



AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE

Sieci komputerowe

Protokoły warstwy sieciowej modelu OSI-ISO

dr inż. Andrzej Opaliński
andrzej.opalinski@agh.edu.pl

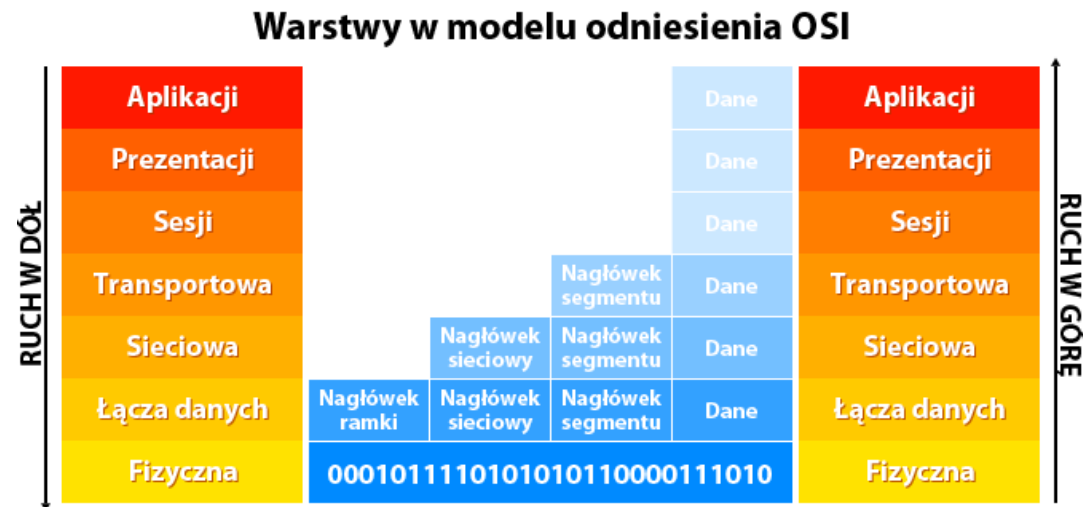
Plan wykładu

- Wprowadzenie
- Opis warstw
- Protokoły
 - IPX
 - AppleTalk (DDP)
 - Routing
 - IPsec
 - IP (IPv4, IPv6),
 - ICMP
 - IGMP
- Uzyskiwanie adresu IP
 - (R)ARP
 - BOOTP
 - DHCP



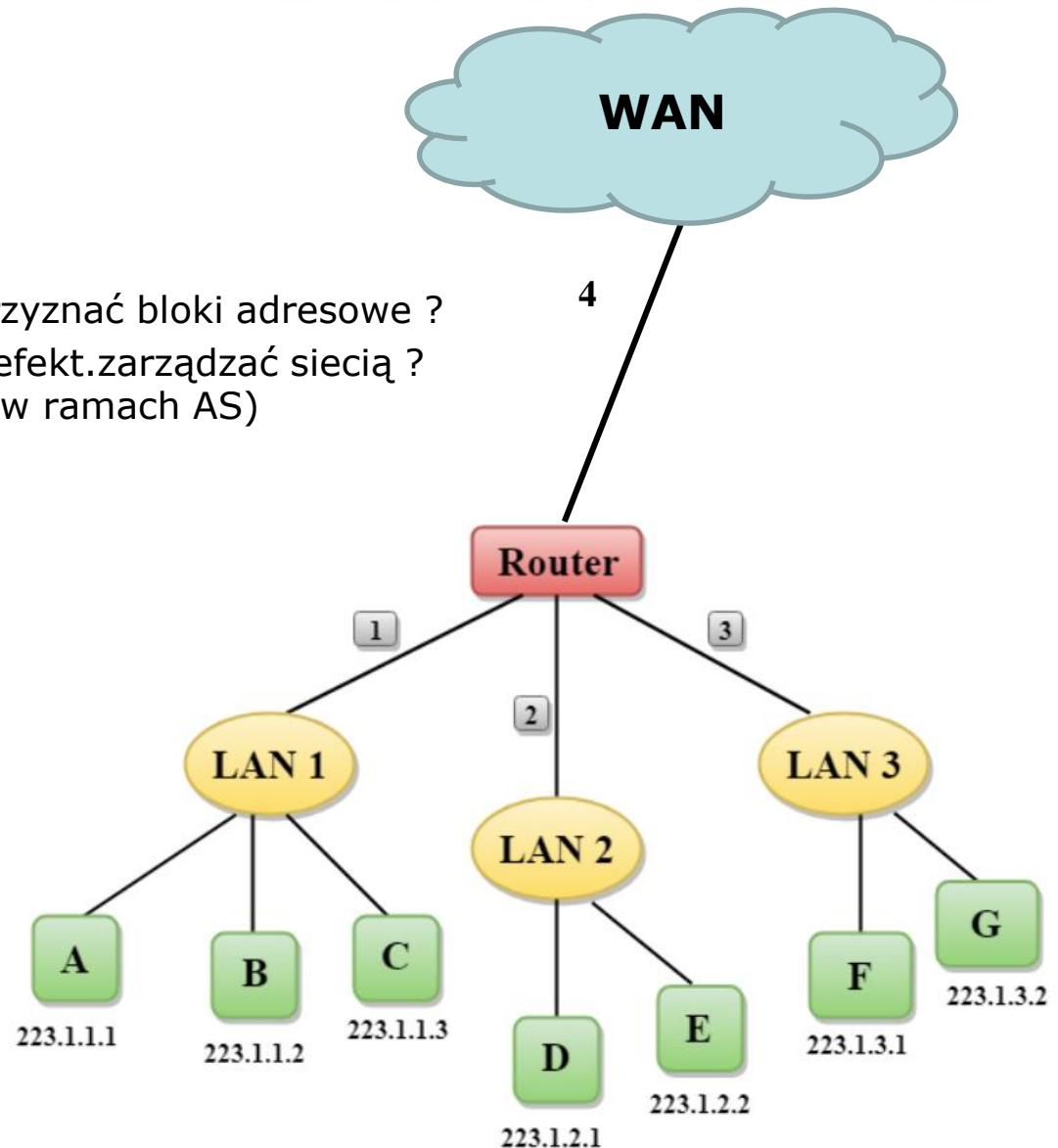
Wprowadzenie

- Warstwy niższe
 - Warstwa fizyczna
 - Zamiana danych w ramach na strumienie binarne
 - Szeregowy przesył strumienia bitów
 - Warstwa łącza danych
 - Pakowanie danych dla warstwy niższej (enkapsulacja)
 - Kontrola poprawności transmisji
 - Sterowanie dostępem do nośnika
- Warstwa sieciowa – umożliwienie komunikacji urządzeń znajdujących się w różnych sieciach lokalnych
 - Jednolita adresacja urządzeń w sieci
 - Mechanizmy trasowania
- Główne protokoły warstwy sieciowej:
 - IP (IPv4, IPv6),
 - ICMP
 - IGMP
 - IPsec
 - IPX
 - AppleTalk (DDP)
 - Routing



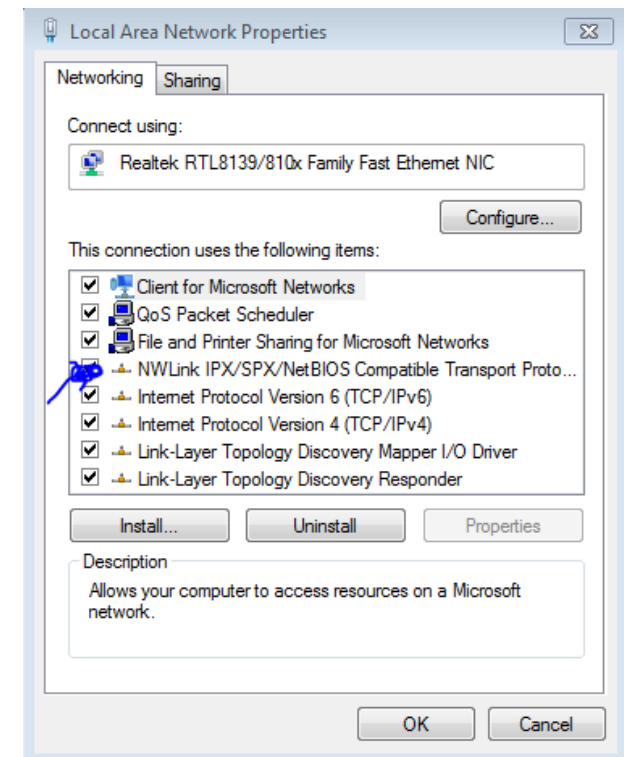
Po co adresacja sieci?

- Adresacja (protokoły)
(różne, nie tylko IPv4)
- Po co i dla kogo ?
 - Organizacje zarządzające – komu przyznać bloki adresowe ?
 - ISP/administratorzy - Jak budować/efekt.zarządzać siecią ?
(klasy/VLSM/pule prywatne/routing w ramach AS)
 - Hosty – czy to adres z mojej sieci ?
 - Routery – co zrobić z pakietem ?



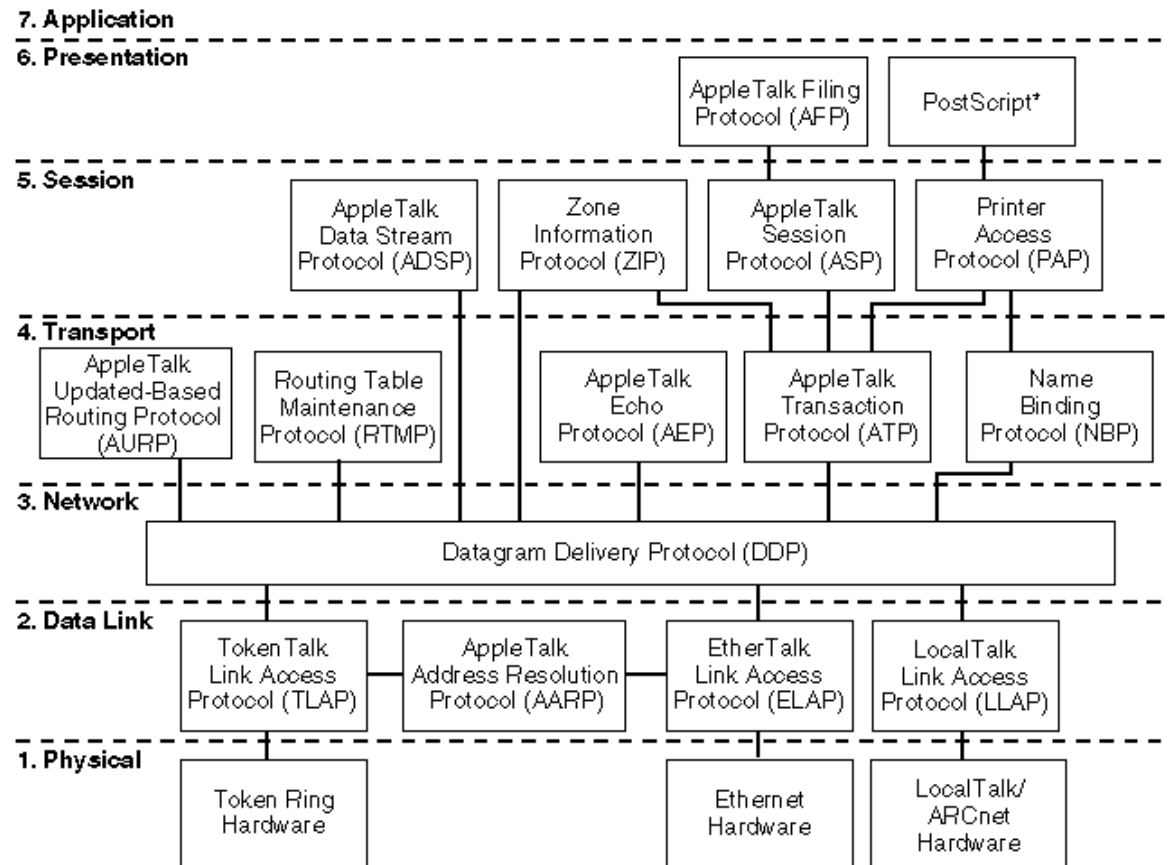
Protokół IPX

- IPX – Internetwork Packet Exchange
- Opracowany przez Novell na potrzeby środowiska sieciowego NetWare (współdziałający w warstwie transportowej z protokołem SPX)
 - Bezpołączeniowy,
 - bez mechanizmów kontroli transmisji
 - Bez gwarancji dostarczenia pakietów
- Popularny w latach 90tych XX wieku
- Wykorzystywany czasami w sieciach LAN ze względów bezpieczeństwa
 - Ruch zewnętrzny (IP), LAN (IPX)
 - Brak dostępu do hostów w sieci LAN poprzez IP
 - Użycie innego formatu ramki
- Brak natywnego wsparcia dla IPX
 - Windows XP 64 bit,
 - Windows Vista 32/64, 7, 8.* i 10
 - Mac OS – wersja 9.2 i wyższe
 - OpenBSD – 4.1 i wyższe



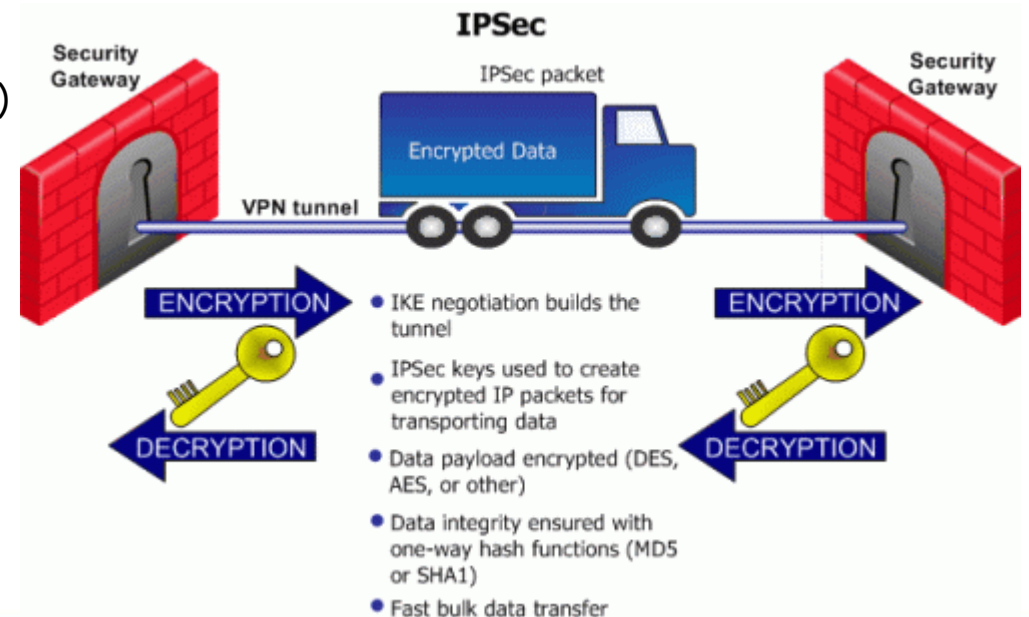
Protokół DDP – AppleTalk

- AppleTalk – pakiet protokołów komunikacyjnych
- Stworzony przez Apple w 1985 roku dla komputerów Macintosh
- W warstwie sieciowej – protokół DDP (Datagram Delivery Protocol)
 - Bezpołączeniowe przesyłanie datagramów
 - bez gwarancji dostarczenia
- Porzucony na rzecz stosu TCP/IP w 2009r.



Protokół IPsec

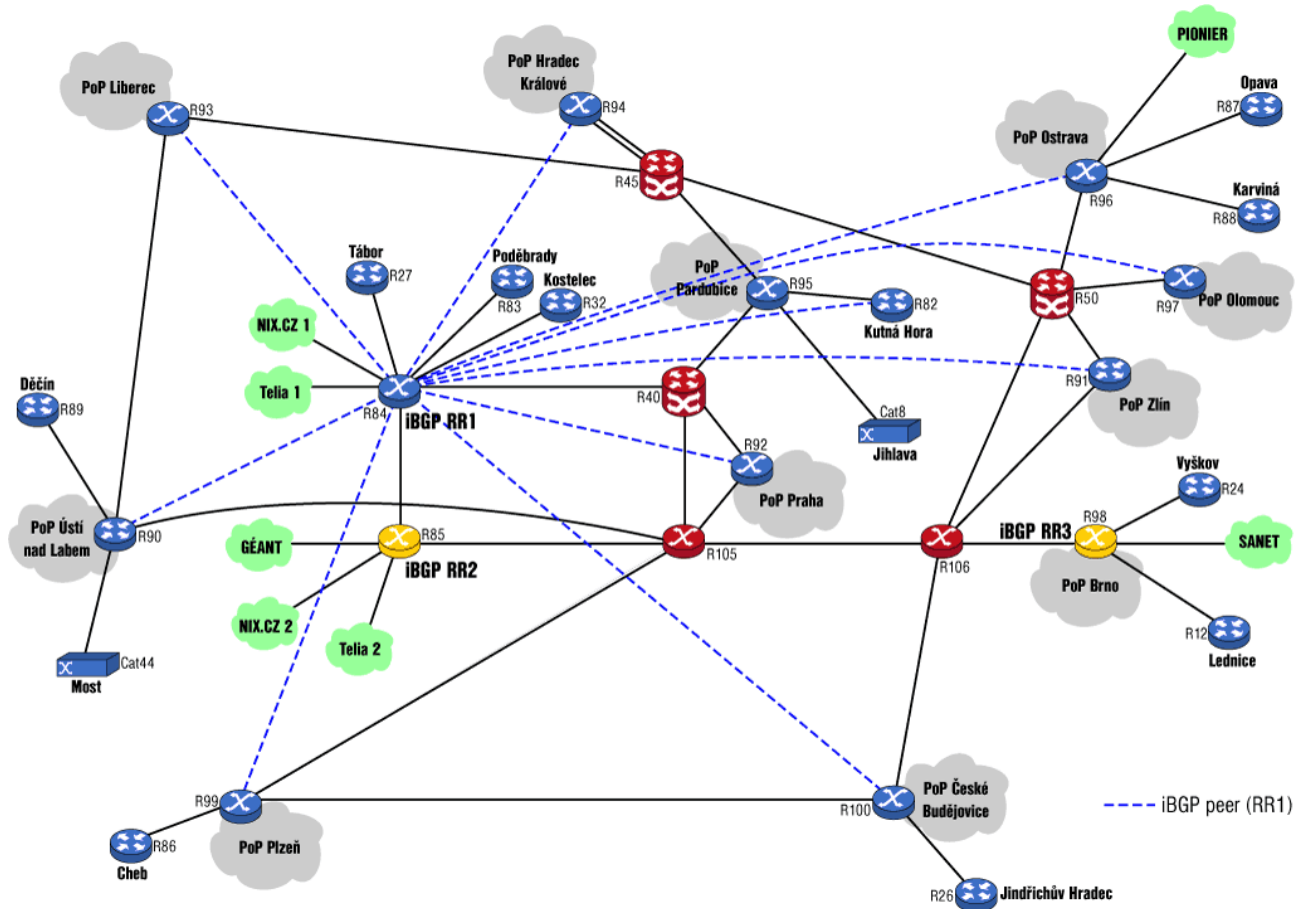
- IPsec – Internet Protocol Security, (IP Security)
- Implementacja bezpiecznych połączeń oraz wymiana kluczy szyfrowania
- Dwa kanały
 - Wymiana kluczy szyfrowania (uwierzytelnianie i szyfrowanie) (protokół UDP:500)
 - Transmisja danych (protokół ESP nr 50)
- Wykorzystywane do tworzenia sieci VPN (Virtual Private Network)
- Szyfrowanie pakietu IP i przesłanie go z dodatkowym nagłówkiem IPsec
- Omówiony na wykładzie dotyczącym bezpieczeństwa
- Klucze
 - Symetryczne (szybkie, problem z dystrybucją)
 - Asymetryczne (mniej efektywne)



Protokoły trasowania

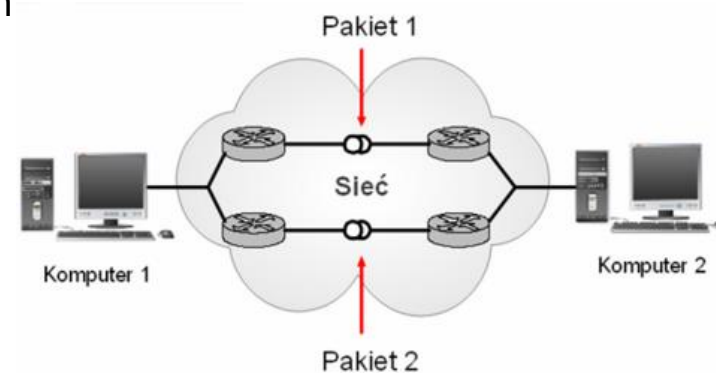
- Protokoły trasowania (routingu)
- Przekazywanie pakietów pomiędzy różnymi sieciami komputerowymi
- Omówione na osobnym wykładzie
- Protokoły:

- RIP,
- IGRP,
- EIGRP,
- OSPF,
- IS-IS,
- BGP.

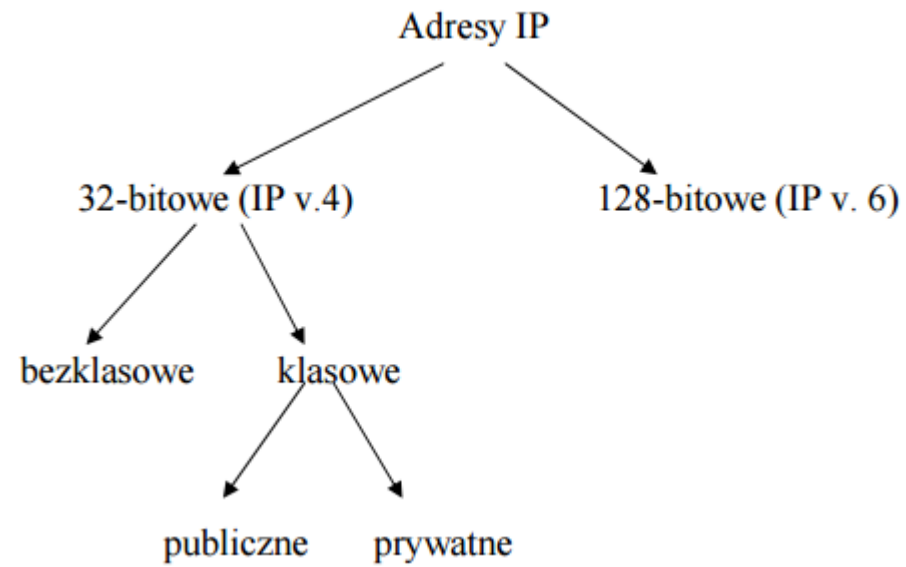


Protokół IP

- Protokół IP (Internet Protocol) – protokół komunikacyjny przeznaczony dla sieci Internet
- Zapewnia jednolitą adresację urządzeń w sieci
- Nie zapewnia:
 - Nie posiada mechanizmów sygnalizujących błędy
 - Nie posiada mechanizmów umożliwiających kontrolowanie przepływu pakietów
- Funkcje realizowane przez inne protokoły w oparciu o zapewnianą w ramach protokołu IP adresację:
 - wybór optymalnej trasy
 - przesłanie pakietów pomiędzy kolejnymi punktami sieci
 - wybór trasy alternatywnej w przypadku awarii sieci
- Protokół bezpołączeniowy
 - Brak nawiązania połączenia z hostem docelowym
 - Różne trasy pakietów
- Powszechnie stosowana wersja 4
- Wprowadzana wersja 6

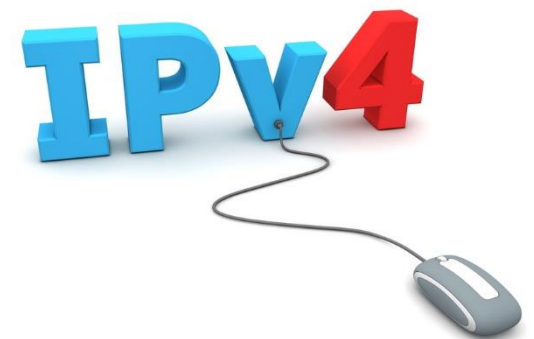


Adresowanie IP



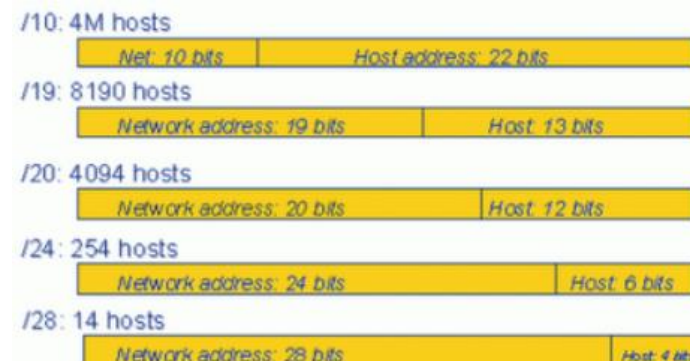
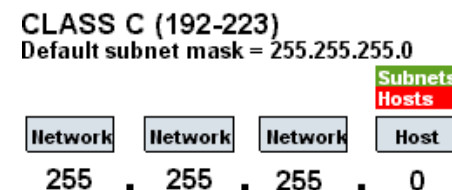
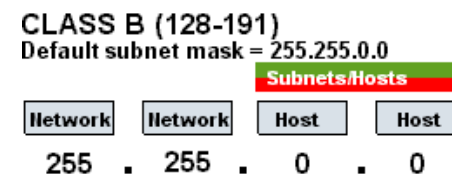
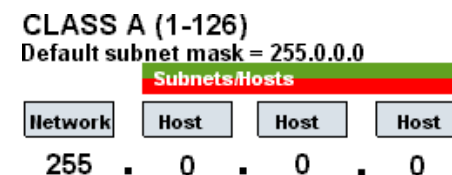
Adres IPv4

- Unikalny identyfikator pozwalający na komunikację w sieci Internet
- Tłumaczony na nazwę domenową za pomocą protokołu DNS (osobny wykład)
- W standardzie IPv4 – 32-bitowa liczba zapisywana w postaci 4 bajtów (oktetów)
- Kolejność zapisu – Big Endian (najbardziej znaczący („najcięższy”) bit jako pierwszy)
- Najpopularniejszy zapis – 4 dziesiętne liczby o 0 do 255 (2^8) oddzielone kropkami
- agh.edu.pl
 - 4 bajtowy format dziesiętny - 149.156.96.52
 - Dziesiętna wartość liczbową – 2 510 053 428
 - Wartość binarna: 10010101 10011100 01100000 00110100
 - Zapis szesnastkowy – 0x959C6034
- Liczba dostępnych adresów – 2^{32} (teoretycznie 4,29 mld)



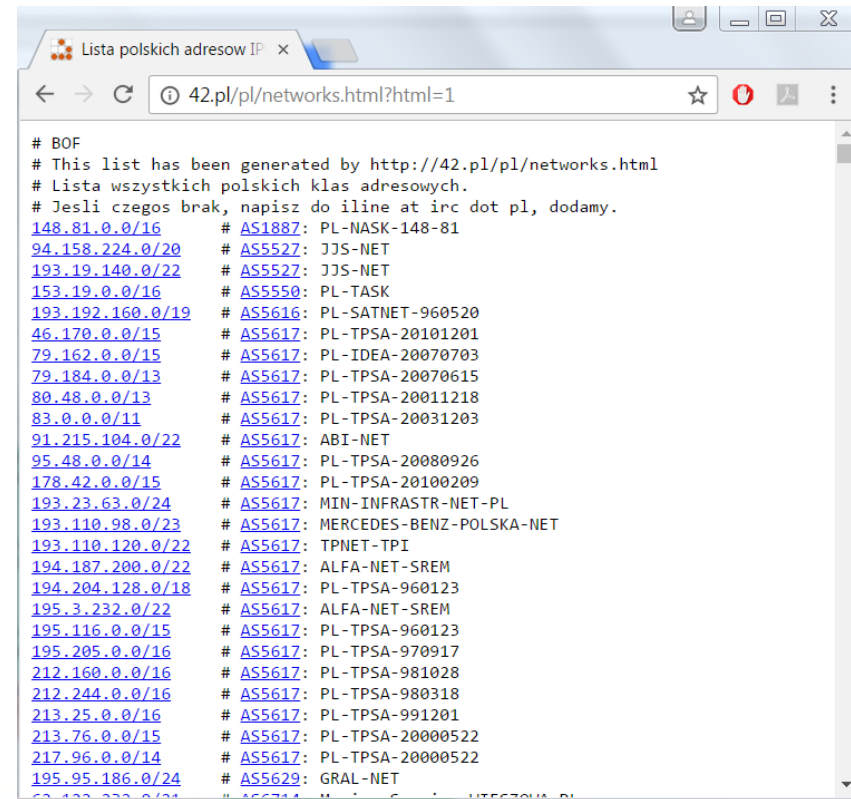
Adres IPv4 – adresy sieci i hostów

- Pula adresowa / blok adresowy – lista adresów IP do wykorzystania przez daną organizację (firmę, instytucję, osobę prywatną)
- Przeznaczona na adresy
 - Sieci
 - Hostów
 - Adresy specjalne
- Różne rodzaje pul adresowych
 - Adresacja klasowa – podział sztywny
 - 5 klas adresowych ze stałymi maskami
 - Adresacja bezklasowa
 - w oparciu o maskę wyznaczoną przez administratora sieci
 - Pula adresowa + maska – wyznacza rozmiar sieci (liczbę hostów)
- Maska (w skrócie)
 - Ciąg najstarszych bitów ustawionych na wartość 1 (11111111.11111111.0000000.0000000)
 - 32 bitowa liczba (tak samo jak adres IP)
 - Dla danej puli adresowej określa
 - Adres sieci
 - Adresy hostów
 - Adres rozgłoszeniowy



Adres IPv4 – bloki adresowe

- Globalny przydział – IANA (Internet Assigned Numbers Authority)
- Przydział lokalny
 - African Network Information Centre (AfriNIC) - dla Afryki.
 - American Registry for Internet Numbers (ARIN) - dla USA, Kanady, części Karaibów i Antarktyki.
 - Asia-Pacific Network Information Centre (APNIC) - dla Azji, Australii, Nowej Zelandii i Oceanii.
 - Latin America and Caribbean Network Information Centre (LACNIC) - dla Ameryki Łacińskiej
 - Réseaux IP Européens Network Coordination Centre (RIPE NCC) - dla Europy, Rosji, Bliskiego Wschodu i cent.Azji.
- Rozdział dla
 - Dostawców Internetu - ISP – Internet Service Provider
 - Organizacji rządowych
 - Placówek akademickich i naukowo badawczych
- Dla poszczególnych komputerów - przez ISP
- Lista polskich puli adresowych
<http://42.pl/pl/networks.html?html=1>
- Liczba dostępnych adresów – 2^{32}
(teoretycznie 4,29 mld)

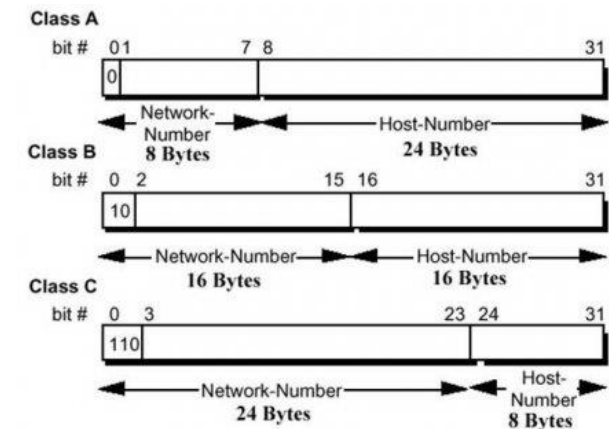


```
# BOF
# This list has been generated by http://42.pl/pl/networks.html
# Lista wszystkich polskich klas adresowych.
# Jesli czegos brak, napisz do inline at irc dot pl, dodamy.
148.81.0.0/16 # AS1887: PL-NASK-148-81
94.158.224.0/20 # AS5527: JJS-NET
193.19.140.0/22 # AS5527: JJS-NET
153.19.0.0/16 # AS5550: PL-TASK
193.192.160.0/19 # AS5616: PL-SATNET-960520
46.170.0.0/15 # AS5617: PL-TPSA-20101201
79.162.0.0/15 # AS5617: PL-IDEA-20070703
79.184.0.0/13 # AS5617: PL-TPSA-20070615
80.48.0.0/13 # AS5617: PL-TPSA-20011218
83.0.0.0/11 # AS5617: PL-TPSA-20031203
91.215.104.0/22 # AS5617: ABI-NET
95.48.0.0/14 # AS5617: PL-TPSA-20080926
178.42.0.0/15 # AS5617: PL-TPSA-20100209
193.23.63.0/24 # AS5617: MIN-INFRASTR-NET-PL
193.110.98.0/23 # AS5617: MERCEDES-BENZ-POLSKA-NET
193.110.120.0/22 # AS5617: TPNET-TPI
194.187.200.0/22 # AS5617: ALFA-NET-SREM
194.204.128.0/18 # AS5617: PL-TPSA-960123
195.3.232.0/22 # AS5617: ALFA-NET-SREM
195.116.0.0/15 # AS5617: PL-TPSA-960123
195.205.0.0/16 # AS5617: PL-TPSA-970917
212.160.0.0/16 # AS5617: PL-TPSA-981028
212.244.0.0/16 # AS5617: PL-TPSA-980318
213.25.0.0/16 # AS5617: PL-TPSA-991201
213.76.0.0/15 # AS5617: PL-TPSA-20000522
217.96.0.0/14 # AS5617: PL-TPSA-20000522
195.95.186.0/24 # AS5629: GRAL-NET
```

Klasy adresowe IPv4

- Klasę określa pierwszy Bajt adresu
- 5 klas
 - Klasa A – duże organizacje (127 sieci – 7 bitów) z bardzo dużą liczbą hostów (16 mln – 24 bity)
 - Klasa B – duża liczba organizacji (16 tys sieci – 14 bitów) z dużą liczbą hostów (65 tys – 16 bitów)
 - Klasa C – małe organizacje (2 mln sieci – 21 bitów), niewielka liczba hostów (256 – 8 bitów)
 - Klasa D – rozsyłanie grupowe pakietów
 - Klasa E – zarezerwowana do celów badawczych

Sposób wyróżnienia	Klasa	Zakres adresów	Bity maski/uwagi
Najstarszy bit 0	A	1.0.0.0 – 127.255.255.255	8
Najstarsze bity 10	B	128.0.0.0 – 191.255.255.255	16
Najstarsze bity 110	C	192.0.0.0 – 223.255.255.255	24
Najstarsze bity 1110	D	224.0.0.0 – 239.255.255.255	specjalne przeznaczenie
Najstarsze bity 1111	E	240.0.0.0 – 254.255.255.255	zarezerwowane



- Nieefektywne zarządzanie pulą adresów – maski jedynie 8,16,24 bity
- Podział historyczny (nieużywany od 1997 roku)
- Niedopasowanie do realnego zapotrzebowania
 - Nadmiarowość w organizacjach z małą liczną hostów (25 vs 256)
 - Brak adresów dla organizacji z dużą liczbą hostów (>255)
- Klasy zastąpione maskami – routing bezklasowy (CIDR)

Rozwiązywanie problemu niedoboru adresów IPv4

- Protokół zaprojektowany na początku lat 80 XX wieku
- Niewystarczająca pula wraz z rozwojem sieci
- Rozwiązania
 - Tworzenie podsieci
 - Zakres hostów dzielony na mniejsze podsieci z mniejszą liczbą hostów
 - Część bitów identyfikująca hosta identyfikowała podsieć
 - Podsieci o zmiennej długości maski
 - (VLSM – Variable Length Subnet Mask)
 - Podział klasy adresowej wewnątrz organizacji na mniejsze podsieci
 - Routery muszą przesyłać pełną informację o sieciach (łącznie z maskami)
 - (CIDR – Classless Inter-Domain Routing)
 - Bezklasowy routing międzydomenowy
 - Długość maski dopasowana do potrzeb podsieci (przez Internet Registry)
 - Działanie wielu podsieci w ramach jednej domeny trasowania
 - Mechanizmy adresów prywatnych
 - odfiltrowywanie przez routery
 - NAT (Network Address Translation) – ukrywanie adresów prywatnych, 1 adres publiczny

	CIDR	Maska	Liczba hostów
/1	128.0.0.0		2147483646
/2	192.0.0.0		1073741822
/3	224.0.0.0		536870910
/4	240.0.0.0		268435454
/5	248.0.0.0		134217726
/6	252.0.0.0		67108862
/7	254.0.0.0		33554430
/8	255.0.0.0		16777214
/9	255.128.0.0		8388606
/10	255.192.0.0		4194302
/11	255.224.0.0		2097150
/12	255.240.0.0		1048574
/13	255.248.0.0		524286
/14	255.252.0.0		262142
/15	255.254.0.0		131070
/16	255.255.0.0		65534
/17	255.255.128.0		32766
/18	255.255.192.0		16382
/19	255.255.224.0		8190
/20	255.255.240.0		4094
/21	255.255.248.0		2046
/22	255.255.252.0		1022
/23	255.255.254.0		510
/24	255.255.255.0		254
/25	255.255.255.128		126
/26	255.255.255.192		62
/27	255.255.255.224		30
/28	255.255.255.240		14
/29	255.255.255.248		6
/30	255.255.255.252		2

Adresacja bezklasowa - maska sieci

- Pozwala w elastyczny sposób dzielić duże sieci na mniejsze podsieci
- Składowe adresu
 - Adres sieci + hosta – adres sieci identyczny dla wszystkich hostów w danej sieci
- Wykorzystanie maski
 - 32 bity
 - 1 na najbardziej znaczących miejscach
 - podział adresu IP na bity określające:
 - sieć (początkowe, jedynki) – adres sieci - iloczyn bitowy maski i adresu IP
 - hosta (końcowe, zera)
 - Różne sposoby zapisu
 - w formacie binarnym, np. 11111111000000000000000000000000
 - W formacie dziesiętnym (z podziałem na 4 bajty) - 255.0.0.0
 - Określając liczbę bitów ustawionych na wartość 1 - /8
- Przykład:

```
11000000.10101000.01111011.10000100 - Adres IP (192.168.123.132)
11111111.11111111.11111111.00000000 - Maska podsieci (255.255.255.0)
```

```
11000000.10101000.01111011.00000000 - Adres sieci (192.168.123.0)
00000000.00000000.00000000.10000100 - Adres hosta (000.000.000.132)
```


Adresacja bezklasowa – VLSM i CIDR

- VLSM – Variable Length Subnet Mask -
- CIDR - Classless Inter-Domain Routing
- Bezklasowy przydział adresów IP
- Mechanizmem wymiany informacji o takim podziale
- Pozwala w elastyczny sposób dzielić duże sieci na mniejsze podsieci
- CIDR – dodatkowo agreguje trasy w tablicach routingu (jedna trasa dla wielu sieci)
- Przykład uelastyczniania bloku z klasy C: 200.200.200.0/24
 - Standardowo – 1 sieć, 256 adresów (254 hosty)
 - Przy zastosowaniu dłuższej maski (VLSM+CIDR)
 - Dla maski /25 – dwie podsieci po 128 adresów (126 hostów)
 - Dla maski /26 – cztery podsieci po 64 adresy (62 hosty)
 - Dla maski /27 – osiem podsieci po 32 adresy (30 hostów)
 - Dla maski /28 – 16 podsieci po 16 adresów (14 hostów)
 - Dla maski /29 – 32 podsieci po 8 adresów (6 hostów)
 - Dla maski /30 – 64 podsieci po 4 adresy (2 hosty)

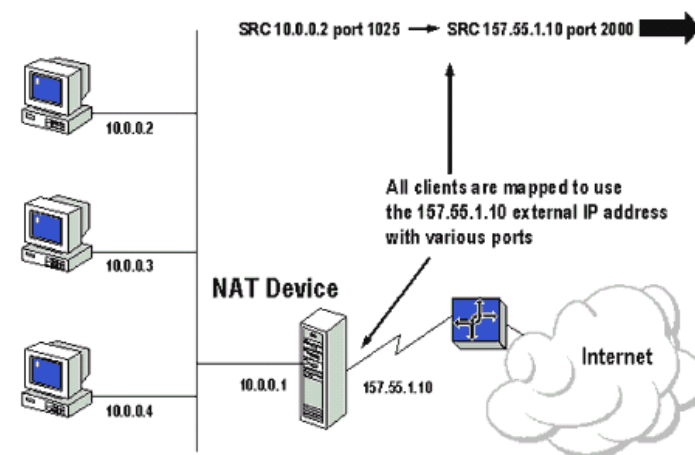
CIDR Maska Liczba hostów

CIDR	Maska	Liczba hostów
/1	128.0.0.0	2147483646
/2	192.0.0.0	1073741822
/3	224.0.0.0	536870910
/4	240.0.0.0	268435454
/5	248.0.0.0	134217726
/6	252.0.0.0	67108862
/7	254.0.0.0	33554430
/8	255.0.0.0	16777214
/9	255.128.0.0	8388606
/10	255.192.0.0	4194302
/11	255.224.0.0	2097150
/12	255.240.0.0	1048574
/13	255.248.0.0	524286
/14	255.252.0.0	262142
/15	255.254.0.0	131070
/16	255.255.0.0	65534
/17	255.255.128.0	32766
/18	255.255.192.0	16382
/19	255.255.224.0	8190
/20	255.255.240.0	4094
/21	255.255.248.0	2046
/22	255.255.252.0	1022
/23	255.255.254.0	510
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/29	255.255.255.248	6
/30	255.255.255.252	2

Prywatne adresy IP

- Pula prywatnych adresów IP
- Do wykorzystania jedynie w sieciach lokalnych
- Infrastruktura Internetu ignoruje te adresy (filtrowanie przez routery)
- Trzy bloki przestrzeni adresowych
 - 10.0.0.0 - 10.255.255.255 - dla sieci prywatnych klasy A (maska 255.0.0.0/8)
 - 172.16.0.0 - 172.31.255.255 - dla sieci prywatnych klasy B (maska 255.240.0.0/12)
 - 192.168.0.0 - 192.168.255.255 - dla sieci prywatnych klasy C (maska 255.255.0.0/16)
- Ułatwienie w routingu
 - Wewnętrzny (w ramach LAN)
 - Zewnętrzny (do sieci Internet) – maskowanie NAT (ukrywanie adresów lokalnych)

RFC1918 name	IP address range	number of addresses	classful description	largest CIDR block (subnet mask)	host id size
24-bit block	10.0.0.0 – 10.255.255.255	16,777,216	single class A	10.0.0.0/8 (255.0.0.0)	24 bits
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576	16 contiguous class Bs	172.16.0.0/12 (255.240.0.0)	20 bits
16-bit block	192.168.0.0 – 192.168.255.255	65,536	256 contiguous class Cs	192.168.0.0/16 (255.255.0.0)	16 bits

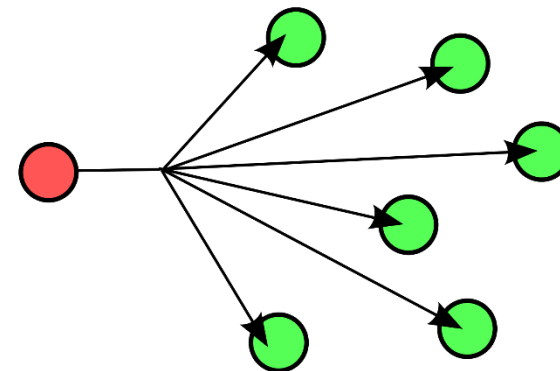


Ograniczenia adresowania IPv4

- 127.X.X.X – zarezerwowany dla lokalnej pętli zwrotnej
- identyfikator hosta – same jedynki - (adres rozgłoszeniowy)
 - Dla maski 24 bitowej, np. 192.168.1.255
 - zarezerwowane do rozsyłania komunikatów typu broadcast
 - Dla adresacji bezklasowej – ostatni adres z puli adresowej hostów
- Identyfikator hosta – same zera - (adres sieci)
 - adres sieci w której znajduje się host
 - Dla maski 24 bitowej, np. 192.168.1.0
 - Adresacja bezklasowa – pierwszy adres z puli adresowej hostów
- Identyfikator hosta (adres IP) nie może powtórzyć się w sieci (paraliż ruchu pakietów)
- Ograniczona użyteczna liczba hostów w sieci – $2^n - 2$ (sieć, broadcast)

Adres rozgłoszeniowy IPv4

- Adres broadcast – rozgłoszeniowy
- Rozsyłanie pakietów do wszystkich hostów w danej sieci
- W sieci lokalnej (warstwa łącza danych)
 - w oparciu o MAC FF:FF:FF:FF:FF:FF
 - protokół ARP (przekształcanie adresów sieciowych MAC na adresy IP)
- W adresowaniu IP (warstwa sieci)
 - W adresacji klasowej ostatnie 1,2,3 bajty adresu
 - Przykład, dla adresu klasy C
 - Adres IP – 192.190.1.100
 - Adres sieci – 192.190.1.0
 - Maska – 255.255.255.0
 - Adres rozgłoszeniowy – 192.190.1.255
 - W adresacji bezklasowej
 - W oparciu o adres IP hosta i maskę podsieci
 - Wstawienie w adres IP jedynek na ostatnich miejscach, gdzie w masce są zera
 - Przykład dla adresu IP: 212.51.219.32 i maski: 255.255.255.192



`11010100.00110011.11011011.00100000` adresIP

`11111111.11111111.11111111.11000000` maska

`11010100.00110011.11011011.00111111` broadcast

broadcast= 212.51.219.63

Podsieci - przykład

- Podział sieci klasy C na 4 podsieci po 62 komputery (+ sieć + broadcast)
- Pula adresowa z klasy C – 198.200.55.0 (jedna sieć, 254 hosty)
 - Adres komputera w klasie C – 1 bajt, 8 bitów
 - Na adresowanie 4 podsieci potrzeba 2 bity – 00, 01, 10, 11 (z przodu)
 - Maska – 255.255.255.192 (192 = 11000000)
- Adresy w poszczególnych podsieciach:

Adres dwójkowy podsieci	Adres dziesiętny podsieci	Numer podsieci	Adres początkowy	Adres końcowy	Adres ogłoszeniowy
00 000000 – 00 111111	198.200.55.0	Podsieć 0	198.200.55.1	198.200.55.62	198.200.55.63
01 000000 – 01 111111	198.200.55.64	Podsieć 1	198.200.55.65	198.200.55.126	198.200.55.127
10 000000 – 10 111111	198.200.55.128	Podsieć 2	198.200.55.129	198.200.55.190	198.200.55.191
11 000000 – 11 111111	198.200.55.192	Podsieć 3	198.200.55.193	198.200.55.254	198.200.55.255

Zadanie

- Dostępna pula adresowa sieci klasy C – 198.200.100.0 (jedna sieć, 254 hosty)
- Požadany podział na 6 podsieci po minimum 20 hostów
- Zadanie
 - Dokonać podziału na podsieci
 - Podać adres dziesiętny podsieci i adres rozgłoszeniowy



Zadanie

- Dostępny adres sieci klasy C – 198.200.100.0
- Požadany podział na 6 podsieci po minimum 20 hostów
- Zadanie
 - Dokonać podziału na podsieci
 - Podać adres dziesiętny podsieci i adres rozgłoszeniowy
- Liczba dodatkowych bitów na podział na 6 podsieci – ?

Zadanie

- Dostępny adres sieci klasy C – 198.200.100.0
- Pożyczany podział na 6 podsieci po minimum 20 hostów
- Zadanie
 - Dokonać podziału na podsieci
 - Podać adres dziesiętny podsieci i adres rozgłoszeniowy
- Liczba dodatkowych bitów na podział na 6 podsieci – 3
 - 000 – 0
 - 001 – 1
 - 010 – 2
 - 011 – 3
 - 100 – 4
 - 101 – 5

Zadanie

- Dostępny adres sieci klasy C – 198.200.100.0
- Pożyczany podział na 6 podsieci po minimum 20 hostów
- Zadanie
 - Dokonać podziału na podsieci
 - Podać adres dziesiętny podsieci i adres rozgłoszeniowy
- Liczba dodatkowych bitów na podział na 6 podsieci – 3
 - 000 – 0
 - 001 – 1
 - 010 – 2
 - 011 – 3
 - 100 – 4
 - 101 – 5
- Maski podsieci: (bitowo/dziesiętnie/liczba bitów) : ???

Zadanie

- Dostępny adres sieci klasy C – 198.200.100.0
- Pożyczany podział na 6 podsieci po minimum 20 hostów
- Zadanie
 - Dokonać podziału na podsieci
 - Podać adres dziesiętny podsieci i adres rozgłoszeniowy
- Liczba dodatkowych bitów na podział na 6 podsieci – 3
 - 000 – 0
 - 001 – 1
 - 010 – 2
 - 011 – 3
 - 100 – 4
 - 101 – 5

Adresy podsieci, adresy rozgłoszeniowe ?

- Maski podsieci: (bitowo/dziesiętnie/liczba bitów) :
11111111.11111111.11111111.11100000 / 255.255.255.224 / 27

Zadanie

- Dostępny adres sieci klasy C – 198.200.100.0
- Pożyczany podział na 6 podsieci po minimum 20 hostów
- Zadanie
 - Dokonać podziału na podsieci
 - Podać adres dziesiętny podsieci i adres rozgłoszeniowy
- Liczba dodatkowych bitów na podział na 6 podsieci – 3

- 000 – 0 .000 00000 – 192.200.100.0
 .000 11111 - 192.168.100.31
- 001 – 1 .001 00000 – 192.200.100.32
 .001 11111 - 192.168.100.63
- 010 – 2 .010 00000 – 192.200.100.64
 .010 11111 - 192.168.100.95
- 011 – 3 .011 00000 – 192.200.100.96
 .011 11111 - 192.168.100.127
- 100 – 4 .100 00000 – 192.200.100.128
 .100 11111 - 192.168.100.159
- 101 – 5 .101 00000 – 192.200.100.160
 .101 11111 - 192.168.100.191

Liczba i adresy hostów w podsieciach : ?

- Maski podsieci: (bitowo/dziesiętnie/liczba bitów) :
11111111.11111111.11111111.11100000 / 255.255.255.224 / 27

Zadanie

- Dostępny adres sieci klasy C – 198.200.100.0
- Pożyczany podział na 6 podsieci po minimum 20 hostów
- Zadanie
 - Dokonać podziału na podsieci
 - Podać adres dziesiętny podsieci i adres rozgłoszeniowy
- Liczba dodatkowych bitów na podział na 6 podsieci – 3

– 000 – 0	.000 00000 – 192.200.100.0 .000 11111 - 192.168.100.31
– 001 – 1	.001 00000 – 192.200.100.32 .001 11111 - 192.168.100.63
– 010 – 2	.010 00000 – 192.200.100.64 .010 11111 - 192.168.100.95
– 011 – 3	.011 00000 – 192.200.100.96 .011 11111 - 192.168.100.127
– 100 – 4	.100 00000 – 192.200.100.128 .100 11111 - 192.168.100.159
– 101 – 5	.101 00000 – 192.200.100.160 .101 11111 - 192.168.100.191

Liczba i adresy hostów w podsieciach :
- 30 hostów w każdej podsieci

- Maski podsieci: (bitowo/dziesiętnie/liczba bitów) :
11111111.11111111.11111111.11100000 / 255.255.255.224 / 27

Protokół IPv4

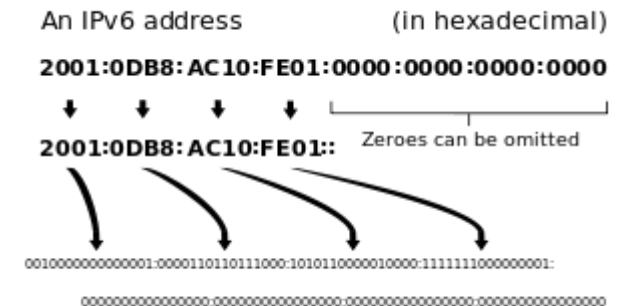
Budowa datagramu protokołu IPv4

- 4 bity – wersja protokołu
- 4 bity – długość nagłówka
- 8 bitów – typ usługi (Type of Service) – poziom ważności i zapotrzebowanie na jakość obsługi
- 16 bitów – całkowita długość datagramu w bajtach (min.72 B, maks 64 kB)
- 16 bitów – sekwencyjny numer bieżącego datagramu
- 3 bity – flagi – sterowanie fragmentacją
 - 1 bit – zawsze 0
 - 2 bit (0 – pakiet może być dzielony na fragmenty, 1 – pakiet nie może być dzielony na fragmenty)
 - 3 bit (0 – pakiet ze środka, 1 – ostatni pakiet z podziału)
- 13 bitów – przesunięcie pakietu
- 8 bitów – czas życia pakietu, liczba routerów (zmniejszana przez routery, 0 – odrzucenie pakietu)
- 8 bitów – typ protokołu warstwy wyższej (1-ICMP, 2-IGMP, 6-TCP, 8-EGP, 17-UDP)
- 16 bitów – suma kontrolna integralności nagłówka
- 32 bity – adres nadawcy
- 32 bity – adres odbiorcy
- 32 bity - opcje – pole specjalne
- dopełnienie nagłówka do wielokrotności 32 bitów
- Kolejne pola do maks 64kB – dane z warstw wyższych

+	Bity 0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Wersja	Długość nagłówka	Typ usługi	Całkowita długość	
32	Numer identyfikacyjny			Flagi	Kontrola przesunięcia
64	Czas życia pakietu (TTL)	Protokół warstwy wyższej	Suma kontrolna nagłówka		
96	Adres źródłowy IP				
128	Adres docelowy IP				
160	Opcje IP			Uzupełnienie	
192	Dane				

Adres IPv6

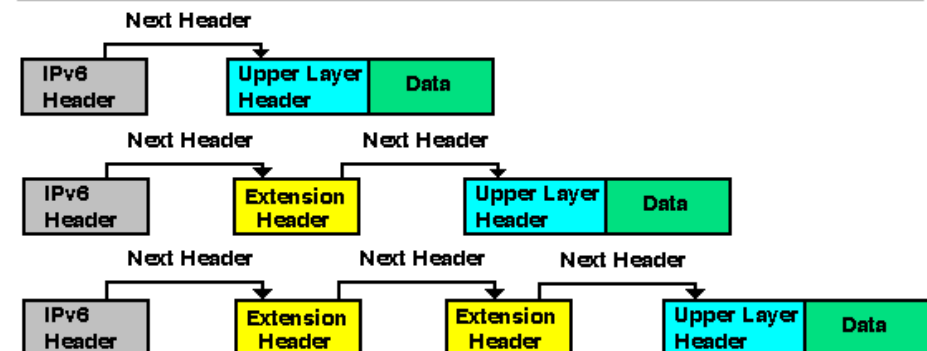
- Powstał ze względu na kończącą się pulę adresów IP (IANA rozdzieliła pulę ostatnich adresów v4 3 lutego 2011 roku)
- Zapotrzebowanie na adresy IP urządzeń peryferyjnych
- IPv4 – $2^{32} = 4,29$ mld adresów
- IPv6 - adres zapisywany na 128 bitach (16 Bajtach)
 - $2^{128} = 3,4 \times 10^{38}$ – 340 trylionów
 - Pokrycie powierzchni ziemi adresami IP = $6,7 \times 10^{17}$ na m² (6 mld adresów IPv6 na osobę)
- Technologie wymagające stałych parametrów łącza
 - Telewizja cyfrowa
 - Video on Demand
- Potrzeba autoryzacji
- Konieczność zapewnienia zgodności – tunelowanie IPv6 w IPv4
- Format adresu – 8 x 16 bitowych bloków
 - Preferowana forma szesnastkowa z dwukropkiem co 16 bitów (0432:5678:abcd:00ef:0000:0000:1234:4321)
 - Dopuszczane omijanie zer wiodących (432:5678:abcd:ef::1234:4321)
 - W infrastrukturze mieszanej dopuszczane zapisywanie ostatnich 32 bitów w wersji dziesiętnej (0:0:0:0:0:FFFF:129.144.52.38)



Adres IPv6 – budowa nagłówka datagramu

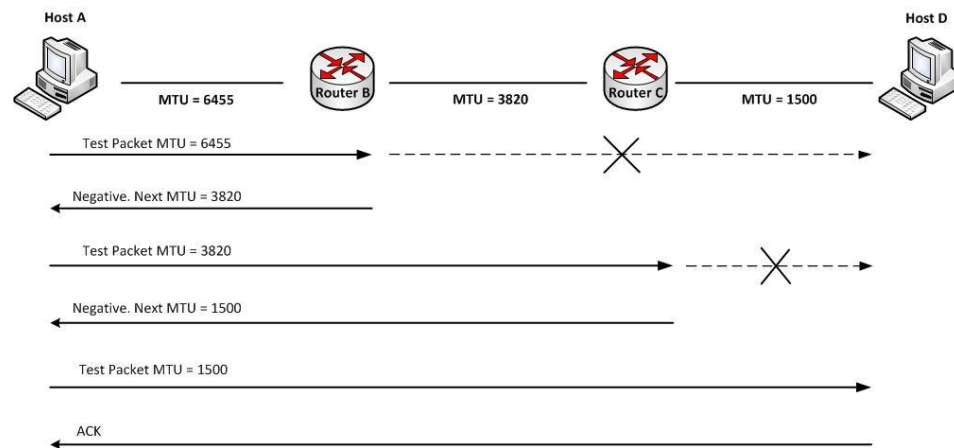
- Stała długość nagłówka (40 bajtów)
- Nagłówek prostszy i łatwiejszy w przetwarzaniu od nagłówka IPv4
- Dodatkowe opcje w nagłówkach rozszerzających
- Budowa podstawowego nagłówka:
 - 4 bity – wersja
 - 8 bitów – klasa ruchu (następca pola Type of Service)
 - 20 bitów – etykieta przepływu – dla pakietów wymagających oddzielnego traktowania
 - 16 bitów – wielkość pakietu bez nagłówka podstawowego (z ew. nagłówkiem opcjonalnym)
 - 8 bitów – typ następnego nagłówka (nagłówek rozszerzający lub warstwy wyższej)
 - 8 bitów – limit przeskoków – stary TTL – ilość przejść routerów przed odrzuceniem pakietu
 - 128 bitów – adres źródłowy hosta
 - 128 bitów – adres docelowy hosta
- Nagłówki rozszerzające
 - Nagłówek routingu
 - Nagłówek fragmentacji
 - Nagłówek opcji docelowych
 - Nagłówek uwierzytelniania
 - Encrypted security payload

Bity	0-3	4-7	8-11	12-15	16-19	20-23	24-27	28-31
0	Wersja	Klasa ruchu	Etykieta przepływu					
32	Długość danych			Następny nagłówek		Limit przeskoków		
64	Adres źródłowy (128 bitów)							
96								
128								
160								
192	Adres docelowy (128 bitów)							
224								
256								
288								



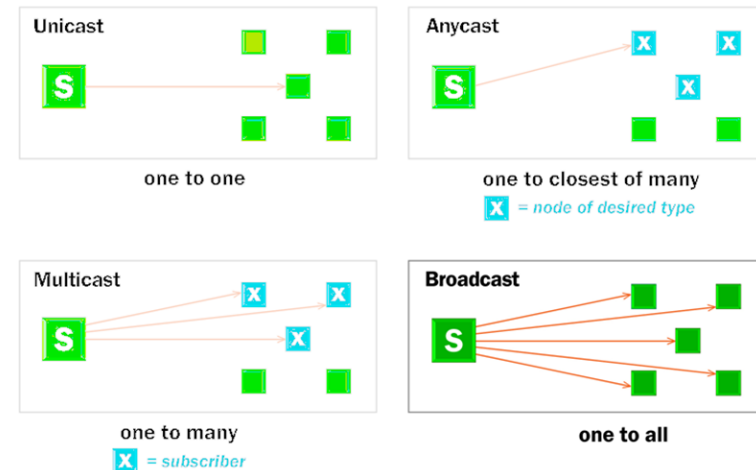
Adres IPv6 – zwiększenie wydajności

- Uproszczona struktura nagłówka – optymalizacja przetwarzania przez routery
 - adres IPv4 * 4 = adres IPv6,
 - nagłówek pakietu IPv4 = 2* nagłówek pakietu IPv6
- Brak fragmentacji pakietów IPv6
 - Urządzenia końcowe ustalają maksymalny rozmiar pakietu (Path MTU)
 - Przy braku ustalonego Path MTU – pakiety mniejsze niż 1280 bajtów
- Brak sumy kontrolnej nagłówka IPv6
 - Spójność w nagłówkach warstw wyższych
 - Routery nie przetwarzają sum kontrolnych
- Rozszerzenia dowolnej wielkości w IPv6
 - W IPv4 stała długość – 40 bajtów
 - Mniej pakietów kontrolnych
- Większy rozmiar pojedynczego pakietu
 - IPv4 do 64 kB danych
 - IPv6 – opcjonalne Jumbogramy (JumboFrame) – do 4GB (nagłówek Jumbo Payload Option)
- Poprawa bezpieczeństwa
 - IPv6 – integracja zabezpieczeń (szyfrowanie i uwierzytelnianie) na poziomie protokołu
 - Obowiązkowa obsługa protokołu IPSec



Typy adresów IPv6

- Brak adresu rozgłoszeniowego (broadcast)
- Global Unicast – identyfikator pojedynczego interfejsu
Routowalny w Internecie.
Pierwsze 64 bity – adres sieci (w tym 16b na podsieć)
Pozostałe 64 bity – adres hosta
- Unique Local – odpowiednik adresu prywatnego IPv4
8 bitów – FD (hex)
40 bitów – dowolny adres sieci
16 bitów – adres podsieci
64 bity – adres hosta
- Uniwersalny (Anycast) – zbiór wielu interfejsów należących do różnych węzłów sieci.
Pakiet dostarczany tylko na jeden z interfejsów z tego zbioru (najbliższy w rozumieniu metryki)
- Grupowy (Multicast) – identyfikator zbioru interfejsów. Pakiet przekazywany do każdego z interfejsów ze zbioru. (Wszystkie urządzenia FF02::1, Wszystkie routery FF02::2, OSPF: FF02::5 oraz FF02::6, EIGRP FF02::A)
- Specjalne pule adresowe:
 - `::/128` - adres zerowy, wykorzystywany tylko w oprogramowaniu
 - `::1/128` - adres pętli zwrotnej (odpowiednik loopback IPv4)
 - `::/96` - adresy kompatybilne z adresem IPv4 dla hosta korzystającego z IPv6 i IPv4
 - `::ffff:0:0/96` - adresy kompatybilne z adresem IPv4 dla hosta korzystającego wyłącznie z IPv4
 - `Ff00::/8` - adresy typu link-local – wykorzystywane wewnątrz sieci lokalnych



Adresy IPv6 – c.d.

- Autokonfiguracja sieci LAN

- Stateless Address Auto Configuration (SLAAC) i EUI-64
- Router dostarcza 64 bitowy prefix adresu
- Druga część adresu w oparciu o adres MAC
- Adres dla MAC (10:22:33:44:55:66) ma postać (64bitowy_prefix_sieci:1222:33FF:FE44:5566)
(zmiana 7 bitu pierwszej połowy MAC na przeciwny i dodanie wartości FFFE)

Prefix uzyskany od routera	Pierwsza połowa MAC	FFFE	Druga połowa MAC
----------------------------	---------------------	------	------------------

- Niebezpieczeństwo – adres MAC sprzętu widoczny w sieci Internet
(zabezpieczenia: włączenie rozszerzeń prywatności i dynamiczny przydział IP dla urządzeń klienta)

- Aktualna sytuacja

- W dalszym ciągu mniej popularny od adresacji IPv4
- W 2018 jedynie 28% spośród 1 000 i 17% spośród 1 000 000 najpopularniejszych witryn WWW wspiera IPv6

Protokół ICMP

- IP – protokół zawodny – nie sprawdza czy dane dotarły do adresata
- Obsługa w protokołach warstw wyższych
- W warstwie sieci można sprawdzić dostępność sieci docelowej – ICMP (Internet Control Message Protocol) RFC 792
- Zadanie:
 - **zgłaszanie braku łączności**,
 - nie naprawa !!,
 - nie potwierdzanie dotarcia !!,
- Wysyłanie komunikatów ICMP najczęściej przez bramy lub hosty
 - Lepsza trasa dla pakietów – komunikat o lepszej trasie do źródła (wysyłany przez router)
 - Host docelowy nieosiągalny – brama wysyła komunikat o niedostępności adresata
 - TTL = 0 – router zgłasza komunikat do źródła i odrzuca pakiet
- Narzędzia diagnostyczne wykorzystujące ICMP
 - Ping
 - Traceroute / tracert

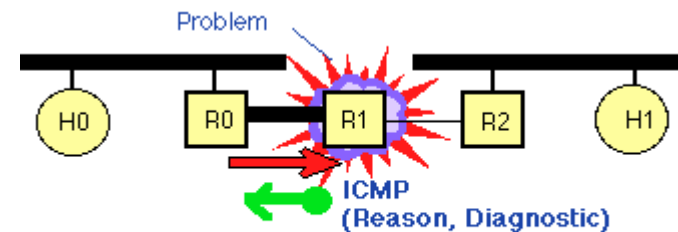
```
C:\Users\opal>tracert nokia.com

Tracing route to nokia.com [147.243.14.149]
over a maximum of 30 hops:

  0  9 ms  2 ms  3 ms  b6rtr.agh.edu.pl [149.156.112.125]
  1  41 ms 11 ms  2 ms  b6rtr.agh.edu.pl [149.156.112.125]
  2   1 ms  5 ms  2 ms  149.156.6.222
  3   3 ms  1 ms  2 ms  149.156.0.217
  4  10 ms 10 ms 10 ms  z-krakowa.poznan-gw3.10Gb.rtr.pionier.gov.pl [212.191.224.69]
  5  24 ms 21 ms 21 ms  de-hmb.nordu.net [109.105.98.124]
  6  33 ms 35 ms 30 ms  nl-sar.nordu.net [109.105.97.17]
  7  33 ms 32 ms 32 ms  uk-hex.nordu.net [109.105.97.125]
  8  33 ms 32 ms 45 ms  195.66.225.94
  9  66 ms 63 ms 62 ms  gb-lon-colo1-bbrtr01-te-2-1.as1248.net [131.228.129.153]
 10 62 ms 63 ms 63 ms  nl-ams-colo-bbrtr02-te-2-3.as1248.net [131.228.128.13]
 11 62 ms 63 ms 63 ms  nl-ams-colo-bbrtr01-te-1-4.as1248.net [131.228.128.1]
 12 66 ms 62 ms 62 ms  fi-sal-kiila-bbrtr01-te-2-3.as1248.net [131.228.128.94]
 13 65 ms 63 ms 62 ms  fi-sal-kiila-dc02-xe-0-0-0.as1248.net [131.228.130.166]
 14
```

Dostarczanie komunikatów ICMP

- Przesyłane w datagramie IP
- Enkapsulacja do postaci pakietów IP -> do ramki warstwy drugiej
- Ramka ICMP
 - Typ - typ komunikatu
 - Kod - podtyp w ramach typu
 - Suma kontrolna - obliczana na podstawie nagłówka
 - Dane - wypełnione w zależności od typu wiadomości
- Typy wiadomości ICMP (przykładowe)
 - 0 - echo replay - odpowiedź na „ping”
 - 3 - nieosiągalne miejsce przeznaczenia
 - 5 - zmień trasowanie
 - 8 - echo request - żądanie echa
 - 9 - ogłoszenie routera
 - 11 - przekroczenie limitu czasu
 - 17 - żądanie maski adresowej
 - 18 - zwrot maski adresowej

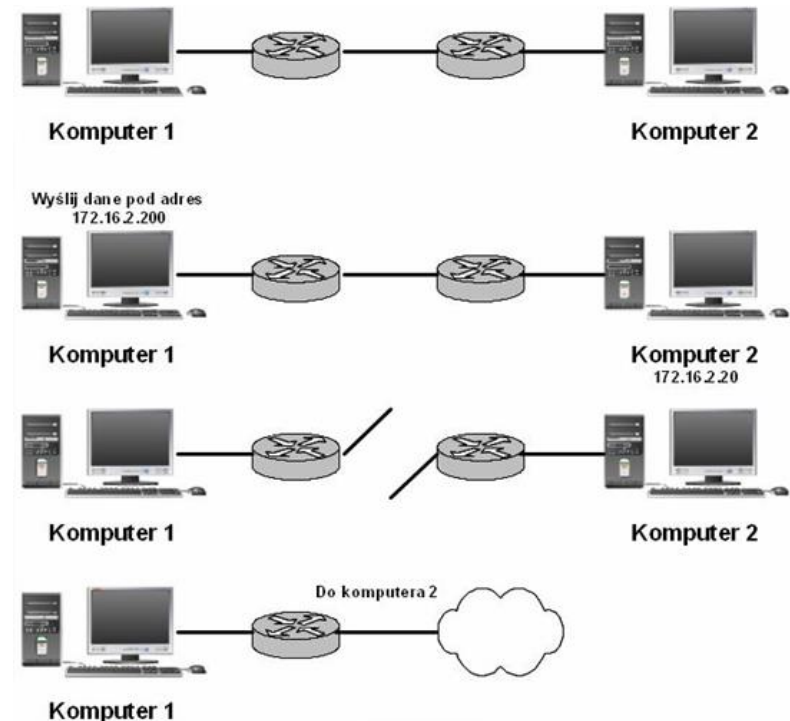


Przykładowe komunikaty ICMP

- Echo request i echo response
 - Typ 0 lub 8
 - Kod zawsze 0
 - Identyfikator i numer sekwencyjny – unikalne wartości w celu połączenia żądania i odpowiedzi
- Destination unreachable
 - Uszkodzenie łącza
 - Błędny adres docelowy
 - Nieznana lokalizacja
 - Wysyłane przez router
 - Kody (przykładowe)
 - 0 – sieć niedostępna
 - 1 – host niedostępny
 - 2 – protokół niedostępny
 - 3 – port niedostępny
 - 4 – niezbędna fragmentacja
 - 6 – nieznana sieć docelowa
 - 11 – host niedostępny dla tego typu usług

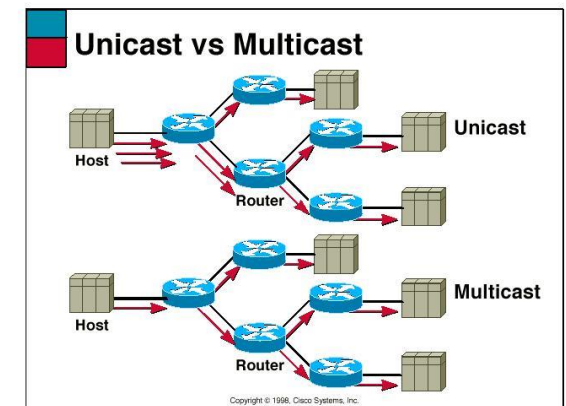
0	8	16	31
Typ (0 lub 8)	Kod (0)	Suma kontrolna	
Identyfikator		Numer sekwencyjny	
Dane opcjonalne			

0	8	16	31
Typ (3)	Kod (0 - 12)	Suma kontrolna	
Nie używane (musi mieć wartość zero)			
Nagłówek internetowy + pierwsze 64 bity datagramu			



Protokół IGMP

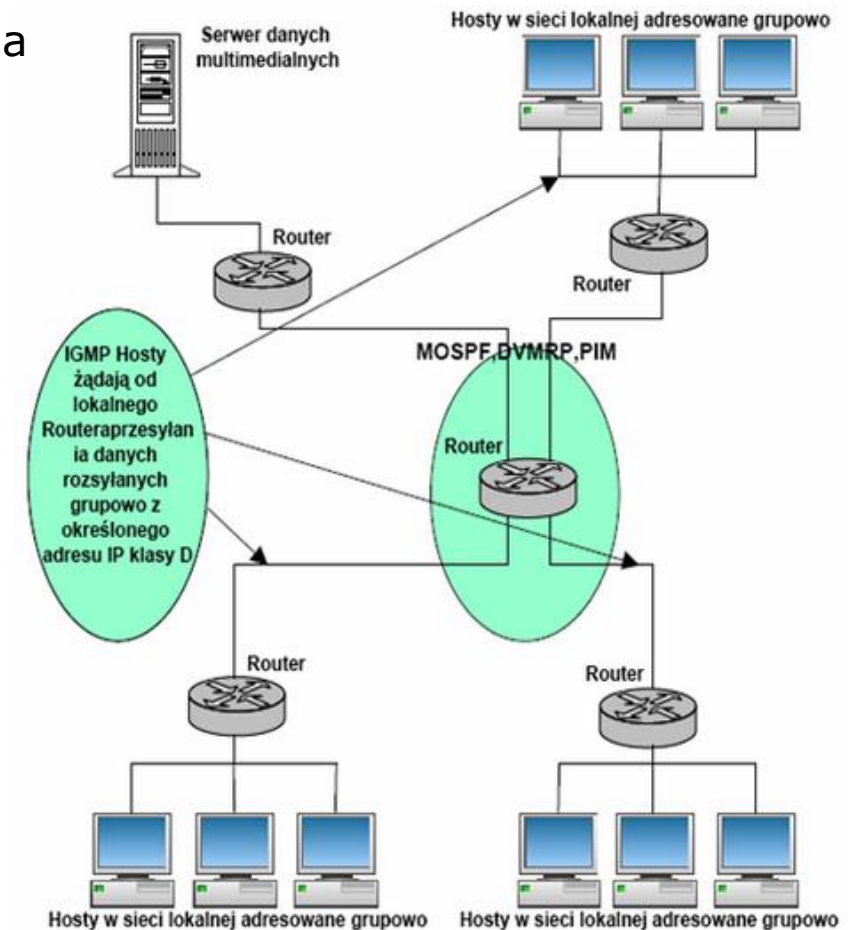
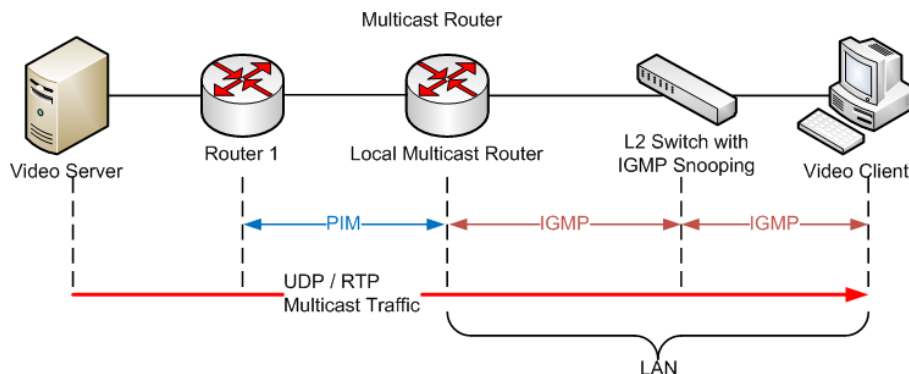
- IGMP (Internet Group Management Protocol) – protokół zarządzania grupami internetowymi (RFC 1112)
- Komunikacja urządzeń sieciowych przy pomocy transmisji grupowych
- Odbieranie/wysyłanie danych przeznaczonych dla kanału, do którego jest się podłączonym
- Oparte na transmisji typu multicast
 - Pakiet wysyłany na adres multicastowy (IP)
 - Routery znają adresy urządzeń podłączonych do poszczególnych grup
 - Zapewnia jednokrotne wysłanie danych do wszystkich hostów w grupie
- Struktura pakietu
 - 4 bity – wersja pakietu
 - 4 bity – typ komunikatu (zapytanie lub raport o przynależności hosta)
 - 8 bitów – nie wykorzystywane
 - 16 bitów – suma kontrolna
 - 32 bity - adres grupy (pusty gdy zapytanie, adres gdy odpowiedź)



0	4	8	16	32
Wersja	Typ	Nie używane	Suma kontrolna	
Adres grupy				

Przesyłanie grupowe

- w ramach sieci lokalnych
 - IGMP dla IPv4
 - MLD (Multicast Listener Discovery) dla IPv6
- między routerami - grupowe protokoły trasowania
 - W obrębie jednej domeny trasowania (systemu autonomicznego, AS – wykład o DNS)
 - PIM (Protocol Independent Multicast Protocol) – protokół adresowania grupowego niezależny od protokołów - RFC 2117
 - MOSPF (Multicast Extensions to OSPF) – rozszerzenie protokołu OSF o adresowanie grupowe – RFC 1584
 - Pomiędzy domenami trasowania
 - MBGP – (Multicast Border Gateway Protocol) RFC4760 – rozszerzenie protokołu BPG do przesyłania adresów grup multicastowych



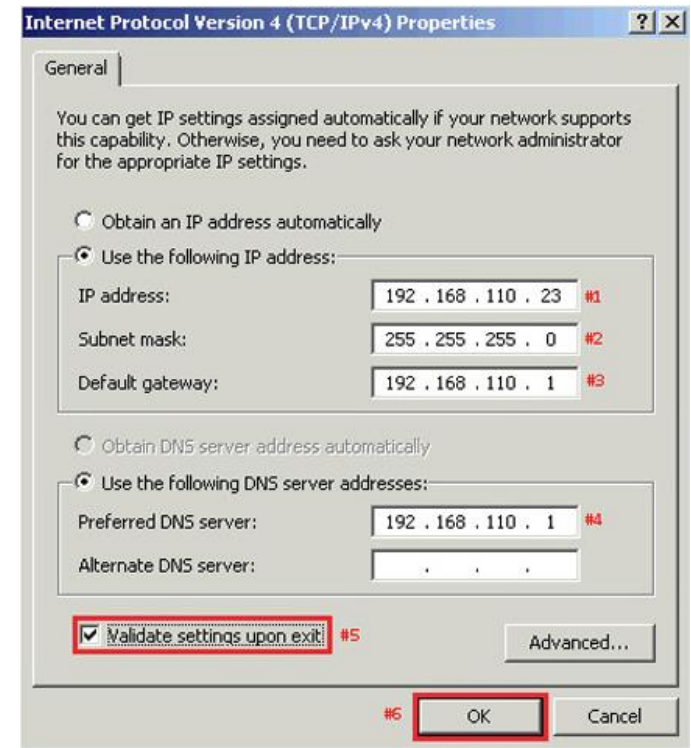
Uzyskiwanie adresu IP

- Statyczne
- Dynamiczne
 - ARP / RARP
 - BOOTP
 - DHCP

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

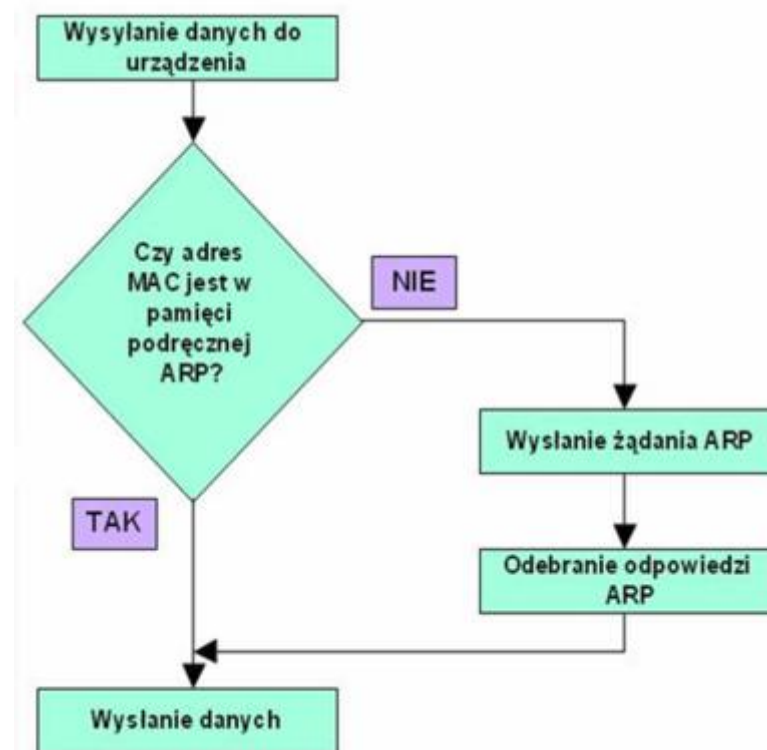
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 172.16.30.25
    netmask 255.255.255.0
    broadcast 192.168.30.255
    network 172.16.30.0
    gateway 172.16.30.1
```



Protokół ARP

- ARP (Address Resolution Protocol) – odwzorowuje znany adres IP na adres sprzętowy MAC
- Adres IP w sieci lokalnej – adres MAC hosta
- Adres IP spoza sieci lokalnej – adres MAC routera
- Wykorzystuje tablicę ARP
- Zapytanie ARP rozsyłane na adres broadcast (wraz z adresem MAC/IP nadawcy)
- Inne komputery uaktualniają swoje tablice ARP
- Wady:
 - Działa tylko dla IPv4
 - Brak możliwości przesyłania maski sieci (bezużyteczny przy adresacji bezklasowej)
 - Identyfikacja hosta jedynie po adresie MAC



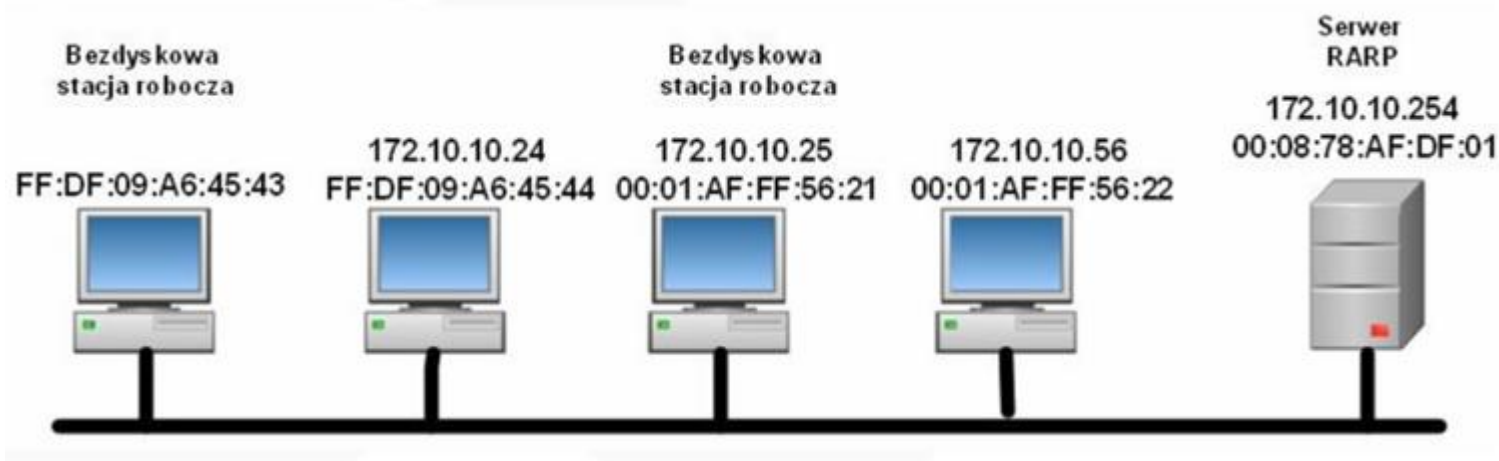
Protokół ARP – odpytanie tablicy arp

```
C:\Users\Benjamin>arp -a
Interface: 169.254.106.108 --- 0x12
  Internet Address      Physical Address      Type
  169.254.255.255      ff-ff-ff-ff-ff-ff    static
  224.0.0.22           01-00-5e-00-00-16    static
  224.0.0.252          01-00-5e-00-00-fc    static
  255.255.255.255      ff-ff-ff-ff-ff-ff    static
Interface: 192.168.187.128 --- 0x15
  Internet Address      Physical Address      Type
  192.168.187.255      ff-ff-ff-ff-ff-ff    static
  224.0.0.22           01-00-5e-00-00-16    static
  224.0.0.252          01-00-5e-00-00-fc    static
  255.255.255.255      ff-ff-ff-ff-ff-ff    static
```

```
dev@ubuntuserver14:~$ arp -an
? (192.168.1.5) at f0:25:b7:fb:16:18 [ether] on eth0
? (192.168.1.100) at 00:0c:29:c0:5a:ef [ether] PERM on eth0
? (192.168.1.4) at e0:db:55:ce:13:f1 [ether] on eth0
? (192.168.1.1) at 00:1f:90:88:e3:2d [ether] on eth0
? (192.168.1.3) at e0:db:55:ce:13:f1 [ether] on eth0
? (192.168.1.2) at f0:25:b7:f0:a7:ba [ether] on eth0
```

Protokół RARP

- Reverse Address Resolution Protocol – protokół wstecznego rozwiązywania adresów
- Zdefiniowany w RFC 903
- Problem maszyn bezdyskowych
 - Brak pamięci nieulotnej
 - Brak możliwości zapisania adresu IP hosta
 - Występuje np. po restarcie
 - Odpytanie innych hostów o swój adres IP w oparciu o swój adres MAC
- Można zapytać także o adresy IP innych hostów
- Odpowiedź przy użyciu serwera RARP



ARP/RARP – format pakietu

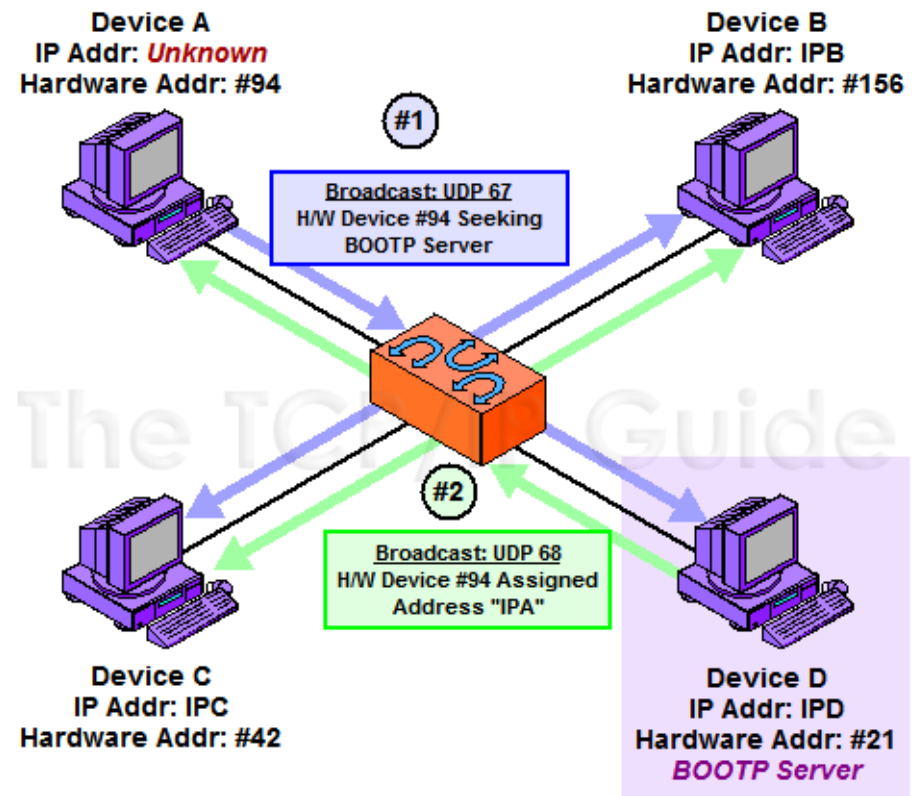
- Typ interfejsu
- Typ protokołu – ... który wysłał żądanie/odpowieź (IP : 0x0800)
- HLen – długość adresu sprzętowego (Ethernet : 48 bit)
- PLen – długość adresu protokołu warstwy sieciowej (IPv4 : 32 bity)
- Operacja:
 - 1 – żądanie ARP
 - 2 – odpowiedź ARP
 - 3 – żądanie RARP
 - 4 – odpowiedź RARP
- Adres sprzętowy/logiczny źródła
- Adres sprzętowy/logiczny urządzenia docelowego

Wartość HTYPE	Typ
1	Ethernet
6	IEEE 802.3
15	Frame Relay
16	ATM
17	HDLC
18	Fibre Channel
19	ATM
20	Serial Line
30	ATM
31	IPsec

+	Bity 0 - 7	8 - 15	16 - 31
0	Typ warstwy fizycznej (HTYPE)		Typ protokołu wyższej warstwy (PTYPE)
32	Długość adresu sprzętowego (HLEN)	Długość protokołu wyższej warstwy (PLEN)	Operacja (OPER)
64	Adres sprzętowy źródła (SHA)		
?	Adres protokołu wyższej warstwy źródła (SPA)		
?	Adres sprzętowy przeznaczenia (THA)		
?	Adres protokołu wyższej warstwy przeznaczenia (TPA)		

Protokół BOOTP

- Bootstrap Protocol – protokół początkowego ładowania systemu
- Umożliwia uzyskanie danych konfiguracyjnych (adresu IP) z serwera BOOTP
- W warstwie transportowej używa UDP (porty 67 i 68)
- Zapytania na adres broadcast
- Klient wysyła zapytanie BOOTREQUEST
- Serwer odsyła pakiet BOOTREPLY
- Klient odczytuje dane konfiguracyjne przy użyciu protokołu TFTP
- Wady:
 - Niepełna dynamika przydziału adresów
 - Plik konfiguracyjny protokołu, parametry sieci – administrator sieci
 - Niezbędne statyczne wprowadzanie wpisów dla poszczególnych hostów (profile bootp)



Protokół BOOTP – format pakietu

- Kod operacji (BOOTREQUEST : 1, BOOTREPLY : 2)
- Typ interfejsu (Ethernet : 1)
- Ilość skoków – zliczanie pośrednich routerów biorących udział w transmisji pakietu
- XID – losowy identyfikator komunikatu (dla niezrozumiałych adresów MAC nadawcy, odpowiedź na BCST)
- Czas w sekundach od pierwszego BOOTREQUEST
- IP klienta – ustawia klient jeśli zna
- ustawia serwer BOOTP
 - Przydzielony adres IP klienta
 - Adres IP serwera
 - Adres IP bramki
 - Nazwa serwera
 - Plik startowy
- Adres sprzętowy klienta – służy do odesłania odpowiedzi
- Przykład zapytania :

```
/usr/sbin/bootpquery 02608cee018e ether -s hpserver
```

```
Received BOOTREPLY from hpserver.hp.com (15.9.18.119)
```

```
Hardware Address:    02:60:8c:ee:01:8e
Hardware Type:      ethernet
IP Address:         15.9.18.113
Boot file:          /export/tftpdire/hp-gw2-config
```

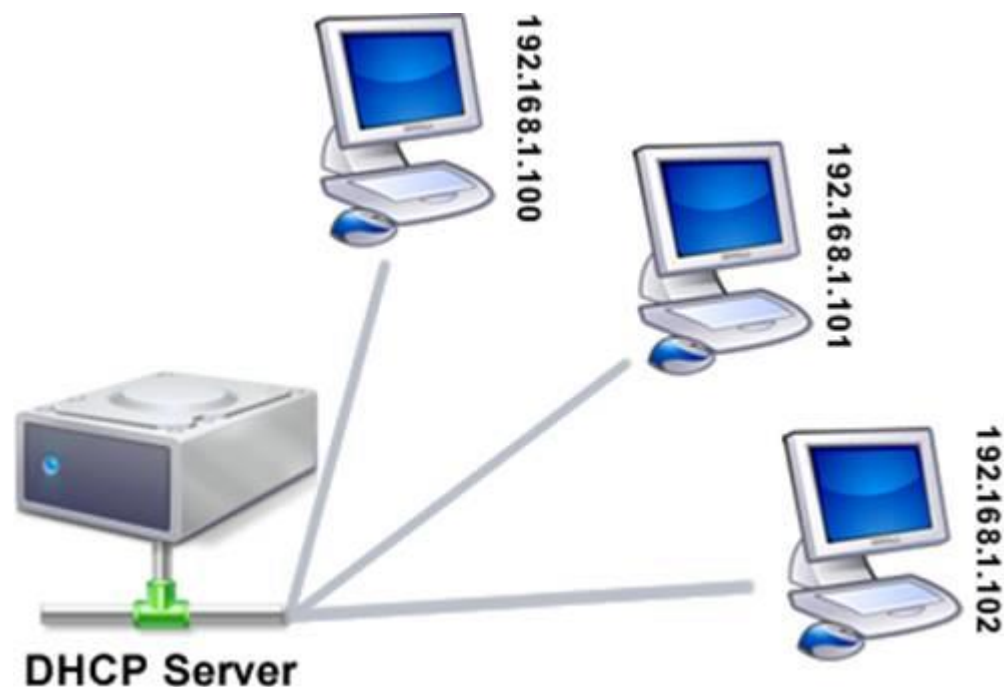
RFC 1048 Vendor Information:

```
Subnet Mask:        255.255.248.0
Bootfile Size:      6 512 byte blocks
Domain Name Server: 15.9.18.119
Host Name:          hp-gw2
```

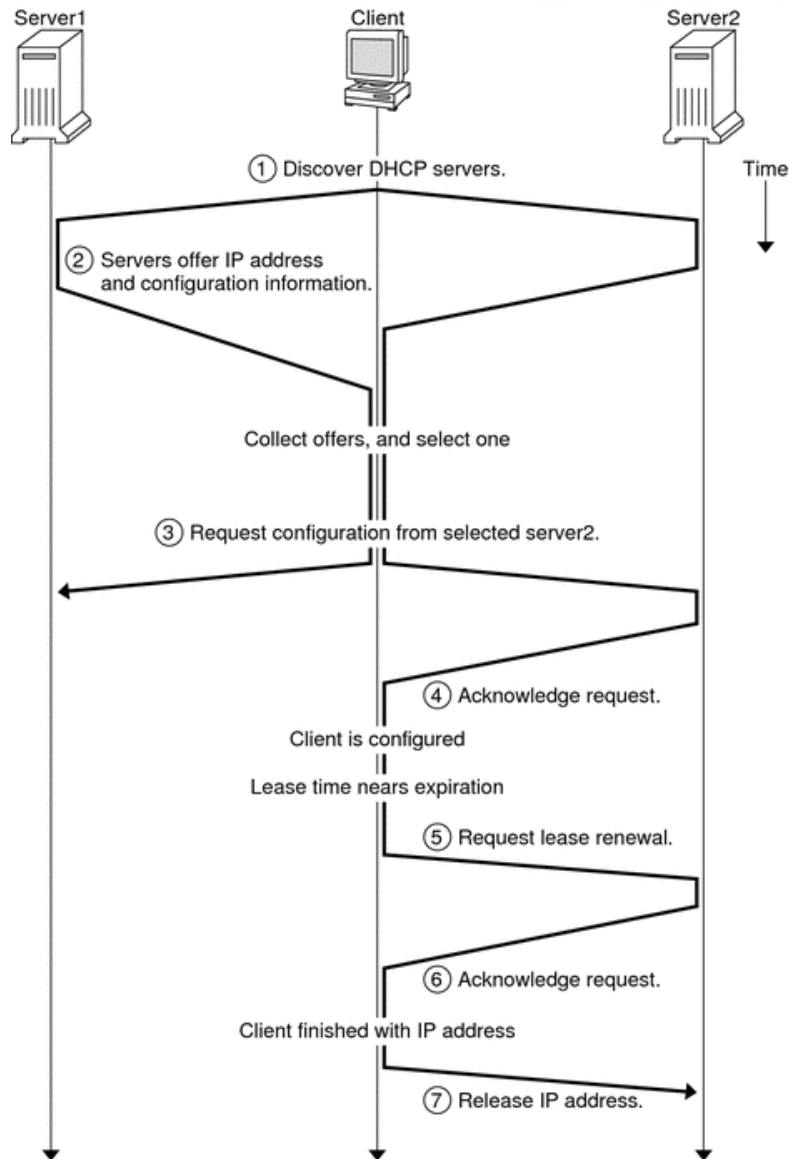
00-07	08-15	16-23	24-31
operacja	typ sprzętu	długość adresu sprzętowego	ilość skoków
xid (identyfikator transakcji)			
ilość sekund		nie używane	
adres IP klienta			
przydzielony adres IP klienta			
adres IP serwera			
adres IP bramki			
adres sprzętowy klienta (16 oktetów)			
nazwa serwera (64 oktety)			
plik startowy (128 oktetów)			
opcje producenta (64 oktety)			

Protokół DHCP

- Dynamic Host Configuration Protocol – ulepszona wersja BOOTP
 - RFC 2131 - 1993 r. – publikacja standardu dotyczącego adresu IP
 - RFC 2132 – rozszerzone parametry konfiguracyjne
 - RFC 3315 – wersja dla IPv6
- Tryby przydzielania adresów IP
 - Allokacja ręczna – przydział przez administratora,
 - Allokacja dynamiczna – przydział przez serwer
 - Dzierżawa – przydział dynamiczny na pewien okres czasu
- Używa protokołu UDP
 - IPv4 porty 67 i 68 (jak BOOTP)
 - IPv6 porty 546 i 547



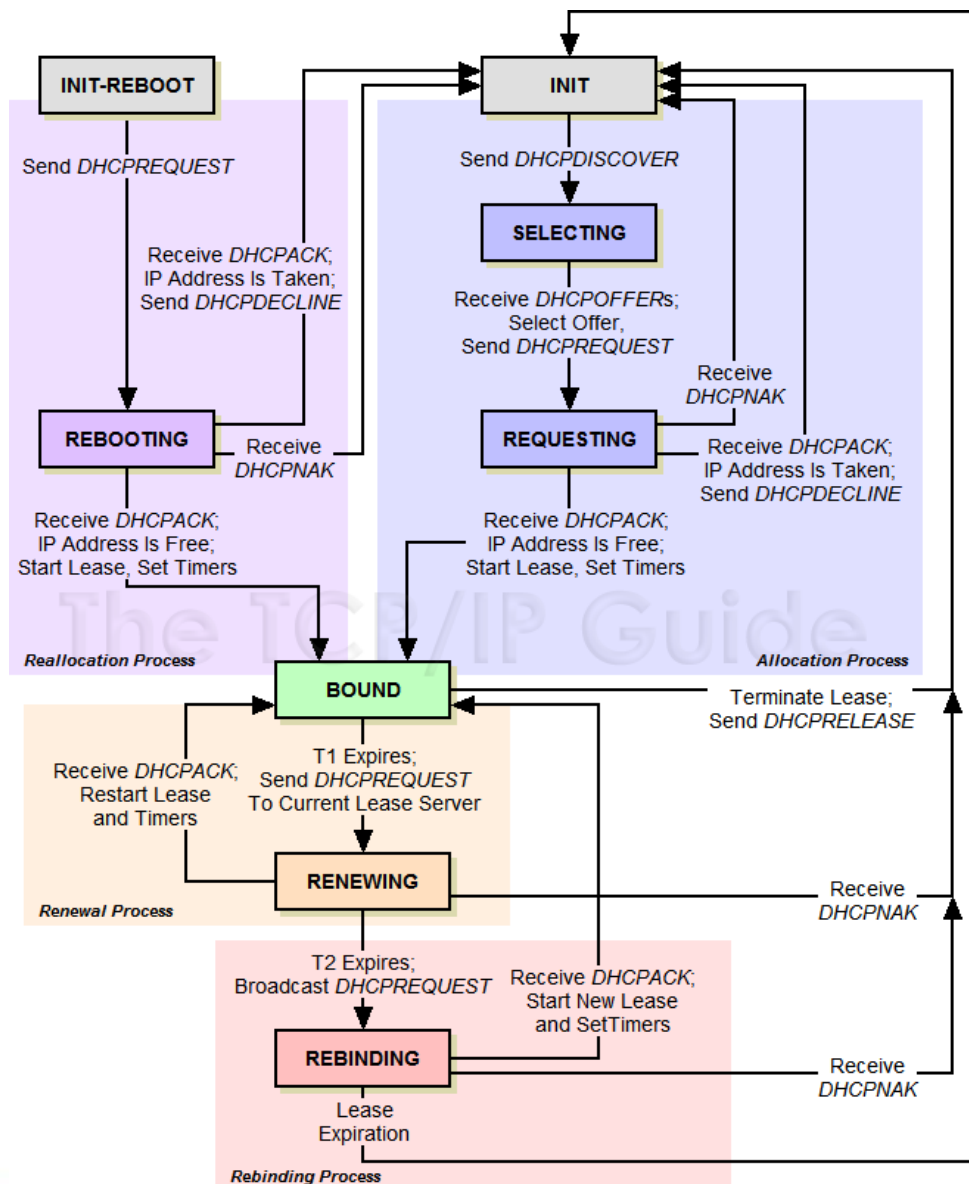
Algorytm działania DHCP – wersja podstawowa



Algorytm działania DHCP – wersja pełna

Typy komunikatów:

- DHCPDISCOVER – zlokalizowanie serwerów
- DHCPOFFER – przesyłanie parametrów
- DHCPREQUEST – żądanie przydzielenia używanych parametrów
- DHCPACK – potwierdzenie przydziału parametrów
- DHCNACK – odmowa przydziału parametrów
- DHCPDECLINE – wskazanie że adres sieciowy jest już używany
- DHCPRELEASE – zwolnienie adresu
- DHCPINFORM – żądanie przydziału parametrów (bez adresu IP)



Format pakietu DHCP

- Bardzo zbliżony do formatu pakietu protokołu BOOTP
- Różnica
 - pole flagi
 - w BOOTP – wartość 0
 - w DHCP – 10000000000000000
 - Pole „opcje”, np.:
 - Dodatkowe dane konfiguracyjne
 - Okres dzierżawy
 - Maska podsieci lokalnej
 - Adres IP serwera czasu
 - Adres IP serwera DNS
 - Rozmiar pliku konfiguracyjnego
 - Opisane w RFC 1533
<http://tools.ietf.org/html/rfc1533>

00 – 07	08 – 15	16 – 23	24 – 31
operacja	typ sprzętu	długość adresu sprzętowego	liczba skoków
xid (identyfikator transakcji)			
liczba sekund		flagi	
adres IP klienta			
przydzielony adres IP klienta			
adres IP serwera			
adres IP bramki (routera)			
adres sprzętowy klienta (16 oktetów)			
nazwa serwera (64 oktety)			
plik startowy (128 oktetów)			
opcje producenta (długość zmienna)			

Literatura i bibliografia

R.Bradford, „Podstawy sieci komputerowych”, WKiŁ, 2009

D.E.Comer, „Sieci komputerowe TCP/IP. Zasady, protokoły, architektura”

L.L.Peterson, B.S.Davie – Sieci komputerowe – podejście systemowe”, Nakom, Poznań 2000

Mark Sportack, Sieci komputerowe, Księga Eksperta, Helion, Warszawa 2008

W.Graniszewski, E.Grochocki, G.Świątek, Uzyskiwanie adresu IP – Studia Informatyczne, <http://wazniak.mimuw.edu.pl/>

D.E.Comer, „Sieci i intersieci”, WNT, Warszawa 2012

S.Wszelak, „Administrowanie sieciami komputerowymi”, Helion, 2015

Charles M. Kozierok, „The TCP/IP Guide”, <http://www.TCPIPGuide.com>, September 20, 2005

P.Jankowski, „Protokół IP wersja 6”