Wydanie VI

Joe Casad

TCP/IP

w 24 godziny

SAMS

Helion

Tytuł oryginału: Sams Teach Yourself TCP/IP in 24 Hours, Sixth Edition

Tłumaczenie: Andrzej Watrak

ISBN: 978-83-283-3708-4

Authorized translation from the English language edition, entitled: SAMS TEACH YOURSELF TCP/lP IN 24 HOURS, Sixth Edition; ISBN 0672337894; by Joe Casad; published by Pearson Education, Inc, publishing as SAMS Publishing.

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/tcp246
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

Godzina 12.

Konfiguracja

W ciągu tej godziny poznasz następujące zagadnienia:

- **dynamiczne przypisywanie adresów IP;**
- **protokół DHCP;**
- **translacja NAT;**
- **konfiguracja Zeroconf.**

W dawnych czasach każdy komputer posiadał statyczny adres IP określony w pliku konfiguracyjnym i aby zmienić adres komputera, administrator musiał ten plik edytować. Dzisiejsze sieci wymagają stosowania bardziej zaawansowanych i wygodniejszych metod, umożliwiających dynamiczne i automatyczne konfigurowanie wszystkich komputerów. W tym rozdziale opisanych jest kilka najczęściej stosowanych metod konfigurowania ustawień TCP/IP.

Po przeczytaniu tego rozdziału będziesz potrafił:

- opisać protokół DHCP i korzyści płynące z jego stosowania;
- opisać proces przypisywania adresu IP za pomocą protokołu DHCP;
- opisać zastosowanie translacji NAT;
- opisać protokoły do automatycznego konfigurowania komputerów.

Dołączanie się do sieci

Protokoły opisane w poprzednich rozdziałach i relacje między nimi mogą przytłaczać, ale współczesne systemy w automatyczny sposób bardzo dobrze radzą sobie z ich wszystkimi niuansami. Od użytkownika wymaga się jedynie podania kilku parametrów konfiguracyjnych TCP/IP podczas instalacji systemu. Choć w różnych systemach wygląda to inaczej, najczęściej trzeba wykonać jedną z poniższych podstawowych operacji:

- skonfigurowanie statycznego adresu IP;
- przystosowanie komputera do automatycznego uzyskiwania adresu IP za pomocą protokołu DHCP.

W większości przypadków należy podać również identyfikator, który będzie pełnił funkcję nazwy komputera w sieci (więcej informacji o nazwach hostów oraz o systemach DNS i NetBIOS zawiera rozdział 10., „Odwzorowywanie nazw").

Jak dowiesz się z dalszej części rozdziału, niektóre systemy operacyjne oferują możliwość automatycznego konfigurowania ustawień TCP/IP, bez konieczności definiowania statycznego ani dynamicznego adresu IP. Funkcjonalność ta stała się w ostatnich latach bardzo popularna.

Po zakończonej instalacji systemu operacyjnego trzeba za pomocą jego interfejsu graficznego wykonać pewne operacje konfiguracyjne. W każdym systemie wygląda to inaczej, ale najbardziej podstawowe parametry są wszędzie takie same. W tym rozdziale poznasz ustawienia TCP/IP stosowane w najnowszych systemach Windows, macOS i Linux Ubuntu. Informacje na temat konfigurowania parametrów w innych systemach znajdziesz w odpowiedniej dokumentacji.

Pojęcie statycznej konfiguracji TCP/IP jest zrozumiałe. Wymaga ona jedynie określenia nazwy komputera, jego adresu IP, maski i adresu bramy domyślnej. Konfiguracja dynamicznego adresu jest jeszcze prostsza, jednak w takim przypadku komputer wykonuje w tle serię operacji za pomocą protokołu **DHCP**, któremu poświęcona jest pierwsza część tego rozdziału.

Przypisywanie adresów IP przez serwer

Jak już wiesz, każdy komputer, aby mógł działać w sieci, musi mieć przypisany adres IP. Pierwotnie adresowanie polegało wyłącznie na konfigurowaniu w każdym komputerze jego własnego adresu IP. Jest to tzw. adresacja statyczna. Każdy komputer po uruchomieniu ma przypisany adres IP i może od razu korzystać z sieci. Adresacja statyczna dobrze sprawdza się w małych, niezmiennych sieciach, ale w dużych sieciach, których konfiguracja nieustannie się zmienia (np. dołączane są i odłączane kolejne komputery), adresacja ta ujawnia pewne swoje ograniczenia.

Adresacja statyczna ma następujące najważniejsze wady:

- **Pracochłonna konfiguracja** — każdy komputer trzeba osobno skonfigurować. Zmiana zakresu adresów lub innego parametru sieciowego (np. adresu serwera DNS) wymaga modyfikowania konfiguracji każdego komputera.
- **Nieefektywne gospodarowanie adresami** — adres IP trzeba przypisać każdemu komputerowi niezależnie od tego, czy aktualnie działa w sieci, czy nie działa.
- **Mała elastyczność** — po przeniesieniu komputera do innej podsieci trzeba ręcznie zmienić jego konfigurację.

W celu rozwiązania powyższych problemów opracowano protokół DHCP umożliwiający konfigurowanie ustawień TCP/IP na żądanie. Jest on udoskonaloną wersją protokołu BOOTP używanego pierwotnie w komputerach bez dysków twardych (takie komputery podczas uruchamiania pobierają przez sieć kompletny system operacyjny). Wraz z wyczerpywaniem się adresów IP i rozwojem dużych, dynamicznych sieci protokół DHCP zyskał w ciągu ostatnich lat ogromną popularność.

Z dużym prawdopodobieństwem można założyć, że większość komputerów korzystających z Internetu uzyskuje konfigurację za pomocą protokołu DHCP. Mały router lub zapora, z której korzystasz w domu do łączenia się z Internetem, prawdopodobnie również pełni funkcje serwera DHCP. Laptop, który łączy się z siecią bezprzewodową w kawiarni, w taki sam sposób uzyskuje adres IP.

Czym jest protokół DHCP?

DHCP jest to protokół umożliwiający automatyczne konfigurowanie ustawień TCP/IP w komputerach. Protokół ten został zdefiniowany w dokumencie RFC 1531 i zaktualizowany w RFC 1534, 1541, 2131 i 2132. Obecnie obowiązujący standard jest opisany w RFC 2131 i aktualizacjach RFC 3396, 4361, 5494 i 6842. Serwer DHCP przesyła do komputera ustawienia TCP/IP, m.in.: adres IP, maskę podsieci i adres serwera DNS.

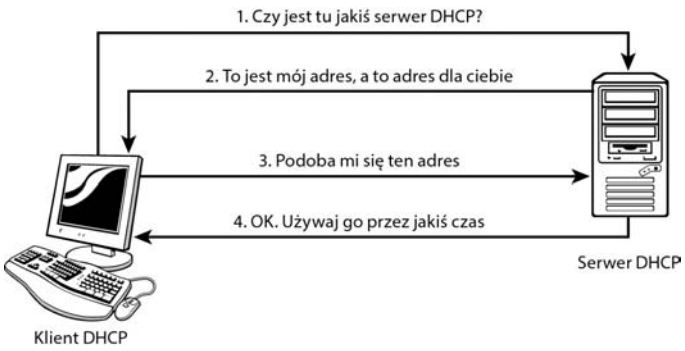
Ponieważ serwer DHCP przypisuje komputerom adresy IP, teoretycznie tylko on musi posiadać statyczny adres IP (inne urządzenia zainstalowane na stałe w sieci, np. drukarki, również często posiadają statyczne adresy). W komputerach stacjonarnych, laptopach i innych urządzeniach klienckich wystarczy skonfigurować parametr umożliwiający uzyskiwanie adresu IP z serwera DHCP. Całą pozostałą konfigurację TCP/IP komputer pobierze z tego serwera. Jeżeli administrator sieci zmieni jakiś jej parametr TCP/IP, wtedy musi jedynie uaktualnić serwer DHCP, a nie każdy komputer użytkownika osobno.

Co więcej, każdy komputer uzyskuje swój adres na określony czas. Jeżeli po upływie tego czasu komputer nie korzysta ze swojego adresu, jest on przypisywany innemu komputerowi. Dzięki temu mechanizmowi zazwyczaj nie jest potrzebnych w sieci tyle adresów IP, ile komputerów z niej korzysta.

Protokół DHCP odgrywa szczególnie ważną rolę w dużych korporacjach, w których wielu użytkowników podłącza swoje laptopy w różnych miejscach sieci. Gdyby taki komputer miał przypisany statyczny adres IP, należałoby go ręcznie zmieniać po każdorazowym podłączeniu komputera do innej podsieci. Jeżeli natomiast komputer korzysta z protokołu DHCP, wtedy automatycznie uzyskuje wszystkie ustawienia TCP/IP z serwera.

Jak działa protokół DHCP?

Gdy komputer korzystający z protokołu DHCP zostanie włączony, uruchamia oprogramowanie obsługujące protokół TCP/IP. Ponieważ komputer nie ma wtedy jeszcze przypisanego adresu IP, nie może się komunikować z innymi komputerami. Może jednak wysyłać i odbierać datagramy rozgłoszeniowe, które stanowią podstawę funkcjonowania protokołu DHCP. Proces uzyskiwania adresu IP z serwera DHCP polega na przesłaniu czterech datagramów (rysunek 12.1):



RYSUNEK 12.1. Proces przypisywania komputerowi użytkownika adresu IP przez serwer DHCP

1. **DHCPDISCOVER** — komputer użytkownika inicjuje proces poprzez wysłanie za pomocą protokołu UDP datagramu rozgłoszeniowego z portem docelowym 67 (jest to port wykorzystywany przez serwery DHCP i BOOTP). Pierwszy datagram jest komunikatem wykrywającym serwer DHCP. Jest to zapytanie o konfigurację skierowane do wszystkich serwerów DHCP. Datagram ten składa się z wielu różnych pól, a jedno z najważniejszych zawiera adres fizyczny komputera użytkownika.
2. **DHCPOFFER** — serwer DHCP przydzielający adresy komputerom w sieci, w której znajduje się komputer użytkownika, wysyła za pomocą protokołu UDP datagram rozgłoszeniowy zawierający odpowiedź na otrzymane zapytanie. Datagram ten ma port docelowy 68 i zawiera adres fizyczny oraz adres IP serwera DHCP, jak również adres IP i maskę podsieci przeznaczone dla komputera użytkownika.

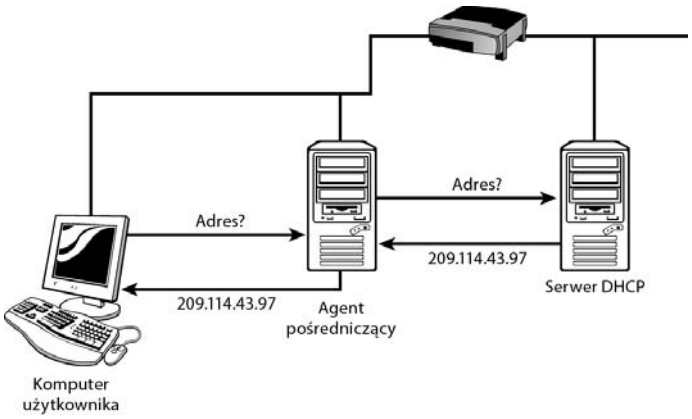
   Jeżeli w sieci jest kilka serwerów DHCP, wtedy komputer użytkownika może otrzymać kilka odpowiedzi. Zazwyczaj komputer akceptuje pierwszą z nich.
3. **DHCPREQUEST** — komputer użytkownika odbiera odpowiedź i wysyła datagram rozgłoszeniowy z informacjami dla serwerów DHCP. Datagram ten zawiera adres IP serwera DHCP, od którego pochodzi odpowiedź, oraz adres fizyczny komputera użytkownika. Datagram realizuje dwie podstawowe funkcje. Po pierwsze, informuje wybrany serwer DHCP, że komputer użytkownika zaakceptował przypisany mu adres IP (i inne ustawienia). Po drugie, informuje wszystkie pozostałe serwery DHCP, że komputer użytkownika odrzucił ich odpowiedzi.
4. **DHCPACK** — serwer DHCP, którego odpowiedź zaakceptował komputer użytkownika, wysyła ostatni **datagram z potwierdzeniem**. Zawiera on przypisany komputerowi adres IP i maskę podsieci. Często zawiera też adres bramy domyślnej, adresy serwerów DNS i jeden lub dwa adresy serwerów WINS. Oprócz tego datagram może zawierać dodatkowe informacje, takie jak typ węzła NetBIOS-a określający sposób odwzorowywania nazw.

   W potwierdzeniu zawarte są również trzy ważne pola określające różne przedziały czasu. Pierwsze pole określa czas przypisania adresu, natomiast dwa pozostałe, oznaczone jako T1 i T2, są wykorzystywane przez komputer użytkownika do przedłużenia czasu przypisania adresu.

Agenty pośredniczące

Jeżeli komputer użytkownika i serwer DHCP znajdują się w tym samym segmencie sieci, proces przypisywania adresu przebiega dokładnie w opisany wyżej sposób. Jeżeli natomiast oba urządzenia znajdują się w różnych podsieciach połączonych za pomocą jednego lub kilku routerów, proces jest bardziej skomplikowany. Routery zazwyczaj nie przesyłają datagramów rozgłoszeniowych, dlatego aby można było używać protokołu DHCP, potrzebne są urządzenia pośredniczące. Takim urządzeniem może być komputer zainstalowany w tej samej podsieci co komputer użytkownika albo sam router. W obu przypadkach urządzenie to nosi nazwę **agenta pośredniczącego DHCP** lub **agenta pośredniczącego BOOTP**.

Agent posiada statyczny adres IP i zna adres IP serwera DHCP, dzięki temu może odbierać i wysyłać datagramy. Ponieważ znajduje się w tej samej podsieci co komputer użytkownika, może się z nim komunikować za pomocą datagramów rozgłoszeniowych (rysunek 12.2).



RYSUNEK 12.2. Agent DHCP umożliwia komputerowi użytkownika komunikowanie się z serwerem DHCP znajdującym się w innej podsieci

Agent odbiera datagramy rozgłoszeniowe wysyłane na port UDP 67. Jeżeli taki datagram zawiera zapytanie skierowane do serwera DHCP, przesyła je bezpośrednio do niego. Gdy agent odbierze odpowiedź z serwera DHCP, wtedy wysyła ją za pomocą datagramu rozgłoszeniowego do wszystkich komputerów w podsieci. W celu zwięzłości opisu zostało tu pominiętych kilka szczegółów, niemniej jednak oddana jest istota funkcji agenta.

Często stosowana praktyka łączenia serwera DHCP i routera w jednym urządzeniu zmniejsza w większości sieci potrzebę stosowania agentów. Więcej informacji o agentach zawiera dokument RFC 1542.

Pola czasu w odpowiedzi DHCP

Komputer użytkownika uzyskuje adres IP z serwera DHCP na określony czas. Ten czas jest skonfigurowany na serwerze DHCP. Pola T1 i T2 umieszczone w komunikacie DHCPACK są wykorzystywane do przedłużania okresu przypisania adresu. Pole T1 oznacza moment, w którym komputer użytkownika powinien rozpocząć proces przedłużania. Zazwyczaj przypada on w połowie okresu przypisania adresu. Załóżmy, że okres przypisania adresu wynosi osiem dni. W takim przypadku po czterech dniach komputer użytkownika wysyła do serwera DHCP datagram DHCPREQUEST z zapytaniem o możliwość przedłużenia okresu przypisania. Jeżeli serwer DHCP jest dostępny, wtedy zazwyczaj odsyła odpowiedź DHCPACK zawierającą przedłużenie okresu. Tym razem jednak oba komunikaty nie są przesyłane za pomocą datagramów rozgłoszeniowych, ale bezpośrednio pomiędzy obydwoma urządzeniami. Jest to możliwe, ponieważ w tym czasie posiadają one ważne adresy IP.

Jeżeli serwer DHCP nie jest dostępny w połowie okresu przypisania adresu (tj. po czterech dniach), wtedy komputer użytkownika ponawia próbę po trzech czwartych okresu, czyli po sześciu dniach. Jeżeli ta próba również się nie powiedzie, następna jest podejmowania po upływie siedmiu ósmych okresu. Za każdym razem komputer użytkownika wysyła datagramy bezpośrednio do serwera DHCP. Jeżeli wszystkie próby zakończą się niepowodzeniem, to w chwili T2 komputer wyśle komunikat rozgłoszeniowy do wszystkich serwerów

DHCP w sieci. Jeżeli i tym razem nie uda się przedłużyć okresu przypisania adresu ani uzyskać nowego, komputer musi zwolnić przypisany mu adres i zaprzestać wykonywania wszelkich operacji za pomocą protokołu TCP/IP.

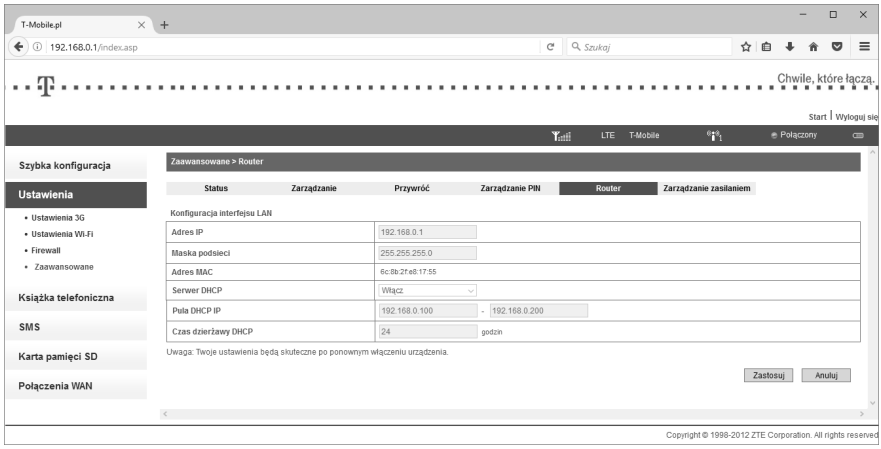
Konfiguracja serwera DHCP

Jeżeli nie jesteś administratorem średniej ani dużej sieci, prawdopodobnie nie miałeś okazji konfigurowania serwera DHCP. Jeżeli jednak konfigurowałeś serwer, to prawdopodobnie korzystałeś z dokumentacji zawierającej znacznie bardziej szczegółowe informacje niż zawarte w tej książce.

System Windows oferuje graficzny interfejs do konfigurowania serwera DHCP. W systemie Linux jest to usługa dhcpd. Konfiguracja tej usługi może być różna w zależności od odmiany systemu, ale zazwyczaj jest zapisana w pliku */etc/dhcpd.conf*. Plik ten zawiera informacje niezbędne do przypisywania adresów IP komputerom użytkowników, jak również opcjonalne ustawienia, np.: adres rozgłoszeniowy, nazwę domeny, adres serwera DNS i bramy domyślnej. Poniżej przedstawiony jest przykładowy plik */etc/dhcpd.conf*:

```
default-lease-time 600;
max-lease-time 7200;
option domain-name "helion.pl";
option subnet-mask 255.255.255.0;
option broadcast-address 185.142.13.255;
subnet 185.142.13.0 netmask 255.255.255.0 {
  range 185.142.13.10 185.142.13.50;
  range 185.142.13.100 185.142.13.200;
}
```

Jak wspomniałem wcześniej w tym rozdziale, funkcję serwera DHCP często pełni router lub zapora. W instrukcji do swojego routera znajdziesz informacje, jak skonfigurować serwer DHCP. W urządzeniach tego typu zazwyczaj wykorzystuje się do tego celu przeglądarkę (rysunek 12.3). Po zalogowaniu się do routera można zmienić konfigurację serwera DHCP. W większości przypadków nie jest to jednak konieczne.



RYSUNEK 12.3. Konfiguracja serwera DHCP w domowym routerze

Czasami zdarza się, że niektóre urządzenia w sieci muszą posiadać statyczny adres IP, nawet jeżeli wszystkie komputery uzyskują swoje adresy dynamicznie. Na przykład drukarka musi mieć statyczny adres, aby w komunikujących się z nią komputerach nie trzeba było nieustannie aktualizować jej adresu. Niektóre serwery oferują usługę zwaną rezerwacją adresu IP, umożliwiającą wiązanie adresów IP z adresami fizycznymi (MAC). Dzięki temu urządzenie w sieci zawsze uzyskuje z serwera ten sam adres IP.

Translacja NAT

Eksperci zauważyli, że skoro serwer DHCP przypisuje komputerom adresy IP, nie ma ważnego powodu, aby były to oficjalne, „legalne" adresy internetowe. Wystarczy, aby tylko router miał taki adres i mógł pełnić funkcję pośrednika w komunikacji komputerów z Internetem, tj. zmieniać lokalne adresy w wysyłanych przez nich datagramach na adresy z publicznego zakresu stosowanego w Internecie. Wiele nowoczesnych routerów oferuje usługę zwaną **translacją adresów** (ang. *Network Address Translation* — NAT).

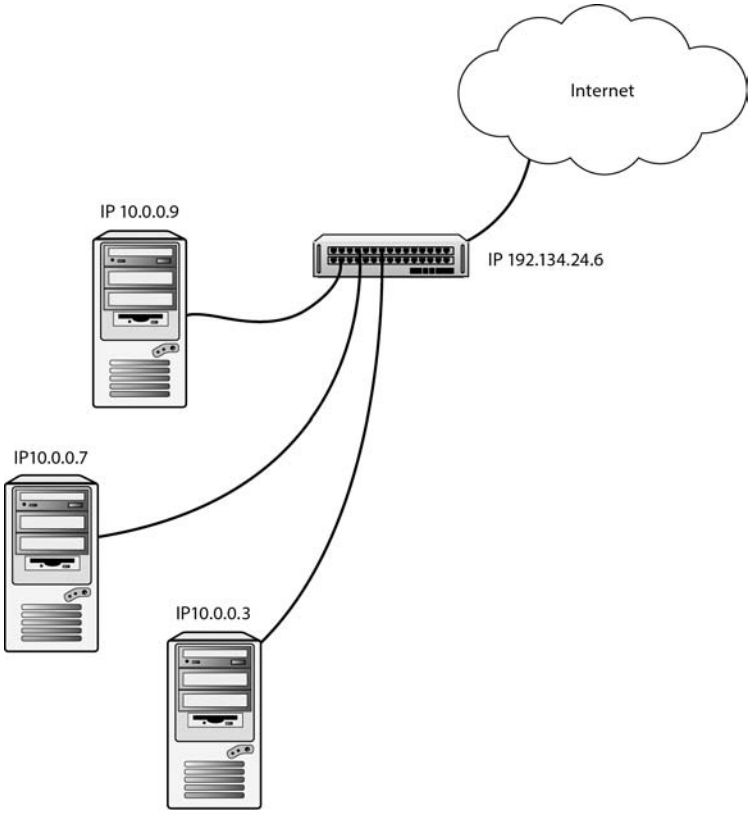
Translacja NAT pozwala ukryć przed zewnętrznymi urządzeniami szczegóły lokalnej sieci, a nawet ukryć jej istnienie. Rysunek 12.4 przedstawia urządzenie realizujące translację NAT. Umożliwia ono komputerom w lokalnej sieci komunikowanie się z Internetem. W lokalnej sieci mogą być stosowane adresy IP z dowolnego zakresu. Gdy komputer w sieci lokalnej potrzebuje skomunikować się z serwerem w Internecie, wtedy w połączeniu pośredniczy urządzenie NAT. Zmienia ono we wszystkich pakietach odbieranych z Internetu adresy docelowe na adresy stosowane w lokalnej sieci i przesyła je do komputera, który nawiązał połączenie.

Translacja NAT zwiększa bezpieczeństwo sieci, ponieważ uniemożliwia hakerowi z zewnątrz jej wykrycie (aczkolwiek sama translacja nie powinna być stosowana jako jedyny środek bezpieczeństwa). Z zewnątrz sieci urządzenie NAT wygląda jak pojedynczy host dołączony do Internetu. Nawet jeżeli haker będzie znał lokalny adres komputera w sieci, nie będzie mógł nawiązać z nim połączenia, ponieważ lokalne adresy nie są w żaden sposób powiązane z adresami stosowanymi w Internecie. Jak dowiedziałeś się z rozdziału 4., „Warstwa sieciowa", dla lokalnych sieci zarezerwowane są poniższe „prywatne" zakresy adresów IP:

- od 10.0.0.0 do 10.255.255.255;
- od 172.16.0.0 do 172.31.255.255;
- od 192.168.0.0 do 192.168.255.255.

(W dalszej części rozdziału dowiesz się, że zakres od 169.254.0.0 do 169.254.255.255 jest przeznaczony do automatycznego konfigurowania adresów IP i nie jest uwzględniany w translacji NAT).

Translacja NAT obejmuje zazwyczaj adresy z powyższych prywatnych zakresów. Adresy te nie są stosowane w sieciach publicznych, więc komputer może komunikować się z Internetem *wyłącznie* za pośrednictwem urządzenia NAT. Dzięki translacji liczba publicznych adresów internetowych wykorzystywanych w instytucji może być mniejsza. Jedynie router realizujący translację musi mieć publiczny adres internetowy. Dzięki możliwości zmniejszenia liczby stosowanych adresów publicznych i poprawie bezpieczeństwa sieci translacja NAT stała się bardzo popularna zarówno w sieciach korporacyjnych, jak i domowych.



RYSUNEK 12.4. Translacja NAT

Oczywiście bezpieczeństwo sieci często nie jest takie, jakiego można sobie życzyć. Nawet pozornie odporne na włamania urządzenie NAT jest podatne na ataki. Niektóre urządzenia oferują specjalne funkcjonalności umożliwiające uzyskanie do nich dostępu administracyjnego z Internetu. Jeżeli funkcjonalności te nie zostaną wyłączone, mogą narazić sieć na niebezpieczeństwo.

Rosnąca popularność translacji NAT spowodowała pojawienie się nowych technik omijania naturalnych zabezpieczeń lokalnych sieci. Jedna z nich, umożliwiająca hakerowi dostanie się do lokalnej sieci, polega na uzyskaniu zaproszenia od użytkownika. Hakerzy często wysyłają wiadomości e-mail z odnośnikami do fałszywych stron WWW, aby sprowokować użytkowników do nawiązania połączenia z niebezpiecznym serwerem. Zagrożenie tego typu atakami jest jednym z powodów, dla których ostrzega się użytkowników przed klikaniem odnośników w nieoczekiwanych wiadomościach. Dzisiejsze przeglądarki udaremniają niekiedy ataki realizowane za pomocą skryptów międzydomenowych i innych metod.

Przy okazji

Protokół IPv6 i translacja NAT

Protokół nowej generacji, IPv6, oferuje funkcje lokalnej adresacji, które mogą sprawić, że urządzenia NAT stosowane w dzisiejszych sieciach staną się niepotrzebne. Więcej informacji na temat protokołu IPv6 znajdziesz w rozdziale 13., „IPv6 — protokół nowej generacji".

Konfiguracja automatyczna

Zapewne zastanawiasz się, co się stanie, gdy komputery w sieci będą przystosowane do pobierania konfiguracji z serwera DHCP, ale serwer ten będzie niedostępny. Komputery nie mają przypisanych statycznych adresów IP ani nie będą mogły ich uzyskać za pomocą protokołu DHCP. W takiej sytuacji istnieje możliwość (choć jest to rzadki przypadek) utworzenia małej grupy komputerów bez łączności z Internetem ani żadnym serwerem DHCP czy routerem.

Twórcy systemów operacyjnych opracowali metody umożliwiające komputerom znajdującym się w lokalnej sieci nawiązywanie między sobą komunikacji bez konieczności statycznego przypisywania adresów IP ani korzystania z protokołu DHCP. Pierwsze protokoły stosowane w sieciach LAN, np. NetBEUI (w systemie Windows) i AppleTalk (w systemie Apple), oferowały funkcje komunikacji sieciowej bez konieczności jej konfigurowania, dlatego dostawcy systemów operacyjnych zaczęli szukać możliwości zaimplementowania ich w modelu TCP/IP.

Pierwszym krokiem w tym kierunku było opracowanie koncepcji **lokalnej adresacji łącza** (ang. *link-local addressing* — IPv4LL). Funkcjonalność tę posiadają systemy Apple, począwszy od wersji iOS9, oraz Microsoft od wersji Windows 98.

W systemach Windows funkcjonalność IPv4LL nosi nazwę **APIPA** (ang. *Automatic Private IP Addressing* — automatyczne przypisywanie prywatnych adresów IP). Jeżeli komputer nie ma przypisanego statycznego adresu IP i nie może go uzyskać w sposób dynamiczny, wtedy sam przypisuje sobie adres z nieużywanego w publicznych sieciach zakresu od 169.254.0.0 do 169.254.255.255. Jeżeli inne komputery w sieci znajdują się w podobnej sytuacji, również przypisują sobie wolne adresy z powyższego zakresu. Dzięki temu komputery mogą komunikować się ze sobą w obrębie lokalnej sieci. Oczywiście ponieważ ich adresy nie są stosowane w publicznych sieciach, nie mogą komunikować się z Internetem ani serwerami spoza lokalnej sieci.

Istota adresacji APIPA polega na tym, że nie wymaga konfiguracji, więc nic więcej na ten temat nie można powiedzieć. W większości systemów Windows funkcjonalność tę można *wyłączyć*, zmieniając klucz w rejestrze. Szczegółowe informacje na ten temat znajdują się w dokumentacji do systemu.

Adresacja APIPA może być przyczyną problemów. Jeżeli komputery uzyskują swoje konfiguracje w prawidłowy sposób, ale jeden z nich dziwnym trafem nie może się komunikować, wtedy trzeba sprawdzić, czy nie utracił łączności z serwerem DHCP i czy nie użył adresacji APIPA do samodzielnego przypisania sobie adresu spoza zakresu stosowanego w sieci.

Nowsza technologia o nazwie **Zeroconf** jest znacznie doskonalsza i całkowicie zautomatyzowana. Stanowi rozszerzenie adresacji IPv4LL i umożliwia w pełni automatyczną konfigurację małych lokalnych sieci. Adresacja Zeroconf zaimplementowana w systemach Apple nosi nazwę Bonjour. W systemach Windows dostępna jest podobna funkcjonalność wykorzystująca nieco inne protokoły. W systemach Linux adresacja ta nosi nazwę Avahi i jest podobna do tej z systemów Apple'a.

Nowa automatyczna adresacja posiada trzy ważne funkcjonalności:

- **Adresacja lokalnego łącza** (ang. *link-local addressing*) — komputery same przypisują sobie adresy IP z zakresu od 169.254.0.0 do 169.254.255.255 (zob. opis IPv4LL wyżej).
- **Rozgłoszeniowe odwzorowywanie nazw** (ang. *Multicast DNS*) — nazwy nie są odwzorowywane za pomocą serwera DNS ani pliku hostów, ale za pomocą zapytań wysyłanych na określony rozgłoszeniowy adres IP i port. Komputery w sieci odbierają te zapytania i odsyłają odpowiedzi zawierające żądane informacje.
- **Wykrywanie usług za pomocą DNS** (ang. *DNS Service Discovery*) — komputery same dowiadują się o dostępnych w sieci usługach.

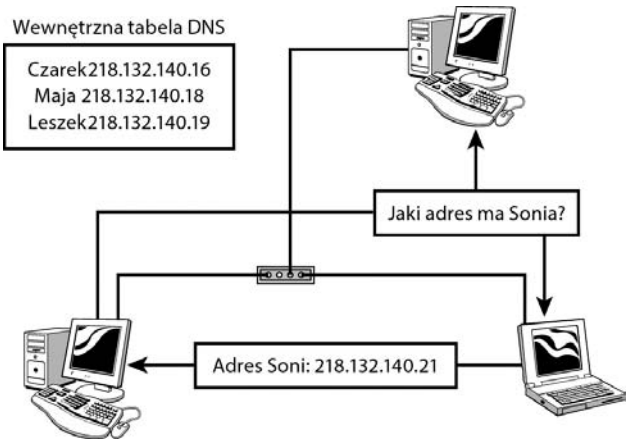
Powyższe funkcjonalności umożliwiają utworzenie środowiska, w którym komputer bez żadnej wstępnej konfiguracji TCP/IP może uzyskać prywatny adres IP, przekazać innym komputerom swoją nazwę i wykryć dostępne usługi (np. serwery plików lub wydruków). Usługi te są dostępne w przeglądarce plików pod nazwą *Otoczenie sieciowe* i można z nich łatwo korzystać, klikając wybraną pozycję.

Gdy pojawiła się potrzeba stworzenia odpowiednika usługi DNS, umożliwiającego korzystanie z usług i urządzeń w prostych sieciach bez konieczności konfigurowania komputerów, jak w przypadku adresacji AppleTalk, firma Apple opracowała technologie uzupełniające funkcjonalności rozgłoszeniowego odwzorowywania nazw i wykrywania usług. Technologie te pozwalają uzyskać wgląd w lokalną sieć, ale nie sprawdzają się w dużych sieciach. Są raczej przystosowane do pojedynczych segmentów LAN.

Komputer obsługujący rozgłoszeniowe odwzorowywanie nazw (mDNS) posiada własną bazę danych, którą wykorzystuje do odwzorowywania nazw. Jak pokazuje rysunek 12.5, gdy komputer musi użyć nazwy, której nie ma w bazie, wtedy rozsyła komunikat na rozgłoszeniowy adres 224.0.0.251. Inne komputery, obsługujące odwzorowywanie mDNS, odbierają zapytania wysyłane na powyższy adres. Komputer, który może odpowiedzieć na zapytanie, wysyła komunikat zawierający adres IP powiązany z daną nazwą.

Funkcjonalność wykrywania usług (DNS-SD) umożliwia komputerom rozgłaszanie informacji o oferowanych przez nich usługach. Popularne dzisiaj małe urządzenia przenośne szeroko korzystają z tej funkcjonalności, dzięki której mogą szybko połączyć się z siecią i wykryć przydane urządzenia, np. drukarki czy serwery muzyczne, bez konieczności uprzedniej konfiguracji.

Wykrywanie DNS-SD polega na przesyłaniu rekordów SRV zawierających informacje o usługach dostępnych w sieci. Na przykład w sieci z konwencjonalną usługą DNS rekord SRV może zawierać nazwę i adres IP serwera FTP lub kontrolera domeny. W wykrywaniu DNS-SD wykorzystywane są na małą skalę odmiany powyższego rekordu i kilku innych.



RYSUNEK 12.5. W usłudze mDNS każdy komputer posiada własną bazę nazw i adresów (w praktyce komputery przesyłają między sobą również inne informacje niezbędne do odwzorowywania nazw)

Na przykład rekord PTR (wykorzystywany do odwzorowywania adresów IP) zawiera informacje o instancjach dostępnych w sieci usług. Odpowiedź na zapytanie może zawierać następujące informacje:

- **Instancja usługi** (możliwy jest przypadek, w którym kilka serwerów w tej samej sieci oferuje tę samą usługę).
- **Nazwa usługi** (lista typów usług jest dostępna na stronie: *http://www.dns-sd.org*).
- **Nazwa domeny**, w której dostępna jest usługa.

Na podstawie odebranych odpowiedzi komputer tworzy listę dostępnych w sieci usług i ich instancji.

Gdy użytkownik lub aplikacja wybierze określoną usługę z listy, wtedy uzyska nazwę hosta i numer portu niezbędne do nawiązania połączenia z serwerem. Ponadto otrzyma rekord TXT zawierający dodatkowe informacje o usłudze.

Wykrywanie usługi opiera się na wysyłaniu rozgłoszeniowych zapytań DNS, dzięki czemu nie jest konieczna konfiguracja tej usługi, ale po wprowadzeniu pewnej minimalnej konfiguracji można z niej korzystać również w sieciach z zaimplementowaną konwencjonalną usługą DNS.

Firma Microsoft opracowała alternatywną do mDNS usługę o nazwie **LLMNR** (ang. *Link-Local Multicast Name Resolution* — lokalne rozgłoszeniowe odwzorowywanie nazw). Protokół **SSDP** (ang. *Simple Service Discovery Protocol* — prosty protokół wykrywania usług) umożliwia wykrywanie usług. Wykorzystuje on jednak protokół HTTP, a nie tradycyjną usługę DNS. Wpisuje się więc w trend tworzenia usług opartych na adresach URL, ale nie jest kompatybilny z konwencjonalną usługą DNS. Protokół UPnP (ang. *Universal Plug and Play* — uniwersalne urządzenie typu „podłącz i korzystaj"), umożliwiający wykrywanie usług podobnie jak w DNS-SD, jest oparty na protokole SSDP.

Microsoft, Apple i inni producenci oprogramowania uczestniczą w otwartej dyskusji na temat automatycznej konfiguracji ustawień TCP/IP, ale ich systemy różnią się od siebie.

Największe różnice są widoczne w protokołach wykrywania usług. Jeszcze inny protokół, SLP (ang. *Service Location Protocol* — protokół lokalizowania usług), jest stosowany w drukarkach HP i wielu innych urządzeniach.

Protokoły automatycznej konfiguracji zostały zdefiniowane w różnych dokumentach RFC, a analogiczny system jest równolegle rozwijany w ramach protokołu IPv6. W ciągu najbliższych lat funkcjonalności automatycznej konfiguracji niewątpliwie będą zyskiwały coraz większą popularność.

Przy okazji

Odmiany adresacji Zeroconf

Fakt, że najwięksi dostawcy systemów operacyjnych oferują własne wersje protokołów, nie oznacza, że w danym systemie można stosować tylko ten akurat protokół. Programiści tworzący aplikacje mogą dowolnie dostosowywać wykorzystywane przez siebie protokoły. Firma Apple opracowała nawet odmianę swojej adresacji Bonjour przeznaczoną dla systemów Windows.

Konfigurowanie ustawień TCP/IP

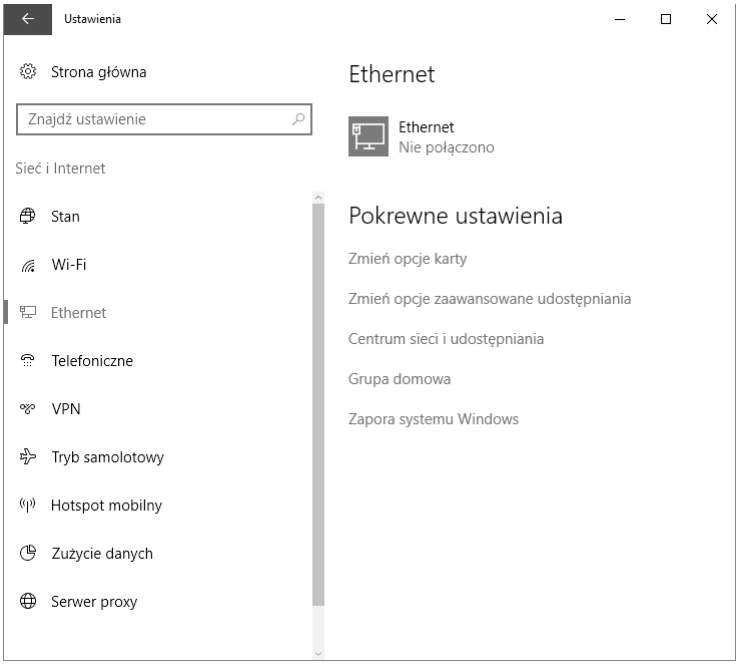
Jak już wspomniałem w tym rozdziale, większość dzisiejszych komputerów wymaga zdefiniowania bardzo prostych ustawień sieciowych, a najczęściej dokonuje się tego, korzystając ze specjalnego kreatora podczas instalacji systemu lub jego pierwszego uruchomienia. Trzeba wtedy określić nazwę komputera, zdecydować, czy ma on posiadać statyczny, czy dynamiczny adres IP, wybrać kilka podstawowych ustawień, a całą resztą zajmie się system. Później jednak może pojawić się potrzeba sprawdzenia ustawień sieciowych, a czasami również ich zmiany. W kolejnych częściach rozdziału opisane są typowe ustawienia TCP/IP w systemach: Windows, macOS i Linux Ubuntu.

Konfiguracji i diagnostyce ustawień sieciowych w powyższych trzech systemach można byłoby z łatwością poświęcić osobną książkę. Poniższe sekcje nie stanowią pełnego podręcznika konfiguracyjnego i diagnostycznego. Ich celem jest dostarczenie ogólnych informacji o konfigurowaniu środowiska sieciowego i pokazanie, jak za pomocą interfejsu graficznego można zmieniać ustawienia protokołów sieciowych. Szczegółowe informacje na temat konfiguracji poszczególnych systemów znajdziesz w dokumentacji i w Internecie.

Windows

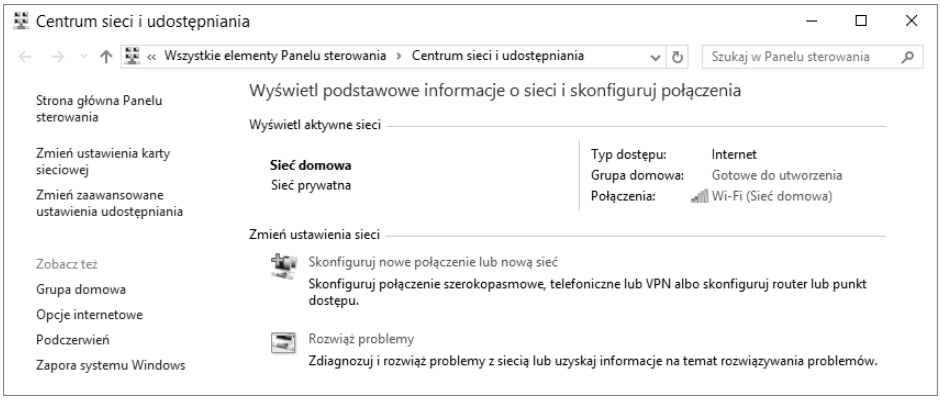
Ustawienia sieciowe w systemie Windows są zapisane w rejestrze. Manipulowanie rejestrem jest niebezpieczną operacją, chyba że wie się dokładnie, co się robi. Dlatego preferowaną metodą konfigurowania ustawień sieciowych jest korzystanie z graficznych narzędzi. Zgodnie z przyjętą w systemie Windows zasadą różnorodne okna dialogowe można otwierać na kilka sposobów. W najnowszych wersjach systemu ustawienia sieciowe są dostępne w narzędziu zwanym *Centrum sieci i udostępniania*. Aby otworzyć to narzędzie w systemie Windows 7, należy kliknąć przycisk *Start* i polecenie *Panel sterowania*. Następnie w głównym oknie panelu należy kliknąć ikonę *Sieć i Internet*, a potem odnośnik *Centrum*

sieci i udostępniania. W systemie Windows 10 po kliknięciu przycisku *Start* trzeba kliknąć ikonę *Ustawienia*. Po wybraniu opcji *Sieć i Internet* pojawią się różne opcje konfiguracyjne (rysunek 12.6).



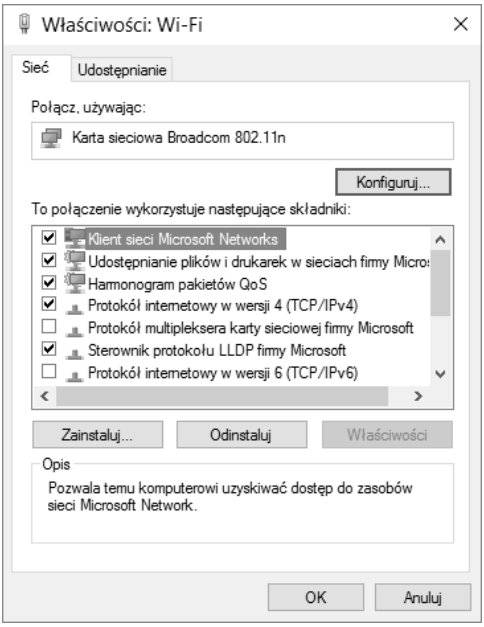
RYSUNEK 12.6. Okno ustawień sieciowych w systemie Windows 10

W górnej części okna *Centrum sieci i udostępniania* (rysunek 12.7) znajdują się bieżące ustawienia sieciowe, a po lewej stronie opcje konfiguracyjne. Aby utworzyć nowe połączenie sieciowe, należy kliknąć odnośnik *Skonfiguruj nowe połączenie lub nową sieć*.



RYSUNEK 12.7. Centrum sieci i udostępniania w systemie Windows 10

W systemie Windows każde połączenie sieciowe jest traktowane jako osobny obiekt. Aby sprawdzić aktualnie skonfigurowane połączenia sieciowe w systemie Windows 7 lub nowszym, należy kliknąć odnośnik *Zmień ustawienia karty sieciowej*. Pojawi się okno zawierające jedną lub kilka ikon reprezentujących połączenia lokalne, bezprzewodowe i inne. Po kliknięciu prawym przyciskiem myszy jednej z ikon i wybraniu polecenia *Właściwości* pojawi się okno z ustawieniami (rysunek 12.8).

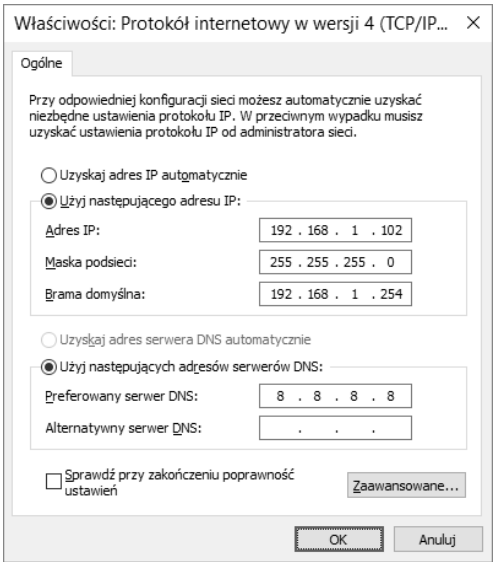


RYSUNEK 12.8. Okno z właściwościami połączenia sieciowego

Jak widać na rysunku 12.8, okno *Właściwości* zawiera listę tzw. *składników* połączenia sieciowego. Słowo „składnik" może wydawać się nieścisłe, ale szybko można się przekonać, że oznacza ono opcjonalny komponent modelu TCP/IP. Trzy pierwsze składniki na rysunku 12.8 należą do warstwy aplikacyjnej modelu TCP/IP.

Aby sprawdzić aktualne ustawienia TCP/IP (przy założeniu, że system wykorzystuje protokół IPv4, jak w ogromnej większości przypadków), kliknij składnik *Protokół internetowy w wersji 4 (TCP/IPv4)*, a następnie przycisk *Właściwości*.

W oknie z właściwościami (rysunek 12.9) można przede wszystkim określić, czy komputer ma uzyskiwać adres IP automatycznie za pomocą protokołu DHCP, czy też ma mieć przypisany adres statyczny. Jeżeli Twój komputer ma ustawione automatyczne uzyskiwanie adresu IP i funkcjonuje prawidłowo, lepiej pozostaw te ustawienia bez zmian. Jeżeli natomiast chcesz ręcznie zmienić ustawienia, kliknij opcję *Użyj następującego adresu IP*, a następnie wpisz adres komputera, maskę i adres bramy domyślnej (muszą to być parametry właściwe dla Twojej sieci; więcej informacji na temat adresów IP i masek znajdziesz w rozdziałach 4., „Warstwa sieciowa", i 5., „Podsieci i adresacja CIDR").



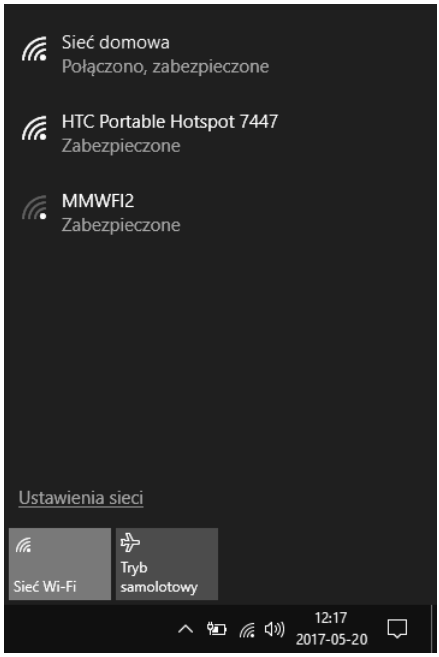
RYSUNEK 12.9. Właściwości protokołu IPv4 w systemie Windows

Przycisk *Zaawansowane* (widoczny na rysunku 12.9) otwiera okno umożliwiające określenie dodatkowych ustawień bramy domyślnej, jak również serwerów DNS i WINS (zob. rozdział 10.).

Zaletą osobnych, logicznych obiektów jest możliwość definiowania osobnych połączeń sieciowych wykorzystywanych w różnych sytuacjach. Jeżeli Twój komputer wykorzystuje protokół DHCP, prawdopodobnie nie ma potrzeby tworzenia dodatkowych połączeń. Wystarczy, że podłączysz komputer do sieci, a swoją konfigurację określi on sam. Jeżeli jednak używasz laptopa, którego podłączasz do różnie skonfigurowanych sieci (np. jednej z zastosowanym protokołem DHCP, a potem innej ze statycznymi adresami IP), wtedy musisz utworzyć osobne połączenia. W tym celu w oknie *Centrum sieci i udostępniania* kliknij polecenie *Skonfiguruj nowe połączenie lub nową sieć*. Otworzy się nowe okno, w którym będziesz mógł uruchomić kreator sieci LAN, sieci bezprzewodowej, szerokopasmowej lub VPN. W każdym przypadku kreator wyszuka niezdefiniowane połączenia i pozwoli Ci wybrać dostępną sieć lub urządzenie.

Jak już wiesz, połączenie bezprzewodowe pod względem funkcjonowania w warstwach wyższych niż sieciowa nie różni się od innego typu połączeń. Jednak ze względu na swój charakter konfigurowanie połączenia bezprzewodowego i korzystanie z niego wygląda nieco inaczej niż w innych połączeniach.

W komputerach z systemem Windows połączenie bezprzewodowe jest zazwyczaj konfigurowane automatycznie. Czasami, w zależności od ustawień, komputer po uruchomieniu może nie łączyć się automatycznie z siecią bezprzewodową. Aby otworzyć listę dostępnych sieci bezprzewodowych, kliknij ikonę połączenia bezprzewodowego znajdującą się w prawym dolnym rogu ekranu. Zaznacz na liście żądaną sieć i kliknij przycisk *Połącz* (rysunek 12.10). Będziesz musiał wpisać niezbędne dane, np. identyfikator SSID (*Service Set Identifier* — identyfikator usługi sieciowej).



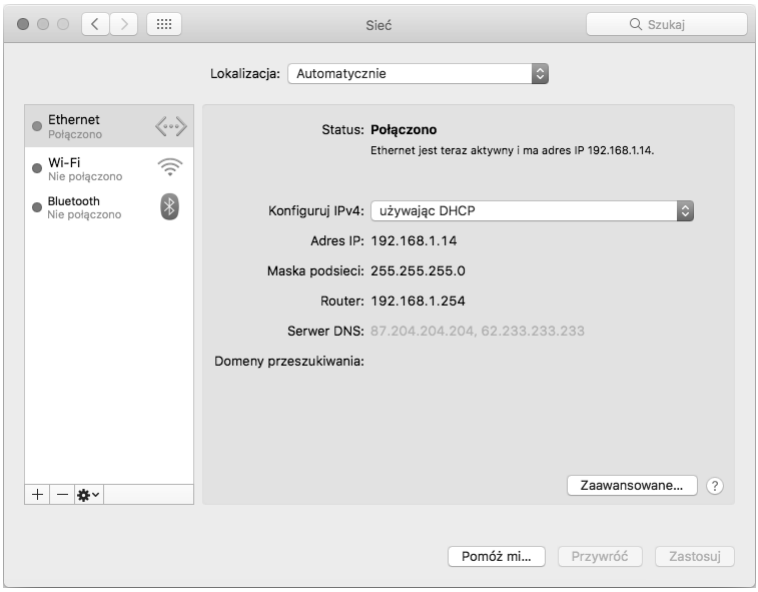
RYSUNEK 12.10. Lista sieci bezprzewodowych w systemie Windows 10

macOS

W systemie macOS, podobnie jak w Windowsie, można w prosty sposób wyszukiwać dostępne sieci przewodowe i bezprzewodowe i łączyć się z nimi, jeżeli jest w nich stosowany protokół DHCP. Aby otworzyć ustawienia sieciowe, kliknij na pasku narzędzi ikonę *Preferencje systemowe*, a następnie ikonę *Sieć*. Okno *Sieć* (rysunek 12.11) jest centralnym miejscem, w którym konfiguruje się ustawienia TCP/IP. Aby zobaczyć ustawienia zwykłego przewodowego połączenia LAN, kliknij na liście sieci po lewej stronie pozycję *Ethernet*.

Kliknij rozwijaną listę *Konfiguruj IPv4* umożliwiającą wybranie protokołu DHCP lub ręczne wpisanie konfiguracji. Jeżeli wybierzesz pozycję *ręcznie*, będziesz mógł wpisać adres IP komputera, maskę i adres bramy domyślnej. Aby wpisać dodatkowe informacje, np. ustawienia serwerów DNS lub WINS, kliknij przycisk *Zaawansowane*. Na koniec kliknij przycisk *Zastosuj*, aby zapisać wprowadzone zmiany.

Aby określić ustawienia sieci bezprzewodowej, kliknij po lewej stronie pozycję *Wi-Fi* (w starszych systemach jest stosowana nazwa *AirPort*). Aby włączyć lub wyłączyć połączenie bezprzewodowe, kliknij przycisk w prawej górnej części okna (rysunek 12.12). W liście *Nazwa sieci* wybierz sieć, z którą chcesz się połączyć. Jeżeli wybierzesz opcję *Przyłącz się do innej sieci*, będziesz musiał podać identyfikator SSID sieci, hasło i inne informacje. Opcja *Sieci komputer-komputer* umożliwia utworzenie połączenia *ad hoc* z innym komputerem wyposażonym w kartę bezprzewodową.



RYSUNEK 12.11. Ustawienia TCP/IP w systemie macOS

RYSUNEK 12.12. Konfiguracja połączenia bezprzewodowego w systemie macOS

Na pasku narzędzi w systemie macOS dostępna jest również ikona umożliwiająca wygodne wybieranie sieci bezprzewodowej i określanie ustawień konfiguracyjnych.

Przy okazji

Wyłączanie sieci Wi-Fi

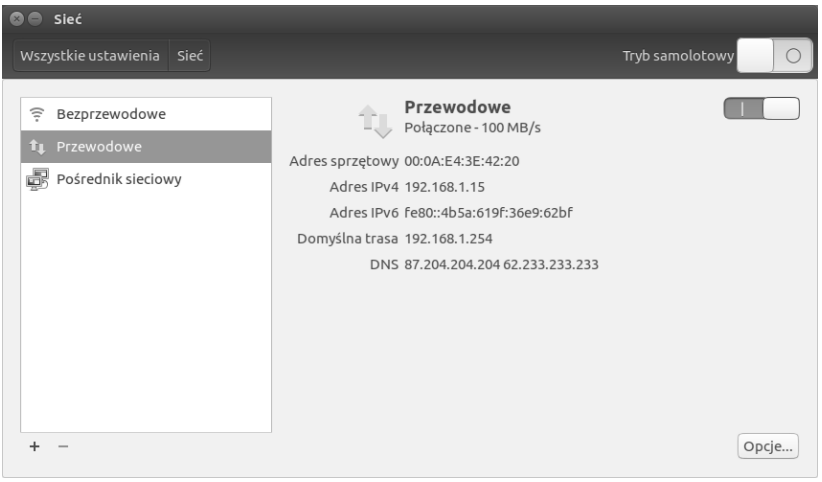
System macOS nie pozwala korzystać z dwóch różnych połączeń sieciowych jednocześnie. Jeżeli zamierzasz eksperymentować z ustawieniami sieci przewodowej i bezprzewodowej, przed wybraniem połączenia Ethernet musisz wyłączyć sieć Wi-Fi. W tym celu w oknie ustawień kliknij przycisk *Wyłącz Wi-Fi*. Sieć Wi-Fi możesz również wyłączyć, klikając ikonę w pasku narzędzi. Sieć będzie wyłączona tak długo, dopóki jej ręcznie nie włączysz. Aby reaktywować połączenie, kliknij je w oknie po lewej stronie. Jeżeli połączenie wykorzystuje protokół DHCP, kliknij przycisk *Zaawansowane*, a następnie przycisk *Odśwież dzierżawę DHCP*.

Linux

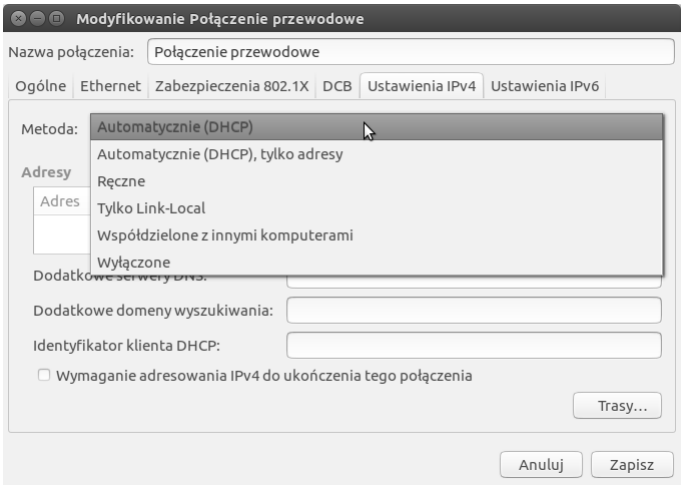
Ubuntu jest popularną odmianą systemu Linux opartą na dystrybucji Debian. W tym systemie wykorzystany jest panel Unity wyglądający nieco inaczej niż w innych dystrybucjach systemu, ale korzysta się z niego w podobny sposób.

Tak jak w systemach Windows i macOS, również w systemie Ubuntu dostępna jest ikona na pasku narzędzi umożliwiająca szybkie uzyskanie dostępu do ustawień sieciowych. Można również kliknąć ikonę *Ustawienia systemu* (przedstawiającą koło zębate i klucz), a następnie ikonę *Sieć* w części *Sprzęt*.

W głównym oknie *Sieć* (rysunek 12.13) można sprawdzić i zmienić ustawienia sieci przewodowej i bezprzewodowej, jak również ustawienia serwera proxy. Aby skonfigurować sieć przewodową, kliknij przycisk *Opcje*. W oknie *Modyfikowanie Połączenie przewodowe* kliknij zakładkę *Ustawienia IPv4*. Za pomocą listy *Metoda* (rysunek 12.14) wybierz dynamiczne przypisywanie adresu IP za pomocą protokołu DHCP lub ręczną konfigurację adresu statycznego. W tej zakładce możesz również wprowadzić dane serwerów DNS, bramy domyślnej i parametry trasowania.

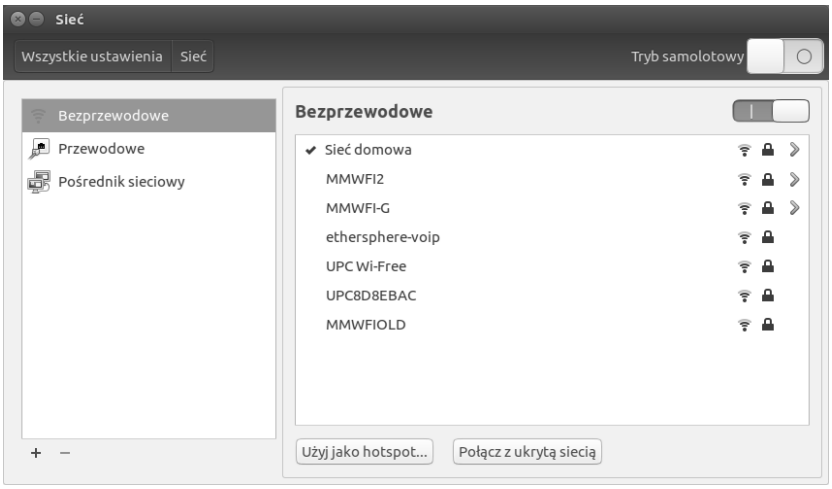


RYSUNEK 12.13. Okno z ustawieniami sieciowymi w systemie Linux Ubuntu



RYSUNEK 12.14. Okno do modyfikowania połączenia sieciowego umożliwiające wybranie automatycznego lub statycznego przypisywania adresu IP

W oknie *Sieć* kliknij w panelu po lewej stronie pozycję *Bezprzewodowe* i otwórz okno z ustawieniami sieci bezprzewodowej (rysunek 12.15). W tym oknie możesz połączyć się z jawną lub ukrytą siecią. Po kliknięciu symbolu strzałki po prawej stronie nazwy sieci otwiera się okno z ustawieniami wybranego połączenia.



RYSUNEK 12.15. Wybierz z listy dostępną sieć bezprzewodową; symbol strzałki po prawej stronie otwiera okno z ustawieniami połączenia

System Linux ma to do siebie, że w jego różnych odmianach (dotyczy to również starszych wersji odmiany Ubuntu) okna konfiguracyjne wyglądają nieco inaczej. Niemniej jednak wszystkie pełnią funkcję interfejsu graficznego służącego do modyfikowania plików konfiguracyjnych. Szczególnie ważny jest plik */etc/network/interfaces* zawierający adresy IP i inne ważne ustawienia.

W powyższym pliku statyczna konfiguracja interfejsu *eth0* (pierwszej karty sieciowej) wygląda następująco:

```
iface eth0 inet static
address 203.121.14.13
netmask 255.255.255.0
gateway 203.121.14.1
```

Wpisy konfigurujące przypisywanie ustawień za pomocą protokołu DHCP wyglądają tak:

```
auto eth0
iface eth0 inet dhcp
```

Plik */etc/network/interfaces* może zawierać wiele innych ustawień. Szczegółowe informacje na ten temat znajdziesz w dokumentacji do systemu Linux.

W systemie Linux, inaczej niż w systemach Windows i macOS, wciąż z powodzeniem jest wykorzystywany wiersz poleceń. Wielu użytkowników woli konfigurować i diagnozować połączenia sieciowe za pomocą narzędzi wiersza poleceń, które poznasz w rozdziale 14.

Z powodu problemów z uzyskiwaniem bieżących informacji o sterownikach sprzętowych i ich funkcjonowaniu w otwartych systemach operacyjnych połączenia bezprzewodowe niekiedy wymagają dodatkowej konfiguracji. Jeżeli używasz systemu Ubuntu, zapoznaj się z przewodnikiem *Ubuntu Wireless Troubleshooting Guide* (podręcznik diagnostyczny do sieci bezprzewodowych w systemie Ubuntu: *https://help.ubuntu.com/community/WifiDocs/WirelessTroubleShootingGuide*). Serwis Linux Wireless Wiki (*http://wireless.wiki.kernel.org*) również jest dobrym źródłem ogólnych informacji o obsłudze sieci bezprzewodowych w systemach Linux.

Podsumowanie

Na początku tego rozdziału został opisany protokół DHCP umożliwiający przypisywanie komputerom adresów IP i innych ustawień sieciowych. Serwer DHCP przydziela komputerom adresy IP (jak również inne ustawienia konfiguracyjne). Protokół DHCP jest dzisiaj tak szeroko stosowany, że w większości sieci stanowi standard. Komputer skonfigurowany tak, aby uzyskiwał dynamicznie adres IP, jest klientem serwera DHCP.

W tym rozdziale została również opisana translacja NAT i protokoły automatycznej konfiguracji. Na koniec przedstawionych zostało kilka przykładów konfigurowania ustawień TCP/IP w systemach Windows, macOS i Linux.

Pytania i odpowiedzi

P.: W jaki sposób komputer użytkownika po uruchomieniu komunikuje się z serwerem DHCP?

O.: Poprzez rozsyłanie i odbieranie komunikatów rozgłoszeniowych.

P. W jaki sposób translacja NAT zwiększa bezpieczeństwo sieci?

O.: Ponieważ lokalne adresy IP nie są powiązane z adresami internetowymi i nie mogą być w tej sieci stosowane, haker z zewnątrz nie może nawiązać połączenia z komputerem w lokalnej sieci. Należy jednak pamiętać, że ta ważna cecha nie gwarantuje pełnego bezpieczeństwa. Haker może zastosować wiele innych technik umożliwiających uzyskanie dostępu do sieci z zastosowaną translacją NAT.

Warsztaty

Poniższe warsztaty składają się z serii pytań i praktycznych ćwiczeń. Pytania mają na celu sprawdzenie Twojej ogólnej wiedzy o tematach opisanych w bieżącym rozdziale. Ćwiczenia praktyczne dadzą Ci możliwość wykorzystania pojęć opisanych w ciągu tej godziny. Zanim przejdziesz do następnego rozdziału, poświęć nieco czasu na rozwiązanie quizu i wykonanie ćwiczeń. Odpowiedzi na pytania znajdziesz w dodatku A, „Odpowiedzi na pytania i rozwiązania ćwiczeń".

Quiz

1. Co należy zrobić, aby komputer użytkownika mógł uzyskiwać adres IP z serwera DHCP znajdującego się w innej sieci?
2. Jakiego rodzaju rekordy są głównie wykorzystywane w usłudze DNS-SD?

Ćwiczenia

Jeżeli Twój komputer nie łączy się z siecią, musisz przede wszystkim odnowić przypisanie adresu IP za pomocą protokołu DHCP. W tym celu, jeżeli używasz systemu macOS, rozwiń główne menu i wybierz polecenie *Preferencje systemowe*. W oknie *Preferencje systemowe* kliknij ikonę *Sieć* (jak w jednej z poprzednich części rozdziału). Następnie wybierz opcję *Ethernet*, jeżeli korzystasz z sieci przewodowej, lub *Wi-Fi* (w starszych wersjach systemu *AirPort*) w przypadku sieci bezprzewodowej.

W oknie konfiguracyjnym będzie widoczny aktualny adres IP. Kliknij przycisk *Zaawansowane*, następnie zakładkę *TCP/IP* i przycisk *Odśwież dzierżawę DHCP*. W zależności od wersji systemu ta procedura może wyglądać inaczej, dlatego jeżeli nie odpowiada powyższemu opisowi, przyjrzyj się dokładnie zawartości okien i poszukaj odpowiedników wyżej wymienionych opcji. Twój komputer powinien usunąć aktualne ustawienia i uzyskać z serwera DHCP nowy adres. (W zależności od serwera DHCP i jego konfiguracji może się zdarzyć, że adres będzie taki sam).

Aby wykonać to samo ćwiczenie w systemie Windows, będziesz potrzebował uprawnień administratora. W celu ich uzyskania kliknij prawym przyciskiem ikonę wiersza poleceń i wybierz opcję *Uruchom jako administrator*. Wpisz hasło administratora, a jeżeli jesteś już zalogowany jako administrator, potwierdź chęć wykonania operacji. Aby sprawdzić bieżący adres IP, w oknie wpisz polecenie:

```
ipconfig
```

Następnie wpisz poniższe polecenie, aby zwolnić przypisany adres IP:

```
ipconfig /release
```

Ponownie wpisz:

```
ipconfig
```

Adres IP powinien zniknąć. Czasami zdarza się, że komputer sam przypisuje sobie lokalny adres z zakresu od 169.254.0.0 do 169.254.255.255.

Wpisz następujące polecenie:

```
ipconfig /renew
```

Jeżeli jeszcze raz wpiszesz polecenie `ipconfig`, zauważysz, że adres IP został przypisany. Więcej na temat tego polecenia i innych narzędzi diagnostycznych dowiesz się z rozdziału 14.

Ważne pojęcia

Poniżej znajduje się lista ważnych pojęć:

- **APIPA (ang. *Automatic Private IP Addressing*)** — technika przypisywania lokalnych adresów stosowana w niektórych wersjach systemu Windows.
- **BOOTP** — protokół pierwotnie stosowany do przypisywania adresów komputerom bez dysków twardych.
- **DHCP (ang. *Dynamic Host Configuration Protocol*)** — protokół dynamicznego przypisywania adresów IP.
- **Klient DHCP** — komputer uzyskujący dynamiczny adres IP za pomocą protokołu DHCP.
- **Serwer DHCP** — komputer przydzielający komputerom użytkowników ustawienia konfiguracyjne TCP/IP za pomocą protokołu DHCP.
- **DNS-SD (ang. *DNS Service Discovery*)** — metoda wykrywania usług stosowana w automatycznie konfigurowanych komputerach.
- **Lokalna adresacja łącza** — metoda automatycznego przypisywania adresów IP.
- **LLMNR (ang. *Link-Local Multicast Name Resolution*)** — alternatywna metoda automatycznego odwzorowywania nazw, opracowana przez Microsoft.
- **Multicast DNS** — technika odwzorowywania nazw bez serwera DNS i bez pliku hostów.
- **SSDP (ang. *Simple Service Discovery Protocol*)** — opracowana przez Microsoft metoda wykrywania usług oparta na protokole HTTP, a nie usłudze DNS. Protokół SSDP jest powiązany z protokołem UPnP.
- **Zeroconf** — zestaw protokołów umożliwiających automatyczną konfigurację ustawień TCP/IP.

Skorowidz

C

D

E

F

G

H

I

J

K

L

Ł

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Ż

Protokół TCP/IP jest podstawą współczesnych technologii sieciowych, a przede wszystkim internetu. Próba rozwiązywania problemów z siecią bez choćby podstawowej wiedzy o TCP/IP prawdopodobnie skończy się porażką. Mimo że ta technologia liczy sobie ponad 30 lat, wciąż jest uważana za kluczową. Założeniem twórców tego protokołu było zbudowanie sieci, która działałaby nieprzerwanie nawet po zniszczeniu części jej fizycznej infrastruktury — i rzeczywiście, internet taki właśnie jest. Niestety, protokół TCP/IP jest dość skomplikowany i wymaga znajomości wielu szczegółów technicznych.

Książka, którą trzymasz w dłoni, została pomyślana jako zwięzły podręcznik składający się z 24 godzinnych lekcji. Znajdziesz tu szczegóły działania protokołów i opis szerokiego spektrum usług dostępnych dziś w internecie. Dowiesz się, jak konfigurować sieci i nimi zarządzać oraz jak rozwiązywać problemy. W obecnym, szóstym już wydaniu znalazły się opisy najnowszych technik, takich jak śledzenie i ochrona prywatności transmisji danych, chmura obliczeniowa, sieci mobilne i internet rzeczy. Zrozumienie prezentowanych treści ułatwią Ci praktyczne przykłady, quizy i ćwiczenia, a także liczne porady i sztuczki niezwykle ułatwiające korzystanie z najlepszych cech TCP/IP.

Najważniejsze zagadnienia ujęte w książce:

- **Standard TCP/IP i jego ewolucja, a także model ISO OSI i warstwy sieci**
- **Bezpieczna transmisja danych**
- **Protokoły IPv4 i IPv6**
- **Protokół TCP/IP w środowiskach chmurowych i IoT**
- **Wydajne strumieniowanie i rozgłaszanie danych**
- **Diagnostyka i rozwiązywanie problemów z siecią komputerową**

Joe Casad — inżynier, który szczególnie interesuje się sieciami komputerowymi i zarządzaniem systemami. Jest również autorem i współautorem kilkunastu książek o tej tematyce. Obecnie ma funkcję redaktora naczelnego pism „Linux Pro Magazine" i „ADMIN Magazine". Wcześniej był redaktorem naczelnym „C/C++ Users Journal" i redaktorem technicznym „SysAdmin Magazine".

Już wkrótce poznasz wszystkie sekrety TCP/IP!

Helion

SAMS

księgarnia internetowa

http://helion.pl

zamówienia telefoniczne

0 801 339900

0 601 339900

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci

ISBN 978-83-283-3708-4

9 788328 337084

Informatyka w najlepszym wydaniu

cena: 79,00 zł