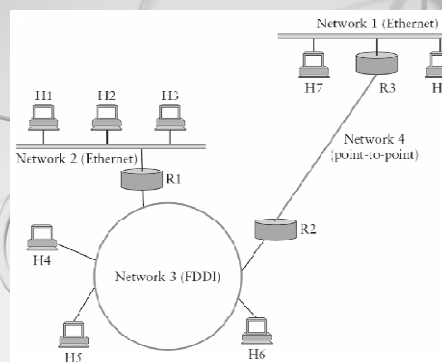


Piotr Kowalski
KAITI



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 jednoznaczna 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

A	0	Sieć (7 bitów)	Komputer (24 bity)
B	1 0	Sieć (14 bitów)	Komputer (16 bitów)
C	1 1 0	Sieć (21 bitów)	Komputer (8 bitów)
D	1 1 1 0	Adres grupowy (28 bitów)	
E	1 1 1 1 0	Zarezerwowane na przyszłość	

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
```

Sieci Komputerowe

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

Sieci Komputerowe

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 - 239.255.254.0	Transmisja grupowa	Brak podziału	Brak podziału	pierwsze cztery bity = 1110
E	-	-	240.0.0.0 - 255.255.255.255	Rezerwowane dla IETF	-	-	pierwsze cztery bity = 1111

Sieci Komputerowe

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 jedynekami np. 192.168.10.255 albo zerami (tzw. rozgłaszanie Berkeley-histeryczne) np. 192.168.10.0.
- **Adres rozgłaszania ograniczonego** – odnosi się do rozgłaszania w lokalnej sieci (używane przy starcie systemu). Prefiks i sufiks wypełniony jedynekami 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.

Sieci Komputerowe

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.

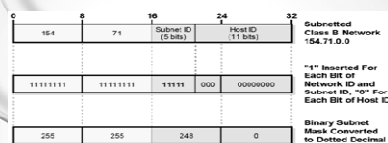
Sieci Komputerowe

Maski podsieci

Adres IP w podsieci składa się z czterech części:

- bitów określających klasę adresu,
- adresu sieci,
- adresu podsieci,
- adresu hosta

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



Sieci Komputerowe

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 Notation)	Subnet Address # Formula (N=1, ... # of Subnets-1)
0 (Default)	16	1	65,534	11111111.11111111.00000000.00000000 255.255.0.0	/16	—
1	15	2	32,768	11111111.11111111.10000000.00000000 255.255.128.0	/17	$x.y.N^*128.0$
2	14	4	16,384	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	2,048	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	$x.y.z.N^*0$
9	7	512	126	11111111.11111111.11111111.00000000 255.255.255.128	/25	$x.y.z.N^*128$
10	6	1,024	62	11111111.11111111.11111111.10000000 255.255.255.192	/26	$x.y.z.N^*64$
11	5	2,048	30	11111111.11111111.11111111.11000000 255.255.255.224	/27	$x.y.z.N^*32$
12	4	4,096	14	11111111.11111111.11111111.11100000 255.255.255.240	/28	$x.y.z.N^*16$
13	3	8,192	6	11111111.11111111.11111111.11110000 255.255.255.248	/29	$x.y.z.N^*8$
14	2	16,384	2	11111111.11111111.11111111.11111100 255.255.255.252	/30	$x.y.z.N^*4$

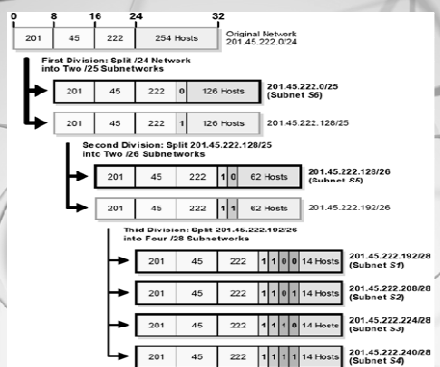
Sienci Komputerowe

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 Notation)	Subnet Address # Formula (N=1, ... # of Subnets-1)
0 (Default)	8	1	254	11111111.11111111.11111111.11000000 255.255.255.0	/24	—
1	7	2	126	11111111.11111111.11111111.11000000 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	$x.y.z.N^*4$

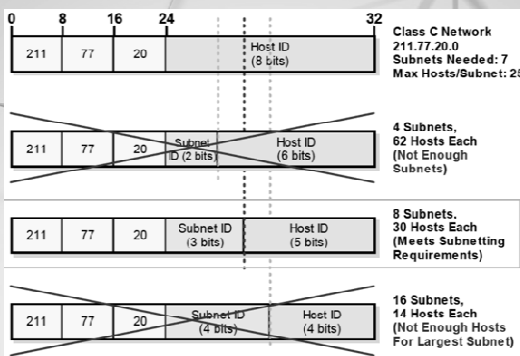
Sienci Komputerowe

Maski podsieci o zmiennej długości



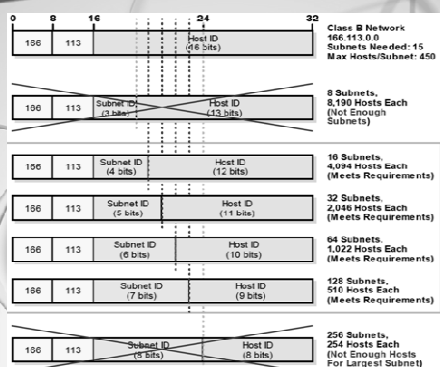
Sienci Komputerowe

Podział na podsieci – przykład 1 (łatwy)



Sienci Komputerowe

Podział na podsieci – przykład 2 (trudniejszy)



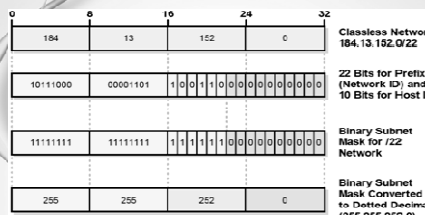
Sienci Komputerowe

Bezklasowy wybór tras między domenami (CIDR)

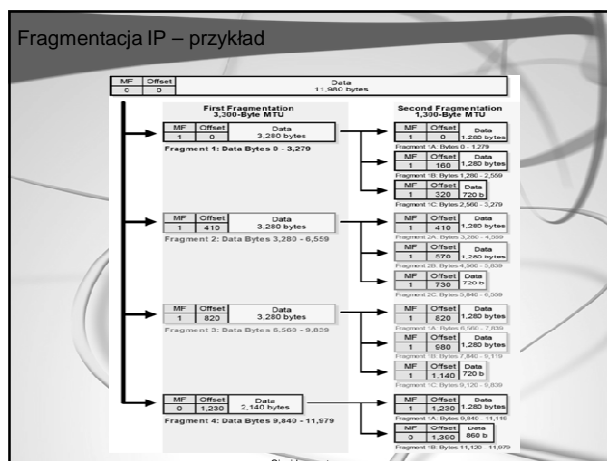
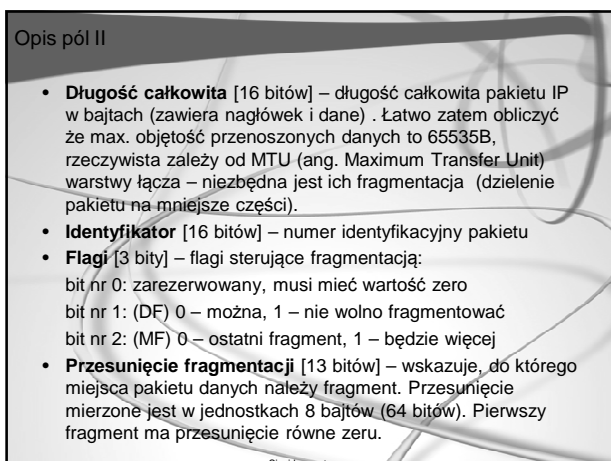
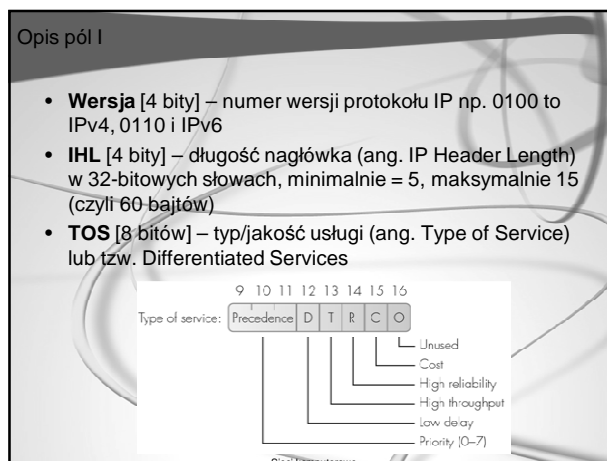
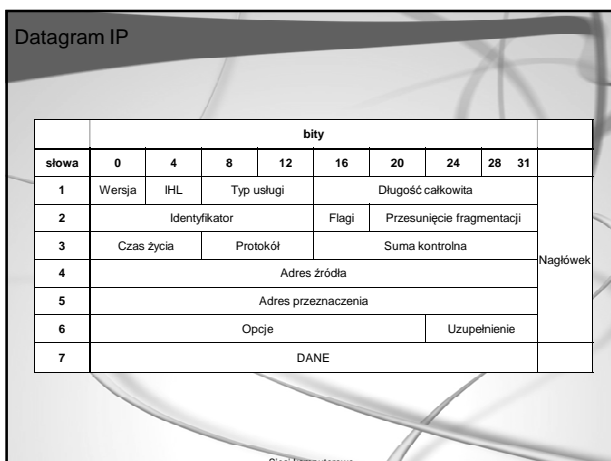
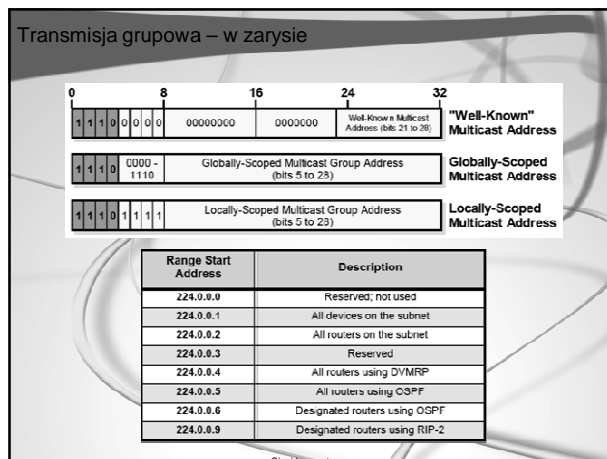
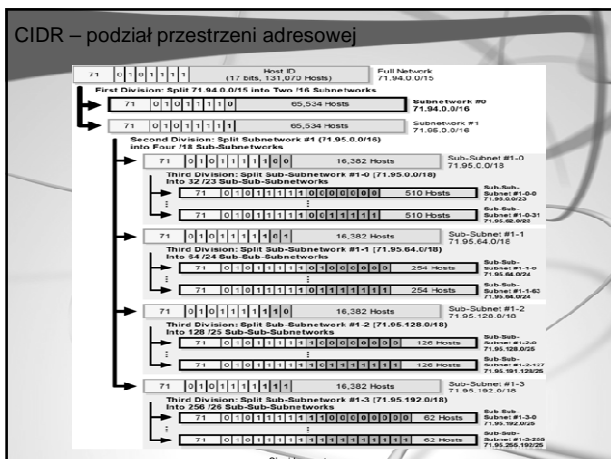
Adres IP z CIDR składa się z dwóch części:

- adresu sieci,
- adresu hosta

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



Sienci Komputerowe

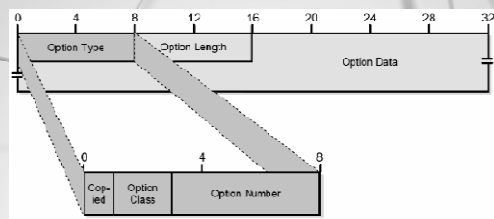


Opis pól III

- **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 odrzucony
- **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** [zmiennie] – opcje protokołu
- **Uzupełnienie** [32bity – długość pola opcji]
- **Dane** [zmiennie]

Sieci Komputerowe

Pole opcji – ogólny schemat



Sieci Komputerowe

Opcje IPv4 (dla docieklwych)

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 option pointers on 32-bit boundaries 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	4	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	5	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 the option is set by the originating device and cannot be enlarged by intermediate devices.
2	10	12	TraceRoute	Used in the enhanced implementation of the traceRoute utility, as described in RFC 1392. Also see the topic on the ICMP TraceRoute messages.

Sieci Komputerowe

DZIĘKUJĘ ZA UWAGĘ!

NASTĘPNY WYKŁAD:

PROTOKOŁY ICMP, ARP, RARP;
ROUTING IP

Sieci Komputerowe