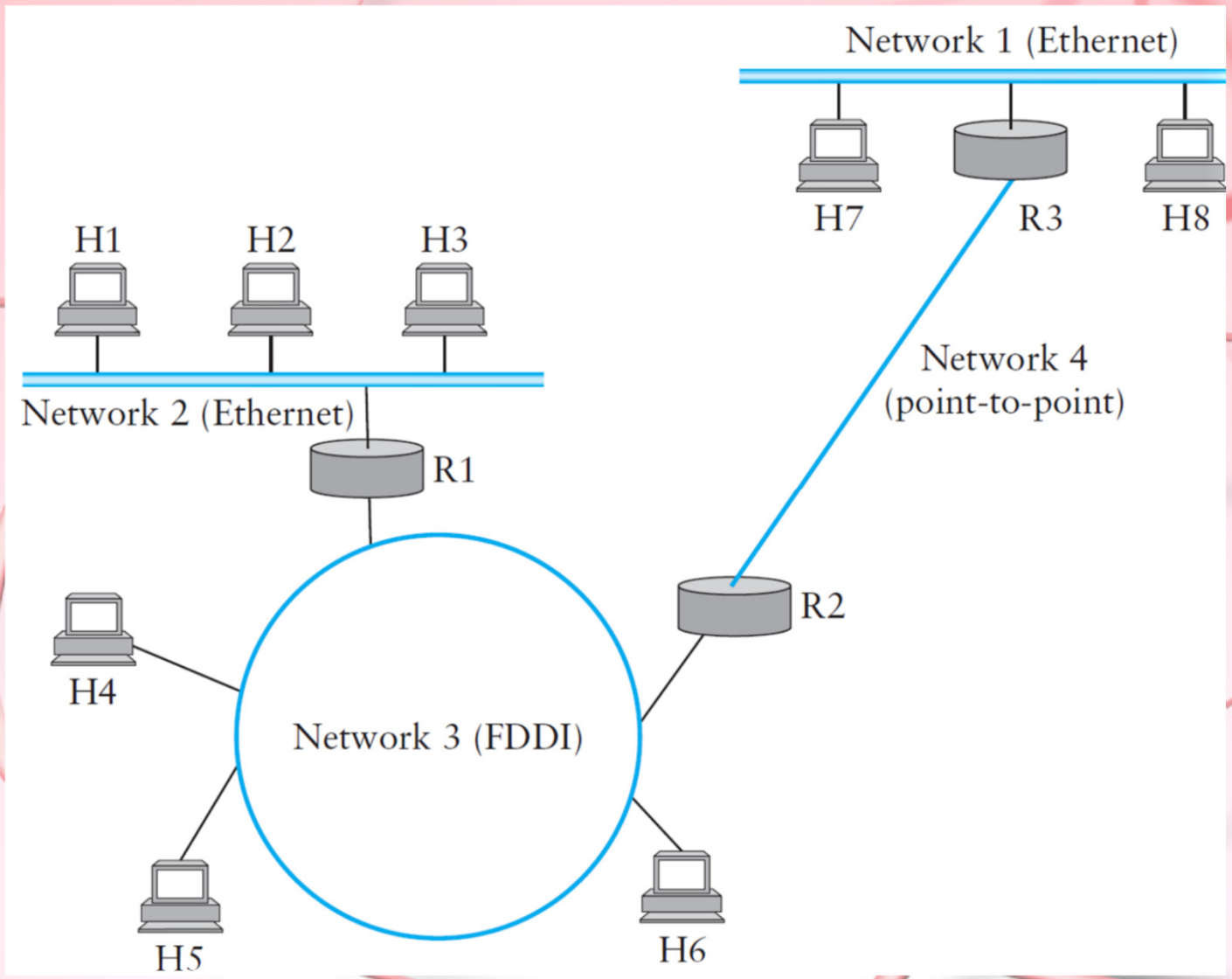
Szymon Łukasik
KAiTI

Sieci komputerowe

- Wstęp do intersieci, protokół IPv4

Internet a internet



Plan wykładu

1. Ogólne informacje na temat sieci Internet i protokołu IP (ang. Internet Protocol) w wersji 4.
2. Adresowanie w protokole IPv4
   - Klasy adresów, identyfikacja i zapis
   - Adresy specjalnego przeznaczenia
   - Podział przestrzeni adresowej
3. Budowa datagramu w protokole IPv4
4. Fragmentacja w IPv4

Informacje ogólne

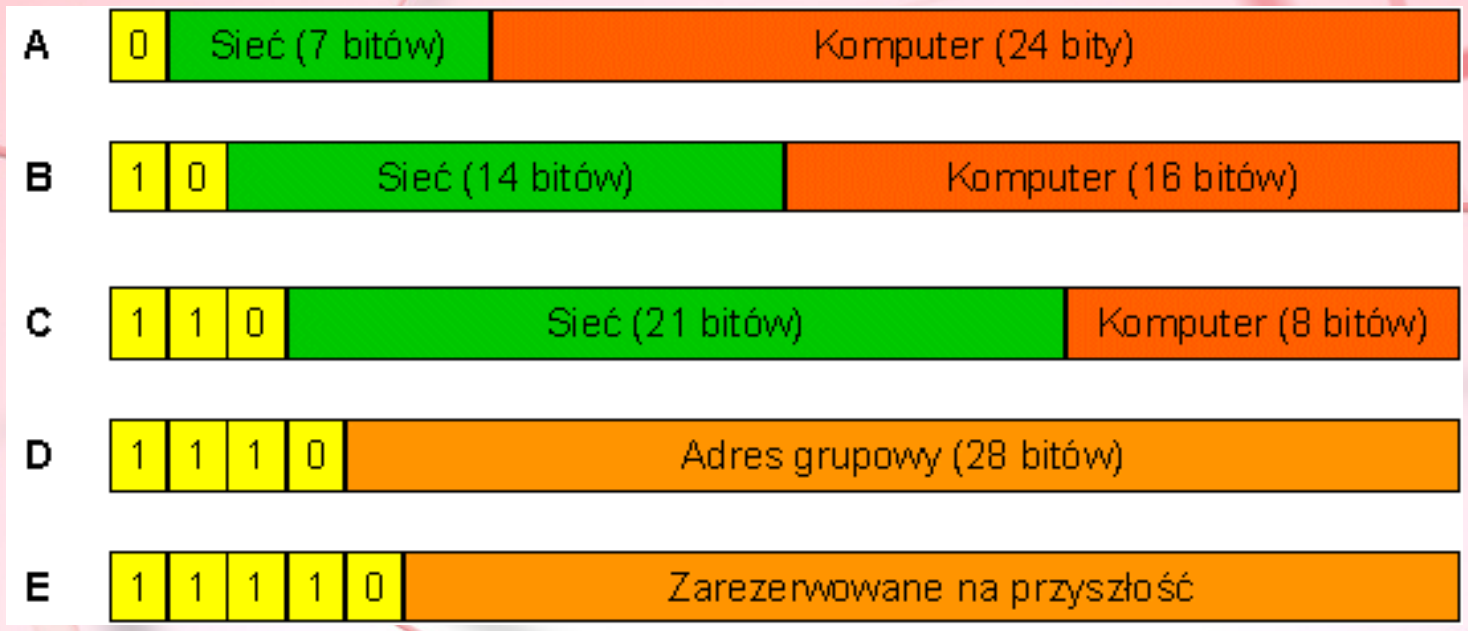
- Początki historii Internetu to lata 70 XX wieku, pierwsza sieć tego typu to ARPANET łączący 4 instytucje w USA
- Jako twórcę protokołu IP uważa się duet Cerf i Kahn, pierwsze „źródło pisane” na jego temat to praca:

  Vinton G. Cerf, Robert E. Kahn, "A Protocol for Packet Network Intercommunication", IEEE Transactions on Communications, Vol. 22, No. 5, May 1974 pp. 637-648
- Dwa najważniejsze elementy:
  - Jednolite adresowanie umożliwiające przesyłanie pakietów między węzłami znajdującymi się w różnych sieciach, o czasami diametralnie odmiennej fizycznej architekturze (mamy złudzenie wielkiej, spójnej wewnętrznie sieci).
  - Konstrukcja datagramu pozwalająca na bezpołączeniowe i zawodne (ang. *unreliable*) przesyłanie informacji od nadawcy do adresata.

Adresowanie – wprowadzenie

- Adres internetowy (adres IP) jest jednoznaczną 32-bitową liczbą dwójkową przypisaną węzłowi (połączeniu danego urządzenia do sieci) i niezbędną do komunikacji z nim w ramach rozważanej intersieci.
- Każdy adres zawiera:
  - Prefiks – identyfikujący sieć fizyczną do której przyłączony jest dany komputer
  - Sufiks – identyfikujący konkretny komputer w w/w sieci
- Adres – jednoznaczny, prefiksy przyznane globalnie, sufiksy – lokalnie bez globalnego uzgadniania
- Podział adresów na pięć podstawowych klas (A, B, C, D i E) – o różnych rozmiarach prefiksu i sufiksu

Klasy adresów IP



Zapis adresów IPv4

32-bitowa liczba binarna:

10000001 00110100 00000110 00000000
11000000 00000101 00110000 00000011
00001010 00000010 00000000 00100101
10000000 00001010 00000010 00000011

Notacja dziesiętna z kropkami:

129.52.6.0
192.5.48.3
10.2.0.37
128.10.2.3

Określanie klasy adresu

Indeks	Bity 0-3	Klasa	Indeks	Bity 0-3	Klasa
0	0000	A	8	1000	B
1	0001	A	9	1001	B
2	0010	A	10	1010	B
3	0011	A	11	1011	B
4	0100	A	12	1100	C
5	0101	A	13	1101	C
6	0110	A	14	1110	D
7	0111	A	15	1111	E

Klasy – więcej detali

Klasa	Bity adresujące sieć	Bity adresujące komputer	Zakres adresów	Sieci	Liczba sieci	liczba hostów w obrębie sieci	Identyfikacja
A	8	24	1.0.0.0 - 126.0.0.0	Bardzo duże	127	16 777 214	pierwszy bit = 0
B	16	16	128.1.0.0 - 191.254.0.0	Średniej wielkości	16 382	65 534	pierwsze dwa bity = 10
C	24	8	192.0.1.0 - 223.255.254.0	Małe	2 097 150	254	pierwsze trzy bity = 110
D	-	-	224.0.0.0 - 239.255.255.254	Transmisja grupowa	Brak podziału	Brak podziału	pierwsze cztery bity = 1110
E	-	-	240.0.0.0 - 255.255.255.255	Rezerwo-wane dla IETF	-	-	pierwsze cztery bity = 1111

Adresy IP specjalnego przeznaczenia

- **Adres sieciowy** – odnosi się do samej sieci, a nie komputera. Sufiks adresu jest wypełniony zerami np. 192.168.10.0.
- **Adres rozgłaszania kierunkowego (ang. broadcast)** – odnosi się do wszystkich komputerów w sieci. Sufiks adresu wypełniony jedynkami np. 192.168.10.255 albo zerami (tzw. rozgłaszanie Berkeley-historyczne) np. 192.168.10.0.
- **Adres rozgłaszania ograniczonego** – odnosi się do rozgłaszania w lokalnej sieci (używane przy starcie systemu). Prefiks i sufiks wypełniony jedynkami tj. 255.255.255.255.
- **Adres bieżącego komputera** – odnosi się do lokalnego komputera (używane przy starcie systemu). Prefiks i sufiks wypełnione zerami tj. 0.0.0.0.
- **Adres pętli zwrotnej (ang. loopback)** – identyfikuje lokalną pętlę zwrotną umożliwiającą testowanie/aplikacji/serwerów/ usług. Prefiks 127, sufiks – dowolny. Np. 127.0.0.1.

Metody podziału przestrzeni adresowej

Aby zwiększyć efektywność podziału przestrzeni adresowej zaproponowano dodatkowe rozszerzenia dla protokołu IPv4.

Należą do nich przede wszystkim:

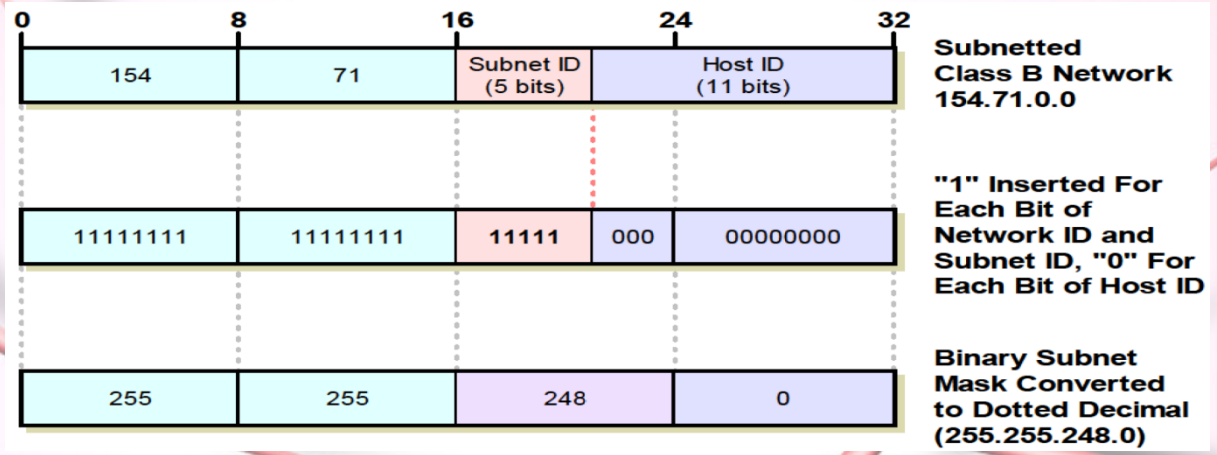
- **Maski podsieci** – umożliwiające dodatkowy podział sieci klasy A, B lub C na podsieci o określonym, nie zawsze idealnie dostosowanym do wymagań, rozmiarze
- **Bezklasowy wybór trasy między domenami** (ang. Classless Inter-Domain Routing, w skrócie: CIDR) – zakłada eliminację idei klas i podział całej dostępnej przestrzeni adresowej na podsieci o dokładnie określonej wielkości. Obecnie to dominująca metoda.

Maski podsieci

Adres IP w podsieci składa się z czterech części:

- bitów określających klasę adresu (obecnie nie obowiązuje),
- adresu sieci,
- adresu podsieci,
- adresu hosta

Podsieci identyfikuje się za pomocą pseudo-adresu IP, zwanego maską podsieci. Maska podsieci jest, podobnie jak sam adres IP, liczbą 32-bitową.



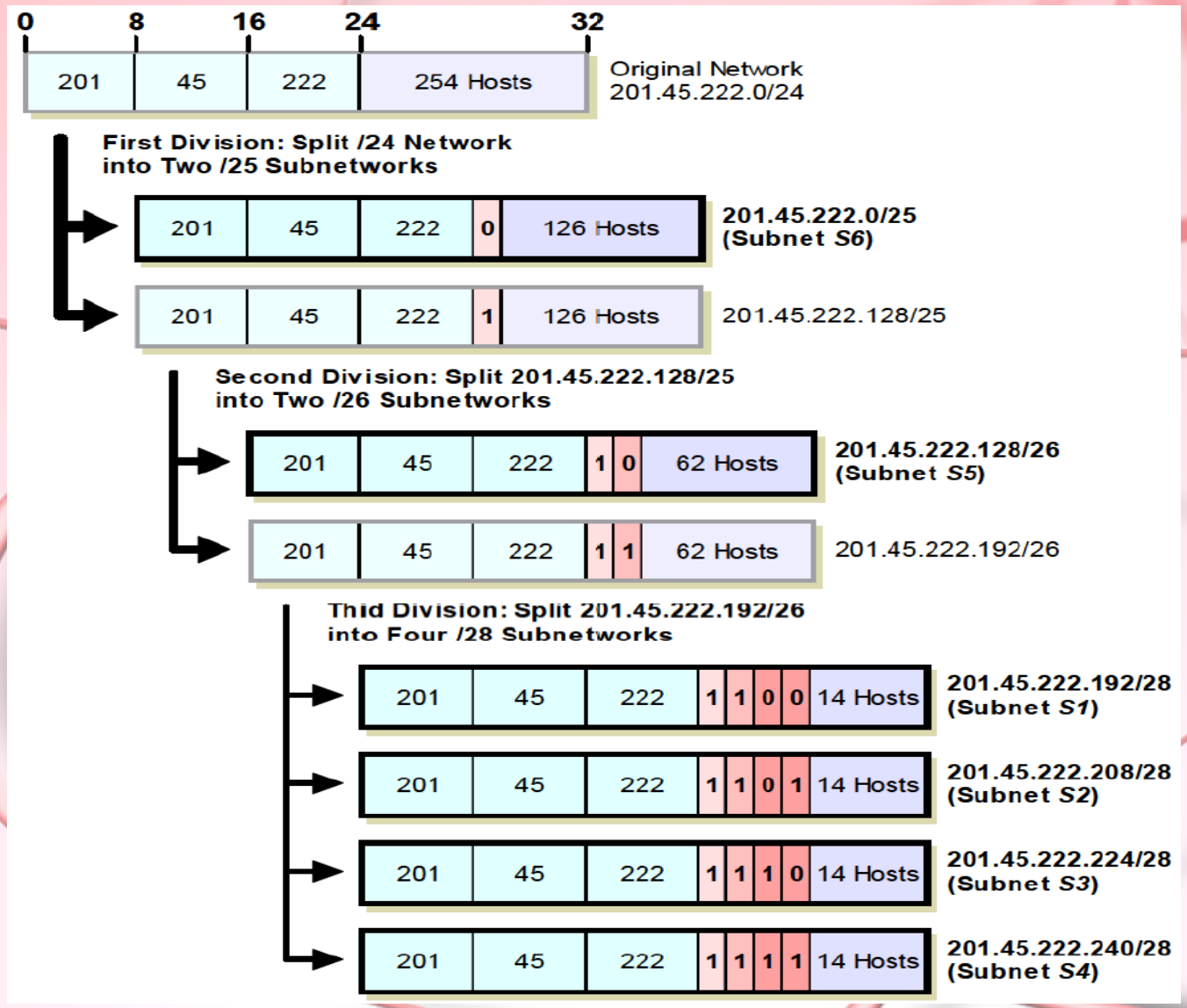
Możliwości podziału sieci klasy B na podsieci

# of Subnet ID Bit	# of Host ID Bits	# of Subnets Per Network	# of Hosts Per Subnet	Subnet Mask (Binary / Dotted Decimal)	Subnet Mask (Slash/ CIDR Nota-tion)	Subnet Address #N Formula (N=0, 1, ... # of Subnets-1)
0 (Default)	16	1	65,534	11111111.11111111.00000000.00000000 255.255.0.0	/16	--
1	15	2	32,766	11111111.11111111.10000000.00000000 255.255.128.0	/17	x.y.N*128.0
2	14	4	16,382	11111111.11111111.11000000.00000000 255.255.192.0	/18	x.y.N*64.0
3	13	8	8,190	11111111.11111111.11100000.00000000 255.255.224.0	/19	x.y.N*32.0
4	12	16	4,094	11111111.11111111.11110000.00000000 255.255.240.0	/20	x.y.N*16.0
5	11	32	2,046	11111111.11111111.11111000.00000000 255.255.248.0	/21	x.y.N*8.0
6	10	64	1,022	11111111.11111111.11111100.00000000 255.255.252.0	/22	x.y.N*4.0
7	9	128	510	11111111.11111111.11111110.00000000 255.255.254.0	/23	x.y.N*2.0
8	8	256	254	11111111.11111111.11111111.00000000 255.255.255.0	/24	x.y.N.0
9	7	512	126	11111111.11111111.11111111.10000000 255.255.255.128	/25	x.y.N/2. (N%2)*128
10	6	1,024	62	11111111.11111111.11111111.11000000 255.255.255.192	/26	x.y.N/4. (N%4)*64
11	5	2,048	30	11111111.11111111.11111111.11100000 255.255.255.224	/27	x.x.N/8. (N%8)*32
12	4	4,096	14	11111111.11111111.11111111.11110000 255.255.255.240	/28	x.y.N/16. (N%16)*16
13	3	8,192	6	11111111.11111111.11111111.11111000 255.255.255.248	/29	x.y.N/32. (N%32)*8
14	2	16,384	2	11111111.11111111.11111111.11111100 255.255.255.252	/30	x.y.N/64. (N%64)*4

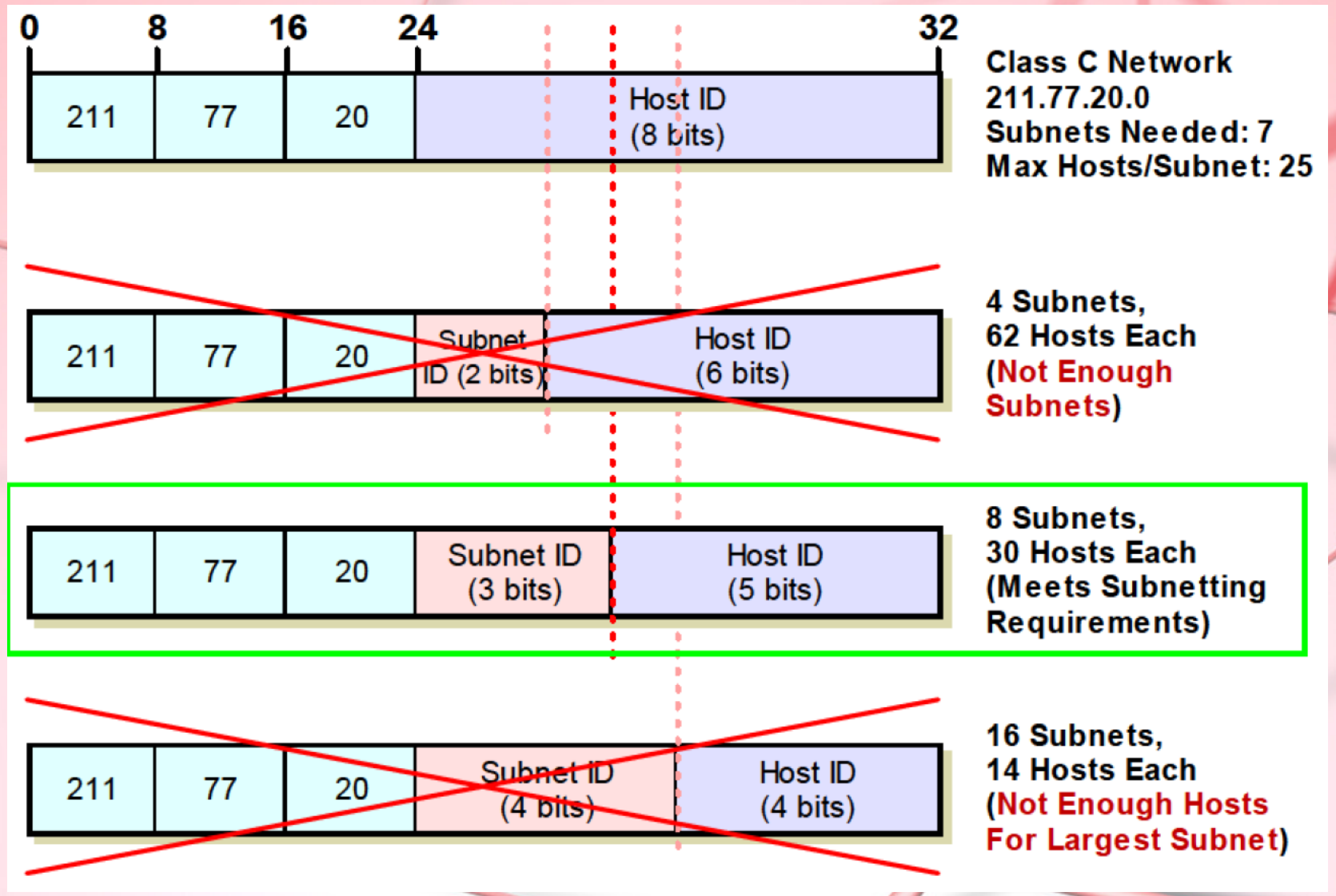
Możliwości podziału sieci klasy C na podsieci

# of Subnet ID Bit	# of Host ID Bits	# of Subnets Per Network	# of Hosts Per Subnet	Subnet Mask (Binary / Dotted Decimal)	Subnet Mask (Slash/ CIDR Nota-tion)	Subnet Address #N Formula (N=0, 1, … # of Subnets-1)
0 (Default)	8	1	254	11111111.11111111.11111111.00000000 255.255.255.0	/24	—
1	7	2	126	11111111.11111111.11111111.10000000 255.255.255.128	/25	x.y.z.N*128
2	6	4	62	11111111.11111111.11111111.11000000 255.255.255.192	/26	x.y.z.N*64
3	5	8	30	11111111.11111111.11111111.11100000 255.255.255.224	/27	x.y.z.N*32
4	4	16	14	11111111.11111111.11111111.11110000 255.255.255.240	/28	x.y.z.N*16
5	3	32	6	11111111.11111111.11111111.11111000 255.255.255.248	/29	x.y.z.N*8
6	2	64	2	11111111.11111111.11111111.11111100 255.255.255.252	/30	x.y.z.N*4

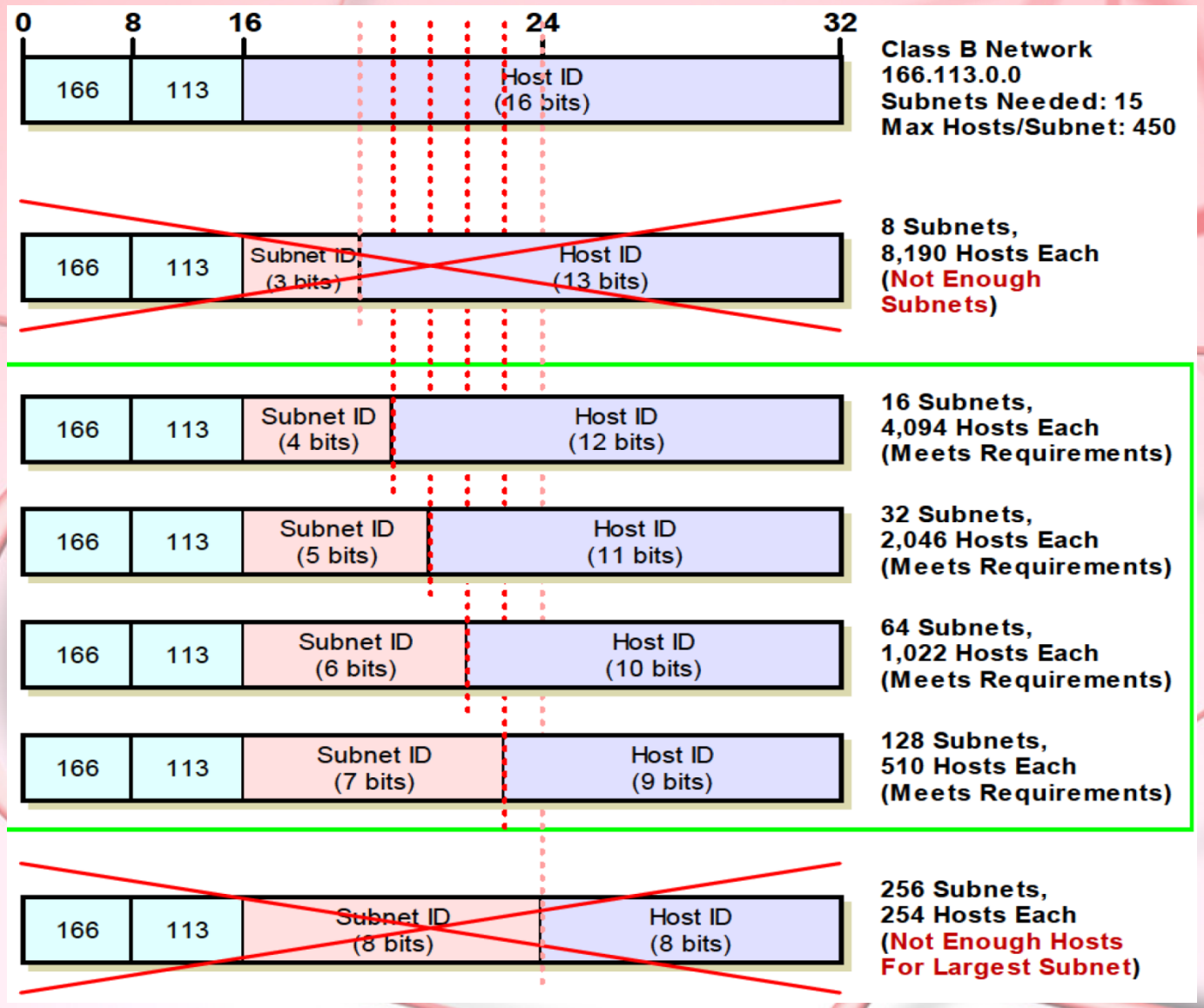
Maski podsieci o zmiennej długości



Podział na podsieci – przykład 1 (łatwy)



Podział na podsieci – przykład 2 (trudniejszy)

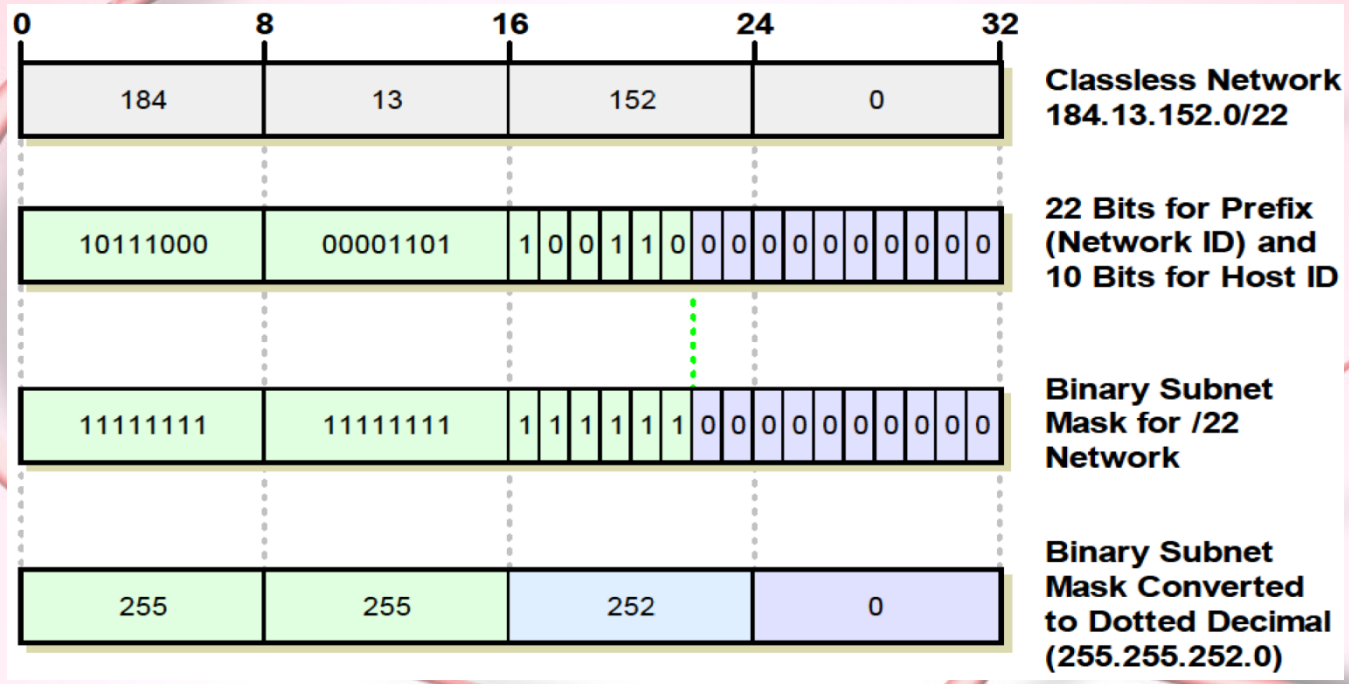


Bezklasowy wybór tras między domenami (CIDR)

Adres IP z CIDR składa się z dwóch części:

- adresu sieci,
- adresu hosta

Część sieciową definiuje „notacja slasha” (ang. slash notation) która określa długość prefiksu sieciowego (w bitach, po znaku /).



Adresy prywatne

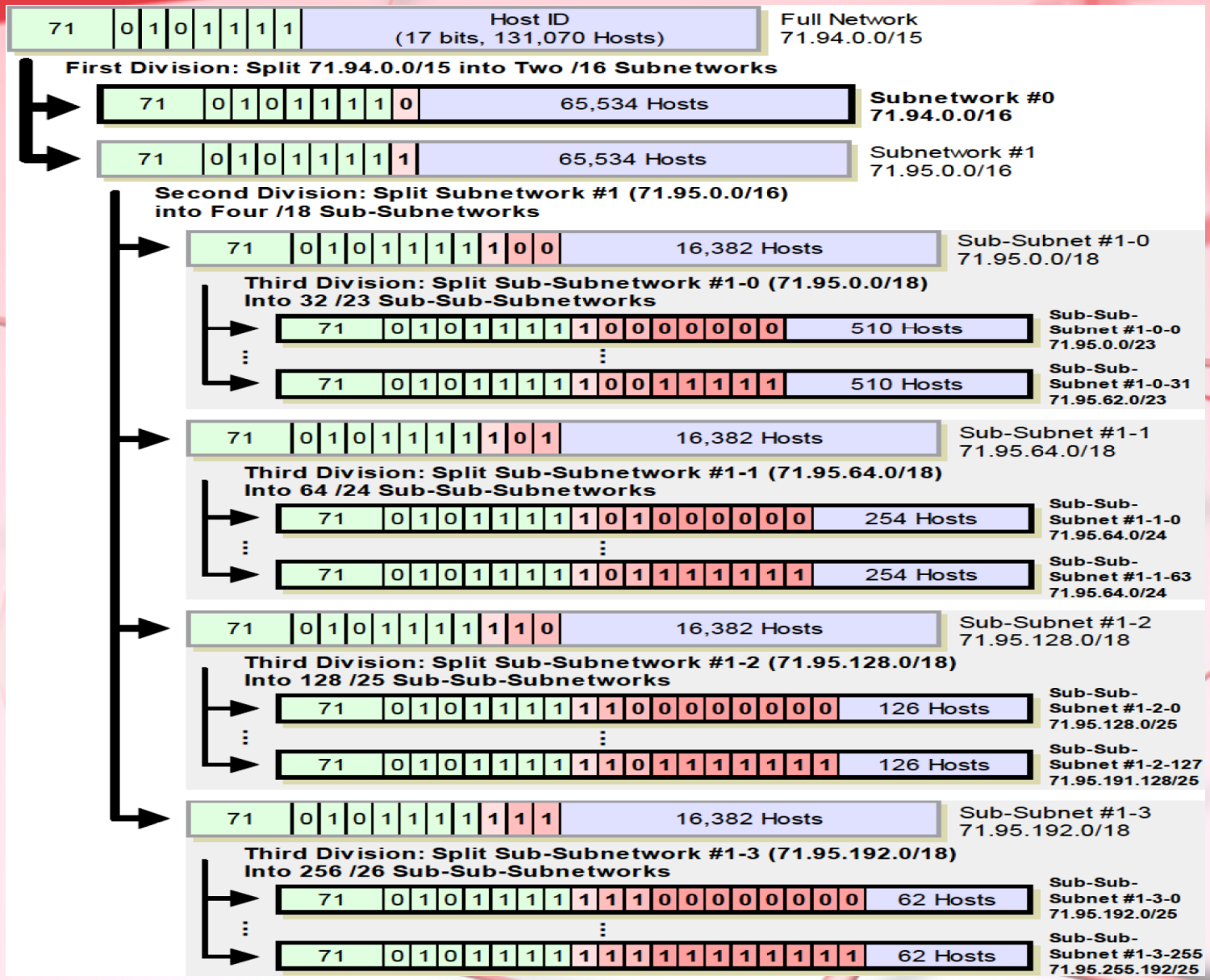
Adresy prywatne używane w sieciach LAN:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

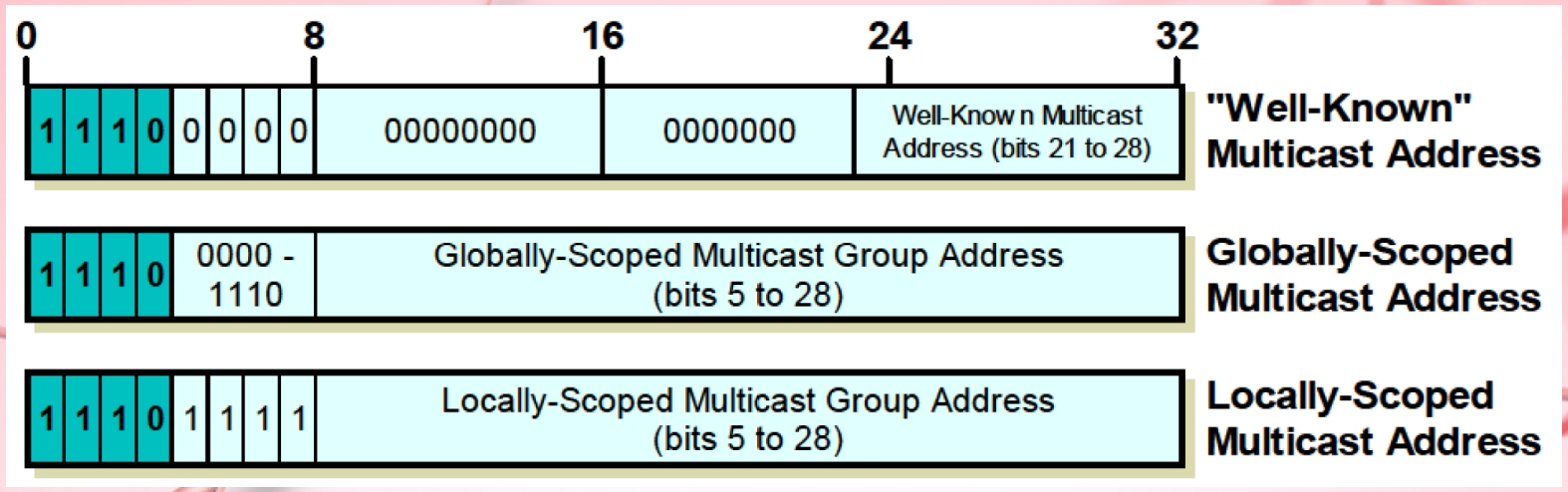
Adresy prywatne używane gdy występuje brak innych:

- 169.254.0.0/16

CIDR – podział przestrzeni adresowej



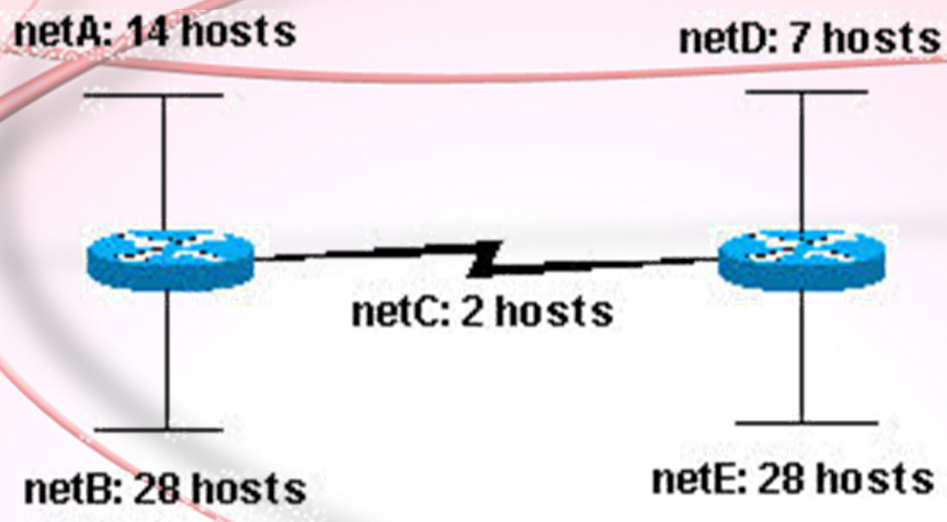
Transmisja grupowa – w zarysie



Range Start Address	Description
224.0.0.0	Reserved; not used
224.0.0.1	All devices on the subnet
224.0.0.2	All routers on the subnet
224.0.0.3	Reserved
224.0.0.4	All routers using DVMRP
224.0.0.5	All routers using OSPF
224.0.0.6	Designated routers using OSPF
224.0.0.9	Designated routers using RIP-2

Ćwiczenie

Mając sieć **204.15.5.0/24** stwórz jej podział tak by spełnić wymagania zaprezentowane poniżej:



Rozwiązanie (podsieci o ustalonym rozmiarze)

netA: 204.15.5.0/27 zakres adresów 1 do 30

netB: 204.15.5.32/27 zakres adresów 33 do 62

netC: 204.15.5.64/27 zakres adresów 65 do 94

netD: 204.15.5.96/27 zakres adresów 97 do 126

netE: 204.15.5.128/27 zakres adresów 129 do 158

Rozwiązanie (VLSM)

- **netA:** wymaga maski /28 (255.255.255.240) by obsłużyć 14 hostów
- **netB:** wymaga maski /27 (255.255.255.224) by obsłużyć 28 hostów
- **netC:** wymaga maski /30 (255.255.255.252) by obsłużyć 2 hosty
- **netD:** wymaga maski /28 (255.255.255.240) by obsłużyć 7 hostów
- **netE:** wymaga maski /27 (255.255.255.224) by obsłużyć 28 hostów

Rozwiązanie (VLSM, cd.)

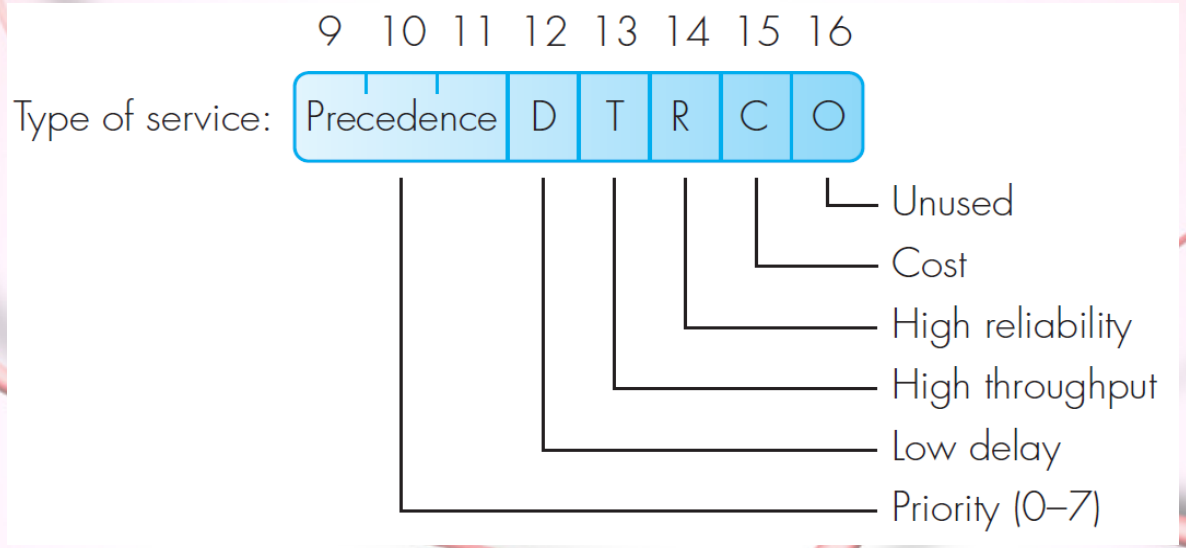
- **netB:** 204.15.5.0/27 zakres adresów 1 do 30
- **netE:** 204.15.5.32/27 zakres adresów 33 do 62
- **netA:** 204.15.5.64/28 zakres adresów 65 do 78
- **netD:** 204.15.5.80/28 zakres adresów 81 do 94
- **netC:** 204.15.5.96/30 zakres adresów 97 do 98

Datagram IP

bity									
słowa	**0**	**4**	**8**	**12**	**16**	**20**	**24**	**28 31**	
1	Wersja	IHL	Typ usługi		Długość całkowita				Nagłówek
2	Identyfikator				Flagi	Przesunięcie fragmentacji			
3	Czas życia		Protokół		Suma kontrolna				
4	Adres źródła								
5	Adres przeznaczenia								
6	Opcje						Uzupełnienie		
7	DANE								

Opis pól I

- **Wersja** [4 bity] – numer wersji protokołu IP np. 0100 to IPv4, 0110 i IPv6
- **IHL** [4 bity] – długość nagłówka (ang. IP Header Length) w 32-bitowych słowach, minimalnie = 5, maksymalnie 15 (czyli 60 bajtów)
- **TOS** [8 bitów] – typ/jakość usługi (ang. Type of Service) lub tzw. Differentiated Services



Opis pól II

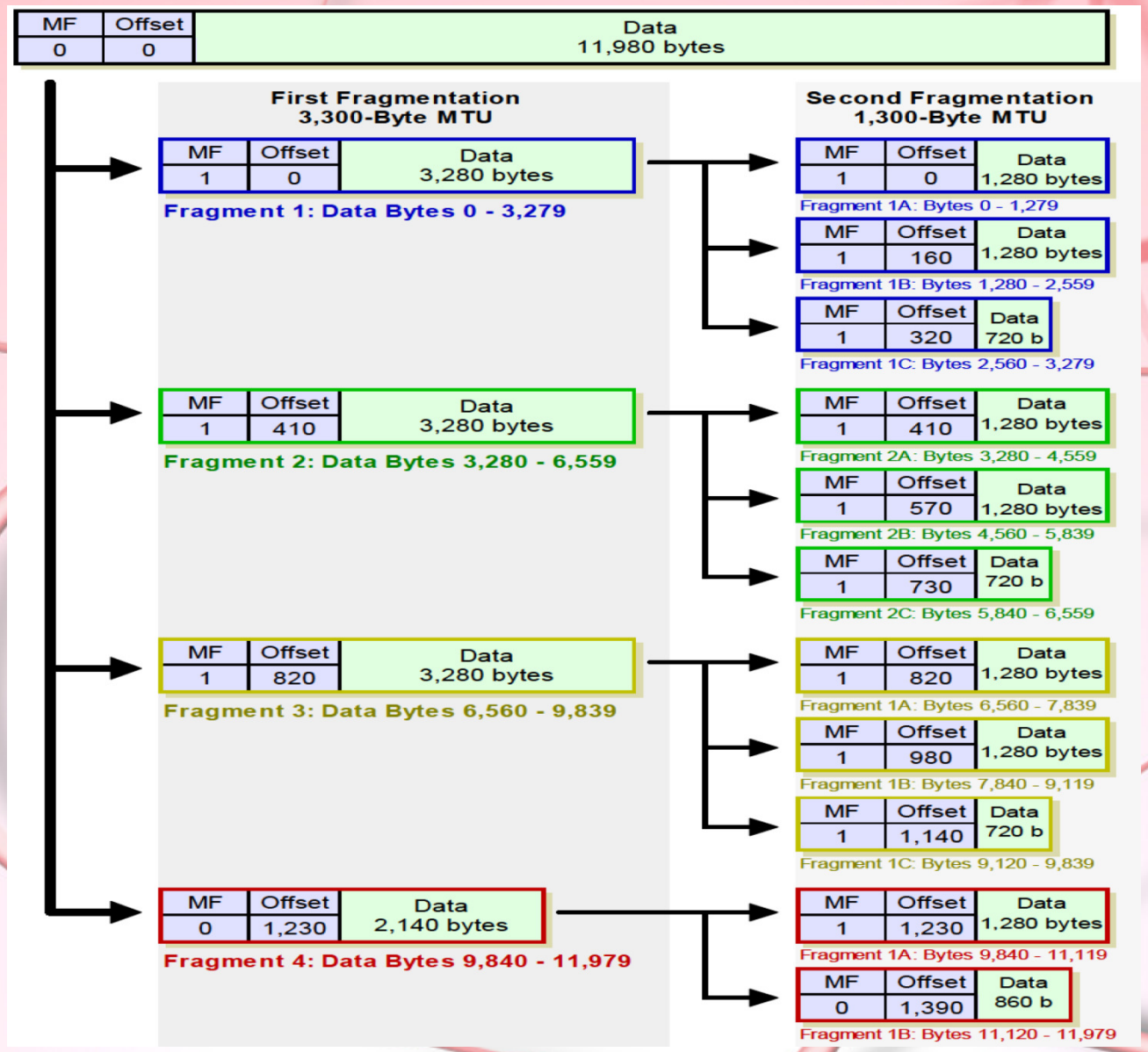
- **Długość całkowita** [16 bitów] – długość całkowita pakietu IP w bajtach (zawiera nagłówek i dane) . Łatwo zatem obliczyć że max. objętość przenoszonych danych to 65535B, rzeczywista zależy od MTU (ang. Maximum Transfer Unit) warstwy łącza – niezbędna jest ich fragmentacja (dzielenie pakietu na mniejsze części).
- **Identyfikator** [16 bitów] – numer identyfikacyjny pakietu
- **Flagi** [3 bity] – flagi sterujące fragmentacją:

  bit nr 0: zarezerwowany, musi mieć wartość zero

  bit nr 1: (DF) 0 – można, 1 – nie wolno fragmentować

  bit nr 2: (MF) 0 – ostatni fragment, 1 – będzie więcej
- **Przesunięcie fragmentacji** [13 bitów] – wskazuje, do którego miejsca pakietu danych należy fragment. Przesunięcie mierzone jest w jednostkach 8 bajtów (64 bitów). Pierwszy fragment ma przesunięcie równe zeru.

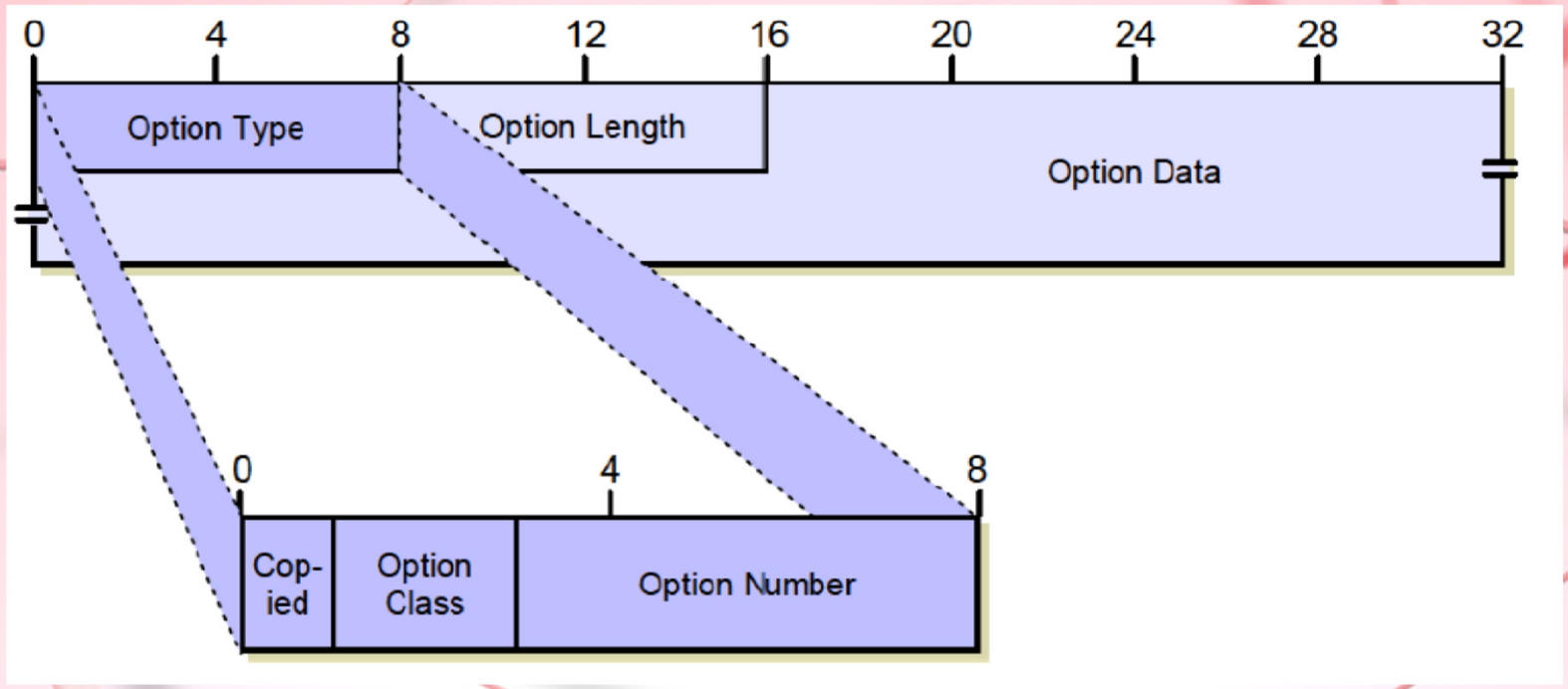
Fragmentacja IP – przykład



Opis pól III

- **Czas życia** [8 bitów] – w skrócie TTL (ang. Time-to-Live) , wskazuje maksymalny czas przebywania pakietu w Internecie, mierzony w praktyce liczbą skoków (ang. hops) między routerami, ustawiany początkowo na pewną wartość i stopniowo (przy każdym skoku) zmniejszany, przy TTL=0 pakiet jest odrzucany
- **Protokół** [8 bitów] – wskazuje oznaczenie protokołu warstwy wyższej, do którego zostaną przekazane dane z pakietu, np. 01h – ICMP, 06h – TCP, 11h – UDP
- **Suma kontrolna** [16 bitów] – suma kontrolna nagłówka
- **Adresy źródła i przeznaczenia** [32 + 32 bity]
- **Opcje** [zmienne] – opcje protokołu
- **Uzupełnienie** [32bity – długość pola opcji]
- **Dane** [zmienne]

Pole opcji – ogólny schemat



Opcje IPv4 (dla dociekliwych)

Option Class	Option Number	Length (bytes)	Option Name	Description
0	0	1	*End Of Options List*	An option containing just a single zero byte, used to mark the end of a list of options.
0	1	1	*No Operation*	A “dummy option” used as “internal padding” to align certain options on a 32-bit boundary when required.
0	2	11	*Security*	An option provided for the military to indicate the security classification of IP datagrams.
0	3	Variable	*Loose Source Route*	One of two options for source routing of IP datagrams. See below for an explanation.
0	7	Variable	*Record Route*	This option allows the route used by a datagram to be recorded within the header for the datagram itself. If a source device sends a datagram with this option in it, each router that “handles” the datagram adds its IP address to this option. The recipient can then extract the list of IP addresses to see the route taken by the datagram. Note that the length of this option is set by the originating device. It cannot be enlarged as the datagram is routed, and if it “fills up” before it arrives at its destination, only a partial route will be recorded.
0	9	Variable	*Strict Source Route*	One of two options for source routing of IP datagrams. See below for an explanation.
2	4	Variable	*Timestamp*	This option is similar to the *Record Route* option. However, instead of each device that handles the datagram inserting its IP address into the option, it puts in a timestamp, so the recipient can see how long it took for the datagram to travel between routers. As with the *Record Route* option, the length of this option is set by the originating device and cannot be enlarged by intermediate devices.
2	18	12	*Traceroute*	Used in the enhanced implementation of the traceroute utility, as described in RFC 1393. Also see the topic on the ICMP Traceroute messages.

DZIĘKUJĘ ZA UWAGĘ!

NASTĘPNY WYKŁAD:

PROTOKOŁY ICMP, ARP, RARP;
ROUTING IP