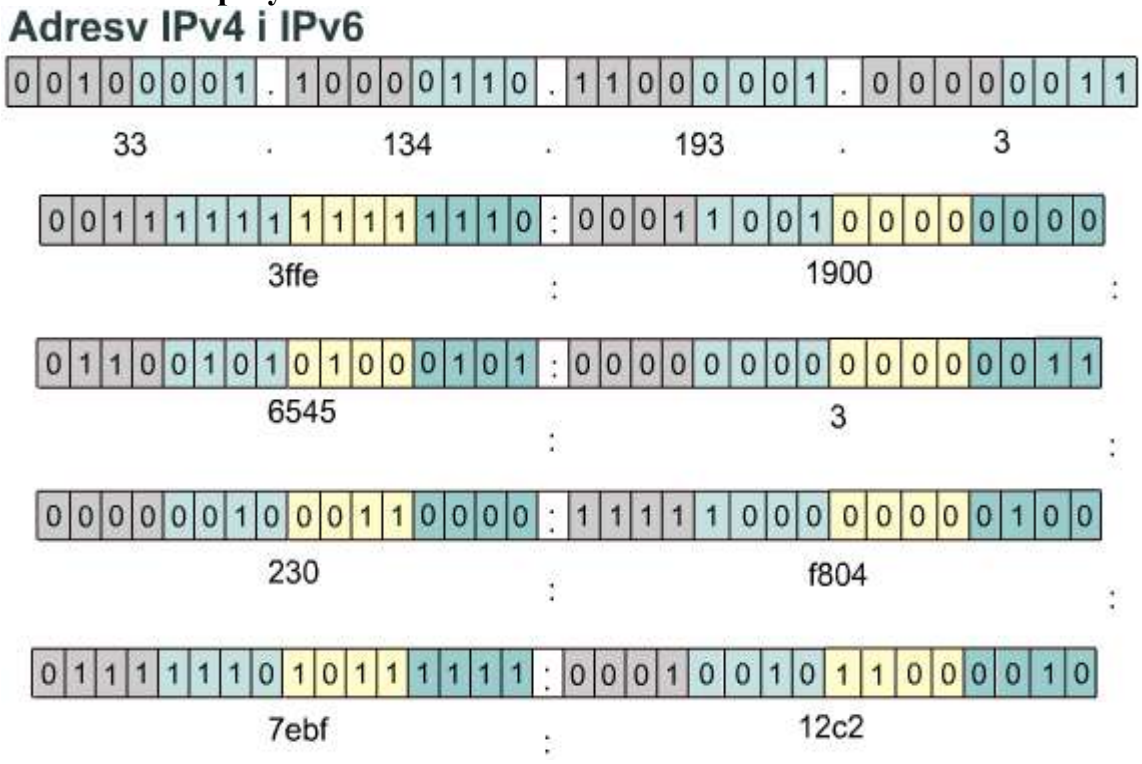
Moduł 9. Zestaw protokołów TCP/IP

Internet został zaprojektowany jako sieć łączności, która mogłaby działać także w okresie wojny. Chociaż Internet ewoluował w zupełnie innych kierunkach, niż wyobrażali to sobie jego twórcy, nadal jego podstawę stanowi zestaw protokołów TCP/IP. Architektura protokołów TCP/IP doskonale nadaje się do wykorzystania w zdecentralizowanej i odpornej na błędy sieci. Taką siecią jest Internet. Wiele z używanych aktualnie protokołów zostało opartych na czterowarstwowym modelu TCP/IP. Warto poznać zarówno model sieciowy TCP/IP, jak i model OSI. Każdy z nich ma własną strukturę, wyjaśniającą działanie sieci, ale modele te mają wiele wspólnych cech. Bez zrozumienia obydwu tych modeli administrator może dysponować zbyt małą wiedzą, aby rozumieć, dlaczego sieć działa w taki, a nie inny sposób.Każde urządzenie w Internecie, które komunikuje się z innymi urządzeniami internetowymi, musi mieć unikatowy identyfikator. Identyfikator ten jest nazywany adresem IP, ponieważ routery w celu znalezienia najlepszej trasy do danego urządzenia używają protokołu IP, należącego do trzeciej warstwy. Aktualnie używana wersja protokołu IP, czyli IPv4, została zaprojektowana w okresie, gdy zapotrzebowanie na adresy nie było duże. Gwałtowny rozwój Internetu zaczął grozić wyczerpaniem puli dostępnych adresów IP. Do zwiększenia możliwości wykorzystania adresów IP bez wyczerpania dostępnej puli adresów wykorzystywany jest podział na podsieci, translacja adresów sieciowych NAT (*Network Address Translation*) oraz adresy prywatne. Inna wersja protokołu IP (protokół IPv6) ma dużo większą przestrzeń adresową, co pozwala na uwzględnienie lub rezygnację z metod wykorzystywanych do wyeliminowania niedostatków protokołu IPv4. Aby stać się częścią Internetu, każdy komputer potrzebuje nie tylko fizycznego adresu MAC, ale i unikatowego adresu IP, nazywanego również adresem logicznym. Istnieje kilka metod przypisywania urządzeniu adresu IP. Niektóre urządzenia zawsze mają adres statyczny, podczas gdy innym przydzielany jest tymczasowy adres za każdym razem, gdy łączą się z siecią. Gdy potrzebny jest adres IP przypisywany dynamicznie, urządzenie może go otrzymać przy użyciu kilku metod. Aby efektywnie routować pakiety pomiędzy urządzeniami, trzeba także rozwiązać inne problemy. Na przykład powtórzone adresy IP mogą uniemożliwić efektywne przekazywanie danych.

9.1 Wprowadzenie do protokołów TCP/IP

9.1.1 Historia i przyszłość modelu TCP/IP

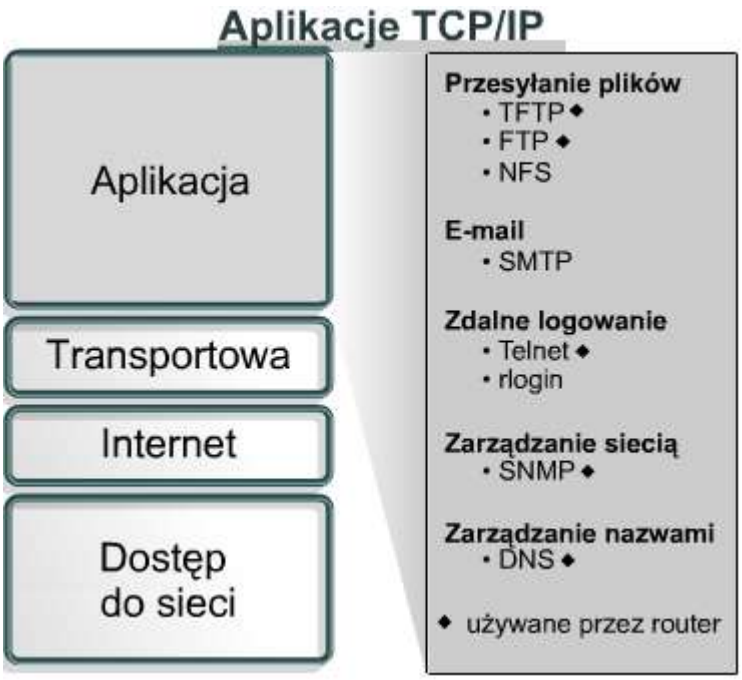


Model odniesienia TCP/IP został utworzony przez Departament Obrony USA w ramach prac nad projektem sieci, która przetrwałaby w każdych warunkach. Aby to lepiej wyjaśnić, wyobraźmy sobie świat połączony różnymi łączami kablowymi, światłowodowymi, mikrofalowymi i satelitarnymi. Następnie wyobraźmy sobie, że chcemy mieć możliwość przesłania danych do dowolnego węzła takiej sieci bez względu na warunki. Departament Obrony USA potrzebował niezawodnej metody transmisji danych do dowolnego miejsca przeznaczenia, niezależnie od warunków. Utworzenie modelu TCP/IP pomogło rozwiązać ten trudny problem. Model TCP/IP stał się od tego czasu standardem, na którym oparty jest Internet.

Czytając o warstwach modelu TCP/IP, należy pamiętać, w jakim celu utworzono Internet. Pomoże to uniknąć nieporozumień. Model TCP/IP składa się z następujących czterech warstw: warstwy aplikacji, warstwy transportowej, warstwy internetowej oraz warstwy dostępu do sieci. Niektóre z warstw modelu TCP/IP mają takie same nazwy jak warstwy modelu OSI. Ważne jest, aby nie pomylić funkcji poszczególnych warstw w tych modelach, ponieważ są one różne w każdym z nich.

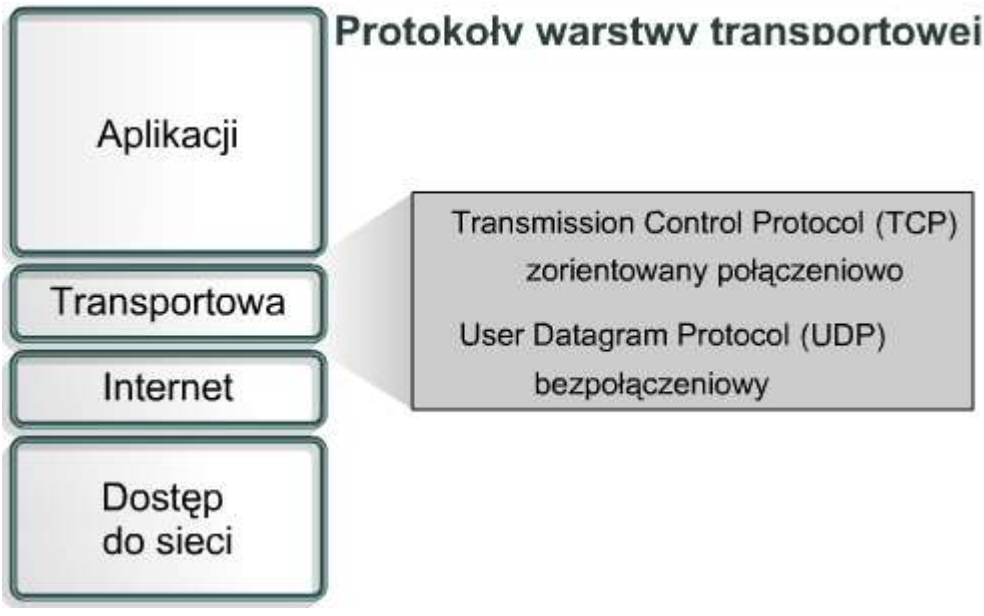
Aktualnie używana wersja TCP/IP stała się standardem we wrześniu 1981 roku.

9.1.2 Warstwa aplikacji



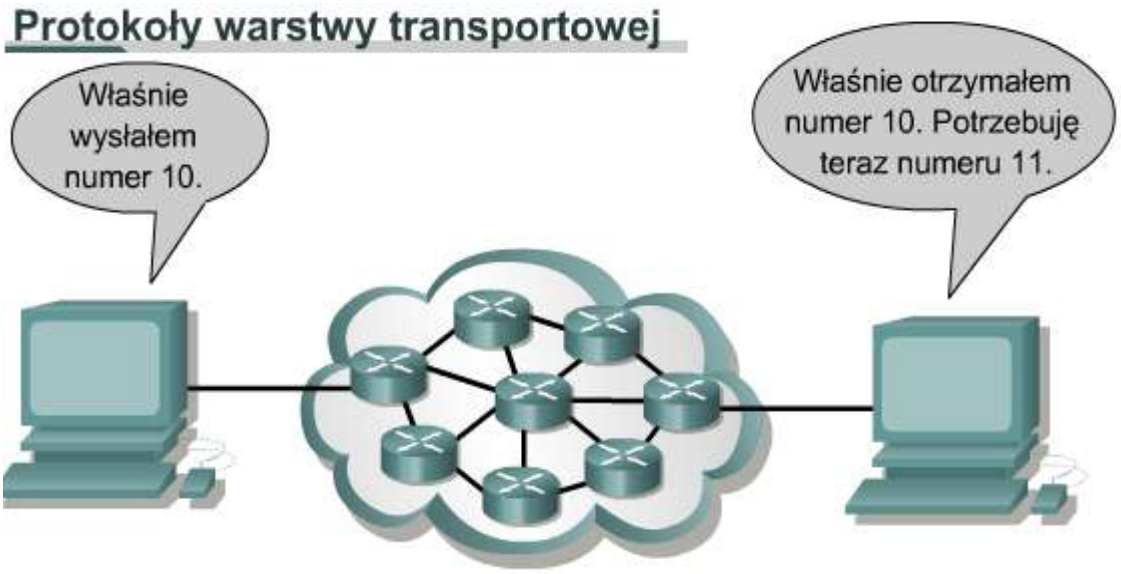
Warstwa aplikacji modelu TCP/IP obsługuje protokoły wysokopoziomowe oraz zajmuje się zagadnieniami związanymi z reprezentacją danych, kodowaniem i sterowaniem konwersacją. Zestaw protokołów TCP/IP łączy w jednej warstwie wszystkie zagadnienia związane z aplikacjami i zapewnia odpowiednie opakowanie danych przed przekazaniem ich do następnej warstwy. Zestaw protokołów TCP/IP zawiera nie tylko specyfikacje protokołów warstwy internetowej i warstwy transportowej, takich jak IP i TCP, ale również specyfikacje powszechnie używanych aplikacji. TCP/IP zawiera protokoły przesyłania plików, poczty elektronicznej i zdalnego logowania, a także:

- **Protokół FTP** ***(File Transfer Protocol)*** — protokół FTP jest niezawodną usługą zorientowaną połączeniowo, używającą protokołu TCP do przesyłania danych pomiędzy systemami korzystającymi z FTP. Umożliwia on dwukierunkowe przesyłanie plików binarnych i tekstowych.
- **Protokół TFTP** ***(Trivial File Transfer Protocol)*** — protokół TFTP jest bezpołączeniową usługą, która używa protokołu UDP. Protokół TFTP jest używany przez router do przesyłania plików konfiguracyjnych oraz obrazów systemu Cisco IOS, a także do przesyłania plików pomiędzy systemami korzystającymi z TFTP. Protokół ten jest użyteczny w niektórych sieciach LAN, ponieważ w stabilnym środowisku działa szybciej niż protokół FTP.
- **Protokół NFS** ***(Network File System)*** — protokół NFS jest utworzonym przez firmę Sun Microsystems zestawem protokołów rozproszonego systemu plików, który umożliwia korzystanie z plików znajdujących się na zdalnych urządzeniach pamięciowych, takich jak dyski sieciowe.
- **Protokół SMTP** ***(Simple Mail Transfer Protocol)*** — protokół SMTP odpowiada za przesyłanie poczty elektronicznej pomiędzy komputerami w sieci. Nie umożliwia on przesyłania danych innych niż tekstowe.
- **Protokół Telnet** ***(Terminal emulation)*** — protokół Telnet umożliwia zdalny dostęp do innego komputera. Pozwala on użytkownikowi na zalogowanie się na hoście internetowym i wykonywanie poleceń. Klient usługi Telnet jest nazywany hostem lokalnym. Serwer usługi Telnet jest nazywany hostem zdalnym.
- **Protokół SNMP** ***(Simple Network Management Protocol)*** — protokół SNMP umożliwia monitorowanie i sterowanie urządzeniami sieciowymi, zarządzanie konfiguracją, zbieranie danych statystycznych oraz zarządzanie wydajnością i zabezpieczeniami.
- **Protokół DNS** ***(Domain Name System)*** — protokół DNS jest używanym w Internecie systemem tłumaczenia nazw domen i należących do nich publicznie dostępnych węzłów sieciowych na adresy IP.



9.1.3 Warstwa transportowa

Warstwa transportowa zapewnia usługi przesyłania danych z hosta źródłowego do hosta docelowego. Ustanawia ona logiczne połączenie pomiędzy punktami końcowymi w sieci, czyli hostem wysyłającym i odbierającym. Protokoły transportowe dzielą i scalają dane wysyłane przez aplikacje wyższej warstwy w jeden strumień danych przepływający między punktami końcowymi, tworzący połączenie logiczne. Strumień danych warstwy transportowej obsługuje transport typu end-to-end, czyli transport między punktami końcowymi. Internet jest zwykle przedstawiany w postaci chmury. Warstwa transportowa wysyła pakiety danych ze źródła do miejsca przeznaczenia poprzez taką chmurę. Przy korzystaniu z protokołu TCP podstawowym zadaniem warstwy



transportowej jest kontrola typu end-to-end, zapewniana przez okna przesuwne, potwierdzenia i niezawodność w stosowaniu kolejnych numerów pakietów. Warstwa transportowa tworzy także połączenia typu end-to-end pomiędzy aplikacjami na hostach. W skład usług transportowych wchodzą wszystkie poniższe usługi:

W przypadku zarówno TCP, jak i UDP

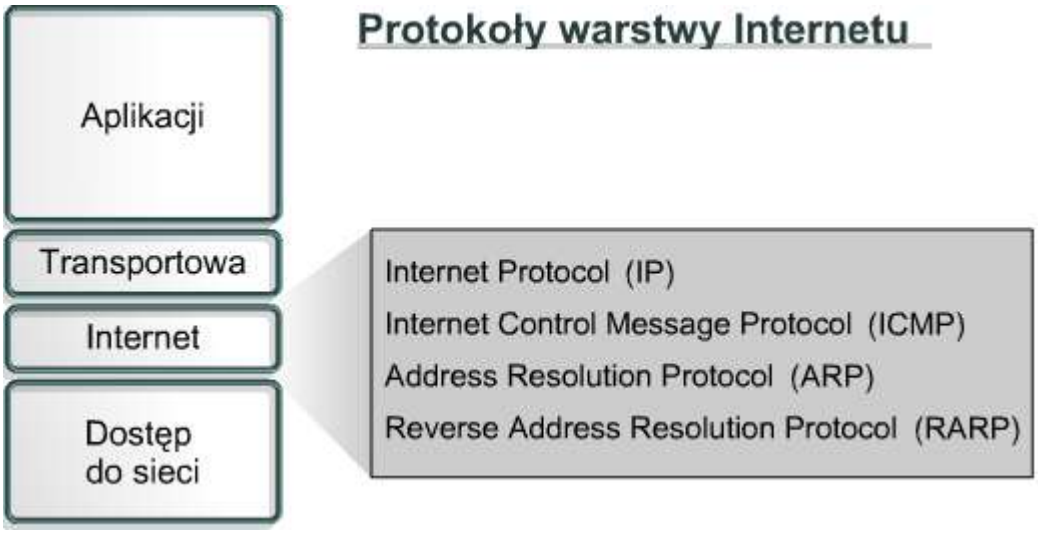
- dzielenie danych aplikacji wyższej warstwy,
- wysyłanie segmentów z jednego urządzenia końcowego do innego,

Tylko w przypadku TCP

- ustanawianie połączenia typu end-to-end,
- kontrola przepływu zapewniana przez okna przesuwne,
- niezawodność zapewniana przez numery sekwencyjne i potwierdzenia.

Internet jest zwykle przedstawiany w postaci chmury. Warstwa transportowa wysyła pakiety danych ze źródła do miejsca przeznaczenia poprzez taką chmurę. Chmura ta musi radzić sobie z takimi zagadnieniami, jak wybór najlepszej trasy spośród kilku dostępnych.

9.1.4 Warstwa Internetu



Zadaniem warstwy Internetu jest wybranie najlepszej ścieżki dla pakietów przesyłanych w sieci. Podstawowym protokołem działającym w tej warstwie jest protokół IP (*Internet Protocol*). W tej warstwie następuje określenie najlepszej ścieżki i przełączanie pakietów.

W warstwie internetowej modelu TCP/IP działają następujące protokoły:

- Protokół IP, który zapewnia usługę bezpołączeniowego dostarczania pakietów przy użyciu dostępnych możliwości. Protokół IP nie bierze pod uwagę zawartości pakietu, ale wyszukuje ścieżkę do miejsca docelowego.
- Protokół ICMP (*Internet Control Message Protocol*), który zapewnia funkcje kontrolne i informacyjne.
- Protokół ARP (*Address Resolution Protocol*), który znajduje adres warstwy łącza danych MAC dla znanego adresu IP.
- Protokół RARP (*Reverse Address Resolution Protocol*), który znajduje adres IP dla znanego adresu MAC.

Protokół IP spełnia następujące zadania:

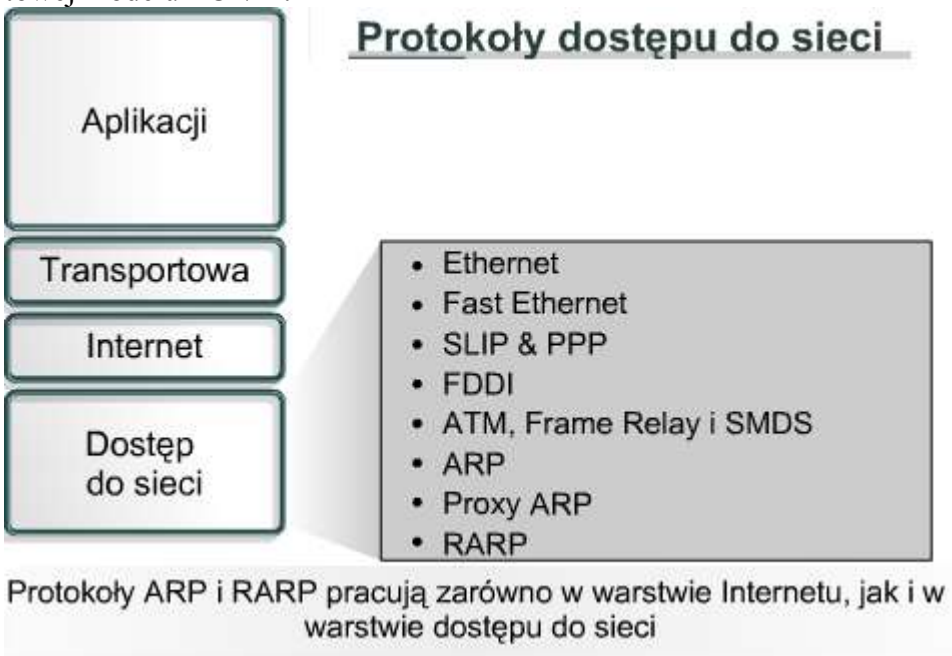
- definiuje format pakietu i schemat adresowania,
- przesyła dane pomiędzy warstwą internetową i warstwą dostępu do sieci,
- kieruje pakiety do zdalnych hostów.

Protokół IP jest czasem nazywany protokołem zawodnym. Nie oznacza to jednak, że protokół IP nie dostarcza poprawnie danych poprzez sieć. Jego „zawodność" polega po prostu na tym, że protokół IP nie wykrywa i nie koryguje błędów. Te funkcje są wykonywane przez protokoły z wyższych warstw, transportowej lub aplikacji.

9.1.5 Warstwa dostępu do sieci

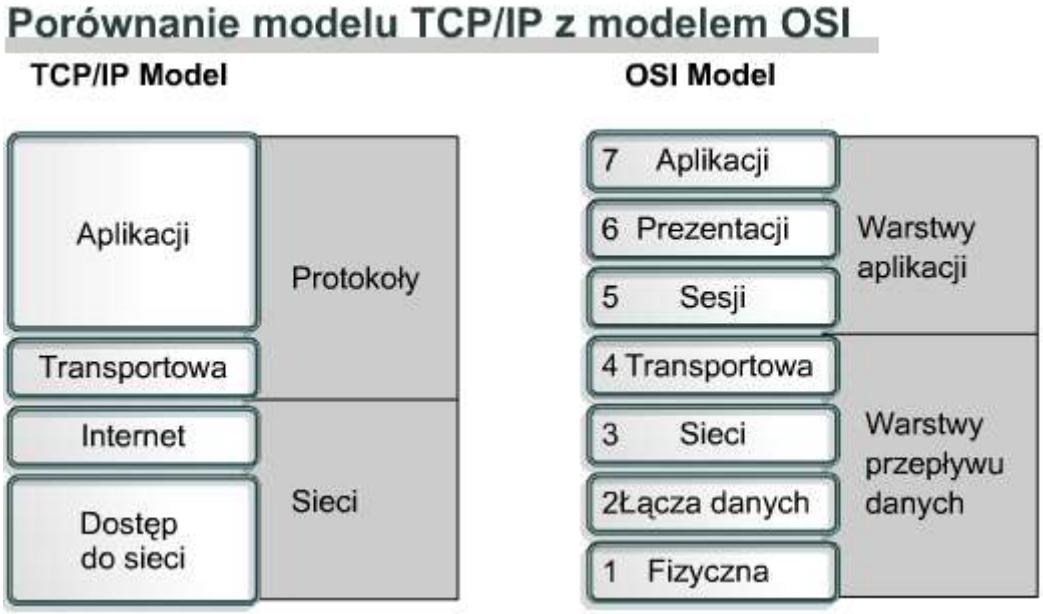
Warstwa dostępu do sieci jest także nazywana warstwą interfejsu sieciowego. Warstwa dostępu do sieci jest odpowiedzialna za wszystkie zagadnienia związane z tworzeniem łącza fizycznego służącego do przekazywania pakietu IP do medium sieciowego. Obejmuje ona szczegółowe rozwiązania dotyczące technologii sieciowych LAN i WAN, łącznie ze szczegółami dotyczącymi warstwy fizycznej i warstwy łącza danych modelu OSI. Sterowniki aplikacji, modemów i innych urządzeń działają na poziomie warstwy dostępu do sieci. Warstwa dostępu do sieci definiuje funkcje umożliwiające korzystanie ze sprzętu sieciowego i dostęp do medium transmisyjnego. Standardowe protokoły modemowe, takie jak SLIP (*Serial Line Internet Protocol*) i PPP (*Point-to-Point Protocol*), umożliwiają dostęp do sieci za pośrednictwem połączenia modemowego. Ponieważ zależności pomiędzy specyfikacjami sprzętu, oprogramowania i medium transmisyjnego są skomplikowane, w warstwie tej działa wiele protokołów. Może to powodować zamieszanie wśród użytkowników. Większość znanych protokołów działa w warstwie internetowej i transportowej modelu TCP/IP.

Warstwa dostępu do sieci odpowiada między innymi za odwzorowywanie adresów IP na adresy sprzętowe i enkapsulację pakietów IP w ramki. Warstwa dostępu do sieci definiuje połączenie z fizycznym medium sieci w zależności od rodzaju sprzętu i interfejsu sieciowego.



Dobrym przykładem konfigurowania warstwy dostępu do sieci jest konfigurowanie systemu Windows po włożeniu do komputera karty sieciowej. W zależności od wersji systemu Windows karta sieciowa może zostać automatycznie wykryta przez system operacyjny, po czym zostaną zainstalowane odpowiednie sterowniki. W starszej wersji systemu Windows użytkownik sam musiałby określić sterownik karty sieciowej. Producent karty dostarcza takich sterowników na dyskietkach lub dyskach CD-ROM.

9.1.6 Porównanie modelu OSI z modelem TCP/IP



Powyżej przedstawiono porównanie modelu OSI z modelem TCP/IP z uwzględnieniem podobieństw i różnic:

Podobieństwa modeli OSI i TCP/IP:

- Oba modele składają się z warstw.
- Oba modele mają warstwy aplikacji, chociaż świadczą one bardzo różne usługi.
- Oba mają porównywalne warstwy sieciowe i transportowe.
- W oby wypadkach zakładane jest wykorzystanie techniki przełączania pakietów, a nie komutacji łączy.
- Specjaliści w dziedzinie sieci powinni znać oba te modele.

Różnice pomiędzy modelem OSI i TCP/IP:

- W modelu TCP/IP zadania warstwy prezentacji i sesji są realizowane przez warstwę aplikacji.
- W modelu TCP/IP jedna warstwa pełni rolę warstw łącza danych i fizycznej modelu OSI.
- Model TCP/IP wydaje się prostszy ze względu na mniejszą liczbę warstw.
- Jeżeli w warstwie transportowej modelu TCP/IP używany jest protokół UDP, nie ma gwarancji pewnego dostarczenia pakietów, co gwarantuje warstwa transportowa modelu OSI.

Internet powstał opierając się na standardach protokołów TCP/IP. Model TCP/IP zyskuje na znaczeniu właśnie dzięki swoim protokołom. Z drugiej strony, zwykle nie buduje się sieci na podstawie modelu OSI. Model OSI jest natomiast używany do wyjaśniania procesu komunikacji.

9.1.7 Architektura Internetu

Chociaż struktura Internetu jest złożona, jego działanie opiera się na kilku prostych zasadach. W tej sekcji przyjrzymy się podstawowej architekturze Internetu. Internet jest oparty na pozornie prostym pomyśle, który powtórzony na dużą skalę umożliwia prawie natychmiastowe przesyłanie w dowolnym momencie danych między dowolnymi klientami sieci.

Sieci LAN są mniejszymi sieciami, obejmującymi ograniczony obszar geograficzny. Połączenie wielu sieci LAN pozwala na funkcjonowanie Internetu. Sieci LAN mają jednak ograniczoną wielkość. Odległość nadal stanowi przeszkodę, chociaż opracowano nowe techniki zwiększające szybkość transmisji, takie jak Gigabit, 10 Gigabit Ethernet lub Metro Optical.

Jednym ze sposobów zapoznania się z architekturą Internetu jest skupienie się na komunikacji w warstwie aplikacji pomiędzy komputerem źródłowym, docelowym i komputerami pośredniczącymi w tej wymianie informacji. Umieszczenie identycznych egzemplarzy aplikacji na wszystkich komputerach w sieci mogłoby uprościć dostarczanie wiadomości w dużej sieci. Jednak takie rozwiązanie nie skaluje się dobrze. Aby nowe oprogramowanie poprawnie działało, trzeba by zainstalować nowe aplikacje na każdym komputerze w sieci. Aby poprawnie działał nowy sprzęt, trzeba by zmodyfikować oprogramowanie. Każda awaria komputera pośredniczącego lub działającej na nim aplikacji spowodowałaby przerwanie łańcucha wymienianych komunikatów.

Internet został oparty na zasadzie połączeń pomiędzy warstwami sieci. Używając jako przykładu modelu OSI można powiedzieć, że celem jest utworzenie niezależnych modułów realizujących poszczególne funkcje sieci. Pozwala to na zróżnicowanie technik wykorzystywanych w sieciach LAN w warstwach 1 i 2 oraz aplikacji działających w warstwach 5, 6 i 7. Model OSI umożliwia odseparowanie szczegółów dotyczących wyższych i niższych warstw. To z kolei umożliwia pośredniczącym urządzeniom sieciowym przekazywanie ruchu bez zajmowania się szczegółami dotyczącymi sieci LAN.

Prowadzi to do koncepcji intersieci, czyli budowania sieci z innych sieci. Sieć złożona z innych sieci jest nazywana internetem (intersiecią), przy czym wyraz ten jest pisany małą literą. Gdy mówimy o sieciach, które powstały z sieci Departamentu Obrony USA, na bazie których działa światowa sieć WWW, używamy pojęcia Internet, pisanego dużą literą. Intersieci muszą się skalować odpowiednio do liczby sieci i przyłączonych komputerów. Muszą one także umożliwiać przenoszenie danych na ogromne odległości. Muszą być na tyle elastyczne, aby uwzględniać ciągłe udoskonalenia techniczne. Jak również muszą być w stanie dostosować się do dynamicznych warunków panujących w sieci. Intersieci powinny być również tanie w utrzymaniu. Poza tym muszą być tak zaprojektowane, aby umożliwiać transmisję danych do dowolnego miejsca o dowolnym czasie.

Na rysunku obok pokazano połączenie dwóch sieci fizycznych poprzez specjalizowany komputer zwany routerem. Sieci te określa się jako bezpośrednio podłączone do routera. Router jest potrzebny do podejmowania wszystkich wymaganych do komunikacji między tymi sieciami decyzji o wyborze tras. Do obsługi dużego ruchu sieciowego potrzebna jest duża liczba routerów.

Na rysunku obok rozszerzono poprzedni schemat do trzech sieci fizycznych połączonych dwoma routerami. Routery podejmują złożone decyzje, które pozwalają wszystkim użytkownikom we wszystkich sieciach na komunikowanie się pomiędzy sobą. Nie wszystkie sieci są ze sobą bezpośrednio połączone. Router musi umieć radzić sobie z taką sytuacją.

Jedną z możliwości jest przechowywanie przez router listy wszystkich komputerów i wszystkich ścieżek do nich. Na tej podstawie router mógłby decydować, w jaki sposób przekazywać pakiety danych. Przekazywanie opiera się na adresie IP komputera docelowego. Takie rozwiązanie stałoby się niewygodne, gdyby wzrosła liczba użytkowników. Lepiej skaluje się rozwiązanie, w którym router przechowuje listę wszystkich sieci, ale pozostawia lokalne dostarczenie pakietów lokalnej sieci fizycznej. W tej sytuacji routery przekazują innym routerom komunikaty. Każdy router dzieli się informacjami o tym, do jakich sieci jest przyłączony. Dzięki tym informacjom tworzona jest tablica routingu.

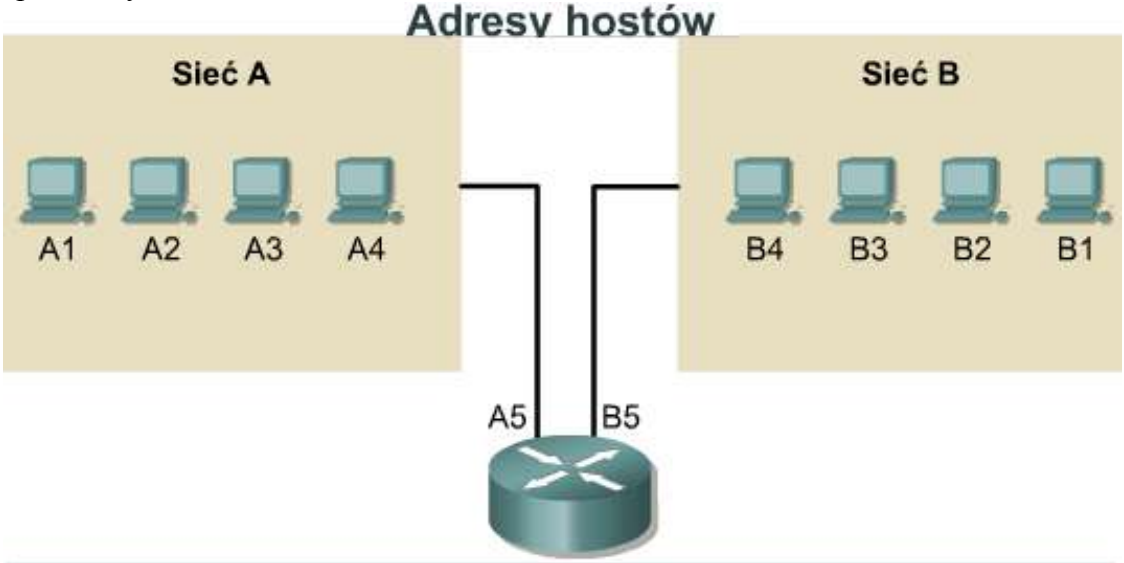
Wymagane przez użytkowników jest ukrycie szczegółów. Jednak fizyczna i logiczna struktura chmury Internetu może być bardzo złożona. Internet gwałtownie rozrósł się, aby mogło z niego korzystać coraz więcej użytkowników. Fakt, że Internet powiększył się na tyle, że zawiera ponad 90 000 routerów szkieletowych oraz 300 000 000 użytkowników końcowych, świadczy o tym, że jego architektura jest oparta na solidnych podstawach.

Dwa komputery znajdujące się w dowolnych miejscach na świecie mogą komunikować się bez problemów, jeżeli tylko spełniają pewne specyfikacje dotyczące sprzętu, oprogramowania i protokołów. Standaryzacja sposobów i procedur przesyłania danych pomiędzy sieciami umożliwiła utworzenie Internetu.

9.2. Adresy internetowe

9.2.1 Adresowanie IP

Aby dwa systemy mogły się komunikować, muszą mieć możliwość zidentyfikowania i odnalezienia siebie nawzajem. Chociaż adresy przedstawione **na rysunku** nie są prawdziwymi adresami sieciowymi, ilustrują jednak pojęcie grupowania adresów.

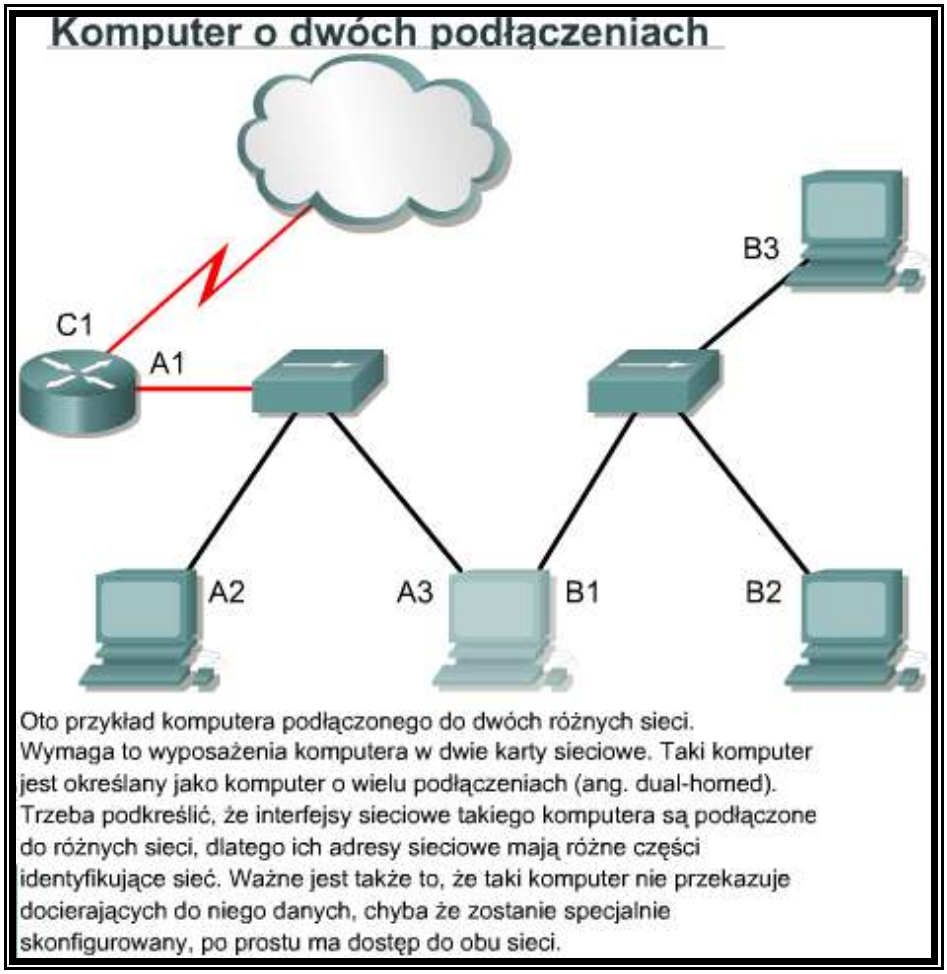


Chociaż podane adresy nie są prawdziwe, jednak obrazują ideę grupowania adresów. Litery A i B oznaczają tutaj sieć, a kolejne liczby identyfikują poszczególne hosty. Połączenie litery (adresu sieci) i liczby (adresu hosta) tworzy unikatowy adres każdego urządzenia w sieci.

Komputer może być przyłączony do więcej niż jednej sieci. W takiej sytuacji komputerowi musi zostać przypisany więcej niż jeden adres. Każdy z tych adresów identyfikuje wtedy połączenie komputera z inną siecią. Nie mówi się, że urządzenie ma adres, ale że każdy punkt przyłączenia, czyli interfejs urządzenia, ma adres w danej sieci. Pozwala to innym komputerom zlokalizować takie urządzenie w odpowiedniej sieci. Połączenie litery (adresu sieci) i liczby (adresu hosta) tworzy unikatowy adres każdego urządzenia w sieci.

Każdemu komputerowi w sieci TCP/IP trzeba przypisać unikatowy identyfikator, czyli adres IP. Adres ten należy do warstwy 3 i pozwala jednemu komputerowi w sieci zlokalizować inny. Wszystkie komputery mają także

unikatowy adres fizyczny zwany adresem MAC. Adresy te są nadawane przez producentów kart sieciowych i należą do warstwy 2 modelu OSI.
Adres IP jest 32-bitową sekwencją zer i jedynek. **Na rysunku** pokazano przykładową liczbę 32-bitową. W celu ułatwienia korzystania z adresów IP zwykle zapisuje się je w postaci czterech liczb dziesiętnych oddzielonych kropkami. Na przykład adres IP pewnego komputera może być równy 192.168.1.2. Inny komputer może mieć adres 128.10.2.1. Ten sposób zapisywania adresów jest nazywany notacją dziesiętną kropkową. W tej notacji każdy adres IP jest zapisywany w czterech częściach oddzielonych kropkami. Każda część adresu jest nazywana oktetem, ponieważ składa się z ośmiu cyfr w systemie dwójkowym. Na przykład adres IP 192.168.1.8 zapisany w systemie dwójkowym ma postać



11000000.10101000.00000001.00001000. Notacja dziesiętna kropkowa jest łatwiejsza do zrozumienia w porównaniu do zapisu dwójkowego. Pomaga ona uniknąć wielu pomyłek, które powstałyby w wypadku użycia jedynie liczb dwójkowych.
Używając notacji kropkowej, łatwiej dostrzec wzory, w jakie układają się liczby. Przedstawione na rysunku liczby w zapisie dwójkowym i dziesiętnym kropkowym reprezentują te same wartości, ale łatwiej porównywać wartości zapisane w notacji dziesiętnej. Jest to jeden z głównych problemów przy bezpośredniej pracy z liczbami dwójkowymi. Długie ciągi powtarzanych jedynek i zer powodują, że łatwiej o pominięcie lub zamianę cyfr. Pomiędzy adresami 192.168.1.8 i 192.168.1.9 łatwo można zauważyć związek, ale jest on już mniej widoczny w wypadku adresów 11000000.10101000.00000001.00001000 i 11000000.10101000.00000001.00001001. Patrząc na zapis w systemie dwójkowym, trudno jest zauważyć, że są to kolejne liczby.

Wartości dwójkowe i dziesiętne

Dwójkowo: 11000000.10101000.00000001.00001000 oraz 11000000.10101000.00000001.00001001

Dziesiętnie: 192.168.1.8 oraz 192.168.1.9

Zarówno liczby dwójkowe, jak i dziesiętne odpowiadają tym samym wartościom. Znacznie łatwiej jest nam jednak posługiwać się liczbami dziesiętnymi rozdzielonymi kropkami. Jest to jeden z często spotykanych problemów przy bezpośredniej pracy z liczbami dwójkowymi. W długich łańcuchach powtarzających się zer i jedynek bardziej prawdopodobne jest przestawienie lub pominięcie cyfr.

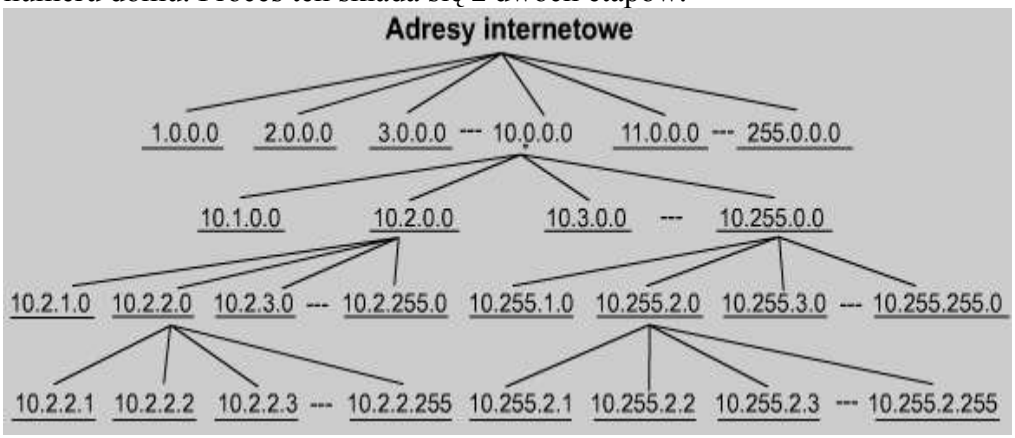
9.2.2 Zamiana liczb dziesiętnych i dwójkowych

Każdy problem można rozwiązać na wiele sposobów. Również w wypadku zamiany liczb dziesiętnych na dwójkowe istnieje szereg różnych metod. Poniżej przedstawiono jedną z nich, nie jest to jednak metoda jedyna. Uczestnik kursu może uznać inne metody za prostsze. Jest to kwestia osobistych upodobań.
Przy zamianie liczby dziesiętnej na dwójkową trzeba znaleźć taką największą potęgę dwójki, która mieści się w liczbie dziesiętnej. Jeżeli proces zamiany dotyczy komputerów, najlepiej rozpocząć od największych wartości, które mieszczą się w jednym lub dwóch bajtach. Jak już wcześniej wspomniano, najczęściej bity grupuje się po osiem i taka grupa tworzy jeden bajt. Jednak czasami największa liczba możliwa do zapisania przy użyciu jednego bajtu jest zbyt mała w stosunku do potrzebnej wartości. W tym celu łączy się bajty. Zamiast dwóch liczb ośmiobitowych tworzy się jedną liczbę 16-bitową. Zamiast trzech liczb ośmiobitowych — jedną 24-bitową. Obowiązują wtedy takie same reguły, jak dla liczb 8-bitowych. Aby uzyskać wartość w danej kolumnie, należy pomnożyć przez dwa wartość z kolumny poprzedniej.

Ponieważ przy pracy z komputerami najczęściej korzysta się z bajtów, najlepiej rozpocząć obliczenia od granic bajtów. Zacznijmy od kilku przykładów. Najpierw zamieńmy liczbę 6783. Ponieważ liczba ta jest większa od 255, największej wartości mieszczącej się w jednym bajcie, będziemy używać dwóch bajtów. Zaczynamy więc liczenie od 2^{15}. Liczba 6783 zapisana w systemie dwójkowym jest równa 00011010 01111111.
Drugim przykładem jest liczba 104. Ponieważ jest ona mniejsza niż 255, będziemy ją przedstawiać za pomocą jednego bajta. Dwójkowym odpowiednikiem liczby 104 jest liczba 01101000.
Metoda ta jest skuteczna w wypadku dowolnej liczby dziesiętnej. Rozważmy liczbę dziesiętną równą milion. Ponieważ milion jest większy niż największa wartość mieszcząca się w dwóch bajtach (liczba 65 535), trzeba użyć przynajmniej trzech bajtów. Mnożąc kolejne wartości przez dwa, otrzymujemy dla 24 bitów, czyli trzech bajtów, wartość 16 777 215. Oznacza to, że największa wartość mieszcząca się w trzech bajtach to 16 777 215. Tak więc rozpoczynamy liczenie od 24-go bitu i kontynuujemy aż do osiągnięcia zera. Wykonując opisaną wcześniej procedurę, możemy stwierdzić, że liczbie dziesiętnej jeden milion odpowiada liczba dwójkowa 00001111 01000010 01000000.
Zamiana liczb dwójkowych na dziesiętne jest procesem odwrotnym. Wystarczy po prostu umieścić liczbę dwójkową w tabeli; jeżeli w danej kolumnie występuje cyfra jeden, należy dodać odpowiadającą jej wartość do wyniku. Zamieńmy liczbę 00000100 00011101 na wartość dziesiętną. Wynikiem jest liczba 1053.

9.2.3 Adresowanie IPv4

Do przekazywania pakietów z sieci źródłowej do sieci docelowej router używa protokołu IP. Pakiety muszą zawierać zarówno identyfikator sieci źródłowej, jak i docelowej. Używając adresu IP sieci docelowej, router może dostarczyć pakiet do odpowiedniej sieci. Gdy pakiet przybywa do routera połączonego z siecią docelową, router ten używa adresu IP do zlokalizowania konkretnego komputera w tej sieci. System ten działa podobnie do poczty. Przy przesyłaniu listu należy najpierw na podstawie kodu dostarczyć go do urzędu pocztowego w mieście docelowym. Ten urząd pocztowy musi odnaleźć punkt docelowy w danym mieście na podstawie nazwy ulicy i numeru domu. Proces ten składa się z dwóch etapów.



Podobnie każdy adres IP składa się z dwóch części. Jedna część identyfikuje sieć, do której komputer jest przyłączony, a druga identyfikuje ten komputer w sieci docelowej. **Jak pokazano na rysunku** , każdy oktet może przedstawiać liczbę od 0 do 255. Każdy z oktetów wyznacza 256 grup, a każda z nich dzieli się na 256 podgrup, z których każda zawiera 256 adresów. Korzystając z adresu grupy znajdującej się bezpośrednio na wyższym poziomie hierarchii nad rozpatrywaną grupą, można opisywać wszystkie grupy, na które dzieli się ten adres, za pomocą pojedynczej jednostki.
Adres taki jest nazywany adresem hierarchicznym, ponieważ składa się z różnych poziomów. W adresie IP dwa identyfikatory połączone są w jedną liczbę. Liczba ta musi być unikatowa, bowiem w przeciwnym wypadku niemożliwy byłby routing pakietów. Pierwsza część identyfikuje adres sieci, w której znajduje się dany system. Druga część, zwana częścią hosta, identyfikuje pojedyncze urządzenie w tej sieci.
Adresy IP są podzielone na klasy, które definiują wielkie, średnie i małe sieci. Adresy klasy A są przypisywane sieciom wielkim. Adresy klasy B są przeznaczone dla sieci średnich, a klasy C — dla sieci małych. Przy określaniu, która część adresu identyfikuje sieć, a która hosta, pierwszym krokiem jest określenie klasy adresu IP.

Klasy adresów IP

Klasa adresu	Liczba sieci	Liczba hostów w sieci
A	126 *	16,777,216
B	16, 384	65,535
C	2,097,152	254
D (rozsyłanie grupowe)	nd.	nd.

* Zakres adresów 127.x.x.x jest zarezerwowany na adres pętli zwrotnej, który jest używany do testowania i celów diagnostycznych.

Rozpoznawanie klas adresów

Klasa adresu IP	Bity najbardziej znaczące	Zakres adresów pierwszego oktetu	Liczba bitów w adresie sieci
Klasa A	0	0 - 127 *	8
Klasa B	10	128 - 191	16
Klasa C	110	192 - 223	24
Klasa D	1110	224 - 239	28

* Zakres adresów 127.x.x.x jest zarezerwowany na adres pętli zwrotnej, który jest używany do testowania i celów diagnostycznych.

9.2.4 Adresy IP klas A, B, C, D i E

Aby dostosować się do potrzeb sieci o różnych rozmiarach oraz ułatwić ich klasyfikowanie, adresy IP zostały podzielone na grupy zwane klasami. Podział ten jest nazywany adresowaniem klasowym. Każdy pełny 32-bitowy adres IP można podzielić na część identyfikującą sieć i część identyfikującą hosta. Bit lub zestaw bitów na początku każdego adresu określa jego klasę. Istnieje pięć klas adresów IP, co pokazano na rysunku .

Adresy klasy A zostały przeznaczone dla wyjątkowo dużych sieci i mogą zawierać ponad 16 milionów adresów hostów. Adresy klasy A do identyfikacji sieci używają tylko pierwszego oktetu. Pozostałe trzy oktety stanowią adres hosta. Pierwszy bit adresu klasy A jest zawsze równy 0. W takim przypadku najmniejsza możliwa do przedstawienia liczba to 00000000, czyli 0 dziesiętnie, a największa to 01111111, czyli 127 dziesiętnie. Liczby 0 i 127 są zarezerwowane i nie można ich używać jako adresów sieci. Każdy adres, którego pierwszy oktet ma wartość z przedziału od 1 do 126, jest adresem klasy A. Adres sieciowy 127.0.0.0 jest zarezerwowany na potrzeby testowania pętli zwrotnej.

Przedrostki klas adresów

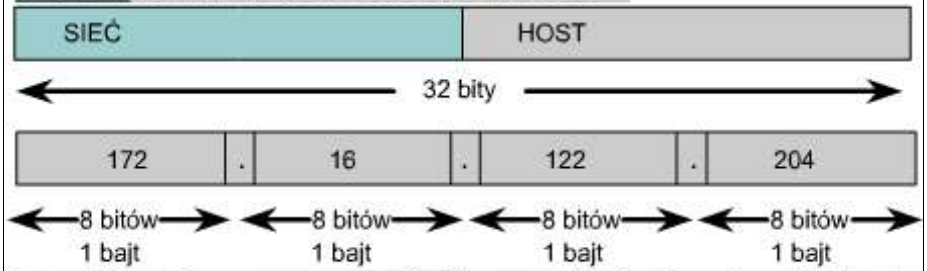
Klasa A	Sieć	Host		
Octet	1	2	3	4
Klasa B	**Sieć**		**Host**	
Octet	1	2	3	4
Klasa C	**Sieć**			**Host**
Octet	1	2	3	4
Klasa D	**Host**			
Octet	1	2	3	4

Adresy klasy D są używane przez grupy przy rozsyłaniu grupowym. Nie trzeba przydzielać oktetów lub bitów w celu rozdzielenia adresu sieci i hosta. Adresy klasy E są zarezerwowane do badań.

Routery lub inne urządzenia mogą używać tego adresu do wysyłania pakietów do samych siebie. Tak więc liczby tej nie można przypisać żadnej sieci.

Adresy klasy B zostały przeznaczone na potrzeby sieci średnich i dużych. Adres IP klasy B do identyfikacji sieci używa pierwszych dwóch z czterech oktetów. Pozostałe dwa oktety określają adres hosta.

Podział na adres sieci i hosta



Adres IP można zawsze podzielić na część sieciową i część hosta. W schemacie adresowania klasowego podział ten przebiega zawsze na granicy pełnych oktetów.

Pierwsze dwa bity pierwszego oktetu adresu klasy B są zawsze równe 10. Pozostałe sześć bitów może zawierać jedynki lub zera. Tak więc najmniejszą liczbą, która może reprezentować adres klasy B, jest 10000000, czyli 128 dziesiętnie, a największą — 10111111, czyli 191 dziesiętnie. Każdy adres, którego pierwszy oktet ma wartość z przedziału od 128 do 191, jest adresem klasy B.

Spośród wszystkich klas adresów najczęściej wykorzystywana jest klasa C. Ta przestrzeń adresowa została przeznaczona dla małych sieci, zawierających maksymalnie 254 hosty.

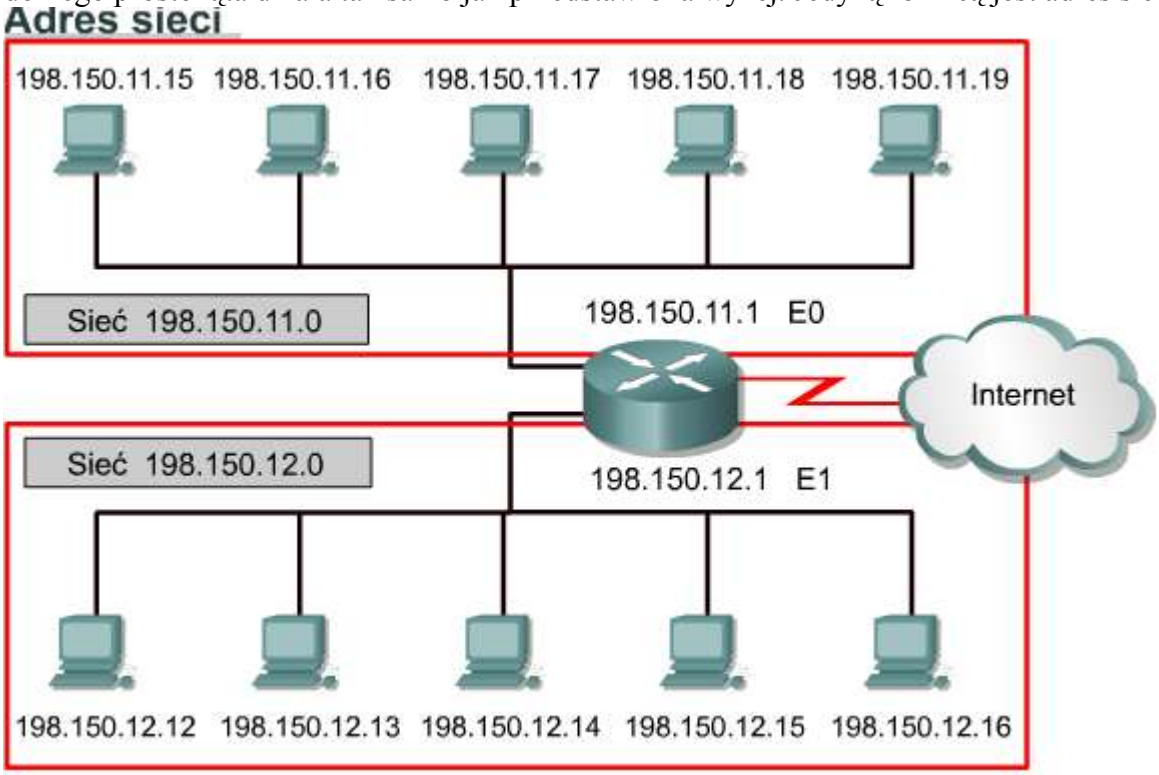
Adres klasy C zaczyna się od dwójkowej wartości 110. Tak więc najmniejszą możliwą do przedstawienia liczbą jest 11000000, czyli 192 dziesiętnie, a największą — 11011111, czyli 223 dziesiętnie. Adres zawierający w pierwszym oktecie wartość z przedziału od 192 do 223 jest adresem klasy C.

Klasa D została utworzona w celu umożliwienia rozsyłania grupowego przy użyciu adresów IP. Adres rozsyłania grupowego jest unikatowym adresem sieciowym, który kieruje pakiety o tym adresie docelowym do

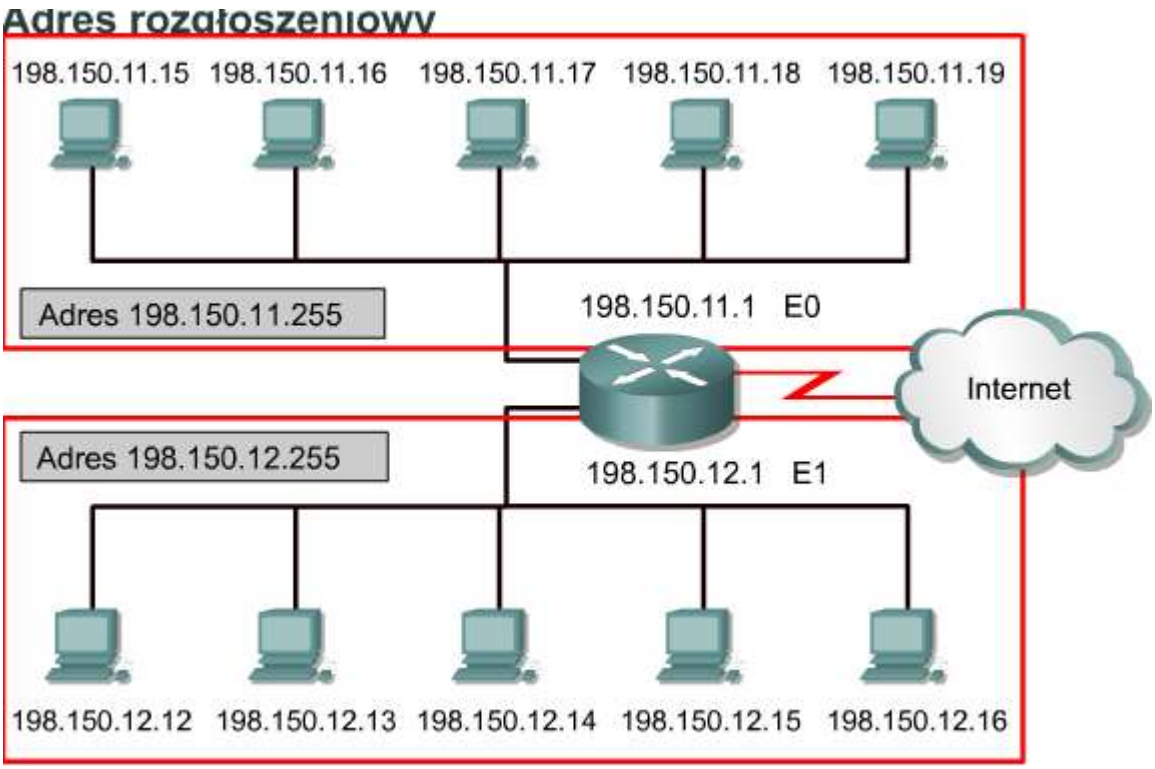
zdefiniowanej wcześniej grupy adresów IP. Dzięki temu pojedynczy komputer może przesyłać jeden strumień danych równocześnie do wielu odbiorców.
Przestrzeń adresowa klasy D, podobnie jak pozostałe przestrzenie adresowe, jest matematycznie ograniczona. Pierwsze cztery bity adresu klasy D muszą być równe 1110. Tak więc w przypadku adresów klasy D wartość pierwszego oktetu należy do zakresu od 11100000 do 11101111, czyli od 224 do 239 dziesiętnie. Adres IP zawierający w pierwszym oktecie wartości z przedziału od 224 do 239 jest adresem klasy D.
Zdefiniowano także klasę E adresów IP. Adresy te zostały jednak zarezerwowane przez Internet Engineering Task Force (IETF) na potrzeby badawcze. Tak więc nie oddano do publicznego użytku żadnych adresów klasy E. Pierwsze cztery bity każdego adresu klasy E mają zawsze wartość 1. Tak więc pierwszy oktet dla adresów klasy E może przyjmować wartości od 11110000 do 11111111, czyli od 240 do 255 dziesiętnie.

9.2.5 Zarezerwowane adresy IP

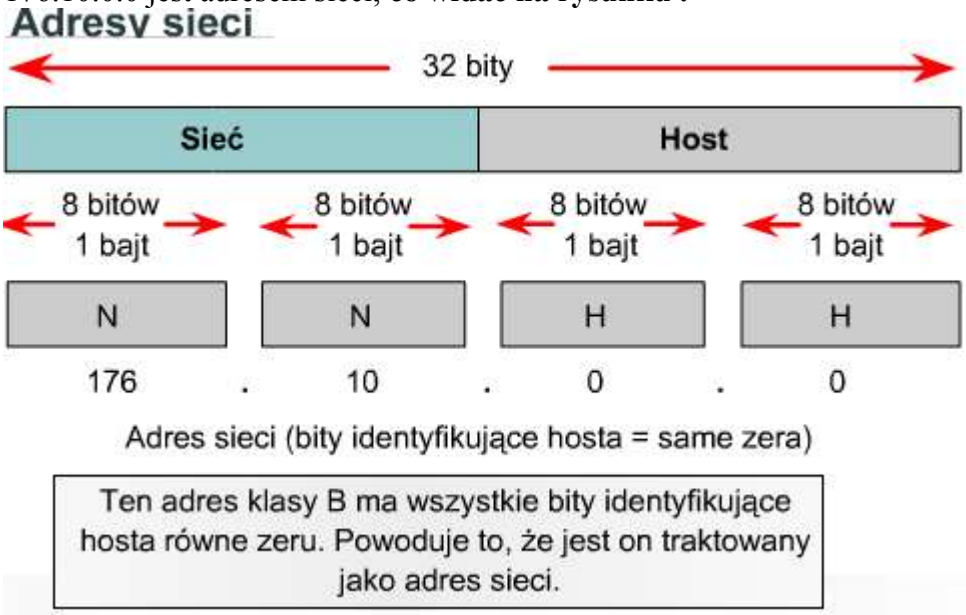
Niektóre adresy hostów są zarezerwowane i nie można ich przypisać urządzeniom w sieci. Te zarezerwowane adresy hostów to:
Adres sieci: używany do identyfikowania samej sieci.
Na rysunku górny obszar zaznaczony prostokątem reprezentuje sieć 198.150.11.0. Dane wysłane spoza tej sieci do dowolnego należącego do niej hosta (198.150.11.1–198.150.11.254) będą w istocie wysyłane na adres sieci (198.159.11.0). Numery hostów mają znaczenie tylko wtedy, gdy dane przesyłane są w sieci lokalnej. Sieć LAN z dolnego prostokąta działa tak samo jak przedstawiona wyżej. Jedyną różnicą jest adres sieci równy 198.150.12.0.



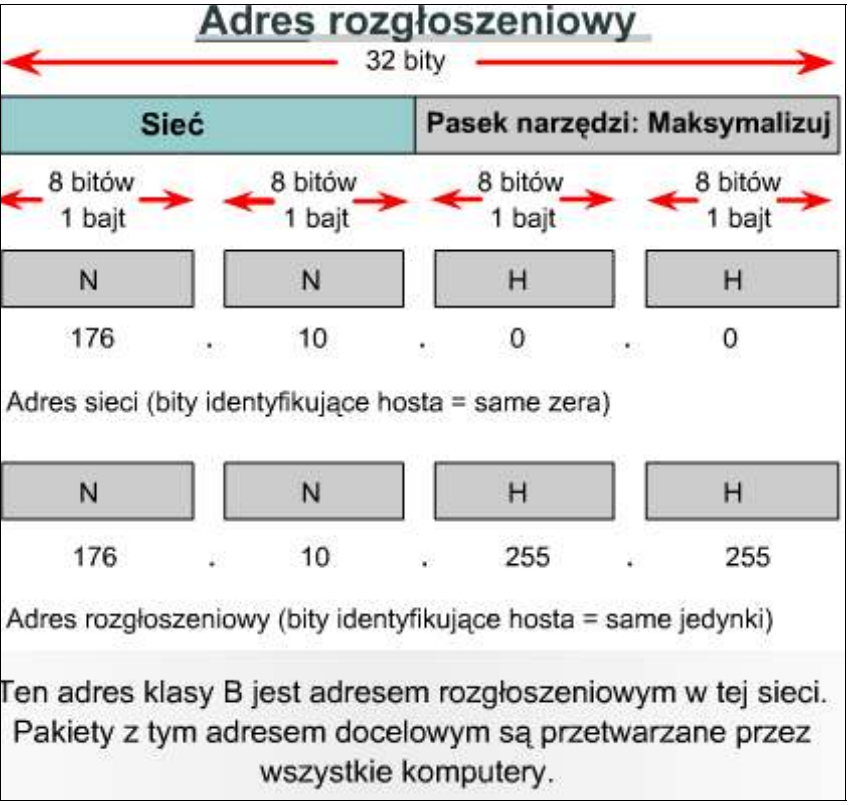
Adres rozgłoszeniowy: używany do rozsyłania pakietów do wszystkich urządzeń w sieci.
Na rysunku górny obszar zaznaczony prostokątem reprezentuje adres rozgłoszeniowy 198.150.11.255. Dane wysyłane na ten adres dotrą do wszystkich komputerów w danej sieci (198.150.11.1–198.150.11.254). Sieć LAN z dolnego prostokąta działa tak samo jak przedstawiona wyżej. Jedyną różnicą jest adres rozgłoszeniowy równy 198.150.12.255.



Adres IP, którego część identyfikująca hosta zawiera same zera, jest zarezerwowany jako adres sieci. W przykładowej sieci klasy A adres 113.0.0.0 jest adresem IP sieci (identyfikatorem sieci), która zawiera host 113.1.2.3. Router używa adresu IP sieci do przesyłania danych w Internecie. W przykładowej sieci klasy B adres 176.10.0.0 jest adresem sieci, **co widać na rysunku .**

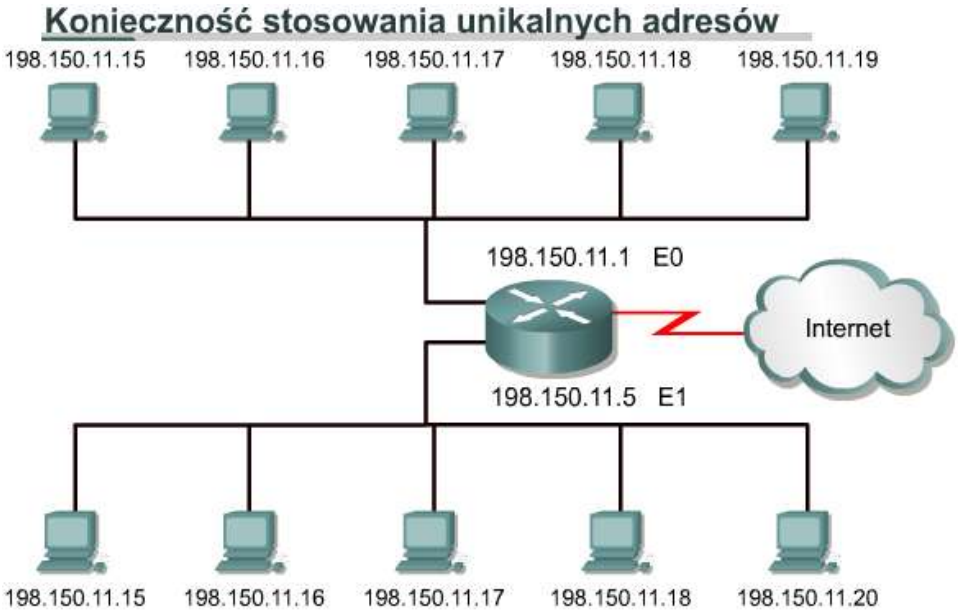


W adresie sieciowym klasy B pierwsze dwa oktety są przeznaczone na część identyfikującą sieć. Pozostałe dwa oktety (czyli 16 bitów) zawierają zera, ponieważ są przeznaczone na część identyfikującą hosta i są używane do identyfikacji urządzeń przyłączonych do sieci. Na przykład adres IP 176.10.0.0 jest adresem sieci. Adres taki nigdy nie zostanie przypisany jako adres hosta. Adresem hosta w sieci 176.10.0.0 mógłby być adres 176.10.16.1. W tym przykładzie „176.10" to część identyfikująca sieć, a „16.1" — hosta.



Aby wysłać dane do wszystkich urządzeń w sieci, potrzebny jest adres rozgłoszeniowy. Rozgłaszanie to rozsyłanie danych do wszystkich urządzeń w sieci. Aby zagwarantować przetworzenie rozgłaszanych danych przez wszystkie urządzenia w sieci, komputer wysyłający musi użyć takiego adresu docelowego, który zostanie rozpoznany i przetworzony. Adresy rozgłoszeniowe mają część identyfikującą hosta wypełnioną jedynkami (przy zapisie adresu w systemie dwójkowym). W przykładowej sieci 176.10.0.0 ostatnie 16 bitów stanowi pole hosta, czyli część identyfikującą go. Pakiet rozgłoszeniowy wysyłany do wszystkich urządzeń w tej sieci zawierałby adres docelowy 176.10.255.255. Liczba 255 pojawia się dlatego, że jest to wartość oktetu zawierającego liczbę dwójkową 11111111.

9.2.6 Publiczne i prywatne adresy IP



Stabilność działania Internetu zależy bezpośrednio od niepowtarzalności używanych publicznie adresów sieciowych. **Na rysunku przedstawiono problem związany ze schematem adresowania sieci**. Widać, że obydwie sieci mają adres 198.150.11.0. W tej sytuacji router nie byłby w stanie prawidłowo przekazywać pakietów danych. Podwojone adresy sieciowe IP uniemożliwiają routerowi wykonywanie zadania, którym jest wybieranie najlepszej ścieżki. Każde urządzenie w sieci wymaga unikatowego adresu.
Konieczne było opracowanie procedury zapewniającej rzeczywistą unikatowość adresów. Początkowo zajmowała się tym organizacja Internet Network Information Center (InterNIC). Organizacja InterNIC już nie istnieje, a jej miejsce zajęła organizacja Internet Assigned Numbers Authority (IANA). IANA ostrożnie rozporządza pozostałą pulą adresów IP, aby nie wystąpiło powielenie publicznie używanych adresów. Sytuacja taka spowodowałaby niestabilność Internetu oraz utrudniłaby dostarczanie datagramów do sieci.
Publiczne adresy IP są unikatowe. Żadne dwa komputery połączone z publiczną siecią nie mogą mieć takich samych adresów IP, ponieważ publiczne adresy IP są globalne i zestandaryzowane. Wszystkie urządzenia podłączone do Internetu stosują się do tego systemu. Publiczny adres IP można otrzymać za pewną opłatą od dostawcy usług internetowych (ISP) lub z rejestru odpowiedniego dla danego regionu.
W związku z gwałtownym rozwojem Internetu publiczne adresy IP zaczęły się wyczerpywać. Aby rozwiązać ten problem, opracowano nowe systemy adresowania, takie jak bezklasowy routing międzydomenowy CIDR (classless interdomain routing) i IPv6. Systemy CIDR i IPv6 zostaną omówione w dalszej części kursu.
Innym rozwiązaniem problemu zbliżającego się wyczerpania publicznych adresów IP jest korzystanie z adresów prywatnych. Jak już wspomniano, w sieciach publicznych hosty muszą mieć unikatowe adresy IP. Jednak prywatne, nie podłączone do Internetu sieci mogą używać dowolnych adresów hostów, jeśli tylko adresy te są unikatowe wewnątrz sieci prywatnej. Obok sieci publicznych istnieje wiele sieci prywatnych. Nie zaleca się jednak używania w prywatnej sieci dowolnych adresów, ponieważ kiedyś sieć taka może zostać podłączona do Internetu. W dokumencie RFC 1918 zarezerwowano trzy bloki adresów IP do prywatnego, wewnętrznego użytku.

Te trzy bloki to jedna klasa A, zakres adresów klasy B oraz zakres adresów klasy C. Adresy należące do tych zakresów nie są routowane w sieci szkieletowej Internetu. Routery internetowe natychmiast odrzucają adresy prywatne. Przypisując adresy w niepublicznym intranecie, sieci testowej lub domowej, można używać tych adresów zamiast adresów globalnie unikatowych. Podłączenie do Internetu sieci używającej adresów prywatnych wymaga translacji adresów prywatnych na adresy publiczne. Proces translacji jest określany jako translacja adresów sieciowych NAT (*Network Address Translation*). Zwykle proces translacji NAT jest wykonywany przez router. Technika NAT, razem z technikami CIDR i IPv6, zostanie szczegółowo opisana w dalszej części materiałów szkoleniowych.

9.2.7 Wprowadzenie do podziału na podsieci

Podział na podsieci jest kolejną metodą zarządzania adresami IP. Sieć 131.108.0.0 została podzielona na podsieci: 131.108.1.0, 131.108.2.0 i 131.108.3.0. Dodatkowo metoda ta zapobiegła całkowitemu wyczerpaniu adresów IP. Opis sieci TCP/IP byłby niekompletny bez przedstawienia podziału na podsieci. Dla administratora systemu podział na podsieci jest sposobem na wydzielenie i zaadresowanie oddzielnych części sieci LAN. Małą sieć nie zawsze trzeba dzielić na podsieci. Jest to jednak konieczne w przypadku dużych lub bardzo dużych sieci. Podział na podsieci oznacza wykorzystanie maski podsieci do podzielenia sieci na mniejsze, bardziej efektywne i łatwiejsze w zarządzaniu segmenty, czyli podsieci. Można to porównać do systemu numeracji telefonicznej, który składa się z numerów regionów, central i numerów lokalnych.

Administrator musi rozwiązać te problemy przy tworzeniu i rozszerzaniu sieci. Ważne jest, aby wiedzieć, ile jest potrzebnych podsieci lub sieci, oraz ile hostów będzie potrzebnych w każdej z nich. Jeśli korzystamy z podziału na podsieci, nie musimy ograniczać się do domyślnych masek sieci klasy A, B lub C, dzięki czemu możliwe jest bardziej elastyczne projektowanie sieci.

Adresy podsieci zawierają część identyfikującą sieć oraz pole podsieci i pole hosta. Pole podsieci i pole hosta są tworzone z części przeznaczonej pierwotnie na adres hosta w całej sieci. Możliwość zdecydowania, w jaki sposób podzielić oryginalną część identyfikującą hosta na nowe pola podsieci i hosta, umożliwia administratorowi sieci elastyczny sposób adresowania. Aby utworzyć adres podsieci, administrator pożycza bity z pola hosta i przeznacza je na pole podsieci. Minimalna liczba pożyczanych bitów wynosi dwa. Gdyby tworząc podsieć, pożyczyć tylko jeden bit, numerem sieci byłaby sieć .0. Adresem rozgłoszeniowym byłaby wtedy sieć .255. Maksymalnie można pożyczyć dowolną liczbę bitów, jeżeli tylko pozostawi się przynajmniej dwa bity na numer hosta.

Podręczna tablica korzystania z podsieci

Pierwszy oktet numeru hosta w notacji dziesiętnej	Liczba podsieci	Liczba hostów klasy A w podsieci	Liczba hostów klasy B w podsieci	Liczba hostów klasy C w podsieci
.192	2	4,194,302	16,382	62
.224	6	2,097,150	8,190	30
.240	14	1,048,574	4,094	14
.248	30	524,286	2,046	6
.252	62	262,142	1,022	2
.254	126	131,070	510	-
.255	254	65,534	254	-

9.2.8 IPv4 kontra IPv6

Gdy w latach 80. zaczęto wprowadzać system TCP/IP, korzystał on z dwupoziomowego schematu adresowania. W tamtych czasach było to wystarczająco skalowalne rozwiązanie. Niestety, twórcy protokołów TCP/IP nie mogli przewidzieć, że ich dzieło stanowić będzie podstawę globalnej sieci wymiany informacji, handlu i rozrywki. W ciągu ostatnich dwudziestu lat protokół IP wersja 4 (IPv4) oferował strategię adresowania, która, choć skalowalna w owym czasie, powodowała nieefektywne przydzielanie adresów.

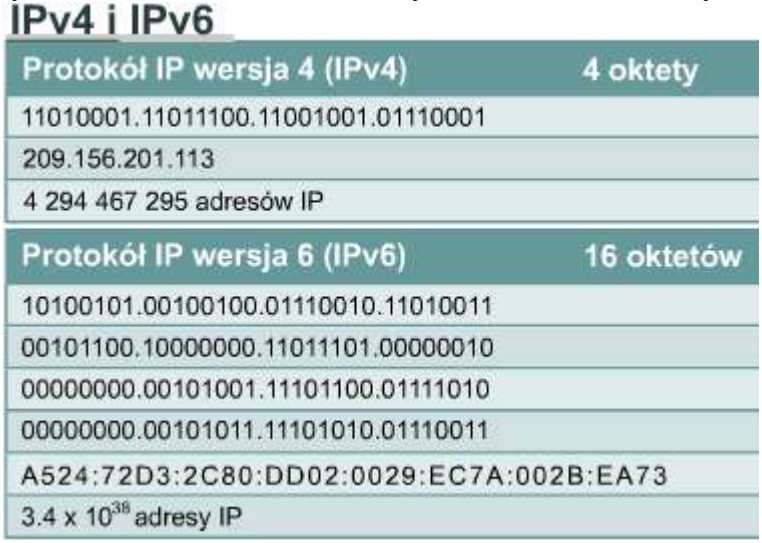
Adresy klas A i B stanowią 75 procent przestrzeni adresowej IPv4, jednak możne je przydzielić tylko mniej niż 17 000 organizacji. Adresów sieci klasy C jest znacznie więcej niż adresów klasy A lub B, jednak stanowią one jedynie 12,5 procent wszystkich możliwych czterech miliardów adresów IP.

Niestety, adresy klasy C są ograniczone do 254 hostów. Jest to zbyt mało, aby zaspokoić potrzeby większych organizacji, które nie mogą otrzymać adresu klasy A lub B. Nawet gdyby było więcej adresów klas A, B lub C, zbyt wiele adresów sieciowych spowodowałoby zatrzymanie pracy routerów w Internecie na skutek olbrzymich tablic routingu, wymaganych do przechowania ścieżek do każdej z sieci.

Już w roku 1992 organizacja Internet Engineering Task Force (IETF) określiła dwa następujące problemy:

- Wyczerpywanie pozostałych, nieprzypisanych jeszcze adresów sieciowych IPv4. W tym czasie przestrzeń adresowa klasy B była bliska wyczerpania.
- Gwałtowny wzrost rozmiarów tablic routingu w związku z coraz większą liczbą wchodzących do użycia sieci klasy C. Będący tego rezultatem zalew informacji o nowych sieciach groził uniemożliwieniem efektywnej pracy routerów internetowych;

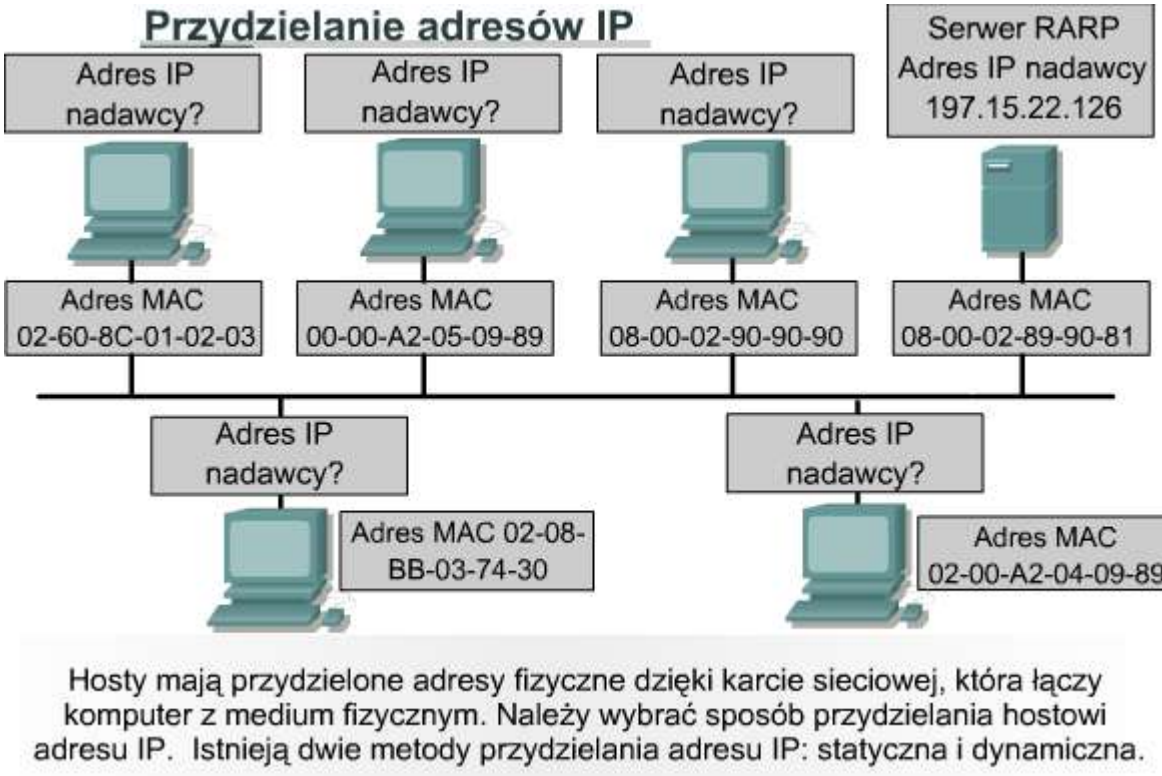
W ciągu ostatnich dwóch dziesięcioleci utworzono wiele rozszerzeń schematu IPv4. Rozszerzenia te były zaprojektowane w celu zwiększenia efektywności wykorzystania 32-bitowej przestrzeni adresowej. Dwa z ważniejszych rozszerzeń to maski podsieci i bezklasowy routing międzydomenowy CIDR, które zostaną omówione bardziej szczegółowo w toku dalszych lekcji.
W międzyczasie zdefiniowano i utworzono jeszcze bardziej skalowalną wersję protokołu IP, czyli IP wersję 6 (IPv6). Protokół IPv6 używa 128 bitów zamiast 32, stosowanych aktualnie w protokole IPv4. Do reprezentowania tych 128 bitów schemat IPv6 używa liczb szesnastkowych. Schemat IPv6 zawiera 340 sekstylionów adresów. Ta wersja protokołu IP powinna zapewnić wystarczającą liczbę adresów, aby zaspokoić przyszłe potrzeby komunikacyjne.



Na rysunku porównano przykładowy adres IPv4 oraz IPv6. Adresy IPv4 są 32-bitowe, zapisywane w postaci dziesiętnej przy użyciu kropek jako separatorów. Adresy IPv6 maja długość 128 bitów i są identyfikatorami poszczególnych interfejsów i zbiorów interfejsów. Adresy IPv6 są przypisywane do interfejsów, a nie do węzłów. Ponieważ każdy interfejs należy do pojedynczego węzła, którykolwiek adres jednostkowy (unicast) przypisany do interfejsów węzła może być użyty jako identyfikator tego węzła. Adresy IPv6 są zapisywane w postaci szesnastkowej przy użyciu dwukropków jako separatorów. Poszczególne pola adresu IPv6 mają rozmiar 16 bitów. Aby adresy łatwiej było odczytywać, w każdym polu można pominąć początkowe zera. Pole :0003: zostało zapisane jako :3:. Skrócona reprezentacja 128-bitowego adresu IPv6 używa ośmiu liczb 16-bitowych, przedstawionych w postaci czterech cyfr szesnastkowych. Po latach badań i rozwoju protokół IPv6 jest powoli wprowadzany w wybranych sieciach. Być może w przyszłości protokół IPv6 zastąpi protokół IPv4 jako podstawowy protokół Internetu.

9.3 Uzyskiwanie adresu IP

9.3.1 Otrzymywanie adresu internetowego



Host, aby móc działać w Internecie, musi otrzymać globalnie unikatowy adres. Fizyczny adres MAC hosta ma znaczenie tylko lokalne, ponieważ identyfikuje hosta w sieci lokalnej. Ponieważ jest to adres warstwy 2, router nie używa go do przekazywania pakietów na zewnątrz sieci LAN.
W komunikacji internetowej najczęściej używane są adresy IP. Protokół ten jest hierarchicznym schematem adresowania, który pozwala na łączenie pojedynczych adresów i traktowanie ich jako oddzielnych grup. Te grupy adresów pozwalają na efektywny transfer danych w Internecie.
Administratorzy mają dwie możliwości przypisania adresu IP. Mogą to zrobić statycznie lub dynamicznie. W dalszej części tej lekcji przedstawimy adresowanie statyczne oraz trzy warianty adresowania dynamicznego. Niezależnie od wybranego schematu adresowania żadne dwa interfejsy nie mogą mieć takich samych adresów IP. Dwa hosty o tym samym adresie IP mogłyby spowodować konflikt nie pozwalający im poprawnie funkcjonować.

Jak pokazano na rysunku , hosty uzyskują adres fizyczny dzięki temu, że mają kartę sieciową, która umożliwia ich podłączenie do medium fizycznego.

9.3.2 Statyczne przypisywane adresu IP

Statyczne przypisywanie działa najlepiej w wypadku małych sieci, w których rzadko zachodzą zmiany. Administrator ręcznie przypisuje i zarządza adresami IP każdego komputera, drukarki lub serwera w intranecie. Prawidłowe zarządzanie zapobiega problemom związanym z powielonymi adresami IP. Jest to możliwe tylko wtedy, gdy trzeba zajmować się jedynie niewielką liczbą urządzeń.

Serwerom należy przypisywać statyczne adresy IP, aby stacje robocze i inne urządzenia zawsze wiedziały, w jaki sposób uzyskać dostęp do wymaganych usług. Wyobraźmy sobie, jak trudno byłoby dodzwonić się do firmy, w której każdego dnia zmieniano by numer telefonu.

Inne urządzenia, którym należy przypisać statyczne adresy IP, to drukarki sieciowe, serwery aplikacji oraz routery.

9.3.3 Przypisywanie adresów IP za pomocą protokołu RARP

Struktura wiadomości ARP/RARP

bity 015		bity 1631
Typ sprzętu		Typ protokołu
HLen (1 bajt)	PLen (1 bajt)	Operacja
Adres sprzętowy nadawcy (bajty 14)		
Adres sprzętowy nadawcy (bajty 56)		Adres protokołowy nadawcy (bajty 12)
Adres protokołowy nadawcy (bajty 34)		Adres sprzętowy odbiorcy (bajty 12)
Adres sprzętowy odbiorcy (bajty 36)		
Adres protokołowy odbiorcy (bajty 14)		
Struktura nagłówka RARP		

Protokół RARP (*Reverse Address Resolution Protocol*) przypisuje znanemu adresowi MAC adres IP. To przypisanie pozwala urządzeniom sieciowym enkapsulować dane przed wysłaniem ich do sieci. Urządzenie sieciowe, takie jak na przykład bezdyskowa stacja robocza, może znać swój adres MAC, ale nie znać adresu IP. Protokół RARP pozwala urządzeniu poznać własny adres IP. Urządzenia używające protokołu RARP wymagają obecności w sieci serwera RARP, który odpowiada na ich żądania.

Opis pól wiadomości ARP/RARP

Pole	Opis
Typ sprzętu	Określa typ interfejsu sprzętowego,dla którego nadawca żąda odpowiedzi.
Typ protokołu	Określa typ adresu protokołu wysokiego poziomu dostarczonego przez nadawcę.
HLen	Długość adresu sprzętowego.
PLen	Długość adresu protokołowego.
Operacja	Używane są następujące wartości: 1. Żądanie ARP. 2. Odpowiedź ARP. 3. Żądanie RARP. 4. Odpowiedź RARP. 5. Dynamiczne żądanie RARP. 6. Dynamiczna odpowiedź RARP. 7. Dynamiczny błąd RARP. 8. Żądanie InARP. 9. Odpowiedź InARP.
Adres sprzętowy (HA) nadawcy	Długość adresu sprzętowego w bajtach (HLen).
Adres protokołowy (PA) nadawcy	Długość adresu protokołowego w bajtach (PLen).
Adres sprzętowy (HA) odbiorcy	Długość adresu sprzętowego w bajtach (HLen).
Adres protokołowy (PA) odbiorcy	Długość adresu protokołowego w bajtach (PLen).

Rozważmy sytuację, gdy urządzenie źródłowe chce wysłać dane do innego urządzenia. W naszym przykładzie urządzenie źródłowe zna swój adres MAC, ale nie może znaleźć własnego adresu IP w tablicy ARP. Aby urządzenie docelowe mogło odebrać dane, przekazać je do wyższych warstw modelu OSI oraz odpowiedzieć urządzeniu źródłowemu, urządzenie źródłowe musi znać zarówno własny adres MAC, jak i adres IP. Tak więc urządzenie źródłowe rozpoczyna proces zwany żądaniem RARP. Żądanie to pomaga urządzeniu źródłowemu wykryć swój adres IP. Żądania RARP są rozgłaszane w sieci LAN i odpowiadają na nie serwery RARP, którymi zwykle są routery.

Protokół RARP używa takiego samego formatu pakietów jak protokół ARP. Jednak w żądaniu RARP występują inne niż w żądaniu ARP nagłówki MAC i pole kodu operacji. Format pakietu RARP zawiera miejsca dla adresów MAC urządzenia źródłowego i docelowego. Pole źródłowego adresu IP jest puste. Pakiet ten jest rozgłaszany wśród wszystkich urządzeń w sieci, dlatego adresem docelowym MAC jest FF:FF:FF:FF:FF:FF.

Stacje robocze używające protokołu RARP mają zapisany w pamięciach ROM kod powodujący rozpoczęcie procesu żądania RARP.

9.3.4. Przypisywanie adresów IP za pomocą protokołu BOOTP

Struktura wiadomości protokołu BOOTP

bity 07	bity 815	bity 1623	bity 2431
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4 bajty)			
Sekundy (2 bajty)		Nieużywane	
Ciaddr (4 bajty)			
Yiaddr (4 bajty)			
Siaddr (4 bajty)			
Giaddr (4 bajty)			
Chaddr (16 bajtów)			
Nazwa serwera (64 bajty)			
Nazwa pliku ładującego (128 bajtów)			
Dane specyficzne dla producenta (64 bajty)			

Struktura wiadomości protokołu BOOTP

Protokół BOOTP (*Bootstrap Protocol*) działa w środowisku typu klient — serwer i wymaga tylko pojedynczej wymiany pakietów do pobrania informacji o adresie IP. W przeciwieństwie do protokołu RARP pakiety BOOTP mogą zawierać nie tylko adres IP, ale i adres routera, adres serwera oraz informacje zależne od producenta sprzętu.
Z protokołem BOOTP związany jest problem polegający na tym, że nie został on zaprojektowany do dynamicznego przypisywania adresów. Aby użyć tego protokołu, administrator sieci tworzy plik konfiguracyjny zawierający parametry dla każdego urządzenia. Administrator musi dodawać do niego hosty i zarządzać bazą danych BOOTP. Chociaż adresy są przypisywane dynamicznie, nadal istnieje relacja jeden do jednego pomiędzy liczbą adresów IP a liczbą hostów. Oznacza to, że dla każdego hosta IP w sieci musi istnieć profil BOOTP zawierający przypisany mu adres IP. Żadne dwa profile nie mogą zawierać takich samych adresów IP. Profile te mogłyby być użyte w tym samym czasie, co oznaczałoby przypisanie dwóm hostom tego samego adresu IP.
Urządzenie przy starcie używa protokołu BOOTP do pobrania adresu IP. Protokół BOOTP do przesyłania komunikatów używa protokołu UDP. Komunikat UDP jest enkapsulowany w pakiecie IP. Komputer używa protokołu BOOTP do wysłania pakietu rozgłoszeniowego na adres IP składający się z samych jedynek, czyli 255.255.255.255 w notacji dziesiętnej. Serwer BOOTP otrzymuje ten pakiet i w odpowiedzi wysyła również pakiet rozgłoszeniowy. Klient otrzymuję ramkę i sprawdza jej adres MAC. Jeżeli w polu adresu docelowego klient znajdzie swój adres MAC, a w polu adresu docelowego IP adres rozgłoszeniowy, pobierze adres IP i inne informacje zawarte w komunikacie odpowiedzi BOOTP.

Opis pól wiadomości protokołu BOOTP

Pole	Opis
Op	Kod operacji dla wiadomości. Wiadomości mogą być typu BOOTREQUEST albo BOOTREPLY
Htype	Typ adresu sprzętowego
HLen	Długość adresu sprzętowego
Hops	Klient wpisuje zero; to pole jest używane przez serwer BOOTP podczas wysyłania żądania do innej sieci
Xid	Identyfikator transakcji
Secs	Liczba sekund, które upłynęły od chwili rozpoczęcia procesu uzyskiwania lub odnawiania adresu
Ciaddr	Adres IP klienta
Yiaddr	"Twój" (klienta) adres IP
Siaddr	Adres IP następnego serwera, który ma być użyty w procesie uruchamiania.
Giaddr	Adres IP agenta przekazującego używany podczas uruchamiania za pośrednictwem takiego agenta.
Chaddr	Adres sprzętowy klienta
Server Host Name	Definiuje określony serwer, z którego mają być pobrane informacje protokołu BOOTP.
Boot File Name	Umożliwia używanie wielu plików uruchomieniowych, dzięki czemu na hostach mogą działać różne systemy operacyjne.
Vendor Specific Area	Zawiera opcjonalne informacje pochodzące od producenta, które mogą zostać przekazane do hosta.

9.3.5 Zarządzanie adresami IP przy użyciu protokołu DHCP

Struktura wiadomości protokołu DHCP

bity 07	bity 815	bity 1623	bity 2431
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4 bajty)			
Sekundy (2 bajty)		Flagi (2 bajty)	
Ciaddr (4 bajty)			
Yiaddr (4 bajty)			
Siaddr (4 bajty)			
Giaddr (4 bajty)			
Chaddr (16 bajtów)			
Nazwa serwera (64 bajty)			
Nazwa pliku ładującego (128 bajtów)			
Obszar używany przez producenta (może zostać zmieniony)			

Struktura wiadomości protokołu DHCP

Protokół dynamicznej konfiguracji hostów DHCP (*Dynamic Host Configuration Protocol*) jest następcą protokołu BOOTP. W przeciwieństwie do protokołu BOOTP protokół DHCP pozwala hostowi pobierać adres IP dynamicznie, dzięki czemu administrator sieci nie musi tworzyć oddzielnych profili dla każdego urządzenia. Do używania protokołu DHCP konieczne jest jedynie zdefiniowane zakresu adresów IP na serwerze DHCP. Host, przyłączając się do sieci, kontaktuje się z serwerem DHCP i żąda przypisania adresu. Serwer DHCP wybiera adres i wydzierżawia go temu hostowi. Protokół DHCP pozwala na pobranie całej konfiguracji sieciowej komputera w jednym komunikacie.

Oznacza to pobranie wszystkich danych przesyłanych w komunikacie BOOTP oraz wydzierżawionego adresu IP i maski podsieci.

Główną zaletą protokołu DHCP w porównaniu z protokołem BOOTP jest możliwość obsługi użytkowników mobilnych. Mobilność umożliwia użytkownikom swobodną zmianę połączeń sieciowych w zależności od miejsca pracy. Nie ma tutaj występującej w systemie BOOTP potrzeby przechowywania stałego profilu dla każdego urządzenia przyłączonego do sieci. Ważną zaletą protokołu DHCP jest możliwość wydzierżawienia adresu IP oraz odzyskania go w celu przypisania innemu użytkownikowi, gdy pierwszy użytkownik zwolni ten adres. Oznacza to, że protokół DHCP umożliwia utworzenie relacji jeden do wielu między adresami IP i komputerami, a także że adres jest dostępny dla każdego, kto przyłącza się do sieci.

Opis pól wiadomości protokołu DHCP

Op	Kod operacji dla wiadomości. Wiadomości mogą być typu BOOTREQUEST albo BOOTREPLY.
Htype	Typ adresu sprzętowego
Hlen	Długość adresu sprzętowego
Hops	Klient wpisuje zero; pole to jest używane przez serwer BOOTP podczas wysyłania żądania do innej sieci.
Xid	Identyfikator transakcji
Secs	Liczba sekund, które upłynęły od chwili rozpoczęcia procesu uzyskiwania lub odnawiania adresu.
Flagi	Flagi
Ciaddr	Adres IP klienta
Yiaddr	"Twój" (klienta) adres IP
Siaddr	Adres IP następnego serwera, który ma być użyty w procesie uruchamiania.
Giaddr	Adres IP agenta przekazującego używany podczas uruchamiania za pośrednictwem takiego agenta.
Chaddr	Adres sprzętowy klienta
Server Host Name	Definiuje określony serwer, z którego mają być pobrane informacje protokołu BOOTP.
Boot File Name	Umożliwia używanie wielu plików uruchomieniowych, dzięki czemu na hostach mogą działać różne systemy operacyjne.
Vendor Specific Area	Zawiera opcjonalne informacje pochodzące od producenta, które mogą zostać przekazane do hosta.

9.3.6 Problemy z określaniem adresów

Jednym z głównych problemów w sieciach jest sposób komunikowania się z innymi urządzeniami sieciowymi. W komunikacji TCP/IP datagram w lokalnej sieci musi zawierać zarówno adres MAC, jak i adres IP urządzenia docelowego. Adresy te muszą być prawidłowe i muszą odpowiadać adresom MAC i IP urządzenia docelowego. Jeżeli nie będą pasowały, datagram zostanie odrzucony przez host docelowy. Komunikacja w segmencie sieci LAN wymaga dwóch adresów. Musi istnieć możliwość automatycznego odwzorowywania adresów IP na adresy MAC. Zbyt dużo czasu zajmowałoby użytkownikom tworzenie takich odwzorowań ręcznie. Zestaw protokołów TCP/IP zawiera protokół o nazwie ARP (*Address Resolution Protocol*), który automatycznie pobiera adres MAC dla transmisji lokalnych. Inaczej jest przy wysyłaniu danych poza sieć lokalną.

Komunikacja pomiędzy dwoma segmentami sieci LAN wymaga dodatkowej pracy. Potrzebne są adresy IP i MAC zarówno urządzenia docelowego, jak i pośredniczącego urządzenia routującego. Zestaw protokołów TCP/IP zawiera odmianę protokołu ARP o nazwie proxy ARP, która dostarcza adres MAC urządzenia pośredniczącego w transmisji z sieci LAN do innego segmentu sieciowego

9.3.7 Protokół odwzorowania adresów ARP (Address Resolution Protocol)

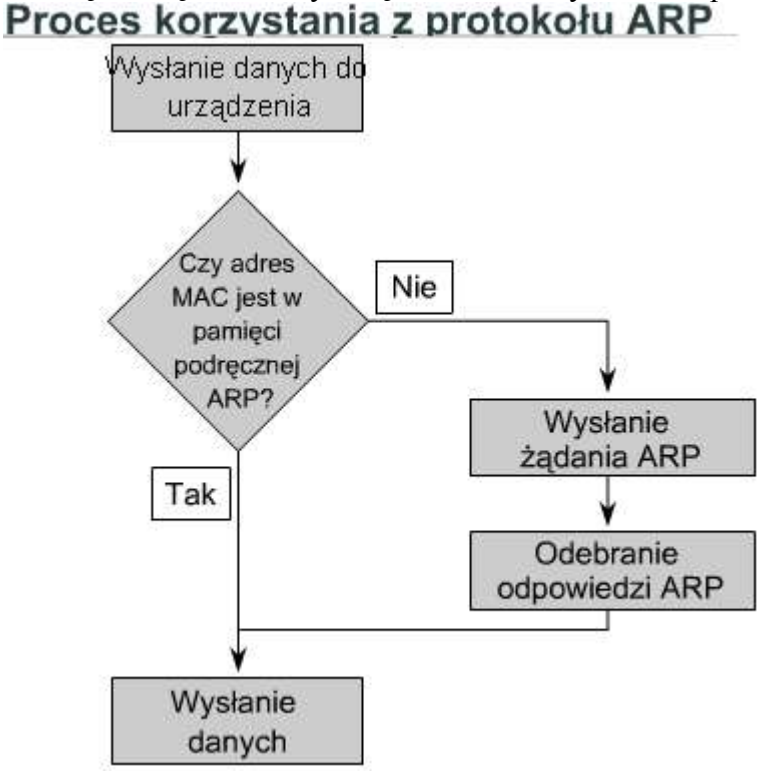
Pozycja tablicy ARP

Pozycja tablicy ARP		
Adres internetowy	Adres fizyczny	Typ
68.2.168.1	00-50-57-00-76-84	dynamiczny

Tablica ARP komputera o adresie 198.150.11.36	
MAC	IP
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:00:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35

W przypadku sieci TCP/IP pakiet danych musi zawierać zarówno adres MAC, jak i adres IP urządzenia docelowego. Pakiet nie zawierający jednego z nich nie zostanie przekazany z warstwy 3 do warstw wyższych. Dzięki temu adresy MAC i IP służą do wzajemnej kontroli. Gdy urządzenie określi adresy IP urządzeń docelowych, może dodać do pakietów danych docelowe adresy MAC.

Niektóre urządzenia przechowują tablice zawierające adresy MAC i IP innych urządzeń podłączonych do tej samej sieci LAN. Tablice te nazywane są tablicami ARP. Przechowywane są one w pamięci RAM urządzenia, które automatycznie zarządza zapamiętanymi informacjami. Bardzo rzadko stosowane jest ręczne dodawanie przez użytkownika wpisów do tablicy ARP. Każde urządzenie w sieci utrzymuje własną tablicę ARP. Gdy urządzenie chce wysłać dane przez sieć, używa informacji zawartych w tej tablicy.



Gdy urządzenie źródłowe określi docelowy adres IP, przeszukuje tablicę ARP w celu znalezienia adresu MAC urządzenia docelowego. Jeżeli urządzenie źródłowe znajdzie pozycję w tablicy dla docelowego adresu IP i docelowego adresu MAC, skojarzy adres IP z adresem MAC i będzie ich używało do enkapsulacji danych. Pakiet danych może wówczas zostać przesłany poprzez medium sieciowe, po czym zostanie odebrany przez urządzenie docelowe.

Istnieją dwie metody zbierania przez urządzenia adresów MAC potrzebnych do enkapsulacji danych. Pierwszą metodą jest monitorowanie ruchu w lokalnym segmencie sieci. Wszystkie stacje w sieci Ethernet analizują ruch, aby sprawdzić, czy dane są przeznaczone dla nich. Częścią tego procesu jest zapisywanie adresu IP i MAC źródła datagramu w tablicy ARP. Zatem podczas przesyłania danych przez sieć pary adresów są umieszczane w tablicy ARP. Innym sposobem pobrania tej pary adresów do transmisji danych jest rozgłoszenie żądania ARP. Komputer potrzebujący pary adresów IP i MAC rozgłasza żądanie ARP. Wszystkie urządzenia w sieci analizują to żądanie. Jeżeli jedno z urządzeń lokalnych będzie miało pasujący do żądania adres IP, wyśle odpowiedź ARP zawierającą parę adresów IP-MAC. W wypadku gdy adres IP należy do sieci lokalnej, a

komputer nie istnieje lub jest wyłączony, nie pojawi się odpowiedź na żądanie ARP. W tej sytuacji urządzenie źródłowe zgłasza błąd. Jeżeli żądanie dotyczy innej sieci IP, można użyć innej metody.
Routery nie przekazują pakietów rozgłaszania. Jeżeli włączony jest mechanizm proxy ARP, router korzysta z niej. Protokół proxy ARP jest odmianą protokołu ARP. W tej odmianie router wysyła do hosta odpowiedź ARP z adresem MAC interfejsu, na którym otrzymał żądanie. Router odpowiada takim adresem MAC na żądania, których adres IP nie należy do zakresu adresów podsieci lokalnej.
Inną metodą wysyłania danych na adres urządzenia w innym segmencie sieci jest skonfigurowanie bramy domyślnej. Brama domyślna to opcja hosta umożliwiająca przechowywanie adresu IP interfejsu routera w konfiguracji hosta. Host źródłowy porównuje docelowy adres IP z własnym adresem, aby sprawdzić, czy oba adresy IP znajdują się w tym samym segmencie. Jeżeli host docelowy znajduje się w innym segmencie, host źródłowy wysyła dane, używając prawdziwego adresu IP urządzenia docelowego i adresu MAC routera. Adres MAC routera jest pobierany z tablicy ARP przy użyciu adresu IP routera.
Jeżeli w routerze nie skonfigurowano mechanizmu proxy ARP albo na hoście nie ustawiono bramy domyślnej, ruch sieciowy nie może opuścić sieci lokalnej. Jeden z tych dwóch warunków musi być spełniony, aby uzyskać połączenie z urządzeniami spoza sieci lokalnej.