Politechnika Śląska

Instytut Informatyki

Porównanie protokołów IPv4 i IPv6

mgr Magdalena Michniewicz

Praca napisana pod kierunkiem

mgr inż. Piotra Kasprzyka

Spis treści

Wstęp

Tematem pracy jest przedstawienie i porównanie protokołów IPv4 i IPv6. Oba protokoły są częścią modelu i protokołów TCP/IP. Prace nad modelem TCP/IP rozpoczęto w latach 70, był to pierwszy model jaki opracowano na potrzeby sieci. Badania nad protokołami TCP/IP prowadziła Advanced Research Project Agency (ARPA) a finansowała armia USA. 1 stycznia 1983 roku protokoły TCP/IP stały się standardowymi protokołami w sieci ARPANET. W wielu krajach na całym świecie zaczęły powstawać lokalne sieci, podłączane do ARPANETu. Tym co pomogło połączyć liczne sieci lokalne w jedną ogromną sieć zwaną Internetem był zestaw protokołów TCP/IP.

Zadaniem zestawu protokołów TCP/IP było udostępnienie jednolitego systemu komunikacyjnego. Protokół IPv4 miał za zadanie określenie podstawowej jednostki przesyłania danych – datagramu, reguł przetwarzania i przenoszenia datagramów, metodyki generowania komunikatów o błędach oraz schematu adresowania. Adres IPv4 jest 32-bitowym adresem identyfikującym docelową sieć i określającym konkretny komputer w tej sieci.

W 1990 roku zakończyła swoje funkcjonowanie sieć ARPANET, jednak sieć internetowa była rozwijana nadal. Do Internetu z każdym rokiem była podłączana coraz większa ilość sieci lokalnych i komputerów osobistych. Projektanci zestawu protokołów TCP/IP nie przewidzieli możliwości tak gwałtownego rozwoju Internetu. W latach 90 zaczęto przewidywać wyczerpanie zapasu adresów IPv4. Wtedy też rozpoczęto pracę nad nową wersją protokołu IPv6. Prace nad rozwojem protokołu IP nadzoruje zespół Internet Engineering Task Force (IETF). Nowy protokół IPv6 jest protokołem 128-bitowym co daje znacznie większą pulę adresów IP.

Pierwsza część tej pracy przedstawi model warstwowy TCP/IP oraz porównanie tego modelu z modelem odniesienia ISO/OSI. Druga część przedstawi ogólne zasady działania protokółu IP i działającego w tej samej warstwie protokołu ICMP. W części trzeciej zostanie zaprezentowany protokół IPv4, oraz protokół ICMPv4. W części czwartej opisany zostanie protokół IPv6, oraz ICMPv6. W części piątej porównane zostaną oba protokoły – ich podobieństwa i różnice. Natomiast w części szóstej i ostatniej przedstawiona zostanie migracja z protokołu IPv4 Na IPv6 i towarzyszące jej mechanizmy.

1. Model TCP/IP a model ISO/OSI

1.1. Model TCP/IP

Model TCP/IP powstał w latach 70. Został stworzony, gdy do ARPANETU zaczęto podłączać coraz większą liczbę sieci lokalnych za pomocą innych mediów transmisyjnych niż linie telefonicznie, takich jak linie satelitarne i radiowe. Aby połączyć te sieci potrzebna była jednolita architektura protokołów. Architekturą tą stał się model TCP/IP, który został opisany przez Cerf'a i Kahn'a w 1974 roku.[17]

WARSTWA APLIKACJI
WARSTWA TRANSPORTOWA TCP/UDP
WARSTWA INTERNET IP/ICMP
WARSTWA DOSTĘPU DO SIECI

Rysunek 1. Warstwy modelu TCP/IP

Warstwa dostępu do sieci - najniższa warstwa w hierarchii protokołów TCP/IP. Model odniesienia TCP/IP nie dostarcza zbyt wiele informacji o tej warstwie. Mówi on tylko o tym, że host musi być połączony do sieci, używając jakiegoś protokołu tak aby mógł wysłać pakiet IP w sieć. Protokół ten nie został zdefiniowany i bywa różny w zależności od hosta, który go używa i od sieci do której dany host jest podłączony.

Warstwa Internet – jest to warstwa, która scala całą architekturę modelu TCP/IP razem. Głównym protokołem tej warstwy jest protokół IP. Warstwa ta określa format pakietów przesyłanych w sieci oraz metody przekazywania pakietów od nadawcy do odbiorcy. Realizuje ona funkcje doboru trasy dla pakietów na podstawie czterobajtowego lub szesnastobajtowego adresu IP identyfikującego źródło informacji oraz ich przeznaczenie.

Warstwa transportowa – warstwa ta określa sposób realizacji usług niezawodnego przesyłania danych. Warstwa transportowa obejmuje dwa protokoły: TCP i UDP. Protokół TCP realizuje usługę połączenia wirtualnego. Protokół ten odbiera strumień danych z warstwy aplikacji, segmentuje dane, transmituje pakiety z wykorzystaniem protokołu IP oraz odtwarza dane użytkowe. Protokół TCP retransmituje także błędne lub zagubione pakiety, a również ustawia

odebrane pakiety w prawidłowej kolejności logicznej. Protokół UDP używany jest przez aplikacje obsługiwane w trybie datagramowym. Protokół ten nie daje gwarancji przekazania datagramu.

Warstwa aplikacji – najwyższa warstwa modelu TCP/IP. Każdy z protokołów tej warstwy odpowiada jednemu programowi użytkowemu w sieci. Warstwa ta realizuje wiele usług sieciowych takich jak np. SNMP (Simple Network Management Protocol), Telnet, FTP (File Transport Protocol), SMTP (Simple Mail Transport Protocol), Ping.

1.2. Model ISO/OSI

Model ISO/OSI powstał w latach 80. Model ten został stworzony i przedstawiony przez International Standard Organization (ISO). Stworzenie tego modelu było pierwszym krokiem w stronę międzynarodowej standaryzacji protokołów używanych w różnych warstwach.[17]

WARSTWA APLIKACJI
WARSTWA PREZENTACJI
WARSTWA SESJI
WARSTWA TRANSPORTOWA
WARSTWA SIECIOWA
WARSTWA ŁĄCZA DANYCH
WARSTWA FIZYCZNA

Rysunek 2. Model ISO/OSI

Warstwa fizyczna – najniższa warstwa zestawu protokołów ISO/OSI. Jej zadaniem jest przesyłanie bitów przez kanał transmisyjny. Podstawowymi zadaniami tej warstwy jest ustalenie pomiędzy łączącymi się ze sobą hostami: ile woltów będzie użytych aby zaprezentować 1 a ile, żeby zaprezentować 0; ile nanosekund ma trwać 1 bit; czy transmisja może odbywać się równocześnie w obu kierunkach; w jaki sposób zostanie nawiązane połączenie a w jaki zakończone; oraz ile pinów ma posiadać gniazdo połączeniowe i do czego ma służyć każdy z pinów. Tak wiec warstwa fizyczna zajmuje się mechanicznymi, elektrycznymi oraz czasowymi cechami medium transmisyjnego, znajdującego się poniżej warstwy fizycznej.

Warstwa łącza danych - jest warstwą której zadaniem jest odebranie z warstw wyższych ramek danych, dołączanie do nich ciągów synchronizujących, znacznika początku ramki, adresu nadajnika, długości bloku danych, wypełniacza i pola CRC a następnie wysyłanie ich kolejno w sieć do hosta odbiorcy. Warstwa ta także odbiera szereg ramek danych od hosta nadawcy i po sprawdzeniu poprawności danych przekazuje je do warstw wyższych. Innym zadaniem warstwy łącza danych tak jak i warstw wyższych jest regulacja szybkości przesyłania danych pomiędzy hostami o różnych prędkościach łączy. Często te dwie powyższe funkcje, czyli kontrola błędów transmisji i szybkość przesyłania danych są zintegrowane. W sieciach natychmiastowych posiada jeszcze jedną bardzo ważną funkcję, kontroluje ona zasady dostępu do współdzielonego medium transmisyjnego. Za poprawne wykonanie tego zadania odpowiada podwarstwa warstwy łącza danych – **podwarstwa kontroli dostępu do medium transmisyjnego**.

Warstwa sieciowa – kontroluje działanie podsieci. Głównym zadaniem tej warstwy jest określenie jak pakiety są rutowane od hosta źródłowego do hosta docelowego. Trasy routingu mogą być zapisane w sposób statyczny w tablicach routing i rzadko zmieniane. Trasy mogą być tworzone także wraz z nawiązaniem każdego połączenia np. w czasie logowania to zdalnego hosta. Mogą być także tworzone dynamicznie – dla każdego pakietu osobno. Drugim zadaniem warstwy sieciowej jest także kontrola nad jakością usług (opóźnieniami, czasem transmisji, przeciążeniami). Kolejnym zadaniem warstwy sieciowej jest przezwyciężenie różnorodnych problemów (różnice w adresowaniu, różne wielkości pakietów, różne protokoły) w sieciach heterogenicznych, aby mogły zostać połączone w jedną sieć. W sieciach broadcastowych problem routingu jest bardzo mały tak więc warstwa sieciowa w tych sieciach jest często cienka albo nawet nie istnieje.

Warstwa transportowa – odbiera dane z warstwy sesji, dzieli je na mniejsze części (jeśli jest to konieczne), przesyła je do warstwy sieciowej upewniając się czy wszystkie części dotarły poprawnie na drugi koniec. Wszystko to musi zostać wykonane wydajnie i w taki sposób aby odizolować warstwy wyższe od nieuniknionych zmian sprzętowych. Warstwa transportowa określa także jaki rodzaj usługi zostanie dostarczony do warstwy sesji. Rodzaj usługi zostaje określony, gdy połączenie zostaje ustanowione (np. połączenie punkt-punkt, które dostarcza wiadomości lub bajty w kolejności, w której zostały wysłane; przesyłanie pojedynczych wiadomości bez gwarancji kolejności ich dostarczenia; oraz broadcast wiadomości do wielu odbiorców). Warstwa transportowa jest prawdziwą warstwą punkt-punkt na całej drodze od źródła do celu. Oznacza to, że program na hoście źródłowym prowadzi rozmowę z podobnym programem na hoście docelowym używając nagłówków wiadomości oraz wiadomości kontrolnych.

Warstwa sesji – pozwala użytkownikom na różnych hostach na nawiązanie sesji pomiędzy sobą. Sesje oferują różne usługi takie jak np. kontrola dialogu (pilnowanie kolejności transmisji danych), zarządzanie żetonem (ochrona przed próbą wykonania tej samej, tak samo istotnej

operacji w tym samym czasie), i synchronizacja (wstawianie punktów kontrolnych w czasie długich transmisji, aby możliwa była kontynuacja od miejsca w którym transmisja została zerwana).

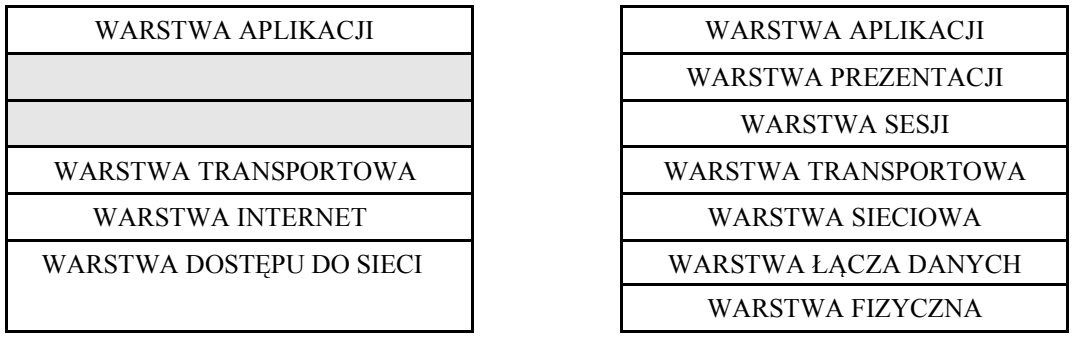
Warstwa prezentacji – zajmuje się składnią i semantyką transmitowanej informacji. Różne hosty mogą mieć różne formaty danych. Aby takie hosty mogły porozumiewać się ze sobą oraz aby była możliwa wymiana struktur danych, są one zdefiniowane w sposób abstrakcyjny wraz ze standardowym kodowaniem na łączu. Warstwa prezentacji zarządza tymi abstrakcyjnymi danymi, pozwala aby struktury danych warstw wyższych zostały zdefiniowane i wymieniane.

Warstwa aplikacji – zawiera wiele protokołów, których potrzebują użytkownicy. Protokoły te to np. HTTP (HyperText Transfer Protocol), który jest podstawowym protokołem dla World Wide Web. Inne protokoły są używane do transportu danych, poczty elektronicznej, lub sieciowych newsów.[17]

1.3. Porównanie modeli TCP/IP i ISO/OSI

Modele TCP/IP i ISO/OSI mają wiele cech wspólnych. Oba są oparte na idei stosu niezależnych protokołów. Także funkcjonowanie warstw jest podobne np. w obu modelach wszystkie warstwy, do warstwy transportowej włącznie dostarczają niezależną od sieci usługę transportową punkt-punkt dla procesów, które komunikują się ze sobą. W obu modelach warstwy wyższe są użytkownikami warstw niższych zorientowanymi na aplikacje.

Poza tymi dwoma podobieństwami modele te posiadają wiele różnic. Zasadniczą różnicą między modelem TCP/IP a ISO/OSI jest liczba protokołów występujących w obu modelach. Model TCP/IP ma 4 warstwy a model ISO/OSI ma 7 warstw.



Rysunek 3. Model TCP/IP i Model ISO/OSI

W obydwóch modelach występują warstwy sieciowa (Internet), transportowa i aplikacji. Pozostałe warstwy w obu modelach są różne.

Kolejną różnicą pomiędzy modelem TCP/IP i ISO/OSI są 3 koncepcje używane w modelu ISO/OSI a nie używane w modelu TCP/IP. W modelu ISO/OSI występują 3 zasadnicze koncepcje:

- USŁUGA – każda warstwa wykonuje pewne usługi dla warstwy wyższej. Definicja usługi mówi co dana warstwa robi, a nie w jaki sposób warstwy wyższe mają do niej dostęp lub w jaki sposób działa. Usługa definiuje semantykę warstwy.
- INTERFEJS – informuje proces warstwy wyższej w jaki sposób można się do niego dostać. Określa on parametry i to, jakich rezultatów należy oczekiwać. Nie informuje natomiast w jaki sposób działa dana warstwa.
- PROTOKOŁY – są wewnętrzną sprawą warstw. Warstwa może używać każdego protokołu jakiego potrzebuje aby wykonać dane zadanie. Warstwa może także zmienić protokół bez wpływu na oprogramowanie warstw wyższych.

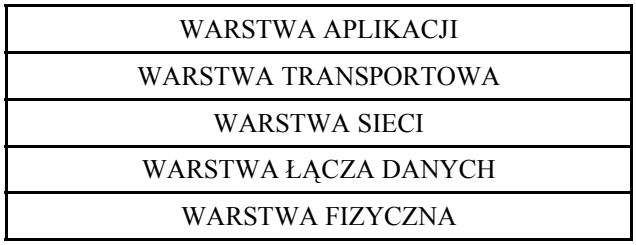
Model TCP/IP nie rozróżnia usług, interfejsów, ani protokołów. Konsekwencją tego jest to, że protokoły w modelu ISO/OSI są lepiej ukryte niż w modelu TCP/IP i mogą być w łatwiejszy sposób zamienione gdy zmiany w technologii będą tego wymagać. Dokonywanie tego typu zmian jest podstawowym celem stworzenia protokołów.[17]

Ewidentną różnicą pomiędzy TCP/IP a modelem ISO/OSI jest to, że protokół może do realizacji swoich funkcji wykorzystywać protokół należący do warstwy niższej bez konieczności przechodzenia przez warstwę pośrednią (np. Aplikacja ping korzysta z protokołu ICMP bezpośrednio, bez uciekania się do mechanizmów warstwy transportowej, a protokół ten przypisany jest do warstwy sieciowej). Innym przykładem nieprzestrzegania ścisłej hierarchii w zestawie protokołów TCP/IP jest sytuacja, gdy protokół niższy zamyka protokół wyższy bez komunikacji protokołów wyższych.[7]

Kolejną różnicą pomiędzy modelami TCP/IP i ISO/OSI była kolejność tworzenia modelu i samych protokołów. Model ISO/OSI został utworzony najpierw a następnie odpowiadające mu protokoły. Ta kolejność oznacza, że ten model nie jest związany z żadnym zbiorem protokołów i w związku z tym jest on ogólny. Gdy zaczęto budować sieci oparte na modelu ISO/OSI i istniejące protokoły, okazało się, że te sieci nie pasują do wymaganych specyfikacji usług. Dlatego też musiano dodać podobne podwarstwy do modelu, aby stworzyć dokumentację dla zaistniałych różnic. Kolejność tworzenia modelu TCP/IP i protokołów była odwrotna. Najpierw powstały protokoły a sam model był po prostu opisem już istniejących protokołów. W tym przypadku nie było problemu z tym aby protokoły pasowały do modelu. Jedynym problemem jest to, że model TCP/IP nie pasuje do żadnego innego stosu protokołów, więc nie może być używany do opisywania sieci innych niż TCP/IP.

Jeszcze jedną różnicą jest rozbieżność w sposobie komunikacji zorientowanej połączeniowo lub bezpołączeniowo. Model ISO/OSI wspiera oba rodzaje komunikacji w warstwie sieciowej, jednak w warstwie transportowej tylko komunikację zorientowaną połączeniowo. Model TCP/IP w warstwie sieciowej wspiera tylko komunikację zorientowaną bezpołączeniowo, natomiast w warstwie transportowej wspiera oba rodzaje komunikacji, dając w ten sposób możliwość wyboru między nimi użytkownikowi.

Podsumowując, modele TCP/IP i ISO/OSI różnią się w zasadniczy sposób. Model ISO/OSI z wykluczeniem warstw sesji i prezentacji jest bardzo użyteczny do opisywania sieci komputerowych. Jednak protokoły tego modelu nie stały się popularne. W przeciwieństwie model TCP/IP nie jest używany, jednak jego protokoły są szeroko używane. Jednak w modelu TCP/IP warstwa dostępu do sieci nie jest właściwie warstwą. Jest ona raczej interfejsem pomiędzy warstwami łącza danych i sieciową. Dlatego też w wielu opracowaniach można spotkać hybrydowy model stworzony z dwóch omawianych wyżej modeli TCP/IP i ISO/OSI.[17]



Rysunek 4. Hybrydowy model TCP/IP i ISO/OSI

W tej pracy jako model odniesienia będzie używany model hybrydowy, który będzie nazwany modelem odniesienia TCP/IP.

2. Protokół IP i ICMP

2.1. Protokół IP

Zadaniem sieci internetowej jest udostępnianie jednolitego systemu komunikacyjnego. Aby ten cel można było zrealizować oprogramowanie protokołów sieci logicznych musi ukrywać szczegóły sieci fizycznych. Zasadniczą różnicą pomiędzy siecią logiczną a fizyczną jest to, że sieć logiczna jest jedynie modelem opracowanym przez jego projektantów i działa tylko dzięki oprogramowaniu. Projektanci takich sieci mogą w dowolny sposób dobierać adresy, metody dostarczania oraz formaty pakietów niezależnie od szczegółów sprzętowych.

Krytycznym elementem modelu sieci logicznej jest adresacja. Aby nadać obraz pojedynczemu systemowi, wszystkie komputery muszą mieć jednolity schemat adresowania a każdy adres musi być jednoznaczny. Tak więc, największym problemem w sieciach logicznych jest to, że sieć logiczna może być budowana na wielu technikach sieciowych, co powoduje, że fizyczny adres sieci nie wystarcza.

Aby zagwarantować jednolite adresowanie we wszystkich węzłach sieci logicznej, oprogramowanie protokołów określa schemat adresowania, który jest niezależny od bazowych adresów fizycznych, co pozwala na stworzenie wielkiej, jednolitej sieci.

W stosie protokołów TCP/IP adresowanie jest zdefiniowane w protokole warstwy internetowej – IP. IP jest najważniejszym protokołem usług bezpołączeniowych, określającym podstawową jednostkę przesyłania danych w sieciach TCP/IP, reguły przetwarzania i przenoszenia datagramów, metodykę generowania komunikatów o błędach oraz schemat adresowania. Standard adresowania określa dla każdego węzła adres węzła w protokole internetowym, który jest 32-bitowym lub 128-bitowym numerem przypisanym węzłowi, nazywany **adresem IP** lub **adresem internetowym**. Pakiet wysyłany przez sieć zawiera zarówno adres IP nadawcy jaki i odbiorcy.[7]

Protokół IP jest protokołem bezpołączeniowym, tzn. że przed przesyłaniem danych protokół ten nie wymienia żadnych informacji sterujących do ustanowienia logicznego połączenia po obu stronach. Protokół IP zdaje się na inne warstwy, gdy konieczna jest realizacja usług wymagających połączenia. Także wykrywanie i ewentualne usuwanie błędów protokół IP zrzuca na protokoły innych warstw.[2]

Adres IP jest dzielony na dwie części, co zapewnia efektywne wyznaczanie tras:

- prefiks – jest to adres identyfikujący sieć fizyczną, do której jest podłączony dany komputer
- sufiks – wskazuje konkretny komputer w danej sieci

Oznacza to, że w każdej sieci fizycznej jest przypisana jednoznaczna wartość – numer sieci. Pojawia się on jako prefiks w adresie każdego komputera podłączonego do danej sieci. Każdy komputer w danej sieci fizycznej ma przypisany jednoznaczny sufiks adresu. Żadne dwie sieci nie mogą mieć przyznanego tego samego numeru ani też żadne dwa komputery w ustalonej sieci nie mogą mieć przyznanego tego samego sufiksu. Wartość sufiksu może być jednak wykorzystywana w więcej niż jednej sieci.

Hierarchia adresów IP zapewnia dwie istotne własności:

- Każdy komputer ma przyznany jednoznaczny adres – dany adres nie jest nigdy przypisany do więcej niż jednego komputera. Własność ta jest zapewniona, gdyż pełny adres zawiera zarówno prefiks, jak i sufiks, które są przyznane tak, aby zagwarantować jednoznaczność. Jeśli dwa komputery są przyłączone do różnych sieci fizycznych, to ich adresy mają różne prefiksy. Jeśli zaś dwa komputery są podłączone do tej samej sieci fizycznej, to ich adresy mają różne sufiksy.
- Pomimo, że przypisania numerów sieci muszą być koordynowane globalnie, sufiksy muszą być przyznane lokalnie bez globalnego uzgadniania.[7]

Istnieją 2 rodzaje protokołu IP w warstwie internetowej. 32-bitowy protokół IPv4 oraz 128-bitowy protokół IPv6. Obydwa protokoły zostaną przedstawione w dalszych rozdziałach tej pracy.

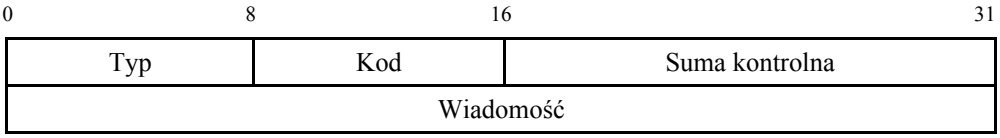
2.2. Protokół ICMP

Internet Control Message Protocol (ICMP) jest protokołem należącym do rodziny protokołów TCP/IP. ICMP jest protokołem kontrolnym. Służy wymianie informacji na temat działania sieci. Informuje o błędach i innych ważnych sytuacjach oraz pomaga kontrolować połączenie. Protokół IP jest zawodny i zdarzają się sytuacje, kiedy któryś z routerów nie może dostarczyć pakietu do odbiorcy. Router musi wtedy poinformować o tym nadawcę. Używa do tego pakietów ICMP. Protokół ICMP używa protokołu IP do przesyłania wiadomości. Każda informacja ICMP jest zawarta w pakiecie IP.

Rysunek 5. Enkapsulacja protokołu ICMP w pakiecie IP

Bezpośrednio za nagłówkiem rozpoczyna się obszar przeznaczony na dane komunikatu ICMP. Jego wielkość jest zmienna a umieszczane w nim informacje są różne w zależności od typu komunikatu. W przypadku wysyłania komunikatu o błędzie na końcu obszaru danych zawsze umieszczany jest początek pakietu, podczas przesyłania którego wystąpił błąd. Dzięki temu urządzenie wysyłające pakiet może, po odebraniu komunikatu ICMP o błędzie, sprawdzić który program wysyłał pakiet i poinformować go o sytuacji jaka wystąpiła.

Pakiet ICMP składa się z nagłówka i danych. Nagłówek ma zawsze wielkość 32 bitów (4 bajtów) i znajdują się w nim trzy pola. Pierwsze z nich ma wielkość 8 bitów i przeznaczone jest na typ wiadomości ICMP. Drugie również ma wielkość 8 bitów i jest przeznaczone na kod wiadomości, który pozwala bardziej szczegółowo zidentyfikować rodzaj komunikatu. Kody mają różne znaczenia w zależności od typu komunikatu ICMP, przy czym pole kodu nie jest wykorzystywane przez każdy typ wiadomości. Trzecie pole nagłówka ICMP zajmuje 16 bitów i zawiera sumę kontrolną obliczoną z całej wiadomości ICMP (nagłówka i danych). Suma kontrolna pozwala wykryć ewentualne uszkodzenia przesyłanego pakietu. Uzyskiwana jest na podstawie takiego samego algorytmu jak suma kontrolna nagłówka IP. Do jej obliczenia musi być skompletowana cała wiadomość ICMP a miejsce przeznaczone na sumę wypełnia się zerami.[8]

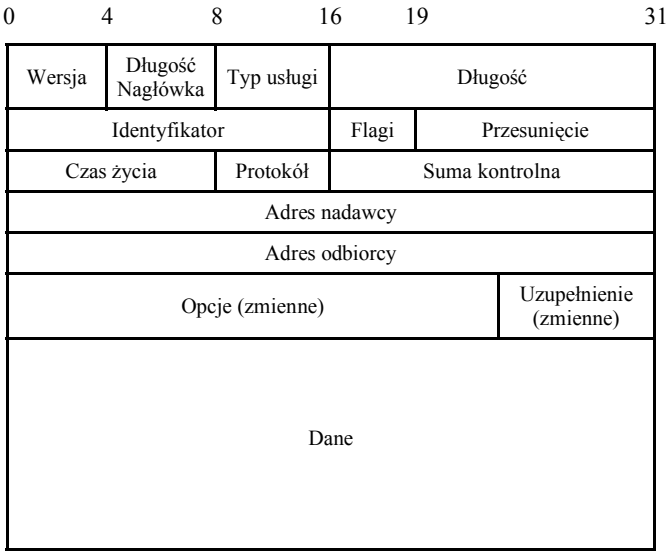


Rysunek 6. Nagłówek pakietu ICMP

3. Protokół IPv4

3.1. Nagłówek protokołu IPv4

Budowę pakietu IPv4 pokazuje rysunek 7. Pakiet IPv6 składa się z części nagłówka i części danych. Nagłówek pakietu wynosi minimalnie 20 bajtów a maksymalnie 60 bajtów. Dane mogą mieć różną długość, jednak cały pakiet (nagłówek + dane) nie może wynosić więcej niż 65 535 bajtów[15].



Rysunek 7. Nagłówek protokołu IPv4

Najważniejsze pola nagłówka IPv4 to:

Wersja – podaje numer używanej aktualnie wersji protokołu IP. Pole to ma długość 4 bitów. 4 w tym polu oznacza, że jest to nagłówek protokołu IPv4.

Długość nagłówka – pole to informuje jak długi jest nagłówek w słowach 32-bitowych (4-bajtowych). Pole to ma długość 4 bitów. Minimalna wartość tego pola wynosi 5, gdy nagłówek nie zawiera żadnych opcji. Maksymalna wartość tego pola wynosi 15, co ogranicza nagłówek do 60 bajtów a tym samym pole opcji do 40 bajtów.

Typ usługi – wskazuje ustawienia priorytetu pakietów w stosunku do innych pakietów z tego samego źródła. Pole to ma długość 8 bitów. Zawiera ono informacje dotyczące, pierwszeństwa, opóźnienia, przepustowości oraz parametry niezawodności. W praktyce, routery często ignorują to pole.

Długość – określa rozmiar pakietu w bajtach (nagłówek + dane). Maksymalny rozmiar pakietu wynosi 65 535 bajtów. Pole to ma długość 16 bitów.

Identyfikator – identyfikuje określony pakiet IP. Jeśli pakiet ulegnie fragmentacji podczas przesyłania, informacja zawarta w tym polu jest wykorzystywana do ponownego złożenia informacji w miejscu przeznaczenia. Wszystkie fragmenty pakietu mają tą samą wartość w polu identyfikator. Pole to ma długość 16 bitów.

Flagi – zawiera znaczniki fragmentacji. Pole to ma długość 3 bitów, ale obecnie wykorzystywane są tylko 2 spośród nich. Bit najmniej znaczący wskazuje czy jest to fragment końcowy w datagramie, czy też będzie ich więcej. Drugi bit najmniej znaczący wskazuje, czy datagram może być fragmentowany, czy też nie.

Przesunięcie – wskazuje pozycję fragmentu w stosunku do oryginalnego ładunku IP. Wszystkie fragmenty z wyjątkiem ostatniego muszą być wielokrotnością 8 bajtów. Ponieważ pole to ma długość 13 bitów, maksymalną liczbą fragmentów przypadającą na jeden pakiet jest 8192, powodując tym samym, że maksymalna długość pakietu wynosi 65 536 bajtów. Jest to o jeden bajt więcej niż wskazuje pole długość.

Czas życia – wskazuje w sekundach czas przez jaki dany datagram pozostaje w sieci (maksymalnie 255), zanim zostanie odrzucony. Ilekroć dany datagram przechodzi przez router, czas życia zostaje zmniejszony conajmniej o jeden. Jeśli pakiet czeka w kolejce przez dłuższy czas wartość tego pola zmniejszane jest wielokrotnie (co sekundę o jeden). Ponieważ router normalnie przekazuje pakiet IP w czasie mniejszym niż jedna sekunda, ustawienia tego pola staje się faktyczną liczbą przeskoków. Pole to ma długość 13 bitów. Wartość tego pola ustawiana jest przez komputer źródłowy i zmniejszana w każdym węźle sieci. Jeśli wartość czasu życia spadnie do zera, datagram jest niszczony, a protokół ICMP wysyła do hosta komunikat o wystąpieniu błędu. Działanie tego pola zabezpiecza sieć przed przeciążeniem pakietami, które z różnych powodów nie mogą dotrzeć do hosta, a także zabezpiecza pakiety przed krążeniem w sieci bez końca.

Protokół – wskazuje protokół, który dał protokołowi IP ładunek do wysłania. Pole to ma długość 8 bitów. Informacja zawarta w tym polu jest wykorzystywana przez warstwy wysokiego poziomu w hoście docelowym do przetwarzania ładunku.

Suma kontrolna – wykorzystywana jest wyłącznie do sprawdzania integralności nagłówka. Pole to ma długość 16 bitów. Ponieważ pole czas życia zmienia swoją wartość przy każdym przeskoku, suma kontrolna jest ponownie obliczana ilekroć datagram przechodzi przez router. Jest ona wyznaczana z wykorzystaniem metody dopełnień do jedności wyłącznie dla danych zapisanych w nagłówku.

Adres nadawcy – zawiera adres nadawcy. Pole to ma długość 32 bitów.

Adres odbiorcy – zawiera adres odbiorcy. Pole to ma długość 32 bitów.

Opcje – pole to zostało stworzone, aby umożliwić kolejnym wersjom protokołu dołączenie informacji, które nie zostały zawarte w oryginalnym projekcie. Opcje mogą zajmować przestrzeń na końcu nagłówka IP. Oryginalnie, zostało zdefiniowanych pięć opcji , jednak z biegiem czasu były dodawane kolejne. Listę opcji można znaleźć na stronie http://www.iana.org/assignments/ip-parameters.[17]

Opcje	Działanie
Bezpieczeństwo	Określa jak tajny jest pakiet
Ścisły routing	Podaje dokładną trasę, którą musi pokonać pakiet
Luźny routing	Podaje listę routerów, które nie mogą zostać pominięte
Zapisywanie trasy	Powoduje zapisanie adresów IP wszystkich routerów, przez które przechodził pakiet
Stempel czasowy	Powoduje zapisanie adresów IP wraz z dokładnym czasem przejścia pakietu przez kolejne routery

Rysunek 8. Pięć podstawowych opcji nagłówka IPv4

Uzupełnienie – jeśli pole opcji nie zajmuje pełnego słowa to zostaje uzupełnione do 32 bitów.[7]

3.2. Format adresu IPv4 i adresy specjalnego przeznaczenia

Adres IPv4 jest adresem 32 bitowym. Normalną praktyką zapisywania adresu IPv4 jest dzielenie go na 4 bajty (oktety) a następnie obliczanie wartości dziesiętnej dla każdego z oktetów (wartości od 0 do 255). Oktety te oddzielone są kropkami i stąd wywodzi się termin ***kropkowa notacja dziesiętna*** (np. szesnastkowo wyrażony adres IPv4 C0290614 w notacji kropkowo dziesiętnej wygląda tak 192.41.6.20). Najmniejszym numerem IPv4 jest 0.0.0.0 a największym 255.255.255.255[1].Format dziesiętny kropkowy wykorzystuje się do wpisywania i wyświetlania adresów IP w szerokiej gamie graficznych interfejsów użytkownika (GUI).[7]

Istnieje szereg adresów IPv4 specjalnego przeznaczenia. Dla wygody, zamiast przyznawania adresu każdemu komputerowi , można określić adresy, które mogą być przypisywane do pewnej sieci lub zbiorowi komputerów. IPv4 określa zestawy adresów o szczególnej postaci, które są zarezerwowane – nie są one nigdy przyznawane komputerom.

Prefiks	*Sufiks*	*Typ adresu*	*Przeznaczenie*
Same zera	Same zera	Bieżący komputer	Używany przy rozruchu
Sieciowy	Same zera	Sieć	Identyfikuje sieć
Sieciowy	Same jedynki	Rozgłaszanie ukierunkowane	Rozgłaszanie w określonej sieci
Same jedynki	Same jedynki	Rozgłaszanie ograniczone	Rozgłaszanie w sieci lokalnej
127	Cokolwiek	Pętla zwrotna	Testowanie

Rysunek 9. Postacie adresów IPv4 specjalnego przeznaczenia

Adres bieżącego komputera – zestaw protokołów TCP/IP obejmuje protokoły, których komputer może używać przy automatycznym uzyskiwaniu adresu IPv4 przy starcie. Komputer korzystając z takich protokołów uruchomieniowych nie może podać prawidłowego adresu IPv4 nadawcy. Radzi sobie w takich sytuacjach tak, że adres IPv4 składa się z samych zer i oznacza adres bieżącego komputera.

Adresy sieciowe – odnoszą się do samej sieci, a nie do komputerów podłączonych do niej. Nie powinien się nigdy pojawić jako adres docelowy w pakiecie. Adres sieci tworzony jest przez przepisanie w niezmienionej postaci wszystkich bitów adresu IPv4, dla których odpowiednie bity maski mają wartość jeden. Resztę należy uzupełnić zerami.

Adres rozgłaszania ukierunkowanego – używany jest do wysyłania kopii pakietu do wszystkich węzłów sieci fizycznej pod adres danej sieci. Przez sieć podróżuje tylko jedna kopia pakietu, aż dotrze do danej sieci. Następnie pakiet ten jest dostarczany do wszystkich węzłów tej sieci. Adres ten jest tworzony przez dodanie do jej prefiksu sufiksu, który cały składa się z jedynek.

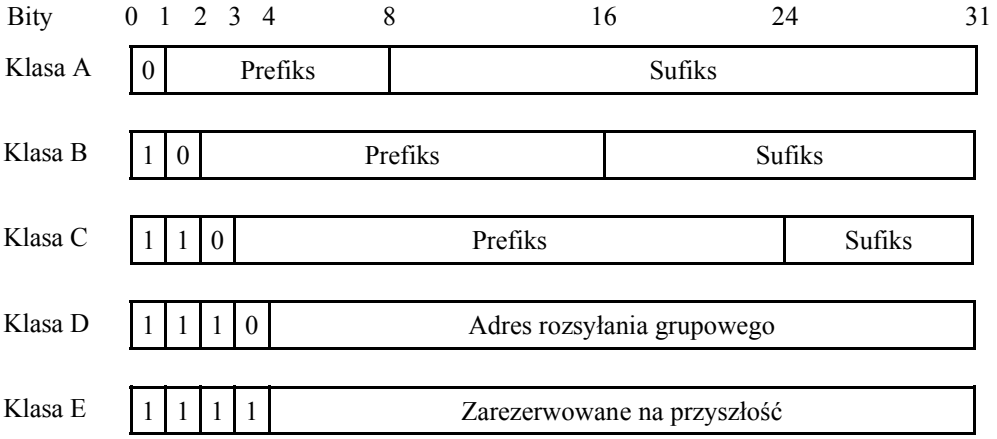
Adres rozgłaszania ograniczonego – odnosi się do rozgłaszania w lokalnej sieci fizycznej. Jest ono używane przy starcie systemu przez komputery, które nie znają w tym momencie numeru sieci. IPv4 na rozgłaszanie ograniczone rezerwuje adres składający się z samych jedynek. W ten sposób pakiet wysyłany pod tym adresem oprogramowanie IPv4 rozgłosi w sieci lokalnej.

Adresy pętli zwrotnej – służą do komunikacji z wykorzystaniem protokołu IPv4 z lokalnym komputerem. Jest to adres zawsze przypisany komputerowi, na którym właśnie pracujemy, ponieważ pakiety z takimi adresami nie powinny wydostawać się na zewnątrz komputera, nie powodując żadnych konfliktów. Protokół IPv4 rezerwuje prefiks sieciowy klasy A równy 127 na adresy pętli zwrotnej. Adres węzła (sufiks) używany przy tym jest bez znaczenia. Najpopularniejszym adresem pętli zwrotnej jest 127.0.01.[7]

3.3. Klasy adresów IPv4

Każdy host i router w Internecie ma adres IP, który zawiera numer sieci i numer hosta. Po wybraniu adresu IPv4 i podzieleniu go na dwie części należy jeszcze określić ile bitów umieścić w każdej części. Prefiks musi mieć wystarczającą liczbę bitów, aby umożliwiał przypisanie każdej sieci fizycznej jednoznacznego numeru sieci. Sufiks musi mieć wystarczającą liczbę bitów, aby umożliwić przypisanie jednoznacznego sufiksu każdemu komputerowi podłączonemu do sieci. Opracowany został schemat adresowania, który może działać przy kombinacji dużych i małych sieci. Przestrzeń adresowa została podzielona na podstawowe klasy, z których każda ma inny rozmiar prefiksu i sufiksu.

Pierwsze cztery bity adresu określają klasę do której należy adres, oraz sposób podziału pozostałej części adresu na prefiks i sufiks.[7]



Rysunek 10. Pięć klas adresów IPv4

Na rysunku 10 został przedstawiony podział adresów IP na 5 klas. Klasy A, B, i C są zwane klasami pierwotnymi, gdyż są przeznaczone na adresy komputerów. Klasa D jest wykorzystywana przy rozsyłaniu grupowym, które umożliwia dostarczenie informacji do zbioru komputerów. Aby użyć rozsyłania grupowego IP, zbiór węzłów musi zgodzić się na wspólny adres rozsyłania grupowego. Po ustanowieniu grupy rozsyłania kopia każdego pakietu wysłanego pod dany adresem rozsyłania będzie dostarczona do każdego komputera będącego członkiem grupy.[7]

Sieci klasy A – w tej klasie tożsamość sieci określana jest przez wartość pierwszego oktetu (ośmiu bitów). Dlatego są one często określane jako sieci/8. Ponieważ zakres wartości dla pierwszego oktetu adresu klasy wynosi od 1 do 126, istnieje 126 niepowtarzalnych sieci klasy A. pozostałe 24 bity adresu identyfikują hosta. Tożsamości hostów nie mogą być wyłącznie jedynkami, ani wyłącznie zerami, więc maksymalna liczba hostów w każdej sieci klasy A to 2^{24}-2. Blok adresowy klasy A zawiera 2^{31} indywidualnych adresów (łącznie z zarezerwowanymi wartościami pierwszego oktetu, wynoszącymi 0 oraz 27), a przestrzeń adresowa IPv4 zawiera 2^{32} adresów. Stąd przestrzeń adresowa klasy A stanowi 50% całkowitej przestrzeni adresowej IPv4. Przykładowy adres tej klasy ma postać: 10.0.0.0, gdzie id. sieci : 10.

Sieci klasy B – w tej klasie tożsamość sieciowa określana jest przez wartość pierwszych dwóch oktetów (16 bitów). Sieci klasy B są zatem określane jako sieci/16. Dwa pierwsze bity identyfikują daną sieć jako sieć klasy B, co pozostawia 14 bitów na określenie niepowtarzalnych tożsamości sieciowych. Stąd też można zdefiniować 2^{14}, albo 16 384 sieci klasy B, przy czym każda z nich może mieć 2^{16}-2 hostów. Blok adresowy klasy B zawiera 2^{30} adresów i stanowi 25% całkowitej przestrzeni adresowej IPv4. Przykładowy adres tej klasy ma postać: 128.3.2.3, gdzie id. sieci: 128.3; id. węzła: 2.3.

Sieci klasy C – w tej klasie tożsamość sieciowa określana jest przez wartość pierwszych trzech oktetów (24 bitów). Sieci klasy C są zatem określane jako sieci/24. Trzy pierwsze bity identyfikują daną sieć jako sieć klasy C, co pozostawia 21 bitów na określenie niepowtarzalnych tożsamości sieciowych. Stąd też można zdefiniować 2^{21} sieci klasy C, przy czym każda z nich może mieć do 2^{8}-2, lub 254 hosty. Blok adresowy klasy C zawiera 2^{29} adresów i stanowi 12,5% całkowitej przestrzeni adresowej IPv4. Przykładowy adres tej klasy ma postać: 192.0.1.255, gdzie id. sieci: 192.0.1; id. węzła: 255.

Sieci klasy D i E – sieci klasy D wykorzystywane są do multiemisji, gdzie pojedynczy adres sieciowy identyfikuje grupę hostów. Sieci klasy E zarezerwowane są do celów doświadczalnych. Blok klasy D stanowi 6,25% całkowitej przestrzeni adresowej IPv4, a blok klasy E nieznacznie mniejszą część, ponieważ 255 nie jest wykorzystywane jako wartość pierwszego oktetu.[7]

Istnieje możliwość obliczenia klasy adresu na podstawie samego adresu, dlatego też adresy IPv4 nazywane są samoidentyfikującymi się. Poniżej przedstawiona jest tablica, która może być wykorzystywana przy obliczaniu klasy adresu. Pierwsze 4 bity adresu są wydobywane i wykorzystywane jako indeks w tablicy.

Pierwsze 4 bity adresu	*Indeks w tablicy (dziesiętnie)*	*Klasa adresu*
0000	0	A
0001	1	A
0010	2	A
0011	3	A
0100	4	A
0101	5	A
0110	6	A
0111	7	A
1000	8	B
1001	9	B
1010	10	B
1011	11	B
1100	12	C
1101	13	C
1110	14	D
1111	15	E

Rysunek 11. Tablica, która może by wykorzystywana przy obliczaniu klasy adresu.

Osiem kombinacji , które zaczynają się od 0 odpowiadają klasie A. Cztery kombinacje, które zaczynają się od 10 odpowiadają klasie B, a dwie kombinacje zaczynające się od 110 odpowiadają klasie C. Adres zaczynający się od 111 należy do klasy D. Adres, który zaczyna się od 1111 należy do klasy E, która nie jest obecnie używana.

Aby rozpoznać klasy adresów w notacji dziesiętnej z kropkami musimy zamienić pierwszy oktet adresu na wartości dziesiętne.

Klasa	**Zakres wartości**
A	Od 0 do 127
B	Od 128 do 191
C	Od 192 do 223
D	Od 224 do 239
E	Od 240 do 255

Rysunek 12. Zakresy wartości dziesiętnych odpowiadające poszczególnym klasom adresów

3.4. ICMPv4

Protokół IPv4 przesyła pakiety od nadawcy poprzez routery do odbiorcy. Jest on zawodny i zdarzają się sytuacje, kiedy któryś z routerów nie może dostarczyć pakietu do odbiorcy. Router musi wtedy poinformować o tym nadawcę. Protokół ICMPv4 umożliwia oznajmianie o różnego rodzaju nieoczekiwanych sytuacjach w sieci.

Istnieje kilka reguł przesyłania pakietów ICMPv4. Komunikaty protokołu ICMP informujące o błędach nie mogą być wysyłane jako odpowiedź na:

- inny komunikat ICMP o błędzie
- pakiet, który nie przeszedł testów poprawności nagłówka IP podczas przesyłania poprzez router (RFC1812)
- pakiet z nieprawidłowym lub wskazującym na więcej niż jeden host adresem źródłowym
- pakiet z adresem docelowym typu broadcast lub multicast (przeznaczony dla więcej niż jednego urządzenia)
- pakiet wysyłany jako broadcast lub multicast w warstwie drugiej modelu OSI - łącza danych
- pakiet zawierający inny niż pierwszy fragment przesyłanego datagramu

Zasady te obowiązują po to, aby uniknąć lawinowego powstawania komunikatów ICMP, które szybko doprowadziłyby do przeciążenia sieci. Bez nich zdarzałyby się sytuacje kiedy z pojedynczego pakietu powstawały by bez końca kolejne komunikaty lub tworzyłyby się tzw. sztormy broadcastowe jako wynik błędnych pakietów broadcastowych. Ponadto komunikaty ICMP o błędach zawierają nagłówek IP oraz co najmniej pierwsze 8 bajtów datagramu, podczas przesyłania którego wystąpił błąd. Nagłówek IP i fragment datagramu muszą być zwrócone w takiej postaci, w jakiej znajdowały się podczas wystąpienia błędu.[3]

Rysunek 13. Lista komunikatów ICMPv4

Typ	*Kody komunikatu*	*Nazwa komunikatu*	*Informacja*	*Błąd*
8	Nieużywane – zawsze 0	Żądanie echa (Echo Request)	tak	
0	Nieużywane – zawsze 0	Odpowiedź na echo (Echo Reply)	tak	

Typ	*Kody komunikatu*	*Nazwa komunikatu*	*Informacja*	*Błąd*
3	- 0 - sieć nieosiągalna (Net unreachable) - 1 - host nieosiągalny (Host unreachable) - 2 - protokół niedostępny (Protocol unreachable) - 3 - port niedostępny (Port unreachable) - 4 - datagram zbyt duży, konieczna fragmentacja podczas gdy w nagłówku protokołu IP ustawiony jest bit DF [do not fragment - nie fragmentuj] (Fragmentation needed and DF set) - 5 - (Source route failed) - 6 - nieznana sieć docelowa (destination network unknown) - 7 - nieznane urządzenie docelowe (destination host unknown) - 8 - urządzenie źródłowe odizolowane (source host isolated) - 9 - komunikacja z siecią docelową zabroniona przez administratora (communication with destination network administratively prohibited) - 10 - komunikacja z hostem docelowym zabroniona przez administratora (communication with destination host administratively prohibited) - 11 - pakiet nie może zostać wysłany do sieci ze względu na ustawienia TOS w nagłówku IP (network unreachable for type of service) - 12 - pakiet nie może zostać wysłany do urządzenia ze względu na ustawienia TOS w nagłówku IP (host unreachable for type of service) - 13 - komunikacja zabroniona przez administratora (Communication Administratively Prohibited) - 14 - (Host Precedence Violation) - 15 - (Precedence Cut off in Effect)	Cel nieosiągalny (Host Unreachable)		tak
4	Nieużywane – zawsze 0	Tłumienie źródła (Source Quench)		tak
5	- 0 - przekierowanie datagramów do sieci (Redirect datagrams for the Network) - 1 - przekierowanie datagramów do hosta (Redirect datagrams for the Host) - 2 - przekierowanie datagramów z ustawionym polem TOS w nagłówku IP do sieci (Redirect datagrams for the Type of Service and Network) - 3 - przekierowanie datagramów z ustawionym polem TOS w nagłówku IP do hosta (Redirect datagrams for the Type of Service and Host)	Przekierowanie (Redirect)		tak
9	- 0 - zwykłe zgłoszenie routera - 16 - zgłoszenie routera nie przekazującego zwykłego ruchu	Ogłoszenie routera (Router Advertisment)	tak	
10	Nieużywane – zawsze 0	Poszukiwanie routera (Router Solicitation)	tak	
11	- 0 - upłynął czas na przesłanie datagramu do hosta docelowego (time to live exceeded in transit) - 1 - upłynął czas na skompletowanie datagramu na hoście docelowym (fragment reassembly time exceeded)	Przekroczenie czasu (Time Exceeded)		tak
12	- 0 - błąd we wskazanym oktecie pakietu (pointer indicates the error) - 1 - brak wymaganej opcji w nagłówku (required option is missing)	Problem z parametrem (Parameter Problem)		tak

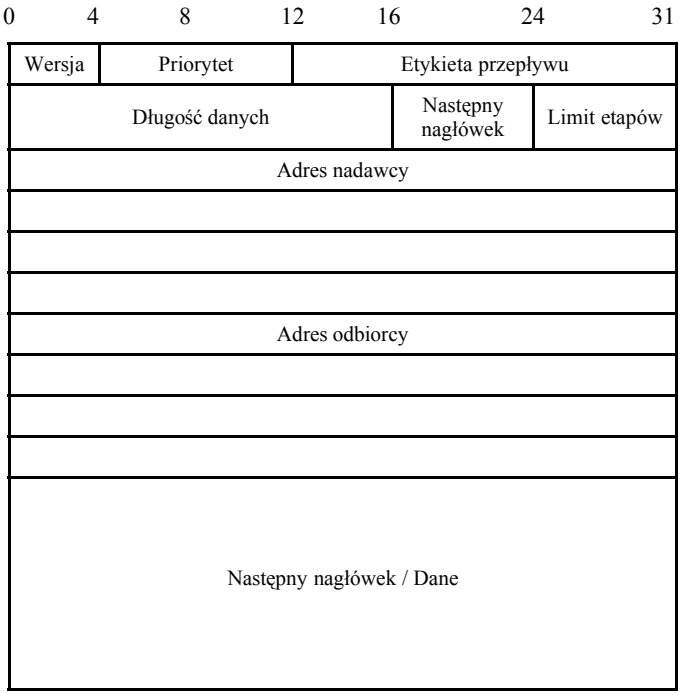
Typ	*Kody komunikatu*	*Nazwa komunikatu*	*Informacja*	*Błąd*
13	Nieużywane – zawsze 0	Pytanie o czas (Timestamp Request)	tak	
14	Nieużywane – zawsze 0	Odpowiedź z czasem ((Timestamp Reply)	tak	
15	Nieużywane – zawsze 0	Żądanie informacji o adresie (Information Request)	tak	
16	Nieużywane – zawsze 0	Odpowiedź z informacją o adresie (Information Reply)	tak	
17	Nieużywane – zawsze 0	Pytanie o maskę (Address Mask Request)	tak	
18	Nieużywane – zawsze 0	Odpowiedź z maską (Address Mask Reply)	tak	
30	- 0 - pakiet został dostarczony do kolejnego urządzenia - 1 - brak dalszej drogi dla pakietu, pakiet porzucony	Wyznaczanie trasy (Traceroute)	tak	

Dokładne informacje o budowie i działaniu poszczególnych komunikatów ICMPv4 znajdują się na stronie http://www.republika.pl/wamarek/icmp/index.html.[3]

4. Protokół IPv6

4.1. Nagłówek protokołu IPv6

Budowę pakietu IPv6 pokazuje rysunek 14. Pakiet IPv6 składa się z części nagłówka i części danych. Nagłówek pakietu wynosi 40 bajtów. Dane mogą mieć różną długość, jednak cały pakiet (nagłówek + dane) nie może wynosić więcej niż 65 535 bajtów. Pakiety większe od 65 535 bajtów mogą być wysyłane przy użyciu opcji jambogramu w nagłówku rozszerzeń międzywęzłowych (Hop-by-Hop)[3].



Rysunek 14. Nagłówek protokołu IPv6

Najważniejsze pola nagłówka IPv6 to:

Wersja - podaje numer używanej aktualnie wersji protokołu IP. Pole to ma długość 4 bitów. 6 w tym polu oznacza, że jest to nagłówek protokołu IPv6.

Priorytet – Określa numer priorytet pakietu w stosunku do innych pakietów pochodzących z tego samego źródła. Pole to wynosi 8 bitów[3].

Wartość priorytetu	*Znaczenie pakietu*
0	Brak priorytetu
1	Ruch “w tle”
2	Transfer danych bez nadzoru
3	Nie zdefiniowane
4	Nadzorowany przepływ danych
5	Nie zdefiniowane
6	Interaktywny przepływ danych
7	Informacje sterujące i zarządzające

Rysunek 15. Numery priorytetów nadawane pakietom IPv6 i ich znaczenie

Etykieta przepływu – identyfikuje wymagający specjalnej obsługi przepływ pakietu przez węzły pośredniczące (np. transmisja w trybie rzeczywistym). Pole to wynosi 20 bitów.

Długość danych – określa wyrażoną w oktetach długość pozostałej następującej po nagłówku części pakietu. Pole to wynosi 16 bitów. Do wartości pola długość danych zaliczane są nagłówki rozszerzeń i PDU warstw wyższych. Jeśli dane są większe niż 65 535 bajtów wtedy pole długość danych ma wartość 0 i użyta zostaje opcja jambogramu w nagłówku rozszerzeń międzywęzłowych (Hop-by-Hop).

Następny nagłówek – identyfikuje pierwszy nagłówek rozszerzeń następujący po nagłówku IPv6 lub protokół PDU wyższej warstwy np. TCP, UDP, lub ICMPv6. Pole to wynosi 8 bitów[3].

Wartość pola	*Znaczenie*
0	Opcje międzywęzłowe
4	IPv6
6	TCP
17	UDP
41	Enkapsulacja nagłówka IPv6
43	Routing
44	Fragmentacja
45	Procedura międzydomenowa
46	Rezerwacja zasobów
50	Bezpieczeństwo enkapsulacji
51	Uwierzytelnianie
58	ICMPv6
59	Brak kolejnego nagłówka
60	Miejsce przeznaczenia

Rysunek 16. Wartości pola następny nagłówek i ich znaczenie

Limit etapów – liczba, która jest zmniejszana o jeden, gdy pakiet przechodzi przez węzeł. Jeśli limit etapów osiągnie 0, to pakiet zostaje zniszczony. Pole to wynosi 8 bitów.

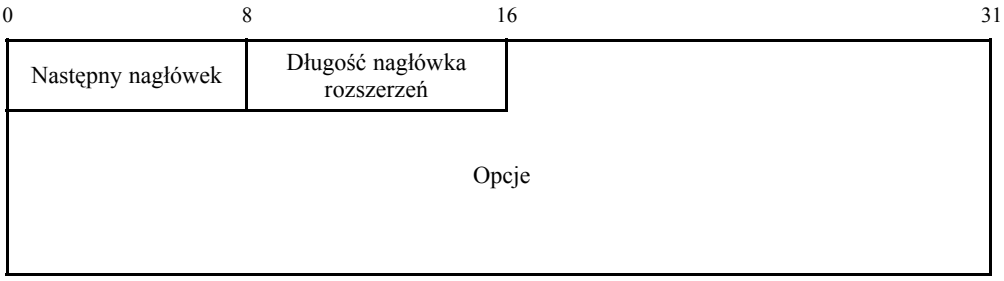
Adres nadawcy – zawiera adres nadawcy pakietu. Pole to wynosi 128 bitów.

Adres odbiorcy – zawiera adres odbiorcy pakietu. Pole to wynosi 128 bitów.

4.2. Nagłówki rozszerzeń protokołu IPv6

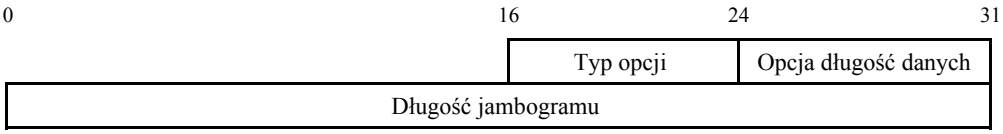
Nagłówek IPv6 ma długość 40 bitów. Tak małą wielkość otrzymano dzięki przesunięciu opcjonalnych funkcji przesyłania i dostarczania do nagłówków rozszerzeń. Typowy pakiet IPv6 nie posiada żadnych nagłówków rozszerzeń. Jeśli dodatkowe opcje są wymagane przez routery pośredniczące lub host docelowy, zostają one umieszczone w nagłówkach rozszerzeń przez host źródłowy. Są one umieszczone pomiędzy nagłówkiem IPv6 oraz nagłówkiem protokołu warstwy wyższej. Nagłówków rozszerzeń jest kilka rodzajów i są one definiowane przez różne wartości pola, następny nagłówek znajdującego się w poprzedzającym nagłówku.[7] W dokumencie RFC 2460 zdefiniowano 6 nagłówków rozszerzeń.

Nagłówek opcje międzywęzłowe (Hop-by-Hop Options Header) – przenosi informację, która musi być sprawdzana i przetwarzana w każdym węźle wzdłuż drogi przesyłania pakietu, również w węźle docelowym. Istnienie tego nagłówka sygnalizowane jest wartością 0 w polu następny nagłówek w nagłówku IPv6[11].



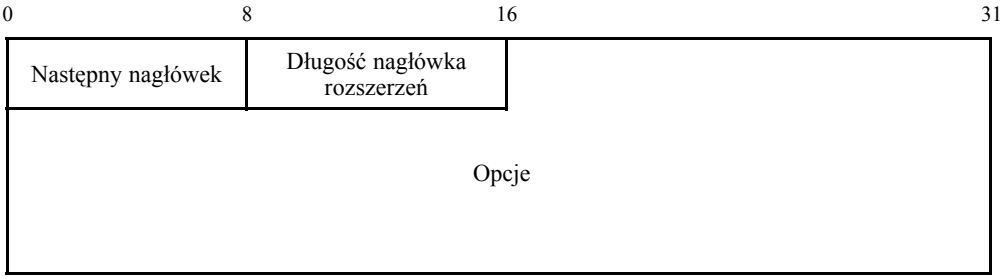
Rysunek 17. Format nagłówka opcje międzywęzłowe

Jedną opcją zdefiniowaną w nagłówku opcji międzywęzłowych jest tak zwana opcja jambogramu. Jambogram jest to pakiet większy niż 64K[12].



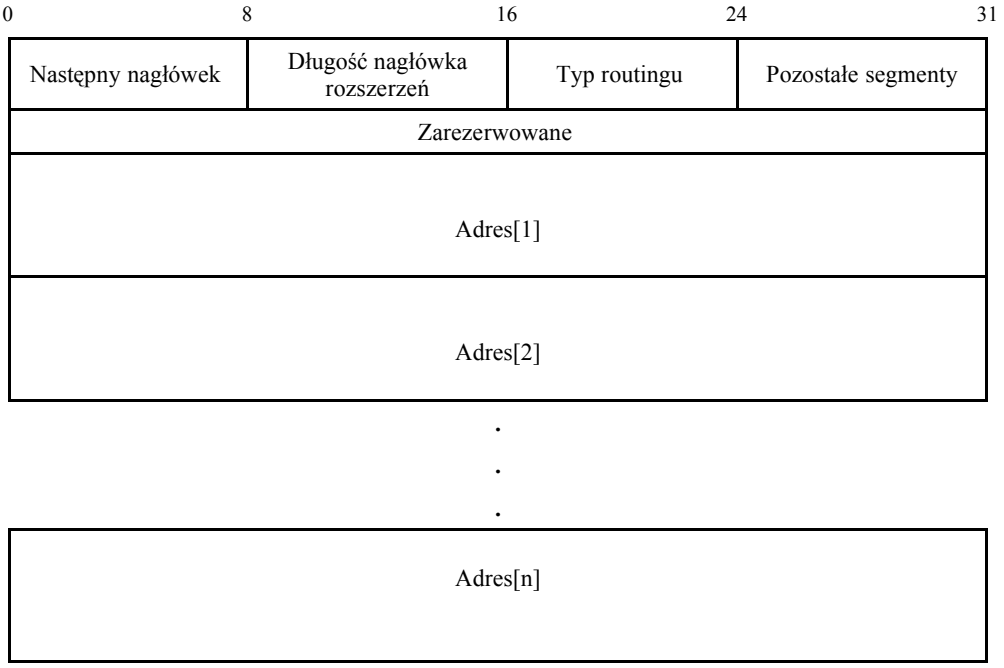
Rysunek 18. Format jambogramu

Nagłówek opcji miejsca przeznaczenia (Destination Options Header) – przenosi informację, która wymaga sprawdzenia tylko w miejscu przeznaczenia. Istnienie tego nagłówka sygnalizowane jest wartością 60 w polu następny nagłówek poprzedzającego nagłówka[11].



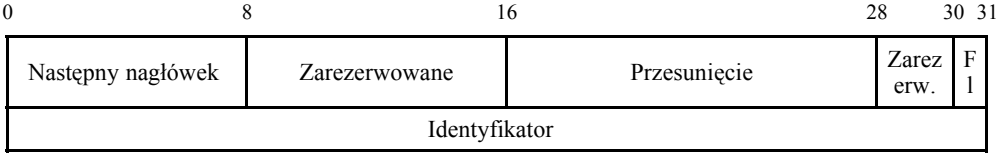
Rysunek 19. Format nagłówka opcji miejsca przeznaczenia

Nagłówek routing (Routing header) – zawiera adres jednego lub więcej węzłów pośrednich, przez które pakiet powinien przejść na drodze od nadawcy do miejsca przeznaczenia. Istnienie tego nagłówka sygnalizowane jest wartością 43 w polu następny nagłówek poprzedzającego nagłówka[11].



Rysunek 20. Format nagłówka routing typu 0

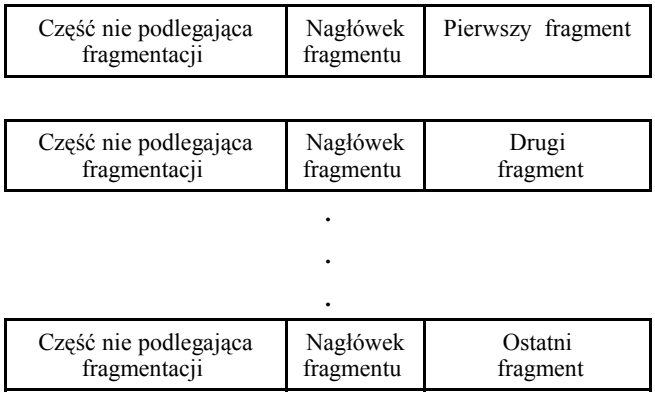
Nagłówek fragmentacji (Fragment header) - wykorzystywany jest przez nadawcę pracującego z protokołem IPv6 do przesyłania pakietów większych od MTU (Maximal Transport Unit) ścieżki, po której pakiet ma trafić do miejsca przeznaczenia. Istnienie tego nagłówka sygnalizowane jest wartością 44 w polu następny nagłówek poprzedzającego nagłówka[11].



Rysunek 21. Format nagłówka fragmentacji

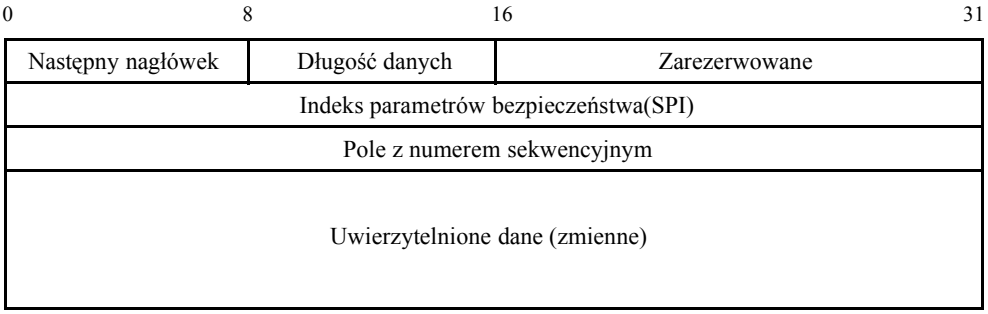
Fragmentacja danych w protokole IPv6 wykonywana jest tylko w węźle, który wysyła pakiety, nie odbywa się natomiast w routerach pośredniczących w przekazywaniu pakietu, znajdujących się na jego ścieżce. Gdy pakiet IPv6 jest fragmentowany jest on początkowo dzielony na dwie części: część nie podlegającej fragmentacji (przetwarzana, przez każdy pośredniczący router i składająca się z nagłówka IPv6, nagłówka opcji międzywęzłowych, nagłówka opcji miejsca przeznaczenia, nagłówka routingu) i części podlegającej fragmentacji (przetwarzanej tylko przez router docelowy i składająca się z pozostałych nagłówków rozszerzeń oraz nagłówka i danych warstwy wyższej). Następnie tworzone są fragmenty pakietu IPv6. Każdy fragment pakietu składa się z części nie podlegającej fragmentacji, nagłówka fragmentacji i części podlegającej fragmentacji.

Rysunek 22. Oryginalny pakiet IPv6



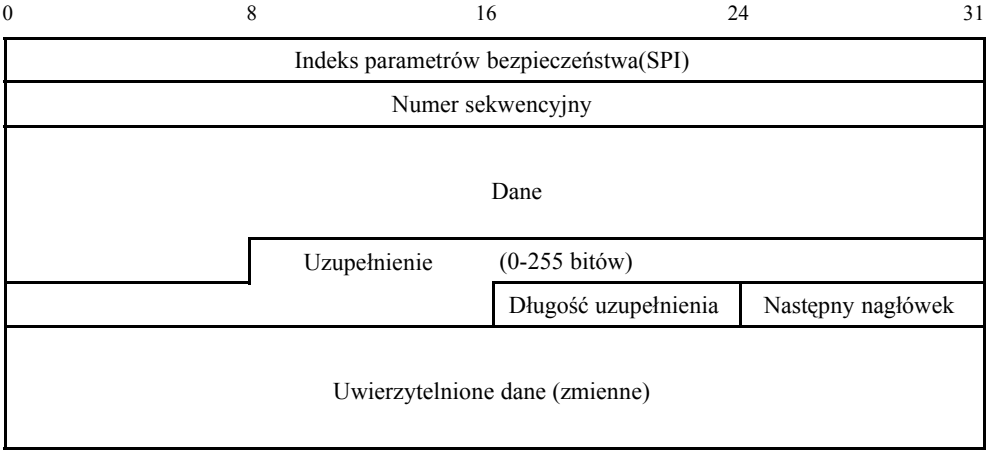
Rysunek 23. Proces fragmentacji IPv6

Nagłówek uwierzytelnianie (Authentication Header) - zapewnia integralność oraz weryfikowanie autentyczności bez zapewnienia poufności. Istnienie tego nagłówka sygnalizowane jest wartością 51 w polu następny nagłówek poprzedzającego nagłówka[9].



Rysunek 24. Format nagłówka uwierzytelniania

Nagłówek bezpieczeństwo enkapsulacji (Encapsulating Security Payload) - zapewnia integralność i poufność danych, może również zapewniać weryfikowanie autentyczności. Istnienie tego nagłówka sygnalizowane jest wartością 50 w polu następny nagłówek poprzedzającego nagłówka[10].



Rysunek 25. Format nagłówka bezpieczeństwo enkapsulacji

Nagłówki rozszerzeń nie są egzaminowane i przetwarzane przez każdy węzeł sieci, a tylko przez odbiorcę (lub odbiorców jeżeli mamy doczynienia z multicastem), zdefiniowanego w polu adres przeznaczenia nagłówka IPv6. Istnieje jeden wyjątek od reguły, że nagłówki rozszerzeń muszą być przetwarzane tylko przez odbiorcę. Jest nim nagłówek, opcje międzywęzłowe (Hop-by-Hop Options) zawierający informacje, które muszą być analizowane i przetwarzane przez każdy węzeł w ścieżce włączając w to nadawcę i odbiorcę.[4]

Pakiet IPv6 może zawierać zero, jeden lub więcej nagłówków rozszerzeń. Jednak, ponieważ tylko jeden z nich musi być przetwarzany przez wszystkie pośrednie węzły w sieci została zdefiniowana kolejność nagłówków w jakiej powinny się one znajdować w pakiecie IPv6:

1. Nagłówek opcji międzywęzłowych (Hop-by-Hop Option header)
2. Nagłówek opcji miejsca przeznaczenia dla węzłów pośrednich (Destionation Options header)
3. Nagłówek routingu (Routing header)
4. Nagłówek fragmentacji (Fragment header)
5. Nagłówek uwierzytelnienia (Authentication header)
6. Nagłówek bezpieczeństwo enkapsulacji (Encapsulating Security Payload)
7. Nagłówek opcji miejsca przeznaczenia dla węzła docelowego (Destionation Options header)[5]

Nagłówek IPv6 Następny nagłówek = 6 (TCP)	Segment TCP		
Nagłówek IPv6 Następny nagłówek = 43 (Routing)	**Nagłówek IPv6** Następny nagłówek = 6 (TCP)	Segment TCP	
Nagłówek IPv6 Następny nagłówek = 43 (Routing)	**Nagłówek IPv6** Następny nagłówek = 44 (Fragmentacja)	**Nagłówek IPv6** Następny nagłówek = 6 (TCP)	Segment TCP

Rysunek 26. Kolejność występowania nagłówków rozszerzeń w pakiecie IPv6

4.3. Format adresu IPv6 i adresy specjalnego przeznaczenia

Adres IPv6 jest adresem 128 bitowym. Adres IPv6 jest dzielony na osiem 16-bitowych części. Każda z tych części zamieniana jest na 4-cyfrowy numer zapisany szesnastkowo a części te są oddzielane od siebie dwukropkami. Ta notacja adresu IPv6 nazywana jest dwukropkową notacją szesnastkową.[5]

Poniżej przedstawiony został adres IPv6 w zapisany w systemie dwójkowym
00100001110110100000000011010011000000000000000000010111100111011
00000010101010100000000011111111111111100010100010011100010110 10

Ten 128-bitowy adres został podzielony na osiem 16-bitowych grup
0010000111011010 0000000011010011 0000000000000000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010

Następnie każdy z bloków zamieniany jest na system szesnastkowy i kolejne części zostają rozdzielone dwukropkami. Utworzony w ten sposób adres IPv6 wygląda tak:

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

Adres ten może zostać uproszczony przez usunięcie przednich zer w każdym 16-bitowym bloku. Jednak każdy blok musi posiadać przynajmniej jedna cyfrę. Po usunięciu zer ten sam adres wygląda tak:

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

Wiele adresów IPv6 może zawierać kilka bloków z samymi zerami. W takim przypadku można jeszcze bardziej uprościć adres IPv6 używając kompresji zer – blok lub kilka bloków składający się z samych zer można zamienić na podwójny dwukropek. Po takiej kompresji adres przedstawiony powyżej może wyglądać tak:

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

Innymi przykładami adresów IPv6 z kompresją zer mogą być:

FE80:0:0:0:2AA:FF:FE9A:4CA2 **FE80::2AA:FF:FE9A:4CA2**

FF02:30:0:0:0:0:0:5 **FF02:30::5**

Kompresja zer może występować tylko raz w danym adresie IPv6. W innym wypadku nie było by możliwe odtworzenie poprawnej liczby bloków zawierających same zera.[5]

W adresacji IPv6 występują 2 adresy specjalne:

- 0:0:0:0:0:0:0:0 lub :: - informuje on o braku adresu. Może on być wykorzystany przy starcie systemu gdy węzeł nie ma jeszcze przypisanego żadnego adresu.
- 0:0:0:0:0:0:0:1 lub ::1 - jest używany przez węzeł do wysyłania pakietów adresowanych do samego siebie. Pakiet z adresem przeznaczenia pętli zwrotnej nie może być nigdy wysłany poza pojedynczy węzeł oraz nie może być przesyłany przez routery IPv6.

4.4. Rodzaje adresów IPv6

Każdy host i router w Internecie ma adres IP, który zawiera numer sieci i numer hosta. Prefiks i sufiks w adresie IPv6 mogą mieć różne wartości i nie można wyznaczyć granicy między nimi na podstawie samego adresu. Jednak, każdemu adresowi może być przypisana długość prefiksu dzięki czemu możliwe jest określenie gdzie kończy się prefiks.

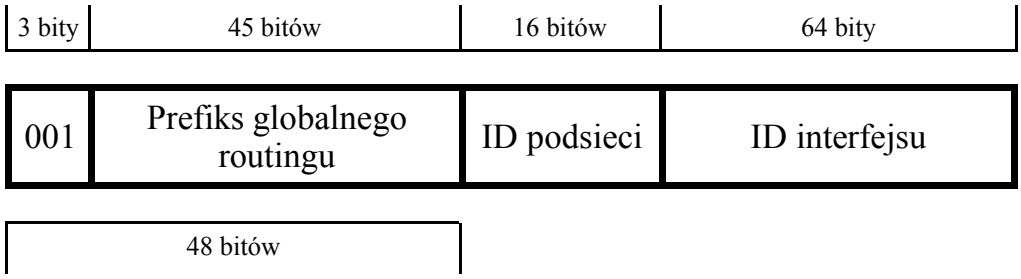
Adresy IPv6 mają strukturę hierarchiczną. Każdy z adresów IPv6 należy do jednego z trzech podstawowych typów:

4.4.1. Adres jednostkowy (Unicast)

Określa pojedynczy interfejs (pakiet wysyłany pod adres jednostkowy zostanie dostarczony do interfejsu skojarzonego z tym adresem).

Wśród adresów jednostkowych można rozróżnić 3 rodzaje adresów:

Globalny adres jednostkowy (Global Unicast Addresses) – jest to adres IPv6 dostępny i routowalny globalnie w części Internetu zbudowanego na bazie adresów IPv6. Ponieważ IPv6 ma strukturę hierarchiczną a nie klasową globalny adres jednostkowy jest unikalny w całym Internecie opartym na bazie adresów IPv6.[5]



Rysunek 27. Format globalnego adresu jednostkowego

Najważniejsze pola globalnego adresu jednostkowego:

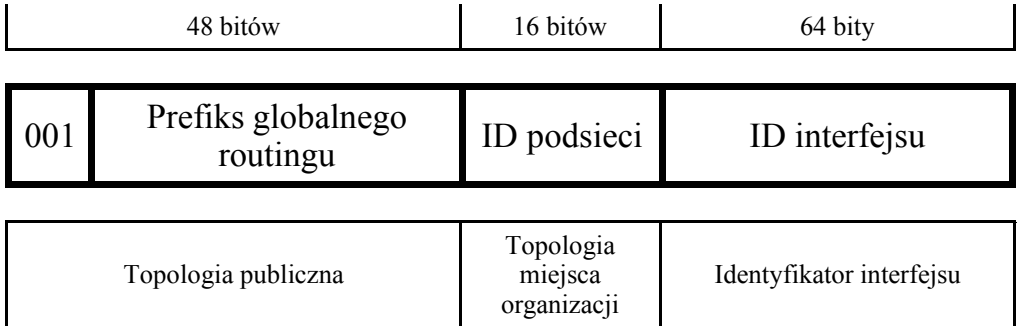
Stałe pole 001 – trzy najstarsze bity ustawione na 001. Prefiks adresu dla dotychczas nadanych globalnych adresów jednostkowych wynosi ***2000::/3***

Prefiks globalnego routingu – wskazuje prefiks globalnego routingu miejsca organizacji (sieci organizacji lub firmy, lub jej części, który ma zdefiniowane umiejscowienie geograficzne np. biuro, kompleks biur lub miasteczko uniwersyteckie). Kombinacja trzech stałych bitów i 45-bitów prefiksu globalnego routingu jest używana, aby stworzyć 48-bitowy prefiks, który jest skojarzony z indywidualnym miejscem organizacji. Gdy ten 48-bitowy prefiks zostanie raz skojarzony z miejscem organizacji przez routery działające w Internecie zbudowanym na bazie adresów IPv6, cały ruch pakietów zawierających adres z tym prefiksem zostaje skierowany do routerów miejsca organizacji.

ID podsieci – jest używane w miejscu organizacji do identyfikacji podsieci. Pole to ma wielkość 16-bitów. Miejsce organizacji może użyć tego pola, aby stworzyć 65 536 podsieci lub wielopoziomową hierarchię adresów i sprawną infrastrukturę routingu.

ID interfejsu – wskazuje interfejs w danej podsieci w miejscu.[5]

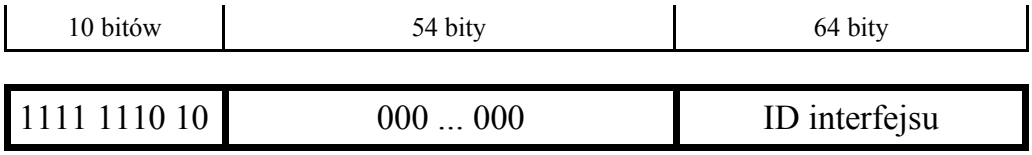
Pola w globalnym adresie jednostkowym tworzą 3-poziomową strukturę pokazaną poniżej.



Rysunek 28. 3-poziomowa struktura globalnego adresu jednostkowego

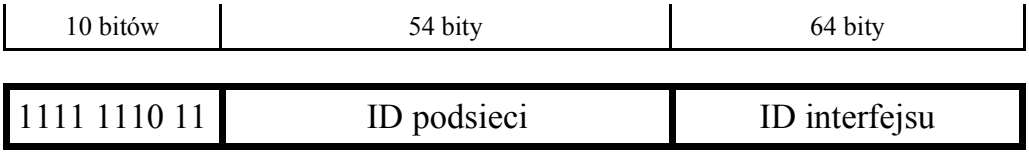
Adresy jednostkowe lokalnego użytku (Local-Use Unicast Addresses):

Adres jednostkowy lokalnego użytku dla łącza (Link-local Address) – jest używany przez pojedynczy węzeł do komunikacji z innymi sąsiednimi węzłami na tym samym łączu. Np. na łączu IPv6 gdzie nie ma routera, adres jednostkowy lokalnego użytku dla łącza jest używany do porozumiewania się przez hosty na tym łączu. Adres jednostkowy lokalnego użytku dla łącza jest wymagany przy procesie odkrywania adresu (Neighbor Discovery). Jest on zawsze automatycznie konfigurowany nawet gdy inne jednostkowe adresy są niedostępne w sieci. Adres ten zawsze zaczyna się od ***FE80::/64***. Router IPv6 nigdy nie przesyła pakietów o tym adresie poza łącze[5].



Rysunek 29. Adres jednostkowy lokalnego użytku dla łącza

Adres jednostkowy lokalnego użytku dla miejsca (Site-local Address) – jest adresem, który może być używany przez prywatne sieci, które nie mają bezpośredniego, routowalnego połączenia do Internetu zbudowanego na bazie adresów IPv6, bez powodowania konfliktu z globalnym adresem jednostkowym. Adresy jednostkowe lokalnego użytku dla miejsca nie są dostępne z innych miejsc a routery nie mogą kierować ruchu poza dane miejsce. Adresy te mogą być używane równolegle z globalnymi adresami jednostkowymi. Adresy jednostkowe lokalnego użytku dla miejsca nie są konfigurowane automatycznie tak jak adresy jednostkowe lokalnego użytku dla łącza, dlatego też muszą być konfigurowane za pomocą stanowej (host otrzymuje adres od serwera DHCPv6) lub bezstanowej (host konstruuje swój adres IPv6 po uzyskaniu identyfikatora interfejsu, unikalnego na łączu do którego jest on podłączony – Ethernet oraz przedrostka adresu dla podsieci nadawanego przez router) konfiguracji. Pierwsze 10 bitów adresu jest stałe i tworzy prefiks ***FEC0::/10***[5].



Rysunek 30. Adres jednostkowy lokalnego użytku dla miejsca

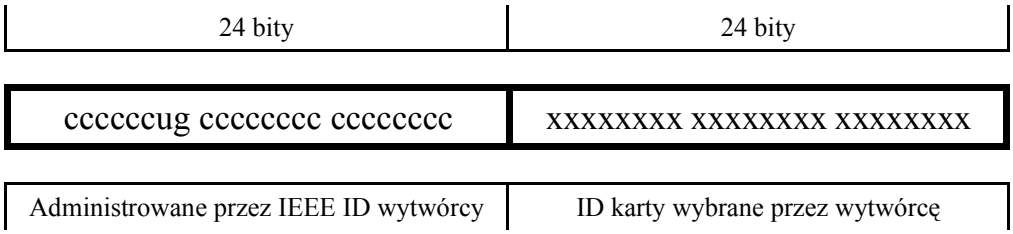
Specyficzne typy adresów IPv6 są identyfikowane przez początkowe bity w adresie. Bity początkowe nazywane są również prefiksem formatu (ang. Format Prefix – FP)[13].

Prefix (binarnie)	*Typ adresu*	*Zajmowana część przestrzeni adresowej*
0000 0000	Nieprzydzielony	1/256
0000 0001	Nieprzydzielony	1/256
0000 001	Adresy NSAP	1/128
0000 01	Nieprzydzielony	1/64
0000 1	Nieprzydzielony	1/32
0001	Nieprzydzielony	1/16
001	Zarezerwowane na globalne adresy jednostkowe	1/8
010	Nieprzydzielony	1/8
011	Nieprzydzielony	1/8
100	Nieprzydzielony	1/8
101	Nieprzydzielony	1/8
110	Nieprzydzielony	1/8
1110	Nieprzydzielony	1/16
1111 0	Nieprzydzielony	1/32
1111 10	Nieprzydzielony	1/64
1111 110	Nieprzydzielony	1/128
1111 1110 0	Nieprzydzielony	1/512
1111 1110 10	Zarezerwowane na adresy jednostkowe lokalnego użytku dla łącza	1/1024
1111 1110 11	Zarezerwowane na adresy jednostkowe lokalnego użytku dla miejsca	1/1024
1111 1111	Zarezerwowane na adresy rozsyłania grupowego	1/256

Rysunek 31. Architektura adresów IPv6

ID interfejsu – wszystkie adresy jednostkowe, które używają prefiksów 001 przez 111 muszą także używać 64-bitowego ID interfejsu, który jest tworzony z adresu EUI-64[13]. Adres EUI-64 jest przypisany do karty sieciowej lub może być wyliczony z adresu IEEE 802[5].

– **adres *IEEE 802*** - Jest to 48-bitowy adres. Składa się z 24-bitowego ID wytwórcy i 24-bitowego ID karty sieciowej. Te dwie części – pierwsza unikalna dla wytwórcy a druga unikalna dla karty sieciowej – tworzą 48-bitowy globalnie unikalny adres (MAC).

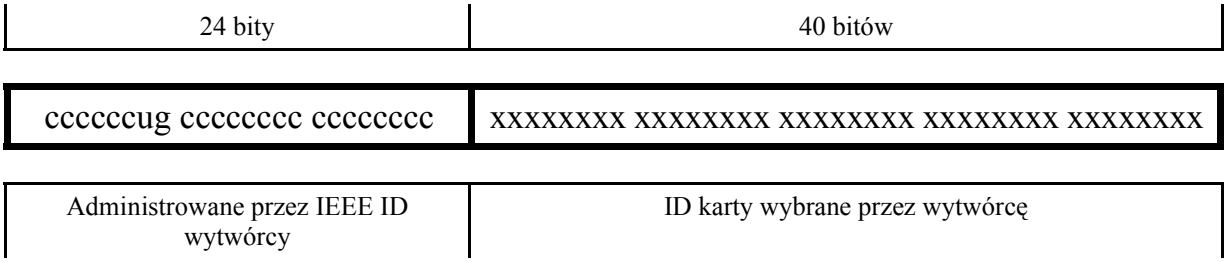


Rysunek 32.Adres IEEE 802

Uniwersalny/Lokalny (U/L) – służy do określenia czy adres jest administrowany uniwersalnie czy lokalnie. Jeśli bit ten wynosi 0, oznacza to, że adres administrowany jest uniwersalnie – przez wytwórcę. Jeśli bit ten wynosi 1, oznacza to, że administrator zmienił adres nadany przez wytwórcę swoim własnym. Na rysunku bit ten oznaczony jest jako **u**.

Indywidualny/Grupowy (I/G) – służy do określenia czy adres jest adresem jednostkowym, czy też adresem rozsyłania grupowego. Gdy bit ten jest ustawiony na 0, oznacza to, że adres jest adresem jednostkowym. Gdy bit ten ustawiony jest na 1, oznacza to, że adres jest adresem rozsyłania grupowego. Na rysunku bit ten oznaczony jest jako **g**.

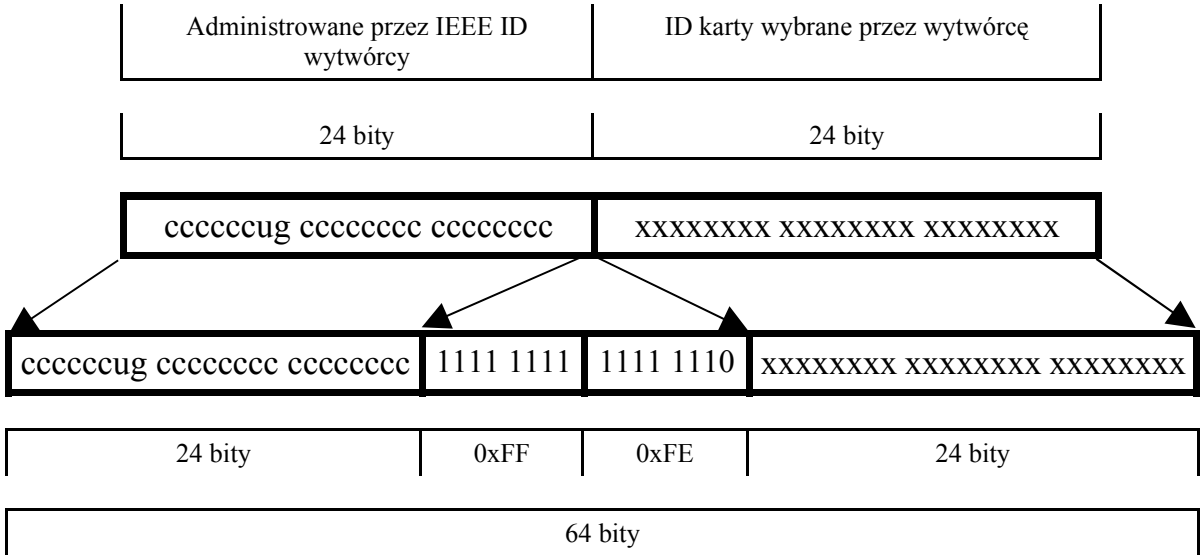
– ***Adres IEEE EUI-64*** **–** w tym adresie ID wytwórcy ma tak jak w adresie IEEE 802 24-bity, jednak ID karty sieciowej ma już 40 bitów[5].



Rysunek 33. Adres EUI-64

Mapowanie adresu IEEE 802 na adres EUI-64

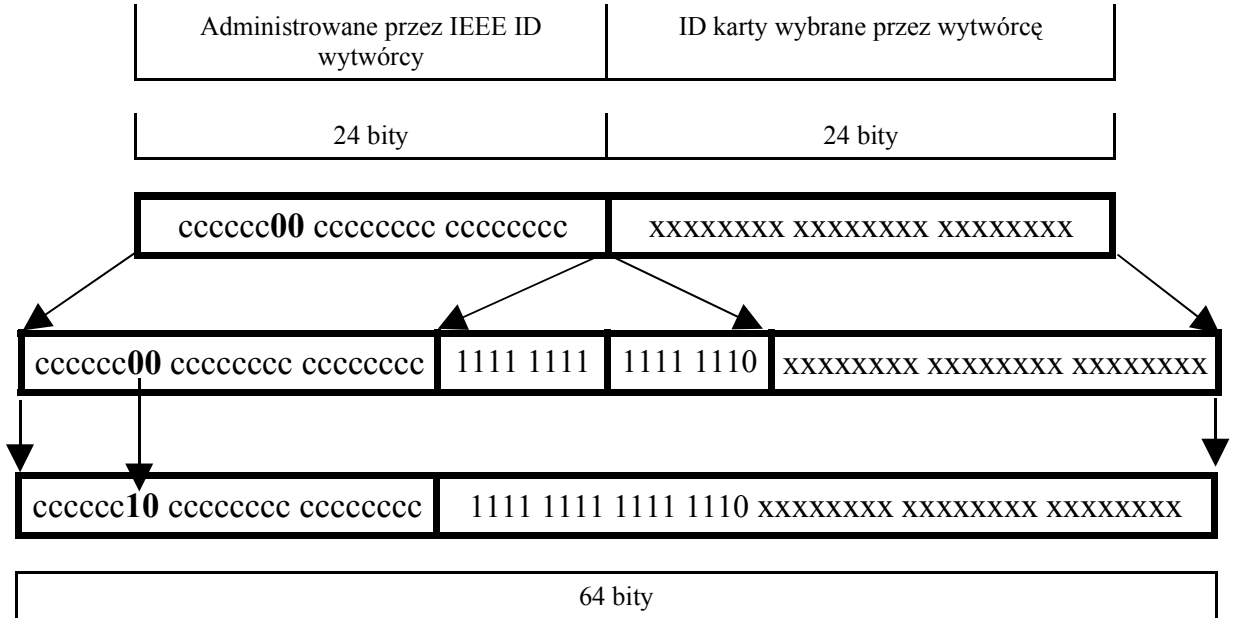
Aby stworzyć adres EUI-64 z adresu IEEE 802 należy wstawić pomiędzy ID wytwórcy a ID karty sieciowej 16 bitów "1111 1111 1111 1110"[5].



Rysunek 34. Konwersja adresu IEEE 802 na EUI-64

Mapowanie adresu EUI-64 na ID interfejsu

Aby dokonać mapowania adresu EUI-64 na ID interfejsu należy zamienić wartość bitu U/L na wartość przeciwną[5].



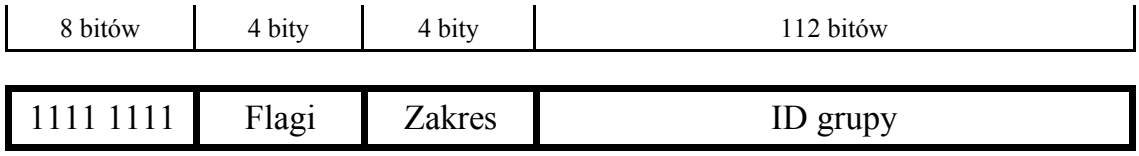
Rysunek 35. Zmiana adresu IEEE 802 na EUI-64 a następnie na ID interfejsu

Przykład konwersji adresu IEEE 802 na ID interfejsu

1) Adres MAC hosta – **00-AA-00-3F-2A-1C**
2) Konwersja na adres EUI-64 przez wstawienie FF-FE pomiędzy trzeci i czwarty bajt – 00-AA-00-FF-FE-3F-2A-1C
3) Bit U/L zostaje zamieniony (siódmy bit w pierwszym bajcie). Pierwszy bajt w systemie binarnym wynosi 0000 0000. Po zmianie 7 bitu bajt ten wynosi 0000 0010. Po tej zmianie adres EUI-64 wynosi 02-AA-00-FF-FE-3F-2A-1C.
4) Adres zostaje zmieniony na ID interfejsu o szesnastkowej notacji dwukropkowej – **2AA:FF:FE3F:2A1C**[5]

4.4.2. Adres rozsyłania grupowego (Multicast address)

Odpowiada zbiorowi hostów znajdujących się być może w różnych miejscach. Gdy pod takim adresem wysyłany jest pakiet, jest on dostarczany za pomocą IPv6 do każdego członka grupy. Hosty mogą nasłuchiwać na kilku na raz adresach rozsyłania grupowego. Hosty mogą w dowolnym czasie dołączać się lub opuszczać daną grupę multikastową. Pierwsze 8 bitów adresu rozsyłania grupowego jest stałe i wynosi 1111 1111. Prefiks tego adresu wynosi ***FF***. Adresy te nie mogą być używane jako adresy źródłowe i jako adresy pośrednie w nagłówku routingu[5].



Rysunek 36. Adres rozsyłania grupowego IPv6

Flagi – W dokumencie RFC 3513 została zdefiniowana tylko jedna flaga T. Gdy flaga ta ustawiona jest na 0 oznacza dobrze znany stały adres rozsyłania grupowego przypisany przez IANA (Internet Assigned Numbers Authority). Gdy flaga ta jest ustawiona na 1 oznacza adres tymczasowy rozsyłania grupowego.

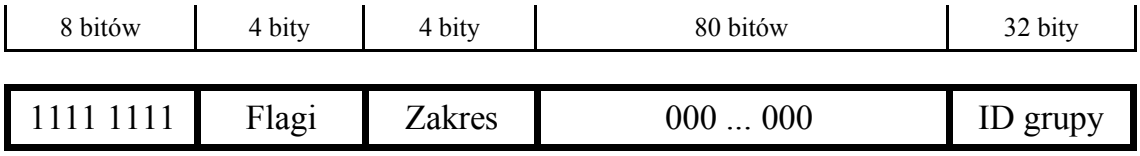
Zakres – określa zakres sieci IPv6 dla której został ustalony adres rozsyłania grupowego. Pole to może mieć różne wartości:

Wartość	*Zakres*
0	Zarezerwowane
1	Zakres lokalnego użytku dla interfejsu
2	Zakres lokalnego użytku dla łącza
3	Zarezerwowane
4	Zakres lokalnego użytku dla administratora
5	Zakres lokalnego użytku dla miejsca
8	Zakres lokalnego użytku dla organizacji
E	Zakres globalny
F	Zarezerwowane

Rysunek 37. Wartości pola zakres w adresie rozsyłania grupowego IPv6

ID grupy – identyfikuje daną grupę multicastową

Z 112-bitowym ID grupy można utworzyć 2^{112} grup ID. Jednak dokument RFC 3513 mówi, że ID grupy należy przypisać tylko 32 ostatnie bity adresu rozsyłania grupowego z powodu sposobu w jaki adresy rozsyłania grupowego są mapowane na Ethernetowe MAC adresy rozsyłania grupowego. Pozostałe 80 bitów nie uwzględnione w ID grupy powinno być ustawione na wartości 0. Gdy zostanie użyty 32-bitowy ID grupy, może on zostać zamapowany na unikatowy Ethernetowy MAC adres rozsyłania grupowego[5].



Rysunek 38. Zmodyfikowany adres rozsyłania grupowego IPv6

4.4.3. Adres grona (Anycast)

Odpowiada zbiorowi hostów ze wspólnym prefiksem adresowym. Pakiet przesyłany jest najkrótszą drogą dokładnie do jednego komputera grupy. W chwili obecnej adresy grona są używane tylko jako adresy docelowe i są przydzielane tylko routerom.

n bitów	128-n bitów

Prefiks podsieci	00000000000000

Rysunek 39. Adres grona

Prefiks podsieci – prefiks identyfikujący określone łącze. Ten adres grona jest syntaktycznie taki sam jak adres jednostkowy dla interfejsu na łączu z identyfikatorem ID ustawionym na 0.

4.5. ICMPv6

W protokole ICMPv6 jest wyraźne rozróżnienie komunikatów o błędach i komunikatów informacyjnych. Wiadomości o błędach mają typy mniejsze niż 128 a wiadomości informacyjne od 128 w górę[8].

Rysunek 40. Lista komunikatów ICMPv6

Typ	*Kody komunikatu*	*Nazwa komunikatu*	*Informacja*	*Błąd*
1	- 0 - brak drogi do urządzenia docelowego (no route to destination) - 1 - komunikacja z siecią docelową zabroniona przez administratora (communication with destination network administratively prohibited - 3 - adres nieosiągalny (address unreachable) - 4 - port niedostępny (port unreachable)	Cel nieosiągalny (Destination Unreachable)		tak
2	Nieużywane – zawsze 0	Za duży pakiet (Paket Too Big)		tak
3	- 0 - upłynął czas na przesłanie datagramu do hosta docelowego (hop limit exceeded in transit) - 1 - upłynął czas na skompletowanie datagramu na hoście docelowym (fragment reassembly time exceeded)	Przekroczenie czasu (Time Exceeded)		tak
4	- 0 - błędne pole nagłówka (erroneous header field encountered) - 1 - nieznany typ następnego nagłówka w polu nagłówka IPv6 (unrecognized Next Header type encountered) - 2 - nieznana opcja IPv6 (unrecognized IPv6 option encountered)	Problem z parametrem (Parameter Problem)		tak
128	Nieużywane – zawsze 0	Żądanie echa (Echo Request)	tak	

Typ	*Kody komunikatu*	*Nazwa komunikatu*	*Informacja*	*Błąd*
129	Nieużywane – zawsze 0	Odpowiedź na echo (Echo Reply)	tak	
133	Nieużywane – zawsze 0	Poszukiwanie routera (Router Solicitation)	tak	
134	Nieużywane – zawsze 0	Ogłoszenie routera (Router Advertisement)	tak	
135	Nieużywane – zawsze 0	Poszukiwanie adresu (Neighbor Solicitation)	tak	
136	Nieużywane – zawsze 0	Ogłaszanie adresu (Neighbor Advertisement)	tak	
137	Nieużywane – zawsze 0	Przekierowanie (Redirect)	tak	

Komunikaty informujące o błędach w protokole ICMPv6 nie mogą być wysyłane jako odpowiedź na:

- inny komunikat ICMPv6 o błędzie
- pakiet z adresem źródłowym wskazującym na więcej niż jeden host
- pakiet z adresem docelowym typu multicast z wyjątkiem komunikatu typu 2 – za duży pakiet (Packet too big) oraz typu 4 kod 2 – Problem z parametrem (Parameter problem).
- pakiet wysłany jako broadcast lub multicast w warstwie drugiej modelu OSI - łącza danych, z wyjątkiem komunikatów wymienionych w poprzednim punkcie

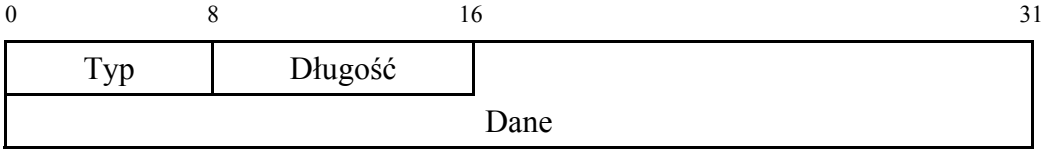
Każdy komunikat o błędzie w protokole ICMPv6 zawiera początek pakietu, podczas przesyłania którego wystąpił błąd. Ilość zwracanych danych jest taka, aby wiadomość ICMPv6 nie przekroczyła rozmiaru równego najmniejszej wartości MTU (Maximum Transmission Unit) protokołu IPv6. W przypadku gdy urządzenie otrzymuje wiadomość ICMPv6, musi podjąć pewne działania. Jeżeli typ wiadomości nie jest znany oprogramowaniu, ICMPv6 musi przekazać komunikat protokołom wyższych warstw w przypadku gdy jest to komunikat o błędzie (typ jest mniejszy niż 128). Komunikat informacyjny ICMPv6 nieznanego typu musi być przez oprogramowanie protokołu odrzucony. Gdy wiadomość o błędzie ICMPv6 musi być przekazana do oprogramowania pracującego w wyższych warstwach modelu OSI, proces który powinien ją otrzymać rozpoznawany jest na podstawie protokołu wyższej warstwy (np. TCP) i numeru portu. Informacje te są uzyskiwane z fragmentu pakietu wywołującego błąd zawartego w wiadomości ICMPv6. Może się jednak zdarzyć tak, że błędny pakiet IPv6 zawierał dużo nagłówków rozszerzeń (extension headers). Nagłówek protokołu wyższej warstwy nie może wtedy zostać dołączony do

wiadomości ponieważ przekroczyłaby ona dopuszczalną wielkość. W takim przypadku komunikat o błędzie jest odrzucany. Protokół ICMPv6 musi ograniczać ilość wysyłanych komunikatów o błędach aby nie obciążać zbytnio łączy. Przykładami takich ograniczeń są:

- ograniczenie ilości wysyłanych komunikatów do najwyżej jednego w ciągu T milisekund
- ograniczenie wykorzystania maksymalnej przepustowości łącza przez ICMPv6 do F procent

W każdym urządzeniu musi być możliwość ustawienia parametrów ograniczających (T oraz F) a przykładowymi wartościami domyślnymi mogą być np. T=1 sekunda, F=2%.[8]

Niektóre z komunikatów ICMPv6 mogą zawierać dodatkowe opcje w wiadomości.



Rysunek 41. Format opcji ICMPv6

Pole typu zawiera rodzaj zawartej opcji. Natomiast długość to liczba całkowita oznaczająca ile słów 64 bitowych zajmuje cała opcja wraz z polami typ i długość. Opcje tego samego typu mogą się powtarzać w jednym komunikacie ICMPv6.[5]

Numer	*Typ*	*Nazwa opcji*
1	1	Adres źródła łącza danych (Source Link-Layer Address)
2	2	Adres przeznaczenia łącza danych (Target Link-Layer Address)
3	3	Informacja o prefiksie (Prefix Information)
4	1	Nagłówek przekierowania (Redirected Header)
5	1	MTU

Rysunek 42. Lista opcji ICMPv6

Dokładne informacje o budowie i działaniu poszczególnych komunikatów ICMPv6 znajdują się na stronie http://www.republika.pl/wamarek/icmp/index.html.[8]

4.6. Autokonfiguracja adresu IPv6

Jedną z najbardziej użytecznych cech IPv6 jest możliwość jego automatycznej konfiguracji, nawet bez użycia protokołu konfiguracji stanowej takiej jak DHCPv6. Każdy host może domyślnie automatycznie skonfigurować adres lokalnego użytku dla łącza dla każdego interfejsu. Przy użyciu Odkrywania Adresu (Neighbor Discovery) host może także określić adresy routerów, inne parametry potrzebne do konfiguracji, dodatkowe adresy i prefiksy obecne na łączu. W wiadomości Ogłoszenie Routera (Router Advertisement) zawarta jest informacja czy powinna być używana stanowa konfiguracja adresu.

Występują 3 rodzaje autokonfiguracji:

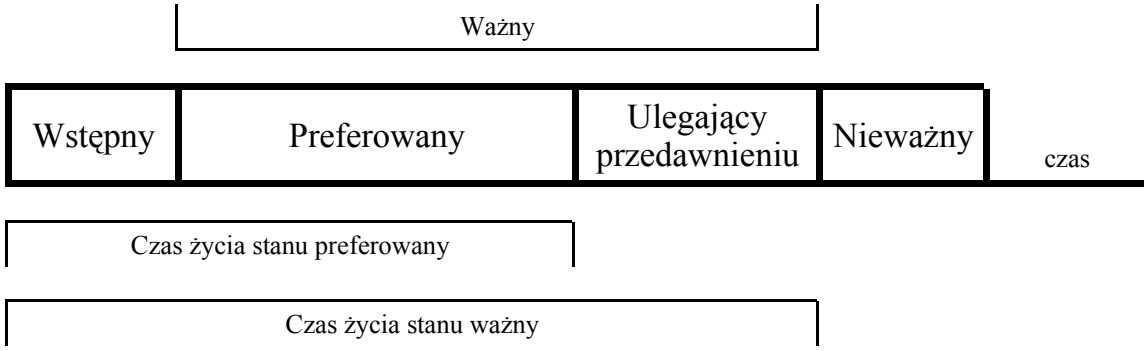
1. **Autokonfiguracja bezstanowa –** konfiguracja adresu bazuje na otrzymaniu wiadomości Ogłoszenie Routera (Router Advertisement) zawierającej flagi Zarządzana Konfiguracja Adresu (Managed Address Configuration flags) i flagi Inna Konfiguracja Stanowa (Other Stateful Configuration flags) ustawione na wartość 0 i jedną lub więcej opcji Informacja Prefiksu (Prefix Information options).
2. **Autokonfiguracja stanowa** – konfiguracja adresu bazuje na otrzymaniu adresu i innych opcji konfiguracji od protokołu stanowej konfiguracji adresu takiego jak DHCPv6. Host używa stanowej konfiguracji adresu, gdy otrzymuje wiadomość Ogłoszenie Routera (Router Advertisement message) bez opcji prefiksu, gdzie flagi Zarządzana Konfiguracja Adresu (Managed Address Configuration flags) lub flagi Inna Konfiguracja Stanowa (Other Stateful Configuration flags) są ustawione na wartość 1. Host użyje także protokołu stanowej konfiguracji adresu gdy nie ma obecnych żadnych routerów na łączu.
3. **Konfiguracja stanowo-bezstanowa** – konfiguracja adresu bazuje na otrzymaniu wiadomości Ogłoszenie Routera (Router Advertisement) zawierającej opcje Informacja Prefiksu (Prefix Information options) i flagi Zarządzana Konfiguracja Adresu (Managed Address Configuration flags) lub flagi Inna Konfiguracja Stanowa (Other Stateful Configuration flags) ustawione na wartość 1.[5]

Autokonfiguracja adresu składa się z kilku stanów. Autokonfigurowany adres może się znajdować w jednym lub więcej niż jednym z poniższych stanów:

- **Wstępny (Tentative) –** adres w czasie sprawdzania jego unikalności. Weryfikacja ta ma na celu wykrywanie zduplikowanych adresów. Węzeł nie może otrzymywać jednostkowego ruchu pakietów skierowanego na adres wstępny. Może natomiast otrzymywać i przetwarzać wiadomości Ogłaszanie Adresu rozsyłania grupowego (multicast Neighbor Advertisment

messages) wysyłane w odpowiedzi na wiadomość Poszukiwanie Adresu (Neighbor Solicitation message), która zostaje wysłana podczas wykrywania zduplikowanego adresu.

- **Ważny (Valid) –** adres , którego unikatowość została sprawdzona i z którego jednostkowy ruch pakietów może być wysyłany i otrzymywany. Stan ważny trwa przez stany preferowany i ulegający przedawnieniu. Ilość czasu jaką adres pozostaje w stanach wstępnym i ważnym jest określona przez pole Czas Życia Stanu Ważny (Valid Lifetime) w opcji Informacja Prefiksu (Prefix Information option) wiadomości Ogłoszenie Routera (Router Advertisement message). Czas życia stanu ważny musi być większy niż, lub taki sam jak czas życia stanu preferowany. Ważny adres musi być albo adresem preferowanym lub adresem ulegającym przedawnieniu.
- **Preferowany (Preferred)** – węzeł może wysyłać i otrzymywać ruch jednostkowy pakietów do i z adresu preferowanego.
- **Ulegający przedawnieniu (Deprecated)** – adres, który jest ciągle ważny, jednak nie jest używany przez nowe połączenia. Istniejące sesje komunikacyjne mogą nadal używać adresu ulegającego przedawnieniu. Węzeł może wysyłać i otrzymywać jednostkowy ruch pakietów do i z adresu ulegającego przedawnieniu.
- **Nieważny (Invalid)** – adres do którego węzeł nie może wysyłać i otrzymywać od niego jednostkowego ruch pakietów.



Rysunek 43. Stany i czasy życia dla autokonfigurowanych adresów

Autokonfiguracja (z wyjątkiem autokonfiguracji adresu lokalnego użytku dla łącza) jest sprecyzowana tylko dla hostów. Adresy IPv6 w routerach muszą być konfigurowane ręcznie.[5]

Przykład procesu autokonfiguracji

Konfiguracja adresu dla interfejsu węzła IPv6:

1) Wstępny adres użytku lokalnego dla łącza zostaje utworzony z prefiksu adresu użytku lokalnego dla łącza FE80::/64 i 64-bitowego ID interfejsu hosta.

2) Używając wykrywania zduplikowanego adresu do zweryfikowania unikalności wstępnego adresu użytku lokalnego dla łącza, interfejs hosta wysyła wiadomość Poszukiwanie Adresu (Neighbor Solicitation) z polem adresu docelowego ustawionym na wstępny adres użytku lokalnego dla łącza.
3) Jeśli host otrzyma wiadomość Ogłaszanie Adresu (Neighbor Advertisement) w odpowiedzi na wiadomość Poszukiwanie Adresu (Neighbor Solicitation), oznacza to, że inny host na łączu lokalnym używa wstępnego adresu użytku lokalnego dla łącza. W tym momencie autokonfiguracja zatrzymuje się i musi zostać przeprowadzona konfiguracja ręczna.
4) Jeśli host nie otrzyma wiadomości Ogłaszanie Adresu (Neighbor Advertisement) w odpowiedzi na wiadomość Poszukiwanie Adresu (Neighbor Solicitation), wstępny adres lokalnego użytku dla łącza jest uznawany za unikalny i ważny. W tym momencie adres użytku lokalnego dla łącza zostaje zainicjalizowany dla interfejsu hosta. Zostaje też zarejestrowany korespondujący adres rozgłaszania grupowego dla łącza w karcie sieciowej węzła poszukującego [5.]

Dalsza konfiguracja adresu dla hosta IPv6:

1) Host wysyła domyślnie do 3 wiadomości Poszukiwanie Routera (Router Solicitation).
2) Jeśli host nie otrzyma wiadomości Ogłaszanie Routera (Router Advertisement), host używa stanowej konfiguracji adresu aby otrzymać adres i inne parametry konfiguracyjne.
3) Jeśli host otrzyma wiadomości Ogłaszanie Routera (Router Advertisement), limit przeskoków, czas dostępności, licznik retransmisji, i MTU jeśli jest obecne, zostają ustawione.
4) Jeśli opcja Informacja Prefiksu (Prefix Information) jest obecna a w niej:
   - flaga Na Łączu (On-Link) jest ustawiona na 1, prefiks zostaje dodany do listy prefiksów
   - flaga Autonomiczny (Autonomous) jest ustawiona na 1, prefiks i 64-bitowy ID interfejsu zostają użyte do stworzenia adresu wstępnego-
5) Jeśli flaga Zarządzana Konfiguracja Adresu (Managed Address Configuration) w wiadomości Ogłaszanie Routera (Router Advertisement) jest ustawiona na 1, do ustalania dodatkowych adresów używany jest protokół stanowej konfiguracji adresu.
6) Jeśli flaga Inna Konfiguracja Stanowa (Other Stateful Configuration) w wiadomości Ogłaszanie Routera (Router Advertisement) jest ustawiona na 1, do ustalania dodatkowych parametrów konfiguracji używany jest protokół stanowej konfiguracji adresu.[5]

5. Porównanie protokołów IPv4 i IPv6

Wersja protokołu IPv4 osiągnęła na świecie ogromny sukces. Protokół ten umożliwił połączenie różnego rodzaju sieci w jedną globalną sieć nazywaną Internetem (zdefiniował jednolity format pakietów oraz zdefiniował zbiór adresów niezależnych od różnych rodzajów adresów sprzętowych). IPv4 potrafił się też dostosować do zmian w technologii sprzętu. Protokół IPv4 jest obecnie stosowany w sieciach działających o kilka rzędów wielkości szybciej, od tych , które były wykorzystywane w czasie jego projektowania. Jednak popularność Internetu i jego stale wzrastający rozmiar sprawiły, że w latach 90 zaczęto przewidywać wyczerpanie zapasu adresów IPv4. Wtedy też rozpoczęto pracę nad nową wersją protokołu IPv6. Protokół ten w przeciwieństwie do protokołu IPv4 jest 128-bitowym protokołem co daje znaczny większy zakres adresów. Protokół IPv6 w przyszłości ma zastąpić protokół IPv4.

Pomimo tego, że protokoły IPv4 i IPv6 mają podobne nazwy i działają w tej samej warstwie modelu TCP/IP – warstwie Internetu, i to, że oba są protokołami bezpołączeniowymi (każdy datagram zawiera adres odbiorcy i ma wyznaczoną trasę niezależnie od innych datagramów) oba protokoły różnią się w znacznym stopniu od siebie.[5]

5.1. Różnice w budowie nagłówka i pakietu

a) różnica w wielkości nagłówka protokołów IPv4 i IPv6
   - nagłówek protokołu IPv4 wynosi od 20 do 60 bajtów
   - nagłówek protokołu IPv6 ma stałą wielkość wynosząca 40 bajtów

b) porównanie nagłówków protokołów IPv4 i IPv6[5]

Rysunek 44. Porównanie nagłówka IPv4 i IPv6

Pola nagłówka IPv4	***Pola nagłówka IPv6***
Wersja – wartość pola 4	Wersja – wartość pola 6
Długość nagłówka – od 20 do 60 bajtów (zależy od wielkości nagłówka opcji)	Usunięte - każdy nagłówek ma stałą wielkość 40 bajtów; nagłówki rozszerzeń opcjonalnie dodawane do niego mają albo wartość stałą, albo mają pole z własną długością
Typ usługi	Priorytet
Długość – długość nagłówka + długość danych	Długość danych – tylko długość danych
Identyfikator	Usunięte – informacje o fragmentacji nie są zawarte w nagłówku, są one zawarte w nagłówku rozszerzeń fragmentacji
Flagi	
Przesunięcie	
Czas życia	Limit etapów
Protokół	Następny nagłówek
Suma kontrolna	Usunięte – sprawdzanie poprawności pakietu wykonywane jest przez warstwę łącza
Adres nadawcy – 32-bitowy	Adres nadawcy – 128-bitowy
Adres odbiorcy – 32-bitowy	Adres odbiorcy – 128-bitowy
Opcje	Usunięte – zastąpione przez nagłówki rozszerzeń
Niedostępne	Etykieta przepływu

c) różnice we fragmentacji pakietów IPv4 i IPv6
   - pakiet IPv4 może być fragmentowany przez nadawcę oraz węzły pośredniczące (nagłówek każdego pakietu zawiera pola dotyczące fragmentacji – identyfikator, flagi, przesunięcie)
   - pakiet IPv6 może być fragmentowany tylko przez nadawcę, nigdy przez węzły pośredniczące (nadawca dodaje do nagłówka IPv6 nagłówek rozszerzeń fragmentacji)

d) różnice w bezpieczeństwie i uwierzytelnianiu danych w pakietach IPv4 i IPv6
   - IPv4 nie wspiera bezpieczeństwa i uwierzytelniania danych w przesyłanych pakietach
   - IPv6 wspiera bezpieczeństwo i uwierzytelnianie danych w wysyłanych pakietach dzięki nagłówkom rozszerzeń uwierzytelniania i bezpieczeństwa enkapsulacji danych

e) różnica w wielkości pakietów IPv4 i IPv6
   - pakiety IPv4 mogą mieć maksymalną wielkość 65 535 bajtów
   - pakiety IPv6 mogą mieć wielkość większą niż 65 535 bajtów (nagłówek rozszerzeń międzywęzłowych – jambogramy)

f) różnice w obsłudze transmisji czasu rzeczywistego przez nagłówki pakietów IPv4 i IPv6
   - brak w nagłówku IPv4 pola identyfikującego ustawień jakości przepływu (QoS) przez routery
   - nagłówek pakietu IPv6 zawiera pole "etykieta przepływu" identyfikujące ustawienia jakości przepływu (QoS) przez routery

Dzięki tym różnicom nagłówek IPv6 może być efektywnej przetwarzany przez routery pośrednie. Uzyskano to dzięki usunięciu zbędnych opcji z nagłówka i przeniesieniu ich do nagłówków rozszerzeń. Tylko jeden z nagłówków rozszerzeń – nagłówek opcji międzywęzłowych musi być sprawdzany przez wszystkie routery. Inna cechą nagłówka IPv6 przyśpieszającą jego przetwarzanie w routerach pośrednich jest to, że routery pośrednie nie mogą fragmentować pakietu. Fragmentacji może dokonywać tylko host wysyłający pakiet dzięki nagłówkowi rozszerzeń fragmentacji. Dzięki usunięciu zbędnych opcji z nagłówka i przesunięciu ich do nagłówków rozszerzeń, nagłówek IPv6 zyskał jeszcze jedną bardzo ważną cech – pomimo tego, że adres IPv6 jest 4 razy większy od adresu IPv6, to nagłówek pakietu IPv6 jest tylko 2 razy większy niż nagłówek IPv4. W nagłówku IPv4 zawarto też opcje bezpieczeństwa, które nie były dostępne w nagłówku IPv4.

5.2. Różnica w formatach adresów i adresach specjalnych IPv4 i IPv6

a) różnica w długości adresów:
   - adresy IPv4 są adresami 32-bitowymi (4-bajtowymi). Przestrzeń adresowa IPv4 wynosi 2^{32} adresów
   - adresy IPv6 są adresami 128-bitowymi (16-bajtowymi). Przestrzeń adresowa IPv6 wynosi $3x10^{38}$ adresów ($6x10^{23}$ adresów przypadających na każdy metr kwadratowy powierzchni ziemi)

b) różnice w notacji adresów IPv4 i IPv6
   - zapis adresów IPv4 dokonywany jest za pomocą dziesiętnej notacji kropkowej np. 192.41.6.20
   - zapis adresów IPv6 dokonywany jest za pomocą szesnastkowej notacji dwukropkowej np. FF02:30::5

c) porównanie występowanie adresów specjalnych

Rysunek 45. Porównanie adresów specjalnych IPv4 i IPv6

Adresy specjalne IPv4	*Adresy specjalne IPv6*
Adres bieżącego komputera – 0.0.0.0	Adres nieokreślony - ::
Adresy sieciowe	Niedostępne
Adresy rozgłaszania kierunkowego	Niedostępne
Adresy rozgłaszania ograniczonego	Niedostępne
Adres pętli zwrotnej – 127.0.0.1	Adres pętli zwrotnej - ::1

Dzięki temu, że adresy IPv6 są 128 bitowe, wzrasta przestrzeń adresowa. Ta cecha IPv6 jest lekarstwem na kończącą się przestrzeń adresową IPv4. Nowa notacja adresów i inny zestaw adresów specjalnych są cechami nowego dłuższego adresu.

5.3. Różnica w klasyfikacji i hierarchii adresów IPv4 i IPv6

a) różnica w występowaniu klas adresów
   - adresy IPv4 są podzielone na 5 klas – A, B, C, D i E
   - adresy IPv6 nie są podzielone na klasy

b) różnice w użyciu pierwszych bitów w wyznaczaniu rodzaju adresu IPv4 i IPv6
   - w IPv4 pierwsze 4 bity adresu wyznaczają klasę tego adresu: A, B, C, D lub E
   - w IPv6 pierwsze bity adresu wyznaczają podstawowe typy adresów: jednostkowy adres globalny, jednostkowy adres użytku lokalnego dla łącza, jednostkowy adres lokalnego użytku dla miejsca lub adres rozsyłania grupowego

c) porównanie różnych typów adresów IPv4 i IPv6

Rysunek 46. Porównanie różnych typów adresów IPv4 i IPv6

Adresy IPv4	*Adresy IPv6*
Adresy publiczne (Unicast)	Adresy globalne (Unicast)
Adresy prywatne nierutowalne - 10.0.0.0/8, 172.16.0.0/12 i 192.168.0.0/16	Adresy użytku lokalnego dla miejsca - FEC0::/10

Adresy IPv4	*Adresy IPv6*
Adresy autokonfigurowane (Microsoft Windows) – 169.254.0.0/16	Adresy użytku lokalnego dla łącza - FE80::/64
Adresy rozsyłania grupowego (Multicast) - 224.0.0.0/4	Adresy rozsyłania grupowego (Multicast) – FF00::/8
Adresy rozsiewcze (Broadcast)	Niedostępne
Niedostępne	Adresy grona (Anycast)

d) różnica w wyznaczaniu sufiksu adresów IPv4 i IPv6
   - w adresach IPv4 sufiksy wyznaczane są przez administratora sieci w taki sposób aby zapewnić unikalność sufiksu w danej sieci
   - w adresach IPv6 sufiksy tworzone są z adresu IEEE 802 interfejsu

e) różnica co do ilości przypisanych adresów IPv4 i IPv6 do danego interfejsu hosta
   - typowy host ma przypisany tylko jeden adres IPv4 do danego interfejsu
   - typowy host ma przypisany przynajmniej trzy lub 4 adresy IPv6 (adres pętli zwrotnej, adres użytku lokalnego dla łącza i adres użytku lokalnego dla miejsca i/lub jeden albo więcej jednostkowych adresów globalnych) do danego interfejsu

Nowy dłuższy adres IPv6 spowodował, że została porzucona klasowość adresów IPv6. Adresy te tworzą tylko strukturę hierarchiczną. Duża ilość adresów spowodowała, że z jednym interfejsem hosta, można skojarzyć wiele różnych adresów IPv6.

5.4. Różnica pomiędzy protokołami ICMPv4 i ICMPv6

a) różnice w kodach komunikatów ICMPv4 i ICMPv6
   - komunikaty o błędach i komunikaty informacyjne ICMPv4 nie mają wyraźnie rozdzielonych numerów kodów komunikatów
   - komunikaty o błędach ICMPv6 mają kody mniejsze od 128, komunikaty informacyjne ICMPv6 mają kody większe od 128, tak więc numery kodów komunikatów są wyraźnie rozdzielone

b) porównanie komunikatów ICMPv4 i ICMPv6[8]

Rysunek 47. porównanie komunikatów ICMPv4 i ICMPv6

Nazwa komunikatu	*ICMPv4*	*ICMPv6*
Żądanie echa (Echo Request)	Tak	Tak
Odpowiedź na echo (Echo Reply)	Tak	Tak
Cel nieosiągalny (Echo Reply)	Tak	Tak
Tłumienie źródła (Source Quench)	Tak	
Przekierowanie (Redirect)	Tak	Tak
Ogłoszenie routera (Router Advertisment)	Tak	Tak
Poszukiwanie routera (Router Solicitation)	Tak	Tak
Przekroczenie czasu (Time Exceeded)	Tak	Tak
Problem z parametrem (Parameter Problem)	Tak	Tak
Pytanie o czas (Timestamp Request)	Tak	
Odpowiedź z czasem ((Timestamp Reply)	Tak	
Żądanie informacji o adresie (Information Request)	Tak	
Odpowiedź z informacją o adresie (Information Reply)	Tak	
Pytanie o maskę (Address Mask Request)	Tak	
Odpowiedź z maską (Address Mask Reply)	Tak	
Poszukiwanie adresu (Neighbor Solicitation)		Tak
Ogłaszanie adresu (Neighbor Advertisement)		Tak
Wyznaczanie trasy (Traceroute)	Tak	
Za duży pakiet (Paket Too Big)		Tak

b) różnice w klasyfikacji komunikatów ICMPv4 i ICMPv6
   - komunikat Przekierowanie (Redirect) w komunikatach ICMPv4 jest zaklasyfikowany jako komunikat o błędzie
   - komunikat Przekierowanie (Redirect) w komunikatach ICMPv6 jest zaklasyfikowany jako komunikat informacyjny

c) porównanie komunikatów o błędach i informacyjnych ICMPv4 i ICMPv6[5]

Rysunek 48. Porównanie komunikatów o błędach i informacyjnych ICMPv4 i ICMPv6

Komunikaty ICMPv4	*Komunikaty ICMPv6*	*Informacja / Błąd*
Cel nieosiągalny (Host Unreachable) - host nieosiągalny (Host unreachable) **typ 3, kod 1**	Cel nieosiągalny (Destination Unreachable) - brak drogi do urządzenia docelowego (no route to destination) **typ 1, kod 0**	Błąd

Komunikaty ICMPv4	*Komunikaty ICMPv6*	*Informacja / Błąd*
Cel nieosiągalny (Host Unreachable) - host nieosiągalny (Host unreachable) **typ 3, kod 1**	Cel nieosiągalny (Destination Unreachable) - adres nieosiągalny (address unreachable) **typ 1, kod 3**	Błąd
Cel nieosiągalny (Host Unreachable) - protokół niedostępny (Protocol unreachable) **typ 3, kod 2**	Problem z parametrem (Parameter Problem) - nieznany typ następnego nagłówka w polu nagłówka IPv6 (unrecognized Next Header type encountered) **typ 4, kod 1**	Błąd
Cel nieosiągalny (Host Unreachable) - port niedostępny (Port unreachable) **typ 3, kod 3**	Cel nieosiągalny (Destination Unreachable) - port niedostępny (port unreachable) **typ 1, kod 4**	Błąd
Cel nieosiągalny (Host Unreachable) - datagram zbyt duży, konieczna fragmentacja podczas gdy w nagłówku protokołu IP ustawiony jest bit DF [do not fragment - nie fragmentuj] (Fragmentation needed and DF set) **typ 3, kod 4**	Za duży pakiet (Paket Too Big) **typ 2, kod 0**	Błąd
Cel nieosiągalny (Host Unreachable) - komunikacja z hostem docelowym zabroniona przez administratora (communication with destination host administratively prohibited) **typ 3, kod 10**	Cel nieosiągalny (Destination Unreachable) - brak drogi do urządzenia docelowego (no route to destination) **typ 1, kod 1**	Błąd
Tłumienie źródła (Source Quench) **typ 4, kod 0**	Niedostępny	Błąd
Przekroczenie czasu (Time Exceeded) - upłynął czas na przesłanie datagramu do hosta docelowego (time to live exceeded in transit) **typ 11, kod 0**	Przekroczenie czasu (Time Exceeded) - upłynął czas na przesłanie datagramu do hosta docelowego (hop limit exceeded in transit) **typ 3, kod 1**	Błąd
Przekroczenie czasu (Time Exceeded) - upłynął czas na skompletowanie datagramu na hoście docelowym (fragment reassembly time exceeded) **typ 11, kod 1**	Przekroczenie czasu (Time Exceeded) - upłynął czas na skompletowanie datagramu na hoście docelowym (fragment reassembly time exceeded) **typ 3, kod 1**	Błąd
Problem z parametrem (Parameter Problem) - błąd we wskazanym oktecie pakietu (pointer indicates the error) **typ 12, kod 0**	Problem z parametrem (Parameter Problem) - błędne pole nagłówka (erroneous header field encountered) **typ 4, kod 0**	Błąd
Problem z parametrem (Parameter Problem) - błąd we wskazanym oktecie pakietu (pointer indicates the error) **typ 12, kod 0**	Problem z parametrem (Parameter Problem) - nieznana opcja IPv6 (unrecognized IPv6 option encountered) **typ 4, kod 2**	Błąd
Problem z parametrem (Parameter Problem) - brak wymaganej opcji w nagłówku (required option is missing) **typ 12, kod 1**	Niedostępny	Błąd
Żądanie echa (Echo Request) **typ 8, kod 0**	Żądanie echa (Echo Request) **typ 128, kod 0**	Informacja

Komunikaty ICMPv4	*Komunikaty ICMPv6*	*Informacja / Błąd*
Odpowiedź na echo (Echo Reply) **typ 0, kod 0**	Odpowiedź na echo (Echo Reply) **typ 129, kod 0**	Informacja
Ogłoszenie routera (Router Advertisment) - zwykłe zgłoszenie routera **typ 9, kod 0**	Ogłoszenie routera (Router Advertisement) **typ 134, kod 0**	Informacja
Ogłoszenie routera (Router Advertisment) - zgłoszenie routera nie przekazującego zwykłego ruchu **typ 9, kod 16**	Ogłoszenie routera (Router Advertisement) **typ 134, kod 0**	Informacja
Poszukiwanie routera (Router Solicitation) **typ 10, kod 0**	Poszukiwanie routera (Router Solicitation) **typ 133, kod 0**	Informacja

d) różnice w występowaniu opcji ICMPv4 i ICMPv6
   - w komunikatach ICMPv4 nie występują opcje
   - komunikaty ICMPv6 mogą zawierać dodatkowe opcje w wiadomości

Zmiany w komunikatach ICMPv6 dodały do starych właściwości ICMPv4, takich jak raportowanie błędów i serwisy związane z wiadomościami echo dla rozwiązywania problemów, dwie nowe usługi. Pierwszą z nich jest Odkrywanie Hosta Nasłuchującego Wiadomości Rozsyłania Grupowego (Multicast Listener Discovery – MLD) – jest to seria trzech wiadomości ICMPv6 zastępujących protokół IGMPv2 (Internet Group Management Protocol) dla IPv4. Drugim jest Odkrywanie Sąsiadów (Neighbor Discovery – ND) – seria pięciu wiadomości ICMPv6, które zarządzają komunikacja od węzła do węzła na łączu. Te pięć wiadomości ICMPv6 zastąpił protokół ARP (Address Resolution), Odkrywanie Routera (Router Discovery) ICMPv4 oraz komunikaty Przekierowanie (Redirect) ICMPv4.

5.5. Różnice w sposobie konfigurowania hostów używających IPv4 i IPv6

a) różnice w konfiguracji routerów IPv4 i IPv6
   - routery IPv4 muszą być konfigurowane ręcznie
   - routery IPv6 muszą być konfigurowane ręcznie

b) różnice w konfigurowaniu hostów IPv4 i IPv6
   - hosty IPv4 mogą być konfigurowane na trzy sposoby: ręcznie, przy użyciu protokołu konfiguracji stanowej DHCPv4 oraz konfiguracji automatycznej (Microsoft Windows)

- hosty IPv6 mogą być konfigurowane na cztery sposoby: ręcznie, przy użyciu protokołu konfiguracji stanowej DHCPv6, przy użyciu konfiguracji bezstanowej – autokonfiguracji oraz przy użyciu konfiguracji stanowo-bezstanowej.

Głównym założeniem konfiguracji IPv6 jest autokonfiguracja. Ma ona w znacznym stopniu 0graniczyć ręczne wpisywanie ustawień dla każdego nowego hosta pojawiającego się w sieci.

6. Migracja z protokołu IPv4 na IPv6

Prace nad IPv6 rozpoczęły się w latach 90, gdy po wielkim sukcesie protokołu IPv4 i ciągle wzrastającej liczbie komputerów podłączanych do Internetu zaczęto przewidywać wyczerpanie się jego przestrzeni adresowej. Pomimo kilku podobieństw między tymi protokołami, więcej jest jednak różnic, co zostało pokazane w tej pracy. Te różnice sprawiają, że te dwa protokoły komunikacyjne nie są ze sobą kompatybilne i hosty oraz routery używające IPv4 nie mogą komunikować się bezpośrednio z hostami oraz routerami używającymi IPv6.

Przejście z protokołu IPv4 na IPv6 nie stanie się z dnia na dzień. Dlatego też na czas tej transformacji ustalono zasady koegzystowania i sposobów komunikacji między tymi dwoma protokołami. W dokumencie RFC2893 opisano pięć typów węzłów używających IPv4 i/lub IPv6. Węzły te to:

- węzły obsługujące tylko protokół IPv4
- węzły obsługujące tylko protokół IPv6
- węzły obsługujące zarówno protokół IPv4 jak i IPv6
- węzły IPv4 – mogą one obsługiwać tylko protokół IPv4, lub obsługiwać oba protokoły
- węzły IPv6 – mogą one obsługiwać tylko protokół IPv6, lub obsługiwać oba protokoły[6]

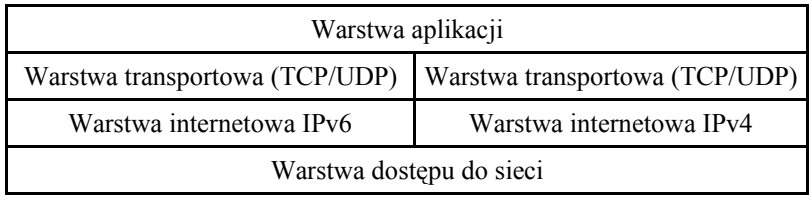
Węzły obsługujące tylko protokół IPv4 mogą się porozumiewać z węzłami IPv6 tylko dzięki proxy IPv4-do-IPv6(IPv4-to-IPv6). Węzły obsługujące zarówno IPv4 jak i IPv6 mogą się porozumiewać dzięki podwójnej warstwie IP lub podwójnemu stosowi.

Podwójna warstwa IP jest implementacją zestawu protokołów TCP/IP zawierającą zarówno warstwę internetową IPv4 jak i warstwę internetową IPv6. Architektura podwójnej warstwy IP zawiera pojedyncze implementacje warstw wyższych (aplikacji, TCP/UDP), które mogą komunikować się przez IPv4, IPv6, lub przez IPv6 tunelowane w IPv4[6].

<table>
<tr><td colspan="2">Warstwa aplikacji</td></tr>
<tr><td colspan="2">Warstwa transportowa (TCP/UDP)</td></tr>
<tr><td>Warstwa internetowa IPv6</td><td>Warstwa internetowa IPv4</td></tr>
<tr><td colspan="2">Warstwa dostępu do sieci</td></tr>
</table>

Rysunek 49. Architektura podwójnej warstwy sieciowej

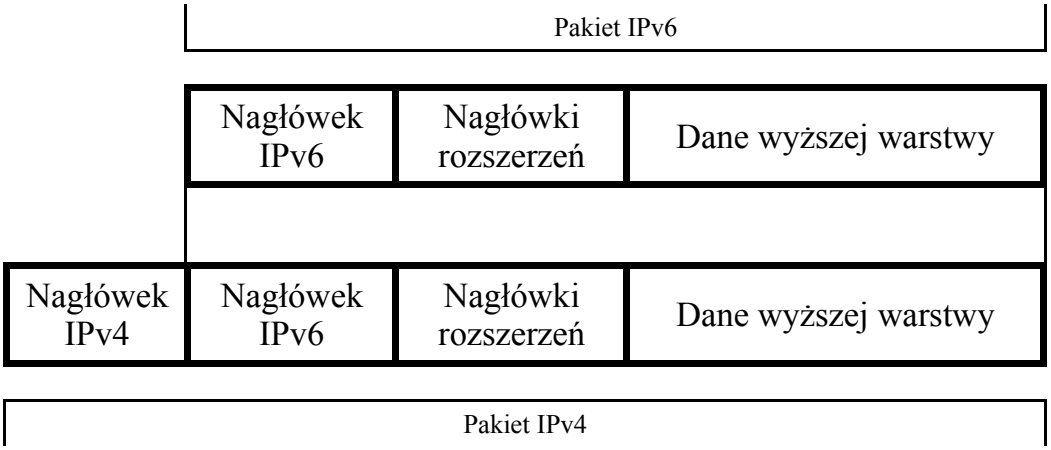
Architektura podwójnego stosu w przeciwieństwie do architektury podwójnej warstwy IP, oprócz implementacji protokołów IPv4 i IPv6 posiada oddzielne implementacje protokołów TCP i UDP.



Rysunek 50. Architektura podwójnego stosu

Aby pakiety IPv6 mogły być przesyłane przez Internet bazujący na adresach IPv4, są one enkapsułowane w nagłówki IPv4 i w ten sposób wysyłane w sieć. Gdy enkapsulacja ma miejsce, wtedy:

- pole protokołu IPv4 jest ustawione na wartość 41 aby zaznaczyć enkapsulację IPv6
- adresy źródłowy i docelowy są ustawione na adresy początku i końca tunelu. Koniec i początek tunelu są konfigurowane na różne sposoby – albo ręcznie, albo automatycznie obliczane z interfejsu wysyłającego pakiet, albo adresu następnego skoku, albo adresu źródłowego i docelowego nagłówków adresów IPv6[6].



Rysunek 51. Enkapsulacja - tunelowanie IPv6 przez IPv4

Aby ułatwić współpracę protokołów IPv4 i IPv6 zostało zdefiniowane 6 adresów[6]:

1) Adresy kompatybilne z IPv4

   Adresy te mają formę **0:0:0:0:0:0:w.x.y.z** lub **::w.x.y.z**, gdzie **w.x.y.z** jest dziesiętną notacją kropkową publicznych adresów IPv4. Adres ten jest używany przez węzły obsługujące zarówno

IPv4 jak i IPv6. Gdy taki adres jest używany jako adres docelowy , ruch IPv6 jest automatycznie enkapsułowany w nagłówku IPv4 i wysyłany przez infrastukturę IPv4

2) Zamapowane adresy IPv4

   Adresy te mają formę **0:0:0:0:0:FFFF:w.x.y.z** lub **::FFFF:w.x.y.z**. Są one używane, aby pokazać węzły obsługujące tylko IPv4 węzłom obsługującym tylko IPv6. Zamapowane IPv4 nie są nigdy używane jako adresy źródłowe i docelowe pakietów IPv6. Te adresy są używane tylko przez niektóre implementacje IPv6, które działają jako tłumacze między węzłami obsługującymi tylko IPv4 i węzłami obsługującymi tylko IPv6.

3) Adresy 6 przez 4 (6 over 4)

   dresy te złożone są z 64-bitowego prefiksu adresu jednostkowego i ID interfejsu **:: WWXX:YYZZ**, gdzie **WWXX:YYZZ** jest szesnastkową notacją dwukropkową reprezentującą publicznego adresu IPv4 przypisanego do interfejsu. Adresy te są używane do prezentacji hosta w czasie mechanizmu automatycznego tunelowania.

4) Adresy 6 do 4 (6 to 4)

   Adresy te bazują na prefiksie **2002:WWXX:YYZZ::/48**, gdzie **WWXX:YYZZ** jest szesnastkową notacja dwukropkową reprezentacją **w.x.y.z** – publicznego adresu IPv4 przypisanego do interfejsu. Adresy te są używane do prezentacji miejsca w czasie mechanizmu automatycznego tunelowania.

5) Adresy ISATAP (Intra-site Automatic Tunnel Addressing Protocol)

   Adresy te złożone są z 64-bitowego prefiksu adresu jednostkowego i **::0:5EFE:w.x.y.z** ID interfejsu, gdzie **w.x.y.z** jest adresem IPv4 przypisanym do interfejsu. Przykładem takiego adresu może być FE80:5EFE:131.107.4.92. Adresy te są używane do prezentacji hosta w czasie mechanizmu automatycznego tunelowania.

6) Adresy Teredo

   Te adresy używają 3FFE:831F::/32. Przykładem takiego adresu jest 3FFE:831F:CE49:7601:8000:EFFF:62C3:FFFE. Za pierwszymi 32 bitami adresy Toredo są używane do zakodowania adresu IPv4 serwerów Toredo, flag, i odkodowanej wersji zewnętrznego adresu i portu klienta Toredo. Adresy te są używane do prezentacji hosta w czasie mechanizmu automatycznego tunelowania.

Podsumowanie

Od swojego powstania w latach 70, model TCP/IP przez wiele lat, aż do dziś prawie nie ulegał zmianom. Przez lata jednym z głównych protokołów tego modelu jest protokół IPv4. Ta stałość i niezmienność działania modelu TCP/IP świadczy o jakości i elastyczności tej konstrukcji. Od czasu powstania modelu TCP/IP kilkadziesiąt razy wzrosły prędkości procesorów i typowe rozmiary pamięci komputerów. Kilkaset razy wzrosła też przepustowość sieci szkieletowej Internetu, a kilka tysięcy razy liczba węzłów w sieci. Model TCP/IP i jego protokoły są na tyle elastyczne, że dostosowywały się do wszystkich zmian. Jednak pomimo wielu zalet protokoły te mają też swoje wady. Jedną z głównych niedogodności protokołów TCP/IP jest mała liczba adresów IP.

Aby poradzić sobie z tym problemem i poprawić kilka innych niedogodności zaczęto pracować nad nowym protokołem, który miałby zastąpić IPv4. Protokołem tym jest oczywiście IPv6. Protokół ten ma w przyszłości rozwiązać problem małej ilości IPv4 – adresy IPv6 są 128 bitowe, co oznacza, że przestrzeń adresowa IPv6 wynosi $3x10^{38}$ adresów ($6x10^{23}$ adresów przypadających na każdy metr kwadratowy powierzchni ziemi).

Ponieważ IPv4 i IPv6 nie są protokołami kompatybilnymi i istnieje między nimi wiele różnic, co zostało pokazane w tej pracy, opracowano metody dzięki którym przez czas migracji z protokołu IPv4 na IPv6 będzie możliwa koegzystencja tych dwóch protokołów. Całkowite przejście z IPv4 na IPv6 może potrwać wiele lat. Dzięki takim mechanizmom jak enkapsulacja ramek IPv6 w ramkach IPv4 i w ten sposób przesyłanie ich przez Internet oparty na adresach IPv4, oraz różnego rodzaju adresom kompatybilnym zarówno z IPv4 jak i IPv6 przejście to zostanie w znaczny sposób ułatwione.

Protokół IPv6 jest ciągle w fazie testowej. W chwili obecnej, działa sieć testowa oparta na IPv6 – 6bone. Komunikacja w tej sieci odbywa się na zasadzie tuneli przez Internet oparty o IPv4. Każdy router podłączony do 6bone przy pomocy tuneli stanowi pomost pomiędzy częścią internetu bazującą na IPv6 z częścią Internetu bazującą na IPv4.

W przyszłości protokół IPv6 może mieć wiele zalet. Pierwszą z nich jest to, że pula adresów jest tak duża, że nie tylko każdy interfejs hosta podłączonego do Internetu może mieć swój adres IP. Adresy IP będą mogły mieć też np. telefony komórkowe, samochody, czy sprzęty domowe co umożliwi łatwiejszą komunikację oraz zdalną diagnostykę. Inną przydatną cechą IPv6 jest autokonfiguracja. Administratorzy sieci nie będą musieli ręcznie wpisywać adreów IP w każdy nowy host podłączany do sieci. Dzięki stanowej i bezstanowej konfiguracji w hostach, które po raz

pierwszy zostaną podłączone do sieci, adres IP zostanie skonfigurowany automatycznie. Poza tymi udogodnieniami w IPv6 poprawiono jeszcze kilka rzeczy np., bezpieczeństwo przesyłania danych.

W ciągu kilku najbliższych lat protokół IPv6 zastąpi całkowicie protokół IPv4. Migracja ta może potrwać kilka, kilkanaście a nawet kilkadziesiąt lat, jednak gdy ta zmiana nastąpi korzystanie z Internetu będzie o wiele łatwiejsze i przyjemniejsze.

Spis rysunków

Spis dokumentów RFC związanych z IPv4 i IPv6

1. **RFC 777** Internet Control Message Protocol - http://rfc.net/rfc777.html
2. **RFC 791** Internet Protocol - http://rfc.net/rfc791.html (zastąpił RFC 760 - http://rfc.net/rfc760.html)
3. **RFC 792** Internet Control Message Protocol - http://rfc.net/rfc792.html
4. **RFC 894** A Standard for the Transmission of IP Datagrams over Ethernet Networks - http://rfc.net/rfc894.html
5. **RFC 917** Internet Subnets - http://rfc.net/rfc917.html
6. **RFC 1042** Standard for the Transmission of IP Datagrams over IEEE 802 Networks - http://rfc.net/rfc1042.html (zastąpił RFC 948 – http://rfc.net/rfc948.html)
7. **RFC 1122** Requirements for Internet Hosts - Communication Layers - http://rfc.net/rfc1122.html
8. **RFC 1180** A TCP/IP Tutorial - http://rfc.net/rfc1180.html
9. **RFC 1219** On the Assignment of Subnet Numbers - http://rfc.net/rfc1219.html
10. **RFC 1256** CMP Router Discovery Messages - http://rfc.net/rfc1256.html
11. **RFC 1375** Suggestion for New Classes of IP Addresses - http://rfc.net/rfc1390.html
12. **RFC 1454** Comparison of Proposals for Next Version of IP - http://rfc.net/rfc1454.html
13. **RFC 1933** Transition Mechanisms for IPv6 Hosts and Routers - http://rfc.net/rfc1933.html
14. **RFC 2402** - IP Authentication Header - http://rfc.net/rfc2402.html (zastąpił RFC 1826 - http://rfc.net/rfc1826.html
15. **RFC 2406** - IP Encapsulating Security Payload (ESP) - http://rfc.net/rfc2406.html (zastąpił RFC 1827 – http://rfc.net/rfc1827.html)
16. **RFC 2474** Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers - http://rfc.net/rfc2474.html (zastąpił RFC 1349 - http://rfc.net/rfc1349.html i 1455 http://rfc.net/rfc1455.html)

17. **RFC 2460** Internet Protocol, Version 6 (IPv6) Specification - http://rfc.net/rfc2460.html (zastąpił RFC 1883 - http://rfc.net/rfc1883.html)

18. **RFC 2461** Neighbor Discovery for IP Version 6 (IPv6) - http://rfc.net/rfc2461.html (zastąpił RFC 1970 - http://rfc.net/rfc1970.html)

19. **RFC 2462** IPv6 Stateless Address Autoconfiguration - http://rfc.net/rfc2462.html (zastąpił RFC 1971 - http://rfc.net/rfc1971.html)

20. **RFC 2463** Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification - http://rfc.net/rfc2463.html (zastąpił RFC 1885 - http://rfc.net/rfc1885.html)

21. **RFC 2675** IPv6 Jumbograms - http://rfc.net/rfc2675.html (zastąpił RFC 2147 - http://rfc.net/rfc2147.html)

22. **RFC 2893** Transition Mechanisms for IPv6 Hosts and Routers (zastąpił RFC 1933 - http://rfc.net/rfc1933.html)

23. **RFC 3142** An IPv6-to-IPv4 Transport Relay Translator - http://rfc.net/rfc3142.html

24. **RFC 3484** Default Address Selection for Internet Protocol version 6 (IPv6) - http://rfc.net/rfc3483.html

25. **RFC 3513** Internet Protocol Version 6 (IPv6) Addressing Architecture - http://rfc.net/rfc3483.html (zastąpił RFC 2373 - http://rfc.net/rfc2372.html)

26. **RFC 3587** IPv6 Global Unicast Address Format - http://rfc.net/rfc3587.html (zastąpił RFC 2374 - http://rfc.net/rfc2374.html)

27. **RFC 3736** Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6 - http://rfc.net/rfc3736.html

Literatura

1. Czeluśniak Tomasz – Protokół internetowy IPv6 - www.prz.rzeszow.pl/we/katedry/zsc/ materialy/projekty/034.pdf
2. Domański, Adam – Sieci komputerowe – wykład 8 - http://rose.iinf.polsl.gliwice.pl/~adamd/a2.php
3. Kajdaniak Jaromir, Kulak Michał – Protokół IPv6 - http://nss.et.put.poznan.pl/study/projekty/sieci_komputerowe/ipv6/html/podstawowe.htm
4. Madej Konrad – IPv6 - http://www.ia.pw.edu.pl/~tkruk/students/kmadej/mydocs/ipv6/
5. Microsoft Windows Server 2003 – Introduction to IP Version 6 - http://www.microsoft.com/windowsserver2003/technologies/ipv6/introipv6.mspx
6. Microsoft Windows Server 2003 – IPv6 Transition Technologies - http://www.microsoft.com/windowsserver2003/techinfo/overview/ipv6coexist.mspx
7. Misiak Anna – Protokoły nowszej generacji – TCP/IP – http://www.prz.rzeszow.pl/we/katedry/zsc/ materialy/projekty/031.pdf
8. Obidowski Dariusz, Wardziński Marek - Protokół ICMPv4 oraz ICMPv6. Sposób działania, przesyłane komunikaty, typowe scenariusze wymiany komunikatów ICMP. - http://www.republika.pl/wamarek/icmp/index.html
9. RFC 2402 - IP Authentication Header - http://rfc.net/rfc2402.html
10. RFC 2406 – IP Encapsulating Security Payload (ESP) - http://rfc.net/rfc2406.html
11. RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification - http://rfc.net/rfc2460.html
12. RFC 2675 – IPv6 Jumbograms - http://rfc.net/rfc2675.html
13. RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture - http://rfc.net/rfc2373.html
14. RFC 3587 - IPv6 Global Unicast Address Format - http://rfc.net/rfc3587.html
15. Sajkowski Michał – Sieci komputerowe – wykład dla kierunku informatyka, semestr 4i 5 – http://www.man.poznan.pl/~michal/sk13w.pdf
16. Stevens W, Richard – Unix programowanie usług sieciowych -Wydawnictwo Naukowo-Techniczne Warszawa
17. Tanenbaum Andrew, S. - Computer Networks, Fourth Edition – Prentice Hall