Większość z wymienionych wyżej protokołów wykorzystywana jest przez usługi umożliwiające wykonanie określonych zadań w sieci, np. wysyłanie lub odebranie poczty elektronicznej, pobranie pliku lub strony WWW.

**System DNS**

Korzystając z sieci komputerowej, należy zidentyfikować komputer, z którego zasobów chce się skorzystać. W tym celu można wykorzystać jego adres IP, ale zapamiętanie długiego ciągu liczb jest dla przeciętnego użytkownika trudne. Ludzie łatwiej zapamiętują nazwy niż ciągi liczb. Komputerom w sieci zaczęto więc nadawać unikatowe nazwy wykorzystywane do ich identyfikacji. Nazwy te tworzy drzewiastą strukturę domen.

(rysunek)

Poszczególne domeny są oddzielone od siebie kropkami. Na samym szczycie drzewa znajdują się **Domeny Najwyższego Poziomu** (Top-Level-Domains). Domeny te grupują serwery według ich przeznaczenia, np.:

* .com - instytucje komercyjne,
* .edu – instytucje edukacyjne,
* .gov – instytucje państwowe, agendy rządowe,
* .mil – organizacje wojskowe,
* .net – firmy oferujące usługi sieciowe,
* .org – organizacje niekomercyjne,

Lub położenia geograficznego, np.:

* ,pl – Polska,
* .it – Włochy,
* .de – Niemcy,
* .fr – Francja itd.

Lista domen krajowych i funkcjonalnych jest uzupełniania, tworzona i zarządzana przez organizację **IANA** (*Internet Assignet Numbers Authority*) i korporację **ICANN** (*The Internet Corporation for Assigned Names and Numbers*). Nowe Domeny są tworzone w ramach jednej z istniejących domen, np. onet.pl jest utworzona jako poddomena domeny.pl.

System **DNS** to hierarchiczna usługa nazw przeznaczona dla hostów w sieci TCP/IP. Pozwala nadawać komputerom świadczącym pewne usługi w sieci nazwy domenowe i tłumaczy je na używane przez komputery adresy IP. Gdy w przeglądarce internetowej wpisze się okno w adres domeny internetowej (adres mnemoniczny), przeglądarka komunikuje się z serwerami DNS i uzyskuje informacje o adresie IP komputera, na którego dysku są umieszczone pliki danej strony. System DNS jest rozproszoną bazą danych obsługiwaną przez wiele serwerów, z których każdy posiada tylko informacje o domenie, którą zarządza, oraz o adresie serwera nadrzędnego. Główne serwery nazw (*root level servers*) zlokalizowane są w Stanach Zjednoczonych i podłączone są do szybkich sieci szkieletowych internetu. Przechowują one adresy serwerów nazw dla domen najwyższego poziomu, np. .com, .edu, .org, oraz domen krajowych, np. .pl, .de, .uk. Adresy serwerów głównych muszą być znane każdemu innemu serwerowi nazw. Wewnątrz każdej domeny można tworzyć tzw. Subdomeny, np. wewnątrz domeny .pl utworzono wiele domen regionalnych, jak .waw.pl, lodz.pl. itp., oraz funkcjonalnych, jak .com.pl, .gov.pl lub .org.ol, należących do firm, organizacji lub osób prywatnych.

Do testowania działania serwera DNS można wykorzystać narzędzie **nslookup**. Narzędzie to wysyła zapytanie do serwera oraz zwraca dokładne informacje dotyczące poszukiwanego komputera. Jeżeli jako argumentu dla polecenia użyje się nazwy komputera, to uzyska się adres IP komputera (pod warunkiem, że taka nazwa istnieje w systemie DNS). Jeżeli jako argumentu dla polecenia użyje się adresu IP, to zyska się nazwę komputera, np.:

nslookup www.onet.plż0

lub

nslookup 213.180.141.140.

Aby móc testować działanie system DNS, należy ustawić w opcjach połączenia sieciowego adres serwera DNS.

Zadanie. Wyszukiwanie informacji w systemie DNS

Uruchom wiersz polecenia systemu Windows. Za pomocą narzędzia nslookup sprawdź:

* Adres IP serwera [www.wp.pl](http://www.wp.pl) oraz serwera udostępniającego stronę WWW Twojej szkoły,a
* nazwę komputera o adresie IP: 194.204.159.1.

Ogólne zasady przyznawania nazw domen i adresów IP nadzorują dwie instytucje: IANA i ICANN. Instytucje te przekazują swoje uprawnienia na lokalne instytucje i firmy, np., w Polsce nadzór nad domeną **.pl** jako całością oraz obsługą rejestrowania domen takich, jak .com.pl, .bic.pl, .org.pl, .net.pl oraz innych domen funkcjonalnych, pełni **NASK** (*Naukowa i Akademicka Sieć Komputerowa*). Aby móc pracować w internecie, komputer musi znać adresy IP serwerów DNS, które udzielają odpowiedzi na zapytania. Serwery te mogą być zlokalizowane poza domeną użytkownika, np. serwery openDNS, lub w obrębie domeny, co pozwala na szybsze uzyskiwanie odpowiedzi i samodzielne konfigurowanie wydzielonej poddomeny. Zazwyczaj dla każdej domeny utrzymywane są dwa niezależne serwery nazw, dzięki czemu w razie awarii lub zbyt dużego obciążenia **podstawowego serwera DNS** (*primary name server*) można korzystać z serwera rezerwowego (*secondary name server*). Informacje o hostach w obrębie domeny są replikowane na inne serwery DNS w celu poprawy odporności na uszkodzenia i/lub dla poprawy wydajności.

Zadanie.

1. Sprawdź adres IP podstawowego i zapasowego serwera DNS Używanego w Twojej sieci.
2. W jakiej domenie umieszczona jest strona Twojej szkoły? Wypisz wszystkie domeny i poddomeny.

Narzędzia diagnostyczne protokołów TCP/IP

Poprawne skonfigurowanie protokołu IP pozwala na pracę z wykorzystaniem zasobów sieciowych. Każdy sieciowy system operacyjny oferuje narzędzia pozwalające sprawdzić poprawność konfiguracji.

1. Polecenie ipconfig – pozwala sprawdzić adresy przypisane do poszczególnych interfejsów. Narzędzie to pomaga przy wykrywaniu błędów w konfiguracji protokołu IP.

Sposoby wykorzystania ipconfig:

- ipconfig – wyświetla skróconą informację o połączeniu

- ipconfig /all – wyświetla szczegółowe dane o konfiguracji wszystkich interfejsów

- ipconfig /renew – odnawia wszystkie karty

- ipconfig /relase – zwalnia wszystkie połączenia

- ipconfig /? – wyświetla informacje o poleceniu

- ipconfig /flushdns – czyści bufor programu rozpoznającego nazwy DNS

Odpowiednikiem ipconfig w systemie Linux jest ifconfig.

2. Polecenie ping – program używany w sieciach komputerowych działających na podstawie protokołu TCP/IP, służący do diagnozowania połączeń sieciowych. Pozwala na sprawdzenie, czy istnieje połączenie między hostem testującym i testowanym, oraz na określenie jakości połączenia przez pomiar liczby zgubionych pakietów oraz czasu potrzebnego na ich transmisję. Ping wysyła pakiety żądania echa ICMP (Echo Request) i odbiera odpowiedzi na żądanie echa ICMP (Echo Reply). Polecenie ping jest dostępna w systemie Windows i Linux.

Aby sprawdzić poprawność konfiguracji połączenia IP, należy użyć składni:

Ping nazwa\_lub\_adres\_do\_sprawdzenia

Jako argument dla polecenia ping można podać adres IP lub nazwę domenową komputera testowanego (np. ping 192.168.0.1 lub ping [www.wp.pl](http://www.wp.pl)).

UWAGA!!!

Komputery powinny odpowiadać na żądanie echa, lecz większość współczesnych programów typu firewall blokuje ten proces, w konsekwencji możemy nie otrzymać odpowiedzi, mimo że istnieje połączenie pomiędzy hostami.

3. Polecenie tracert

Program **tracert** (w systemach Linux program nazywa się **traceroute**) jest przeznaczony do śledzenia trasy, po jakiej są przesyłane pakiety w sieci. Program ten wysyła pakiet żądania echa z polem TTL (*Time To Live*) ustawionym na kolejce wartości, od 1 do 30. Wartość TTL jest zmniejszana przy przechodzeniu przez kolejne routery na trasie. Jeżeli pole TTL osiągnie wartość 0, pakiet jest kasowany przez router. Router dodatkowo wysyła za pomocą protokołu ICMP Informację zwrotną o błędzie. Komputer źródłowy uzyskuje, bezpośrednio po wysłaniu żądania o wartości 1, adres IP pierwszego routera na trasie. W następnym pakiecie pole TTL ma wartość 2, co powoduje, że pierwszy router zmniejszy tę wartość 1, drugi router zmniejszy TTL do 0 i skasuje pakiet, wysyłając komunikat o błędzie w ten sposób program tracert może prześledzić trasę w sieci zawierającej nie więcej niż 30 routerów. Brak odpowiedzi na zadany pakiet jest sygnalizowany znakiem gwiazdki \* i może wynikać z konfiguracji firewall lub przeciążenia sieci.

4. Polecenie netstat

Polecenie **netstat** jest jednym z najbardziej rozbudowanych poleceń, pozwalającym na sprawdzanie połączeń sieciowych. Dostępne jest zarówno dla systemu Windows, jak i Linux. Umożliwia wyświetlenie aktywnych połączeń sieciowych TCP, a także portów, na których komputer nasłuchuje, tabeli routingu, statystyk itp.

Polecenie netstat użyte bez parametrów powoduje wyświetlenie aktywnych połączeń protokołu TCP. Inne najważniejsze parametry polecenia to:

* -a – służy do wyświetlenia wszystkich aktywnych połączeń oraz portów nasłuchu protokołów TCP i UDP.
* -b – służy do wyświetlenia aktywnych połączeń protokołu TCP i nazw programów, które są przypisane do obsługi danego portu.
* -e – wyświetla statystykę sieci Ethernet.
* -n – wyświetla aktywne połączenia TCP (adresy i numery portów są wyrażane numerycznie).
* -o – wyświetla aktywne połączenia TCP i identyfikatory procesów (PID) poszczególnych połączeń.
* -p protokół – ukazuje połączenia wybranego protokołu (udp, tcpv6, tcp lub udpv6).
* -s – służy do wyświetlania oddzielnych statystyk dla poszczególnych protokołów.
* -r – służy do wyświetlania zawartości tabeli trasowania protokołu IP.

**Adresowanie w sieci komputerowej**

Do sieci komputerowej mogą być podłączone różne urządzenia, np. serwery, komputery, drukarki. Każde z nich musi mieć możliwość wymiany danych z innymi. Aby to było możliwe, potrzebny jest mechanizm pozwalający na zidentyfikowanie każdego urządzenia podłączonego do sieci. Identyfikacja odbywa się za pomocą unikatowych ciągów znaków, nazywanych adresami. W najpopularniejszych obecnie sieciach lokalnych spotyka się 2 rodzaje adresów:

* **Fizyczne** – adresy MAC (Medium Access Control)
* **Logiczne** – adresy IP (Internet Protocol)

1. Adresy fizyczne

Adres fizyczny jest nadawany przez producenta każdej karcie sieciowej NIC (*Network Interface Card*) podczas jej wytworzenia. Adres ten jest niepowtarzalny i umieszczony w pamięci ROM karty. Długość adresu fizycznego wynosi 48 bitów lecz jest przedstawiony w zapisie heksadecymalnym (szesnastkowym). Pierwsze 24 bity oznaczają producenta karty sieciowej, pozostałe 24 bity są unikatowym identyfikatorem danego egzemplarza karty. Aby sprawdzić adres fizyczny karty, można w wierszu poleceń systemu Windows 2000 i nowszych wersji wpisać polecenie ipconfig /all lub getmac.

2. Adresy logiczne

Adres logiczny wskazuje punktu przyłaczenia do sieci, który jest nazywany identyfikatorem. Komputer pracujący w sieci wyposażony w kilka interfejsów, może mieć kilka adresów logicznych – po jednym dla każdego z tych interfejsów. Interfejsy to zwykłe urządzenia fizyczne, np. karty sieciowe, ale mogą być nimi również urządzenia logiczne, np. w niektórych kartach sieciowych można utworzyć podinterfejsy.

Adres logiczny może określać urządzenie, np. komputer, grupę urządzeń (adres grupowy) lub całą sieć (adres sieci). Może on być *statyczny* – przypisany przez administratora lub uzyskany *dynamicznie* za pośrednictwem serwera DHCP (*Dynamic Host Configuration Protocol*). Niezależnie jednak od sposobu uzyskania adresu logicznego, w danej sieci **nie mogą** istnieć dwa urządzenia o takim samym dresie.

Obecnie funkcjonują dwie wersje adresów IP:

* **IPv4** – starsza wersja, bardzo rozpowszechniona,
* **IPv6** – nowsza wersja, mniej popularna.

3. Adresy IPv4

Adres IP w wersji 4 ma długość 32 bitów. Jest on podzielony na cztery 8-bitowe bloki, zwane **oktetami**. Administratorzy najczęściej przedstawiają adresy w postaci dziesiętnej (notacja dziesiętna z kropkami). Każdy oktet jest liczbą dziesiętną z zakresu 0-255. Taka postać adresu jest łatwiejsza do zapamiętania niż jedna liczba z zakresu 0 – 232-1.

Porównanie różnych sposobów zapisu tej samej liczby:

* Zapis binarny: 1100000010101000000000000000000001
* Zapis dziesiętny: 3 232 235 521
* Zapis tradycyjny: 192.168.0.1

Adres IP w zapisie binarnym i dziesiętnym:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | . | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | . | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | . | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 192 | | | | | | | | . | 168 | | | | | | | | . | 0 | | | | | | | | . | 1 | | | | | | | |

Przykład zamiany adresów z postaci dwójkowej na dziesiętną

Systemy komputerowe przetwarzają adresy w postaci dwójkowe. Dla człowieka zapamiętanie adresu złożonego z 32 bitów jest prawie niemożliwe. Wygodniej jest posługiwać się adresami, w których każdy oktet zamieniony zastał na liczbę dziesiętną z zakresu od 0 do 255. W tym miejscu zostanie przedstawiona prosta metoda zamiany liczby z postaci dwójkowej na dziesiętną. Każdemu bitowi należy przypisać jego wartość wynikającą z pozycji w liczbie dwójkowej (wagę). Następnie sumuje się te wartości, dla których bit adresu przybiera wartość 1.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Wartość w postaci wykładniczej | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 |  |
| Wartość bitu | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |  |
| Postać binarna | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |  |
| Wynik | 128 | + | 32 | + | 8 | + | 2 | = | 170 |

Przykład zamiany adresów z postaci dziesiętnej na dwójkową

Aby zamienić adres podany w postaci dziesiętnej na postać dwójkową, należy spośród wartości dziesiętnych poszczególnych bitów wybrać te, których suma jest równa zamienianej liczbie. Zadanie to jest dość trudne, dlatego zostanie wyjaśnione na przykładzie – liczbę 123 należy zapisać w systemie dwójkowym. Poniżej przedstawiono wartości kolejnych bitów, zaczynając od lewej strony (najbardziej znaczącego bitu):

* wartość pierwszego bitu wynosi 128 i jest większa niż liczba 123 – ten bit ma wartość 0,
* wartość drugiego bitu wynosi 64 i jest mniejsza niż liczba 123 – ten bit ma wartość 1 (reszta 123 – 64 = 59),
* wartość trzeciego bitu wynosi 32 i jest mniejsza niż liczba 59 – ten bit ma wartość 1 (reszta 59 – 32 = 27),
* wartość czwartego bitu wynosi 16 i jest mniejsza niż liczba 27 – ten bit ma wartość 1 (reszta 27 – 16 = 11),
* wartość piątego bitu wynosi 8 i jest mniejsza niż liczba 11 – ten bit ma wartość 1 (reszta 11 – 8 = 3),
* wartość szóstego bitu wynosi 4 i jest większa niż liczba 3 - ten bit ma wartość 0 (reszta wynosi ciągle 3),
* wartość siódmego bitu wynosi 2 i jest mniejsza niż liczba 3 – ten bit ma wartość 1 (reszta 3 – 2 = 1),
* wartość ósmego bitu wynosi 1 i jest równa liczbie 1 – ten bit ma wartość 1 (reszta wynosi 0, co oznacza koniec obliczeń).

Liczba 123D w postaci dwójkowej jest reprezentowana przez 01111011.

4. Klasy adresów IP

Teoretycznie, mając do dyspozycji 32 bity, można wygenerować 4 294 967 296 (=232) adresów IP. Adres IP ma budowę hierarchiczną. Część adresu IP oznacza identyfikator sieci, a część identyfikator hosta (urządzenia). Adresy IP zostały podzielone na klasy A, B, C, D i E.

**Adresy klasy A**

Adresy **klasy A**  przeznaczono do obsługi bardzo dużych sieci. Adres sieci zajmuje pierwszy oktet, natomiast adres hosta pozostałe trzy. Pierwszy (najstarszy) bit oktetu adresu IP klasy A jest zawsze równy **0**. Ostatnie 24 bity (3 oktety) adresu klasy A są dresem hosta.

Podział bitów w adresie klasy A

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **sieć** | | | | | | | | **.** | **host** | | | | | | | | **.** | **host** | | | | | | | | **.** | **Host** | | | | | | | |
| **0** |  |  |  |  |  |  |  | **.** |  |  |  |  |  |  |  |  | **.** |  |  |  |  |  |  |  |  | **.** |  |  |  |  |  |  |  |  |

Nie używa się adresu 0. Adresy klasy A obejmują zakres od 1.0.0.0 do 127.255.255.255. Wartość pierwszego oktetu adresu klasy A mieści się w zakresie od 1 do 127. Maksymalna liczba sieci klasy A to 127. Adres 127.0.0.0 również powinien być adresem sieci klasy A, jest jednak zarezerwowany jako adres pętli zwrotnej do testowania hosta i nie można go przypisać żadnej sieci.

Każda sieć klasy A może obsługiwać 16 777 214 stacji. Na 24 bitach można zapisać 16 777 216 (=224) różnych wartości, jednak 2 spośród tych adresów (adresy specjalne: sieci i rozgłoszeniowy) przeznaczony zostały do innych celów i nie mogą być przypisane hostom.

**Adresy klasy B**

Adresy **klasy B** przeznaczono do obsługi sieci dużych i średnich. Pierwsze dwa oktety adresu IP klasy B oznaczają numer sieci, a pozostałe dwa – numer hosta.

Podział bitów w adresie klasy B

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **sieć** | | | | | | | | **.** | **sieć** | | | | | | | | **.** | **host** | | | | | | | | **.** | **Host** | | | | | | | |
| **1** | **0** |  |  |  |  |  |  | **.** |  |  |  |  |  |  |  |  | **.** |  |  |  |  |  |  |  |  | **.** |  |  |  |  |  |  |  |  |

Najstarsze dwa bity pierwszego oktetu adresu klasy B wynoszą **10** (dwójkowo), natomiast pozostałe są dowolne. Adresy klasy B obejmują zakres od 128.0.0.0 do 191.255.255.255. Wartość pierwszego oktetu adresu klasy B mieści się w zakresie od 128 do 191. Ostatnie 16 bitów (2 oktety) określa dopuszczalne adresy hostów. Każda sieć klasy B może obsługiwać 65 534 hosty (wyłączone są adresy specjalne). Maksymalnie może istnieć 16 384 sieci klasy B (214 = 16 384).

**Adresy klasy C**

Adresy **klasy C** przeznaczono do obsługi dużej liczby małych sieci. W adresie klasy C pierwsze trzy oktety określają sieć, a ostatni – hosta.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **sieć** | | | | | | | | **.** | **sieć** | | | | | | | | **.** | **Sieć** | | | | | | | | **.** | **Host** | | | | | | | |
| **1** | **1** | **0** |  |  |  |  |  | **.** |  |  |  |  |  |  |  |  | **.** |  |  |  |  |  |  |  |  | **.** |  |  |  |  |  |  |  |  |

Najstarsze trzy bity pierwszego oktetu adresu klasy C wynoszą **110** (dwójkowo). Adresy klasy C obejmują zakres od 192.0.0.0 do 223.255.255.255. Każda sieć klasy C może obsługiwać 254 stacje (wyłączone są adresy specjalne). Maksymalnie może istnieć 2 097 152 sieci klasy C (221 = 2 097 152).

**Adresy klasy D**

Adresy **klasy D** do transmisji grupowej (multicast – multiemisja) w sieciach IP. Adres grupowej jest niepowtarzalnym adresem sieciowym, kierującym pakiety do zdefiniowanych z góry grup adresów IP. Jedna stacja może przesyłać strumień kierowany do wielu odbiorców jednocześnie. Przestrzeń adresowa klasy D obejmuje zakres od 224.0.0.0 do 239.255.255.255.

**Adresy klasy E**

Adresy **klasy E** zespół IETF (*Internet Engineering Task Force* – organizacja odpowiedzialna za ustanowienie standardów w Internecie) zarezerwował do własnych badań. Nie można korzystać z nich w Internecie (zakres prawidłowy adresów klasy E to 240.0.0.0 – 255.255.255.255).

**Adres sieci i adres rozgłoszeniowy**

W każdej z klas adresów dwa spośród nich były zarezerwowane do celów specjalnych. Adres, w którym w części przeznaczonej dl hosta znajdują się same zera (dwójkowo), jest **adresem sieci**. Adres, w którym w części przeznaczonej dla hosta znajdują się same jedynki, jest **adresem rozgłoszeniowym** (*broadcast*). Adresów tych nie można przypisać hostom.

Adresy sieci są wykorzystywane w procesie przełączania pakietów IP – routery przechowują w tablicach routingu adresy sieci oraz adresy, przez które są one dostępne.

Przykład wyznaczania adresu sieci oraz adresu rozgłoszeniowego

Adres IP: 77.213.126.82

Postać binarna: 01001101 11010101 01111110 01010010

Jest to adres z klasy A, więc część sieci jest określana przez pierwsze 8 bitów, a adres sieci uzyskuje się przez ustawienie na ostatnich 24 bitach liczby 0.

Postać binarna adresu sieci: 01001101 00000000 00000000 00000000

Postać dziesiętna adresu sieci: 77.0.0.0

Postać binarna adresu rozgłoszeniowego: 01001101 11111111 11111111 11111111

Postać dziesiętna adresu rozgłoszeniowego: 77.255.255.255

Liczba adresów IP w sieci jest wyliczana według wzoru:

LIP = 2n,

gdzie LIP - liczba adresów IP w sieci (liczba adresów do wykorzystana wymaga odjęcia pierwszego adresu (sieci) i ostatniego adresu (rozgłoszeniowego)), n – liczba bitów w części hosta.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Klasa adresu** | **Liczba bitów w części sieci** | **Liczba bitów w części hosta** | **Liczba dostępnych sieci** | **Liczba adresów w części hosta** | **Liczba dostępnych adresów w części hosta** |
| Klasa A | 8 | 24 (=32-8) | 126 | 16 777 216 | 16 777 214 |
| Klasa B | 16 | 16 (=32-16) | 16384 | 65 536 | 65 534 |
| Klasa C | 24 | 8 (=32-24) | 2 097 152 | 256 | 254 |

Ponadto istnieją jeszcze inne specjalne adresy:

|  |  |  |
| --- | --- | --- |
| **Adres** | **Funkcja** | **Zastosowanie** |
| 0.0.0.0 | Adres domyślnej trasy | Użycie w tablicach routingu |
| 127.0.0.1 | Adres pierwszej pętli zwrotnej | Komunikacja sieciowa hosta z samym |
| 255.255.255.255 | Adres rozgłoszeniowy w sieci lokalnej | Komunikacja hosta ze wszystkimi hostami w ramach jednej sieci fizycznej |

5. Translacja i przydzielanie adresów

Liczba komputerów przyłączonych do internetu ciągle rośnie. Za rozwój internetu w Europie odpowiada stowarzyszenie **RIPE** – Europejska Sieć IP (fr. *Reseaux IP Europeens*). Zadaniem stowarzyszenia jest administracyjna i techniczna koordynacja zadań i prac związanych z rozwojem i utrzymaniem internetu. Każdy z komputerów pracujących w sieci musi mieć unikatowy adres IP, przydzielony przez odpowiedni urząd – Internet Assigned Numbers Authority (IANA). Adresy takie są nazywane **publicznymi** – można je uzyskać w urzędzie IANA lub od dostawcy usług internetowych.

W Polsce **NASK** (Naukowa i Akademicka Sieć Komputerowa) prowadzi tzw. **Local Internet** **Registry** i przydziela adresy IP swoim klientom (również tym, którzy łącza się za pośrednictwem firm nieposiadających własnego rejestru, a dołączonych do NASK). Wszystkie informacje są rejestrowane w **RIPE NCC** (*RIPE Network Coordination Centre*), która jest osobną organizacją zajmującą się zarządzaniem zasobami internetowymi, takimi jak adresy IPv4 i IPv6. RIPE NCC przydziela adresy IP firmom i organizacjom ze swojego regionu, czyli także z Polski. Prowadzi również bazę danych (*RIPE Database*) zawierającą dane dotyczące przydzielonych zasobów internetowych.

Adres publiczny IP można uzyskać od dostawcy usług internetowych. W takim przypadku otrzymuje się adres z puli przydzielonej dostawcy. Aby umożliwić wszystkim komputerom w danej instytucji, np. w szkole, korzystanie z internetu, należałoby przydzielić każdemu z nich indywidualny adres publiczny. Sytuacja taka byłaby niekorzystna z powodu szybkiego wyczerpania dostępnej puli adresów. W celu zmniejszenia zapotrzebowania na adresy publiczne zarezerwowano pule **adresów prywatnych**. Adresy te można dowolnie stosować w sieciach lokalnych, nie są natomiast widoczne w internecie. Adresy prywatne mogą się powtarzać w różnych sieciach lokalnych, nie powodując konfliktu.

Istnienie adresów prywatnych przewidziano dla każdej klasy adresów nieroutowalnych i zarezerwowano:

* dla klasy A adresy od 10.0.0.0 do 10.255.255.255 (jedna sieć z 16 777 214 hostów),
* dla klasy B adresy od 172.16.0.0 do 172.31.255.255 (16 sieci po 65 534 hosty),
* dla klasy C adresy od 192.168.0.0 do 192.168.255.255 (256 sieci po 254 hosty).

Komputery z adresami prywatnymi nie mogą bezpośrednio wymieniać danych w internecie. Jest to możliwe dopiero po przetłumaczeniu adresów prywatnych na adres publiczny za pomocą usługi NAT (*Network Address Translation*). Tłumaczenie adresów odbywa się w bramie internetowej umieszczonej między siecią prywatną a internetem.

W systemach Windows jest wykorzystywana usługa APIPA (Automatic Private IP Addressing). Usługa ta jest odpowiedzialna za automatyczne przydzielanie adresu IP komputerowi w przypadku, gdy karta sieciowa komputera jest skonfigurowana do żądania przyznania adresu IP z serwera DHCP, a serwer DHCP w danym momencie jest nieosiągalny. Adres IP jest przydzielany z puli 169.254.0.1 – 169.254.255.254 z domyślną maską 255.255.0.0. Gdy serwer DHCP stanie się osiągalny, komputer automatycznie uzyska adres IP z puli przyznawanej przez serwer.

6. Zapobieganie wyczerpywaniu się puli adresów.

Początkowo sieć komputerowa zbudowana była z kilku komputerów. Dostępna liczba adresów (ponad 4 miliardy – 326) wydawała się twórcom standardu IPv4 wystarczająca do zaspokojenia potrzeb użytkowników. Szybki rozwój sieci i przyłączanie nowych komputerów doprowadziły do sytuacji, w której zaczęło brakować dostępnych adresów. Inną przyczyną tego stanu było adresowanie klasowe. Jeżeli, np. występuje konieczność przyłączenia do internetu sieci złożonej z 15 komputerów, to należy zarezerwować całą najmniejszą sieć klasy C. Sieć klasy C pozwala na zaadresowanie 254 hostów, co oznacza, że nie wykorzysta się 239 adresów (mimo zarezerwowania w IANA puli 254 adresów). Kolejną niezgodnością przyjętego schematy adresowania jest to, że na sieci klasy A przeznaczono połowę wszystkich dostępnych adresów. Ponieważ tych sieci jest tylko 126, trudno jest znaleźć organizację, która będzie w stanie wykorzystać wszystkie adresy klasy A. Istnieje wiele metod zapobiegania wyczerpaniu się adresów.

Należą do nich m.in:

* wykorzystanie adresów prywatnych
* adresowanie bezklasowe
* adresowanie IPv6

7. Adresowanie bezklasowe

Dla adresów zgrupowanych w klasach przyjęto domyślnie maski podsieci: 8-bitową dla klasy A, 16-bitową dla klasy B i 24-bitową dla klasy C. Maski podsieci określają, które bity w adresie identyfikują sieć, a które hosta.

|  |  |  |
| --- | --- | --- |
| **Klasa adresu** | **Najstarsze bity 1 oktetu** | **Zakres wartości 1 oktety** |
| Klasa A | 0 | 0-127 (126) |
| Klasa B | 10 | 128-191 |
| Klasa C | 110 | 192-223 |
| Klasa D | 1110 | 224-239 |
| Klasa E | 1111 | 240-255 |

|  |  |  |
| --- | --- | --- |
| Klasa A  128 | Klasa B  64 | |
| Klasa C  32 | Klasa D  16 |
| Klasa E  16 |

W celu zapewnienia większej elastyczności w przydzielaniu adresów IP wprowadzono pojęcie maski podsieci (Subnetwork Mask), oznaczonej skrótem SM. Maska podsieci określa ile bitów w adresie jest przeznaczonych do identyfikacji sieci i podsieci (ID network), a ile bitów do identyfikacji hosta (IP host). Maska podsieci składa się z tej samej liczby bitów, co adres IP. W masce w części sieci (IP network) i podsieci (ID subnetwork) występują same jedynki (w systemie dwójkowym), a w części hosta (ID host) same zera. Przykładowo w sieci klasy C w części sieci adresu IP przeznaczono 24 bity, a w części hosta 8 bitów:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Reprezentacja dwójkowa | 11111111 | . | 11111111 | . | 11111111 | . | 00000000 |
| Reprezentacja dziesiętna | 255 | . | 255 | . | 255 | . | 0 |
| Reprezentacja krótka (notacja CIDR) | /24 | . |  | . |  | . |  |

Reprezentacja krótka maski podsieci, zwana również notacją CIDR (Classless Intel-Domain Routing), informacje o ilości jedynek występujących w zapisie dwójkowym maski dzięki masce podsieci można wydzielić podsieci z mniejszą liczbą komputerów, niż wynikałoby to z użycia pełnej klasy adresów. Aby utworzyć podsieć, należy wykorzystać bity z części przeznaczonej na hosta. Jeśli zostaną wykorzystane np. trzy bity z części przeznaczonej na hosta w klasie C, to otrzyma się następujący podział bitów na poszczególne części i wartości maski podsieci:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sieć | | | | | | | | | | | | | | | | | | | | | | | | | | . | podsieć | | | host | | | |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 |  |  |  |  |
| 255 | | | | | | | | . | 255 | | | | | | | | . | 255 | | | | | | | | . | 224 | | | | | | |
| /27 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Podsieci można również wyodrębnić w sieciach klasy A i B. Należy jednak pamiętać, że do tworzenia podsieci zawsze wykorzystuje się bity z części przeznaczonej dla hosta.

**Wyznaczanie adresu sieci**

Każdy z komputerów któremu przydzielono adres IP musi należeć do jakiejś sieci. Aby ustalić, do jakiej sieci należy komputer, koniecznie jest wykonanie obliczeń w systemie dwójkowym. W tym celu należy najpierw przedstawić adres komputera i jego maski podsieci w systemie dwójkowym. Omówiony zostanie przykład komputera o adresie 192.168.0.123 i masce podsieci 255.255.255.224. Adresy komputera i maski podsieci w postaci dwójkowej:

Adres IP

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 192 | | | | | | | | 168 | | | | | | | | 0 | | | | | | | | 123 | | | | | | | |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |

Adres maski podsieci SM

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 255 | | | | | | | | 255 | | | | | | | | 255 | | | | | | | | 224 | | | | | | | |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |

Aby określić do jakiej podsieci należy ten adres, należy wykonać operację obliczania iloczynu logicznego AND na poszczególnych bitach adresu IP i mask podsieci SM.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| 192 | | | | | | | | 168 | | | | | | | | 0 | | | | | | | | 96 | | | | | | | |

Komputer należy do podsieci 192.168.0.96

Porada

Adres sieci można określić w następujący sposób:

* przepisz z adresu IP wszystkie bity na pozycjach w których w masce sieci i podsieci jest wartość 1.
* W pozostałych miejscach adresu sieci wpisz 0.

**Wyznaczanie adresu rozgłoszeniowego**

Adres rozgłoszeniowy (broadcast to adres, dzięki któremu komputer może wysyłać wiadomość do wszystkich urządzeń w danej sieci lub podsieci (domenie rozgłoszeniowej). Aby ustalić adres rozgłoszeniowy w danej sieci, należy także wykonać obliczenia w systemie dwójkowym. W tym celu zostanie przedstawiony adres komputera i jego maski podsieci w systemie dwójkowym. Omówiony zostanie ten sam przykład: komputer o adresie 192.168.0.123 i masce podsieci 255.255.255.224.

Aby określić adres rozgłoszeniowy na podstawie adresu IP oraz maski podsieci, należy wykonać operację obliczania sumy logicznej OR na adresie IP oraz negacji maski podsieci na poszczególnych bitach.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| 192 | | | | | | | | 168 | | | | | | | | 0 | | | | | | | | 127 | | | | | | | |

Adres rozgłoszeniowy w tej postaci to 192.168.0.127.

Porada

Adres rozgłoszeniowy można określić w następujący sposób:

- przepisz adresy IP wszystkie bity na pozycjach, w których w masce podsieci jest wartość 1

- w pozostałych miejscach wpisz 1

**Obliczanie ilości podsieci**

Liczba możliwych do utworzenia podsieci zależy od liczby bitów z części hosta przeznaczonych do utworzenia podsieci. W powyższym przykładzie na podsieci zostały przeznaczone 3 bity. Na 3 bitach można reprezentować 23 = 18 różnych wartości i tyle podsieci możemy utworzyć. Jednak pierwsza (same zera) i ostatnia (same jedynki) z tych podsieci nie będzie mogła być wykorzystywana, chyba że wszystkie urządzenia w sieci spełnią dodatkowe warunki dotyczące wymagań sprzętowych i programowych. Pierwsza podsieć ma taki sam adres sieci, jak cała klasa C, natomiast ostatnia ma taki sam adres rozgłoszeniowy jak klasa C. Efektywność spośród 8 podsieci możemy wykorzystać tylko 6.

**Zadanie**

Obliczyć liczbę podsieci, które można wydzielić z podsieci 172.160.0 przy zastosowaniu maski 255.255.192.0.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 255 | | | | | | | | 255 | | | | | | | | 192 | | | | | | | | 0 | | | | | | | |
| 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Liczba podsieci wynosi 22 = 4 - 2

**Obliczanie liczby hostów w danej podsieci**

Liczba możliwych hostów w podsieci zależy od liczby bitów w części hosta. W powyższym przykładzie na część hosta pozostało 5 bitów. Na 5 bitach można reprezentować 25 (= 32) wartości. Jednal adres zawierający w części hosta same zera jest adresem rozgłoszeniowym podsieci. Adresy te są zarezerwowane i nie wolno ich przypisać do żadnego urządzenia w sieci. Oznacza to, że w omawianej podsieci i może być maksymalnie 30 hostów.

**Zadanie**

Obliczyć liczbę adresów, które można przypisać hostom w podsieci 172.16.0.0, przy zastosowaniu maski 255.255.252.0.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 255 | | | | | | | | . | 255 | | | | | | | | . | 252 | | | | | | | | . | 0 | | | | | | | |
| 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | . | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | . | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | . | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | . | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Liczba adresów, które można przypisać hostom wynosi 210 = 1024 – 2.

UWAGA!!!

Minimalna liczba bitów przeznaczona na część podsieci adresu IP wynosi 2. Jeżeli na część podsieci zostanie przeznaczony 1 bit, to liczba podsieci wyniesie 2, a liczba podsieci efektywnych 0 – tzn. nie moglibyśmy utworzyć podsieci. Liczba bitów przeznaczona na część hosta adresu IP nie może być mniejsza niż 2 - -liczba hostów w takiej podsieci wynosi 2.

**Przydzielanie adresów IP**

Tabela zawiera wszystkie informacje o adresach w analizowanej sieci klasy C dla maski podsieci /27:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Numer podsieci** | **Adres sieci** | **Adresy hostów** | **Adres rozgłoszeniowy** | **Uwagi** |
| 0 | 192.168.0.0 | 192.168.0.1 do 192.168.0.30 | 192.168.0.31 | Adres całej sieci (podsieć możliwa do wykorzystania tylko w sieciach spełniających dodatkowe wymagania) |
| 1 | 192.168.0.32 | 192.168.0.33 do 192.168.0.62 | 192.168.0.63 |  |
| 2 | 192.168.0.64 | 192.168.0.65 do 192.168.0.94 | 192.168.0.95 |  |
| 3 | 192.168.0.96 | 192.168.0.97 do 192.168.0.126 | 192.168.0.127 |  |
| 4 | 192.168.0.128 | 192.168.0.129 do 192.168.0.158 | 192.168.0.159 |  |
| 5 | 192.168.0.160 | 192.168.0.161 do 192.168.0.190 | 192.168.0.191 |  |
| 6 | 192.168.0.192 | 192.168.0.193 do 192.168.0.222 | 192.168.0.223 |  |
| 7 | 192.168.0.224 | 192.168.0.225 do 192.168.0.254 | 192.168.0.255 | Adres rozgłoszeniowy całej sieci (podsieć możliwa do wykorzystania tylko w sieciach spełniających dodatkowe wymagania) |

Zadanie

Postępując analogicznie jak w omówionym przykładzie, wpisz w tabeli wszystkie informacje o dresach w sieci 192.168.16.0 z maską 255.255.255.240.

**Sprawdzanie komunikacji między komputerami**

Komputery będą mogły bezpośrednio komunikować się ze sobą, jeżeli będą w tej samej sieci, to znaczy będą miały taki sam adres sieci. Jeżeli adresy będą różne, to bezpośrednia komunikacja między nimi nie będzie możliwa. Aby sprawdzić, czy komputery będą mogły komunikować się w sieci, należy (jak w poprzednim ćwiczeniu), wyznaczyć adresy sieci obu komputerów i je porównać. Na przykład weźmy dwa komputery, którym przydzielono adresy odpowiednio 10.20.30.40 i 10.20.30.140 oraz maskę podsieci 255.255.255.240.

Wyznaczanie adresu sieci komputera o adresie IP 10.20.30.40 i masce SM 255.255.255.240:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | . | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | . | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | . | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | . | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | . | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | . | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 10 | | | | | | | | . | 20 | | | | | | | | . | 30 | | | | | | | | . | 32 | | | | | | | |

Wyznaczanie adresu sieci komputera o adresie IP 10.20.30.140 i masce SM 255.255.255.240:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | . | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | . | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | . | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | . | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | . | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | . | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | | | | | | | | . | 20 | | | | | | | | . | 30 | | | | | | | | . | 128 | | | | | | | |

Komputer o adresie 10.20.30.40 należy do sieci 10.20.30.32. Komputer o adresie 10.20.30.140 należy do sieci 10.20.30.128. Ponieważ adresy sieci są różne, komputery nie będą mogły bezpośrednio się komunikować.

Zadanie

Sprawdź, czy komputery o adresach 10.1.12.123 i 10.1.12.234, pracujące w sieci z maską 255.255.255.224, będą mogły się komunikować.

Wyznaczanie adresu sieci komputera o adresie IP 10.1.12.123 i masce SM 255.255.255.224:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | . | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | . | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | . | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | . | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | . | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | . | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 10 | | | | | | | | . | 1 | | | | | | | | . | 12 | | | | | | | | . | 96 | | | | | | | |

Wyznaczanie adresu sieci komputera o adresie IP 10.1.12.234 i masce SM 255.255.255.224:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | . | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | . | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | . | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | . | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | . | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | . | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | . | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 10 | | | | | | | | . | 1 | | | | | | | | . | 12 | | | | | | | | . | 224 | | | | | | | |

Komputer o adresie 10.1.12.123 należy do sieci 10.1.12.96. Komputer o adresie 10.1.12.234 należy do sieci 10.1.12.224. Ponieważ adresy sieci są różne, komputery nie będą mogły bezpośrednio się komunikować.

Zadanie

Jesteś administratorem szkolnej sieci komputerowej, która składa się z 6 pracowni komputerowych, a w każdej z nich jest po 18 komputerów, pracujących w różnych podsieciach. Twoim zadaniem jest przydzielenie komputerom adresów prywatnych z klasy C. Należy przydzielić komputerom adresy w taki sposób, aby jak najwięcej adresów pozostało do dyspozycji w przyszłości. Komputery nie mogą mieć możliwości wymiany danych z urządzeniami z innej pracowni. Określ:

* maskę podsieci, jednakową dla wszystkich komputerów,
* adres sieci i rozgłoszeniowy dla wszystkich podsieci,
* adresy IP, jakie będą przypisane do komputerów w poszczególnych podsieciach,
* maksymalną liczbę podsieci w szkole,
* maksymalną liczbę komputerów w podsieci.

8. Pętla zwrotna

W puli wszystkich adresów IP istnieje zakres adresów, które zostały zarezerwowane do specyficznego wykorzystania. Jednym z takich zakresów jest sieć 127.0.0.0, czyli adresy IP z przydziału 127.0.0.1 – 127.255.255.254. Adresy te są wykorzystywane w celu adresowania komputera (urządzenia) lokalnego. Komunikacja z tym adresem odwołuje się do urządzenia, które tę komunikację wywołało.

Mechanizm tej komunikacji jest nazywany **pętlą lokalną** lub **pętlą zwrotną** (*loopback*). Pętla zwrotna to wirtualne urządzenie sieciowe, które z poziomu systemu operacyjnego nie różni się od fizycznej karty sieciowej. Komunikacja między adresem pętli zwrotnej może odbywać się poprzez dowolny adres należący do sieci 127.0.0.0 lub poprzez nazwę **localhost** (w systemie operacyjnym nazwa przypisana dla adresu 127.0.0.1).

Mechanizm pętli zwrotnej może być wykorzystywany do kontroli poprawności instalacji obsługi protokołu IP w systemie operacyjnym.

**Zasady projektowania adresacji IP**

Podczas nadawania urządzeniom w sieci adresów IP należy przestrzegać następujących reguł:

* wszystkie urządzenia w jednym fizycznym segmencie sieci powinny mieć ten sam adres sieci;
* część adresu IP określająca hosta musi być unikatowa dla każdego urządzenia w segmencie sieci;
* nie można stosować adresów składających się z samych jedynek, tzn. 255.255.255.255 – jesto to adres rozgłoszeniowy całej sieci;
* nie można stosować adresów, w których wszystkie bity mają wartość zero tzn. 0.0.0.0 – jest to adres rozgłoszeniowy całej sieci;
* nie można stosować adresów, w których w części hosta są same zera – jest to adres podsieci;
* nie można stosować adresów, w których w części hosta są same jedynki – jest to adres rozgłoszeniowy podsieci;
* długość maski podsieci dobrać tak, aby zapewnić wystarczającą liczbę dostępnych adresów, dla wszystkich urządzeń w podsieci.

Podczas projektowania struktury IP należy dobrać wielkość podsieci tak, aby maksymalnie wykorzystywać dostępne adresy, a jednocześnie struktura adresów była czytelna dla administratora sieci i użytkowników. W celu lepszego wykorzystywania dostępnych adresów wprowadzono technikę **podsieci o zmiennej długości maski VLSM** (*Variable Lenght Subnet Mask*). Technika ta pozwala na używanie w jednej przestrzeni adresowej wielu masek sieci o różnej długości. Zastosowanie tej techniki jest jednak możliwe tylko w sieciach korzystających z nowoczesnych protokołów routingu, takich jak OSPF, EIGRP lub RIPv2.

**Projektowanie sieci z wykorzystaniem techniki VLSM**

Przykład sieci obejmującej 5 miast Mława i Łódź (po 10 komputerów w podsieci), Warszawa, Wrocław i Poznań (po 25 komputerów w podsieci). Należy przydzielić każdej podsieci odpowiednią ilość adresów IP z puli adresów klasy C, np. 192.168.1.0 z maską 255.255.255.0.

Liczba komputerów w największej podsieci wynosi 25. Na część hosta należy więc przeznaczyć 5 bitów (25 = 32). Na adres podsieci pozostają 3 bity, co pozwala na efektywne zaadresowanie 6 podsieci (28 – 2). Zastosowanie jednakowej maski do wszystkich podsieci powoduje, że w każdej podsieci pozostaną niewykorzystane adresy, natomiast dla czterech podsieci zabraknie adresów z dostępnej puli (należy utworzyć 5 podsieci dla komputerów i 5 podsieci łączących routery).

Technika VLSM pozwala przydzielić podsieciom maski o różnej długości. W Warszawie, Wrocławiu i Poznaniu można zastosować maskę o długości 27 bitów, w Mławie i Łodzi – 28 bitów, a do połączenia między routerami maski 30-bitowe.

Adresy w podsieci w technice VLSM:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Numer podsieci** | **Adres podsieci** | **Adres podpodsieci** | **Liczba hostów** | **Maksa podsieci** | **Uwagi** |
| 0 | 192.168.1.0 |  |  |  | Adres całej sieci |
| 1 | 192.168.1.32 |  | 30 (=25-2) | /27 | Warszawa (25 komputerów) |
| 2 | 192.168.1.64 |  | 30 (=25-2) | /27 | Wrocław (25 komputerów) |
| 3 | 192.168.1.96 |  | 30 (=25-2) | /27 | Poznań (25 komputerów) |
| 4 | 192.168.1.128 | 192.168.1.128 | 14 (=24-2) | /28 | Łódź (25 komputerów) |
| 192.168.1.144 | 14 (=24-2) | /28 | Mława (10 komputerów) |
| 5 | 192.168.1.160 | 192.168.1.164 | 2 (=22-2) | /30 | Wrocław-Poznań |
| 192.168.1.168 | 2 | /30 | Poznań-Łódź |
| 192.168.1.172 | 2 | /30 | Łódź-Mława |
| 192.168.1.176 | 2 | /30 | Mława-Warszawa |
| 192.168.1.180 | 2 | /30 |  |
| 192.168.1.184 | 2 | /30 |  |
| 192.168.1.188 | 2 | /30 |  |
| 6 | 192.168.1.192 |  | 30 | /27 |  |
| 7 | 192.168.1.224 |  |  |  | Adres rozgłoszeniowy całej sieci |

Dzięki technice VLSM można nie tylko przydzielić każdej z podsieci wymaganą liczbę adresów, ale jeszcze część adresów pozostanie wolna z możliwością wykorzystania w przyszłości.

Zadanie

Na potrzeby sieci komputerowej przeznaczono jedną podsieć klasy B. Zaprojektuj strukturę adresów IP dla sieci obejmują 7 miast: Warszawa i Moskwa po 50 hostów, Berlin i Praga po 20 hostów, Paryż, Londyn i Rzym po 12 hostów. Dobierz schemat adresowania, w którym do wszystkich podsieci zastosowano jednakową maskę podsieci oraz schemat z maskami o zmiennej długości. Podaj adresy: sieci i rozgłoszeniowe oraz zakresy dopuszczalnych adresów dla każdej podsieci, zakładając, że maksymalna liczba adresów powinna pozostać do wykorzystania w przyszłości.

**Adresowanie IPv6**

Adresowanie **IPv6** wprowadzono ze względu na wyczerpywanie się dostępnej puli adresów IPv4. Adresy IPv6 mają długość 128 bitów, co pozwala na uzyskanie 2128 adresów (3,4\*1038). Protokół IPv6 nie jest zgodny z protokołem IPv4. Aby host lub router rozpoznawał i przetwarzał obie wersje adresów, musi korzystać zarówno z protokołu IPv4, jak i IPv6. Protokół IPv6 obsługuje zarówno konfigurację adresów przy wykorzystaniu serwera DHCP, jak i bez tego serwera. Do IPv6 dodano nową wersję protokołu dynamicznej konfiguracji hostów **DHCPv6** (*Dynamic Host Configuration Protocol for IPv6*) umożliwiającego komputerom uzyskanie od serwera danych konfiguracyjnych, np. adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski podsieci. Jego specyfikacja została opisana w **RFC 3315**. Hosty podłączone do tego samego łącza mogą automatycznie konfigurować dla siebie adresy lokalne dla łącza i komunikować się bez konfiguracji ręcznej.

Adres IPv6 składa się ze **128 bitów** podzielonych na osiem **16-bitowych** bloków, oddzielonych dwukropkami. Każdy 16-bitowy blok reprezentowany jest za pomocą **4-cyfrowej** liczby szesnastkowej, np. adres binarny:

0010000111011010 0000000011010011 0000000000000000 0010111100111011

0000001010101010 0000000011111111 1111111000101000 1001110001011010

Reprezentowany jest przez adres szesnastkowy:

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9c5A.

Reprezentacja IPv6 może zostać uproszczona poprzez usunięcie poprzedzających zer z każdego 16-bitowego bloku. W tym uproszczeniu każdy blok musi posiadać przynajmniej jeden znak. Po pominięciu poprzedzających zer reprezentacja adresu wygląda następująco:

21DA:D3:0:2F3B:2AA:FF:FE28:9C5A.

Dozwolone jest pominięcie ciągu bloków składających się wyłącznie z zer. Pomijając bloki zer, wprowadza się separator bloków:: (podwójny dwukropek). Dopuszczalny jest tylko jeden podwójny dwukropek :: w adresie. Poniższe adresy są równoznaczne:

2001:0db8:0000:0000:0000:0000:1234:abcd

2001:0db8:0:0:0:0:1234:abcd

2001:0db8:0:0:::1234:abcd

2001:0db8::1234:abcd

2001:db8::1234:abcd.

W adresacji wykorzystywanej w protokole IPv6 używane są trzy typy adresów:

* **unicast** – identyfikujące pojedynczy interfejs
* **multicast** – identyfikujące grupę interfejsów (mogą one należeć do różnych węzłów),
* **anycast** – podobnie jak adresy multicast, identyfikują one grupę interfejsów, jednak pakiet wysyłany na adres anycast jest dostarczany do najbliższego węzła, np. najbliższego serwera DNS.

W protokole IPv6 nie występuje pojęcie komunikacji broadcastowej (dane rozsyłane do wszystkich węzłów w danej podsieci). Aby wysyłać dane do wielu odbiorców jednocześnie, należy korzystać z komunikacji multicastowej.

W IPv6 rozróżniane są zakresy adresów:

* **Adresy lokalne dla łącza** (*link-local address*) – wykorzystywane tylko do komunikacji w jednym segmencie sieci lokalnej lub przy połączeniu typu point-to-point. Routery nie przekazują pakietów z adresami lokalnymi. Adresy te mają prefiks FR80::/10. Każdy interfejs musi mieć przydzielony co najmniej jeden adres lokalny dla łącza, nawet jeżeli posiada adres globalny lub unikalny adres lokalny. Zakres ten odpowiada zakresowi APIPA w IPv4 (169.254.0.0/16).
* **Unikalne adresy lokalne** (*unique local address*) – adresy będące odpowiednikami adresów prywatnych z protokołu IPv4. Adresy te mają prefiks FC00::/7.
* **Adresy globalne** (*global unicast address*) – adresy będące odpowiednikami adresów publicznych z protokołu IPv4. Adresy te to wszystkie inne nie wymienione we wcześniejszych punktach.

W protokole IPv6 zdefiniowano również adresy specjalne, np.:

* ::/128 – adres nieokreślony (zawierający same zera);
* ::1/128 – pętla zwrotna (*loopback*) – adres wskazujący na host lokalny;
* 2001:db8::/32 – pula wykorzystywana w przykładach i dokumentacji – nigdy nie będzie wykorzystywana produkcyjnie;
* Ff00::/8 – pula multicastowa używana do komunikacji milticast.

Nagłówek pakietu w protokole IPv6 został uproszczony (składa się z mniejszej liczby pól) i jest łatwiejszy w przetwarzaniu przez routery. Składa się z nagłówka podstawowego i nagłówków rozszerzających. Nagłówki rozszerzające, następujące po nagłówku głównym IPv6, są opcjonalne i zawierają dodatkowe opcje protokołu.

W skład podstawowego nagłówka wchodzą następujące pola:

* Wersja (4 bity) – definiująca wersję protokołu, w przypadku IPv6 pole to zawiera wartość 6 (bitowo 0110);
* Klasa ruchu (8 bitów) – określa priorytet przesyłania pakietu (odpowiednik pola *Type of service* z IPv4);
* Etykieta przepływu (20 bitów) – pole służące do oznaczania strumienia pakietów IPv6;
* Długość danych (16 bitów) – wielkość pakietu, nie wliczając długości podstawowego nagłówka (wliczając jednak nagłówki rozszerzające);
* Następny nagłówek (8 bitów) – identyfikuje nagłówek rozszerzający występujący bezpośrednio po nagłówku IPv6;
* Limit przeskoków (8 bitów) – ilość węzłów sieci, po przejściu których pakiet zostaje usunięty z sieci (odpowiednik pola TTL z IPv4);
* Adres źródłowy (128 bitów) – adres węzła, który wysłał pakiet;
* Adres docelowy (128 bitów) – adres węzła, do którego adresowany jest pakiet.

Mimo zalet oraz gotowości systemów operacyjnych do obsługi, adresowanie IPv6 nie jest jeszcze powszechne stosowane. Jest to spowodowane koniecznością wymiany sprzętu sieciowego (lub przynajmniej oprogramowania) u dostawców internetu, co jest operacją kosztowną i wymaga czasu.

Zadanie 1

Sprawdź, czy Twój komputer ma przydzielony adres IPv6 (polecenie ipconfig).

* Jeżeli Twój komputer ma przydzielony adres IPv6, to sprawdź, czy odpowiada na ping (polecenie ping -6 ::1),
* Jeżeli Twój komputer ma przydzielony adres IPv6, to sprawdź, czy komputer kolegi odpowiada na ping (polecenie -6 <adres IPv6>).

Zadanie 2

Podzielić sieć adresów klasy C na 4 podsieci dla adresu 199.10.20.0.

Rozwiązanie

Maska podsieci dla sieci klasy C składa się z 24 bitów oznaczających adres sieci oraz z 8 bitów oznaczających adres hosta.

Aby utworzyć nową maskę, która podzieli pulę adresów danej sieci na 4 podsieci, należy znaleźć taką liczbę bitów, by możliwe było stworzenie 4 kombinacji. Posługując się wzorem *2n>=LSUB*, wyznaczamy liczbę n = 2:

22>= 4.

Mając wyznaczoną liczbę n, należy zwiększyć liczbę bitów oznaczonych 1 w części hosta o dwa.

|  |  |
| --- | --- |
| Adres sieci do podziału | 199.10.20.0 |
| Domyślna maska podsieci | 255.255.255.0 |
| Domyślna maska podsieci w postaci binarnej | 11111111 11111111 11111111 00000000 |
| Nowa postać maski podsieci w zapisie binarnym | 11111111 11111111 11111111 11000000 |
| Nowa postać maski podsieci w zapisie dziesiętnym | 255.255.255.192 |

Mając określoną długość maski podsieci, możemy określić zakresy adresów w poszczególnych podsieciach, a także adresy podsieci i adresy rozgłoszeniowe (tabela poniżej).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Numer podsieci** | **Zakres adresów w podsieci (dwójkowy)** | **Adres podsieci** | **Adres początkowy** | **Adres końcowy** | **Adres rozgłoszeniowy** |
| Podsieć 0 | 00000000 00111111 | 199.10.20.0 | 199.10.20.1 | 199.10.20.62 | 199.10.20.63 |
| Podsieć 1 | 01000000 01111111 | 199.10.20.64 | 199.10.20.65 | 199.10.20.126 | 199.10.20.127 |
| Podsieć 2 | 10000000 10111111 | 199.10.20.128 | 199.10.20.129 | 199.10.20.190 | 199.10.20.191 |
| Podsieć 3 | 11000000 11111111 | 199.10.20.192 | 199.10.20.193 | 199.10.20.254 | 199.10.20.255 |