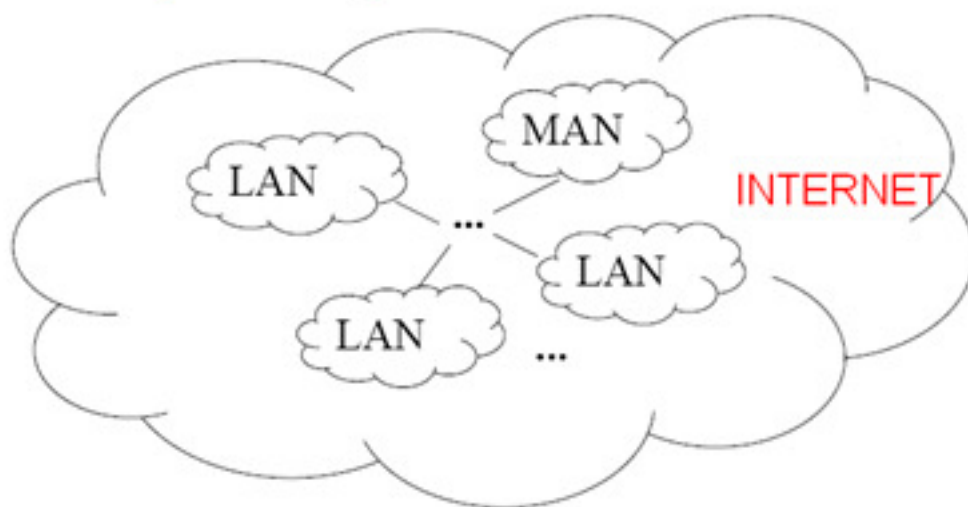


Adresacja IP - wstęp

Podstawy adresacji IP



Problem: Jak adresować urządzenia w tak dużej sieci?

Adresy IP

- adres IP składa się z 2 części: numeru sieci i numeru hosta,
- numer sieci należy uzyskać od NIC (Network Information Center),
- numery hostów przydziela lokalny administrator,
- adres jest związany z kartą sieciową,

Budowa adresu IP

- IP v4 - $4 \cdot 8 = 32$ bity - zaczyna brakować adresów IP,
- IP v6 - $6 \cdot 8 = 48$ bitów - przypada 1500 adresów na każdy m² kuli ziemskiej (łącznie z morzami),
- najczęściej stosuje się zapis kropkowo-dziesiętny:
00000110 | 10000100 | 00000010 | 00000001 = 6.132.2.1
- istnieje 5 klas adresowych: A, B, C, D, E

Adresowanie IPv4

W IPv4, czyli obecnym standardzie adresowania Internetu, adres IP to liczba 32-bitowa.

Liczby w adresie IP nazywają się oktetami, ponieważ w postaci binarnej mają one osiem bitów.

Te osiem bitów daje w sumie 256 kombinacji, więc każdy oktet przedstawia liczbę od 0 do 255.

Najpopularniejszy sposób zapisu adresów IP, to przedstawianie ich jako 4 dziesiętnych liczb od 0 do 255 oddzielonych kropkami. W rzeczywistości komputery traktują adres jako liczbę 32-bitową:

```
3482223596
```

Taki zapis jest mało czytelny, wobec czego stosuje się podział adresu IP na cztery oktety. Adres zapisujemy binarnie:

```
11001111 10001110 10000011 11101100
```

po czym każdą grupę 8-bitów przekształcamy do postaci dziesiętnej:

```
207      142      131      236
```

Z adresowaniem IP wiąże się pojęcie maski sieciowej. Wyobraźmy sobie sieć złożoną z 3 komputerów o adresach:

```
Komputer 1: 192.168.1.1  
Komputer 2: 192.168.1.2  
Komputer 3: 192.168.1.3
```

Łatwo zauważyć, że początek adresu dla wszystkich z nich jest ten sam, a końcówka się zmienia. Aby ściśle zdefiniować adresy przynależne do danej sieci wymyślono pojęcie maski podsieci. Umawiamy się, że określona ilość pierwszych bitów adresu IP ma być taka sama, a pozostałe bity w sieci mogą się różnić. W ten sposób powstaje proste kryterium, pozwalające komputerom na określenie swojego położenia na podstawie adresu. Maskę sieci zapisuje się podobnie jak adres IP. Dla przykładu

```
255.255.255.0
```

co binarne daje:

```
11111111 11111111 11111111 00000000  
 255      255      255      0
```

Jeżeli komputery oprócz komunikacji w swojej sieci lokalnej mają łączyć się z internetem, to maska sieciowa staje się bardzo ważna. Gdy urządzenie sieciowe stwierdzi, że adres docelowy, z którym chce wymieniać dane nie pasuje do maski, to próbuje się z nim łączyć przez bramę sieciową. Porównywanie opiera się na zerowaniu w adresie bitów równych zeru w masce. Jeżeli komputer 3 łączy się komputerem 2, to wykonuje następujące operacje:

Maska	11111111	11111111	11111111	00000000
	255	255	255	0
Mój IP	11000000	10101000	00000001	00000011
	192	168	1	3
Wynik a	11000000	10101000	00000001	00000000
	192	168	1	0
Maska	11111111	11111111	11111111	00000000
	255	255	255	0
Docelowy IP	11000000	10101000	00000001	00000010
	192	168	1	2
Wynik b	11000000	10101000	00000001	00000000
	192	168	1	0

Wynik a oraz Wynik b są równe wobec czego komputer 3 wie, że komputer 2 jest w tej samej podsieci. Jeżeli komputer 3 będzie chciał pobrać stronę z serwera www to operacja porównania będzie następująca:

Maska	11111111	11111111	11111111	00000000
	255	255	255	0
Mój IP	11000000	10101000	00000001	00000011
	192	168	1	3
Wynik a	11000000	10101000	00000001	00000000
	192	168	1	0
Maska	11111111	11111111	11111111	00000000
	255	255	255	0
IP serwera WWW	11001111	10001110	10000011	11101100
	207	142	131	236
Wynik b	11001111	10001110	10000011	00000000
	207	142	131	0

Jak widać wynik a, oraz wynik b są różne. W takiej sytuacji komputer 1 będzie się próbował połączyć z serwerem przez skonfigurowaną w nim bramę sieciową.

3). Rozdzielanie adresów

Nazwa	Pierwszy adres IP	Ostatni adres IP	Klasa	Największy ciągły blok
Blok 24-bitowy	10.0.0.0	10.255.255.255	pojedyncza sieć klasy A	10.0.0.0/8
Blok 20-bitowy	172.16.0.0	172.31.255.255	16 kolejnych sieci klasy B	172.16.0.0/12
Blok 16-bitowy	192.168.0.0	192.168.255.255	256 kolejnych sieci klasy C	192.168.0.0/16
Blok 12-bitowy	224.0.0.0	239.255.255.254	Klasa D	224.0.0.0/20
Blok 8-bitowy	240.0.0.0	255.255.255.254	Klasa E	240.0.0.0/24

Klasy adresowe

A	126 sieci, 16 mln hostów	0xxxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
B	65 tys. sieci i hostów	10xxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
C	16 mln sieci, 254 hostów	110xxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
D	multicast	1110xxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
E	zarezerwowane	1111xxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx

xxxxxxxx - numer sieci,

xxxxxxxx - numer hosta,

W adresach klasy A tylko pierwszy oktet wskazuje adres sieci; pozostałe trzy oktety opisują unikatowy adres węzła w sieci. Choć jest tylko 127 adresów sieci klasy A, każdy taki adres może obejmować w przybliżeniu 17 milionów węzłów. Jak nietrudno zgadnąć, adresy klasy A zostały przyznane organizacjom rządowym i wielkim instytucjom.

Adresy klasy B używają pierwszych dwóch oktetów do wskazania adresu sieci i ostatnich dwóch jako unikatowego węzła sieci. Z uwagi na większą długość, adresów klasy B jest więcej, ale w ramach każdego można unikatowo opisać tylko około 65 000 węzłów.

W adresach klasy C używa się pierwszych trzech oktetów jako adresu sieciowego i tylko ostatniego oktetu jako adresu węzła. Stąd istnieje wiele dostępnych adresów klasy C, ale każdy z nich może być użyty tylko do 254 węzłów.

Ze względu na skończoną ilość adresów oraz konieczność ich agregacji dla celów uproszczenia routingu powstały Regionalne Rejestry Internetowe (ang. *RIR*) - organizacje zajmujące się przydzielaniem puli adresów dla poszczególnych dostawców Internetu (ang. *ISP*). Organizacją nadrzędną jest Agencja Zarządzania Numeracją Internetową (ang. *IANA*), która zajmuje się dystrybucją poszczególnych klas A. Do organizacji regionalnych należą:

- APNIC (ang. *Asia Pacific Network Information Centre*) - dla rejonu Azji i Pacyfiku,
- ARIN (ang. *American Registry for Internet Numbers*) - dla rejonu Ameryki Północnej,
- LACNIC (ang. *Regional Latin-American and Caribbean IP Address Registry*) - dla rejonu Ameryki Łacińskiej i wysp Karaibskich,
- RIPE (fr. *Réseaux IP Européens*) - dla rejonu Europy, Bliskiego Wschodu i centralnej Azji.

Jeżeli ISP potrzebuje więcej adresów zwraca się do właściwej organizacji regionalnej i otrzymuje kolejny zakres numerów IP. Dla przykładu ARIN przydzielił adresy od 64.78.200.0 do 64.78.207.255 firmie Verado, Inc, która przekazała pulę od 64.78.205.0 do 64.78.205.15 firmie Bomis. Bomis adres 64.78.205.6 udostępnił Wikipedii.

Powszechnie panuje pogląd, że pula dostępnych adresów jest na wyczerpaniu, jednak w oficjalnym zestawieniu zajętości adresacji IP jest jeszcze wiele bloków.

Adresy należące do puli 127.0.0.0/8 (127.x.x.x) są przypisane do urządzenia loopback i zawsze odnoszą się do komputera lokalnego. Adres 0.0.0.0 to adres domyślny (ang. *default*).

Prywatne adresy IPv4

Istnieje pula prywatnych adresów IP. Mogą być one wykorzystane tylko w sieciach lokalnych. Infrastruktura Internetu ignoruje te adresy IP. IANA (*Internet Assigned Numbers Authority*) zarezerwował następujące trzy bloki przestrzeni adresów IP dla prywatnych sieci:

- 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)

Adresy prywatne można wykorzystywać za pomocą lokalnych routerów w sieciach lokalnych, ale nie działają one w publicznej części internetu. Jeżeli administrator sieci lokalnej przydzieli swoim komputerom adresy IP z puli prywatnej, to routery mogą łatwo rozpoznać kiedy komputery chcą się łączyć z internetem. W takiej sytuacji brama internetowa wykorzystuje technikę maskowania adresów sieciowych NAT, która pozwala na łączenie się z internetem komputerom nie posiadającym własnych publicznych adresów IP. Komputery z adresami prywatnymi nie mogą pełnić roli serwerów sieciowych w Internecie chyba, że posłużymy się techniką maskowania adresów docelowych (DNAT).

Automatyczne przydzielanie adresów IPv4 może być realizowane poprzez zastosowanie protokołów DHCP, RARP, BOOTP, PPP.

5). Wykorzystanie adresów IPv4

Początkowo wszystkie adresy IPv4 były zarządzane bezpośrednio przez IANA, która w zależności od wnioskowanych potrzeb przydzielała określoną pulę adresów klasy A, B lub C. Wielkie firmy, jak Xerox, Ford czy IBM automatycznie otrzymywały po ponad 16 mln adresów internetowych, nawet jeżeli tak duża liczba nie była im potrzebna. Jeżeli mała firma z kilkunastoma węzłami chciała podłączyć się do Internetu przyznawano jej adresy z klasy C. To z kolei dawało jej kontrolę nad ponad dwustoma adresami węzłów, z których nikt inny nie mógłby skorzystać. Ze względu na marnotrawstwo oraz niespodziewanie duże zapotrzebowanie na adresację internetową z całego świata zmieniono zasady i powołano do życia organizacje regionalne, których zadaniem stało się nadzorowanie wykorzystania dostępnych adresów.

Obecnie klasy A przydzielane są organizacjom regionalnym, te dalej rozdzielają je do ISP w blokach po 4 klasy C (1024 adresy), a następnie ISP przydzielają adresy swoim klientom. Duży nacisk kładzie się na wykorzystywanie mechanizmów NAT, umożliwiających korzystanie z jednego adresu zewnętrznego przez wiele urządzeń posiadających adresy lokalne. W ten sposób ogranicza się przydzielanie adresów urządzeniom (tj. drukarki, access pointy, itp) działającym jedynie w obrębie zamkniętych sieci. Wciąż można dostać przypisanie do klasy C dla swojej organizacji, ale staje się to coraz trudniejsze. Trzeba wykazać rzeczywistą potrzebę dysponowania taką liczbą adresów.

Istnieją koncepcje, według których każde urządzenie elektroniczne ma zostać podłączone do Internetu. W takiej sytuacji pula adresów IPv4 będzie stanowczo za mała. Z tego powodu nastąpi prawdopodobnie przejście z protokołu IPv4 na IPv6 który zwiększy o cztery rzędy wielkości pulę dostępnych adresów.

W ramach klasy C adresów istnieje podział na tzw. podsieci (subnets). Rozmiar podsieci wyznaczany jest przez jej maskę. Najmniejszą podsiecią jest sieć składająca

się z 4 adresów, największą ze 128. Dla sieci 4 komputerowej maska wynosi: $256 - 4 = 252$ (NETMASK = 255.255.255.252). Dla tak wyznaczonej podsieci można określić następujące parametry:

NETWORK = 195.205.36.32 (**Adres IP** - przykładowa podsieć sieci klasy C przyznana przez dostawcę)

NETMASK = 255.255.255.252 (maska podsieci)

adresy komputerów = 195.205.36.33 i 195.205.36.34

BROADCAST = 195.205.36.35 (adres rozgłoszeniowy)

W praktyce maska 255.255.255.252 oznacza, iż do sieci tej można podłączyć 2 komputery i używana jest przez administratorów sieci komputerowych do spinania poszczególnych segmentów sieci.

Aby znaleźć adres rozgłoszeniowy musimy przekształcić **Adres IP** oraz maskę podsieci na system binarny:

Adres IP:	11000011	11001101	00100100	00100000
	195	205	36	32
Maska podsieci:	11111111	11111111	11111111	11111100
	255	255	255	252

Teraz patrzymy na maskę i zamiast zer wpisujemy w adresie IP jedyńki. To jest nasz adres rozgłoszeniowy (broadcast):

Broadcast	11000011	11001101	00100100	00100011
	195	205	36	35

Aby znaleźć adres sieci musimy przekształcić **Adres IP** oraz maskę podsieci na system binarny:

Adres IP:	11000011	11001101	00100100	00100011
	195	205	36	35
Maska podsieci:	11111111	11111111	11111111	11111100
	255	255	255	252

Następnie mnożymy AND adres IP komputera oraz maskę.

Adres Sieci:	11000011	11001101	00100100	00100000
	195	205	36	32

Cele tworzenia podsieci:

- zbyt dużo komputerów w klasach A i B,
- zmniejszenie domeny rozgłoszeniowej,

IPv5 IPv6

Protokół **IPv5** był w zasadzie propozycją, która nie wyszła poza fazę eksperymentów. Zarzucono nad nim pracę w momencie gdy pojawiła się kolejna propozycja

rozwiązania problemu zbyt małej liczby adresów IP: protokół **IPv6**. IPv6 to nowy 128-bitowy rodzaj adresów IP. Pula IPv6 obejmuje zakres od 0 do 340282366920938463463374607431768211455 co oznacza, że w dającej się przewidzieć przyszłości nie powinny wystąpić problemy związane z brakiem dostępnych adresów.

Adres IPv6 zapisuje się jako osiem liczb szesnastkowych rozdzielonych dwukropkami:

1080:0:0:0:0:800:0:417A

Jeżeli w adresie występują powtarzające się zera, to można je pominąć, ale ze względu na jednoznaczność, tylko w jednym miejscu adresu:

1080::800:0:417A

Adresy IPv6 dzieli się na dwie części, z których pierwsza stanowi adres sieci, zaś druga jest adresem urządzenia w tej sieci.

Maska sieci w przypadku protokołu IPv6 określa liczbę bitów adresu IPv6 przypadającą na adres sieci:

12AB::CD30:0:0:0:0/60

Automatyczne przydzielanie adresów IPv6 jest integralną częścią protokołu IPv6 i nie wymaga żadnych dodatkowych usług jak DHCP dla IPv4.

Przykład adresacji IPv4

Obliczanie zakresu adresów komputerów

- Przykład:

adres sieci 150.150.0.0 /16

10010110 10010110 00000000 00000000

10010110 10010110 00000000 00000001

10010110 10010110 00000000 00000010

...

10010110 10010110 11111111 11111110

10010110 10010110 11111111 11111111

adres sieci

Adres pierwszego komputera

Adres ostatniego komputera

adres rozgłoszeniowy

- Dziesiętnie

adres sieci: 150.150.0.0 /16,

adres rozgłoszeniowy: 150.150.255.255,

zakres adresów komputerów: od 150.150.0.1 do 150.150.255.254

Adres fizyczny MAC

MAC *Media Access Control* - sprzętowy adres karty sieciowej Ethernet i Token Ring, unikalny w skali światowej, nadawany przez producenta danej karty podczas produkcji.

Adres MAC (ang. *MAC address*) jest 48-bitowy i zapisywany jest heksadecymalnie (szesnastkowo). Pierwsze 24 bity oznaczają producenta karty sieciowej, pozostałe 24 bity są unikalnym identyfikatorem danego egzemplarza karty. Na przykład adres **00-0A-E6-3E-FD-E1** oznacza, że karta została wyprodukowana przez Elitegroup Computer System Co. (ECS) i producent nadał jej numer 3E-FD-E1. Czasami można się spotkać z określeniem, że adres MAC jest 6-bajtowy. Ponieważ 1 bajt to 8 bitów, więc 6 bajtów odpowiada 48 bitom. Pierwsze 3 bajty (vendor code) oznaczają producenta, pozostałe 3 bajty oznaczają kolejny (unikalny) egzemplarz karty. Nowsze karty ethernetowe pozwalają na zmianę nadanego im adresu MAC.

Zadania:

1. Sprawdź adres IP, maskę podsieci oraz bramę domyślną Twojego komputera.
2. Podaj wzór na liczbę komputerów w sieci, której maska jest znana.
3. Oblicz zakres adresów komputerów i adres rozgłoszeniowy w sieci o adresie IP 150.150.64.0 i masce 255.255.192.0.
4. Oblicz zakres adresów IP komputerów w każdej z klas A, B i C.
5. Sprawdź adres MAC Twojego komputera.
6. * Sprawdź, czy na podstawie adresu MAC można określić:
 - Producenta karty sieciowej
 - Rodzaj karty sieciowej (USB, PCMCIA, PCI, wbudowana)
 - Podaj ewentualne numery kart konkretnych producentów i rodzaj kart.