

6. Protokoły IPv4 i IPv6

Sieć Internet rozpoczęła swoją międzynarodową ekspansję m.in. dzięki określeniu standardów komunikacji między różnymi urządzeniami zlokalizowanymi w różnych sieciach. Standardy te przetrwały wprowadzenie sieci bezprzewodowych, światłowodowych i komórkowych. Nie przetrwały jednego – zwiększającego się zapotrzebowania na adresy, które można przydzielać poszczególnym urządzeniom. Pula ponad 4,29 mld adresów IP okazała się zdecydowanie za mała.

Cele lekcji

- Zrozumiesz potrzebę podziału adresów IP.
- Poznasz różnice między protokołami IPv4 i IPv6.
- Nauczysz się zapisywać adresy IP w protokole IPv6.
- Dowiesz się, na czym polega problem procesu migracji z protokołu IPv4 do IPv6.

6.1. Adresy IP i podział na podsieci

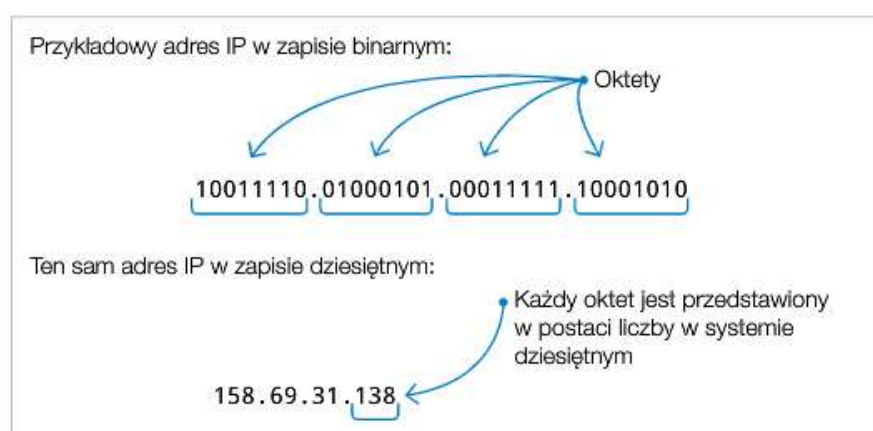
Wiemy już, że zarówno **adresy IP**, jak i **maski podsieci** mają postać czterech liczb od 0 do 255 oddzielonych kropkami. Można je również przedstawić w postaci binarnej, będącej ciągiem zer i jedynek. Choć taki sposób zapisu może się wydawać niewygodny, pozwala łatwiej zrozumieć praktyczne wykorzystanie adresów IP i masek podsieci.

Adres IP,
s. 60 [↗](#)

Maska podsieci,
s. 61 [↗](#)

Adres IP w postaci binarnej

Adres IP w postaci binarnej składa się z 32 bitów podzielonych na **Adres IP (binarny)** cztery **oktety**, czyli 8-bitowe części. Każdy bit jest reprezentowany **Oktet** przez 0 albo 1. W każdym oktecie można zapisać liczby od 00000000 do 11111111, czyli od 0 do 255.



Dobra rada

Adresy dziesiętne możesz przeliczyć na adresy binarne z wykorzystaniem kalkulatora. Wystarczy dla każdego oktetu wykonywać kolejne dzielenia przez 2 i zapisywać kolejne reszty. Zobacz dodatek 6 na s. 446.

Rys. 6.1. Zapis adresu IP w postaci binarnej i dziesiętnej

Ćwiczenie 1

Korzystając z dostępnych narzędzi, np. kalkulatora, zapisz adres:

- a. 11000001.00000000.01100000.11011010 w postaci dziesiętnej,
- b. 188.184.64.53 w postaci binarnej.

Warto wiedzieć

Regionalne rejestry IP (ang. *RIR – Regional Internet Registry*) to instytucje, które są odpowiedzialne za przydzielanie adresów IP w ustalonych regionach świata. Każda z nich może przydzielać adresy IP firmom telekomunikacyjnym, dostawcom usług internetowych oraz instytucjom i przedsiębiorstwom.

Adres prywatny

Klasy i typy adresów IP

Różne sieci komputerowe muszą mieć różne adresy IP, a każde urządzenie podłączone do danej sieci musi mieć przypisany inny adres. Przydziałem adresów dla urządzeń w podsieciach trzeba zarządzać bardzo precyzyjnie. Pierwotna koncepcja podziału całej sieci na mniejsze podsieci zakładała wykorzystanie trzech głównych klas adresów IP: A, B i C, które różnią się liczbą sieci oraz hostów możliwych do zaadresowania. Istnieją również specjalne klasy adresów: D – do rozsyłania grupowego – oraz E – do celów eksperymentalnych.

Część adresów z klas A, B i C jest przeznaczona dla sieci lokalnych, co oznacza, że adresy te mogą być wielokrotnie wykorzystywane w wielu sieciach. Są to tak zwane **adresy prywatne**, czyli adresy IP przydzielone urządzeniom podłączonym do sieci LAN. W tabeli 6.1 przedstawiono zakresy adresów IP dla klas A–D oraz zakresy adresów prywatnych dla klas A–C.

Klasa adresu IP	Zakres adresów IP	Zakres prywatnych adresów IP
A	1.0.0.0–127.255.255.255	10.0.0.0–10.255.255.255
B	128.0.0.0–191.255.255.255	172.16.0.0–172.31.255.255
C	192.0.0.0–223.255.255.255	192.168.0.0–192.168.255.255
D	224.0.0.0–239.255.255.255	-
E	240.0.0.0–254.255.255.255	-

Tabela 6.1. Zakresy wszystkich adresów IP oraz prywatnych adresów IP w poszczególnych klasach

A to ciekawe

Who is...?

Protokół o nazwie WHOIS świadczy usługi informacyjne dotyczące zarejestrowanych domen internetowych. Po wysłaniu zapytania do bazy obsługiwanej przez ten protokół użytkownik otrzymuje dane właściciela domeny. Pierwotnie protokół ten służył do szybkiego odnajdywania administratora wybranej strony internetowej w celu nawiązania kontaktu. Dzisiaj może być wykorzystywany do weryfikacji lub uwierzytelniania informacji dostępnych na stronie internetowej.

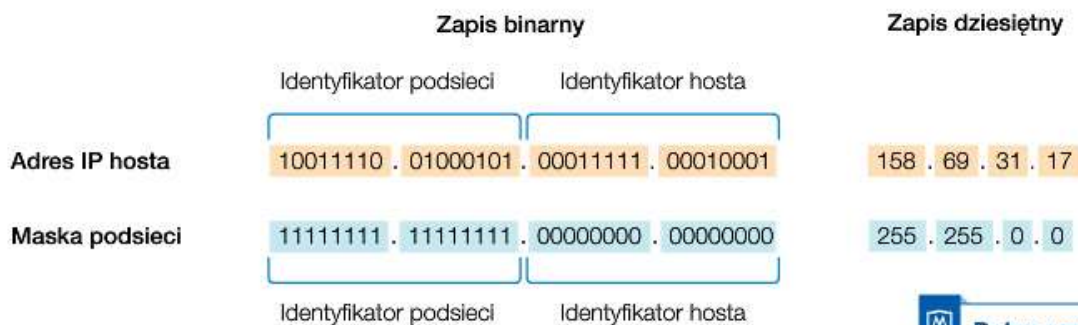


Maska podsieci w postaci binarnej

Zauważ, że np. adresami IP klasy A można opisać tylko 127 sieci, ale do każdej z nich można podłączyć ponad 16 milionów hostów. Podział adresów IP na klasy w praktyce okazał się nieefektywny, ponieważ trudno było obsłużyć stale zwiększającą się liczbę organizacji posiadających małe podsieci. Ten problem częściowo rozwiązują maski podsieci.

Maska podsieci w postaci binarnej, podobnie jak adres IP, składa się z 32 bitów podzielonych na 4 oktety (rys. 6.2). Część maski złożona z:

- ▶ samych jedynek odpowiada za wyodrębnienie identyfikatora sieci, czyli adresu sieci z adresu IP urządzenia,
- ▶ samych zer odpowiada za wyodrębnienie identyfikatora hosta z adresu IP urządzenia.



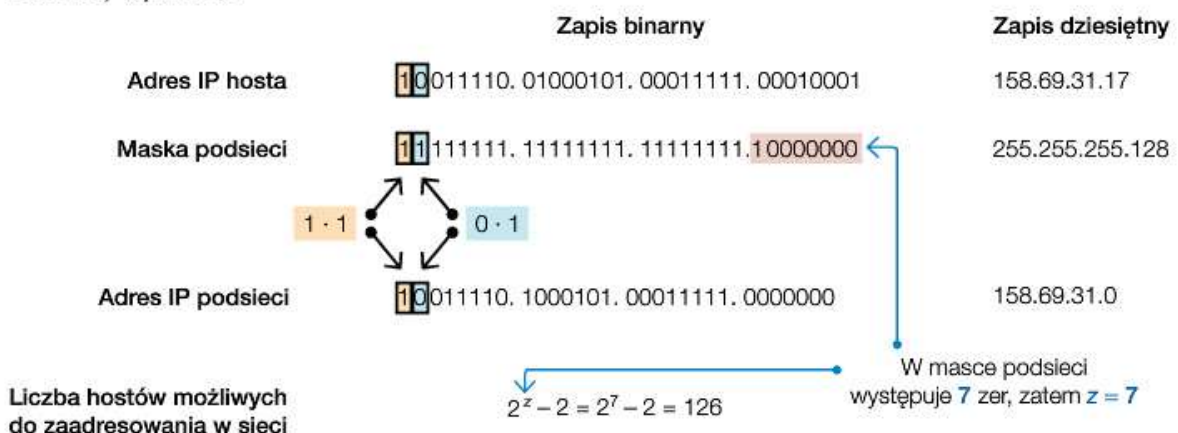
Rys. 6.2. Przykładowy adres IP hosta i przykładowa maska podsieci

Dobra rada

W zapisie binarnym adresów IP i masek podsieci oktety zapisujemy przy użyciu 8 cyfr również wtedy, gdy cyfra znacząca nie jest na najwyższej pozycji w oktecie, np. zamiast 111 zapisujemy 00000111.

Wyznaczanie adresu podsieci i liczby hostów możliwych do zaadresowania

Aby wyznaczyć adres podsieci, mając dostępny adres IP urządzenia w sieci oraz maskę podsieci, należy wykonać mnożenie liczb na wszystkich bitach adresu IP oraz maski (rys. 6.3). Aby obliczyć liczbę hostów możliwych do zaadresowania w sieci, wystarczy skorzystać ze wzoru $2^z - 2$, gdzie z oznacza liczbę zer w masce podsieci zapisanej w postaci binarnej (rys. 6.3).



Rys. 6.3. Wyodrębnianie adresu sieci i liczby hostów

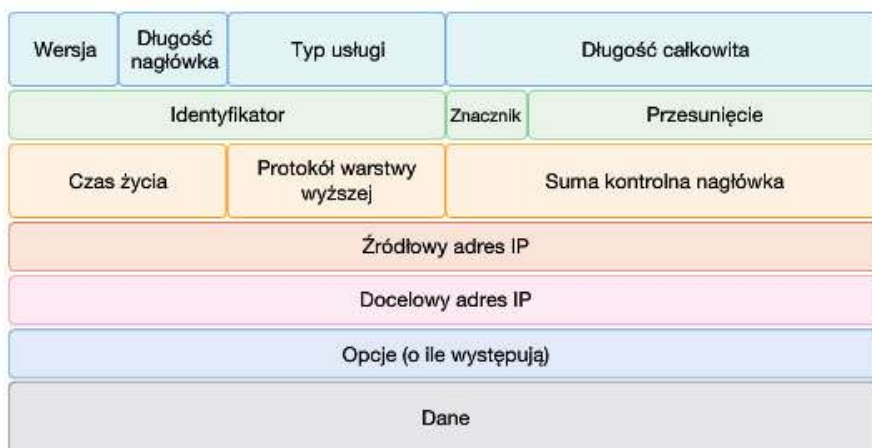
6.2. Protokół IPv4

Warstwa Internetu,
s. 79 [↗](#)

32-bitowe adresy IP są tworzone zgodnie z założeniami protokołu IP w wersji czwartej – w skrócie: IPv4. Funkcjonuje on w **warstwie Internetu**.

Budowa pakietu IPv4

Budowę pojedynczego pakietu przesyłanego zgodnie z tym protokołem przedstawia rysunek 6.4, a tabela 6.2 zawiera opis pól pakietu.



Rys. 6.4. Budowa pakietu IPv4

Pole	Liczba bitów	Opis
Wersja	4	Określa numer wersji protokołu IP.
Długość nagłówka	4	Umożliwia wyznaczenie miejsca, od którego zaczynają się dane pakietu IP.
Typ usługi	8	Pozwala rozróżnić typ usługi, dla której wykorzystywany jest dany pakiet IP, np. pozwala odróżnić usługę HTTP od FTP.
Długość całkowita	16	Określa całkowitą długość pakietu (nagłówek i dane).
Identyfikator	16	Pola te są wykorzystywane podczas fragmentacji pakietów.
Znacznik	3	
Przesunięcie	13	
Czas życia	8	Pozwala odrzucić pakiet, który zbyt długo jest przekazywany w sieci między routerami (po każdym przekazaniu pakietu do routera wartość z tego pola się zmniejsza).
Protokół warstwy wyższej	8	Informacja o protokole warstwy wyższej.
Suma kontrolna nagłówka	16	Pozwala stwierdzić, czy nagłówek został poprawnie przesyłany.
Źródłowy adres IP	32	Adres IP nadawcy pakietu.
Docelowy adres IP	32	Adres IP odbiorcy pakietu.
Opcje	32	Niewymagane pole opcji, opisujące dodatkowe cechy pakietów IP.
Dane		Dane przesyłane w pakiecie IP.

Tabela 6.2. Opis pól pakietu IPv4

Tryby transmisji danych w protokole IPv4

Wyróżniamy trzy sposoby komunikacji między hostami: transmisję pojedynczą, rozsyłanie grupowe i rozgłaszanie.

Transmisja pojedyncza (ang. *unicast*) dotyczy przesyłania pakietu danych przez pojedyncze hosty w sieci. Przykładem może być wysłanie zapytania do serwera WWW przez pojedynczego hosta. • Transmisja pojedyncza

Rozsyłanie grupowe (ang. *multicast*) pozwala na rozsyłanie danych do różnych hostów znajdujących się w różnych sieciach. Pojedynczy pakiet jest przesyłany do wszystkich hostów należących do danej grupy (np. do wszystkich uczestników telekonferencji). W komunikacji tej wykorzystuje się adresy IP klasy D. • Rozsyłanie grupowe

Rozgłaszanie (ang. *broadcast*) polega na wysłaniu pakietów danych do wszystkich hostów znajdujących się w danej sieci. W tym celu wykorzystuje się tzw. **adres rozgłoszeniowy**, który umożliwia przekazanie danych do wszystkich hostów w sieci, nawet takich, których adresy nie są znane. • Rozgłaszanie
• Adres rozgłoszeniowy

Aby obliczyć adres rozgłoszeniowy w sieci o znanym adresie IP i masce podsieci, należy wykonać poniższe czynności.

Krok 1

Wykonujemy operację NOT na masce podsieci, tzn. zapisujemy maskę podsieci w postaci binarnej, a następnie zamieniamy w niej wszystkie zera na jedyńki, a jedyńki na zera.

Krok 2

Zapisujemy maskę po operacji NOT w postaci dziesiętnej, a następnie dodajemy ją do adresu sieci.

Wyjaśnia to poniższy schemat.

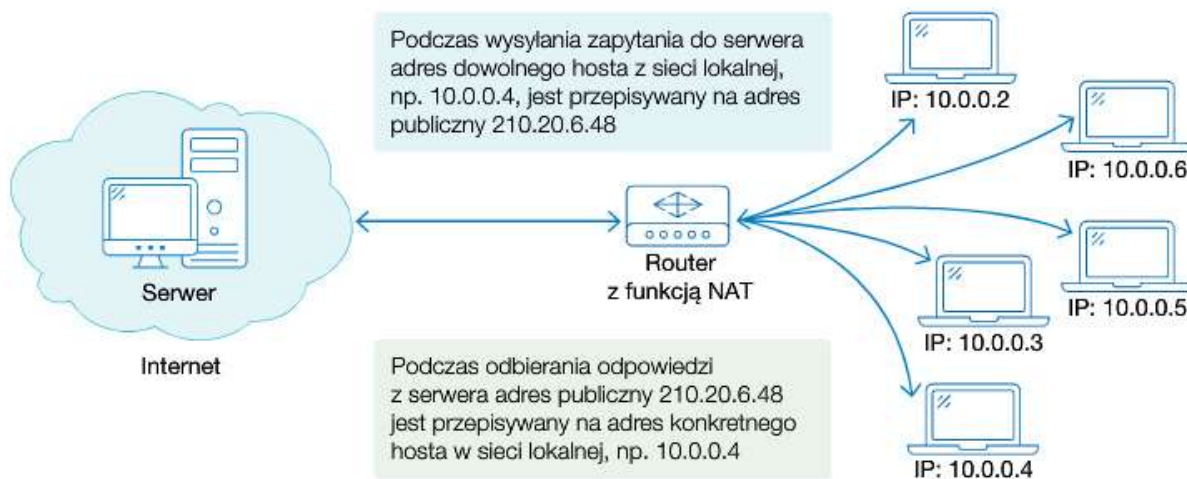
Maska podsieci	11111111 . 11111111 . 11111111 . 10000000
Operacja NOT na masce podsieci w postaci binarnej i dziesiętnej	00000000 . 00000000 . 00000000 . 01111111 0 . 0 . 0 . 127
Postać dziesiętna maski po operacji NOT	0 . 0 . 0 . 127
Adres sieci	+ 158 . 69 . 31 . 17
Adres rozgłoszeniowy	158 . 69 . 31 . 144

Usługa NAT

Usługa NAT (ang. *network address translation*) umożliwia ograniczenie wykorzystania liczby publicznych adresów IP poprzez zastosowanie prywatnych adresów IP w sieciach lokalnych. Te prywatne (wewnętrzne) adresy są przepisywane na jeden adres publiczny (zewnętrzny). Operację tę, nazywaną również **translacją adresów IP**, wykonują najczęściej routery z funkcją NAT. Adresy wykorzystywane w sieci wewnętrznej należą do puli **adresów prywatnych**, zarezerwowanych do użytku w sieciach lokalnych. Schemat działania usługi NAT przedstawia rysunek 6.5 na s. 90. • Usługa NAT
• Translacja adresów IP

Adresy prywatne,
s. 86 [↗](#)

Usługa NAT pozwala obsłużyć bardzo duże sieci wewnętrzne z wieloma urządzeniami z wykorzystaniem dla danej sieci tylko jednego adresu publicznego przydzielonego przez dostawcę internetu (rys. 6.5).



Rys. 6.5. Schemat działania usługi NAT

Warto wiedzieć

Niekiedy usługę NAT realizuje zaporą ogniową (firewall).

Warto wiedzieć

W lutym 2011 r. organizacja IANA (ang. *Internet Assigned Numbers Authority*) przyznała ostatnią pulę adresów IPv4 regionalnym jednostkom rejestracyjnym.

Budowa pakietu w protokole IPv6

Usługa ta pozwoliła częściowo rozwiązać problem braku adresów tworzonych zgodnie z protokołem IPv4. Oprócz tego zaletą technologii NAT jest wyższy poziom bezpieczeństwa sieci prywatnej, ponieważ routery ukrywają urządzenia pracujące w tej sieci.

6.3. Protokół IPv6

Problem braku adresów IP przewidziano już w latach 90. i wówczas rozpoczęły się prace nad nowszym standardem. Wynikiem tych prac jest protokół IPv6, który pozwala określać adresy o długości nie 32 bitów, ale 128 bitów.

Budowę pojedynczego pakietu przesyłanego zgodnie z protokołem IPv6 przedstawia rysunek 6.6. Zwróć uwagę na to, że budowa pakietu została znacznie uproszczona w stosunku do poprzedniej wersji. Pozwala to na jego szybsze przetwarzanie.

Warto wiedzieć

Protokół IPv6 zakłada obsługę tzw. nagłówków rozszerzeń, które przekazują dodatkowe informacje o przesyłanych danych.



Rys. 6.6. Budowa pakietu IPv6

Opisy pól pakietu przesyłanego zgodnie z protokołem IPv6 przedstawiono w tabeli 6.3.

Pole	Liczba bitów	Opis
Wersja	4	Określa numer wersji protokołu IP.
Kategoria danych sieciowych	8	Wskazuje, w jaki sposób ma zostać przetworzony pakiet danych sieciowych, np. pozwala zapewnić wyższy priorytet VoIP.
Etykieta przepływu	20	Pozwala zidentyfikować pakiet danych.
Rozmiar danych	16	Określa całkowitą długość pakietu (nagłówek i dane).
Następny nagłówek	8	Identyfikuje protokół, np. TCP lub UDP, do którego zostanie przekazana zawartość pakietu.
Limit przeskoków	8	Pozwala odrzucić pakiet, który zbyt długo jest przekazywany między routerami (po każdym przekazaniu do routera wartość z tego pola się zmniejsza).
Źródłowy adres IP	128	Adres IP nadawcy pakietu.
Docelowy adres IP	128	Adres IP odbiorcy pakietu.
Dane		Dane przesyłane w pakiecie IP.

Tabela 6.3. Opis pól pakietu IPv6

Adresy IPv6

Adres IPv6 w postaci binarnej składa się ze 128 zer i jedynek. Podobnie jak w przypadku adresów zgodnych z IPv4 zaplanowano jego krótszy, łatwiejszy do rozczytania zapis. Nie jest to jednak zapis dziesiętny, a szesnastkowy (heksadecymalny).

Adres IPv6 zapisujemy w postaci szesnastkowej w ośmiu 16-bitowych blokach, np. 183C:1024:9423:1:752F:7AD8:FFFF:5B5. Adres ten w postaci binarnej wygląda następująco:

```
00011000001111100 0001000000100100 1001010000100011
00000000000000001 0111010100101111 0111101011011000
1111111111111111 0000010110110101
```

A to ciekawe

Poprzednia taka rewolucja w Internecie

Wdrożenie protokołu IPv6 jest ogromnym wyzwaniem dla instytucji odpowiedzialnych za funkcjonowanie Internetu. Ostatnia tak poważna zmiana miała miejsce w latach 80., kiedy powstał plan zastąpienia protokołu NCP protokołem TCP (RFC 801). Choć zasoby Internetu były wówczas jeszcze bardzo skromne, to instytucje odpowiedzialne za tę zmianę nie potrafiły przewidzieć terminu zakończenia tego procesu.



Przekształcanie adresu IPv6 z postaci binarnej na postać szesnastkową

Warto wiedzieć

Google od kilku lat monitoruje wdrożenie protokołu IPv6 w poszczególnych krajach przez zliczanie użytkowników Google korzystających z tego protokołu. W kwietniu 2019 r. w Polsce około 10% użytkowników korzystało z protokołu IPv6. Dla porównania w Niemczech było to 40%, we Francji – 25%, w Hiszpanii – 2%, a na Ukrainie – 1%.

System szesnastkowy, s. 444 [↗](#)

Wiemy już, że adres IPv6 składa się ze 128 bitów. Pokażemy, w jaki sposób przekształcić zapis binarny w zapis szesnastkowy.

Punktem wyjścia będzie 128-bitowy adres IPv6:

```
01110000000011000000000001010000000000011110101000010100
10011100101100000000000000000000000000000000000000000000
00000000001100
```

Krok 1

Zapis dzielimy na osiem 16-bitowych części oddzielonych dwukropkami:

```
0111000000001100 : 0000000001010000 : 0000000011110101 :
0000101001001110 : 0101100000000000 : 0000000000000000 :
0000000000000000 : 000000000001100
```

Krok 2

Każdy 16-bitowy blok dzielimy na cztery równe ciągi bitów:

```
0111 0000 0000 1100 : 0000 0000 0101 0000 :
0000 0000 1111 0101 : 0000 1010 0100 1110 :
0101 1000 0000 0000 : 0000 0000 0000 0000 :
0000 0000 0000 0000 : 0000 0000 0000 1100
```

Krok 3

Każdy 4-bitowy ciąg zastępujemy cyfrą w kodzie **szesnastkowym (heksadecymalnym)**. Uzyskujemy poprawny zapis adresu IPv6:

```
700C:0050:00F5:0A4E:5800:0000:0000:000C
```

Krok 4

Usuujemy nieznaczące zera, tak aby pozostawić co najmniej jedną cyfrę w każdym bloku. Uzyskujemy drugi poprawny zapis adresu IPv6:

```
700C:50:F5:A4E:5800:0:0:C
```

Krok 5

Sprawdzamy możliwość uproszczenia zapisu. W tym celu szukamy bloku adresów, których wartość jest zerowa, np.: 0000:0000.

Jeśli istnieje taki blok, możemy go zastąpić podwójnym dwukropkiem ::. Ostatecznie uzyskujemy najprostszy poprawny zapis adresu IPv6:

```
700C:50:F5:A4E:5800::C
```

Wykorzystanie znaków :: pozwala maksymalnie skrócić adresy IP zawierające długie ciągi zer. Na przykład zapisy: 2A03:1380:: oraz 2A03:1380:0:0:0:0:0:0 oznaczają dokładnie ten sam adres IPv6.

Ćwiczenie 2

Korzystając z powyższego algorytmu, przekształć adres 1103:B38C:FA04::AAAA na postać binarną. Możesz do tego celu wykorzystać dowolne narzędzie, np. arkusz kalkulacyjny lub kalkulator.

6.4. Współistnienie protokołów IPv4 i IPv6

Nowe systemy obsługujące protokoły IPv6 zachowują tzw. **zgodność wsteczną**, czyli potrafią wysyłać, trasować oraz odbierać pakiety IPv4.

Międzynarodowe instytucje podjęły się stopniowego zastępowania protokołu IPv4 protokołem IPv6. Plan zakłada współistnienie dwóch protokołów przez bliżej nieokreślony czas. Ten stopniowy proces wprowadzania protokołu IPv6 ma także pewne wady:

- ▶ nie sprzyja szybszej wymianie oraz dostosowaniu sprzętu i oprogramowania do obsługi protokołu IPv6,
- ▶ może spowodować pogorszenie jakości dostępu do wielu e-usług, co w pierwszej kolejności dotknęłyby kraje słabiej rozwinięte,
- ▶ może opóźnić wprowadzenie wielu innowacyjnych rozwiązań, np. **Internetu rzeczy**.

Warto wiedzieć

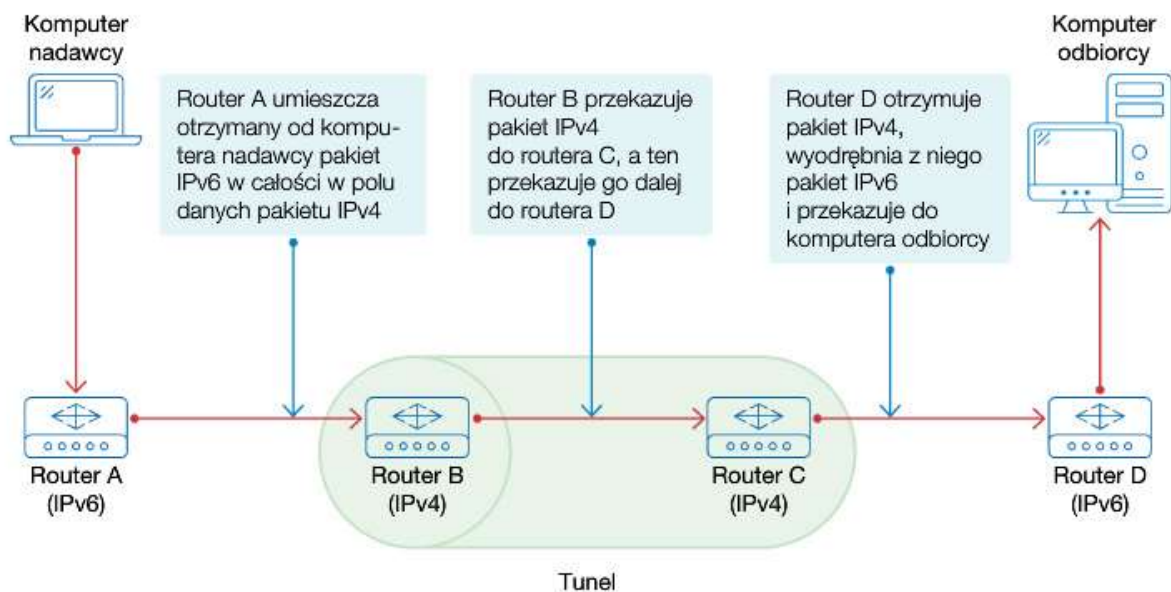
Szacuje się, że protokół IPv4 może jeszcze funkcjonować nawet kilkadziesiąt lat.

Internet rzeczy,
s. 96 [↗](#)

Tunelowanie

Jedną z najpopularniejszych metod, które pozwalają już dziś na funkcjonowanie urządzeń w sieciach obsługiwanych przez protokoły IPv4 i IPv6, jest tunelowanie.

Mechanizm **tunelowania** pozwala łączyć dwie sieci pracujące wyłącznie w jednym protokole kanałem pracującym w innym protokole. Wykorzystuje on możliwość umieszczenia pakietu IPv6 w polu danych pakietu IPv4. Schematycznie przedstawia to rysunek 6.7.



Rys. 6.7. Opis mechanizmu tunelowania

Ćwiczenie 3

Odszukaj w internecie test sprawdzający gotowość sieci, w której pracujesz, do stosowania protokołu IPv6.

Podsumowanie

- Jednym z fundamentów rozwoju Internetu był protokół IPv4.
- Podział puli adresów IPv4 na klasy przewiduje wydzielenie adresów: publicznych, prywatnych, rozsyłania grupowego oraz eksperymentalnych.
- Z powodu ograniczonej puli adresów IP zaczęto identyfikować adresy sieci i adresy hostów za pomocą maski podsieci.
- Istnieją trzy sposoby komunikacji w ramach protokołu IPv4: transmisja pojedyncza, rozsyłanie grupowe i rozgłaszanie.
- Obecnie trwa proces zastępowania 32-bitowych adresów protokołu IPv4 128-bitowymi adresami zgodnymi z protokołem IPv6.
- Usługa NAT pozwala na wykorzystanie puli adresów prywatnych do adresowania hostów w sieci lokalnej. Adresy te są przepisywane na adresy zewnętrzne w celu komunikacji z zewnętrznymi hostami.
- Istnieją metody umożliwiające współdziałanie protokołów IPv4 i IPv6, np. mechanizm tunelowania.

Zadania

- ★ **1** Uzasadnij, dlaczego adres IPv4 156.256.11.200 jest niepoprawny.
- ★ **2** Uzasadnij, dlaczego trudno jest przydzielić unikalny adres IPv4 każdemu komputerowi, a w protokole IPv6 jest to dużo łatwiejsze.
- ★ **3** Przygotuj w edytorze tekstu notatkę, w której opiszysz rozwiązania techniczne pozwalające na rozwój Internetu mimo malejącej liczby adresów IPv4.
- ★★ **4** Dla adresów IP klasy B określ liczbę możliwych do utworzenia podsieci oraz liczbę hostów możliwych do zaadresowania w każdej z nich.
- ★★ **5** Dla podanych niżej adresów IP oraz masek podsieci oblicz liczbę możliwych do zaadresowania hostów:
 - a. adres IP: 168.155.12.5, maska podsieci: 255.255.192.0
 - b. adres IP: 168.155.12.5, maska podsieci: 255.255.255.128
 - c. adres IP: 168.155.12.5, maska podsieci: 255.224.0.0
- ★★ **6** Zapisz w systemie binarnym adres IPv6: A1:7:8E::1:F.
- ★★ **7** Odszukaj listę organizacji, które zajmują się w Polsce wdrażaniem protokołu IPv6.
- ★★★ **8** Przygotuj w edytorze tekstu notatkę dotyczącą adresów jednostkowych w protokole IPv6 oraz wyjaśnij pojęcie „anycast” w odniesieniu do protokołu IPv6.
- ★★★ **9** Przygotuj prezentację na temat mechanizmu translacji adresów IPv4 i IPv6 oraz mechanizmu obsługi podwójnego stosu.