KOMUNIKACJA SIECIOWA Z WYKORZYSTANIEM PROTOKOŁU IPV6

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

Abstract. IPv4 is one of the most popular protocol used in global communication. However, due to its limitations, addressing pool exhaustion and rapid growth of the number of various devices connected to the Internet, the new version of Internet Protocol was introduced. The TCP/IP dual stack technique applied in modern operating systems enables running both IPv4 and IPv6 at the same time, which is very important in transitional period. This paper shows new ideas of IPv6, presents advantages and differences between both protocols.

1. Wstęp

W ostatnich latach obserwowany jest bardzo dynamiczny rozwój technologii informatycznych oraz związanych z nimi różnych usług sieciowych. Sieć Internet już dawno przestała być utożsamiana tylko z serwisami informacyjnymi, a stała się globalną platformą służącą do wymiany różnego rodzaju informacji wykorzystywanych zarówno w pracy zawodowej jak i w życiu prywatnym. W efekcie coraz więcej osób nie wyobraża sobie funkcjonowania w społeczeństwie bez możliwości korzystania z portali społecznościowych, poczty elektronicznej czy też komunikatorów, co znacząco wpłynęło również na rozwój mobilnych technologii szerokopasmowych. Uruchomienie rozwiązań umożliwiających szybkie przesyłanie danych w sieciach GSM (np. protokoły HSPA+, HSDP czy LTE) spowodowało, iż obecnie telefony komórkowe częściej wykorzystywane są do obsługi portali społecznościowych niż wykonywania klasycznych połączeń telefonicznych. Ponadto wyposażenie telefonów w interfejsy pracujące w standardzie IEEE 802.11 pozwala na podłączanie tych urządzeń do globalnej sieci za pomocą lokalnych sieci bezprzewodowych WLAN.[6] Oznacza, to iż w takim przypadku użytkownik może korzystać z istniejącej infrastruktury sieciowej

niezależnie od wybranego operatora telekomunikacyjnego, co znacząco wpływa na obniżenie kosztów związanych z transmisją danych. Co więcej, telefon taki standardowo wykorzystywany w sieci GSM po podłączeniu do sieci lokalnej WLAN może jednocześnie stać się telefonem IP dostępnym zarówno z poziomu sieci lokalnej jak i rozległej.

Powszechność i dostępność sieci Internet została również wykorzystana przez producentów kontrolerów, sterowników, czujników, a nawet sprzętu RTV i AGD. W interfejsy sieciowe wyposażane są układy odpowiadające za sterowanie oświetleniem, monitoringiem, ogrzewaniem, telewizory, odtwarzacze audio-wideo, głośniki, a nawet kuchenki elektryczne oraz pojedyncze żarówki.[4] Obserwowany proces polegający na podłączaniu do sieci coraz to nowych niezależnych, jednoznacznie identyfikowanych urządzeń, które mogą gromadzić, przetwarzać lub wymieniać między sobą informacje został opisany przez Kevina Ashtona w 1999 roku jako Internet Rzeczy (*ang. Internet of Things*).[18] Zjawisko wydaje się być znacznie szersze, dlatego firma Cisco zaproponowała nowy termin: Internet Wszechrzeczy (*ang. Internet of Everything – IoE*) obejmujący oddziałujące ze sobą poprzez sieć cztery elementy: ludzi, dane, procesy oraz rzeczy. W środowisku IoE definiuje się trzy typowe sposoby wymiany informacji:

- komunikacja ludzi z ludźmi (P2P),
- komunikacja maszyn z ludźmi (M2P),
- komunikacja maszyn z maszynami (M2M).

Wzajemne interakcje między tymi elementami generują bardzo wiele danych, których odpowiednie uporządkowanie, przetworzenie i wykorzystanie prowadzi do stworzenia coraz to nowych funkcjonalności. Już dzisiaj produkowane są drukarki sieciowe, które w automatyczny sposób mogą zamawiać w sklepie brakujący toner, zatem nie stoi nic na przeszkodzie, aby wyprodukować lodówki, które w sposób automatyczny nie tylko będą tworzyły listę brakujących produktów, ale również przekazywały ją do realizacji w sklepie internetowym. Jak widać dodanie interfejsu sieciowego do dobrze znanych nam urządzeń umożliwia znaczne rozszerzenie ich funkcji.

Obecnie szacuje się, iż do sieci podłączonych jest około 20 mld urządzeń, a do roku 2020 liczba ta wynosić będzie 50 mld. Stanowić to będzie 2,7% wszystkich urządzeń („rzeczy") na świecie. Ilość ta wpłynie znacząco na obniżenie kosztów podłączania urządzeń do sieci, ale spowoduje pojawienie się szeregu problemów związanych z ich obsługą i zarządzaniem.[1] Należy zauważyć, iż z punktu widzenia sieci komputerowych traktowane są one jako pełnoprawne urządzenia końcowe, a co za tym idzie muszą posiadać jednoznaczny identyfikator umożliwiający ich rozróżnienie.

Zatem samo jednoznaczne określenie tych identyfikatorów dla tak dużej liczby urządzeń może stanowić już dosyć poważny problem.

2. Protokół IPv4 i jego ograniczenia

Obecnie najczęściej stosowanym zestawem protokołów w komunikacji sieciowej jest stos TCP/IP. Protokołem wchodzącym w jego skład umożliwiającym jednoznaczne rozróżnienie urządzeń w całej sieci Internet jest protokół IPv4 (*ang. Internet Protocol*) opisany w dokumencie RFC 791 opublikowany w 1981 roku.[7] Zakłada on, iż każde urządzenie posiada niepowtarzalny 32-bitowy adres, który jest nadawany w procesie konfiguracji interfejsu sieciowego. Najczęściej przedstawiany jest on w postaci czterech oktetów w notacji dziesiętnej oddzielonych kropkami (np. 156.26.12.1). W adresie tym zawarty jest zarówno identyfikator sieci, w której pracuje dane urządzenie końcowe jak i identyfikator jego interfejsu sieciowego. Dzięki tak zdefiniowanej hierarchiczności protokół ten umożliwia odnalezienie i przesłanie danych do dowolnego urządzenia (tzw. hosta) obsługiwanego w sieci Internet.[5] Analizując liczbę dostępnych bitów można zauważyć, iż teoretycznie dzięki takiemu schematowi możemy zaadresować maksymalnie 2^{32}= 4294967296 urządzeń. Pierwotnie protokół IP przewidywał, iż pierwszy oktet adresu IP opisywać będzie adres sieci, a pozostałe trzy oktety określać będą adres hosta. Jednakże w celu lepszego zarządzania pulami adresowymi w zależności od wielkości obsługiwanych sieci zdecydowano się na podział przestrzeni adresowej na trzy klasy adresowe przeznaczone do adresacji hostów (klasa A, B, C). Z klasami tymi związane zostały maski pozwalające na określenie jaka część adresu IP opisuje sieć, a jaka interfejs hosta. Z klasą A związana jest maska 255.0.0.0, z klasą B maska 255.255.0.0, a z klasą C maska 255.255.255.0. Pozostałe dwie pule adresów zostały zarezerwowane dla komunikacji grupowej (*ang. multicast,* klasa D), oraz do celów testowych (klasa E). Ponadto grupę adresów 127.0.0.0 z maską 255.0.0.0 przeznaczono do testowania wewnętrznej pętli zwrotnej interfejsu sieciowego, a adres 255.255.255.255 określono jako adres rozgłoszeniowy wykorzystywany do adresowania pakietu, który ma zostać dostarczony do wszystkich hostów z danej sieci. Klasowy podział przestrzeni adresowej IPv4 przedstawia Tabela 1.

Tabela 1 Klasowy podział przestrzeni adresowej IPv4.

Klasa adresowa	Adres początkowy	Adres końcowy	Liczba sieci	Liczba wszystkich adresów w sieci
Klasa A	0.0.0.0	127.255.255.255	128 (2^7)	16.777.216 (2^{24})
Klasa B	128.0.0.0	191.255.255.255	16.384 (2^{14})	65.536 (2^{16})
Klasa C	192.0.0.0	223.255.255.255	2.097.152 (2^{21})	256 (2^8)
Klasa D	224.0.0.0	239.255.255.255	Adresy grupowe	nie dotyczy
Klasa E	240.0.0.0	255.255.255.255	Adresy zarezerwowane	nie dotyczy

Wraz ze wzrostem ilości sieci komputerowych oraz zwiększającą się ilością urządzeń podłączanych do sieci okazało się, iż sztywny podział zakresów adresowych powoduje szybkie wyczerpywanie się dostępnych adresów IP. Zauważmy, iż przy takim podejściu sieci, które miały obsługiwać 500 hostów otrzymywały adres klasy B, co oznaczało przydzielenie im puli liczącej ponad 65 tysięcy adresów. W celu lepszego zarządzania przestrzenią adresową zdecydowano się zrezygnować z klas adresowych na rzecz technologii CIDR (*ang. Classless Inter-Domain Routing*), czyli tzw. bezklasowego routingu międzydomenowego opisanego w dokumentach RFC 1518 [8] oraz RFC 1519.[9] Pozwala ona na przydzielanie sieciom przestrzeni adresowej z dokładnością do jednego bitu w masce, co oznacza, iż sieć obsługująca 500 hostów może otrzymać pulę adresową z maską 255.255.254.0 (zapisywaną też w postaci prefiksu /9), definiującą 2^9=512 adresów IP. Ze względu na zarezerwowany pierwszy (adres sieciowy) i ostatni adres (adres rozgłoszenia w danej sieci), do konfiguracji interfejsów sieciowych pozostaje 510 adresów. Problem z dopasowaniem przestrzeni adresowych dotyczył nie tylko sieci, ale również podsieci tworzonych w celu lepszego zarządzania ruchem danych oraz realizowania dedykowanych połączeń pomiędzy routerami. W związku z powyższym, aby móc tworzyć podsieci o dowolnej wielkości zastosowano technikę VLSM (*ang. Variable Length Subnet Mask*) opartą na dokumencie RFC 1878.[11]

Niezależnie trwały prace nad mechanizmami umożliwiającymi podłączenie do Internetu wielu hostów przy wykorzystaniu pojedynczych (lub niewielkiej puli) adresów IP. Zwróćmy uwagę, iż w izolowanych sieciach, do prawidłowego zaadresowania hostów można wykorzystać dowolną przestrzeń adresową. Problem pojawi się jed-

nakże, gdy za pomocą routera podłączymy tą sieć do Internetu. O ile wysłanie pakietów przez hosty znajdujące się w takiej sieci nie będzie stanowiło problemu, to ze względu na nieprawidłowy przydział adresów IP (niezgodny z danymi dostawcy usług internetowych tzw. ISP *ang. Internet Service Provider*) hosty te zwrotnie nie otrzymają żadnych danych. Wprowadzenie techniki NAT (*ang. Network Address Translation*) rozwiązało ten problem umożliwiając zmianę adresów IP w przesyłanych przez router pakietach tak, aby dla urządzeń spoza sieci widoczne były one jako pakiety wysyłane z pojedynczego źródła, któremu ISP przydzielił odpowiedni adres. O ile tak obsługiwane urządzenia bez problemu mogą korzystać z różnych usług dostępnych w sieci Internet, to mają one ograniczoną funkcjonalność w zakresie świadczenia usług dla hostów znajdujących się poza ich rodzimą siecią. Technika ta została opisana w dokumencie RFC 1631.[10] W szczególnym przypadku rozwiązanie to umożliwia podłączenie do Internetu wielu hostów przy wykorzystaniu pojedynczego adresu IP przydzielonego przez ISP. Dodatkowo zastosowanie tej techniki wymagało zdefiniowania przestrzeni prywatnych (nieroutowalnych) adresów IP, które w odróżnieniu od adresów publicznych (obsługiwanych przez ISP) mogą być dowolnie wykorzystywane w sieciach lokalnych. Dokument RFC 1918 definiuje trzy dostępne przestrzenie adresów IP:

- 10.0.0.0 – 10.255.255.255 (prefiks 10 /8),
- 172.16.0.0 – 172.31.255.255 (prefiks 172.16/12),
- 192.168.0.0 – 192.168.255.255 (prefiks 192.168/16).[12]

Oznacza to, iż adresy te nie mogą być już wykorzystane do adresacji publicznych sieci, tym samym powodując uszczuplenie dostępnej puli adresowej obsługiwanej w Internecie. Pomimo licznych ograniczeń technika ta jest szeroko stosowana między innymi w sieciach domowych, do obsługi których najczęściej wykorzystywany jest pojedynczy publiczny adres IP.

Problemy związane z automatyczną konfiguracją interfejsów sieciowych przy wykorzystaniu protokołu DHCP (*ang. Dynamic Host Configuration Protocol*) spowodowały, iż dla adresów IPv4 w dokumencie RFC 3927 określono alternatywny, bezstanowy, automatyczny sposób konfiguracji interfejsu.[15] Mechanizm ten wykorzystywany jest w przypadku, gdy pomimo stosowania protokołu DHCP klient nie uzyskuje z serwera DHCP odpowiedniej konfiguracji. Dzieje się tak najczęściej podczas problemów z samą usługą DHCP lub pośredniczącymi urządzeniami sieciowym. W takiej sytuacji w celu zapewnienia lokalnej komunikacji z innymi hostami system operacyjny automatycznie konfiguruje swój interfejs adresem IP wylosowanym z puli 169.254.0.0 /16 nazywanej pulą lokalnego łącza (*ang. link-local address*). Należy zaznaczyć, iż adres 169.254.255.255 zarezerwowany jest jako adres rozgłoszeniowy i

nie może być wykorzystany do konfiguracji interfejsu. Pamiętajmy, iż metoda ta nie może doprowadzić do skonfigurowania kilku hostów z tym samym adresem IP. W związku z powyższym przed ostateczną konfiguracją interfejsu system operacyjny wysyła do sieci zapytanie ARP dotyczące wylosowanego adresu IP. W przypadku gdy otrzyma odpowiedź oznaczać to będzie, iż testowany adres jest już wykorzystywany przez innego hosta i należy ponownie przeprowadzić losowanie. Brak odpowiedzi oznacza brak duplikatu adresu IP w sieci lokalnej i możliwość jego wykorzystania do konfiguracji interfejsu. Zakładając, iż wszystkie hosty skonfigurują swoje interfejsy dokładnie w ten sam sposób, uzyskają one możliwość wzajemnej komunikacji pomimo niedziałającej usługi DHCP. Jednocześnie cyklicznie system operacyjny cały czas będzie próbował skomunikować się z serwerem DHCP i po otrzymaniu nowej konfiguracji odpowiednio zmieni ustawienia swojego interfejsu. Oczywiście opisana metoda wpływa również na zmniejszenie przestrzeni adresowej wykorzystywanej do publicznej adresacji sieci, gdyż wydzielenie puli adresowej 169.254/16 powoduje, iż nie może ona już być obsługiwana w sieci Internet. Czytelnicy pragnący pogłębić swoją wiedzę z zakresu działania protokołu DHCP dla IPv4 mogą skorzystać między innymi z opracowania „Automatyczna konfiguracja interfejsu sieciowego, czyli protokół DHCP w praktyce”.[2]

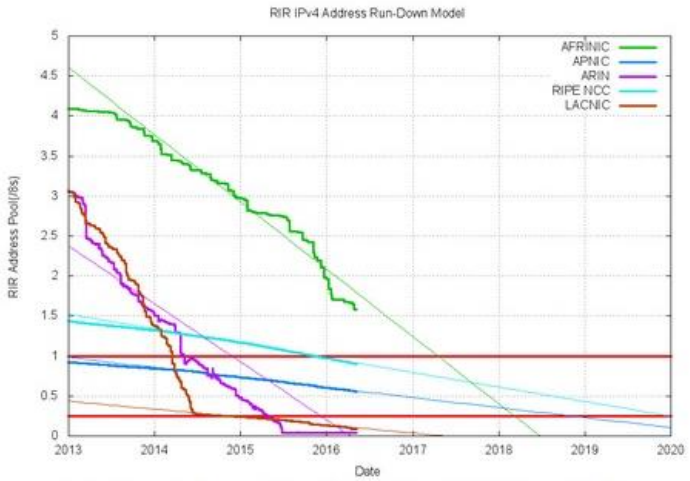
Opisane powyżej mechanizmy pozwoliły na rozwiązanie pewnych problemów związanych z działaniem protokołu IPv4 i znacząco opóźniły moment, w którym pula przeznaczona do adresowania hostów zostanie zupełnie wyczerpana. Organizacja IANA (*ang. Internet Assigned Numbers Authority*) w celu lepszego zarządzania przestrzenią adresową przydzieliła odpowiednie pule publicznych adresów IP regionalnym organizacjom RIR (*ang. Regional Internet Registries*), które zarządzają nimi na różnych obszarach terytorialnych (Rys.1).

Rysunek 1 Zakres terytorialnego działania organizacji Regional Internet Registries (RIRs). [19]

Obecnie część z organizacji RIR nie dysponuje już dużymi wolnymi przestrzeniami adresowymi. Przewiduje się, iż całkowite wykorzystanie publicznej puli adresowej IPv4 nastąpi przed rokiem 2020 (Rys.2).

Projected RIR Address Pool Exhaustion Dates:

RIR	Projected Exhaustion Date	Remaining Addresses in RIR Pool (/8s)
APNIC:	**19-Apr-2011** (actual)	0.5568
RIPE NCC:	**14-Sep-2012** (actual)	0.9013
LACNIC:	**10-Jun-2014** (actual)	0.0864
ARIN:	**24 Sep-2015** (actual)	
AFRINIC:	**02-Apr-2018**	1.5839



Rysunek 2 Wykorzystanie publicznej przestrzeni adresowej IPv4 dla poszczególnych regionalnych dostawców RIR. [17]

3. Wprowadzenie do IPv6

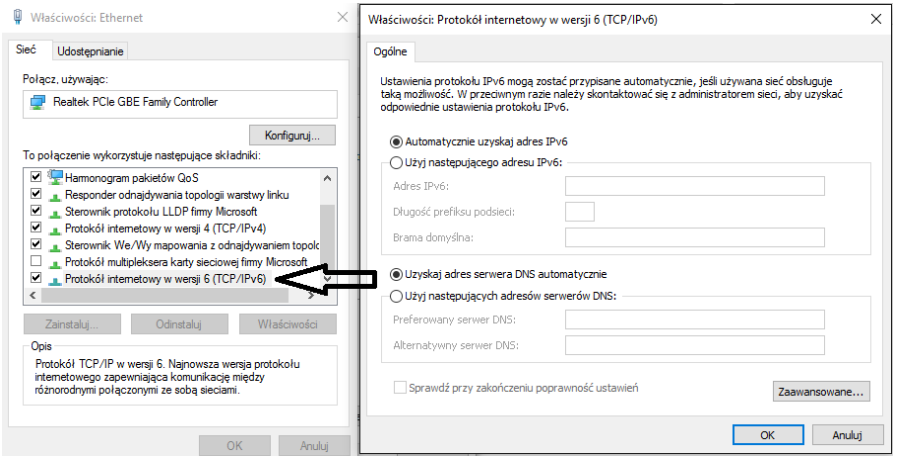
Świadomość, iż w niedalekiej przyszłości nastąpi ostatecznie moment, w którym nie będzie już dostępnych wolnych adresów IPv4 powodowała, że równolegle cały czas trwały prace nad nową wersją protokołu sieciowego. Miał on nie tylko rozwiązać problem z adresacją hostów, ale również bezpośrednio wspierać nowe rozwiązania w zakresie szyfrowania danych, optymalizacji przełączania, znakowania danych i mobilności hostów. Protokół IPv6 opisany został w dokumencie RFC 2460 w 1998 roku.[13] W tym momencie pojawia się pytanie dlaczego do dnia dzisiejszego pomimo upływu tak długiego czasu nadal korzystamy z IPv4? Okazuje się, iż warstwa

sieciowa modelu OSI jest najtrudniejszą warstwą do implementowania zmian, gdyż w warstwie tej działają routery, które są odpowiedzialne za przekazywanie danych w sieciach lokalnych jak i w szkielecie Internetu. Oznacza to, iż zastąpienie w jednym momencie protokołu IPv4 protokołem IPv6 wymagałoby nie tylko dokonania zmian w systemach operacyjnych użytkowników końcowych, ale również włącznie obsługi nowego protokołu na wszystkich routerach sieci Internet. Rozwiązanie takie nie jest możliwe do realizacji, dlatego też stopniowo wdrażane jest rozwiązanie oparte na podwójnym stosie TCP/IP. Oznacza ono, iż istniejąca fizyczna infrastruktura będzie umożliwiała przesyłanie danych zarówno przy wykorzystaniu starego protokołu IPv4 jak i nowego IPv6. Zmiana ta nie jest prosta do przeprowadzenia, gdyż uruchomienie nowego protokołu sieciowego na routerach wymaga stworzenia oddzielnych tablic routingu, nowych wersji protokołów routingu dynamicznego i oddzielnej konfiguracji interfejsów sieciowych. Ostatecznie po zastosowaniu takiego podejścia każdy interfejs fizyczny będzie posiadał oddzielną konfigurację dla protokołu IPv4 i protokołu IPv6. Oczywiście w miejscach gdzie zmiany te nie zostały jeszcze zastosowane wykorzystywany jest wyłącznie protokół IPv4. W celu zapewnienia obsługi danych w protokole IPv6 poprzez sieć działającą wyłącznie w standardzie IPv4 opracowano technologię związaną z tworzeniem tuneli polegającą na enkapsulowaniu datagramów IPv6 w datagramy IPv4. Ponadto możliwe jest również wykorzystanie mechanizmu NAT64 do dokonywania automatycznej translacji pomiędzy adresami IPv4 i IPv6 przy zmianie formatu datagramu. To ostatnie rozwiązanie ze względu na modyfikacje pakietów nie pozwala na wykorzystanie zaawansowanych funkcji IPv6.

Obecnie wszystkie nowoczesne systemy operacyjne stosują podejście podwójnego stosu TCP/IP, co widoczne jest zarówno na etapie konfiguracji interfejsu (Rys. 3), jak i przy weryfikacji jego ustawień (Rys. 4).

Pozostaje jednakże pytanie czy wprowadzenie nowej wersji protokołu IP nie wymaga również dalszych modyfikacji związanych z protokołami wyższych i niższych warstw modelu OSI oraz fizycznych zmian w interfejsie sieciowym. Okazuje się, iż warstwowość przytoczonego modelu zapewnia, iż zmiany realizowane w pojedynczej warstwie nie powinny wymuszać zmian w warstwach sąsiednich. Zatem dbając o standaryzację, twórcy IPv6 spowodowali, iż zastosowanie nowego protokołu w systemie operacyjnym urządzenia końcowego wymaga tylko aktualizacji odpowiedniego oprogramowania bez potrzeby dokonywania jakichkolwiek modyfikacji fizycznych sprzętu. Oznacza to również, iż w takiej sieci możemy stosować nadal standardowe przełączniki warstwy drugiej, gdyż z ich punktu widzenia protokół IPv6 tak jak i IPv4 nie jest interpretowany, a traktowany jako zwykłe dane, które należy po prostu przesłać do następnego urządzenia. Sytuacja jest znacznie bardziej skomplikowana w

przypadku routerów, gdyż włączenie na nich routingu dla IPv6 oznacza uruchomienie dedykowanych funkcji i procesów związanych z tym protokołem.

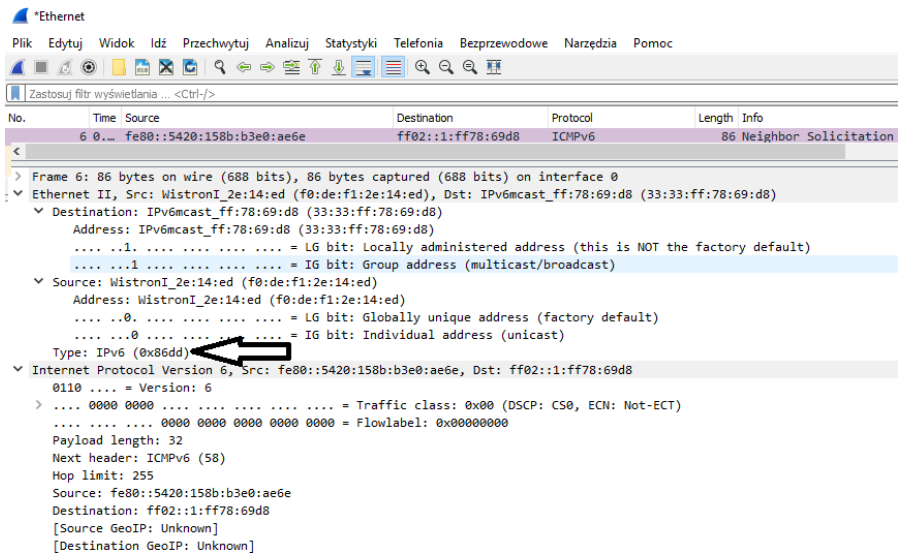


Rysunek 3 Konfiguracja interfejsu sieciowego w systemie Windows przy wykorzystaniu podwójnego stosu TCP/IP.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : fizyka.umk.pl
   IPv6 Address. . . . . . . . . . . : 2001:470:71:a1b:d002:a04f:2a53:6993
   Temporary IPv6 Address. . . . . . : 2001:470:71:a1b:a552:ec2d:6ab8:329a
   Link-local IPv6 Address . . . . . : fe80::d002:a04f:2a53:6993%5
   IPv4 Address. . . . . . . . . . . : 158.75.5.54
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::a236:9fff:fe78:69d8%5
                                       158.75.5.254
```

Rysunek 4 Weryfikacja konfiguracji interfejsu sieciowego w systemie Windows przy pomocy komendy ipconfig.

Typową technologią dostępową wykorzystywaną do obsługi hostów w lokalnych sieciach przewodowych jest Ethernet. Ze względu na stosowany stos protokołów posiada on w swojej ramce pole „Typ" wskazujące kolejny protokół obsługujący przesyłane dane. W przypadku protokołu IPv4 pole to posiada wartość 0x0800, dla protokołu ARP wartość ta wynosi 0x0806, a dla protokołu IPv6 odpowiednio 0x86dd (Rys. 5).



Rysunek 5 Przechwycona za pomocą programu Wireshark transmisja związana z obsługą protokołu IPv6.

4. Adresacja IPv6

W protokole IPv6 wprowadzono zupełnie nowe podejście do adresacji, które opisano w dokumencie RFC 4291.[16] Po pierwsze wydłużono adres do 128 bitów zapewniając tym samym 2^{128} (ponad $3{,}4 \times 10^{38}$) jego możliwych kombinacji. Ze względu na długość adresu zapisuje się go w postaci 32 cyfr szesnastkowych, gdzie każde 16 bitów (4 znaki, tzw. hextety) oddzielone są dwukropkiem. Adres taki może być zapisany np. w postaci ABCD:EF01:2345:6789:ABCD:EF01:2345:6789. W celu uproszczenia zapisu dodatkowo wprowadzono możliwość pomijania wiodących zer w ramach danego hextetu oraz pomijanie całych hextetów, które są wypełnione samymi zerami wskazując ten fakt podwójnym dwukropkiem (::). Dla przykładu adres 2001:0DB8:0000:0000:ABCD:000A:0451:1234 można zapisać w skróconej postaci 2001:0DB8::ABCD:A:451:1234. Zatem adres pętli zwrotnej zapisany w skróconej postaci jako ::1 oznacza 0000:0000:0000:0000:0000:0000:0000:0001.

W odróżnieniu od adresacji IPv4 wyróżniono tutaj tylko trzy rodzaje adresów, nie wyróżniając żadnych klas adresowych:

- **unicast** – adresy jednostkowe przeznaczone do konfiguracji interfejsów i obsługi transmisji jednostkowej,
- **multicast** – adresy służące do obsługi komunikacji grupowej,

- **anycast** – adresy typu unicast, które mogą być przypisane do wielu interfejsów, pakiet wysłany pod ten adres zostanie przekierowany do najbliższego urządzenia posiadającego skonfigurowany taki adres.

W przeciwieństwie do adresacji IPv4, nie zdefiniowano tutaj adresów rozgłoszeniowych, a ich funkcje mają przejąć adresy grupowe.

Podobnie jak IPv4, nowy protokół jest hierarchiczny, co oznacza, iż w jednym adresie zawarta jest informacja dotycząca prefiksu sieciowego jak i identyfikatora interfejsu. Zdefiniowanych jest sześć rodzajów adresów unicast:

- **global unicast** – unikatowy adres globalny przydzielany interfejsowi podczas konfiguracji statycznej lub dynamicznej, typowa postać tego adresu zawiera: prefiks globalny określający globalny routing, identyfikator podsieci oraz identyfikator interfejsu,
- **link-local** – adres lokalnego łącza, służący do komunikacji wyłącznie w obrębie danej sieci, w postaci FE80::/10,
- **loopback** – adres związany z pętlą zwrotną interfejsu, mający postać ::1/128,
- **unspecified** – adres nieokreślony, posiadający wszystkie bity ustawione na 0, zapisywany w postaci ::/128, wykorzystywany jest w przypadku, gdy urządzenie nie ma jeszcze skonfigurowanego interfejsu sieciowego,
- **unique local** – unikalny adres lokalny wykorzystywany w ramach pojedynczej sieci, lub pewnej grupy sieci, w odróżnieniu od adresów link-local, adresy te powinny być routowalne w globalnej sieci IPv6, zakres tych adresów zdefiniowany jest jako FC00::/7 do FDFF::/7,
- **embedded** – adresy wbudowane, mające na celu łatwą translację adresów IPv4 na IPv6,(IPv4-Compatible IPv6 address oraz IPv4-Mapped IPv6 Address).

Urządzenie posiadające interfejs wykorzystujący protokół IPv6 musi posiadać skonfigurowany adres IPv6 lokalnego łącza (link-local) niezależnie od tego czy został skonfigurowany unikatowy adres globalny czy też nie. Adres ten ma znaczenie wyłącznie lokalne, ale jest niezbędny do prawidłowego działania protokołu. Konfiguracja ta realizowana jest w sposób automatyczny, ale również może zostać określona w sposób statyczny. Na zamieszczonym Rysunku 4 widać, iż wykorzystywany interfejs ethernetowy skonfigurowany jest zarówno przy wykorzystaniu adresu IPv4 jak i trzech adresów IPv6. Adres lokalnego łącza zdefiniowany został jako **fe80::d002:a04f:2a53:6993%5**, gdzie wartość „%5” określa identyfikator interfejsu,

z którym związany jest ten adres. W systemie Windows wyświetlenie identyfikatorów poszczególnych interfejsów możliwe jest np. przy wykorzystaniu komendy *netstat –r*, która pozwala na wyświetlenie tablic routingu dla protokołów IPv4 i IPv6 (Rys. 6).

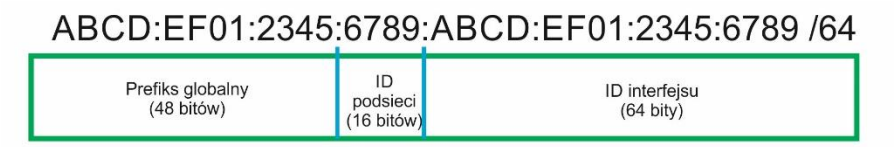
```
C:\>netstat -r
===========================================================================
Interface List
 10...18 4f 32 30 82 cf ......Dell Wireless 1705 802.11b/g/n (2.4GHZ)
 11...1a 4f 32 30 82 cf ......Microsoft Wi-Fi Direct Virtual Adapter
  5...64 00 6a 07 b2 4c ......Realtek PCIe GBE Family Controller
  6...18 4f 32 30 82 d0 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
  3...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
  2...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     158.75.5.254      158.75.5.54     20
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
       158.75.4.0    255.255.254.0         On-link       158.75.5.54    276
      158.75.5.54  255.255.255.255         On-link       158.75.5.54    276
    158.75.5.255  255.255.255.255         On-link       158.75.5.54    276
       224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
       224.0.0.0        240.0.0.0         On-link       158.75.5.54    276
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link       158.75.5.54    276
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  5    276 ::/0                     fe80::a236:9fff:fe78:69d8
  1    306 ::1/128                  On-link
  3    306 2001::/32                On-link
  3    306 2001:0:5ef5:79fb:882:2a96:61b4:fac9/128
                                    On-link
  5    276 2001:470:71:a1b::/64     On-link
  5    276 2001:470:71:a1b:a552:ec2d:6ab8:329a/128
                                    On-link
  5    276 2001:470:71:a1b:d002:a04f:2a53:6993/128
```

Rysunek 6 Wynik wywołania komendy *netstat –r* w systemie Windows umożliwiający sprawdzenie listy interfejsów oraz tablic routingu IPv4 i IPv6.

Typowo dla urządzeń znajdujących się w danej sieci adres link-local routera staje się adresem bramy domyślnej, co widać również w konfiguracji IPv6 interfejsu sieciowego (Rys. 4).

Podobnie jak publiczne adresy IPv4, unikatowe adresy globalne IPv6 przydzielane są lokalnym organizacjom RIR przez Internet Committee for Assigned Names and Numbers (ICANN), który działa w imieniu organizacji Internet Assigned Numbers Authority (IANA). Obecnie został przekazany do wykorzystania jeden blok adresów globalnych z pierwszymi bitami określonymi jako 001 (2000::/3 w zapisie szesnastkowym), który stanowi zaledwie 12,5% wszystkich dostępnych adresów.

Typowa postać unikatowego adresu globalnego IPv6 dla 64 bitowego prefiksu została przedstawiona na Rysunku 7.



Rysunek 7 Typowa postać unikatowego adresu globalnego IPv6.

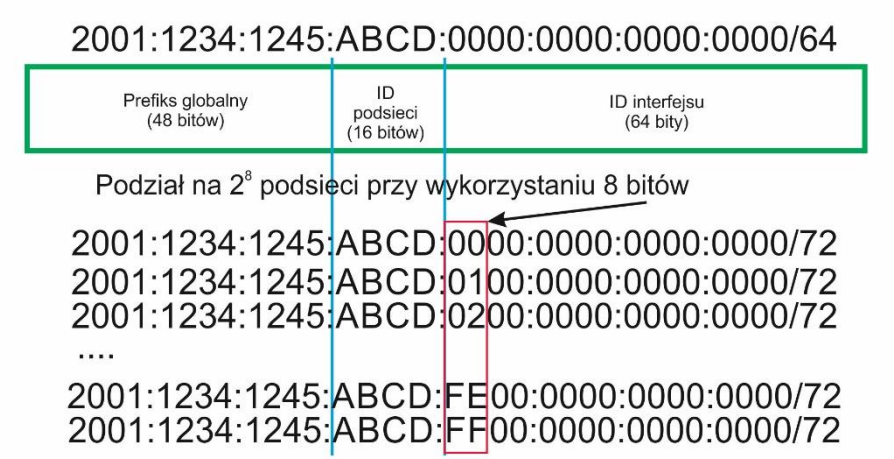
Warto zwrócić uwagę, iż przydział takiej puli adresowej dla konkretnej sieci oznacza możliwość zaadresowania w niej 2^{64} urządzeń co stanowi kwadrat liczby określającej wszystkie możliwe kombinacje adresu IPv4.

5. Podział na podsieci w IPv6

Schemat wykorzystywany w przypadku protokołu IPv4 umożliwiający podział sieci na podsieci może być stosowany również w przypadku protokołu IPv6. Oznacza to możliwość określania puli adresowej z dokładnością do jednego bitu w adresie IP. Jednakże ze względu na zapis heksadecymalny oraz dużą liczbę adresów, dobrą praktyką jest stosowanie podziału z dokładnością do 4 bitów, czyli jednego znaku w zapisie heksadecymalnym (tzw. nibbla).

Dla przykładu przeanalizujmy sytuację, w której firma XYZ wykupiła u dostawcy usług internetowych standardową pulę adresową 2001:1234:1245:ABCD::/64. Po analizie struktury firmy okazało się, iż wymaga ona utworzenia siedmiu podsieci zawierających od 2000 do 100 hostów. W przypadku gdybyśmy analizowali podobną sytuację dla protokołu IPv4, to ze względu na ograniczoną ilość adresów zapewne należałoby teraz zastosować technikę VLSM, tak aby dopasować wielkość podsieci do odpowiednich grup użytkowników. W przypadku IPv6 można zastosować dokładnie taki sam schemat postępowania, ale czy jesteśmy zmuszeni do wykorzystywania takich

rozwiązań? Załóżmy, że w uzyskanej przestrzeni adresowej IPv6 administrator postanowił wydłużyć maskę o 8 bitów, co oznacza, iż teraz prefiks będzie liczył 72 bity. Taki podział pozwala na zaadresowanie w firmie 2^8=256 podsieci, a w każdej z nich można umieścić 2^{56} hostów, co oczywiście w pełni zaspokaja potrzeby firmy. Zatem stosowanie techniki VLSM nie jest tutaj niezbędne. Podział ten został przedstawiony na Rysunku 8. Warto zwrócić uwagę, iż liczba 2^{56} jest znacznie większa niż liczba wszystkich urządzeń obecnie podłączonych do sieci Internet. Ten prosty przykład pokazuje jak duże przestrzenie adresowe zapewnia protokół IPv6.



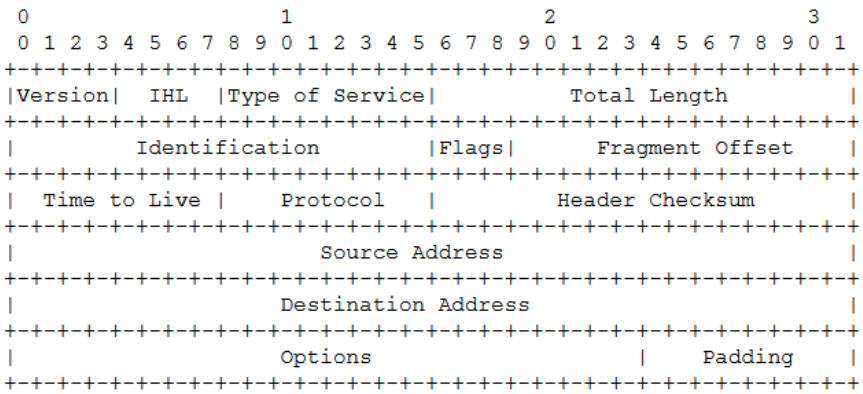
Rysunek 8 Podział adresu IPv6 z 64 bitowym prefiksem na podsieci przy wykorzystaniu 72 bitowego prefiksu.

6. Datagramy IPv4 i IPv6

Protokół IPv6 oprócz dostarczenia 128-bitowej przestrzeni adresowej wspiera również szereg nowych funkcji, które nie były do tej pory obsługiwane przez protokół IPv4. Oznacza to, iż nowy datagram musi posiadać pola, które pozwolą na przekazywanie dodatkowych informacji. Ostatecznie takie rozwiązanie prowadzi do zwiększenia ilości danych sterujących znajdujących się w pakiecie, które muszą zostać przesłane, aby obsłużyć dane wyższej warstwy modelu OSI. Zwiększanie wielkości tzw. narzutu nie jest elementem pożądanym, zatem twórcy protokołu IPv6 zastosowali bardzo ciekawe rozwiązanie, które w efekcie uprościło postać datagramu. Dla porównania Rysunek 9 przedstawia schemat datagramu IPv4, a Rysunek 10 postać datagramu IPv6, który składa się z następujących pól:

- Wersja (*ang. version*), 4 bity – definiuje wersję protokołu, w przypadku IPv6 pole to zawiera wartość 6 (bitowo 0110),

- Klasa ruchu (*ang. Traffic Class*), 8 bitów – pozwala na klasyfikację ruchu. W IPv4 pole to nosiło nazwę *Type of Service,*
- Etykieta przepływu (*ang. Flow Label*), 20 bitów – pozwala znakować pakiety, które mają być tratowane w specjalny sposób,
- Długość danych (*ang. Payload Length*), 16 bitów – wielkość pakietu bez długości podstawowego nagłówka (wliczając jednak nagłówki rozszerzające),
- Następny nagłówek (*ang. Next Header*), 8 bitów – identyfikuje typ następnego nagłówka, pozwalając określić czy jest to nagłówek rozszerzający czy nagłówek warstwy wyższej. W tym drugim przypadku, wartość pola jest identyczna z wartością pola w protokole IPv4,
- Limit przeskoków (*ang. Hop Limit*), 8 bitów – określa ilość węzłów, po odwiedzeniu których pakiet zostaje porzucony,
- Adres źródłowy (*ang. Source Address*), 128 bitów – adres nadawcy,
- Adres docelowy (*ang. Destination Address*), 128 bitów – adres odbiorcy.



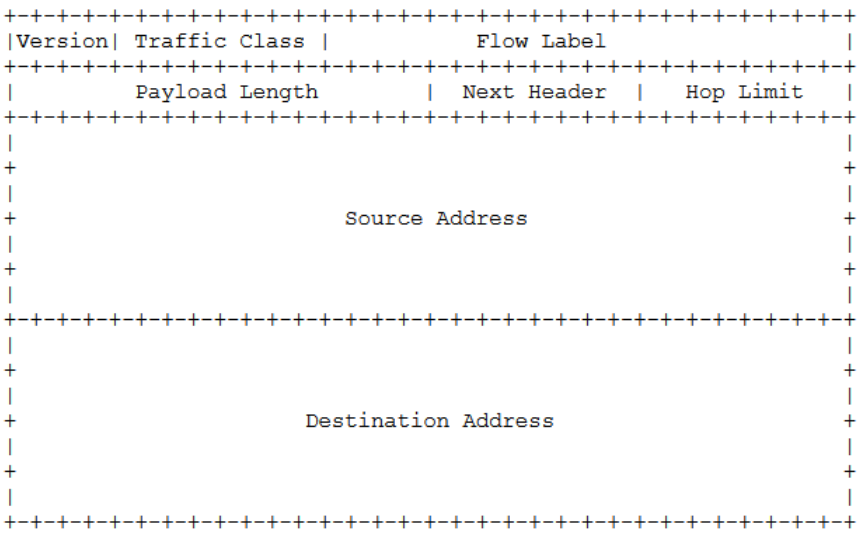
Rysunek 9 Datagram IPv4 zdefiniowany w dokumencie RFC 791.[7]

W przypadku protokołu IPv4 mamy do czynienia z jedną uniwersalną postacią datagramu, która wykorzystywana jest do obsługi wszystkich danych. Oznacza to, iż pola takie jak Fragment Offset, Options czy Padding bardzo często nie niosą żadnych informacji, a w efekcie wypełnione są samymi zerami, które jednak trzeba przesłać przez sieć. W protokole IPv6 zdecydowano się na maksymalne uproszczenie nagłówka i tym samym uniknięcie opisywanej sytuacji. W przypadku gdy wymagane

jest zastosowanie bardziej skomplikowanych mechanizmów nagłówek IPv6 może zostać rozszerzony o kolejny nagłówek, co wskazywane jest w polu „Następny nagłówek”. Dokument RFC 2460 definiuje następujące nagłówki rozszerzeń:

- Hop-by-Hop Options,
- Routing,
- Fragment,
- Destination Options,
- Authentication,
- Encapsulating Security Payload.

Nagłówki te między innymi pozwalają na zdefiniowanie węzłów przez które ma przejść przesyłany pakiet, obsługują fragmentację pakietów oraz wspierają opcje związane z bezpieczeństwem danych.



Rysunek 10 Datagram IPv6 zdefiniowany w dokumencie RFC 2460. [13]

7. Konfiguracja IPv6

Protokół IPv6 przewiduje trzy główne sposoby konfiguracji interfejsu:

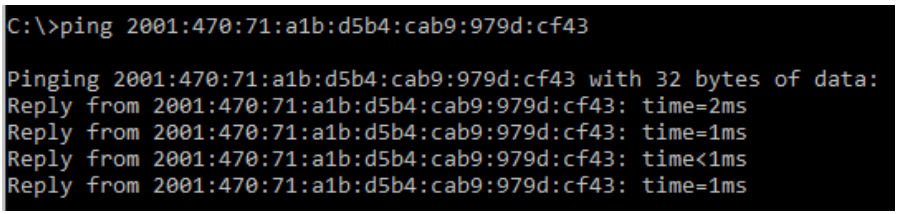
- statyczny, realizowany przez administratora systemu operacyjnego,

- dynamiczny stanowy, realizowany za pomocą protokołu DHCPv6,
- dynamiczny bezstanowy, umożliwiający automatyczną konfigurację interfejsu na podstawie komunikatów rozgłaszanych przez router, zawierających prefiks sieci.

Rysunek 3 przedstawia okno konfiguracji interfejsu sieciowego w systemie Windows umożliwiające statyczne zdefiniowanie konfiguracji IPv6 lub włączenie konfiguracji automatycznej. Ta druga opcja oznacza, iż host będzie oczekiwał informacji od routera (Router Advertisement) określających prefiks sieci oraz dodatkowe opcje konfiguracji. W szczególności mogą one wskazywać hostowi, iż w celu uzyskania szerszej konfiguracji musi skomunikować się z serwerem DHCP. Serwer ten może przesyłać hostowi informacje dodatkowe takie jak nazwa domeny, adresy serwerów DNS itp., ale również nową konfigurację IPv6. Takie elastyczne rozwiązanie powoduje, iż nawet w przypadku problemów z usługą DHCP host uzyska od routera podstawowe informacje umożliwiające mu poprawną konfigurację interfejsu.

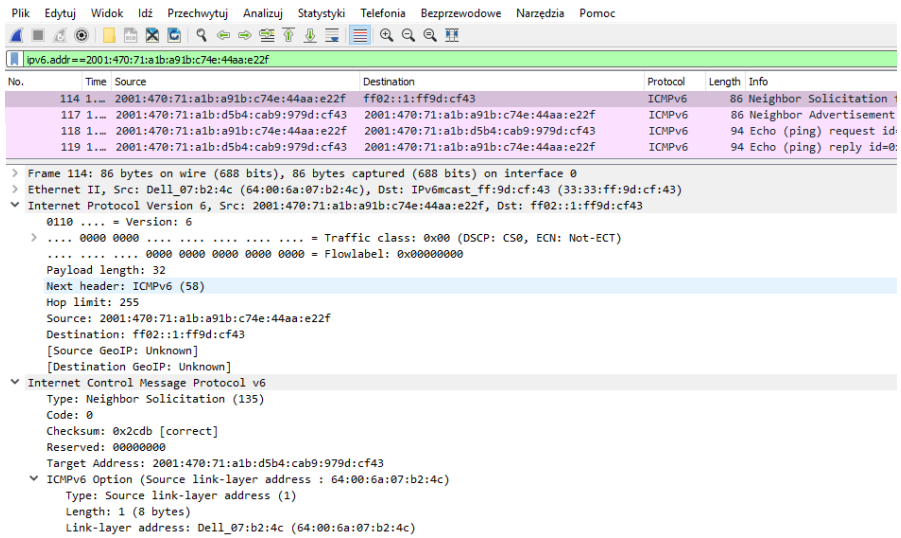
8. ICMPv6

Protokół ICMPv6 (*ang. Internet Control Message Protocol*) opisany w dokumencie RFC 2463 [14] stanowi integralną część protokołu IPv6 i w celu jego prawidłowego działania nie może być blokowany przez zapory ogniowe. Pozwala on uzyskiwać informacje o błędach w sieci, posiada funkcje diagnostyczne (ping, tracert), wspiera mechanizm pozwalający na określenie minimalnej wartości MTU (*ang. Maximum Transmission Unit*) na ścieżce oraz umożliwia uzyskanie informacji o sąsiadach (*Neighbor Discovery*). Jak już wspomniano protokół IPv6 nie wykorzystuje transmisji rozgłoszeniowej, co więcej nie korzysta również z protokołu ARP. Mając jednak na względzie współpracę z technologią Ethernet musi on posiadać mechanizm umożliwiający poznanie adresu MAC hosta, który został skonfigurowany określonym adresem IPv6. W tym celu wykorzystywany jest protokół ICMPv6. Proces ten można łatwo zaobserwować badając komunikację między hostami związaną z wywołaniem komendy ping na adres IPv6 z sieci lokalnej (Rys. 11).



Rysunek 11 Wydanie komendy ping w systemie Windows przy wykorzystaniu protokołu IPv6.

Uzyskany na ekranie wynik nie daje pełnej informacji, a zatem w celu przeprowadzenia głębszej analizy należy wykorzystać oprogramowanie umożliwiające przechwycenie przesyłanych danych. Jednym z najbardziej popularnych programów narzędziowych wykorzystywanych w tym zakresie jest Wireshark.[20] Umożliwia on nie tylko przechwytywanie przesyłanych danych, ale również ich szeroką analizę z wykorzystaniem datagramów protokołów stosu TCP/IP.[3] Wracając do badanej komunikacji pomiędzy hostami należy zauważyć, iż przed wysłaniem żądania ping, host źródłowy musi uzyskać informację o adresie MAC hosta docelowego. W związku z tym wysyła do wszystkich urządzeń pracujących w sieci lokalnej pakiet ICMPv6 Neighbor Solicitation, prosząc o odpowiedź tylko jednego hosta, który faktycznie posiada adres 2001:470:71:a1b:d5b4:cab9:979d:cf43. Ze względu na fakt, iż dane te mają trafić do wszystkich hostów w sieci lokalnej, w przesyłanej ramce pole adres docelowy przyjmuje wartość 33:33:ff:9d:cf:43, co stanowi adres grupowy warstwy drugiej powiązany z adresem grupowym IPv6. Jako adres docelowy IPv6 wykorzystywany jest adres grupowy ff02::1:ff9d:cf43. Host posiadający adres IPv6 wskazany w datagramie ICMPv6 (Target Address) przesyła do hosta źródłowego odpowiedź Neighbor Advertisement zawierającą wymagane dane (Link-layer address). Należy zwrócić uwagę, iż jest to już komunikacja typu unicast. Mając wszystkie niezbędne informacje host źródłowy może już wysyłać do hosta docelowego pakiet ping ICMPv6 Echo request, na który po chwili uzyskuje odpowiedź w postaci Echo reply. Rysunek 12 przedstawia opisywaną komunikację przechwyconą w programie Wireshark.



Rysunek 12 Przechwycona w programie Wireshark komunikacja związana z wydaniem komendy ping 2001:470:71:a1b:d5b4:cab9:979d:cf43.

Podobnie jak dla IPv4 system operacyjny przechowuje w tablicach ARP informacje dotyczące powiązań adresów MAC z adresami IPv4, tak również dla IPv6 tworzone są tablice sąsiadów przechowujące informacje dotyczące powiązań adresów MAC z adresami IPv6. W systemie Windows dane te można zweryfikować wydając komendę *netsh int ipv6 sh neighbor* (Rys. 13).

```
C:\>netsh int ipv6 sh neighbor

Interface 5: Ethernet


Internet Address                              Physical Address   Type
--------------------------------------------  -----------------  -----------
2001:470:71:a1b:d5b4:cab9:979d:cf43           00-17-31-9f-82-93  Stale
fe80::a236:9fff:fe78:69d8                     a0-36-9f-78-69-d8  Stale (Router)
ff02::1                                       33-33-00-00-00-01  Permanent
ff02::2                                       33-33-00-00-00-02  Permanent
```

Rysunek 13 Wyświetlenie tablicy sąsiadów IPv6 w systemie Windows poprzez wydanie komendy *netsh int ipv6 sh neighbor.*

Wykorzystując fakt, iż obecnie w sieci lokalnej większość komputerów stosuje podwójny stos TCP/IP, zgodnie z przedstawionym przykładem w prosty sposób można testować różne aspekty działania protokołu IPv6. Co ważniejsze nie wymaga to dokonania żadnych zmian w konfiguracji urządzeń pośredniczących pracujących w warstwie drugiej modelu OSI. W sytuacji gdy chcielibyśmy wykorzystać protokół IPv6 w komunikacji globalnej, a nasz dostawca usług internetowych nie zapewnia nam takiej funkcji, można zastosować mechanizmy tunelowania udostępnianie przez zewnętrznego dostawcę np. firmę Hurricane Electric (ipv6.he.net). Po uzyskaniu puli adresowej oraz uruchomieniu tunelu, pakiety wykorzystujące adresację IPv6 będą enkapsulowane w datagramy IPv4 i przesyłane (poprzez infrastrukturę IPv4) do serwera obsługującego tunel, a następnie rozpakowywane i dalej obsługiwane już za pomocą infrastruktury IPv6. Szersze omówienie tego zagadnienia wychodzi jednakże poza zakres niniejszego opracowania, którego celem było zaprezentowanie głównych idei i podstaw protokołu IPv6.

9. Podsumowanie

Niniejsza praca miała na celu zapoznanie czytelnika z podstawami dotyczącymi protokołu IPv6, który obecnie coraz szerzej wykorzystywany jest w sieciach komputerowych. Opisane różnice występujące pomiędzy datagramami oraz sposobem działania obu protokołów pozwalają na lepsze zrozumienie zastosowanych nowych rozwiązań oraz mechanizmów. Ponadto proste ćwiczenia dotyczące badania komunikacji przy wykorzystaniu programu Wireshark umożliwiają praktyczną obserwację i

szerszą analizę sposobu obsługi przesyłanych danych. Uzyskana w ten sposób wiedza może okazać się bardzo przydatna przy konfiguracji urządzeń w sieci IPv6 oraz rozwiązywaniu pojawiających się problemów. Autor niniejszego opracowania ma nadzieję, iż stanowić ono będzie dla czytelnika zachętę do dalszego samodzielnego studiowania bardziej zaawansowanych aspektów związanych ze stosowaniem IPv6.

Literatura

1. newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342
2. Piwiński M., Automatyczna konfiguracja interfejsu sieciowego, czyli protokół DHCP w praktyce, Uczyć się będąc połączonym, 235-247, Teksty wystąpień, red. M. Sysło, A. B. Kwiatkowska, X Konferencja "Informatyka w Edukacji" 2013, Wydawnictwa Naukowe UMK, ISBN 978-83-231-3105-2, Toruń, 2013, http://repozytorium.umk.pl/handle/item/1729
3. Piwiński M., 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
4. Piwiński M., Sieci komputerowe, konfiguracja i bezpieczeństwo, Informatyka w Edukacji, Nauczyciel przewodnik i twórca, Monografia naukowa, red. A.B. Kwiatkowska, M.M. Sysło, Wydawnictwo Naukowe UMK, ISBN 978-83-231-3411-4, Toruń, 85-99, (2015) https://repozytorium.umk.pl/handle/item/2759
5. Piwiński M., „Uczniowie i komputery w sieci...", „Komputer w Szkole", nr 5, (2003), s 38, https://repozytorium.umk.pl/handle/item/1667
6. Piwiński M., Marczak G., Sieci bezprzewodowe wykorzystujące technologie wirtualnej komórki i wirtualnego portu na przykładzie Meru Networks, Informatyka w Edukacji, Informatyka dla wszystkich od najmłodszych lat, A.B. Kwiatkowska, M. Sysło, (2014) 978-83-231-3251-6 https://repozytorium.umk.pl/handle/item/2101
7. RFC 791, tools.ietf.org/html/rfc791#page-34
8. RFC 1518, tools.ietf.org/html/rfc1518
9. RFC 1519, tools.ietf.org/html/rfc1519
10. RFC 1631, www.ietf.org/rfc/rfc1631.txt
11. RFC 1878, tools.ietf.org/html/rfc1878
12. RFC 1918, www.ietf.org/rfc/rfc1918.txt

13. RFC 2460, tools.ietf.org/html/rfc2460
14. RFC 2463, www.ietf.org/rfc/rfc2463.txt
15. RFC 3927, www.ietf.org/rfc/rfc3927.txt
16. RFC 4291, tools.ietf.org/html/rfc4291
17. www.potaroo.net/tools/ipv4/
18. www.rfidjournal.com/articles/view?4986
19. www.ripe.net/participate/internet-governance/internet-technical-community/the-rir-system
20. www.wireshark.org