
chabińska

# Nowy Internet?

**32-bitowe adresy IP na pozór wystarczają do zaadresowania niemal nieograniczonej liczby urządzeń wpiętych do Sieci. Obecnie zbyt wąska przestrzeń adresowa IP jest jednym z hamulców ograniczających rozwój Internetu.**

Znany dobrze wszystkim internautom protokół IP wywodzi się jeszcze z *ARPANET-u* (Advanced Projects Research Agency Network), powstałej w 1968 roku sieci łączącej agendy rządowe Stanów Zjednoczonych. Jako że ARPANET miał połączyć co najwyżej kilkadziesiąt instytucji, przyjęcie 32-bitowej przestrzeni adresowej wydawało się rozwiązaniem nowoczesnym i przyszłościowym. W pierwotnej wersji protokołu IP najstarsze 8 bitów adresów identyfikuje sieć, natomiast pozostałe 24 bity reprezentują hosta (urządzenie wpięte do Sieci).

Ponieważ szybko okazało się, iż ARPANET połączy więcej niż 256 sieci, wydzielono trzy klasy 32-bitowych adresów. Adresy klasy A rozpoczynają się od bitu zerowego, po którym następują: 7-bitowy identyfikator sieci i 24-bitowy deskryptor hosta. Adres klasy B zawiera 14-bitowy adres sieci i 16-bitowy identyfikator hosta, poprzedzone dwubitowym prefiksem 10, tak więc adresy tej klasy mogą zidentyfikować 16 384 sieci liczących do 65 535 hostów. Przeznaczona dla najmniejszych struktur klasa C rozpoczyna się trzybitowym prefiksem 110, po którym następuje 21-bitowy identyfikator sieci i 8-bitowy adres hosta. Stosując adresy tej klasy, można wydzielić 2 097 152 sieci po 256 hostów każda.

## Odraczanie wyroku

Taki sposób przydzielania adresów IP w Sieci ma bardzo poważne konsekwencje – liczba adresów klasy B, a więc tych interesujących dostawców usług internetowych i inne duże organizacje, jest stanowczo zbyt mała. Na początku lat dziewięćdziesiątych prorokowano, opierając się na dotychczasowym tempie rozwoju Sieci, iż zasób dostępnych adresów klasy B wyczerpie się najdalej na początku 1994 roku – do 1992 rozdzielono już ponad połowę dostępnej puli.

Obecnie problem ten rozwiązywany jest w sposób właściwy dobrym księgowym – poprzez szukanie oszczędności w zmianie sposobu dysponowania zasobami. Stało się to możliwe dzięki wprowadzeniu technologii routingu bezklasowego między domenami (CIDR, Classless Interdomain Routing), znanej również jako supernetting. Jej podstawą była obserwacja, iż duża część zasobów adresowych przydzielanych w ramach klas A i B pozostaje nie wykorzystana: niewiele organizacji, którym przydzielono klasy A, potrzebuje kilku milionów adresów. Podobna sytuacja dotyczy adresów klasy B – jeśli firma potrzebowała pięć tysięcy adresów, przydzielano jej pełną klasę B, co blokowało wykorzystanie ponad 60 000 pozostałych adresów do niej należących. Zasada działania techniki CIDR polega na tym, by zamiast pełnej klasy A bądź B przydzielić ciągły blok adresów klasy C, o wspólnych najbardziej znaczących bitach określających podsieć, przy czym najmniej znaczące bity adresu sieci przydzielane są na potrzeby identyfikacji

podstawy

## 32-bitowy adres IPv4

| | | Liczba sieci | Liczba hostów |
|---|---|---|---|
| Klasa A | 0 1010101 . 01010101.01010101.01010110 | 128 | 16777216 |
| Klasa B | 10 101010.01010101 . 01010101.01010101 | 16384 | 65535 |
| Klasa C | 110 10101 .10101010.10101010 . 01010101 | 2097152 | 256 |
| Identyfikator | klasy sieci hosta | | |

**Zbyt mała przestrzeń adresowa przewidziana na identyfikację poszczególnych sieci spowodowała konieczność wprowadzenia podziału przestrzeni adresowej IP na klasy A, B i C, przeznaczone odpowiednio dla dużych, średnich i małych organizacji.**

hosta. I tak przykładowo, wykorzystując trzy kolejne klasy C od 192.199.199.5 do 192.199.199.7, otrzymujemy podsieć o pojemności 768 adresów, określaną maską 255.255.252.0 – wspólne 22 najstarsze bity adresu).

Technikę tę można jednak zastosować jedynie wówczas, gdy zapotrzebowanie wynosi najwyżej kilka tysięcy adresów, gdyż w przeciwnym razie trudno znaleźć ciągły obszar adresów klasy C. Ponadto wszystkie routery pośredniczące w przekazywaniu pakietów do tak zaadresowanych hostów muszą obsługiwać technologię CIDR.

Inne metody, pozwalające ograniczyć „zużycie" adresów IP, to techniki translacji i dynamicznego przydzielania adresów. Pierwsza z nich, znana najczęściej jako NAT (Network Address Translation) lub IP Masquerading, polega na zastosowaniu w sieci wewnętrznej odmiennej puli adresów IP niż te, które są wykorzystywane do komunikacji z resztą Internetu. W tym celu niezbędny jest serwer, który dokona konwersji adresów intranetowych na właściwe adresy używane do komunikacji zewnętrznej. Technika ta ma tę wielką zaletę, iż nawet pełna klasa adresów C przydzielona komputerom w sieci wewnętrznej może być widziana od strony Internetu jako zaledwie jeden adres IP. Same adresy wewnętrzne nie muszą spełniać wymogu niepowtarzalności w skali całego Internetu, gdyż pakiety z sieci wewnętrznej nigdy nie są przez mechanizm NAT wysyłane bezpośrednio do adresata. Dodatkowo, dokument RFC 1918 definiuje kilka klas zalecanych adresów intranetowych – pochodzące z tych adresów pakiety są blokowane przez routery obsługujące ruch w Internecie, co zabezpiecza przed kolizjami pomiędzy sieciami intranetowymi wykorzystującymi te same klasy adresowe. Technika NAT ma jednak istotne wady – przede wszystkim obniża ona wydajność sieci, gdyż każdy przesyłany do lub z Internetu pakiet danych musi zostać przeanalizowany, a następnie przekierowany do właściwego odbiorcy. Translacja taka powoduje również, że niektóre aplikacje sieciowe nie będą funkcjonować poprawnie, gdyż serwer danej usługi wstawia adres odbiorcy do danych pakietu (a więc w tym wypadku adres serwera NAT, a nie rzeczywistego odbiorcy pakietu), a tego serwer NAT nie jest w stanie zmienić.

Z kolei technika DHCP (Dynamic Host Configuration Protocol) bazuje na fakcie, że zazwyczaj część komputerów w sieci lokalnej jest wyłączona bądź nie korzysta w danym momencie z protokołu TCP/IP. W związku z tym serwer prowadzący usługę DHCP przydziela hostowi adres IP ze zdefiniowanej puli dopiero na żądanie. Jeżeli komputer, któremu przydzielono adres, przez dłuższy czas nie korzysta z protokołu TCP/IP, adres ten jest zwalniany i ponownie przekazywany do wykorzystania przez inne komputery.

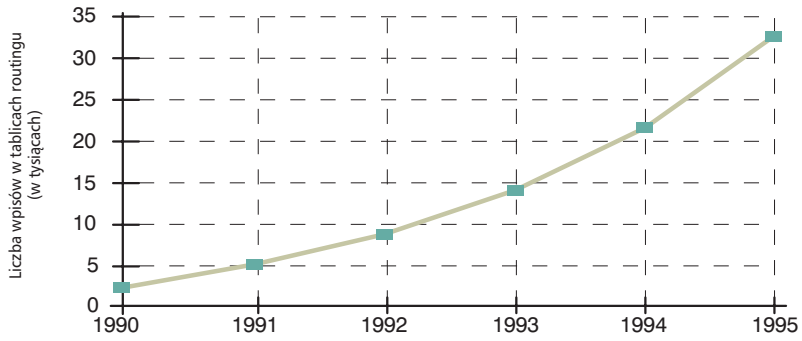
Jednak, stosując powyższe techniki, nie da się odwlekać katastrofy w nieskończoność – według ostatnich szacunków, pomimo wszelkich metod „oszczędzania" adresów IP, ich pula wyczerpie się pomiędzy rokiem 2005 a 2010. W tej sytuacji niezbędne stało się opracowanie nowego modelu adresowania urządzeń dostępnych w Sieci.

### Idzie nowe

Ze swym rodowodem sięgającym 1968 roku IP jest w tej chwili koncepcją właściwie historyczną. Opracowując nowy model adresów IP, IETF (Internet Engeneering Task Force) postanowiła wykorzystać nadarzającą się okazję i gruntownie zmodernizować schemat adresowania urządzeń w Internecie, nie ograniczając się jedynie do poszerzenia przestrzeni adresowej. W opublikowanym na początku 1995 roku dokumencie „The Recommendation for the IP Next Generation Protocol" (RCF 1752) zaprezentowano IPv6 (analogicznie do IPv4, IP wersji czwartej). Zawiera on oprócz 128-bitowej przestrzeni adresowej hierarchiczny model adresowania, zmodyfikowany nagłówek pakietu oraz szereg usług związanych z transmisją pakietów, zapewniających na przykład szyfrowanie danych czy automatyczną konfigurację adresów ▶ 136

podstawy

## Przyrost liczby wpisów w tabelach routingu




**Niemal wykładniczy przyrost liczby wpisów w tabelach przekierowań routerów pracujących w połączeniach szkieletowych Internetu (backbone) powoduje, że za parę lat nawet najpotężniejsze urządzenia telekomunikacyjne nie będą w stanie efektywnie kierować ruchem w Sieci.**

Źródło: 3Com

hostów. Efektem kilkuletnich prac, prowadzonych przez IETF IPnG Working Group, są dokumenty: RFC 2460, definiujący podstawowe pojęcia i rozwiązania wprowadzone w IPv6, oraz „The Case for IPv6", prezentujący techniczne i ekonomiczne uwarunkowania, jakie doprowadziły do powstania IPv6 w takiej, a nie innej postaci. Pełną listę dokumentów opisujących technologie i rozwiązania powiązane z IPnG można znaleźć pod adresem *http://playground.sun.com/pub/ipng/html/specs/standards.html*.

Wprowadzeniu IPv6 musi towarzyszyć modyfikacja prawie wszystkich standardów i usług funkcjonujących w Sieci (np. DNS), tak aby zapewnić ich współpracę z obiema wersjami protokołu i obsługę 128-bitowych adresów hostów. Dla większości ważnych usług IETF opublikował już odpowiednie specyfikacje. I tak w dokumencie RFC 1886 przedstawiono zmodyfikowaną specyfikację mechanizmu DNS. Obsługuje on obie wersje protokołu i zawiera nowy typ rekordu AAAA, przeznaczony do zapisu 128-bitowego adresu hosta. Z tym standardem zgodny jest na przykład serwer DNS zawarty w NT Serverze, mimo iż sam protokół nie jest przez niego obsługiwany.

Testowanie nowych rozwiązań odbywa się w ramach tzw. 6bone, eksperymentalnej sieci łączącej instytucje pracujące nad IPv6.

## Adresy, adresy...

Wraz z poszerzeniem przestrzeni adresowej IP do 128 bitów w IPv6 pojawiły się trzy typy adresów: unicast, multicast i anycast. Pierwszy z nich odpowiada najpowszechniejszemu w Sieci typowi transmisji, punkt-punkt (point-to-point), a więc o jednoznacznie zdefiniowanym odbiorcy. W celu ułatwienia organizacji ruchu pakietów w sieci lokalnej zdefiniowano dwa dodatkowe typy adresów unicastowych: segmentowy (LLUA, link local unicast address) oraz ośrodka (SLUA, site local unicast address). Ruch pakietów oznaczonych pierwszym typem adresu ograniczony jest do określonego fragmentu intranetu, drugi zaś do wewnętrznej sieci firmy – routery pośredniczące w komunikacji z resztą Internetem nie będą tak adresowanych pakietów przesyłać dalej.

Rodzina adresów typu multicast jest rozszerzeniem znanej z IPv4 idei adresów typu broadcast, czyli takich, które określają wielu odbiorców jednego pakietu. Adresy multicast mogą być czasowe (transient) i trwałe (permanent). Adresy czasowe definiuje się pod kątem konkretnego zastosowania, np. w celu zestawienia telekonferencji, natomiast adresy trwałe definiują raczej funkcjonalne grupy odbiorców, np. wszystkie serwery prowadzące mirror danego serwisu tematycznego.

Trzeci typ adresu, unicast, nie ma swego odpowiednika w IPv4. Podobnie jak w przypadku adresu multicast, pakiety rozsyłane są do grupy odbiorców, jednak ich dystrybucja kończy się wówczas, gdy dowolny z nich dotrze na miejsce przeznaczenia. Jako że w ramach obecnej specyfikacji IPv6 adresy typu anycast mogą określać jedynie routery, ich najpowszechniejszym zastosowaniem będzie zapewne rozsyłanie zapytań w celu określenia najszybszej dostępnej ścieżki transmisji danych.

## IP po remoncie

128 bitów przestrzeni adresowej IPv6 zorganizowano zupełnie inaczej niż w wersji czwartej protokołu: adres składa się z ośmiu szesnastobitowych części, oddzielanych dwukropkami (zapewne dla łatwiejszego odróżnienia od IPv4). Ponieważ przykładowy adres w tej formie wygląda następująco: 1716:1A7F:DDEA:1325:3D2A:3A1D:2C6B:5G3H, zapamiętanie nawet kilku adresów wymagałoby niemałych umiejętności mnemotechnicznych. Aby uczynić 128-bitowe adresy łatwiejszymi do zapamiętania, wprowadzono możliwość „kompresji" ich zapisu przez usunięcie zer rozpoczynających każdy 16-bitowy segment. Co prawda adresu z naszego przykładu nie dałoby się w ten sposób w ogóle skrócić, jednak adres 1716: 0A7F: 00B0: 0025: 0D2A: 0000: 0000B: 003H przyjąłby postać 1716:A7F:B0:25:D2A::B:3H.

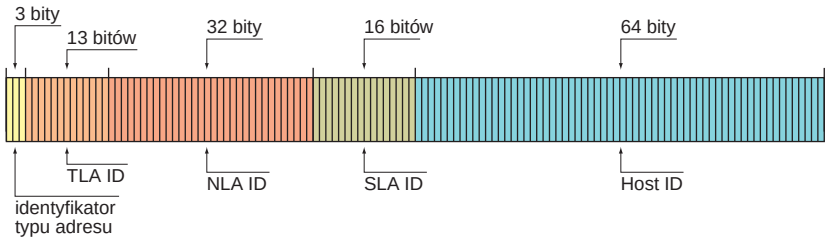
O ile 32-bitowa przestrzeń adresowa IPv4 jest zbyt skromna, aby zapisać w niej dodatkowe informacje o topologii sieci, o tyle 128 bitów IPv6 pozwala na zastosowanie hierarchicznej struktury adresów unicastowych (punkt-punkt), tzw. składanych adresów globalnych (aggregatable global unicast address). Tak skonstruowany adres podzielony jest na pięć części (patrz rys. poniżej). Pierwsza, trzybitowa liczba to identyfikator typu adresu. Drugi, 13-bitowy segment to TLA (Top Level Aggregators), opisujący operatorów obsługujących podstawowy ruch w Sieci. Przydzielany jest firmom telekomunikacyjnym zapewniającym funkcjonowanie szkieletowych, długodystansowych połączeń sieciowych przez organizacje takie jak IANA (Internet Assigned Numbers Authority). Kolejne 32 bity adresu to identyfikator NLA (Next Level Aggregators), identyfikujący dużych dostawców usług internetowych, którzy z kolei rozdysponowują 16-bitowe identyfikatory SLA (Site Level Aggregators), czyli odpowiedniki dzisiejszych klas adresowych. Identyfikatory SLA przydzielane są bądź organizacjom, które samodzielnie obsługują własną komunikację internetową, a więc uczelniom, instytutom czy dużym firmom, bądź bezpośrednim dostawcom usług internetowych. Organizacje te z kolei własnym użytkownikom lub klientom przydzielają 64-bitowe adresy hostów.

Przestrzeń adresowa pozostająca do dyspozycji pojedynczego providera jest, jak widać, wielokrotnie większa od całej przestrzeni adresowej wchodzącej w skład IPv4, co pozwala na przydzielenie własnego, niepowtarzalnego adresu IP każdemu urządzeniu włączonemu do Sieci.

▶ 139

*podstawy*

### Budowa adresu IPv6




**128 bitów przestrzeni adresowej IPv6 pozwala na hierarchiczną organizację adresowania w Sieci, a także zapewnia wystarczająco dużą pulę adresów, aby przydzielić niepowtarzalny adres IP każdemu urządzeniu, nawet takiemu jak pager czy komputer pokładowy w samochodzie.**

Hierarchiczna struktura adresów ipv6 ma niebagatelne znaczenie dla organizacji ruchu w Sieci. Obecnie tablice przekierowań routerów obsługujących szkieletowe magistrale Internetu liczą sobie po kilkadziesiąt tysięcy wpisów. Wprowadzenie modelu hierarchicznego spowoduje ich znaczące odciążenie – każdy router będzie tłumaczył jedynie część adresu. I tak routery obsługujące ruch na poziomie TLA będą interpretowały tylko segment TLA adresu, po czym będą przekazywały pakiet do właściwego docelowego TLA. Ten skieruje go do odpowiedniego NLA (nie interpretując już segmentu TLA), który prześle go do określonego w segmencie SLA lokalnego dostawcy usług. Taki sposób organizacji ruchu pakietów pozwala, aby każdy router znał jedynie swoje „najbliższe otoczenie": router struktury nadrzędnej i podlegające mu urządzenia struktur niższego rzędu.

## Radź sobie sam

O tym, jak niewdzięcznym zadaniem jest ręczne przydzielanie adresów IP, przekonał się zapewne każdy administrator sieci lokalnej, który stanął wobec konieczności zmiany przydzielonych komputerom adresów IP choćby ze względu na zmianę dostawcy Internetu. Czynność ta staje się dużo prostsza, jeśli korzystamy z DHCP czy maskowania adresów IP – wystarczy przekonfigurować serwer przydzielający adresy.

W nowym modelu adresowania przewidziano dwa mechanizmy automatycznej konfiguracji i przydzielania adresów IP. Pierwszy z nich, autokonfiguracja z uwzględnieniem stanu (stateful autoconfiguration), jest analogiczny do DHCP – host otrzymuje z serwera adres IP ze zdefiniowanej uprzednio puli, wraz z informacją o domyślnym routerze i adresie serwera nazw (DNS).

Drugi, autokonfiguracja bez uwzględnienia stanu, zakłada większą samodzielność hosta podłączanego do Sieci. Na podstawie numeru karty sieciowej MAC konstruuje on 64-bitowy identyfikator hosta LLUA (Link Local Unicast Address), po czym rozsyła do routerów SLA tzw. zapytanie konfiguracyjne (router solicitation). W odpowiedzi otrzymuje prefiks adresu, zawierający pozostałe segmenty, po czym automatycznie konfiguruje adres IP przez dodanie utworzonego ID do otrzymanego prefiksu. Korzystając z tej techniki, w celu zmiany adresów wszystkich hostów wystarczy zdefiniować na routerze nowy prefiks, a router sam go roześle do obsługiwanych hostów.

## Bezpieczny Internet

Bezpieczeństwo nie jest najmocniejszą stroną obecnej implementacji protokołu IP. O ile w IPv4 wszystkie zadania związane z zapewnieniem bezpieczeństwa w sieci spoczywały bądź na aplikacjach klienckich i serwerowych, bądź na protokołach wyższego poziomu, o tyle IP nowej generacji towarzyszy cały zestaw protokołów zabezpieczających IPSec, zapewniających potwierdzenie tożsamości nadawcy i odbiorcy pakietu oraz szyfrowanie przesyłanych danych.

IPSec działa niezależnie od aplikacji funkcjonujących w wyższych warstwach, tak więc nie zastępuje stosowanych w nich procedur bezpieczeństwa, a jedynie uzupełnia je, zabezpieczając przed próbami podszywania się pod innego nadawcę czy zmiany zawartości przesyłanego pakietu.

## Powoli do celu

Wszyscy zdają sobie doskonale sprawę, iż mimo oczywistych zalet IP nowej generacji wprowadzanie tego protokołu będzie procesem długim i stopniowym. W tej sytuacji przez pewien czas będziemy mieli do czynienia ze środowiskiem heterogenicznym, w którym współistnieć będą ze sobą obie wersje protokołu IP. Taka koegzystencja wymagać będzie odpowiedniego wsparcia zarówno ze strony osprzętu komunikacyjnego oraz oprogramowania systemowego, jak i samego protokołu. Obecnie większość nowych routerów posiada wbudowaną (bądź możliwość jej dodania) obsługę IPv6, również dla Uniksa powstał już odpowiedni stos IPv6. Windows 9x i NT 4.0 nie obsługują wprawdzie IPv6, jednak firma FTP Software napisała dla nich odpowiednie implementacje IP. Microsoft nie zaimplementował co prawda IPv6 w Windows 2000 (NT 5), mimo to znaleźć w nim można wiele usług wchodzących w skład IPv6, takich jak wspomniany IPSec, co może sugerować pełną implementację protokołu w przyszłości. „Roboczą" wersję stosu IPv6 dla Windows NT można znaleźć pod adresem *http://www.research.microsoft.com/msripv6/*. Aktualna lista produktów obsługujących IPv6 dostępna jest na stronie *http://playground.sun.com/pub/ipng/html/ipng-implementations.html*.

Również sam protokół IPv6 zawiera mechanizmy umożliwiające koegzystencję ze starszą wersja IP. Pierwszym z nich jest translacja adresów IPv4 na IPv6. Odbywa się ona w ten sposób, iż adres ipv4 zapisywany jest na ostatnich 32 bitach adresu typu unicast, pozostałe 96 bitów adresu wypełniane jest zerami. Technika służąca zachowaniu zgodności w drugą stronę jest bardziej skomplikowana i nosi nazwę tunelowania. W tym procesie pakiet IPv6 jest po stronie nadawcy pakowany do postaci pakietu IPv4 (enkapsulacja), przesyłany do odbiorcy za pośrednictwem sieci zgodnej z IPv4, po czym przekształcany z powrotem do pierwotnej postaci (dekapsulacja).

Mechanizmy tunelowania oraz szyfrowania przesyłanych danych, oprócz zapewnienia komunikacji pomiędzy sieciami pracującymi w różnych wersjach protokołu, ułatwiają również zestawianie tzw. VPN (Virtual Private Network), czyli bezpiecznych łączy komunikacyjnych przy wykorzystaniu sieci publicznej.

Obecnie prace nad implementacją IP nowej generacji prowadzone są dla większości systemów operacyjnych; również wszyscy liczący się producenci sieciowych urządzeń transmisyjnych bądź już przystosowali swe produkty do obsługi IPv6, albo intensywnie nad tym pracują.

*Marcin Pawlak*

### info

**Grupa dyskusyjna**

Pytania, uwagi i komentarze do artykułu można umieścić na grupie dyskusyjnej *news://news.vogel.pl/chip.artykuly*

**Internet**

**IPv6 w Polsce:**
http://www.6bone.pl/

**6Bone Home Page:**
http: //www.6bone.net/

**IPnG Home Page:**
http: //playground.sun.com/pub/ipng/html/

**IPnG Working Group:**
http: //www.ietf.org/html.charters/ipngwg-charter.html

**IPv6 Information Page:**
http: //www.ipv6.org/

**Understanding IP Addressing:**
http://www.3com.com/nsc/501302.html

CHIP CD 7/99 Specyfikacje protokołu Ipv6 można znaleźć na CHIP-CD 7/99 w dziale *CHIP-offline | Internet | Protokoły internetowe*