Informatyka w Edukacji, Toruń, 5-7 lipca 2013

Automatyczna konfiguracja interfejsu sieciowego czyli protokół DHCP w praktyce

Mariusz Piwiński
Instytut Fizyki, Wydział Fizyki, Astronomii i Informatyki Stosowanej
Uniwersytet Mikołaja Kopernika
ul. Grudziądzka 5, 87-100 Toruń
Mariusz.Piwinski@fizyka.umk.pl

Abstract: Dynamic Host Configuration Protocol is one of the most popular network protocols which is widely used for automatic configuration of hosts in the Local Area Networks. However, in most cases computer users have a very limited knowledge of its operation, which can lead to many problems with an access to network services. The purpose of this paper is to present and explain the DHCP operation using network protocol analyser software.

1. Wstęp

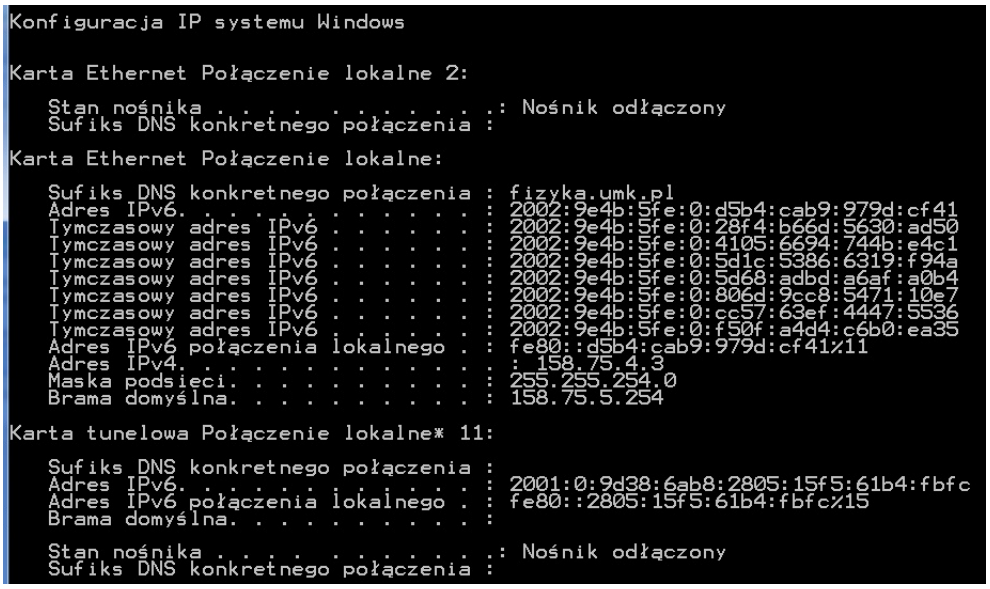
Dynamiczny rozwój Internetu sprawił, iż na przestrzeni ostatnich lat usługi sieciowe stały się nieodzowną częścią naszego życia. Coraz częściej spotykamy się z sytuacjami, w których wiele spraw znacznie łatwiej i szybciej można załatwić w trybie "on-line", niż w tradycyjny sposób. Wygoda związana z łatwością publikowania informacji oraz szerokie możliwości weryfikacji użytkownika sprawiły, iż za pomocą serwisów internetowych, nie tylko dowiadujemy się o bieżących wydarzeniach z kraju i ze świata, ale również korzystamy z usług bankowych, dokonujemy zakupów, a także składamy deklaracje podatkowe. Obecnie coraz więcej firm oraz instytucji realizując swoją działalność zakłada wręcz, iż obsługa klientów realizowana jest w głównej mierze za pośrednictwem odpowiednich usług elektronicznych. Przykładem mogą być tutaj sklepy internetowe, które coraz częściej ograniczają swoje działania do świata wirtualnego, nie posiadając tzw. fizycznych punktów sprzedaży. Rozwiązania oparte na serwisach sieciowych zostały również zastosowane w

sferze edukacji publicznej w postaci systemów wspomagających nauczanie, systemów rekrutacji i zarządzania oraz dzienników elektronicznych.

2. Stos protokołów TCP/IP

Szeroko rozpowszechnione usługi elektroniczne spowodowały, iż obecnie przeciętny użytkownik Internetu pragnie mieć dostęp do globalnej sieci z dowolnego miejsca przy wykorzystaniu możliwie szerokiej gamy urządzeń. Sytuacja ta stała się jedną z przyczyn dynamicznego rozwoju urządzeń mobilnych wykorzystujących różne technologie dostępowe. We współczesnym świecie zasoby sieciowe dostępne są nie tylko przy wykorzystaniu komputerów stacjonarnych, ale również notebooków, netbooków, tabletów, telefonów komórkowych oraz smartfonów. Wszystkie te urządzenia niezależnie od swojego typu oraz zastosowanego systemu operacyjnego posiadają aplikacje, które pozwalają na korzystanie z tych samych serwisów internetowych. Rozwiązania takie są możliwe dzięki praktycznemu wykorzystaniu warstwowych modeli sieci (głównie TCP/IP oraz OSI) pozwalających w pełny sposób opisać proces komunikacji pomiędzy urządzeniami podłączonymi do sieci komputerowej[1]. W wyniku realizacji takiego podejścia, wykorzystanie stosu standaryzowanych protokołów TCP/IP sprawia, iż możliwe jest przesyłanie informacji pomiędzy zupełnie różnymi urządzeniami końcowymi.

Jednym z podstawowych wymogów dotyczących możliwości korzystania z zasobów sieciowych jest prawidłowa konfiguracja interfejsu sieciowego urządzenia. Najczęściej związana jest ona z wykorzystaniem protokołu IP działającym w warstwie trzeciej modelu OSI[2]. Obecnie protokół ten może być wykorzystywany w dwóch wersjach: starszej IPv4 z 32 bitowymi adresami[3] oraz nowej IPv6 wykorzystującej adresy 128 bitowe[4]. Należy zwrócić uwagę, iż systemy operacyjne umożliwiają konfigurację pojedynczego interfejsu sieciowego z zastosowaniem obu protokołów jednocześnie, co związane jest z utworzeniem odpowiednich interfejsów logicznych (Rysunek 1). W przypadku możliwości obsługi komunikacji sieciowej przy wykorzystaniu obu protokołów, protokół IPv6 jest rozwiązaniem preferowanym przez system operacyjny ze względu na możliwość wykorzystania szeregu dodatkowych funkcji.



Rysunek 1 Konfiguracja interfejsu z wykorzystaniem protokołu IPv4 oraz IPv6. Wynik wywołania polecenia *ipconfig* w trybie wiersza poleceń w systemie Windows 7.

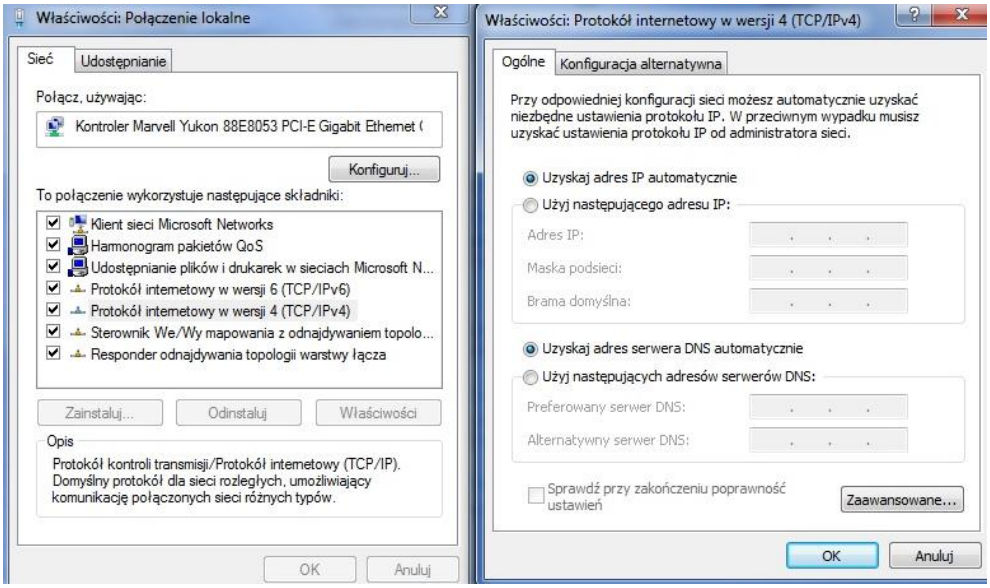
Niestety konfiguracja interfejsu sieciowego z zastosowaniem nowoczesnego protokołu IPv6 nie gwarantuje jeszcze możliwości jego wykorzystania w komunikacji z innymi urządzeniami. W przypadku gdy analizujemy wyłącznie przesyłanie danych w obrębie określonej sieci/podsieci, w której znajduje się skonfigurowany host, warunkiem wystarczającym do uruchomienia nowej komunikacji z wykorzystaniem protokołu IPv6 jest przeprowadzenie poprawnej konfiguracji interfejsów sieciowych interesujących nas urządzeń końcowych. Należy przypomnieć, iż urządzenia końcowe pracujące w jednej sieci/podsieci połączone są ze sobą przełącznikami ethernetowymi (pracującymi w warstwie 2 modelu OSI) lub koncentratorami wieloportowymi (warstwa 1), które nie są w stanie analizować przesyłanych danych na poziomie warstwy trzeciej modelu OSI. Zakładając, iż przeprowadzona konfiguracja hostów nie wpłynie na zamianę wykorzystywanej przez nie technologii dostępowej związanej z warstwą drugą i pierwszą modelu OSI, można stwierdzić, iż opisywane urządzenia pośredniczące zapewnią poprawną obsługę przesyłanych danych bez względu na wykorzystywaną wersję protokołu IP.

W przypadku komunikacji pomiędzy urządzeniami znajdującymi się w różnych sieciach, obsługa datagramów IPv6 dodatkowo wymaga prawidłowej analizy tego protokołu przez wszystkie urządzenia pośredniczące związane z trzecią warstwą modelu OSI, znajdujące się na drodze, którą przesyłane są dane pomiędzy dwoma hostami. Jak widać spełnienie warunku dotyczącego uru-

chomienia prawidłowego routingu pakietów wykorzystujących protokół IPv6 przez urządzenia pośredniczące pracujące w warstwie sieciowej (czyli routery) nie jest już tak oczywiste. W związku z powyższym istnieje cały szereg mechanizmów pozwalających odpowiednio skonfigurowanym routerom na tunelowanie protokołu IPv6 w IPv4 i odwrotnie w celu rozwiązania pojawiających się problemów z obsługą nowego protokołu przez starsze urządzenia sieciowe. Rozwiązania te niosą jednakże ze sobą różne ograniczenia, które ostatecznie sprawiają, iż jak do tej pory stary protokół IPv4 jest nadal częściej wykorzystywany niż nowoczesny IPv6. Sytuacja ta dotyczy zwłaszcza niewielkich sieci oraz podłączonych do nich użytkowników domowych.

3. Konfiguracja interfejsu sieciowego

W sieciach LAN ze względu na wygodę oraz minimalizowanie możliwości wystąpienia potencjalnych błędów administratorzy najczęściej wykorzystują automatyczną konfigurację urządzeń końcowych. Takie podejście wymaga ustawienia automatycznego trybu konfiguracji interfejsów sieciowych urządzeń końcowych oraz uruchomienia odpowiedniej usługi sieciowej.



Rysunek 2 Włączenie dynamicznej konfiguracji interfejsu sieciowego.

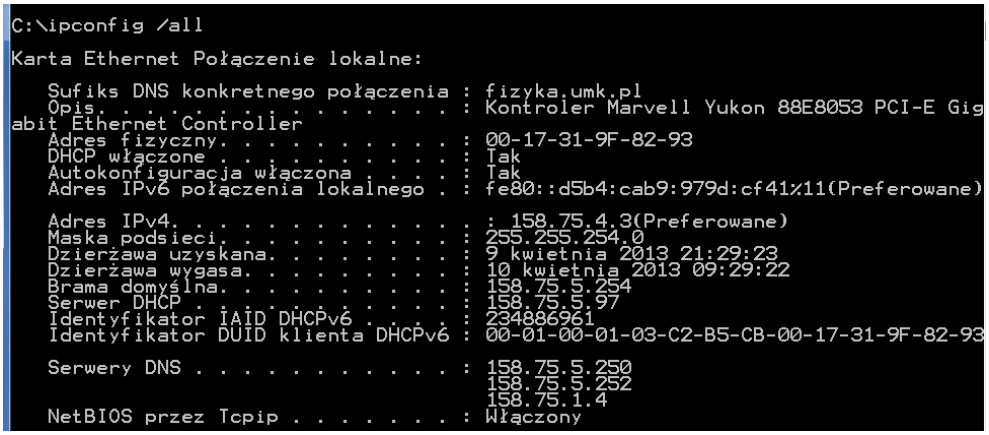
W przypadku urządzeń końcowych opcje dotyczące automatycznej konfiguracji interfejsu sieciowego powiązane są bezpośrednio z zainstalowanymi protokołami TCP/IP. W systemie Windows 7 są one dostępne po wywołaniu okna dialogowego „Właściwości: Połączenia lokalne", a

następnie kliknięciu na przycisku „Właściwości" dotyczącego protokołu IPv4. Po tej czynności uzyskamy dostęp do okna dialogowego umożliwiającego określenie konfiguracji interfejsu sieciowego. W przypadku konfiguracji automatycznej należy zadbać o włączenie opcji „Uzyskaj adres IP automatycznie" (Rysunek 2). Wraz z otrzymywaniem informacji dotyczących adresu IP możemy wybrać również opcję „Uzyskaj adres serwera DNS automatycznie" pozwalającą na automatyczne uzyskanie informacji na temat adresów serwerów DNS. Zatwierdzenie obu okien spowoduje, iż system operacyjny będzie przygotowany do współpracy z serwerem DHCP. Automatyczna konfiguracja interfejsów stała się tak bardzo popularnym rozwiązaniem, iż opisane powyżej opcje obecnie są wartościami domyślnymi większości systemów operacyjnych.

3.1. Problemy z automatyczną konfiguracją interfejsu sieciowego

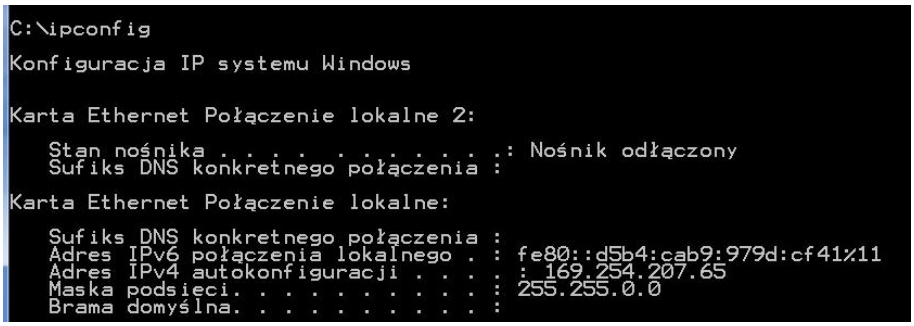
Po zweryfikowaniu ustawień opisywanych w poprzednim paragrafie warto sprawdzić, czy automatyczna konfiguracja interfejsu sieciowego komputera przebiegła w sposób prawidłowy. W tym celu można wykorzystać komendę *ipconfig /all* dostępną w trybie wiersza poleceń (Rysunek 3).

Istnieją jednak sytuacje, w których pomimo przeprowadzenia w sposób prawidłowy wszystkich ustawień przedstawionych na Rysunku 2, interfejs sieciowy nie zostanie automatycznie skonfigurowany. Najczęstszą przyczyną występowania takiego problemu jest brak możliwości wymiany informacji pomiędzy urządzeniem końcowym a serwerem DHCP. Jeżeli problem nie zostanie rozwiązany, po pewnej chwili okaże się, iż mimo braku informacji otrzymanych z serwera DHCP interfejs sieciowy zostanie automatycznie skonfigurowany przez system operacyjny. Wykorzystując znaną już komendę *ipconfig* (Rysunek 4) lub odpowiednie okna dialogowe związane z właściwościami interfejsu, można przeprowadzić weryfikację uzyskanej konfiguracji.



Rysunek 3 Weryfikacja konfiguracji interfejsu sieciowego. Wynik wywołania polecenia *ipconfig /all* w trybie wiersza poleceń.

Po przeprowadzeniu analizy przedstawionych informacji należy stwierdzić, iż uzyskana konfiguracja jest bardzo ograniczona w porównaniu z poprzednio omawianym przypadkiem, gdy interfejs został prawidłowo skonfigurowany (Rysunek 3). Należy zatem zastanowić się dlaczego tym razem konfiguracja interfejsu ograniczona jest tylko do adresu IP 169.254.207.65 z maską 255.255.0.0, a nie zawiera ona informacji o adresie IP bramy, serwera DHCP oraz serwera DNS. Brak informacji dotyczącej adresu IP bramy spowoduje, iż nasz system nie będzie w stanie połączyć się z innymi zasobami znajdującymi się poza siecią posiadającą adres 169.254.0.0 /16. Ponadto brak adresów serwerów DNS uniemożliwi realizację komunikacji z wykorzystaniem nazw domenowych, co powoduje, iż przeglądanie stron WWW staje się praktycznie niemożliwe. Pozostaje zatem pytanie co jest przyczyną takiej nietypowej konfiguracji naszego interfejsu i dlaczego jest ona ograniczona tylko do lokalnej sieci. Aby wyjaśnić te problemy należy przybliżyć działanie protokołu DHCP, z którego funkcji zamierzamy skorzystać.



Rysunek 4 Weryfikacja konfiguracji interfejsu sieciowego przy pomocy komendy *ipconfig /all* przy braku połączenia z serwerem DHCP.

4. Protokoły wykorzystywane do automatycznej konfiguracji hosta

Potrzeba konfiguracji wielu urządzeń pracujących w sieci spowodowała pojawienie się rozwiązań, które umożliwiły zautomatyzowanie tego procesu. Historycznie pierwszym wykorzystywanym w tym celu protokołem był RARP opublikowany w 1984 roku w dokumencie RFC 903[5]. Jego zadaniem było umożliwienie urządzeniom sieciowym uzyskanie adresu IP na podstawie adresu sprzętowego MAC. Jedną z jego wad był fakt, iż protokół ten działał w warstwie drugiej modelu OSI, co oznaczało, iż serwer RARP musiał znajdować się w tej samej sieci co urządzenia z nim współpracujące. Problem ten miał rozwiązać protokół BOOTP (Bootstrap Protocol) opisany w dokumencie RFC 951 w 1985 roku [6]. Jako następca protokołu RARP został on stworzony, aby w oparciu o stos protokołów UDP/IP zapewnić możliwość automatycznej konfiguracji bezdyskowych terminali. Urządzenia te po uzyskaniu swojego adresu IP, adresu serwera oraz nazwy odpowiedniego zasobu miały możliwość pobrania odpowiedniego pliku, załadownia go do pamięci i uruchomienia. Najczęściej rozwiązanie to wykorzystywane jest podczas pobierania zbiorów w oparciu o protokół TFTP, ale możliwa jest również jego współpraca z protokołem FTP i SFTP. Do dnia dzisiejszego pojawiło się kilka aktualizacji tego protokołu, z czego ostatnia opisana została w dokumencie RFC 5494 w 2009 roku[7].

Ze względu na ograniczone funkcje protokołu BOOTP rozpoczęto prace nad jego rozszerzeniami, w wyniku których w 1993 roku zdefiniowano protokół DHCP (*ang. Dynamic Host Configuration Protocol*) opisany w dokumencie RFC 1531 [8]. Umożliwia on przesłanie do klienta informacji dotyczących jego adresu IP, maski, bramy domyślnej, serwerów DNS oraz innych dodatkowych informacji. Istotnym jego elementem jest również czas dzierżawy, po którego wygaśnięciu otrzy-

mane informacje tracą swoją ważność. Oznacza to, iż tak skonfigurowane urządzenie klienckie będzie zmuszone cyklicznie wysyłać zapytania do serwera DHCP w celu uzyskania bieżącej konfiguracji, co daje administratorowi sieci możliwość elastycznego zarządzania posiadaną przestrzenią adresów IP. Na przestrzeni kolejnych lat protokół ten był modyfikowany, aby umożliwić obsługę kolejnych funkcji. Obecnie protokół ten stał się standardem automatycznej konfiguracji urządzeń końcowych w sieciach IPv4.

Wykorzystywanie w sieciach nowej wersji protokołu IPv6 sprawiło, iż pojawiła się naturalna potrzeba wsparcia dynamicznej konfiguracji użytkowników wykorzystujących tą wersję protokołu. Protokół DHCP dla protokołu IPv6 nazywany w skrócie DHCPv6 został opisany w 2003 roku w dokumencie RFC3315[9]. Następnie w tym samym roku w dokumencie RFC 3633 opisano również możliwość obsługi przez protokół DHCPv6 prefiksów zawartych w 128-bitowych adresach IPv6[10]. Dodatkowo w 2004 roku opublikowano dokument RFC 3736, który precyzuje sposób obsługi klientów korzystających z bezstanowego serwisu DHCPv6[11]. W niniejszym opracowaniu przytoczone zostały tylko najważniejsze dokumenty RFC opisujące protokoły umożliwiające automatyczną konfigurację urządzenia użytkownika końcowego. W przypadku próby prześledzenia wszystkich wersji i modyfikacji tych protokołów niezbędną okaże się baza danych dokumentów RFC dostępna pod adresem http://www.rfc-editor.org. Przeszukując bazę dokumentów pod kątem informacji o protokole DHCP możemy otrzymać listę wszystkich dokumentów RFC związanych z tym protokołem. Ich długa lista świadczy, iż protokół ten jest cały czas rozwijany o kolejne funkcje. Z dostępnej on-line bazy dokumentów RFC można dowiedzieć się, że ostatnia modyfikacja dotycząca tego protokołu została opublikowana w lutym 2013 roku pod numerem RFC 6853[12].

5. Protokół DHCP

5.1. Charakterystyka działania DHCP

Protokół DHCP umożliwia realizowanie automatycznej konfiguracji urządzeń sieciowych w oparciu o jeden lub więcej serwerów DHCP. Rozwiązanie to jest bardzo użyteczne nawet w małych sieciach, gdyż pozwala na szybką konfigurację nowo dodanego urządzenia końcowego. Jednocześnie stosunkowo proste zarządzanie usługami serwera DHCP spowodowało, iż obecnie prawie wszystkie routery domowe klasy SOHO wykorzystują tą technologię do przydzielania adresów w sieciach domowych.

Korzystanie z protokołu DHCP wymaga włączenia opisywanej już automatycznej konfiguracji interfejsu hosta oraz uruchomienia serwera DHCP. Wybór automatycznej konfiguracji interfejsu powoduje uruchomienie w systemie usługi klienta DHCP, który wysyła zapytanie do sieci oczekując od serwera DHCP informacji niezbędnych do konfiguracji interfejsu. Serwer DHCP zarządza skonfigurowaną pulą adresów IP, przydzielając odpowiednie numery IP oraz maski kolejnym klientom. Ponadto usługa ta umożliwia przesłanie do klienta informacji na temat takich parametrów jak: brama domyślna, nazwa domeny, adresy serwerów DNS oraz adresy innych serwerów (np. WINS, NTP).

Protokół DHCP stosuje trzy główne metody przydzielania adresów IP:

- **przydział dynamiczny**: urządzenie klienckie otrzymuje adres ze skonfigurowanej puli adresów na określony czas nazywany czasem dzierżawy. Po wygaśnięciu czasu dzierżawy serwer DHCP może odzyskać przydzielony adres i przydzielić go innemu urządzeniu,
- **przydział automatyczny**: serwer DHCP na stałe przydziela wolny adres IP do klienta z przestrzeni adresowej skonfigurowanej przez administratora. Jednocześnie serwer utrzymuje tablicę ostatnio przydzielonych adresów IP powiązanych z adresami MAC dbając o to, aby przy kolejnych żądaniach klient otrzymywał ten sam adres IP,
- **przydział statyczny**: serwer DHCP przydziela adres IP na podstawie tabeli zawierającej zarejestrowane adresy MAC interfejsów sieciowych wraz z odpowiadającymi im numerami IP. Oznacza to, iż tylko urządzenia posiadające zarejestrowany adres MAC mogą otrzymać niezbędne dane do konfiguracji interfejsu,

Protokół DHCP opierając swoje działanie na stosie UDP/IP używa takich samych numerów portów przydzielonych przez organizację IANA (*ang. Internet Assigned Numbers Authority*), jak protokół BOOTP. Oznacza to, że usługa serwera działa na porcie UDP 67, a usługa klienta na porcie UDP 68.

Operacje DHCP można podzielić na cztery podstawowe etapy:

1. ***DHCP discover* (wykrywanie adresacji IP),**

Po uruchomieniu systemu, lub włączeniu automatycznej konfiguracji interfejsu klient DHCP wysyła do sieci zapytanie w celu znalezienia serwerów DHCP. Zapytanie to ma formę

rozgłoszenia z adresem docelowym 255.255.255.255 lub adresem rozgłoszeniowym konkretnej podsieci. W tym procesie w swoim żądaniu klient może umieścić również ostatni przydzielony mu adres IP. Jeżeli klient znajduje się w tej samej sieci co ostatnio przydzielony jemu adres IP, to serwer może udzielić mu zgody na używanie tego adresu. W przypadku, gdy proponowany przez klienta adres nie należy do sieci, w której obecnie znajduje się klient, serwer autorytatywny odrzuci żądanie zmuszając klienta do bezzwłocznego wysłania żądania o nowy adres IP. W przypadku gdy serwer DHCP nie jest autorytatywnym, zignoruje on żądanie klienta, co oznacza, że po przekroczeniu limitu czasu klient wyśle normalne żądanie do serwera, które zostanie obsłużone w standardowy sposób.

2. *DHCP offer* (oferowanie adresacji IP),

W przypadku, gdy serwer DHCP otrzymuje od klienta żądanie dotyczące przydzielenia adresu IP, wyszukuje on w swojej puli wolny adres, rezerwuje go, a następnie wysyła do klienta odpowiedni datagram DHCP OFFER. Wiadomość ta zawiera adres MAC klienta, oferowany adres IP dla klienta, maskę podsieci, czas trwania dzierżawy, adres IP serwera DHCP składającego ofertę oraz dodatkowe opcje takie jak adresy serwerów DNS, czy sufiks DNS.

3. *DHCP request* (żądanie adresacji IP),

W odpowiedzi na oferty serwerów, klient wysyła żądanie DHCP (DHCP REQUEST) w postaci pakietu typu unicast żądając przydzielenia oferowanego adresu. Klient otrzymując oferty z wielu serwerów DHCP, może potwierdzić tylko jedną z nich. Dzięki wartości pola identyfikatora transakcji występującego w żądaniu serwery dowiadują się, która oferta została przyjęta przez klienta. Po otrzymaniu takiej informacji serwery, których oferty nie zostały przyjęte, zwracają zarezerwowany oferowany adres do puli wolnych adresów IP, co oznacza, że może on zostać zaoferowany innemu klientowi. W niektórych przypadkach datagram żądania DHCP wysyłany jest jako pakiet rozgłoszeniowy. Dotyczy to sytuacji, w której klient nie otrzymał jeszcze adresu IP. Jednocześnie taka forma umożliwia innym serwerom poznanie oferty wybranej przez klienta.

4. *DHCP acknowledgement* (potwierdzenie dzierżawy adresacji IP).

W sytuacji gdy serwer DHCP otrzymuje żądanie DHCP REQUEST od klienta, potwierdza on oferowany adres wysyłając datagram DHCP ACK. Pakiet ten zawiera czas dzierżawy oraz wszystkie informacje żądane przez klienta.

W celu usystematyzowania opisanego powyżej sposobu działania protokołu DHCP poniżej przedstawiono sekwencję kolejnych etapów dynamicznej konfiguracji interfejsu sieciowego zawartą w dokumencie RFC 2131. Można wyróżnić tutaj następujące etapy konfiguracji:

- DHCP DISCOVER – klient szuka serwerów DHCP,
- DHCP OFFER – serwery wysyłają swoje oferty do klienta DHCP,
- DHCP REQUEST – klient wysyła żądanie do serwera DHCP,
- DHCP ACK – serwer potwierdza możliwość wykorzystania konfiguracji przez klienta,
- Klient konfiguruje swój interfejs (element może być poprzedzony sprawdzeniem duplikatu adresu IP przy wykorzystaniu protokołu ARP),
- DHCP RELEASE – klient zwalnia adres IP wysyłając taką informację do serwera.

W typowej sytuacji klienci oraz serwery DHCP znajdują się w tej samej sieci, co oznacza, iż nie znając na początku swoich adresów IP, komunikują się wykorzystując ruch rozgłoszeniowy. Po poznaniu swoich wzajemnych adresów, aplikacje te mogą komunikować się za pomocą ruchu typu unicast. W przypadku, gdy serwer DHCP znajduje się w innej sieci niż klienci, lub serwer obsługuje klientów z wielu sieci, to ze względu na początkowe wykorzystywanie ruchu rozgłoszeniowego, do prawidłowego działania tego protokołu wymagane jest uruchomienie dodatkowych usług na routerach takich jak adres pomocniczy (DHCP Helper) lub agenta służącego do przekazywania ruchu rozgłoszeniowego (DHCP Relay Agent)[13].

Włączenie na urządzeniu klienta automatycznej konfiguracji w oparciu o protokół DHCP nie gwarantuje niestety rozwiązania problemu związanego z wystąpieniem dwóch takich samych adresów IP w sieci LAN. Sytuacja taka możliwa jest w przypadku, gdy część użytkowników wykorzystuje dynamiczną, a część statyczną konfigurację interfejsu sieciowego, lub w przypadku gdy w sieci istnieje klika serwerów DHCP oferujących adresy IP z tej samej puli adresowej. W związku z powyższym, aby uniknąć tego typu problemów klient po uzyskaniu potwierdzenia od serwera DHCP może wykorzystać protokół ARP do wykrycia ewentualnych hostów używających adres IP oferowany przez serwer.

Ponadto podczas swojego działania klient DHCP może wysłać do serwera żądanie dotyczące informacji, które nie są standardowo zamieszczane w datagramie DHCP OFFER. Może on również zażądać do serwera DHCP powtórzenia konkretnych informacji. Takie działanie nie wpływa na potrzebę odświeżenia adresu IP klienta, czy też przedłużenia jego czasu dzierżawy. Dodat-

kowe parametry konfiguracyjne, które mogą być przesyłane do klienta za pomocą protokołu DHCP zostały opisane w dokumencie RFC 2132.

Standardowa specyfikacja protokołu DHCP nie przewiduje mechanizmu autentykacji, co powoduje podatność tego protokołu na różnego rodzaju ataki sieciowe. Ze względu na potrzebę rozwiązania tego problemu podjęto prace nad zabezpieczeniem protokołu DHCP. Rozwiązania takie zaproponowano w dokumentach RFC 3118 oraz 3046.

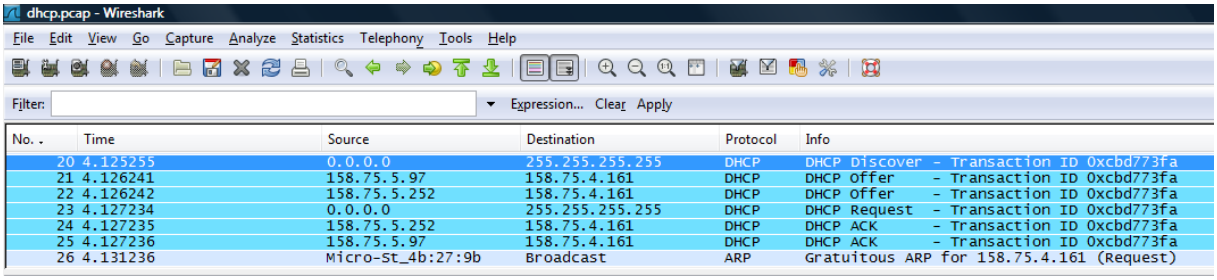
W celu zapewnienia maksymalnego wykorzystania puli adresowej protokół DHCP umożliwia również zwolnienie adresu IP przez klienta. Jednakże ze względu na fakt, iż trudno jest jednoznacznie określić czas po którym użytkownik przestaje korzystać z dostępu do sieci specyfikacja protokołu DHCP nie wymaga zwalniania adresu IP przez klienta.

6. Konfiguracja karty sieciowej z użyciem adresu IPv4 z zakresu Link-Local Addresses

W przypadku, gdy klient DHCP nie nawiąże komunikacji z serwerem DHCP, można zauważyć, iż interfejs klienta będzie miał przypisany adres IP 0.0.0.0 z maską 0.0.0.0. Ze względu na fakt, iż urządzenia sieciowe takie jak np. drukarka sieciowa nie zawsze wymagają realizacji połączenia z siecią zewnętrzną, a głównie mają obsługiwać urządzenia lokalne, możliwym jest ich automatyczna konfiguracja bez wykorzystania serwera DHCP. Oznacza to, iż w przypadku włączenia dla nich opcji automatycznej konfiguracji z wykorzystaniem serwera DHCP oraz braku możliwości uzyskania prawidłowej konfiguracji z serwera DHCP, urządzenia te same przypiszą sobie adres z sieci 169.254.0.0 /16. Jednocześnie wykorzystując protokół ARP są one w stanie zapewnić niepowtarzalność wykorzystywanych adresów w obrębie swojej sieci lokalnej. Takie rozwiązanie oczywiście nie pozwala na pełne wykorzystanie zasobów sieciowych, zwłaszcza tych zdalnych, ale umożliwia wykorzystywanie zasobów lokalnych w przypadku awarii serwera DHCP. W związku z powyższym opisywana poprzednio w rozdziale 3.1 „ograniczona konfiguracja" interfejsu dotyczy właśnie takiej sytuacji. W przypadku, gdy serwer DHCP zacznie działać prawidłowo i urządzenia końcowe będą mogły nawiązać z nim połączenie i cała sytuacja automatycznie powróci do normy. Rozwiązanie to zostało opisane w 2005 roku w dokumencie RFC 3927, który definiuje adresy lokalnego łącza (*ang. Link-Local Adresses*) należące do sieci 169.254.0.0/16. Pakiety z takimi adresami, tak jak z adresami prywatnymi, zgodnie z zaleceniami nie powinny być obsługiwane w Internecie, co ma zostać zapewnione poprzez ich odfiltrowywanie na granicy sieci[14].

7. Badanie dynamicznej konfiguracji urządzeń realizowanej w oparciu o protokół DHCP

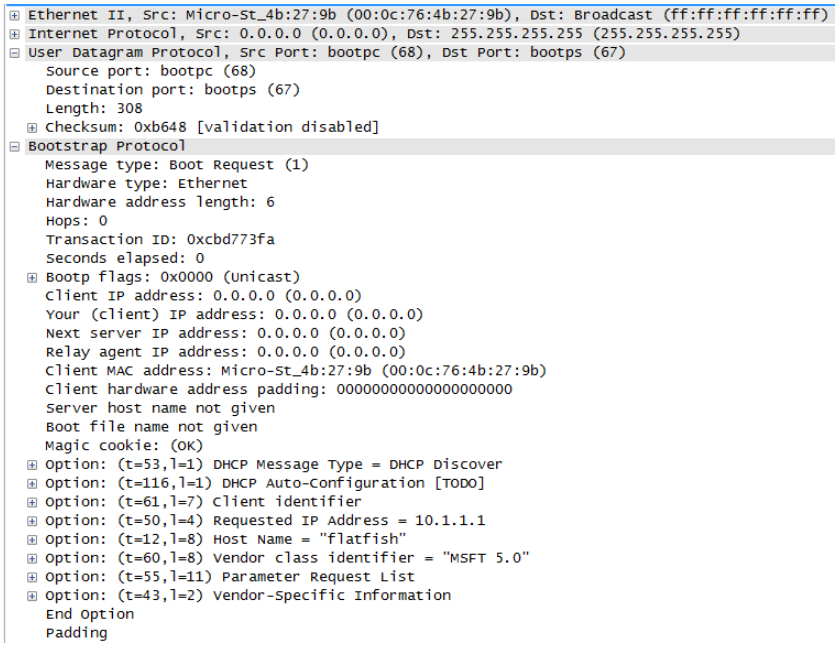
Znając już charakterystykę protokołu DHCP należy podjąć próbę interpretacji poszczególnych etapów jego działania w oparciu o analizę danych przesyłanych pomiędzy klientem a serwerem DHCP. Rysunek 5 przedstawia transmisję przechwyconą za pomocą programu Wireshark dotyczącą protokołu DHCP.



Rysunek 5 Transmisja związana z konfiguracją interfejsu za pomocą protokołu DHCP.

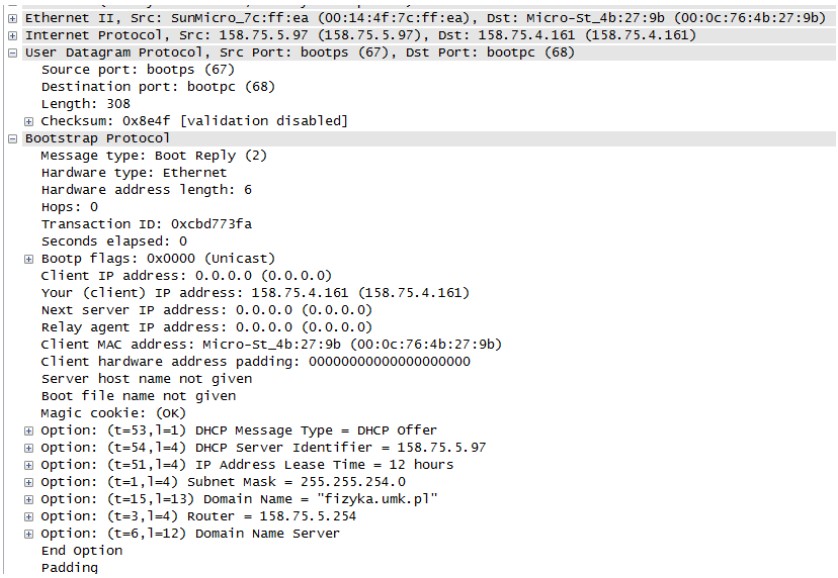
Czytelników, którzy nie posiadają wcześniejszych doświadczeń z analizą przesyłanych danych przy wykorzystaniu programu Wireshark, zachęcam do zapoznania się licznymi przykładami znajdującymi się na stronie www.wireshark.org lub też innymi opracowaniami na ten temat (np. M. Piwiński „Praktyczna analiza sieci komputerowych z wykorzystaniem programu Wireshark” [15]).

Postarajmy się teraz prześledzić w sposób bardziej szczegółowy kolejne etapy uzyskiwania danych przez klienta DHCP. Jak pamiętamy w pierwszej kolejności wysyła on rozgłoszenie poszukując serwerów DHCP. Komunikacja realizowana jest za pomocą protokołu UDP, gdzie port klienta ma wartość 68, a port serwera 67 (Rysunek 6). Jak widać klient w swoim zapytaniu umieścił swój adres MAC, oraz proponowany ostatnio używany adres IP 10.1.1.1.



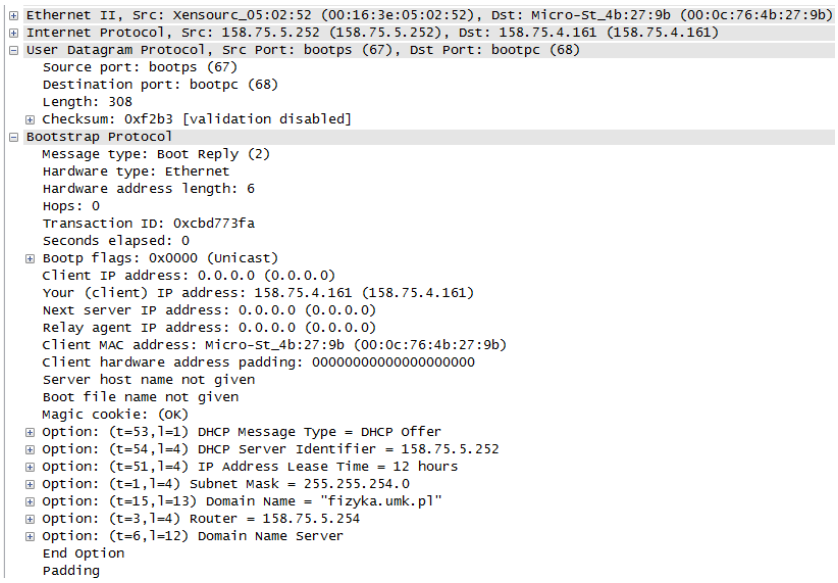
Rysunek 6 Pakiet DHCP Discover.

Kolejny pakiet jest odpowiedzią z serwera o adresie IP 158.75.5.97 (DHCP Offer), która zawiera komplet żądanych informacji (Rysunek 7). Należy zwrócić uwagę, iż realizowana transmisja jest typu unicast, czyli w swoich założeniach ma trafić tylko do klienta.



Rysunek 7 Pakiet DHCP Offer wysłany z serwera 158.75.5.97.

Jak się okazuje w sieci, do której podłączony jest klient istnieją dwa serwery DHCP, stąd widoczna jest również oferta serwera 158.75.5.252 (Rysunek 8). Oba serwery skonfigurowane w identyczny sposób oferują klientowi ten sam zestaw danych.



Rysunek 8 Pakiet DHCP Offer wysłany z serwera 158.75.5.252.

W związku z powyższym klient odpowiada na te oferty swoim żądaniem wysyłanym w postaci rozgłoszenia (Rysunek 9).

```
⊞ Ethernet II, Src: Micro-St_4b:27:9b (00:0c:76:4b:27:9b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊟ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
    Length: 325
  ⊞ Checksum: 0x1e44 [validation disabled]
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xcbd773fa
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Micro-St_4b:27:9b (00:0c:76:4b:27:9b)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Request
  ⊞ Option: (t=61,l=7) Client identifier
  ⊞ Option: (t=50,l=4) Requested IP Address = 158.75.4.161
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 158.75.5.97
  ⊞ Option: (t=12,l=8) Host Name = "flatfish"
  ⊞ Option: (t=81,l=12) Client Fully Qualified Domain Name
  ⊞ Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  ⊞ Option: (t=55,l=11) Parameter Request List
  ⊞ Option: (t=43,l=3) Vendor-Specific Information
    End Option
```

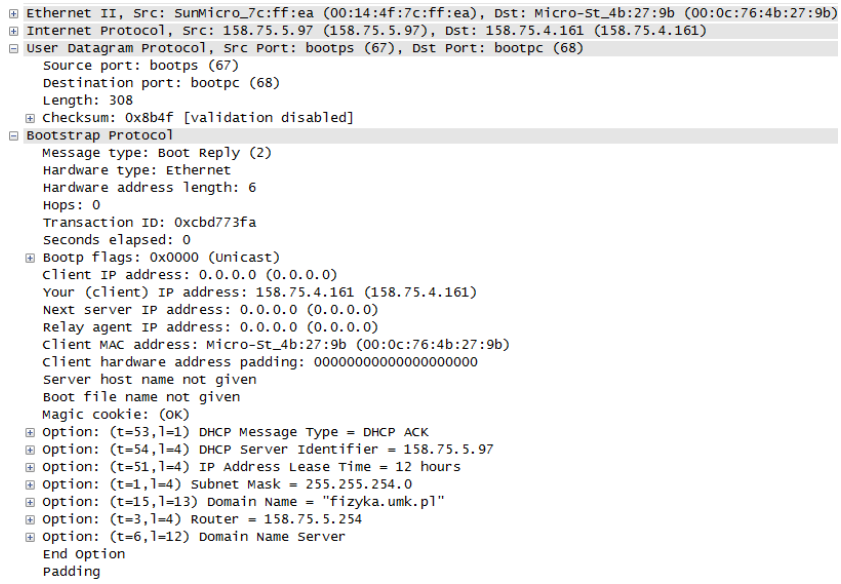
Rysunek 9 Pakiet DHCP Request.

Kolejny krok polega na wysłaniu przez serwer DHCP potwierdzenia informującego o przydzieleniu klientowi adresu IP 158.75.4.161. W tym przypadku informację taką wysyła serwer 158.75.5.252 (Rysunek 10).

```
⊞ Ethernet II, Src: Xensourc_05:02:52 (00:16:3e:05:02:52), Dst: Micro-St_4b:27:9b (00:0c:76:4b:27:9b)
⊞ Internet Protocol, Src: 158.75.5.252 (158.75.5.252), Dst: 158.75.4.161 (158.75.4.161)
⊟ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
    Source port: bootps (67)
    Destination port: bootpc (68)
    Length: 308
  ⊞ Checksum: 0xefb3 [validation disabled]
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xcbd773fa
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 158.75.4.161 (158.75.4.161)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Micro-St_4b:27:9b (00:0c:76:4b:27:9b)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP ACK
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 158.75.5.252
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 12 hours
  ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.254.0
  ⊞ Option: (t=15,l=13) Domain Name = "fizyka.umk.pl"
  ⊞ Option: (t=3,l=4) Router = 158.75.5.254
  ⊞ Option: (t=6,l=12) Domain Name Server
    End Option
    Padding
```

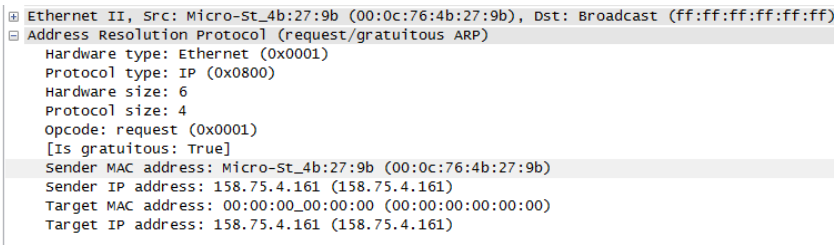
Rysunek 10 Pakiet DHCP ACK wysłany z serwera 158.75.5.252.

Oba serwery wysłały identyczną ofertę DHCP, a klient odpowiedział pakietem rozgłoszeniowym, w związku z powyższym serwer 158.75.5.97 również odpowiada swoim potwierdzeniem (Rysunek 11). Należy zwrócić uwagę, iż pakiety przesyłane z obu serwerów są pakietami typu unicast.



Rysunek 11 Pakiet DHCP ACK wysłany z serwera 158.75.5.97.

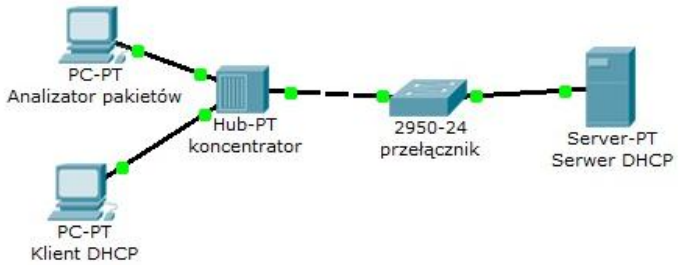
Ostatnim etapem realizowanym przez system operacyjny przed konfiguracją interfejsu jest sprawdzenie, czy w lokalnej sieci nie znajduje się host używający obecnie oferowanego adresu IP 158.75.4.161. W związku z powyższym klient wysyła w postaci rozgłoszenia zapytanie ARP zawierające adres 158.75.4.161 (Rysunek 12). Należy zwrócić uwagę, iż w tym przypadku pola protokołu ARP „Sender IP address" i „Target IP address" mają taką samą wartość, czyli badany adres IP. Brak odpowiedzi oznacza, iż w lokalnej sieci nie istnieje urządzenie posiadające badany adres, a zatem nie pojawi się problem duplikatu adresu IP. W związku z powyższym klient konfiguruje swój interfejs sieciowy z otrzymanymi od serwera DHCP informacjami, tym samym kończąc cały proces.



Rysunek 12 Pakiet ARP request/gratuitous.

7.1. Realizacja badań dotyczących zachowań protokołu DHCP

W celu samodzielnego przeprowadzenia testów oraz obserwacji umożliwiających bliższe poznanie protokołu DHCP należy wykorzystać przynajmniej dwa komputery, w których w dowolny sposób będziemy mogli modyfikować konfigurację interfejsu sieciowego. Ponadto niezbędny jest również dostęp do urządzenia zapewniającego usługę serwera DHCP. W celu analizy transmitowanych danych należy wykorzystać program pozwalający na przechwytywanie pakietów docierających do wybranego interfejsu sieciowego. Jednym z najbardziej znanych programów tego typu jest Wireshark dostępny na stronie www.wireshark.org. Ze względu na fakt, iż najczęściej podczas konfiguracji interfejsu sieciowego nie jest on dostępny dla uruchomionych w systemie operacyjnym programów, przechwytywanie ruchu najlepiej zrealizować za pomocą drugiego komputera podłączonego do tej samej sieci. Należy przy tym pamiętać, iż badany protokół wykorzystuje zarówno ruch rozgłoszeniowy jak i ruch typu unicast, co oznacza, że podłączając oba komputery do tego samego przełącznika będziemy mogli analizować tylko ruch rozgłoszeniowy. Zatem w przypadku gdy zastosowany przełącznik nie jest w stanie realizować funkcjonalności typu Port Mirroring (kopiowanie ramek na wybrany port) problem ten można rozwiązać podłączając oba komputery do jednego koncentratora wieloportowego, który następnie zostanie podłączony do przełącznika. Rozwiązanie takie sprawi, iż oba komputery zawsze będą otrzymywały dokładnie takie same pakiety, co pozwoli na pełną analizę przesyłanych danych. Jednocześnie w takiej topologii bardzo łatwo jest również symulować problemy związane z nawiązywaniem połączenia z serwerem DHCP poprzez fizyczne rozłączanie połączenia pomiędzy koncentratorem a przełącznikiem ethernetowym (Rysunek 13). Niniejsze rozwiązanie umożliwia łatwe przeprowadzenie badania protokołu DHCP opisanego w niniejszej pracy oraz wykonanie szeregu innych testów związanych z problemami automatycznej konfiguracji interfejsu.



Rysunek 13 Topologia logiczna sieci wykorzystywanej do przeprowadzenia badania sposobu działania protokołu DHCP.

8. Podsumowanie

Celem niniejszego opracowania było przybliżenie czytelnikom sposobu działania protokołu DHCP, który obecnie stanowi podstawę mechanizmu automatycznej konfiguracji interfejsów sieciowych urządzeń końcowych. Zaproponowana analiza przesyłanych danych pomiędzy klientem a serwerem DHCP pozwala na lepsze poznanie i zrozumienie różnych aspektów wykorzystania badanego protokołu, co w konsekwencji umożliwia optymalizację jego działania. Ponadto zdobyta w ten sposób wiedza praktyczna staje się kluczowa podczas rozwiązywania różnych problemów związanych z automatyczna konfiguracją interfejsów sieciowych.

Literatura

1. M. Piwiński, „Uczniowie i komputery w sieci...", „Komputer w Szkole", nr 5, (2003), s 38, http://repozytorium.umk.pl/handle/item/1667
2. M. Piwiński, Internet - wybrane aspekty bezpieczeństwa, IX Konferencja Informatyka w Edukacji, Toruń, 3-4 lipca 2012, http://repozytorium.umk.pl/handle/item/1712
3. http://www.ietf.org/rfc/rfc791.txt
4. http://tools.ietf.org/html/rfc3513
5 . http://tools.ietf.org/html/rfc903
6 . http://tools.ietf.org/html/rfc951
7 . http://tools.ietf.org/html/rfc5494
8 . http://tools.ietf.org/html/rfc1531
9. http://www.ietf.org/rfc/rfc3315.txt
10 . http://www.ietf.org/rfc/rfc3633.txt
11 . http://tools.ietf.org/html/rfc3736
12 http://www.rfc-editor.org
13 . http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
14 . http://www.ietf.org/rfc/rfc3927.txt
15 . Piwiński, „Praktyczna analiza sieci komputerowych z wykorzystaniem programu Wireshark", „Informatyka w Edukacji, V", A.B. Kwiatkowska, M. Sysło, (2008) 277 285, http://repozytorium.umk.pl/handle/item/1686