1. Budowa stosu TCP/IP

Stos protokółów TCP/IP jest zestawem kilku protokółów sieciowych zaprojektowanych do komunikowania się komputerów w dużych, rozległych sieciach typu WAN. Protokóły TCP/IP zostały po raz pierwszy zastosowane w roku 1969 w ramach projektu sieci ARPANET.

Model logiczny stosu protokółów TCP/IP składa się z czterech warstw:

- warstwy interfejsu sieciowego
- warstwy internetowej
- warstwy transportowej
- warstwy aplikacji.

Każda z tych warstw odpowiada jednej lub kilku warstwom modelu OSI. Na rysunku 1 przedstawiono architekturę logiczną stosu protokółów TCP/IP oraz odpowiadające poszczególnym warstwom tego modelu warstwy modelu OSI.

Rysunek 1 Architektura stosu TCP/IP

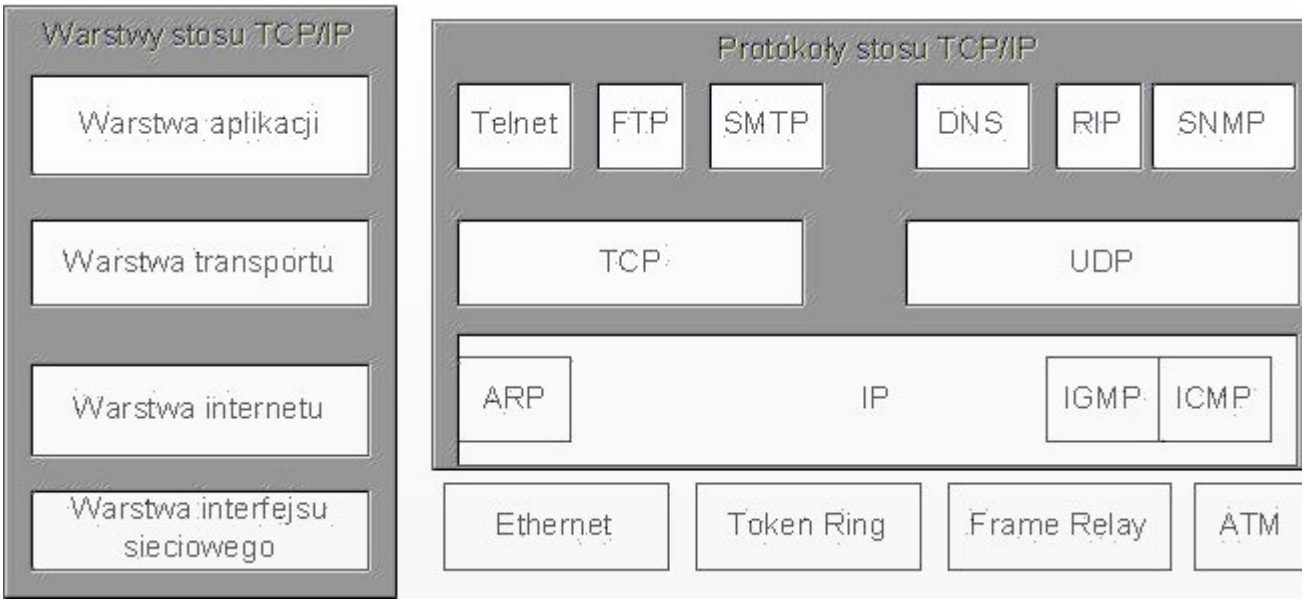
(1.1) Warstwa interfejsu sieciowego

Warstwa interfejsu sieciowego *(ang. Network Interface layer)* jest odpowiedzialna za przekazywanie i odbieranie pakietów z kanału transmisyjnego. Stos protokółów TCP/IP został przy tym tak zaprojektowany, aby uniezależnić się od rodzaju kanału transmisyjnego, formatu ramki fizycznej czy architektury sieciowej. Dzięki temu protokół TCP/IP może być stosowany w sieciach wykorzystujących różna technologie taka jak na przykład Ethernet, Token Ring, X.25, Frame Relay, ATM.

(1.2) Warstwa internetowa

Warstwa internetowa *(ang. Internet layer)* jest odpowiedzialna za adresowanie, podział na pakiety oraz routing. W skład tej warstwy wchodzą następujące protokóły:

- Protokół IP Protokół IP *(ang. Internet Protocol)* odpowiada za prawidłowe adresowanie pakietów oraz dostarczanie ich do miejsca przeznaczenia.
- Protokół ARP Protokół ARP *(ang. Address Resolution Protocol)* jest odpowiedzialny za identyfikacje sprzętowego adresu interfejsu sieciowego komputera docelowego (identyfikacja adresów MAC).
- Protokół ICMP Protokół ICMP *(ang. Internet Control Message Protocol)* jest odpowiedzialny za diagnozowanie transmisji datagramów IP oraz za raportowanie o błędach, które mogą pojawić się w trakcie przesyłania datagramów IP.
- Protokół IGMP Protokół IGMP *(ang. Internet Group Management Protocol)* jest odpowiedzialny za rozsyłanie informacji w trybie multicasting.



Rysunek 2 Protokoły stosu TCP/IP

(1.3) Warstwa transportowa

Warstwa transportowa *(ang. Transport layer)* gwarantuje poprawna komunikacje miedzy komputerami w sieci oraz przepływ danych miedzy warstwa internetowa a warstwa aplikacji. Do podstawowych protokółów warstwy transportowej należą:

- Protokół TCP
- Protokół UDP

UDP i TCP różnią się dbałością o transmitowane dane: UDP nie daje żadnej gwarancji ze dane dotrą do celu i służy do przesyłania krótkich informacji, które mogą się zmieścić w jednym datagramie. Mówimy, ze UDP jest protokółem bezpołączeniowym *(connectionless)*. TCP ma zapewnić pewny kanał transmisji, w którym dotarcie danych do celu jest potwierdzane przez odbiorcę. W razie potrzeby dane są retransmitowane. Innymi słowy aplikacja, która używa TCP do przesłania danych do odbiorcy może się już nie martwic, czy poszczególne pakiety IP dotarły do odbiorcy. O kontrole tego zadba TCP i tylko zbiorczo, na koniec, poinformuje aplikacje, czy transmisja zakończyła się sukcesem.

NASTĘPNA

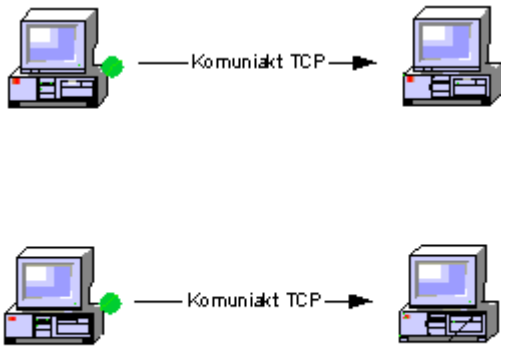
2. Protokół TCP

Protokół TCP *(ang. Transmission Control Protocol)* jest odpowiedzialny za bezbłędne dostarczanie informacji. Charakteryzuje się następującymi cechami:

- jest zorientowany na połączenie: oznacza to, że program użytkowy, który chce skorzystać z protokółu TCP musi najpierw zwrócić się do odbiorcy z prośbą o uzyskanie połączenia i uzyskać jego zgodę;
- jest protokółem typu punkt-punkt: oznacza to, że każde połączenie TCP ma dokładnie dwa końce;
- zapewnia niezawodność: oznacza to, że protokół TCP zapewnia pełna niezawodność w dostarczaniu pakietów;
- zapewnia dwukierunkową komunikację: oznacza to, że komunikacja w połączeniu TCP odbywa się w dwu kierunkach, czyli zarówno od nadawcy do odbiorcy jak i od odbiorcy do nadawcy;
- zapewnia strumieniowy interfejs: oznacza to, że program może wysyłać połączeniem całą sekwencję bajtów, w konsekwencji prowadzi to do tego, że dane nie musza być dostarczane do odbiorcy w kawałkach tych samych wielkości, w których zostały wysłane;
- zapewnia łagodne kończenie połączenia: oznacza to, ze protokół gwarantuje niezawodne dostarczenie pakietów przed zamknięciem połączenia.

(2.1) Retransmisja

Jednym z mechanizmów zapewniających niezawodność transportu danych jest retransmisja. Polega on na tym, ze odbiorca po odebraniu danych zobowiązany jest do przesłania do nadawcy potwierdzenia odebrania danych. Jeżeli potwierdzenie nie nadejdzie w określonym czasie, to nadawca wysyła dane ponownie.



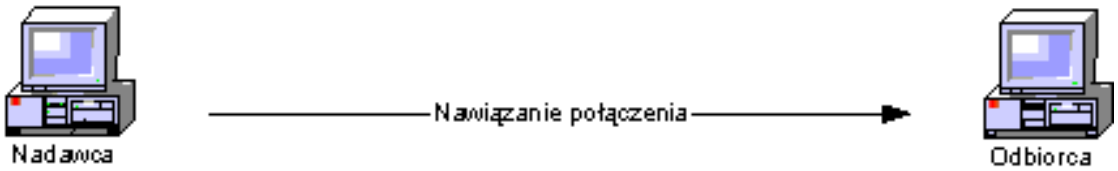
Rysunek 3 Retransmisja TCP

Jak długo należy czekać na nadejście potwierdzenia?
Jest to ważne pytanie. Jak wiadomo opóźnienia w dostarczaniu pakietów w sieci TCP/IP mogą być znaczne. Gdyby czas oczekiwania był zbyt krótki, to nadawca wysyłał by retransmisje za każdym razem nie mogąc doczekać się na odpowiedz. Skutki takiego postępowania są łatwe do przewidzenia. Dlatego protokół TCP stosuje retransmisje z adaptacja. Polega ona na tym ,ze komputer nadawcy mierzy czas jaki potrzebny jest pakietowi do przejścia do odbiorcy i z powrotem. Na tej podstawie stosując odpowiedni aparat statystyki matematycznej szacowany jest czas potrzebny na oczekiwanie na otrzymanie potwierdzenia od odbiorcy.
Dzięki takiemu rozwiązaniu protokół TCP może optymalizować ruch w sieci. Tam gdzie siec jest bardziej wydajna, a wiec gdzie pakiety wędrują szybciej tam również czas oczekiwania jest

mniejszy. W wypadku zagubienia pakietu nadawca decyduje się wiec szybciej na dokonanie retransmisji.

(2.2) Okna

Kolejnym mechanizmem pozwalającym na kontrole przepływu danych stosowanym w protokole TCP jest mechanizm okien.
Każdy z komputerów uczestniczący w połączeniu TCP dysponuje swoim własnym buforem, w którym gromadzi nadchodzące dane. Dane oczekują w buforze na przyjęcie ich przez odpowiednia aplikacje. Bufor ma oczywiście ograniczony rozmiar. Komputer odbiorcy wraz z potwierdzeniem otrzymania danych wysyła dodatkowo informacje o wolnym rozmiarze bufora czyli o oknie.
Jeśli odbiorca nie jest w stanie czytać nadchodzących danych tak szybko jak są one wysyłane, to za którymś razem wyśle do nadawcy informacje o zerowym rozmiarze okna. Jest to sygnał dla nadawcy, ze ma przerwać nadawanie. Przerwa tarwa, aż do momentu, gdy odbiorca ponownie prześle niezerowy rozmiar okna.



Rysunek 4 Wykorzystanie okien TCP

W przykładzie powyżej nadawca otrzymuje propozycje okna o wielkości 2500 oktetów. Nadawca rozpoczyna wysyłanie trzech segmentów 1-1000, 1001-2000 i 2001-2500. Po nadejściu do odbiorcy wysyłane jest potwierdzenie wraz z rozmiarem okna. Ponieważ rozmiar okna osiągnął zero, wiec nadawca czeka z transmisja. Dopiero, gdy odbiorca przeczyta 2000 oktetów wysyła potwierdzenie i nowy rozmiar okna (2000). Po otrzymaniu tego komunikatu wysyła następna nastepna porcje

NASTĘPNA

3. Protokół UDP

Protokół UDP *(ang. User Datagram Protocol)* jest odpowiedzialny za dostarczanie danych nie gwarantuje jednak niezawodności tej operacji. Protokół TCP jest protokółem połączeniowym, czyli do pracy potrzebuje ustanowienia połączenia miedzy komputerem nadawcy a komputerem odbiorcy. Aby wiec mógł nastąpić transfer danych w protokole TCP nadawca musi poprosić o nawiązania połączenia, następnie otrzymać zgodę. Również po zakończeniu transferu należy zadbać o zamkniecie połączenia.

Nie zawsze taki mechanizm jest potrzebny. Aplikacje, które nie potrzebują odporności i solidności protokółu TCP mogą wykorzystywać inny protokół transportowy protokół UDP.
Protokół UDP pracuje w trybie bezpołączeniowym. Nie musi on nawiązywać połączenia . Po prostu wysyła on dane do określonego odbiorcy.

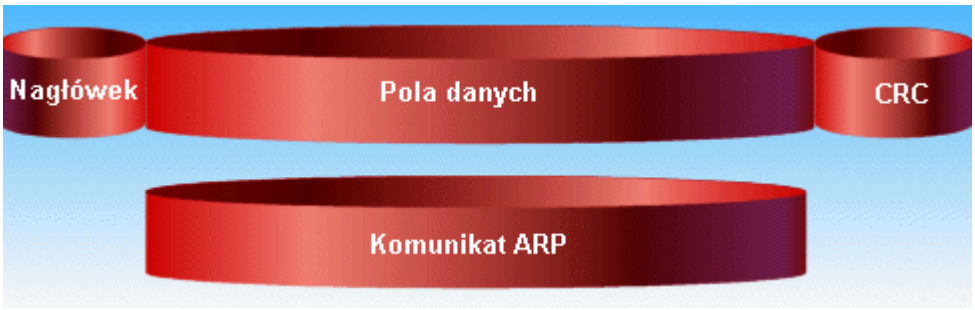
Wyobraźmy sobie na przykład, ze musimy przesłać dane do 1000 odbiorców. Wykorzystując do tego protokół TCP musimy otworzyć, kontrolować a następnie zamknąć 1000 połączeń. Koszt tych operacji jest stosunkowo wysoki. Wykorzystanie natomiast protokółu UDP nie wymaga wykonania tych wszystkich czynności.

Tak wiec protokół UDP zapewnia zawodne, bezpołączeniowe usługi transportowe ponad protokółem IP.

NASTĘPNA

4. Protokół ARP

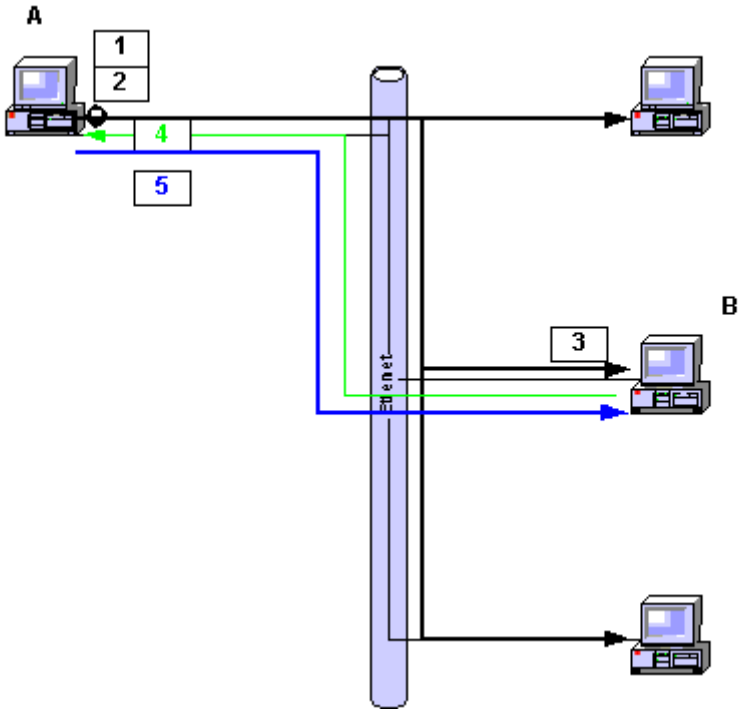
Protokół ARP jest protokółem odwzorowywania adresów. Definiuje on dwa rodzaje komunikatów: pytanie o adres MAC i odpowiedz. Komunikat ARP transportowany jest oczywiście wewnątrz ramki sprzętowej. Kapsułkowanie komunikatu ARP w ramce Ethernet pokazane jest na rysunku.



Rysunek 5 Ramka ARP

Informacja o tym, ze przesyłany jest komunikat ARP zawarta jest w nagłówku ramki w polu określającym typ ramki (dla komunikatu ARP wartość 0x806).

W celu wysłania pakietu z danymi musi być ustalony adres MAC odpowiadający adresowi IP. Protokół ARP po prostu odpytuje wszystkie komputery w sieci, czy maja potrzebny mu adres IP i prosi o przesłanie odpowiadającego mu adresu fizycznego. Aby ograniczyć ruch w sieci budowana jest dynamiczna tablica ARP, w której zapisywane są pary adres IP adres MAC komputerów z którymi został nawiązany kontakt. Tablica ta ma ograniczony rozmiar. Jeśli tablica ARP przepełni się, to jest z niej usuwany najstarszy wpis.



Rysunek 6 Mechanizm ARP

Mechanizm odwzorowywania adresów przez wymianę komunikatów z wykorzystaniem protokółu ARP przebiega następująco:

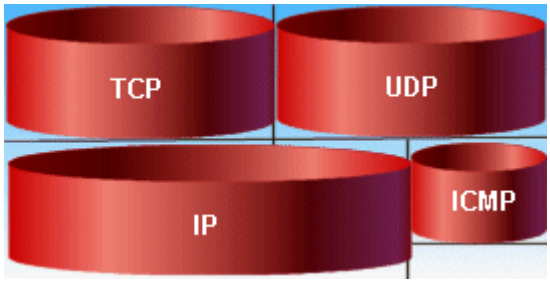
1. Komputer A, który chce wysłać pakiet z danymi sprawdza czy w jego tablicy ARP jest szukany adres IP komputera B; jeśli taki adres jest w tablicy to wykonywany jest punkt 5, jeśli nie to punkt 2
2. Komputer A, który chce wysłać pakiet z danymi wysyła najpierw zapytanie ARP do wszystkich komputerów w sieci, w którym pyta: Kto ma potrzebny mi adres IP?
3. Komputer B, który pozytywnie odpowiada na to pytanie dopisuje do swojej tablicy ARP adres IP i MAC komputera A i odsyła odpowiedz ze swoim adresem MAC
4. Komputer A, który wysłał pytanie w pkt 1 odbiera odpowiedz, dopisuje adres IP i MAC komputera B do swojej tablicy ARP
5. Komputer A wysyła pakiet IP z danymi do komputera B

NASTĘPNA

5. Protokół ICMP

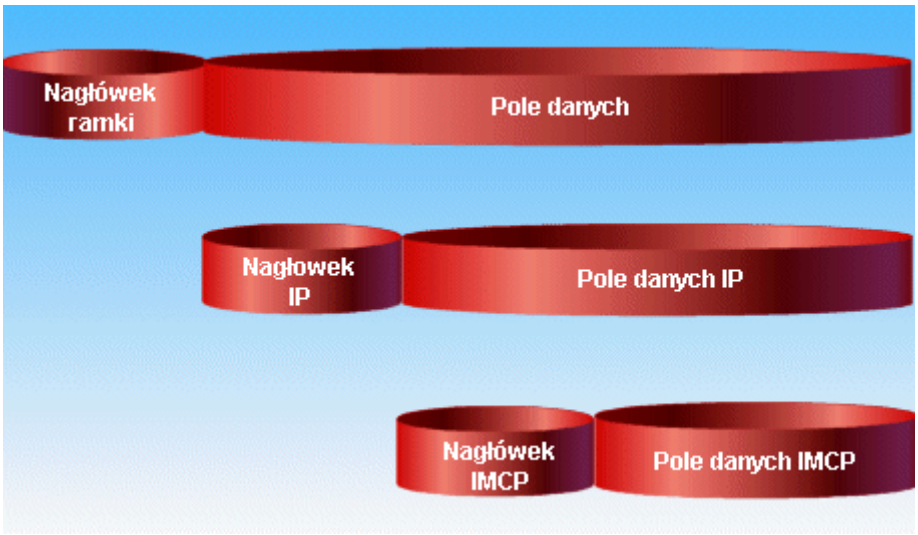
Protokół IP zajmuje się jedynie dostarczaniem datagramów. Nie zapewnia natomiast mechanizmów kontroli błędów.
Jednym z mechanizmów wykrywania błędów jest w protokole IP suma kontrolna, która omawialiśmy w poprzednich wykładach.
Jeśli suma kontrolna nie jest prawidłowa datagram jest po prostu porzucany. Odbiorca nie przekazuje natomiast informacji o tym, ze cos jest nie tak do nadawcy, bo nie może ufać danym odebranym w datagramie w szczególności suma kontrolna

Dlatego stos protokółów TCP/IP został wyposażony w protokół ICMP służący do przekazywania informacji o błędach w dostarczaniu datagramów za pomocą protokółu IP. Ulokowanie protokółu ICMP w stosie protokółów TCP/IP pokazuje rysunek.



Rysunek 7 Ulokowanie protokółu ICMP

Komunikat protokółu ICMP przesyłany jest za pomocą protokółu IP. Kapsułkowanie tego protokółu w ramce sieci fizycznej pokazuje rysunek.



Rysunek 8 Komunikat protokółu IMCP

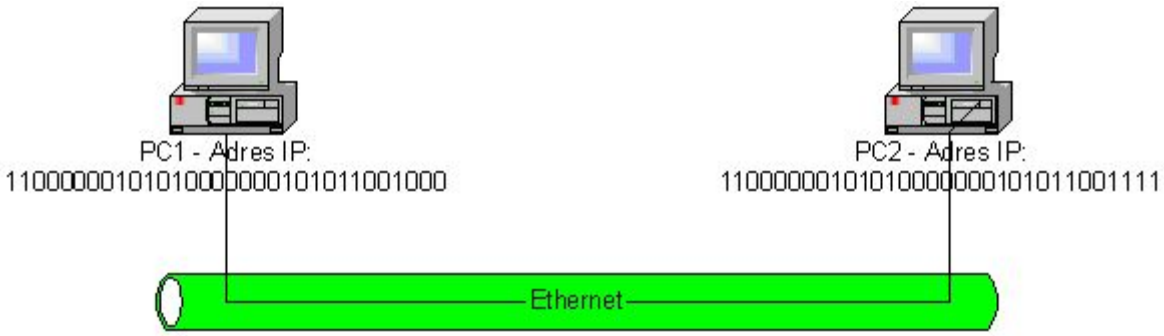
Jeśli w trakcie transmisji wystąpią pewne błędy, to komunikat o ich zaistnieniu zosta-nie przesłany protokółem ICMP. Przykładowe komunikaty o błędach ICMP to:
Tłumienie nadawcy wysyłany przez router, jeśli liczba odebranych datagramów przekracza pojemność jego buforów; po odebraniu tego komunikatu nadawca powinien zmniejszyć szybkość wysyłania komunikatów
Przekroczenie terminu komunikat wysyłany przy porzuceniu datagramu z powodu przekroczenia czasu życia datagramu

Odbiorca nieosiągalny komunikat wysyłany przez router, jeśli nie może on dostarczyć datagramu; pozwala na odróżnienie, czy nie działa cala siec odbiorcy czy tylko pojedynczy komputer

NASTĘPNA

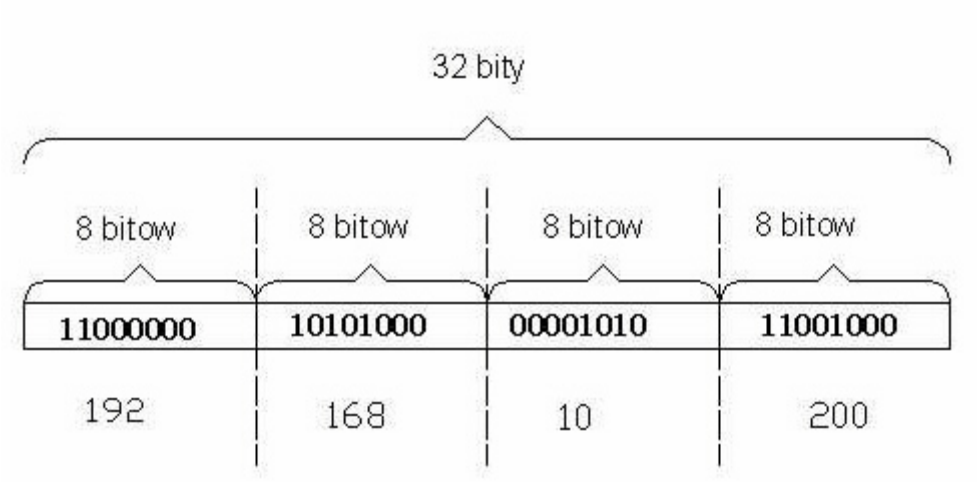
6. Adresy IP

Aby możliwa była komunikacja miedzy komputerami w sieci każdy z nich musi mieć jednoznaczny identyfikator. W sieciach wykorzystujących protokół IP takim identyfikatorem jest 32-bitowy numer. Numer ten zwany adresem przypisany jest w sposób jednoznaczny do danego komputera w sieci.



Rysunek 9 Adresy IP

Choć adres zapisany w postaci 32 bitów jest bardzo wygodny z punktu widzenia protokółu IP, to jednak dla człowieka nie jest on "przyjazny". W celu łatwiejszego posługiwania się adresami IP zapisujemy go w specjalnej postaci. Postać ta polega na podziale 32 bitowego adresu na 4 części (po 8 bitów) od-dzielonych od siebie kropkami i zapisaniu każdej z nich w notacji dziesiętnej. Tak wiec adres IP komputera PC1 wygląda tak:



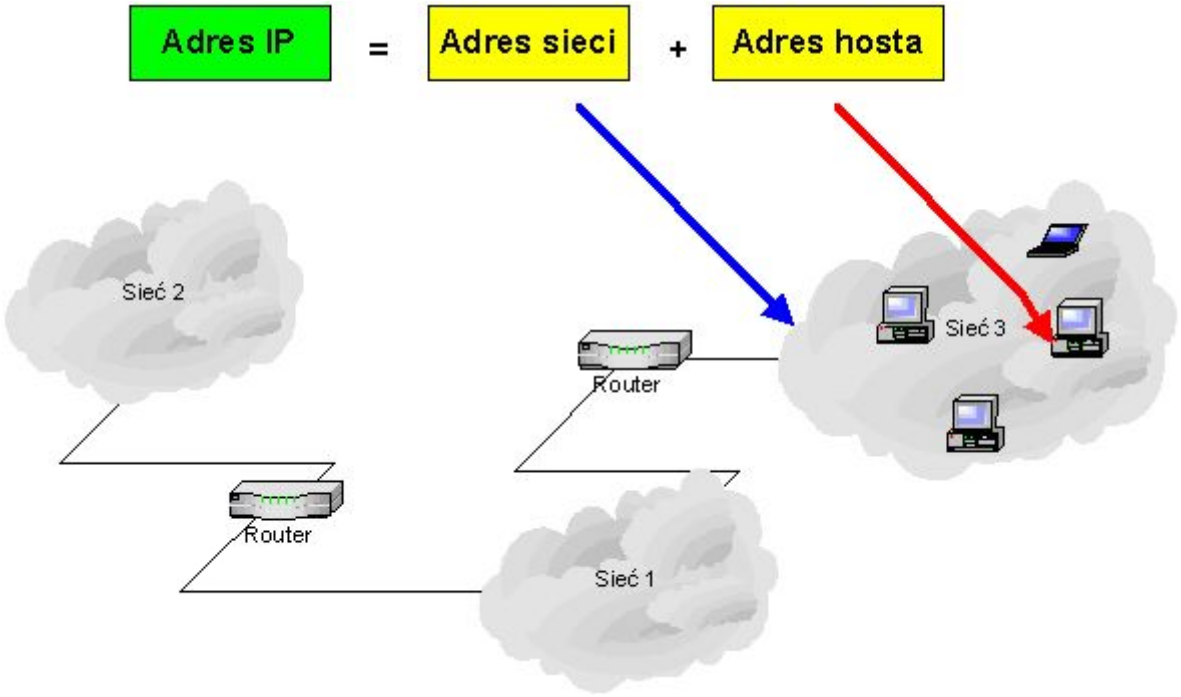
Rysunek 10 Segmentowa budowa adresu IP

Notacja binarna	Notacja dziesiętna
11000000 10101000 00001010 11001000	192.168.10.200

Tabela 1 Zapis adresu IP

Każdy host w sieci pracuje w obrębie określonej sieci lokalnej. Sieci lokalne mogą być oczywiście ze sobą połączone tworząc siec rozległą.

Ta struktura odzwierciedlona jest w adresie IP. Zawiera on w sobie dwie informacje identyfikujące jednoznacznie host w sieci rozległej: numer sieci *(ang. network ID)* jest to unikalny w obrębie sieci globalnej identyfikator danej sieci komputerowej. Określa on wszystkie urządzenia znajdujące się w tym samym segmencie sieci fizycznej i połączone z tym samym routerem. Wszystkie urządzenia podłączone do jednej sieci fizycznej musza mieć ten sam numer sieci. Numer sieci określany jest tez często adresem sieciowym. numer hosta *(ang. host ID)* jest to unikalny w obrębie danej sieci fizycznej identyfikator urządzenia (komputera, routery, drukarki sieciowej itp.) pracującego w sieci. Numer hosta określany jest tez często adresem hosta



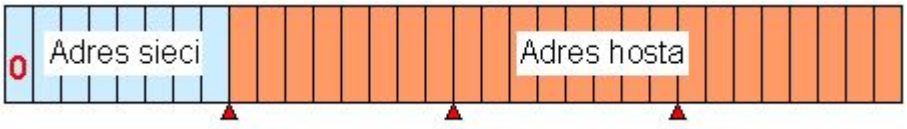
Rysunek 11 Składniki adresu IP

NASTĘPNA

7. Klasy adresu

Ze względu na podział adresu IP na cześć zawierająca adres sieci i adres hosta wyróżnia się piec klas adresów IP.
Klasa adresu określa, które bity w adresie zawierają informacje o numerze sieci, a które o numerze hosta.
Ze względu na podział adresu na cześć zawierająca numer sieci i cześć zawierająca numer hosta wyróżnia się następujące klasy adresów IP:

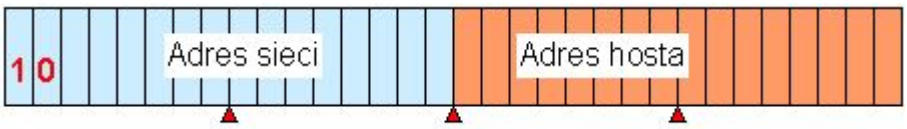
(7.1) Klasa A



Rysunek 12 Adres IP - klasa A

Klasa A jest przeznaczona dla sieci, w których liczba hostów w jednej sieci jest bardzo duża. W tej klasie na numer sieci przeznaczony jest pierwszy oktet (pierwsze osiem bitów) adresu IP, z tym ze najstarszy bit jest zarezerwowany i zawsze ma wartość 0.
Do zaadresowania różnych sieci pozostaje wiec w tej klasie 7 bitów. Jak z tego wynika, w klasie A można zaadresować 27=128 sieci. Rzeczywista liczba sieci, które można zaadresować w tej klasie jest jednak mniejsza, gdyż adresy złożone z samych zer (0000000) oraz samych jedynek (1111111) są zarezerwowane dla specjalnych celów.
Pozostałe 24 bity służą do adresowania hostów. Również i tutaj adresy składające się z samych zer i samych jedynek zostały zarezerwowane. Tak wiec w klasie A możemy w każdej sieci zaadresować 224-2=16 777 214 hostów.

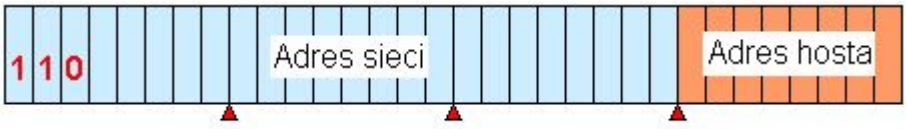
(7.2) Klasa B



Rysunek 13 Adres IP - klasa B

W klasie B na adres sieci przeznaczono dwa pierwsze oktety z całego adresu IP, z tym ze dwa pierwsze bity ustalono na 10. W klasie B mamy wiec do wykorzystania 14 bitów na adres sieci oraz 16 bitów na numer hosta.
Wobec tego w klasie B możemy zaadresować 214-2=16 384 sieci, a w każdej z nich 216-2=65 534 hostów.

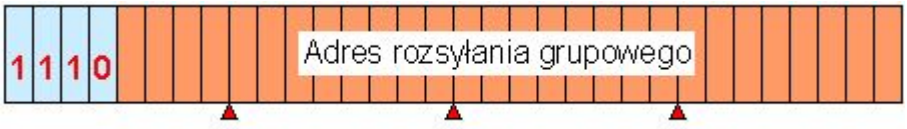
(7.3) Klasa C



Rysunek 14 Adres IP - klasa C

W klasie C na adres sieci zarezerwowano aż trzy pierwsze oktety z całego adresu IP, z tym ze trzy pierwsze bity ustalono na 110. W klasie C mamy do wykorzystania 21 bitów na adres sieci oraz 8 na adres hosta.
Wobec tego w klasie C możemy zaadresować 221-2=2 097 152 sieci, a w każdej z nich 28-2=254 hosty.

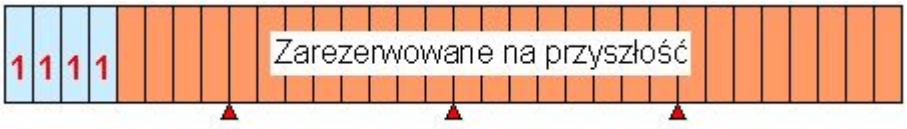
(7.4) Klasa D



Rysunek 15 Adres IP - klasa D

Klasa D jest przeznaczona do specjalnego celu jakim jest rozsyłanie grupowe. Rozsyłanie grupowe polega na dostarczaniu komunikatów do całej grupy komputerów. Adresy klasy D rozpoczynają się od sekwencji bitów 1110, po których następuje adres rozsyłania grupowego.

(7.5) Klasa E



Rysunek 16 Adres IP - klasa E

W klasie E pierwsze cztery bity są ustawione na 1111. Pozostała cześć adresu jest zarezerwowana dla przyszłych zastosowań

Obecnie do adresowania urządzeń w sieciach IP stosuje trzy klasy: A, B i C. Pozostałe dwie klasy klasa D i E nie są stosowane do adresowania hostów. Obecnie
Klasę adresu można rozpoznać po jego pierwszych czterech bitach. Tak wiec adres IP jest adresem samoidentyfikującym, gdyż informacja o jego klasie jest zawarta w nim samym.

Klasa	4 pierwsze bity	Pierwszy oktet	Adres sieci	Liczba sieci	Liczba hostów w jednej sieci
A	0???	1-126	w.0.0.0	126	16 777 214
B	10??	128-191	w.x.0.0	16 384	65 534
C	110?	192-223	w.x.y.0	2 097 152	254
D	1110	224-239	----	----	----
E	1111	240-255	----	----	----

Tabela 2 Klasy adresów IP

NASTĘPNA

8. Zasady adresowania IP

Zasady poprawnego adresowania IP można zebrać w kilku następujących punktach:

1) numer sieci musi w sposób jednoznaczny identyfikować siec, dlatego tez musi być unikalny w obrębie całej sieci;
2) numer hosta w obrębie danej sieci musi być unikalny;
3) w numerach sieci nie można stosować numerów zaczynających się od 127, np. 127.0.0.0. Adresy rozpoczynające się od 127 są adresami zarezerwowanymi i służą do adresowania pętli zwrotnej. Pętla zwrotna wykorzystywana jest przy testowaniu systemów. Pakiety wysłane na adres pętli zwrotnej nie opuszczają komputera. Przechodzą one przez warstwy oprogramowania sieciowego od jednego programu do drugiego. Najczęściej stosowanym adresem pętli zwrotnej stosowanym przy testowaniu oprogramowania jest adres 127.0.0.1;

4) nie można stosować adresów, w których wszystkie bity maja wartość jeden. Adres złożony z samych jedynek przeznaczony jest do rozgłaszania ograniczonego w lokalnej sieci fizycznej. Każdy pakiet wysłany na adres złożony z samych jedynek trafi do wszystkich interfejsów sieciowych pracujących w danej sieci lokalnej;

5) nie można stosować adresów, w których wszystkie bity maja wartość zero. Adres składający się z samych zer jest zarezerwowany do oznaczenia bieżącego komputera. Adres bieżącego komputera wykorzystywany jest na przykład w sytuacjach kiedy nie można podąć prawidłowego numeru komputera;
6) nie można stosować numerów hostów składających się z samych zer. Numer IP o postaci numer_sieci.same_zera (np. 193.254.0.0) przeznaczony jest do oznaczenia samej sieci, a nie konkretnego hosta w tej sieci;

7) nie można stosować numerów hostów składających się z samych jedynek. Adres IP o postaci numer_sieci.same_jedynki (np. 193.254.255.255) przeznaczony jest do oznaczenia pakietu rozgłaszania ukierunkowanego (ang. broadcast adress). Pakiet wysłany na taki adres wędruje do danej sieci (routera), a następnie jest rozsyłany do wszystkich interfejsów sieciowych pracujących w danej sieci.

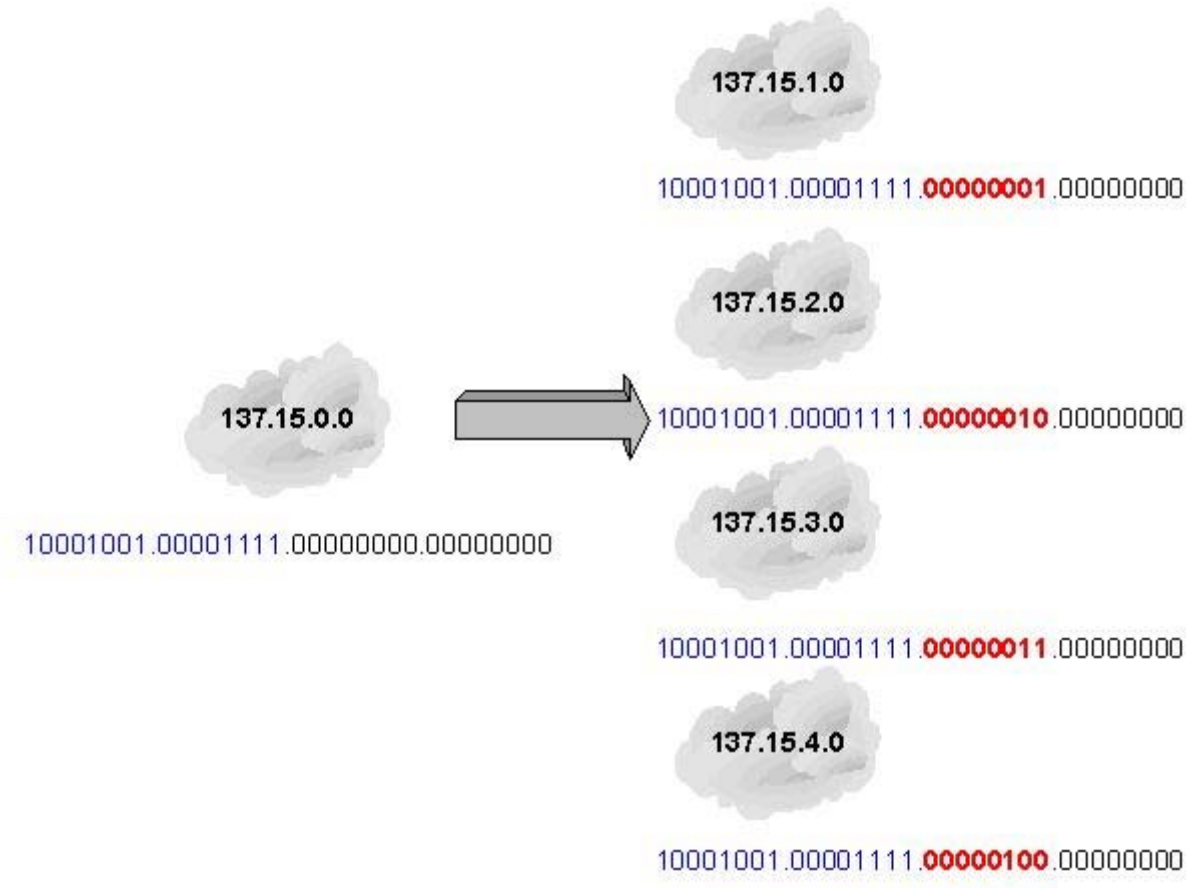
Adresy specjalnego przeznaczenia, których nie można używać do adresowania hostów zebrane zostały w tabeli.

Adres	Przykład	Znaczenie
127.*.*.*	127.0.0.1	Adres pętli zwrotnej
same_jedynki	255.255.255.255	Adres rozgłaszania ograniczonego
same_zera	0.0.0.0	Adres bieżącego komputera
numer_sieci.same_zera	137.15.0.0.	Adres sieci
numer_sieci.same_jedynki	137.15.255.255	Adres rozgłaszania ukierunkowanego

NASTĘPNA

9. Podsieci

Stosowanie samych tylko klas adresów IP może okazać się mało wygodne ze względu na duża liczbę komputerów w jednej sieci. W adresach klasy A liczba komputerów w jednej sieci przekracza przecież 16 milionów, w adresach klasy C wynosi co prawda "zaledwie" 254 ale i to jest często liczba zbyt duża.
Aby ograniczyć liczbę komputerów w jednej sieci adresowej IP stosuje się dodatkowy podział na podsieci w obrębie jednej przestrzeni adresowej sieci IP.
W tym celu cześć bitów adresu IP przeznaczonych pierwotnie na adres hosta, wykorzystuje się do zapisania numeru podsieci.



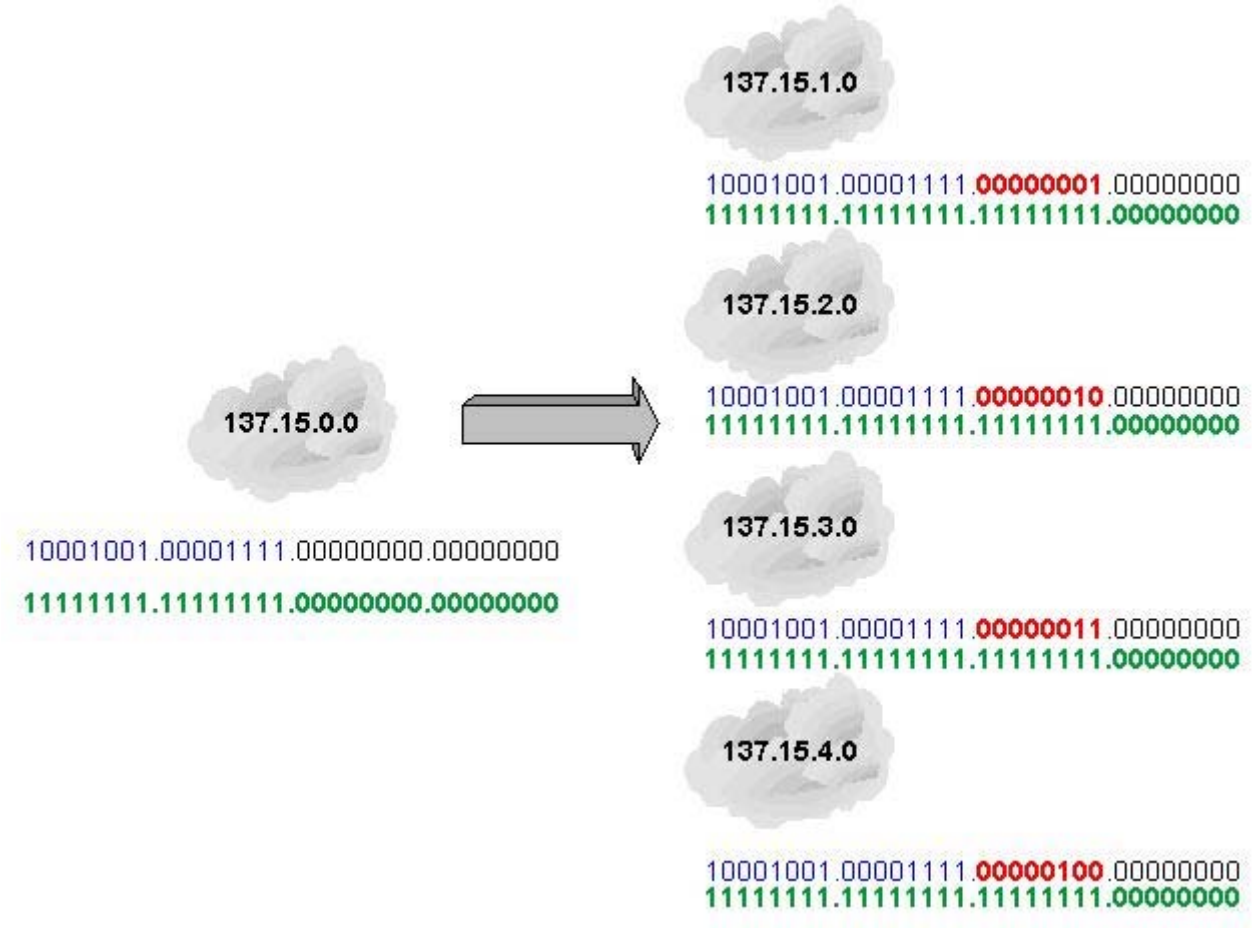
Rysunek 17 Podział na podsieci

Jako przykład rozpatrzmy siec 137.15.0.0. Jest to adres klasy B, w której można zaadresować do 65 534 hostów. Tak duża siec jest niewygodna w eksploatacji choćby z powodu dużego ruchu pakietów rozgłoszeniowych generowanych w tej sieci. Spróbujemy wiec podzielić te siec na podsieci. W tym celu wykorzystamy pierwsze osiem bitów z adresu hosta (trzeci oktet adresu) na zapisanie numeru podsieci. Każda z tak utworzonych podsieci możemy podłączyć do osobnego interfejsu sieciowego routera, a tym samym odseparować podsieci od siebie.
Musimy jeszcze opracować mechanizm, który poinformuje router o dokonanym przez nas podziale i będzie dostarczał informacje, które bity służą do oznaczenia numeru sieci, a które do oznaczenia numeru hosta. Mechanizm ten realizowany jest za pomocą maski podsieci. Maska podsieci jest ciągiem 32 bitów, który zawiera informacje o tym ,które bity w adresie oznaczają adres podsieci, a które numer hosta.
Bity w masce podsieci zostały zdefiniowane następująco:

- bity oznaczające numer sieci maja wartość 1

- bity oznaczające numer hosta maja wartość 0

W naszym wypadku maska podsieci ma wobec tego wartość:
11111111.11111111.11111111.00000000
lub w notacji dziesiętnej 255.255.255.0.



Rysunek 18 Podział na podsieci z maskami podsieci

Pełen adres komputera w sieci TCP/IP składa się z dwu elementów: adresu IP oraz maski podsieci.
W tabeli przedstawiono maski podsieci dla klas adresowych IP w notacji binarnej, dziesiętnej oraz skróconej.
W notacji skróconej podawana liczba jedynek występujących w masce podsieci

Klasa IP	Notacja binarna	Notacja dziesiętna	Notacja skrócona
A	11111111.00000000.00000000.00000000	255.0.0.0	/8
B	11111111.11111111.00000000.00000000	255.255.0.0	/16
C	11111111.11111111.11111111.00000000	255.255.255.0	/24

Tabela 3 Podstawowe maski podsieci dla klas IP

Wszystkie komputery w tej samej sieci fizycznej musza oczywiście mieć ten sam numer sieci, a wiec te sama maskę podsieci.

NASTĘPNA

10. Adresy prywatne

Każdy węzeł (komputer) podłączony do globalnej sieci Internet musi mieć nadany unikalny, niepowtarzalny numer IP. Adres urządzenia podłączonego bezpośrednio do sieci Internet nosi nazwę adresu publicznego i musi być przyznawany przez odpowiednia organizacje dbającą o unikalność adresów publicznych.
W puli adresów IP, obok adresów publicznych , zarezerwowano kilka adresów, które nie mogą być przypisane do urządzeń bezpośrednio podłączonym do sieci Internet. Adresy takie nazywane są adresami prywatnymi i wykorzystywane są w sieciach lokalnych odseparowanych od sieci globalnej. Dzięki temu organizacje mogą budować swoje sieci lokalne, które nie maja bezpośredniego połączenia z Internetem, bez konieczności ustalania puli adresów z organizacja koordynująca.
Adresy prywatne nigdy nie występują w globalnej sieci Internet, a pakiety przesyłane na te adresy nie są przesyłane przez routery do sieci globalnej.
Do adresów prywatnych należą następujące adresy:

- 10.0.0.0./8
- 172.16.0.0/12
- 192.168.0.0/16

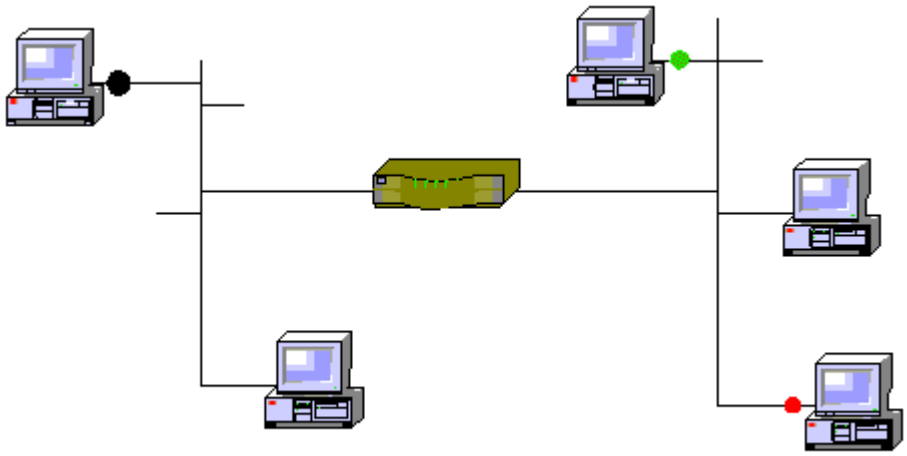
Sieć prywatna	Początkowy adres prywatny	Końcowy adres prywatny
10.0.0.0/8	10.0.0.1	10.255.255.254
172.16.0.0/12	172.16.0.1	172.31.255.254
192.168.0.0/16	192.168.0.1	192.168.255.254

Tabela 4 Adresy prywatne

NASTĘPNA

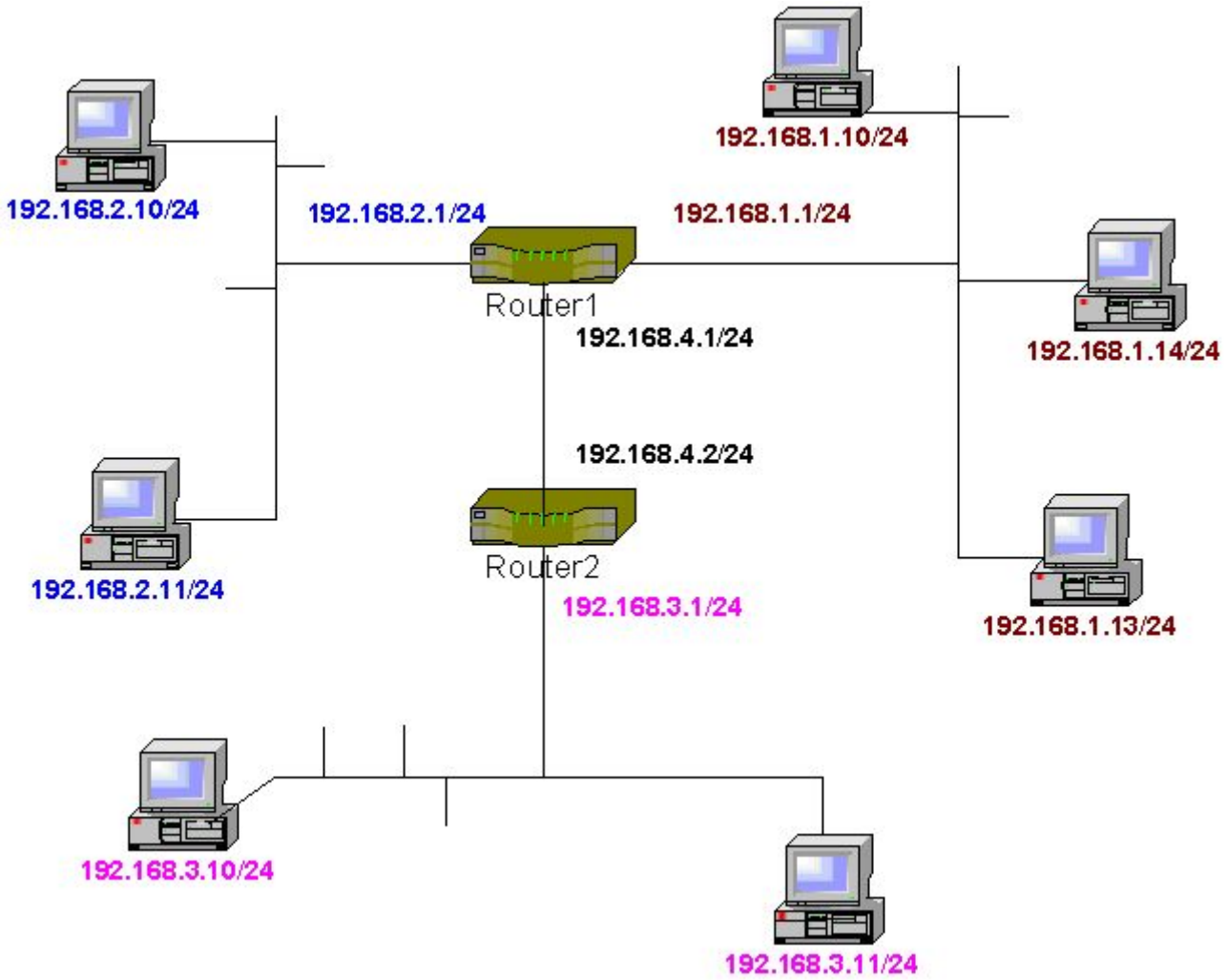
11. Routing

Każdy pakiet wysyłany w sieci, aby mógł być prawidłowo dostarczony, musi zawierać adres MAC odbiorcy. W sieciach złożonych tylko z jednego segmentu mechanizm tłumaczenia adresu IP na adres MAC jest stosunkowo prosty i został opisany podczas omawiania protokółu ARP. W sieciach złożonych z kilku segmentów sprawa się nie-co komplikuje.
Jeśli pakiet jest adresowany do komputera, który nie jest w sieci lokalnej, to jest on wysyłany do routera, który odpowiada za dalsza transmisje takiego pakietu



Rysunek 19 Router

Router zajmuje się przekazywaniem pakietów miedzy różnymi segmentami sieci. Na rysunku 19 przedstawiono router łączący dwa segmenty sieci. Liczba segmentów łączonych przez jeden router może być oczywiście większa. Każdemu segmentowi sieci łączonemu przez router musi odpowiadać oddzielna karta sieciowa.
Jeżeli pakiet jest wysyłany do komputera znajdującego się poza siecią lokalna, to trafia on do routera. Router na podstawie specjalnej tablicy, zwanej tablica routingu, decyduje do którego segmentu sieci przesłać taki pakiet. Jeśli jest on adresowany do komputera, który jest bezpośrednio połączony z routerem , to jest on wtedy kierowany do niego bezpośrednio. Jeśli natomiast jest adresowany do komputera, który nie jest w tej samej sieci co router, to jest przekazywany do kolejnego routera.



Rysunek 20 Routing

Przykładowa tablica routingu routera 2 dla sieci przedstawionej na rysunku 20 została przedstawiona w tabeli

Numer sieci	Maska	Next hop
192.168.1.0	255.255.255.0	192.168.4.1
192.168.2.0	255.255.255.0	192.168.4.1
192.168.3.0	255.255.255.0	Połączony bezpośrednio
192.168.4.0	255.255.255.0	Połączony bezpośrednio

Tabela 4 Tabela routingu Router2

Tablica routingu zawiera informacje, o tym, co należy zrobić z pakietem, czyli do jakiej sieci należy go przesłać. Jeśli router nie znajduje w tablicy routingu odpowiedniego wpisu, oznacza to dla niego ze pakiet powinien być przesłany do domyślnego routera (ang. default route).
Tablica routingu może być budowana ręcznie lub automatycznie. Proces przekazywania pakietu z wykorzystaniem mechanizmu routingu wygląda następująco:

(11.1) Nadawca

1) ustawiany jest parametr TTL;

2) dopisywany jest adres IP odbiorcy;
3) protokół ARP ustala odpowiedni adres MAC (adres komputera lokalnego lub routera w wypadku przesyłania pakietu do komputera odległego);

(11.2) Router

1) protokół IP sprawdza poprawność sumy kontrolnej;
2) jeśli adres docelowy nie jest adresem routera, zmniejszana jest wartość para-metru TTL; jeśli wartość TTL wynosi zero, to pakiet taki jest porzucany, a protokół ICMP wysyła odpowiedni komunikat do nadawcy;
3) protokół IP wylicza ponownie sumę kontrolna;
4) protokół IP sprawdza tablice routingu w poszukiwaniu miejsca, do którego powinien być dostarczony pakiet; jeśli w tablicy routingu nie zostanie odnaleziona odpowiednia informacja, to protokół ICMP wysyła odpowiedni komunikat do nadawcy;
5) po odnalezieniu odpowiedniej informacji w tabeli routingu protokół IP. ustala adres kolejnego odbiorcy pakietu oraz numer interfejsu sieciowego, który zajmie się wysłaniem tego pakietu;

(11.3) Odbiorca

1) protokół IP sprawdza sumę kontrolna;
2) protokół IP sprawdza poprawność adresu IP;
3) pakiet po odrzuceniu nagłówka jest przekazywany do wyższej warstwy stosu protokółów (TCP lub UDP).

NASTĘPNA

12. Diagnostyka

W tym punkcie omówimy najczęściej wykorzystywane narzędzia służące do diagnostyki działania sieci TCP/IP. W wypadku nieprawidłowego funkcjonowania sieci TCP/IP należy sprawdzić następujące elementy:

1. konfiguracje stosu protokółów TCP/IP
2. poprawność działania interfejsu sieciowego
3. poprawność działania sieci lokalnej
4. poprawność działania domyślnego routera
5. poprawność działania sieci rozległej

(12.1) Ping

(ang. Packet InterNet Groper) program narzędziowy dostępny w Windows 9x/NT/2000 do diagnostyki połączenia w sieciach TCP/IP
Składania

```
PING [-t] [-a] [-n liczba] [-l długość] [-f] [l czas-życia] [-v
typ-usługi] [-r liczba] [-s liczba] [[-j lista-komputerow] | [-k
lista-komputerów] [-w czas] lista-miejsc-przeznaczenia
```

Argumenty	*Opis*
-t	ping uje w sposób ciągły do chwili przerwania
-a	Podczas pingowania wyświetla nazwę komputera o podanym adresie IP
-n liczba	Liczba pingowań
-l długość	Liczba bajtów, które są wysyłane do pingowanego komputera (domyślnie 32)
-f	Zakaz fragmentowania pakietów routerom będącym na trasie
-l czas-życia	Ustawia pole TTL
-v typ-usługi	Ustawia pole TOS
-r liczba	Wyświetla rasę dla pakietów PING (od 1 do 9)
-s liczba	Żądanie umieszczenia znacznika czasowego dla określonej liczby skoków
-j lista-komputerów	Określenie trasy pakietu
-k lista-komputerów	Określenie trasy pakiety, jeśli komputery nie mogą być rozdzielone routerami pośredniczącymi
-w czas	Czas oczekiwania (w milisekundach)
Lista-miejsc-przeznaczenia	Lista komputerów do pingowania

(12.2) Tracert / traceroute

- program narzędziowy dostępny w Unixie/Windows 9x/NT/2000 do śledzenia trasy datagramów IP w sieciach TCP/IP
Składania

```
TRACERT [-d] [-h maksymalna-liczba-skoków] [-j lista-komputerów] [-
w czas] host-przeznaczenia
```

Argument	*Opis*
-d	Brak konwersji adresów IP komputerów znajdujących się pomiędzy lokalnym komputerem a hostem przeznaczenia na nazwy symboliczne
-h maksymalna-liczba-skoków	Maksymalna liczba skoków pomiędzy lokalnym komputerem a hostem przeznaczenia
-j lista-komputerów	Określa rasę przez komputery na liście
-w czas	Czas oczekiwania w milisekundach przez zakończeniem testowania
Host-przeznaczenia	Komputer do zlokalizowania

(12.3) Arp

- program narzędziowy dostępny w Windows 9x/NT/2000 do badania i modyfikowania wartości w tablicy bufora ARP w sieciach TCP/IP
Składania

```
ARP –a [adres-intern] [-N [adres-interfejsu]
ARP –d –g adres-intern [adres-interfejsu]
ARP –s adres-intern adres-ethern [adres-interfejsu]
```

Argument	*Opis*
-a	Pokazuje bieżące wpisy w buforze ARP
-g	Tak samo jak –a
Adres-intern	Adres IP
-N	Pokazuje wpisy bufora dla karty sieciowej określonej przez adres-interfejsu
Adres-interfejsu	Adres interfejsu, wykorzystywany jeśli w systemie jest wiele kart sieciowych
-d	Usuwa wpis
-s	Dodaje wpis do bufora
Adres-ethern	Adres MAC

(12.4) Netstat

program narzędziowy dostępny w Windows 9x/NT/2000 do wyświetlania bieżących połączeń sieciowych TCP/IP oraz statystyk dla poszczególnych protokołów
Składania

```
NETSTAT [-a] [-e] [-n] [-s] [-p protokół] [-r] [odstęp]
```

Argument	*Opis*
-a	Wyświetla połączenia i porty oczekujące na połączenie
-e	Wyświetla statystyki Ethernet
-n	Wyświetla adresy i numery portów
-s	Wyświetla statystyki dla poszczególnych protokołów

-p protokół	Wyświetla połączenia dla określonego protokołu
-r	Wyświetla zawartość tablicy trasowania
Czas	Wyświetla statyki co odstęp czas

Podsumowanie

Stos protokołów TCP/IP jest podstawowym zestawem protokołów stosowanych w komunikacji w sieciach rozległych. Zapewnia od uniwersalne i pewne połączenie między dwoma komputerami. Każda maszyna pracująca w sieci TCP/IP musi mieć przydzielony unikalny numer zwany adresem IP. Dzięki temu numerowi może być ona jednoznacznie zidentyfikowana w sieci. Numer IP zawiera informację zarówno o numerze sieci jak i numerze komputera w tej sieci. O tym, która część adresu jest adresem sieci, a która hosta decyduje klasa adresu. Dodatkowo administrator sieci może dzielić ją na mniejsze fragmenty w danej klasie stosując tak zwane maski podsieci. Dzięki takiemu rozwiązaniu adresowanie IP jest bardzo elastyczne.