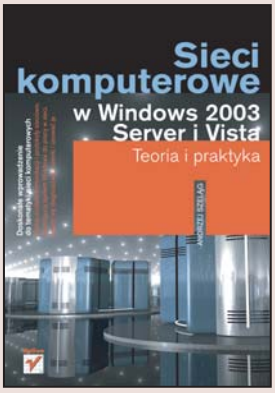
Sieci komputerowe w Windows 2003 Server i Vista. Teoria i praktyka



Autor: Andrzej Szeląg
ISBN: 978-83-246-1132-4
Format: B5, stron: 313
Przykłady na ftp: 4303 kB

Doskonałe wprowadzenie do tematyki sieci komputerowych

- Poznaj modele komunikacji i protokoły sieciowe
- Skonfiguruj system Windows do pracy w sieci
- Naucz się diagnozować usterki i usuwać je

„Dopiero sieć to komputer" – to hasło, spopularyzowane kilka lat temu, dziś nabiera nowego znaczenia. Popularnoś ć internetu roś nie w niesamowitym tempie, niemal na każdym osiedlu można znaleźć amatorską sieć komputerową, a w przedsiębiorstwach sieci są równie powszechne jak telefony i faksy. W każdym dostępnym obecnie systemie operacyjnym zaimplementowano mniej lub bardziej rozbudowane mechanizmy obsługi sieci. Nie inaczej jest w przypadku najnowszych wersji systemu Windows – Vista i 2003 Server. Producent tych systemów operacyjnych zapewnił użytkownikom nie tylko wygodne i czytelne mechanizmy konfiguracyjne, ale także zadbał o wysoki poziom bezpieczeństwa i ochrony przed zagrożeniami pochodzącymi z internetu.

Książka „Sieci komputerowe w Windows 2003 Server i Vista. Teoria i praktyka" to podręcznik adresowany do początkujących i ś rednio zaawansowanych użytkowników systemów Windows. W przejrzysty sposób objaś nia nie tylko zasady konfiguracji połączeń sieciowych w tych systemach, ale także podstawowe zagadnienia związane z funkcjonowaniem sieci komputerowych. Czytając ją poznasz model komunikacji OSI i TCP/IP, protokoły IPv4 i IPv6, różne architektury sieci komputerowych i mechanizmy działania usług sieciowych takich, jak DHCP i DNS. Nauczysz się definiować parametry sieci w systemach Windows, administrować siecią i monitorować jej działanie. Dowiesz się także, jak diagnozować i eliminować najczęś ciej występujące problemy.

- Zastosowania sieci komputerowych
- Urządzenia sieciowe
- Modele OSI i TCP/IP
- Protokoły internetowe IPv4 i IPv6
- Planowanie infrastruktury sieci
- Zadania serwera DNS i DHCP
- Instalacja i konfiguracja usług ActiveDirectory oraz DNS w Windows 2003 Server
- Przygotowanie systemu Windows Vista do pracy w sieci
- Korzystanie z narzędzi administracyjnych Windows
- Analiza ruchu sieciowego
- Narzędzia do rozwiązywania problemów z połączeniami sieciowymi

Poznaj zasady działania sieci komputerowych i skorzystaj z tej wiedzy w praktyce!

Wydawnictwo Helion
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl

Spis treści

Rozdział 3.

Protokoły sieciowe IPv4 i IPv6

W dobie niezwykle dynamicznego rozwoju Internetu zarządzanie różnymi sieciami komputerowymi wkracza w zupełnie nowy wymiar. O ile w niedalekiej przeszłości do różnych zastosowań wystarczały niepowiązane ze sobą standardy sieciowe, tworzone przez różne organizacje i instytucje, o tyle obecnie koniecznością staje się opracowanie jednej koncepcji zarządzania, która potrafiłaby zintegrować istniejące standardy sieciowe, a z drugiej strony pozwoliła korzystać z najnowszych rozwiązań. Jednym z tych rozwiązań jest protokół internetowy IPv6, któremu w znacznej części zostanie poświęcony niniejszy rozdział. Ten nowy protokół internetowy pozwala globalnej sieci wykorzystać ogromny potencjał, który jest dostępny za jej pośrednictwem. Dzięki wręcz nieograniczonej puli adresów i niezwykle wydajnym technikom adresacji protokół ten potrafi zapewnić dużo lepszy, znacznie wydajniejszy i bezpieczniejszy rozwój zarówno sieci lokalnych, jak też rozległych niż dotychczas obowiązujący protokół IPv4.

Protokół internetowy (ang. *Internet Protocol*) w wersji 4. (IPv4) został szczegółowo opisany w dokumencie *RFC 791* we wrześniu 1981 roku, a protokół IP w wersji 6. (IPv6) został opisany w dokumencie *RFC 1883* w grudniu 1995 roku oraz *RFC 2460* w grudniu 1998 roku. Wcześniej, w lipcu 1998 roku, pojawił się dokument *RFC 2373* dotyczący architektury adresowania IPv6. Wszystkie powyższe protokoły są dostępne w formie elektronicznej na stronie internetowej grupy IETF (ang. *The Internet Engineering Task Force*):

1. *IPv4*:
   - Internet Protocol (*http://www.ietf.org/rfc/rfc0791.txt*).
2. *IPv6*:
   - Internet Protocol, Version 6 (IPv6) Specification (*http://www.ietf.org/rfc/rfc1883.txt* oraz *http://www.ietf.org/rfc/rfc2460.txt*),
   - IP Version 6 Addressing Architecture (*http://www.ietf.org/rfc/rfc2373.txt*).

Dokumenty: *RFC 791*, *1833*, *2373* i *2460* znajdują się pod adresem *ftp://ftp.helion.pl/przyklady/siekwi.zip* w katalogu *RFC*.

Protokół internetowy (IP) jest bezpołączeniowym, a także zawodnym protokołem warstwy sieciowej, odpowiedzialnym za transport danych, czyli wymianę datagramów IP, i służy do adresowania oraz routingu (kierowania) tych datagramów między różnymi urządzeniami sieciowymi — między odbiorcą a nadawcą. Użyty tutaj termin *bezpołączeniowy* oznacza, że sesja nie jest ustanawiana przed rozpoczęciem wymiany danych, tzn. nie muszą zostać zapewnione wstępne warunki komunikacji, takie jak ustanowienie połączenia. Stąd też protokół IP jest określany mianem *zawodny*. Termin ten oznacza, że dostarczenie datagramu IP nie jest gwarantowane przez ten protokół, tj. nie jest zagwarantowana żadna kontrola poprawności dostarczenia datagramu IP od nadawcy do odbiorcy. Protokół IP jest jednym z podstawowych mechanizmów wykorzystywanych w Internecie i służy zazwyczaj jako wspólna platforma dla innych protokołów warstw wyższych, np. protokołu transportowego TCP (ang. *Transmission Control Protocol*).

Do podstawowych funkcji protokołu internetowego (IP) należą m.in.:

- enkapsulacja datagramów IP w ramki, które przesyłane są nośnikiem transmisyjnym do odbiorcy,
- udostępnianie podstawowych usług dostarczania datagramów IP,
- zapewnienie podziału datagramu IP na mniejsze części, które będą akceptowane przez sieć komputerową (fragmentacja), i ponowne ich złożenie w jedną całość (defragmentacja).

Protokół internetowy (IP) zawsze próbuje dostarczyć datagram IP. Jednak przesyłane datagramy mogą zostać zagubione, dostarczone w innej kolejności niż ta, w której zostały wysłane, opóźnione lub zdublowane. Z jednej strony jest to ograniczenie możliwości poprawnej komunikacji, z drugiej zaś — przy założeniu, że kontrolę nad poprawnym przesłaniem datagramu IP przejmuje protokół transportowy TCP — protokół IP zyskuje dzięki temu wszechstronność zastosowań. Mianowicie dzięki niemu można szybko i łatwo przesłać za pomocą sieci komputerowych takie dane, jak głos, wideo czy inne dane strumieniowe. Protokół IP doskonale nadaje się do wykorzystania w przypadku wideokonferencji, gdy nie jest wymagane, by dane te były w 100% w stanie nienaruszonym.

Protokół ten nigdy nie naprawia wymienionych błędów. Są one naprawiane dopiero przez protokoły warstwy wyższej, tj. przez wspomniany już protokół transportowy TCP.

W tym rozdziale zostanie zaprezentowany protokół IP zarówno w wersji 4. (IPv4), jak też 6. (IPv6). Poza tym zostaną przedstawione cechy obu protokołów.

Wprowadzenie do protokołu IP

Zarówno systemy operacyjne Windows Server 2003, jak i Windows Vista zawierają protokół IP w wersji 4. (oznaczonej jako IPv4) oraz jego najnowszą wersję, 6. (oznaczoną jako IPv6). Jednakże w systemie Windows Server 2003 domyślnie instalowany jest jedynie protokół IP w wersji 4. Protokół IP w wersji 6. jest dostępny po zainstalowaniu go oraz odpowiednim skonfigurowaniu. W przypadku systemu operacyjnego Windows Vista domyślnie zainstalowane są obie wersje protokołu. Protokół IPv6 jest wbudowany w ten system.


Uwaga

Przed wersją 6. protokołu IP powstała wersja 5., jednak została ona zastrzeżona dla różnych niezrealizowanych protokołów, które miały zastąpić protokół IPv4.

Generalnie działanie protokołu internetowego (IP) można przedstawić następująco. Podczas wysyłania danych protokół internetowy źródłowego urządzenia sieciowego (np. komputera klienckiego) ustala, czy miejsce przeznaczenia tych danych znajduje się w tym samym segmencie sieci czy w innym. Protokół IP określa to, wykonując dokładnie dwa obliczenia, a następnie porównuje ich wynik. Jeżeli wyniki są identyczne, oznacza to, że miejsce przeznaczenia znajduje się w segmencie sieci lokalnej. W przeciwnym razie jest to miejsce odległe, np. w innym segmencie lub innej sieci. Jeżeli miejsce przeznaczenia jest lokalne, protokół IP inicjuje połączenie bezpośrednie. W przypadku odległego punktu docelowego protokół IP nawiązuje łączność przez bramę domyślną. W sieciach rolę takiej bramy zwykle pełni urządzenie aktywne, zwane routerem. Gdy źródłowy protokół IP zakończy przygotowywanie datagramu IP do wysłania, przekazuje go do warstwy dostępu do sieci; następnie sieć przekazuje go do nośnika transmisji, po którym wędruje do miejsca przeznaczenia. Gdy dane dotrą do miejsca przeznaczenia (np. innego komputera), otrzymuje je najpierw warstwa dostępu do sieci na tym docelowym komputerze. Następnie dane są sprawdzane pod kątem ewentualnych błędów, weryfikowany jest też adres IP (jego poprawność). Jeśli testy wypadły pozytywnie, warstwa dostępu do sieci oddziela właściwe dane od reszty ramki i przekazuje je do protokołu (zazwyczaj jest to protokół IP), który został podany w polu *typ ramki*. Po otrzymaniu datagramu z warstwy dostępu do sieci protokół IP sprawdza, czy nie został on uszkodzony podczas transmisji. Następnie sprawdza ponownie miejsce przeznaczenia (docelowe), porównując adres IP urządzenia docelowego (zapisanego w datagramie) z adresem IP lokalnego komputera. Jeżeli adresy są identyczne, oznacza to, że dane zostały dostarczone we właściwe miejsce. Protokół IP sprawdza tzw. pola w datagramie, aby odczytać instrukcje wysłane przez protokół IP urządzenia źródłowego. Instrukcje te wymagają zazwyczaj, aby protokół IP na komputerze docelowym wykonał określone funkcje. Dość często są to informacje dotyczące dostarczenia danych do protokołów TCP lub UDP w warstwie transportowej systemu protokołów TCP/IP.

W aplikacjach sieciowych niemal każda warstwa i protokół muszą dołączyć informację dla swoich potrzeb, która jest umieszczana przed polem *dane* i jest określana jako *nagłówek*. Nagłówek ten obejmuje kilka oddzielnych fragmentów informacji określanych jako *pola*. Pole może zawierać adres docelowy datagramu IP albo informować, co należy zrobić z danymi, gdy osiągną miejsce przeznaczenia. Zazwyczaj jest tak, że protokół IP tworzy nagłówek w komputerze źródłowym. W miejscu odbioru protokół IP analizuje

instrukcje zawarte w nagłówku oraz ustala, co zrobić, tj. gdzie przesłać dane zawarte w datagramie IP. W nagłówku znajduje się dużo informacji, w tym adres komputera źródłowego i docelowego oraz informacje dla routerów, jeżeli są w sieci. Każdy router, przez który przechodzi datagram IP na drodze od źródła do miejsca przeznaczenia, także analizuje część nagłówka IP.


Uwaga

W numerze IP (w wersji 4.) komputera są zawarte dwie ważne informacje: *numer podsieci* oraz *numer hosta* w tej podsieci. Aby je odseparować od siebie, potrzebna jest *maska podsieci*, która jest 32-bitową liczbą składającą się z czterech liczb oddzielonych kropkami, np. 255.255.255.0.

Protokół Internetu w wersji 4. (IPv4)

Adresowanie IPv4

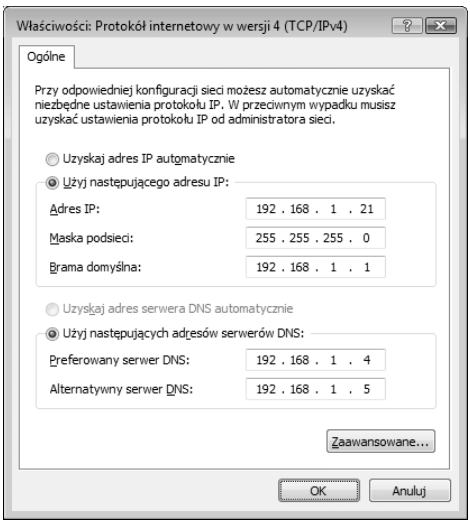
Sieci lokalne, jak już wspomniano, są często dzielone za pomocą routerów na podsieci, czyli mniejsze fragmenty, zwane *segmentami*. Taki podział zwykle ma na celu ograniczenie nadmiernego ruchu sieciowego. Pozwala to nie tylko ograniczyć nadmierny ruch w sieci, ale także wprowadzić hierarchiczną strukturę, tak aby dane mogły bez przeszkód znaleźć drogę do miejsca przeznaczenia. Protokół TPC/IP zapewnia możliwość tworzenia podsieci dzięki użyciu *adresowania logicznego*.

Adres logiczny (ang. *logical address*) to adres nadany każdemu urządzeniu sieciowemu podczas konfigurowania ustawień oprogramowania sieciowego. Inaczej mówiąc, jest to adres skonfigurowany przez oprogramowanie sieciowe. W przypadku karty sieciowej adres ten jest konfigurowany w jej właściwościach za pomocą interfejsu wbudowanego w system operacyjny.

Każde urządzenie sieciowe podłączone do sieci, zanim zacznie się komunikować, musi mieć nadany adres logiczny, który jest dość często nazywany adresem IP (ang. *IP address*). Adres ten używany jest w sieci TCP/IP do zlokalizowania dowolnego urządzenia sieciowego w sieci. Przykładowa konfiguracja ustawień protokołu TCP/IP fizycznej karty sieciowej zainstalowanej w komputerze działającym pod kontrolą systemu Microsoft Windows Vista Business została przedstawiona na rysunku 3.1.

Trzy z zaznaczonych na powyższym rysunku pól, które są zawarte w oprogramowaniu IP, są kluczowe dla komunikacji pomiędzy komputerami znajdującymi się w różnych sieciach:

- *pole adresu IP* — unikatowy 32-bitowy adres przypisany do hosta sieciowego;
- *pole maski podsieci* — 32-bitowe pole, które pozwala określić, jaką część adresu IP stanowi część sieciowa adresu (sieci), a jaką część hosta;



Rysunek 3.1. *Okno dialogowe Właściwości: Protokół internetowy w wersji 4 (TCP/IPv4)*

- *pole bramy domyślnej* — 32-bitowy adres, który identyfikuje adres routera oraz kieruje pakiety danych (datagramy IP) w odpowiednie miejsce w innej podsieci.


Uwaga

System adresowania logicznego umożliwia implementację takiego systemu numeracji sieci, który będzie odzwierciedlał jej wewnętrzną strukturę. W przypadku sieci opartych na protokole TCP/IP adres logiczny jest przekształcany za pomocą protokołów ARP w adres fizyczny karty sieciowej. Adresy IP zapewniają dostarczenie danych we właściwe miejsce. Istnieje tu pewna analogia do adresów budynków. Dzięki nim poczta wie, gdzie dostarczyć przesyłkę.

Każde urządzenie sieciowe, takie jak komputer i drukarka, które korzysta z protokołu TCP/IP, powinno mieć nadany 32-bitowy adres IP (w wersji 4.). Adres ten podzielony jest na dwie części:

- *ID sieci*,
- *ID hosta*.

Protokół TCP/IP (w wersji 4.) korzysta z 32-bitowych adresów IP złożonych z liczb *0* oraz *1*, które trudno jest zapamiętać, dlatego że jest to ciąg nic nieznaczących dla człowieka liczb *0* oraz *1*. Dla ułatwienia ten ciąg bitów podzielono na cztery części, które nazwano *oktetami* i rozdzielono kropkami, tak jak na listingu 3.1.

Listing 3.1. *Adres IP podzielony na cztery oktety rozdzielone kropkami*

```
110000000.10101000.00000001.00010001
```

Każdy z czterech powyższych oktetów zawiera bloki po 8 bitów (liczb 0 i 1), które dla jeszcze większego uproszczenia przekształca się w liczby dziesiętne, dość łatwe do zapamiętania. I tak jednemu oktetowi (np. 11111111) można przypisać liczbę dziesiętną z zakresu 0 – 255.

W dalszej części rozdziału (w przykładzie 3.) znajduje się szczegółowe wyjaśnienie sposobu, w jaki można dokonać szybkiej konwersji liczby binarnej (np. 11111111) na jej postać dziesiętną, czyli 255.

Praca z TCP/IP wymaga umiejętności przekształcania liczby binarnej zapisanej w oktecie na jej odpowiednik dziesiętny (liczbę dziesiętną), a także operacji odwrotnej. Proces ten nie jest skomplikowany i każdy, kto potrafi obsługiwać kalkulator dostępny w systemie Windows, może to zrobić.

Poniżej pokazano, jak prosto i szybko można wykonać tę konwersję i jak zapisać 32-bitowy adres w postaci czterech liczb dziesiętnych oddzielonych kropkami (.), czyli w *notacji kropkowo-cyfrowej*.

Aby skonwertować liczbę binarną na dziesiętną i na odwrót, należy uruchomić kalkulator systemu Windows Vista Business.

Przykład 1.

Aby uruchomić kalkulator wbudowany w system Windows Vista Business oraz odpowiednio go przygotować do przeprowadzania konwersji pomiędzy różnymi systemami liczb, należy wykonać dwa poniższe kroki:

1. Z poziomu systemu Windows Vista Business należy wybrać przycisk *Start* i z wiersza poleceń wpisać polecenie `calc`. Zostanie uruchomiony wbudowany kalkulator Windows z ustawieniami domyślnymi, które przedstawia rysunek 3.2.

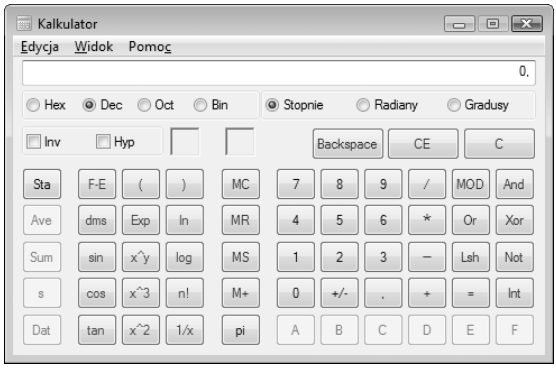
Rysunek 3.2. *Kalkulator Windows w trybie standardowym*

2. Na pasku menu należy wybrać opcję *Widok*, a następnie przełączyć kalkulator na tryb *Naukowy*. Domyślnie kalkulator ustawiony jest na system dziesiętny (aktywna opcja *Dec*), co pokazuje rysunek 3.3.

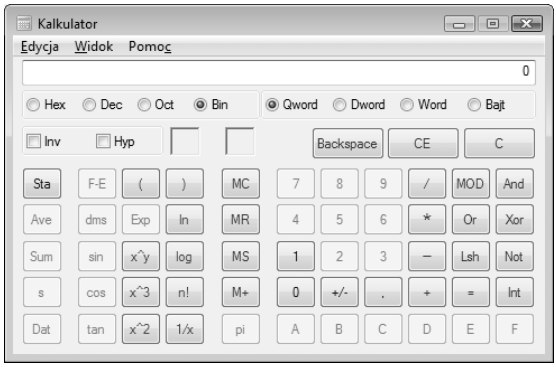
Przykład 2.

Aby skonwertować liczbę binarną, np. 11000000, na jej dziesiętny odpowiednik, należy:

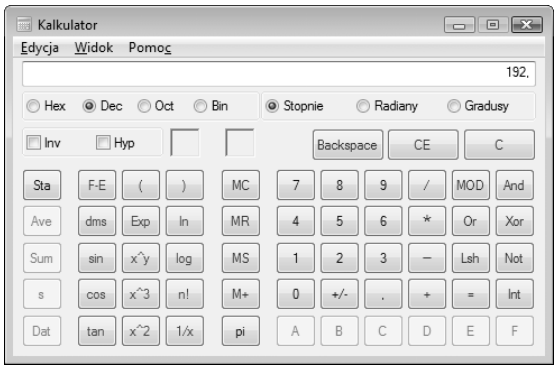
1. Uaktywnić w kalkulatorze opcję *Bin* (zamiast domyślnej *Dec*), co przedstawia rysunek 3.4.
2. Wpisać w polu liczbę binarną, np. 11000000, i wybrać opcję *Dec*. Zostanie wyświetlona wartość dziesiętna liczby 11000000, czyli 192, co przedstawia rysunek 3.5.



Rysunek 3.3. *Kalkulator Windows w trybie naukowym*



Rysunek 3.4. *Kalkulator w trybie naukowym*

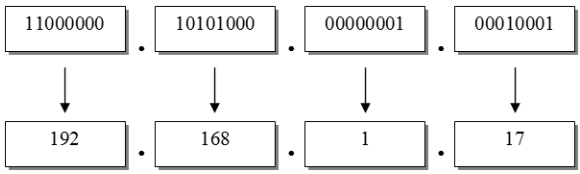


Rysunek 3.5. *Kalkulator — zamiana liczby binarnej na dziesiętną*

Jak widać na powyższych rysunkach, konwersja liczby binarnej na jej postać dziesiętną nie jest trudna. I tak liczbie binarnej 11000000 odpowiada liczba dziesiętna 192.

W bardzo podobny sposób można wykonać konwersję odwrotną, tj. liczby dziesiętnej 192 na binarną 11000000. Wystarczy wpisać w kalkulatorze wartość 192 i wybrać opcję *Bin*.

Po skonwertowaniu wszystkich czterech oktetów adresu IP z listingu 3.1 (zapisanego w postaci binarnej) na postać dziesiętną otrzymuje się bardziej przystępną dla człowieka postać adresu IP (w notacji kropkowo-cyfrowej), co pokazuje rysunek 3.6.



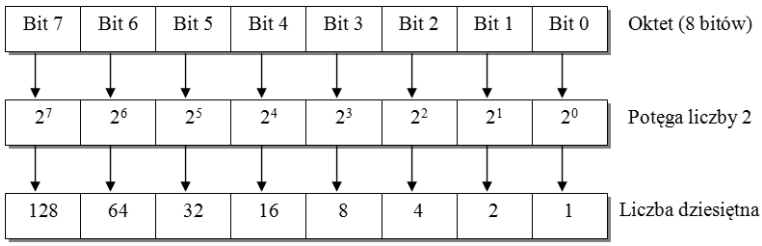
Rysunek 3.6. *Konwersja adresu binarnego na dziesiętny*

Jak oktet binarny adresu IP został przekonwertowany na postać dziesiętną? Otóż arytmetyka binarna opiera się na potęgach liczby 2, gdyż są w niej tylko dwie liczby: 0 oraz 1. Przed przystąpieniem do konwersji należy te potęgi dokładnie poznać. Tabela 3.1 pokazuje kolejnych osiem potęg liczby 2. I tak kolejne potęgi liczby 2 to: 1, 2, 4, 8, 16, 32, 64 oraz 128. Najmniejszą potęgę umieszczono w oktecie po prawej stronie, największą — lewej.

Tabela 3.1. *Potęgi liczby 2 oraz ich odpowiedniki*

Potęga liczby 2	Odpowiednik binarny	Odpowiednik dziesiętny
2^7	**1**0000000	**128** (**1**+0+0+0+0+0+0+0)
2^6	0**1**000000	**64** (0+**1**+0+0+0+0+0+0)
2^5	00**1**00000	**32** (0+0+**1**+0+0+0+0+0)
2^4	000**1**0000	**16** (0+0+0+**1**+0+0+0+0)
2^3	0000**1**000	**8** (0+0+0+0+0+**1**+0+0)
2^2	00000**1**00	**4** (0+0+0+0+0+0+**1**+0)
2^1	00000**1**0	**2** (0+0+0+0+0+0+0+**1**)
2^0	00000000	**1** (0+0+0+0+0+0+0+0)

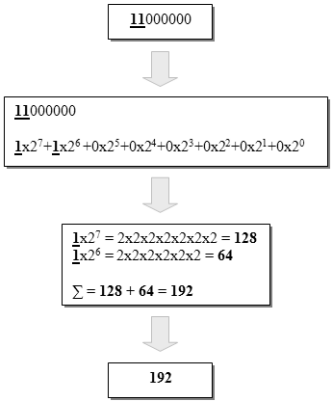
Rozpoczynając obliczenia (zgodnie z powyższą tabelą), należy wypisać te pozycje, którym odpowiada liczba 1 (jeden). Zera należy pominąć, gdyż dodawanie zer nic (poza zerem) nie daje. Następnie należy dodać wybrane z danego oktetu liczby 1. Jeżeli przykładowo liczba binarna ma postać 110000000, to pierwsza skrajna lewa jedynka (1) odpowiada liczbie dziesiętnej 128, druga liczbie 64 itd. Pozostałe liczby (te z zerami) pomija się. Na rysunku 3.7 przedstawiono w formie graficznej potęgi liczby 2 oraz ich odpowiedniki.



Rysunek 3.7. *Potęgi liczby 2 oraz ich odpowiedniki*

Suma liczb 128 i 64 daje wartość dziesiętną 192. Tak więc przekształcenie liczby binarnej 11000000 na liczbę dziesiętną daje wartość 192, co pokazano na rysunku 3.8.

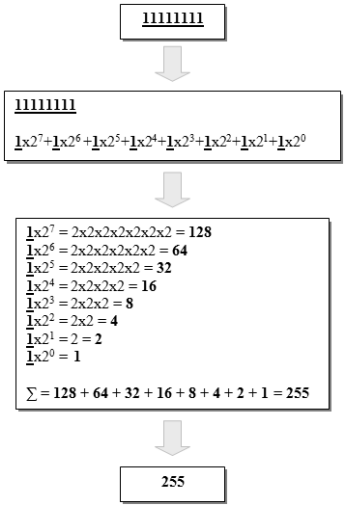
Rysunek 3.8.
Konwersja oktetu binarnego na postać dziesiętną



Przykład 3.

Jak przekształcić liczbę binarną 11111111 na wartość dziesiętną? W taki sam sposób jak w przykładzie 2. Rysunek 3.9 przedstawia proces konwersji.

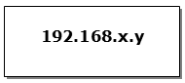
Rysunek 3.9.
Konwersja liczby 11111111 na postać dziesiętną



Czytelnik już wie, jak przekształcić pojedynczy oktet (osiem bitów 0 i 1) na liczbę dziesiętną. Jednak adres logiczny ma 32 bity, a nie 8. Aby zapisać całą liczbę binarną, należy skorzystać z powyżej przedstawionej notacji dziesiętno-kropkowej. Zapis taki składa się z czterech liczb dziesiętnych rozdzielonych kropkami.

Ponieważ liczby dziesiętne mogą się zmieniać, dość często w zapisie korzysta się ze zmiennych reprezentujących cztery liczby: *w, x, y* oraz *z*. Można więc spotkać się z ogólnym zapisem *w.x.y.z* lub zapisem mieszanym, który wygląda jak na rysunku 3.10.

Rysunek 3.10.
Zapis mieszany 32-bitowego adresu IP



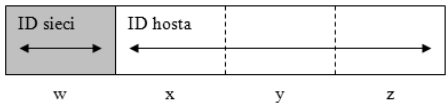
Klasy adresów IPv4

W sieci lokalnej każdy host sieciowy powinien mieć ten sam ID sieci, gdyż wszystkie należą do jednej sieci. Również każdy z hostów powinien mieć unikatowy adres IP hosta, aby całość tworzyła niepowtarzalny adres IP. Większość hostów sieciowych ma jeden adres IP i dla nich jest to IP hosta. Jednak niektóre komputery (np. serwery pełniące wiele ważnych funkcji sieciowych) mogą mieć więcej niż jedną kartę sieciową, a zatem i kilka adresów IP.

Kiedy TCP/IP zaczynał funkcjonować, nikt nie przewidywał skali i dynamiki jego rozwoju. Za pomocą 32-bitowego adresu logicznego (adresu IPv4) można zaadresować 2^{32} urządzeń sieciowych, tj. około 4 miliardy ($4{,}2*10^9$). W praktyce nie jest to aż tak duża liczba, jak można by przypuszczać, dlatego długi adres został podzielony na grupy, które zostały nazwane *klasami*. Istnieją klasy oznaczone jako: *A, B, C, D* oraz *E*. Najważniejsze z punktu widzenia sieci komputerowych są obecnie trzy klasy: *A, B* oraz *C*, które odnoszą się do różnych typów identyfikatorów sieciowych (*ID sieci*). Klasa *D* jest używana zwykle do *multiemisji*, klasa *E* zaś jest zarezerwowana do celów eksperymentalnych (na potrzeby badań dla organizacji standaryzacyjnej IETF, która działa w zakresie szeroko pojętych sieci komputerowych oraz protokołów transmisji danych) i nie jest wykorzystywana do adresacji hostów sieciowych. Stąd też klasami *D* oraz *E* nie będę się zajmował. Skupię się jedynie na trzech najważniejszych klasach adresów IP, najczęściej wykorzystywanych w sieciach komputerowych: *A, B* oraz *C*.

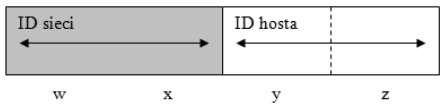
Adresy klasy *A* mają 8-bitowy identyfikator sieci (ID sieci) i zazwyczaj są przyporządkowane organizacjom, które potrzebują dużej liczby adresów IP, co przedstawia rysunek 3.11. Istnieje 126 możliwych sieci klasy *A*.

Rysunek 3.11.
Adresy klasy A



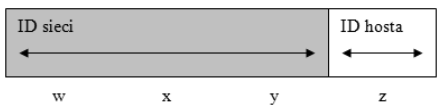
Adresy klasy *B* mają 16-bitowy identyfikator sieci (ID sieci) oraz są przyporządkowane tym organizacjom, które potrzebują średniej liczby adresów IP, co przedstawia rysunek 3.12. Istnieje 16 384 możliwych sieci klasy *B*.

Rysunek 3.12.
Adresy klasy B



Adresy klasy *C* mają 24-bitowy identyfikator sieci (ID sieci) oraz są przyporządkowane organizacjom potrzebującym małej liczby adresów IP, co przedstawia rysunek 3.13. Sieci klasy *C* są ponad 2 miliony (dokładnie 2 097 152).

Rysunek 3.13.
Adresy klasy C



W tabeli 3.2 przedstawiono charakterystykę klas adresów IPv4 wraz z domyślnymi maskami podsieci, liczbą sieci oraz hostów sieciowych.

Tabela 3.2. *Charakterystyka klas adresów IP*

Klasa	Pierwszy oktet	Domyślna maska podsieci	Liczba sieci	Liczba hostów w sieci
A	1 – 126	255.0.0.0	126	16 777 214
B	128 – 191	255.255.0.0	16 384	65 534
C	192 – 223	255.255.255.0	2 097 152	254
D	224 – 239	-	-	-
E	240 – 255	-	-	-


Uwaga

Maska podsieci służy do dzielenia wszystkich adresów na logicznie powiązane ze sobą grupy.

Do komunikacji w sieci publicznej należy używać adresów, które zostały przydzielone przez urząd IANA (ang. *Internet Assigned Numbers Authority*). Mała firma ma adres publiczny przydzielony przez usługodawcę internetowego ISP (ang. *Internet Service Provider*), który otrzymał zakres adresów publicznych od IANA.


Uwaga

Zakres jest pełnym obszarem kolejnych możliwych do przydzielenia w danej sieci adresów IP.

Nie wszystkie adresy są wykorzystywane w sieci publicznej, np. wspomniana klasa *E*. Dodatkowo istnieje pula *prywatnych adresów IP*[1], które mogą być wykorzystane tylko w sieciach lokalnych, tj. można je przypisywać tylko do hostów sieciowych zlokalizowanych w sieciach lokalnych.

Organizacja IANA zarezerwowała następujące trzy bloki przestrzeni adresów IP dla sieci prywatnych:

- *10.0.0.0 – 10.255.255.255* — dla sieci klasy *A* z maską podsieci *255.0.0.0*;
- *172.16.0.0 – 172.31.255.255* — dla sieci klasy *B* z maską podsieci *255.255.0.0*;
- *192.168.0.0 – 192.168.255.255* — dla sieci klasy *C* z maską podsieci *255.255.255.0*.

Wady protokołu IPv4

Obecnie wykorzystywana wersja protokołu internetowego, IPv4, nie zmieniła się w dość istotny sposób od czasu opublikowania go w dokumencie *RFC 791*, tj. od roku 1981. Jak wiadomo, protokół ten funkcjonuje do dziś w praktycznie wszystkich sieciach,

[1] Więcej informacji na temat prywatnych adresów IP można znaleźć w dokumencie *RFC 1918*, który dostępny jest pod adresem *http://www.rfc-editor.org/rfc/rfc1918.txt*.

zarówno lokalnych, jak i rozległych. Jednak jego twórcy nie przewidzieli kilku podstawowych zjawisk, do których można zaliczyć:

- *Gwałtowny rozwój Internetu oraz wyczerpanie się przestrzeni adresowej IPv4*. Zmusiło to organizacje do używania translatorów adresów sieciowych NAT (ang. *Network Address Translation*) w celu mapowania wielu adresów prywatnych na jeden adres publiczny. Takie rozwiązanie powoduje jednak problemy z zaszyfrowanym za pomocą protokołu IPSec ruchem sieciowym, co znacznie ogranicza jego zastosowanie.
- *Potrzebę uproszczenia konfiguracji*. Bieżące implementacje protokołu IP w wersji 4. (IPv4) konfigurowane są ręcznie albo przy użyciu protokołu DHCP. Protokół DHCP daje skalowalność protokołowi IPv4, z drugiej jednak strony wymusza konieczność konfigurowania infrastruktury DHCP i zarządzania nią.
- *Płaską infrastrukturę routingu*. Obecnie Internet to połączenie routingu płaskiego oraz hierarchicznego, co skutkuje m.in. wolniejszym przekazywaniem ruchu.
- *Wymaganie zabezpieczeń na poziomie protokołu IP*. W obecnych czasach jest to bardzo ważny element, gdyż komunikacja prywatna przez Internet wymaga usług szyfrowania, które chronią dane przed odczytywaniem i modyfikowaniem podczas ich przesyłania. Ten problem starano się rozwiązać, tworząc osobny standard: IPSec.
- *Mobilność*. Tworzy nowe wymagania stawiane urządzeniom sieciowym podłączonym do Internetu oraz umożliwia zmianę adresu internetowego w zależności od fizycznego miejsca przyłączenia do Internetu, z jednoczesnym zachowaniem istniejącego połączenia.

Z myślą o rozwiązaniu powyższych problemów grupa IETF (ang. *Internet Engineering Task Force*) opracowała w roku 1995 zestaw protokołów oraz standardów znanych jako protokół IPv6, czyli protokół internetowy IP w wersji 6. Ta nowa wersja protokołu internetowego łączy w sobie wiele proponowanych metod zaktualizowania dotychczasowego protokołu, czyli IPv4, a także stwarza nowe możliwości. Jednocześnie jest ogromnym wyzwaniem, jeśli chodzi o zarządzanie coraz większymi i bardziej złożonymi sieciami w kontekście wielu istniejących standardów i niewielkiej liczby aplikacji, które by ją obsługiwały. Z drugiej strony przy projektowaniu protokołu IPv6 starano się unikać dodawania wielu nowych funkcji, tak aby wpływ nowego projektu na protokoły wyższych i niższych warstw był jak najmniejszy. Twórcy nowego protokołu mieli głównie na uwadze zastosowanie go nie tylko w różnych urządzeniach sieciowych, ale także w telefonach komórkowych, czy nawet kamerach.

Protokół Internetu w wersji 6. (IPv6)

Systemem firmy Microsoft, w którym protokół IPv6 pojawił się po raz pierwszy, był Windows XP w roku 2001. Od tego czasu firma Microsoft wyposaża w niego wszystkie swoje systemy. I tak systemy z rodziny Windows Server 2003 obsługują protokół IPv6, choć domyślnie nie jest on w nich instalowany, jako standardowy protokół do obsługi

komunikacji sieciowej. Dopiero w najnowszych systemach operacyjnych, tj. Windows Vista, protokół IPv6 został wbudowany i standardowo jest wykorzystywany do obsługi zarówno sieci lokalnych, jak i rozległych.

Protokół internetowy IPv6 stanowi odpowiedź na ograniczenia poprzedniej jego wersji, IPv4, i ma następujące funkcje:

1. *Nowy format nagłówka datagramu IP*. Został zaprojektowany tak, aby zminimalizować obciążenia związane z jego przetwarzaniem.


Wskazówka

Zarówno nagłówki protokołu IPv4, jak też IPv6 nie współdziałają ze sobą, gdyż protokół IPv6 nie jest zgodny z protokołem IPv4. Aby więc host sieciowy działający pod kontrolą systemu operacyjnego Windows Vista mógł rozpoznawać i przetwarzać oba formaty nagłówków, musi korzystać z implementacji zarówno protokołu IPv4, jak też IPv6 (ustawienie domyślne). Nowy nagłówek protokołu IPv6 jest dwa razy większy od nagłówka protokołu IPv4, chociaż 128-bitowe adresy IPv6 są aż czterokrotnie dłuższe od 32-bitowych adresów IPv4.

2. *Duża przestrzeń adresowa*. Adresy IPv6 mają długość 128 bitów, co daje ogromną liczbę adresów do wykorzystania. Jednak głównym celem zaprojektowania tak dużej przestrzeni adresowej protokołu internetowego IPv6 było umożliwienie tworzenia wielu poziomów podsieci, alokacji adresów w Internecie oraz sieciach lokalnych.


Wskazówka

Konfiguracja sieci komputerowej opartej na protokole IPv6 odbywa się w sposób analogiczny jak w poprzedniej wersji, IPv4. Każdy użytkownik jest w stanie samodzielnie wykonać potrzebne operacje.

3. *Wydajna i hierarchiczna infrastruktura adresowania i routingu*. Adresy IPv6 używane w części IPv6 Internetu zostały tak zaprojektowane, aby tworzyły bardzo wydajną, hierarchiczną infrastrukturę routingu, która zakłada istnienie wielu poziomów usługodawców internetowych.
4. *Bezstanowa i akumulująca stan konfiguracja adresów*. Protokół IPv6 obsługuje:
   - *konfigurację adresów IPv6 akumulującą stan* — konfigurację adresów IPv6 przy obecności serwera DHCP;
   - *bezstanową konfigurację adresów IPv6* — konfigurację adresów IPv6 przy braku serwera DHCP. W tej konfiguracji hosty podłączone do łącza konfigurują dynamicznie swoje adresy IPv6 dla tego łącza (adresy lokalne dla łącza) oraz adresy, które uzyskują na podstawie prefiksów anonsowanych przez routery lokalne.
5. *Wbudowane zabezpieczenia*. Protokół internetowy IPv6 wymaga obsługi protokołu IPSec do zabezpieczania ruchu sieciowego, dlatego jest bezpieczniejszy od IPv4.
6. *Obsługa mechanizmu jakości usługi (Quality of Service)*. Identyfikacja ruchu sieciowego na podstawie nowego pola zaimplementowanego w nagłówku IPv6 o nazwie *Etykieta strumieniowa* umożliwia, np. routerom, zidentyfikowanie

datagramów IP należących do strumienia i zapewnienie ich lepszej obsługi. Należy pamiętać, że strumień ten jest serią wielu datagramów IP i jest przesyłany między hostem źródłowym a docelowym.

7. *Nowy protokół interakcji pomiędzy hostami*. Jest to protokół pomocniczy Neighbor Discovery (ND). Wchodzi w skład protokołu ICMPv6, który zarządza interakcją między hostami sieciowymi czy routerami. Protokół pomocniczy Neighbor Discovery dla IPv6 zajmuje się m.in. zamianą adresów IP na adresy fizyczne (tak jak protokół ARP dla IPv4).

Protokół Neighbor Discovery to zestaw komunikatów oraz procesów, które są używane do określania relacji między sąsiednimi hostami sieciowymi czy routerami. Protokół ten został opisany w dokumencie *RFC 2461*, który jest dostępny pod adresem *http://www.ietf.org/rfc/rfc2461.txt*, oraz w dalszej części niniejszego rozdziału.

Adresowanie IPv6

Jak już wspomniano, obecnie do adresacji sieci lokalnych oraz rozległych wykorzystywane są 32-bitowe adresy IPv4, podzielone na oktety, czyli cztery bloki 8-bitowe, z których każdy przekształcany jest na jego dziesiętny odpowiednik i rozdzielany kropką.

Protokół IPv6 może używać dużo dłuższych adresów IP niż IPv4. Rozmiar adresu IPv6 wynosi aż 128 bitów, czyli czterokrotnie więcej niż w protokole IPv4. Jak łatwo policzyć, 32-bitowa przestrzeń adresowa w protokole IPv4 umożliwia utworzenie 2^{32} możliwych adresów IPv4, co odpowiada około 4 miliardom urządzeń sieciowych ($4{,}2*10^{9}$), a 128-bitowa przestrzeń adresowa IPv6 umożliwia utworzenie 2^{128} ($3{,}4*10^{38}$) możliwych adresów IPv6. W odróżnieniu od adresów pojedynczej transmisji IPv4 struktura takiego samego adresu IPv6 jest niezwykle prosta. Otóż pierwsze 64 bity adresu IPv6 są generalnie przeznaczone do identyfikowania podsieci (adresów logicznych), a ostatnie — fizycznej karty sieciowej (adresów fizycznych).

Znajomość podstawowych właściwości nowego protokołu internetowego w wersji 6. oraz związanych z nim wymiernych korzyści jest niezbędna w zrozumieniu zasad wdrażania tego protokołu.

Ze względu na ogromną przestrzeń adresową protokołu internetowego IPv6 przedstawianie pojedynczego adresu może być trudne, a to ze względu na jego zapis, tj. notację szesnastkową z dwukropkami. Dlatego 128-bitowe adresy IPv6 dzielone są na bloki 16-bitowe, a następnie każdy z tych bloków jest przekształcany na 4-cyfrową liczbę szesnastkową (w przeciwieństwie do formatu dziesiętnego w protokole IPv4), którą rozdziela się znakiem dwukropka (:). Taka reprezentacja adresu internetowego IPv6 jest nazywana *zapisem dwukropkowo-cyfrowym* i została przedstawiona na rysunku 3.14.

Rysunek 3.14. *Przykładowy adres IPv6*

2001:0:4136:E38C:2C8A:A338:7EAE:FEE1

Jak widać na powyższym rysunku, adresy IPv6 są znacznie dłuższe oraz dużo trudniejsze do zapamiętania niż adresy IPv4. Zamiast zapamiętywać skomplikowane adresy IPv6, można używać nazw, które są łatwiejsze do zapamiętania i dużo bardziej przystępne dla człowieka. Przykładowy adres IPv6 w zapisie binarnym przedstawiono na listingu 3.2.

Listing 3.2. *Przykładowy adres IPv6 w zapisie binarnym*

```
10000000000001000000000000000010000010011011011100011100011100
10110010000010101000110011100011111101010111011111111011100001
```

128-bitowy adres IPv6 jest dzielony na mniejsze bloki (8 bloków) o wielkości 16-bitów (czyli 8*16 = 128), co przedstawia listing 3.3.

Listing 3.3. *128-bitowy adres IPv6 podzielony na 8 bloków o wielkości 16-bitów*

```
10000000000001 0000000000000000 1000001001101l0 1110001110001100
10110010000010 1010001100111000 1111110101011l0 1111111011100001
```

Każdy blok 16-bitowy jest przekształcany na liczbę szesnastkową, a następnie oddzielany dwukropkiem, co przedstawia listing 3.4.

Listing 3.4. *128-bitowy adres IPv6 przekształcony na liczbę szesnastkową*

```
2001:0:4136:E38C:2C8A:A338:7EAE:FEE1
```

Reprezentacja każdego 128-bitowego adresu IPv6 może być dodatkowo uproszczona przez usunięcie z każdego bloku 16-bitowego początkowych zer. Należy pamiętać, że każdy taki blok musi zawierać przynajmniej jedną cyfrę. Idąc dalej w przekształcaniu adresów IPv6 zawierających wiele zer, można np. skompresować adres multiemisji *FF02:0:0:0:0:0:0:2* do postaci *FF02::2*.

Kompresja zer w adresach IPv6 może być używana tylko do kompresowania pojedynczej ciągłej serii bloków 16-bitowych, które wyrażone są w zapisie dwukropkowo-cyfrowym. Kompresja zer nie może obejmować części bloku 16-bitowego. Dlatego nie można na przykład wyrazić adresu *FF02:10:0:0:0:0:0:3* jako *FF02:1::3*.

Aby łatwo określić, ile bitów *0* jest reprezentowanych przez podwójny dwukropek (*::*), można policzyć liczbę bloków w skompresowanym adresie, a następnie otrzymaną liczbę odjąć od 8 i pomnożyć otrzymany wynik przez 16. I tak w adresie *FF02::2* są dwa bloki (*FF02* oraz *2*). Liczba bitów reprezentowanych przez podwójny dwukropek (*::*) jest tu równa (8 − 2)*16 = 96.

Kompresja zer może być używana tylko raz w danym adresie IPv6. W przeciwnym razie nie byłoby możliwe określenie liczby bitów *0* reprezentowanych przez każde wystąpienie podwójnego dwukropka (*::*).

Do wyrażania identyfikatorów podsieci, tras lub zakresów adresowych protokół internetowy IPv6 wykorzystuje notację z *prefiksem formatu* (ang. *Format Prefix*), w protokole

IPv4 znaną jako CIDR (ang. *Classless Inter-Domain Routing*)[2], która jest usprawnieniem tego protokołu, pozwalającym na dużo efektywniejsze wykorzystywanie puli adresów IPv4 oraz zmniejszenie tablic routingu.

Podobnie jak w przypadku przestrzeni adresowej IPv4, przestrzeń adresowa protokołu IPv6 jest podzielona na podstawie wartości najbardziej znaczących bitów w adresie, które nazywa się wspomnianym już prefiksem formatu. W tabeli 3.3 przedstawiono podział 128-bitowej przestrzeni adresowej IPv6 według prefiksu formatu.

Tabela 3.3. *Podział przestrzeni adresowej IPv6 według prefiksu formatu*

Przeznaczenie przestrzeni adresowej protokołu IPv6	Prefiks formatu (bin)	Prefiks formatu (hex)	Część przestrzeni adresowej
Przestrzeń zarezerwowana	0000 0000	00	1/256
Przestrzeń niezdefiniowana	0000 0001	01	1/256
Przestrzeń zarezerwowana dla NSAP (ang. *Network Service Access Point*)	0000 001	02	1/128
Przestrzeń niezdefiniowana	0000 010	04	1/128
	0000 011	06	
Przestrzeń niezdefiniowana	0000 1	08	1/32
	0001	10	
Kumulowane globalne adresy emisji pojedynczej (odpowiednik publicznych adresów protokołu IPv4)	001	20	1/8
Przestrzeń niezdefiniowana	010	40	1/8
	100	60	1/8
	100	80	1/8
	101	A0	1/8
	110	C0	1/8
	1110	E0	1/16
	1111 0	F0	1/32
	1111 10	F8	1/64
	1111 110	FC	1/128
	1111 1110 0	FE	1/512
Adresy emisji pojedynczej lokalne dla łącza (odpowiednik adresów APIPA protokołu IPv4)	1111 1110 10	FE80	1/1024
Adresy emisji pojedynczej lokalne dla witryny (odpowiednik adresów prywatnych protokołu IPv4)	1111 1110 11	FEC0	1/1024
Adresy multiemisji (identyfikują wiele adresów)	1111 1111	FF	1/256

[2] Więcej informacji na temat adresacji CIDR można znaleźć w dokumencie *RFC 1519* na stronie internetowej pod adresem *http://www.ietf.org/rfc/rfc1519.txt.*

Mając na uwadze informacje przedstawione w powyższej tabeli, należy pamiętać, że:

1. *Adresy specjalne IPv6* to:
   - *Adres nieokreślony*. Jest używany jedynie do wskazania braku adresu i ma zawsze postać *0:0:0:0:0:0:0:0* lub *::* (znak podwójnego dwukropka), i jest równoważny adresowi nieokreślonemu *0.0.0.0* protokołu IPv4. Adres ten jest używany jako adres źródłowy dla pakietów, które próbują zweryfikować unikatowość niepewnego adresu. Adres ten nigdy nie jest przypisywany fizycznej karcie sieciowej ani używany jako adres docelowy.
   - *Adres sprzężenia zwrotnego*. Jest używany jedynie do identyfikowania fizycznej karty sieciowej, która jest zainstalowana w lokalnym hoście sieciowym, co umożliwia temu hostowi wysyłanie pakietów danych do samego siebie. Adres ten ma postać *0:0:0:0:0:0:0:1* lub *::1* i jest równoważny adresowi sprzężenia zwrotnego o adresie *127.0.0.1* (lub *localhost*) protokołu IPv4. Taki adres zapewnia, że pakiety, które są adresowane na adres sprzężenia zwrotnego, nigdy nie są wysyłane do sieci.
2. *Adresy zgodności* ułatwiają migrację z protokołu IPv4 do protokołu IPv6 i umożliwiają współistnienie obu typów hostów sieciowych, dla których zdefiniowano poniższe adresy:
   - *Adres zgodny z protokołem IPv4*. Są to adresy o postaci *0:0:0:0:0:0:w.x.y.z* lub *::w.x.y.z*, gdzie *w.x.y.z* reprezentuje publiczny adres IPv4. Adresy tego typu są używane przez hosty sieciowe, które mają zaimplementowane dwa stosy, tj. IP w wersji 4. i 6., i komunikują się z siecią IPv6 przez infrastrukturę IPv4. Takimi hostami są hosty działające pod kontrolą systemu Windows Vista. W tych systemach, jeśli jako docelowy adres IPv6 używany jest adres IPv4, cały ruch IPv6 jest automatycznie hermetyzowany z nagłówkiem IPv4, a następnie wysyłany do miejsca przeznaczenia przy użyciu infrastruktury IPv4.
   - *Adres mapowany na IPv4*. Są to adresy typu *0:0:0:0:0:FFFF:w.x.y.z* lub *::FFFF:w.x.y.z*. Są używane do reprezentowania hosta sieciowego, na którym jest uruchomiony tylko protokół IPv4, przed hostem z protokołem IPv6. Adres mapowany na IPv4 charakteryzuje się tym, że nigdy nie jest używany jako adres źródłowy lub docelowy dla pakietu IPv6, gdyż protokół internetowy IPv6 nie obsługuje korzystania z adresów mapowanych na IPv4.
   - *Adres 6to4*. Jest używany w przypadku komunikacji przez Internet na przykład między dwoma hostami sieciowymi, na których są uruchomione protokoły IPv4 i IPv6. Adres 6to4 jest tworzony przez połączenie prefiksu *2002::/16* z 32 bitami publicznego adresu IPv4 hosta, co daje w sumie prefiks 48-bitowy o postaci *2002:wwxx:yyzz::/48*.
3. *Kumulowane globalne adresy emisji pojedynczej* są routowane i osiągalne w sieci rozległej Internet IPv6, opartej na protokole IPv6, który obsługuje hierarchiczne adresowanie oraz wydajny routing.
4. Istnieją dwa typy adresów emisji pojedynczej używanych lokalnie:

- *Adresy lokalne dla łącza*. Używane są między dwoma sąsiadami podłączonymi do jednego łącza a także w procesach nowego protokołu ND (ang. *Neighbor Discovery*), będącego serią komunikatów protokołu ICMPv6, które zarządzają interakcją pomiędzy hostami sieciowymi działającymi w tej samej sieci. *Adresy lokalne dla łącza*, tj. pierwsze 64 bity, zawsze zaczynają się od prefiksu *FE80::/64*, a router nigdy nie przesyła ruchu lokalnego dla danego łącza poza to łącze.
- *Adresy lokalne dla witryny (sieci lokalnej organizacji)*. Używane są zazwyczaj pomiędzy hostami sieciowymi komunikującymi się z innymi hostami działającymi w tej samej lokalnej sieci organizacji i nie są nigdy osiągalne z innych sieci lokalnych. Routery zaś nie mogą przesyłać ruchu lokalnego poza lokalną sieć organizacji. *Adresy lokalne dla witryny*, tj. pierwszych 48 bitów, zawsze zaczynają się od prefiksu *FEC0::/48*. Po tych 48 bitach jest 16-bitowy identyfikator podsieci, który znajduje się w polu ID podsieci, co daje możliwość utworzenia aż 65 536 podsieci w danej organizacji.

5. *Adresy multiemisji* zaczynają się zawsze od adresu *FF* (*11111111*) oraz nie mogą być używane jako adresy źródłowe. Jak przykład takiego adresu można podać *FF01::1*. Jest to adres wszystkich węzłów z zakresu lokalnego dla węzła, czyli sieci lokalnej organizacji.
6. W protokole IPv6 nie występuje pojęcie *maski podsieci*, która jest wymagana w protokole IPv4. Na przykład adres o postaci *3FFE:FFFF:2C:23CD::/64* oznacza identyfikator podsieci, *3FFE:FFFF:2D::/48* — trasę, *FF::/8* — zakres adresów multiemisji.

Usługa *6to4* to technika tunelowania opisana w dokumencie *RFC 3056* w lutym 2001 roku, który dostępny jest pod adresem internetowym *http://www.ietf.org/rfc/rfc3056.txt*. Podczas wykorzystywania usługi 6to4 cały ruch IPv6 jest hermetyzowany z nagłówkiem IPv4 przed wysłaniem przez Internet (IPv4). Obsługę urządzeń sieciowych 6to4 zapewnia usługa *Pomocnik IPv6* (ang. *IPv6 Helper*), która jest dołączona do protokołu IPv6 dla systemów operacyjnych z rodziny Windows Server 2003. Mechanizm ten służy przede wszystkim do przesyłania datagramów IPv6 w starszych sieciach. Utworzony tunel widziany jest przez protokół IPv6 jako jeden skok (ang. *hop*), podczas gdy rzeczywista droga między dwoma punktami może składać się z wielu routerów pośrednich.

Typy adresów IPv6

Protokół internetowy IPv6 definiuje generalnie trzy typy adresów, które częściowo zostały opisane powyżej. Są to adresy:

1. *Pojedynczej emisji* — wykorzystywany jest do dostarczania datagramów IP w relacji typu *jeden do jednego*.
2. *Multiemisji* — wykorzystywany jest do dostarczania datagramów IP w relacji typu *jeden do wielu*.
3. *Ogólnej emisji* — wykorzystywany jest do dostarczania datagramów IP w relacji typu *jeden do jednego z wielu.*

Dwa pierwsze adresy funkcjonują taka samo jak w protokole internetowym IPv4, a trzeci jest połączeniem dwóch pierwszych, czyli pojedynczej emisji i multiemisji. Datagramy IP adresowane do grupy ogólnej emisji odbierane są przez zbiór interfejsów sieciowych (fizycznych kart sieciowych), które są znane jako grupa ogólna emisji. Mianowicie datagramy IP są zazwyczaj dostarczane do najbliżej zlokalizowanego nadawcy — członka tej grupy za pomocą mechanizmu routingu, a dokładniej tras, z którymi związane są metryki pozwalające zlokalizować najbliższych członków grupy ogólnej emisji.

Host sieciowy IPv4 wyposażony w jedną kartę sieciową ma jeden adres IPv4 przypisany tej karcie ręcznie lub automatycznie za pomocą serwera DHCP, natomiast host sieciowy IPv6 (z jedną kartą sieciową) ma zazwyczaj kilka adresów IPv6. Hosty takie mają przynajmniej dwa adresy logiczne, przy użyciu których mogą odbierać datagramy IP, i mają przypisane:

1. *Adresy pojedynczej emisji*:
   - *adresy lokacji lokalnej* — stanowią odpowiednik prywatnych adresów internetowych IPv4 oraz mogą być wykorzystywane wewnątrz danej organizacji bez jakichkolwiek konfliktów z adresami globalnymi;
   - *adresy łącza lokalnego* — stanowią odpowiednik adresów internetowych IPv4 zwanych w skrócie APIPA, które służą do automatycznego adresowania hostów sieciowych w danym segmencie bez routera;
   - *adres sprzężenia zwrotnego* — jest to adres o postaci *0:0:0:0:0:0:0:1* lub *::1*.
2. *Adresy multiemisji*, na których nasłuchują ruchu:
   - *adres wszystkich węzłów z zakresu lokalnego dla węzła* — jest to adres *FF01::1*;
   - *adres wszystkich węzłów z zakresu lokalnego dla łącza* — jest to adres *FF02::1*;
   - *adres węzła żądanego dla każdego adresu emisji pojedynczej na każdej karcie sieciowej*;
   - *adresy multiemisji grup dołączonych na każdej karcie sieciowej*.

Podstawowe protokoły IPv6

Do podstawowych protokołów, które wchodzą w skład zestawu protokołów IPv6, należą:

1. *Internet Protocol w wersji 6. (IPv6)*. Nagłówek IPv6 ma nową, zoptymalizowaną strukturę, z której usunięto zbędne i rzadko wykorzystywane (w stosunku do nagłówka IPv4) pola. Dzięki temu jest on dużo efektywniej przetwarzany przez urządzenia aktywne, jak routery. Stąd też nagłówek IPv6 nie jest zgodny z nagłówkiem IPv4, a hosty sieciowe obsługujące wyłącznie protokół IPv4 odrzucają bez powiadamiania datagramy IPv6 i na odwrót.

Nagłówek IPv6 został szczegółowo opisany w dokumencie *RFC 2460*, który znajduje się pod adresami internetowymi *http://www.ietf.org/rfc/rfc2460.txt* i *ftp://ftp.helion.pl/przyklady/siekwi.zip* (w katalogu *RFC*).