DR INŻ. PIOTR GOETZEN

Administracja Sieci Komputerowych

PROTOKOŁY SIECIOWE

Polski Uniwersytet Wirtualny

Protokoły sieciowe

Zrozumienie działania protokołów sieciowych jest jednym z podstawowych zagadnień, którym administrator powinien poświęcić dużo czasu. Poniżej przedstawione zostały aktualnie najważniejsze protokoły stosowane w sieciach (warstwa 2, 3, 4 modelu ISO/OSI). Ich poznanie ułatwi zrozumienie tematyki poruszanej w dalszej części kursu Administracji sieciami.

1. ARP – Address Resolution Protocol

Do komunikacji miedzy hostami w sieci stosuje się dwa rodzaje adresów – adresy w warstwie łącza danych nazywa się **adresami fizycznymi**, a adresy w warstwie sieciowej **adresami logicznymi**. W przypadku protokołu IP adresem logicznym jest adres IP, a w technologii Ethernet adresem fizycznym jest adres MAC, wpisany w pamięć karty sieciowej. Protokołem spełniającym funkcję „pośrednika" jest protokół tłumaczenia adresów ARP, który kojarzy adres logiczny IP hosta z odpowiadającym mu adresem fizycznym MAC.

1.1. Zasada działania protokołu ARP

Na przykład host A o adresie IP 10.1.1.1 zamierza wysłać dane do hosta B (adres IP 10.1.1.2). Hosty te zostały właśnie skonfigurowane i wcześniej nie wymieniały żadnych informacji między sobą. Użytkownik A chce sprawdzić, czy komputer B działa, w tym celu skorzysta z programu ***ping***. Na komputerze A w wierszu poleceń użytkownik wpisze polecenie:

```
ping 10.1.1.2
```

Z warstwowego modelu komunikacji w sieci wiadomo, że dane (zanim zostaną wypuszczone na zewnątrz komputera) przechodzą „po stosie" od najwyższej do najniższej warstwy modelu ISO/OSI. Dochodząc do warstwy trzeciej zostają obudowane nagłówkiem IP. W nagłówku tym znajdują się miedzy innymi adresy IP – hosta źródłowego (10.1.1.1) oraz docelowego (10.1.1.2). Adres IP komputera źródłowego jest ustalany na podstawie aktualnie skonfigurowanego interfejsu sieciowego. Adres IP hosta docelowego podaje jawnie użytkownik jako argument polecenia *ping*.

Dane zostają następnie przesłane do warstwy drugiej – łącza danych, ale w ramce ethernetowej system musi podać fizyczne adresy komputera źródłowego oraz docelowego. Adresy te są potrzebne do jednoznacznej identyfikacji komunikujących się stron. Nie będzie problemu z adresem MAC hosta A – system pobierze go z pamięci karty. W jaki sposób jednak ustalić adres MAC docelowego hosta B? Do tego właśnie zostanie wykorzystany protokół ARP. Host A, aby ustalić adres MAC stacji B, wysyła **zapytanie rozgłoszeniowe** ARP. Zapytanie to trafi do wszystkich stacji w tym segmencie sieci, ale tylko host B na nie odpowie. Wygląd takiego zapytania przedstawiono na rysunku 1:

Rozgłoszeniowe zapytanie ARP:

<table>
<tr><td>Adres źródłowy:

AA:AA:AA:AA:AA:AA</td><td>Adres docelowy:
(rozgłoszeniowy)

FF-FF-FF-FF-FF-FF</td><td>Adres źródłowy:

10.1.1.1</td><td>Adres docelowy:

10.1.1.2</td><td>Zapytanie:

Jaki jest twój adres MAC?</td></tr>
<tr><td colspan="2">Nagłówek Ethernet</td><td colspan="3">Nagłówek ARP</td></tr>
</table>

Rys. 1. Uproszczona ramka ethernetowa, zawierająca zapytanie protokołu ARP

W momencie, gdy host B otrzyma takie zapytanie, w odpowiedzi zwraca swój adres fizyczny BB:BB:BB:BB:BB:BB, sam natomiast wpisuje do swojej tablicy adres fizyczny (AA:AA:AA:AA:AA:AA) i logiczny (10.1.1.2) hosta A (otrzymane w zapytaniu).

Adres źródłowy: BB:BB:BB:BB:BB:BB	Adres docelowy: AA:AA:AA:AA:AA:AA	Adres źródłowy: 10.1.1.2	Adres docelowy: 10.1.1.1	Odpowiedź: Podaje swój adres MAC
Nagłówek Ethernet		Nagłówek ARP:		

Rys. 2. Uproszczona ramka ethernetowa, zawierająca odpowiedź protokołu ARP

W tym momencie hosty A oraz B posiadają (każdy w swojej tablicy ARP) dane na temat adresów fizycznych i logicznych drugiego komputera. Z tej informacji mogą skorzystać także inne protokoły. Protokół ICMP może teraz przejść do warstwy łącza danych, ponieważ zna fizyczny adres hosta docelowego. Host B może już bez żadnego zapytania wysłać odpowiedź bezpośrednio do hosta A, ponieważ zna jego adres logiczny i fizyczny.

Uzyskane informacje przechowywane są w podręcznym buforze. Następnym razem, gdy host A będzie chciał ponownie wysłać pakiet IP do hosta B, sprawdzi najpierw w swojej tablicy, czy nie ma odpowiedniego wpisu – pary adresów: logicznego i fizycznego hosta B. Jeśli ma, skorzysta z niego bez konieczności ponownego wysyłania zapytania ARP. Należy zwrócić uwagę, że pakiet ARP wysyłany jest na adres rozgłoszeniowy warstwy łącza danych. W związku z tym, na przykład przy dużej ilości zapytań, może generować zbędny ruch w sieci i niepotrzebnie obciążać inne hosty.

1.2. Schemat budowy nagłówka protokołu ARP

16		32
Hardware type (16 bits)		Protocol type (16 bits)
Hardware address length (8 bits)	Protocol address length (8 bits)	*Opcode* (16 bits)
Source hardware address		
Source protocol address		
Destination hardware address		
Destination protocol address		
Data		

Rys. 3. Nagłówek ARP

Tab. 1. Przykładowe wartości pola *Hardware type* (Typ sprzętu)

Wartość	Opis
1	Ethernet
6	IEEE 802
15	Frame Relay
16	ATM, Asynchronous Transmission Mode
17	HDLC
18	Fibre Channel
19	ATM, Asynchronous Transmission Mode
20	Serial Line
21	ATM, Asynchronous Transmission Mode
31	Ipsec tunnel

Tab. 2. Przykładowe wartości pola *Protocol type* (Typ protokołu warstw wyższych)

Value	Description
0 x 86DD	IPv6
0 x 800	IPv4

Długość adresu sprzętowego (ang. *Hardware Address Length*) 8 bitów – podawana w bajtach.

Długość adresu sieciowego (ang. *Protocol Address Length*) 8 bitów – podawana w bajtach.

Kod operacji (ang. *Opcode*) 16 bitów.

Tab. 3. Przykładowe wartości pola *Opcode* (*Kod operacji*)

Wartość	**Opis**	**Dokument RFC**
1	zapytanie (ang. *request*)	RFC 826
2	odpowiedź (ang. *reply*)	RFC 826, RFC 1868
3	zapytanie odwrotne (ang. *request reverse*)	RFC 903
4	odpowiedź odwrotna (ang. *reply reverse*)	RFC 903

1.3. Proxy-ARP

W przypadku tzw. *proxy-arp* router jest urządzeniem pośredniczącym dla stacji docelowej. Przykładem takiej konfiguracji jest modemowe połączenie punkt-do-punktu (*point-to-point*) stacji docelowej z routerem. Po pojawieniu się w sieci zapytania o adres IP urządzenia połączonego z routerem, router stwierdza, że poszukiwany adres IP pasuje do jednego z podłączonych do niego urządzeń. Odpowiada na zapytanie, udając, że dany adres IP jest jego własnym adresem. Urządzenie nadające przyporządkowuje w swojej tablicy ARP adres IP komputera docelowego do adresu MAC routera i kieruje transmisje do routera. Router przekazuje dalej pakiety do stacji docelowej.

1.4. Reverse-ARP

Istnieje także protokół **odwrotny ARP** (*reverse ARP*) używany głównie przy konfiguracji bezdyskowych stacji roboczych. W momencie, gdy host podczas inicjalizacji odkrywa, że nie został mu przydzielony żaden adres IP, wysyła odwrotne zapytanie ARP. Podaje swój MAC adres (który ma każde urządzenie ethernetowe) i oczekuje na odpowiedź. Ramka taka jest ramką rozgłoszeniową o wszystkich bitach w adresie docelowym równych jeden FF:FF:FF:FF:FF:FF. Zawarty w niej adres docelowy IP jest również adresem rozgłoszeniowym 255.255.255.255. Adres źródłowy jest ustawiony na zero: 0.0.0.0.

Nagłówek Ethernet		Nagłówek ARP		
Adres źródłowy	Adres docelowy	Adres źródłowy	Adres docelowy	Jaki jest mój adres IP?
aa:aa:aa:aa:aa:aa	FF:FF:FF:FF:FF:FF	0.0.0.0	255.255.255.255	

Rys. 4. Uproszczona forma ramki protokołu Reverse-ARP

Odpowiedzi na takie zapytania zapewniają serwery protokołu Reverse-ARP, że zdefiniowana tablica zawierająca adresy MAC i przypisane im adresy IP. Serwer w odpowiedzi podaje hostowi wartość adresu IP, jaka powinien sobie skonfigurować do poprawnego działania.

2. IP – Internet Protocol

Protokół Internetowy IPv4 (ang. *Internet Protocol version 4*), zdefiniowany przez międzynarodową grupę inżynierów IETF w RFC 791, jest protokołem warstwy sieciowej modelu OSI. Należy do stosu protokołów TCP/IP. Jednostkę danych tego protokołu (PDU) określa się jako **datagram** albo **pakiet**. Wszystkie inne protokoły w stosie TCP/IP (oprócz ARP i RARP) używają protokołu IP do przekazywania danych między hostami.

2.1. Budowa datagramu IP

Datagram IP składa się z dwóch podstawowych części: nagłówka oraz właściwych danych, które zawierają pakiety protokółów warstw wyższych, które są w nim transportowane. Nagłówek to informacje adresowe oraz dane kontrolne, potrzebne do dostarczenia datagramu do miejsca przeznaczenia.

Format tego nagłówka przedstawiony jest na rysunku 5.

<table>
<tr><td>4</td><td>8</td><td>16</td><td colspan="2">32 bits</td></tr>
<tr><td>Ver. (4 bits)</td><td>IHL (4 bits)</td><td>Type of service (8 bits)</td><td colspan="2">Total length (16 bits)</td></tr>
<tr><td colspan="3">Identification (16 bits)</td><td>Flags (3 bits)</td><td>Fragment offset (13 bits)</td></tr>
<tr><td colspan="2">Time to live (8 bits)</td><td>Protocol (8 bits)</td><td colspan="2">Header checksum (16 bits)</td></tr>
<tr><td colspan="5">Source address (32 bits)</td></tr>
<tr><td colspan="5">Destination address (32 bits)</td></tr>
<tr><td colspan="5">Option + Padding</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

Rys. 5. Nagłówek datagramu IP

2.2. Budowa nagłówka IP

Wersja (*Version*) 4 bity – określa wersje użytego protokołu IP.

Długość nagłówka (IHL – *Internet Header Length*) 4 bity – mówi o wielkości informacji w nagłówku, wyrażonej w wielokrotnościach 32 bitów. Minimalna wartość dla tego pola wynosi 5, co oznacza, że długość nagłówka jest większa albo równa 160 bitom, natomiast maksymalna długość nagłówka nie może przekroczyć 512 bitów.

Rodzaj usługi (*Type of Service*) 8 bitów – pole to ma różne zastosowania. Ma ono postać jednobitowych flag, określających priorytet pakietu, czyli między innymi parametr pierwszeństwa, stopień wymaganej niezawodności, przepustowość czy opóźnienia.

Tab. 4. Rodzaj usługi – znaczenie poszczególnych bitów

Numer bitu	Znaczenie	Wartości
0, 1, 2	pierwszeństwo	111 — sterowanie siecią (maks. priorytet) 110 — sterowanie siecią wewnętrzną 101 — CRITIC/ECP 100 — natychmiastowe zastąpienie 011 — zastąpienie 010 — natychmiastowe 001 — priorytet 000 — program standardowy (min. priorytet)
3	opóźnienie	0 — normalne 1 — małe
4	przepustowość	0 — normalna 1 — wysoka
5	niezawodność	0 — normalna 1 — wysoka
6, 7	Bity zarezerwowane do przyszłego użycia	

Całkowita długość datagramu (*Datagram Lenght*) 16 bitów – informuje o całkowitej długości datagramu IP (nagłówka łącznie z danymi), mierzonej w bajtach. W związku z tym długość datagramu IP może wynieść maksymalnie 65 536 bajtów. Powszechnie hosty akceptują datagramy o długości minimalnej 576 bajtów. Przy maksymalnej długości nagłówka (zwykle 64 bajty) resztę, czyli około 90% informacji, stanowią właściwe dane.

Identyfikacja (*Identification*) 16 bitów – identyfikator przypisany datagramowi przed fragmentacją (jeżeli była przeprowadzona). W przypadku fragmentacji określa ona przynależność fragmentu do datagramu. Identyfikator winien być jak najbardziej przypadkowy. Fragmentacja umożliwia transportowanie datagramu przez sieci o zróżnicowanej budowie. Technologie, takie jak Ethernet czy Token-Ring, mają określony maksymalny rozmiar danych, które są w stanie przesłać. W przypadku, gdy rozmiar datagramu przewyższa MTU (ang. *Maximum Transfer Unit*) danej sieci, konieczny staje się jego podział na akceptowalne fragmenty.

Flagi (*Flags*) 3 bity – to trzy jednobitowe wskaźniki, informujące, czy system może dokonać fragmentacji datagramu i czy jest ona aktualnie dokonywana.

Tab. 5. Flagi - znaczenie poszczególnych bitów

Numer bitu	Znaczenie	Wartości
0	zarezerwowany, musi mieć wartość zero	
1	DF (*Don't Fragment*)	0 — można fragmentować 1 — nie wolno fragmentować
2	MF (*More Fragments*)	0 — ostatnia fragmentacja (ostatni lub jedyny fragment) 1 — więcej fragmentacji (datagram jest jednym z kilku fragmentów)

Protokół IP jest bardzo elastyczny i zapewnia transport danych przez bardzo różne architektury sieci (np. Token Ring, X.25). Każdy z tych rodzajów sieci ma określony maksymalny rozmiar pakietu **MTU**

(*Maximum Transmission Unit*). Podczas przekazywania datagramu pomiędzy sieciami może się okazać, ze rozmiar transmitowanych danych jest większy od MTU sieci docelowej. W takim wypadku datagram zostaje podzielony na fragmenty i przesłany w rozmiarze wymaganym przez sieć go transportującą. Odbiorca datagramów na podstawie pól *Identyfikator*, *Przesuniecie fragmentacji* oraz *Flagi* łączy fragmenty w całość.

Przesuniecie fragmentu (*Fragment offset*) 13 bitów – zawiera dane wykorzystywane przy składaniu datagramów podzielonych na mniejsze fragmenty. Wskazuje miejsce, gdzie należy wstawić dany fragment względem początku całego datagramu. Jego jednostka są 64-bitowe przesunięcia. Jeśli przeprowadzono fragmentacje, to pierwszy fragment ma przesuniecie równe zeru.

Czas życia (*Time to Live*) 8 bitów – pole to (TTL) określa maksymalna ilość routerów, przez które datagram może zostać przetransmitowany. Wielkość ta ustawiana jest w momencie wysyłania pakietu. Każdy router, do którego dociera pakiet, zmniejsza wartość tego pola o jeden. Gdy osiągnięta zostanie wartość zero, pakiet jest usuwany, a do nadawcy powinien zostać wysyłany komunikat ICMP, informujący o zaistniałym fakcie. Ograniczenie to zapobiega wiecznemu krążeniu pakietów w sieci.

Protokół (*Protocol*) 8 bitów – pole to informuje, jaki protokół warstwy wyższej (np. TCP, UDP) umieścił swoje dane w datagramie IP. Określa numer protokołu warstwy wyższej, do którego mają zostać dostarczone dane z datagramu. Przykładowe numery i odpowiadające im protokoły zestawione są poniżej:

protokół	identyfikator	nazwa protokołu
ICMP	*1*	*Internet Control Message Protocol*
TCP	*6*	*Transmission Control Protocol*
UDP	*17*	*User Datagram Protocol*

Suma kontrolna (*Header checksum*) 16 bitów – pole kontroli błędów. Węzeł sieciowy, najczęściej router, może na podstawie tego pola określić, czy nagłówek datagramu został uszkodzony. Wadliwe datagramy są odrzucane. Ponieważ nagłówek przy przejściu przez każdy router zmienia się (zmieniane jest pole TTL), wartość jego sumy kontrolnej jest ponownie przeliczana. Dane transportowane poza nagłówkiem standardowo nie są chronione.

Adres źródłowy (*Source address*) 32 bity – pole to zawiera adres IP nadawcy pakietu.

Adres docelowy (*Destination address*) 32 bity — pole to zawiera adres docelowego hosta, dla którego przeznaczony jest datagram.

Opcje (*Options*) – długość pola jest zmienna – pole opcji nie jest obowiązkowe, służy do bardziej szczegółowego opisu zachowania datagramu w sieci. Jest to pole złożone z różnorodnych kodów o zmiennej długości. W przypadku wystąpienia większej liczby opcji, są one podawane w jednym ciągu. Wszystkie opcje są definiowane przez jeden, podzielony na trzy pola, bajt.

- Pierwsze pole jest jednobitowe (*copy flag*) i określa zachowanie opcji w przypadku fragmentacji.
  Jeśli bit ma wartość 0, opcja pojawia się jedynie w pierwszym datagramie, jeśli bit ma wartość 1, opcja jest kopiowana do nagłówków wszystkich kolejnych fragmentów.
- Drugie pole jest dwubitowe i definiuje klasę opcji (*option class*). Aktualnie zostały zdefiniowane jedynie dwie wartości klasy opcji:
  - 0 – stosowana do kontroli datagramów lub sieci,
  - 2 – opcja jest używana do wykrywania błędów.
- Trzecie pole jest 5-bitowe i określa numer opcji (*option number*).

Tab.6. Stosowane wartości klas i numerów opcji

Klasa opcji	Numer opcji	Opis
0	0	Oznacza koniec listy opcji
0	1	Brak opcji — używane jako wypełnienie
0	2	Opcje bezpieczeństwa (do użytku wojskowego)
0	3	Swobodny routing źródłowy. Opcja ta umożliwia podanie listy routerów, przez które powinien przejść datagram, dążąc do celu; umożliwia jednocześnie stosowanie dowolnych tras dojścia do wymienionych routerów.
0	7	Aktywacja zapisywania routingu; dodawane są pola z zapisem kolejnych odwiedzanych przez datagram routerów.
0	9	Dokładny routing źródłowy. Opcja ta umożliwia podanie listy routerów, przez które powinien przejść datagram, dążąc do celu; nie pozwala na żadne zbaczanie datagramu z wyznaczonej trasy.
0	4	Aktywacja zapisywania czasu w kolejnych odwiedzanych routerach. Czas jest obliczany w milisekundach od godziny zero (północy). Z powodu braku synchronizacji czasu w routerach opcja ta jest mało użyteczna.

Wypełnienie (*Padding*) – długość pola jest zmienna – to ostanie pole nagłówka, jeśli pole opcji nie zajmuje pełnego słowa, to zostaje uzupełnione tutaj do 32 bitów.

3. ICMP – Internet Control Message Protocol

ICMP jest to protokół komunikacyjny, służący do sterowania siecią Internet, opisany w RFC 972 (dla IPv4). Rozszerza on funkcjonalność protokołu IP o zarządzanie sytuacjami nietypowymi – np. awariami. Oba protokoły są od siebie zależne i powinny być implementowane razem. Protokół ICMP wykorzystywany jest głównie do przesyłania wszelkiego rodzaju pakietów informujących o błędach, ważnych sytuacjach oraz do kontroli stanu połączeń.

3.1. Zadania ICMP

1 Protokół ICMP dostarcza informacji diagnostycznych dla warstw wyższych. System, który wykrył problem wysyła do nadawcy komunikat *Miejsce docelowe nieosiągalne* (*Destination Unreachable*).

Możliwe są dwa przypadki:

1 komunikat wysłany jest przez router:
   a) host nieosiągalny (ang. *Host Unreachable*) — gdy adres docelowy nie istnieje, ma to miejsce w przypadku, gdy komputer docelowy jest wyłączony, nie ma fizycznego połączenia z siecią lub jest źle skonfigurowany,
   b) sieć nieosiągalna (ang. *Network Unreachable*) — gdy router nie może dostarczyć datagramu do tej sieci,

2 komunikat wysyłany jest przez host:
   a protokół nieosiągalny (ang. *Protocol Unreachable*) — w przypadku braku wsparcia dla protokołu warstw wyższych, którego dotyczył pakiet,
   b port nieosiągalny (ang. *Port Unreachable*) — w przypadku, gdy na przykład usługa korzystająca z portu protokołu TCP jest nieosiągalna.

2 Ocena sprawności urządzeń — polega na żądaniu potwierdzenia, na przykład w przypadku testowania osiągalności odległego węzła sieciowego. Do takiego sprawdzenia używane jest polecenie ping, zaimplementowane w większości sieciowych systemów operacyjnych. Cały proces polega na wysłaniu komunikatu Echo Request (Zadanie echa do badanego systemu). Jeśli badany węzeł odpowie komunikatem Echo Replay (Odpowiedź na echo), należy uznać, że można z nim nawiązać kontakt. W przeciwnym razie, gdy nadawca w określonym czasie nie uzyska odpowiedzi, host docelowy zostanie uznany za nieosiągalny.

3 Przesyłanie komunikatów o błędach (ang. Error Messages) — w przypadku przechodzenia datagramu przez router, każdorazowo zmniejszana jest wartość pola TTL (Time to Live) w nagłówku pakietu IP o 1. Datagram taki jest usuwany, gdy wartość tego pola osiągnie zero. Jeśli, przykładowo, wartość początkowa pola TTL była ustawiona na 10, a pakiet przechodząc przez dziesiąty router nadal nie osiągnął odbiorcy, wówczas ostatni router usunie go. Router powinien wysłać do nadawcy komunikat ICMP Time-exceeded (czas przekroczony).

4 Zmiana trasy ramek, wspomaganie wyznaczania tras (ang. Routing Assistance) — komunikaty takie wysyłane są w przypadku, gdy router, który odebrał datagram uzna, że lepsza bramka będzie inny router w tej samej sieci. Wysłany zostanie wówczas pakiet Redirect, wskazujący na inny węzeł sieciowy z tej samej podsieci. Odbiorca, po otrzymaniu takiego komunikatu, powinien zaktualizować swoja tablice routingu.

5 Oddziaływanie na częstotliwość przesyłania ramek ma miejsce, kiedy stacja nadawcza odbierze zadanie zmiany tempa ich nadawania (np. w przypadku, gdy komputer docelowy nie nadąża

z przetwarzaniem nadchodzących datagramów) — wysyłany jest wówczas komunikat Source Quench.

6 Kontrola datagramów bez możliwości korygowania błędów.

7 Nie zajmuje się informowaniem o błędach w datagramach, których był nadawca, inaczej mówiąc — nie wysyła komunikatów ICMP na temat uszkodzonych datagramów ICMP.

8 W celu uniknięcia zbyt dużego obciążenia sieci, protokół ICMP informuje tylko o błędach datagramów IP, które mają pole Fragment offset ustawione na zero.

3.2. Nagłówek protokołu ICMP

Format datagramu ICMP jest stosunkowo prosty. Zazwyczaj składa się z trzech pól:

1) *Typ komunikatu* — określa rodzaj sytuacji powodującej wysłanie komunikatu,
2) *Kod* — zawiera dodatkowe informacje o typie komunikatu,
3) *Suma kontrolna* — służy do wykrywania uszkodzonych datagramów ICMP.

Protokół ICMP może zawierać jeszcze nagłówek i dane pakietu, który spowodował jego wysłanie (np. w wyniku błędu — wyzerowanie pola *TTL* w nagłówku IP). Na podstawie tych danych można ustalić protokół oraz aplikacje warstwy wyższej, której dane miały problemy z dotarciem do miejsca przeznaczenia.

8	16	32
Type (8 bits)	Code (8 bits)	Checksum (16 bits)
Identifier (16 bits)		Sequence number
Address mask		

Rys. 6. Schemat budowy nagłówka protokołu ICMP

Zadania protokołu ICMP rozpoznaje się po polach Typ i Kod wiadomości.

3.3. Pola Typ i Kod komunikatu ICMP

Najważniejsze 16 typów komunikatów ICMP zostało zdefiniowanych w RFC 792.

Lista pozostałych RFC definiujących protokół ICMP:

- RFC 777: Internet Control Message Protocol.
- RFC 778: DCNET Internet Clock Service.
- RFC 792: INTERNET CONTROL MESSAGE PROTOCOL.
- RFC 816: FAULT ISOLATION AND RECOVERY.
- RFC 844: Who Talks ICMP, too? Survey of 18 February 1983.
- RFC 950: IP Subnet Extension.
- RFC 1108: U.S. Department of Defense Security Options for the Internet Protocol.
- RFC 1122: Requirements for Internet Hosts – Communication Layers.
- RFC 1123: Requirements for Internet Hosts – Application and Support.
- RFC 1127: A Perspective on the Host Requirements RFCs.
- RFC 1156: Management Information Base for Network Management of TCP/IP-based internets.
- RFC 1191: Path MTU Discovery.
- RFC 1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II.
- RFC 1256: ICMP Router Discovery Messages.
- RFC 1393: Traceroute Using an IP Option.
- RFC 1435: IESG Advice from Experience with Path MTU Discovery.
- RFC 1475: TP/IX: The Next Internet.
- RFC 1788: ICMP Domain Name Messages.
- RFC 1812: Requirements for IP Version 4 Routers.

- RFC 1940: Source Demand Routing: Packet Format and Forwarding Specification (Version 1).
- RFC 2003: IP Encapsulation within IP.
- RFC 2011: SNMPv2 Management Information Base for the Internet Protocol using SMIv2.
- RFC 2401: Security Architecture for the Internet Protocol.
- RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.
- RFC 2521: ICMP Security Failures Messages.
- RFC 2765: Stateless IP/ICMP Translation Algorithm (SIIT).
- RFC 2780: IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers.
- RFC 2893: Transition Mechanisms for IPv6 Hosts and Routers.
- RFC 3344: IP Mobility Support for Ipv4.

Polem definiującym format komunikatu jest pole *Typ*, które zawsze znajduje się w pierwszych 8 bitach pola danych datagramu IP.

Tab. 7. Pola Typ i Kod komunikatu ICMP

Typ		**Kod**		
W	**Znaczenie**	**W**	**Znaczenie**	**Z**
0	*Echo*	0	Dane odebrane w tym komunikacie muszą być zwrócone w komunikacie *Echo Reply* (typ = 8).	GH
3	*Destination Unreachable*	0	*Net unreachable* — sieć nieosiągalna.	G
		1	*Host unreachable* — komputer nieosiągalny.	G
		2	*Protocol unreachable* — host docelowy nie obsługuje wymaganego protokołu warstwy wyższej.	H
		3	*Port unreachable* — port nieosiągalny.	H
		4	*Fragmentation needed and DF set* — gdy datagram nie może być fragmentowany w celu dostarczenia do sieci docelowej.	G
		5	*Source route failed* — gdy datagram nie może być dostarczony w wyniku problemów z routingiem źródłowym lub odłączenia sieci docelowej.	G
4	*Source Quench*	0	Komunikat pojawia się w przypadku, gdy datagramy są wysyłane zbyt szybko, aby host lub router docelowy mógł je opracować. W odpowiedzi na każdy usunięty datagram powinien zostać wysłany jeden komunikat *Source Quench*.	HG
5	*Redirect*	0	*Redirect datagrams for the Network* — przekieruj datagramy dla danego adresu sieci.	G
		1	*Redirect datagrams for the Host* — przekieruj datagramy dla adresu pojedynczego komputera.	G
		2	*Redirect datagrams for the Type of Service and Network* — przekieruj datagramy dla danego adresu sieci i równoczesnego wystąpienia określonej wartości pola TOS.	G
		3	*Redirect datagrams for the Type of Service and Host* — przekieruj datagramy dla adresu pojedynczego komputera i równoczesnego wystąpienia określonej wartości pola TOS.	G

8	*Echo Reply*	0	Jest odpowiedzią na komunikat *Echo* (typ = 0).	GH
9	*Router Advertisement*	0	Część protokołu „ICMP Router Discovery Messages" — RFC 1256. Wysyłany cyklicznie na adres *multicast* przez router umożliwia wykrywanie routera przez stacje.	G
10	*Router Solicitation*	0	Część protokołu „ICMP Router Discovery Messages" — RFC 1256. Stacja podczas uruchamiania może wysłać taki komunikat na adres *broadcast* w celu wykrycia routerów.	H
11	*Time Exceeded*	0	*Time to live exceeded in transit* — jeśli bramka, przesyłając datagram i zmniejszając wartość pola TTL, otrzyma wartość zero, usuwa datagram oraz powinna poinformować o tym host źródłowy za pomocą tego komunikatu.	G
		1	*Fragment reassembly time exceeded* — wysyłany, gdy komputer nie może złożyć fragmentów datagramu ze względu na przekroczenie czasu oczekiwania na kolejny fragment. Jeśli fragment zerowy nie został dostarczony, nie jest wysyłany żaden komunikat.	H
12	*Parameter Problem*	0	*Pointer indicates the error* — jeśli bramka wykryje nieprawidłowości w nagłówku datagramu uniemożliwiające jego dalsze przetwarzanie, usuwa go i wysyła ten komunikat ICMP. Wartość pola *Kod* określa bajt, w którym błąd został wykryty.	GH
13	*Timestamp*	0	Dane odebrane w tej wiadomości są zwracane razem z dodatkową wartością równą ilości milisekund od północy czasu uniwersalnego (UT). Komunikat zawiera trzy wartości *timestamp*: czas wysłania, czas odebrania i czas transmisji.	GH
14	*Timestamp Reply*	0		
15	*Information Request*	0	Ten komunikat służył do samokonfiguracji stacji (np. bezdyskowych) i uzyskiwania adresu sieci. Aktualnie jest przestarzały i został zastąpiony protokołami RARP i BOOTP.	GH
16	*Information Reply*	0		
17	*Address mask request*			
18	*Address mask reply*			
19	*Reserved (for security)*			
20 – 29	*Reserved (for robustness experiment)*			
30	*Traceroute*			
31	*Conversion error*			
32	*Mobile Host Redirect*			
33	*IPv6 Where-Are-You*			

34	*IPv6 I-Am-Here*
35	*Mobile Registration Request*
36	*Mobile Registration Reply*
37	*Domain Name request*
38	*Domain Name reply*
39	*SKIP Algorithm Discovery Protocol*
40	*Photuris, Security failures*
41 – 255	*Reserved*

Skróty użyte w tabeli:

W – oznacza wartość,

Z – opisuje, czy źródłem tego komunikatu ICMP może być:

H – host,

G – bramka.

4. TCP/UDP

Działanie współczesnych sieci jest oparte głównie o stos protokołów TCP/IP, do którego zaliczają się również protokoły TCP i UDP. Protokoły te znajdują się w warstwie transportowej modelu ISO/OSI, która zajmuje się zarządzaniem przepływem informacji w komunikacji typu punkt–punkt, tzn. takiej, w której protokoły transportowe działają tylko miedzy końcowymi systemami. Dane protokołów TCP i UDP są przesyłane w pakietach IP.

4.1. UDP – User Datagram Protocol

Protokół UDP stosowany jest do transportu danych w bezpołączeniowym trybie dostarczania datagramów, tzn. nie ustanawia w żaden sposób połączenia i nie sprawdza gotowości odległego komputera do odebrania przesyłanych danych. W przypadku, gdy pakiet nie dotrze do nadawcy lub suma kontrolna nie będzie się zgadzała, protokół UDP nie podejmie żadnych kroków w celu retransmisji bądź korekty danych, nie gwarantując tym samym dostarczenia danych do odbiorcy. W związku z brakiem mechanizmów kontroli dostarczenia danych zmniejszona została ilość informacji kontrolnych przenoszonych przez protokół, co zwiększyło efektywność tego protokołu podczas transmisji danych.

0	16 31
Source port	Destination port
Length	Checksum
Data	

Rys. 7. Budowa pakietu UDP

Pierwsze dwa bajty nagłówka zawierają adres portu źródłowego, następne adres portu docelowego pakietu UDP. Protokół UDP sprawdza się w sytuacjach, gdy ilość przesyłanych danych jest niewielka. W tym przypadku obciążenie, wynikające z dodania informacji dotyczących kontroli poprawności połączenia, mogłoby stać się porównywalne z ilością przesyłanych informacji. Ponadto niektóre aplikacje same dbają o kontrolę poprawności transmisji i wykorzystywanie do ich transmisji protokołu połączeniowego byłoby dublowaniem tych samych funkcji.

4.2. TCP – Transmission Control Protocol

Główną funkcją protokołu kontroli transmisji TCP jest zarządzanie połączeniami między komputerami. Wykorzystywany jest on do transportu danych w trybie połączeniowym. Posiada funkcję gwarancji dostarczenia danych do odbiorcy, tzn. sprawdza, czy dane zostały dostarczone przez sieć poprawnie i w określonej kolejności. Do sprawdzenia stosuje **potwierdzenia** (ang. *Acknowledgement*). TCP jest protokołem niezawodnym, połączeniowym, działającym na strumieniach bajtów. Połączenia negocjowane są w trzyetapowym procesie i jeśli nie nastąpi przerwanie połączenia, to protokół utrzymuje je do końca transmisji. Komunikacja w trybie połączeniowym odbywa się w trzech fazach:

- ustanowienie połączenia,
- transfer danych,
- rozłączenie połączenia.

4.3. Budowa segmentu TCP

Budowa segmentu TCP jest przedstawiona na rysunku 8.

	Bits									
words	0	4	8	12	16	20	24	27	31	
1	Source port				Destination port					Header
2	Sequence number									
3	Acknowledgement number									
4	Data offset	Reserved		Flags	Window					
5	Checksum				Urgent Pointer					
6	Options						Padding			
7	Data									

Rys. 8. Budowa segmentu TCP

Port źródłowy (Source port) – numer portu źródłowego

Port docelowy (Destination port) – numer portu docelowego

Numer kolejny (Sequence number) – kolejny numer pierwszego bajtu przesyłanych w tym segmencie danych. Jeżeli protokół TCP otrzyma dane z wyższych warstw, których nie może przesłać w postaci jednego pakietu, wówczas dzieli je na mniejsze fragmenty, zwane segmentami. Do identyfikacji tych segmentów wykorzystuje liczbę przesłanych bajtów, będącą początkiem nowego segmentu. Liczba ta jest każdorazowo powiększana o pierwszy numer kolejny (ISN – Initial Sequence Number) i umieszczana w nagłówku TCP w polu Numer kolejny. Jeśli flaga SYN jest ustawiona, to numer kolejny jest równy ISN, a pierwszy bajt danych ma numer ISN + 1.

Numer potwierdzenia (Acknowledgement number) – jeśli jest ustawiona flaga ACK, pole to zawiera wartość następnego numeru kolejnego, który nadawca spodziewa się otrzymać. Wykorzystane jest po nawiązaniu transmisji.

Przesuniecie (Data offset – 4 bity) – przesuniecie danych – liczba 32-bitowych słów w nagłówku TCP. Wskazuje początek danych.

Zarezerwowane (Reserved – 6 bitów) – zarezerwowane do przyszłego wykorzystania, musi posiadać wartość zero.

Flagi (Flags – 6 bitów) – kolejne bity oznaczają:

URG – oznaczenia pola pilnego wskaźnika,
ACK – oznaczenia pola potwierdzenia,
PSH – funkcja przepychania,
RST – zresetuj połączenie,
SYN – zsynchronizuj kolejne numery,
FIN – nie pobieraj więcej danych od nadawcy.

Okno (16 bitów) – liczba bajtów danych, które nadawca zgodzi się przyjąć. Pole to służy do sterowania przepływem danych (ang. Windowing). Okno o wartości zero informuje nadawcę, że powinien wstrzymać transmisję dopóki nie otrzyma segmentu z inną wartością w tym polu.

Suma kontrolna (Checksum – 16 bitów) - jest sumą kontrolną nagłówka i danych.

Wskaźnik pilności (Urgent pointer – 16 bitów) - zawiera numer kolejny bajtu następującego po „pilnych danych”. Pole to jest używane jedynie, gdy jest ustawiona flaga UGR.

Opcje (Options – 0-44 bajtów) – mają długość będącą wielokrotnością 8 bitów. Suma kontrolna obejmuje również opcje. Ciąg opcji kończy się zawsze polem o nazwie End of option list.

Tab. 8. Opcje segmentu TCP

Rodzaj	Długość	Opis	RFC
0	1	End of option list	RFC 793
1	1	No operation	RFC 793
2	4	Maximum Segment Size	RFC 793
3	3	Window scale factor	RFC 1072, RFC 1323
4	2	SACK permitted	RFC 2018
5	zmienna	SACK	RFC 2018, RFC 2883
6	6	Echo	RFC 1072
7	6	Echo reply	RFC 1072
8	10	Timestamp	RFC 1323
9	2	Partial Order Connection Permitted	RFC 1693
10	3	Partial Order Service Profile	RFC 1693
11	6	CC, Connection Count	RFC 1644
12	6	CC.NEW	RFC 1644
13	6	CC.ECHO	RFC 1644
14	3	TCP Alternate Checksum Request	RFC 1146
15	zmienna	TCP Alternate Checksum Data	RFC 1146
16		Skeeter	
17		Bubba	
18	3	Trailer Checksum Option	
19	18	MD5 signature	RFC 2385
20		SCPS Capabilities	
21		Selective Negative Acknowledgements	
22		Record Boundaries	
23		Corruption experienced	
24		SNAP	
25			
26		TCP Compression Filter	

Uzupełnienie (Padding) – uzupełnia zerami opcje do długości będącej wielokrotnością 32 bitów.

Segment TCP teoretycznie może mieć długość aż 65 535 bajtów, ale zwykle jest ona o wiele mniejsza, ze względu na protokoły warstwy drugiej ISO/OSI. Przykładowo Ethernet może przenieść jedynie 1 500 bajtów. Aby wynegocjować długość segmentu, protokół TCP używa jednej ze swoich opcji – Maximum Segment Size.

4.4. Nawiązywanie połączenia – TCP

Protokół TCP w celu zapewnienia niezawodności wykorzystuje mechanizm potwierdzenia z retransmisją (PAR – *Positive Acknowledgment with Re-transmission*). Dane przesyłane są dopóty, dopóki system wysyłający nie otrzyma potwierdzenia, że dane przeszły bezbłędnie. Każdy segment TCP zawiera sumę kontrolną wykorzystywaną przez odbiorcę do sprawdzenie poprawności przesłanych danych. Jeżeli segment danych został odebrany bezbłędnie, wysyłane jest potwierdzenie odebrania danych. Jeżeli segment jest uszkodzony, odbiorca nie wysyła potwierdzenia. Po pewnym czasie nadawca retransmituje segment danych, dla którego potwierdzenie nie doszło.

Połączenie jest nawiązywane przez przesłanie serii **komunikatów kontrolnych**, tzw. *Handshake*. O tym, czy dany segment jest kontrolny, świadczy ustawienie bitu SYN w polu flagi. TCP stosuje potwierdzenie trójfazowe:

I faza:

Host A, nawiązujący połączenie, wysyła do hosta B segment z ustawionym bitem SYN. W segmencie tym podany jest początkowy numer sekwencji danych, które zostaną przesłane przez host A.

II faza:

Host B odpowiada segmentem z ustawionymi bitami ACK (potwierdzenia) i SYN (synchronizacja), potwierdzając odebranie poprzedniego segmentu. W polu Numer kolejny podaje, jaki będ będzie numer początkowy sekwencji przesłanych przez niego danych.

III faza:

Host A wysyła segment potwierdzający odbiór segmentu od hosta B (ustawiony bit ACK) i zawierający pierwsze przesyłane dane.

Po zakończeniu transmisji danych hosty wymieniają trzy segmenty potwierdzenia z ustawionym bitem FIN (koniec danych), co powoduje zerwanie połączenia między nimi. Ponieważ dane dostarczane przez TCP traktowane są jako strumień, należy dbać o ich kolejność. Nie jest istotne od jakiej liczby systemy zaczną numerację danych — może być ona dowolna i dla tego wartości te są wymieniane podczas nawiązywania połączenia (przy ustawionych bitach SYN) w polach Numer kolejny. Liczby te określa się mianem „początkowy numer sekwencji” (ISN — *Initial Sequence Number*). Bajtom danych nadawane są numery począwszy od ISN + 1.

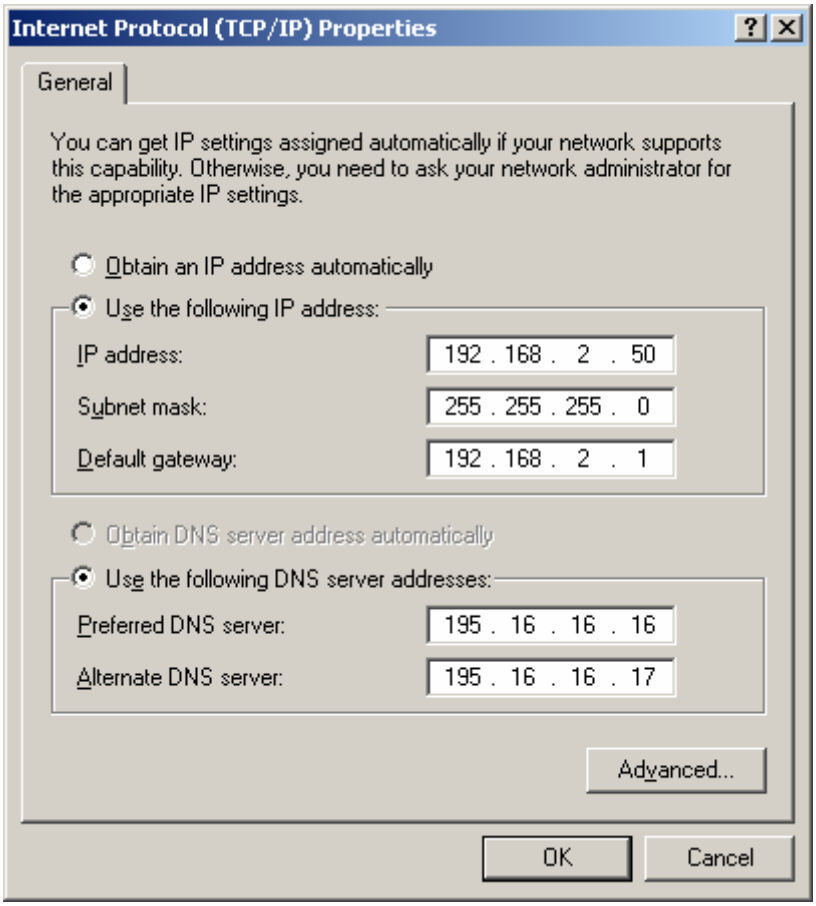
Segmenty z ustawionym bitem potwierdzenia ACK pełnią dwie funkcje: potwierdzają otrzymanie danych i sterują ich przepływem. Standard TCP nie wymaga potwierdzania każdego segmentu danych. Segment z ustawionym bitem ACK potwierdza odebranie wszystkich danych od początku transmisji. Wartość w polu Numer potwierdzenia jest równa ilości prawidłowo odebranych danych w bajtach.

5. ADRESOWANIE IP

Każdy host używający stosu protokołów TCP/IP powinien mieć prawidłowo ustawiony adres sieciowy warstwy 3 – IP. Obecnie najczęściej używaną implementacją adresu IP jest jej wersja 4 (IPv4).

Kiedy dokonuje się konfiguracji karty sieciowej stacji roboczej czy serwera, należy podać kilka niezbędnych wartości (rys. 9):

1. adres IP hosta (IP address), np. 192.168.2.50
2. maskę podsieci (subnet mask), np. 255.255.255.0
3. bramkę (default gateway),
4. adresy serwerów DNS (Domain Name System): podstawowego i zapasowego.



Rys. 9. Zakładka konfiguracji adresów IP w systemie Microsoft Windows XP

Taka konfiguracja interfejsu umożliwi połączenie się z Internetem. Użytkownik będzie mógł używać nazw domen, np. www.wp.pl zamiast adresów IP (zamiany dokona serwer DNS) – by się połączyć z serwerami Internetu. Jeśli ustawi się wyłącznie adres IP hosta i maskę podsieci, to taka konfiguracja też będzie poprawna, ale umożliwi komunikację tylko w ramach tego samego segmentu sieci (tej samej podsieci).

Obecnie funkcjonują dwie wersje adresów IP – starsza, bardzo rozpowszechniona IPv4 oraz nowsza, mniej popularna IPv6.

Adres IP w wersji 4 ma zawsze i niezmiennie długość 32 bitów. Należy zwrócić uwagę, że mimo binarnej natury administratorzy najczęściej przedstawiają go postaci dziesiętnej, co znacznie ułatwia posługiwanie się nim. Adres podzielony jest na cztery 8-bitowe bloki zwane oktetami:

11000011. 01111101.00000010. 00110010

odpowiada dziesiętnej postaci adresu:

192.168.2.50

Maksymalna wielkość liczby w każdym oktecie nie może przekroczyć wartości 255 (11111111 dwójkowo).

Administrator sieci musi biegle przeliczać liczby z systemu dwójkowego na dziesiętny i odwrotnie.

Kiedy trzeba przedstawić adres IP w postaci binarnej, mając jego postać dziesiętną należy rozpocząć od najstarszego oktetu:

192.168.2.50

Przy przeliczaniu z postaci dziesiętnej na dwójkową pomocna może być tabela 9 obrazująca wagi dziesiętne dla poszczególnych bitów:

Tab. 9. Wagi dziesiętne dla poszczególnych bitów w oktecie

→ kierunek przeliczania →							
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
pozycja bitu							
8	7	6	5	4	3	2	1
bit najstarszy							bit najmłodszy

Od liczby dziesiętnej należy odjąć wartość 128. Jeżeli wynik tej operacji będzie liczbą dodatnią (lub zerem) w polu najstarszego, ósmego bitu należy ustawić wartość binarną 1. Od otrzymanej różnicy należy odjąć wartość 64. Jeśli wynik będzie liczbą dodatnią, w polu bitu (2^6) należy ustawić wartość 1. Jeśli wynik odejmowania będzie liczbą ujemną, dla danej pozycji bitu przypisać należy 0.

Schemat liczenia przedstawiony jest w tabeli 10. NIE – przenieś liczbę do następnego kroku. TAK – do następnego kroku przenieś różnicę.

Tab. 10. Schemat przeliczania oktetu adresu z postaci dziesiętnej na dwójkową

Pozycja bitu 12345678		START		Pozycja bitu 12345678
0_____	NIE	Czy różnica: liczba przeliczana - 128 ≥ **0** ?	TAK	1_____
_0_____	NIE	Czy różnica: liczba przeniesiona - 64 ≥ **0**?	TAK	_1_____
__0_____	NIE	Czy różnica: liczba przeniesiona - 32 ≥ **0**?	TAK	__1_____
___0____	NIE	Czy różnica: liczba przeniesiona - 16 ≥ **0**	TAK	___1____
____0___	NIE	Czy różnica: liczba przeniesiona - 8 ≥ **0**	TAK	____1___
_____0__	NIE	Czy różnica: liczba przeniesiona - 4 ≥ **0**	TAK	_____1__
______0_	NIE	Czy różnica: liczba przeniesiona - 2 ≥ **0**	TAK	______1_
_______0	NIE	Czy różnica: liczba przeniesiona - 1 **= 0**	TAK	_______1

Przykład:

192.168.2.50

1. Czy różnica 192 – 128 ≥ 0 ?

192-128=64 => TAK

na pozycji najstarszego bitu należy ustawić wartość 1

128	64	32	16	8	4	2	1
1							

2. Czy różnica 64-64 ≥ 0 ?

64-64=0 => TAK

na pozycji kolejnego bitu należy ustawić wartość 1

128	64	32	16	8	4	2	1
1	1						

Pozostałe bity wypełnić należy zerami (wynik ostatniej operacji odejmowania to zero).

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Podobnie postępuje się dla kolejnych oktetów:

192.168.2.50

1. Czy różnica 168-128 ≥ 0 ?

168-128=40 => TAK

na pozycji najstarszego bitu należy ustawić wartość 1

128	64	32	16	8	4	2	1
1							

2. Czy różnica 40-64 ≥ 0 ?

40-64= - 24 => NIE

na pozycji kolejnego bitu należy ustawić wartość 0

128	64	32	16	8	4	2	1
1	0						

3. Czy różnica 40-32 ≥ 0 ?

40-32=8 => TAK

na pozycji kolejnego bitu należy ustawić wartość 1

128	64	32	16	8	4	2	1
1	0	1					

4. Czy różnica 8-16 ≥ 0 ?

8-16= - 8 => NIE

na pozycji kolejnego bitu należy ustawić wartość 0

128	64	32	16	8	4	2	1
1	0	1	0				

5. Czy różnica 8-8 ≥ 0 ?

8-16= - 8 => TAK

na pozycji kolejnego bitu należy ustawić wartość 1

128	64	32	16	8	4	2	1
1	0	1	0	1			

Pozostałe bity wypełnić należy zerami (wynik ostatniej operacji odejmowania to zero).

128	64	32	16	8	4	2	1
1	0	1	0	1	0	0	0

Podobnie wykonane obliczenia dla pozostałych dwóch oktetów dadzą wartości

192.168.2.50

128	64	32	16	8	4	2	1
0	0	0	0	0	0	1	0

192.168.2.50

128	64	32	16	8	4	2	1
0	0	1	1	0	0	1	0

Przeliczanie adresu z postaci dwójkowej na dziesiętną odbywa się zgodnie z przedstawionym przykładem: należy przedstawić adres **01011011 . 00011010 . 00100110 . 11101010**. w postaci dziesiętnej.

128	64	32	16	8	4	2	1
0	1	0	1	1	0	1	1
0 +	64 +	0+	16+	8+	0+	2+	1
= 91							

128	64	32	16	8	4	2	1
0	0	0	1	1	0	1	0
0+	0+	0+	16+	8+	0+	2+	0
= 26							

128	64	32	16	8	4	2	1
0	0	1	0	0	1	1	0
0+	0+	32+	0+	0+	4+	2+	0
= 38							

128	64	32	16	8	4	2	1
1	1	1	0	1	0	1	0
128+	64+	32+	0+	8+	0+	2+	0
234							

Adresowi w postaci binarnej 01011011 . 00011010 . 00100110 . 11101010 odpowiada adres w postaci dziesiętnej 91.26.38.234

Teoretycznie, mając do dyspozycji 32 bity, możliwe jest wygenerowanie 2^{32}=4'294'967'296 adresów IP. Adresy IP zostały jednak tak zaprojektowane, aby można było określić, która część jest związana z adresem całej sieci (N), a która z adresem poszczególnych hostów (H) w tejże sieci. Adresy IP zostały podzielone na klasy A, B, C, D i E (tab. 11):

Tab.11. Klasy adresów IPv4 – zakres i maski domyślne (binarnie i dziesiętnie oraz zapis skrócony). Zapis skrócony wskazuje, ile bitów w masce, licząc od najstarszego, ma wartość 1.

Klasa	1 oktet	2 oktet	3 oktet	4 oktet
A	**0**NNNNNNN 1-127	HHHHHHHH	HHHHHHHH	HHHHHHH
	11111111 **255**	00000000 0	00000000 0	00000000 0
/8				
B	**10**NNNNNN 128-191	NNNNNNNN	HHHHHHHH	HHHHHHHH
	11111111 255	11111111 255	00000000 0	00000000 0

/16				
C	**110**NNNNN 192-223	NNNNNNNN	NNNNNNNN	HHHHHHHH
	11111111 255	11111111 255	11111111 255	00000000 0
/24				
D	**1110**NNNN 224-239	NNNNNNNN	NNNNNNN	NNNNHHHH
	11110000 240	00000000 0	00000000 0	00000000 0
/4				
E	**11111**NNN 240-255	wyłączone z użytkowania		

Klasa A zaczyna się od 0 do 127 (najstarszy bit ma wartość **0**). Dla tej klasy adres sieci jest zdefiniowany przez 8 najstarszych bitów, natomiast pozostałe 24 bity służą do zaadresowania urządzeń w tejże sieci. W każdej sieci klasy A jest dostępnych 2^{24} =16'777'216 (zatem przeszło szesnaście milionów siedemset siedemdziesiąt siedem tysięcy) adresów hostów. Przykład takiego adresu to:

80.17.255.14

W przypadku klasy B, która zawiera się w przedziale od 128 do 191, dwa najstarsze bity będą miały odpowiednio wartość **10**. Część identyfikująca sieci to dwa pierwsze oktety. Liczba dostępnych sieci w klasie B to 2^{14} = 16'384, a ilość adresów hostów w każdej z nich przekracza sześćdziesiąt pięć tysięcy (2^{16}=65'536). Przykład takiego adresu to:

130.125.44.56

W przypadku adresu klasy C, której adresy zawierają się w przedziale od 192 do 223 trzy najstarsze bity ustawione są odpowiednio na **110.** Liczba dostępnych sieci to 2^{21}=2'097'152, a każda z nich to obszar 2^{8}=256 adresów IP. Przykład takiego adresu to:

195.17.14.33

Adresy klas A-C są używane do transmisji unicastowych, czyli pomiędzy wyłącznie dwoma hostami w sieci (one-to-one communication). Stosowane są również do komunikacji rozgłoszeniowej – broadcastowej (one-to-everyone communication).

W przypadku adresu klasy D, o przedziale adresowym od 224 do 239, najstarsze bity mają wartości **1110**. Adresy klasy D używane są do transmisji grupowej (multicast – one-to-many communication), czyli skierowanej do większej ilości hostów (np. wideokonferencja). Zastosowanie tej klasy adresów zostało dokładnie omówione m.in. w RFC-1020 i -1060.

Dla adresów klasy E najstarsze bity pierwszego oktetu przyjmują wartość binarną **1111.** Adresy te są zarezerwowane do celów testowych i nie wolno ich używać do adresowania hostów.

Nie wszystkie adresy IP mogą być używane w Internecie. IANA (Internet Assigned Numbers Authority www.iana.org) jest odpowiedzialna za przydział adresów IP dla potrzeb komercyjnych i doświadczalnych. Dla Europy adresy IP są przydzielane przez organizację Resaux IP Europeens – www.ripe.net. Na stronach tej organizacji znajdują się wyszukiwarki ***whois***, które umożliwiają zdobycie informacji o właścicielu adresu IP.

Adresy można podzielić na ogólne (publiczne) i do zastosowań specjalnych, w tym prywatne.

Adresy ogólne są stosowane do adresowania hostów w Internecie.

Adresy prywatne, nieroutowalne w sieci internetowej, są używane tylko w ramach sieci lokalnej. Administrator sieci lokalnej może używać tych adresów bez konieczności ich uzyskania od w/w organizacji. Na ten cel zostały zarezerwowane następujące adresy (tab. 12):

Tab. 12. Prywatne adresy IP

Klasa	Zakres adresów	Maska domyślna
A	10.0.0.0-10.255.255.255	255.0.0.0 (/8)
B	172.16.0.0-172.31.255.255	255.240.0.0 (/12)
C	192.168.0.0-192.168.255.255	255.255.255.0 (/16)

Adresy te mają głównie zastosowanie do adresowania hostów w Intranecie. Sieć intranetowa używa m.in. operacji NAT (Network Address Translation, RFC 1631) do komunikacji z Internetem (mapowanie adresów prywatnych na adresy publiczne). Zastosowanie tej techniki pozwala zaoszczędzić adresy publiczne i dodatkowo wpływa na bezpieczeństwo sieci intranetowych.

Najważniejsze adresy do zastosowań specjalnych zostały zestawione w tabeli 13:

Tab. 13. Przykłady adresów specjalnych

Adres	Funkcja	Zastosowanie
0.0.0.0	Adres domyślnej trasy	Użycie w tablicach routingu
127.0.0.1	Adres pierwszej pętli zwrotnej	Komunikacja sieciowa hosta ze sobą samym
255.255.255.255	Adres rozgłoszeniowy w lokalnej sieci	Komunikacja hosta ze wszystkimi hostami (one-to-everyone transmission) w ramach jednej fizycznej sieci. Ten adres nie może być trasowany

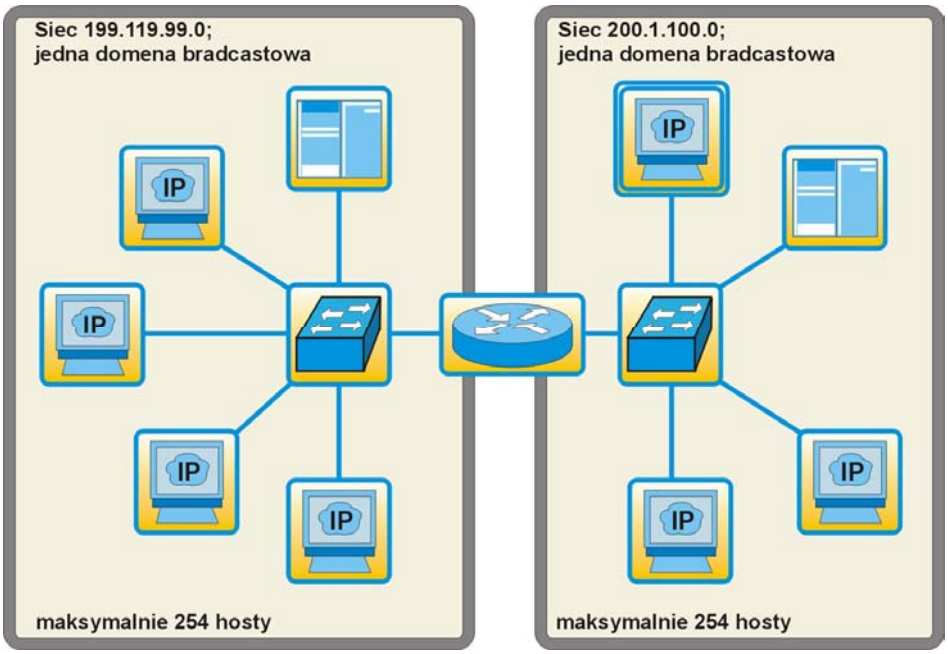
Adresów prywatnych i specjalnych nie wolno używać w ruchu zewnętrznym, poza siecią lokalną (Intranetem).

Czy aktualnie jest możliwość uzyskania pełnej klasy adresów A lub B? Odpowiedź brzmi NIE. Uzyskanie pełnej puli adresów klasy C jest w tej chwili bardzo trudne. Kiedy otrzymuje się pulę adresów klasy C (256 adresów) to do zaadresowania hostów pozostają 254 adresy. Każda bowiem sieć musi mieć swój adres sieci i adres rozgłoszeniowy (broadcastowy). Te dwa adresy nie mogą być użyte do zaadresowania hostów, np. dla sieci klasy C 199.119.99.x (tab. 14, rys.10):

Tab. 14. Zakres adresów klasy C

Adres sieci	199.119.99.0
Zakres adresów hostów	199.119.99.1-199.119.99.254
Adres rozgłoszeniowy sieci	199.119.99.255

Adres broadcastowy 199.119.99.255 będzie użyty wtedy, kiedy host w sieci 199.119.99.x będzie chciał nadać komunikat do wszystkich hostów do niej należących (wspólna domena rozgłoszeniowa). Komunikat broadcastowy nie zostanie przekazany do sieci 200.1.100.0.



Rys. 10. Dwie domeny broadcastowe rozdzielone routerem.
Każda domena wykorzystuje całą klasę adresów IP

Adres sieci będzie użyty w tablicach routingu jest niezbędny do wyznaczania tras pakietów pomiędzy sieciami. Przykładowa tablica routingu routera CISCO obsługującego złożoną sieć (protokół routingu: RIP) przedstawiona jest poniżej.

R4#***sh ip route***

Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B – BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * – candidate default
U – per-user static route, o – ODR

Gateway of last resort is not set

[1] R 192.168.200.0/24 [120/3] via 192.168.6.1, 00:00:12, Serial0
[2] R 192.168.201.0/24 [120/3] via 192.168.6.1, 00:00:12, Serial0
[3] C 192.168.8.0/24 is directly connected, Ethernet0
[4] R 192.168.4.0/24 [120/4] via 192.168.6.1, 00:00:13, Serial0
[5] C 192.168.6.0/24 is directly connected, Serial0
[6] R 192.168.7.0/24 [120/1] via 192.168.6.1, 00:00:13, Serial0
[7] R 192.168.1.0/24 [120/1] via 192.168.6.1, 00:00:13, Serial0
[8] R 192.168.2.0/24 [120/3] via 192.168.6.1, 00:00:13, Serial0
[9] R 192.168.3.0/24 [120/3] via 192.168.6.1, 00:00:13, Serial0

R4#

W linii [1] zdefiniowana jest trasa do sieci 192.168.200.0 poprzez interfejs routera o adresie 192.168.6.1. Linie [2], [4], [6]-[9] definiują trasę do kolejnych sieci. Linie [3] i [5] definiują sieci bezpośrednio przyłączone do routera.

Okazało się, że podział adresów na klasy spowodował bardzo szybkie wyczerpanie ze względu na ich nieefektywne wykorzystanie. Kiedy przedsiębiorstwo potrzebuje 257 adresów IP, jedna pełna klasa C nie wystarcza, trzeba użyć obszaru adresów dwóch klas C lub jednego obszaru klasy B (strata ponad 65 tysięcy adresów IP). Rozwiązaniem problemu okazało się wprowadzenie nowego systemu adresowania, w którym całą pulę adresów danej klasy dzieli się na podsieci. W systemie klasowym

routery rozpoznawały adres sieci po najstarszych bitach najstarszego oktetu adresu.

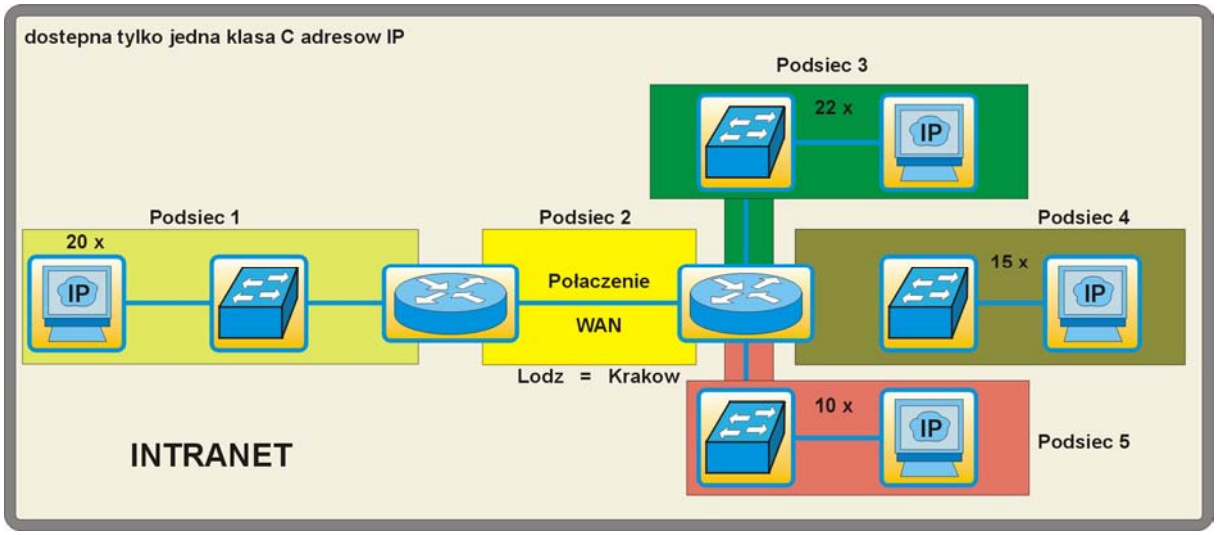
Można sobie wyobrazić sytuację, kiedy istnieje konieczność podziału sieci na segmenty (np. podzielenie sieci na segment administracyjny i studencki). Co zrobić, kiedy dostaje się pulę adresów klasy C, a trzeba rozdzielić sieć na kilka obszarów? Taką pulę trzeba podzielić na podsieci. Dokonuje się tej operacji, wykorzystując tę część adresu, dla której domyślna maska sieci ma wartość 0 (obszar adresu hosta). Z adresów hostów „pożycza" się wymaganą ilość bitów (tzw. bitów podsieci – S), która określi ilość utworzonych podsieci. „Pożyczanie" polega na ustawieniu wartości 1 w masce sieci wyłącznie w obszarze adresu hosta, wtedy:

Adres IP = ADRES_SIECI ADRES_PODSIECI ADRES_HOSTA

Proces podziału sieci na podsieci zobrazowany jest w przykładzie 1.

Przykład 1:

Pewne przedsiębiorstwo dostało adres 199.119.99.0 z maską 255.255.255.0 (199.119.99.0/24) Administrator musi podzielić sieć na pięć podsieci zgodnie ze schematem przedstawionym na rys. 11 (każda podsieć zaznaczona innym kolorem).



Rys. 11. Pięciosegmentowa sieć z zaznaczoną wymaganą ilością hostów w każdym segmencie (podsieci).

Wyznaczyć adresy podsieci, adresy rozgłoszeniowe i adresy hostów w każdej podsieci. Jaka maksymalna liczba hostów będzie mogła pracować w każdej podsieci?

1. W pierwszej kolejności należy wyznaczyć maskę podsieci

   Należy określić klasę otrzymanego adresu. W przykładzie adres jest klasy C, więc jego struktura ma postać

   NNNNNNN.NNNNNNNN.NNNNNNN.HHHHHHHH

   (maska domyślna: 255.255.255.0 lub /24).

   Nie można wykorzystać adresu sieci do operacji wydzielenia podsieci (domyślna maska), dostępne są więc TYLKO bity w czwartym oktecie adresu (8 bitów).

   Ile bitów "S" (- s ang. subnet–podsieć) z obszaru HHHHHHHH powinno się pożyczyć, by utworzyć wystarczającą **L**iczbę **E**fektywnych **P**od**s**ieci (LEPS)?

UWAGA: Kiedy dokonuje się podziału sieci na podsieci trzeba pamiętać, że adresy hostów pierwszej (adres całej sieci) i ostatniej podsieci (adres broadcastowy całej sieci) nie powinny być wykorzystywane do adresowania urządzeń sieciowych (RFC890). Stąd pojęcie „efektywnych podsieci" i „całkowita liczba podsieci". Niektóre routery umożliwiają wykorzystanie tych zakresów adresów. Routery CISCO wymagają w tym celu podania polecenia ***ip subnet-zero*** w procesie ich konfiguracji Choć dokument RFC1812 zezwala na użycie przestrzeni adresowej pierwszej i ostatniej podsieci, to nie ma gwarancji, że wszystkie hosty i routery będą w stanie je obsługiwać.

Chcąc odpowiedzieć na powyższe pytanie, trzeba rozwiązać nierówność względem S.

$$2^S - 2 >= LEPS$$

gdzie:
LEPS – liczba efektywnych podsieci,
S – liczba bitów pobranych z obszaru hostów maski.

Jednocześnie trzeba policzyć **C**ałkowitą **L**iczbę **P**odsieci (CLP) zgodnie z równaniem:

$$CLP=2^S$$

Jeśli pożyczone zostaną dwa bity: SSHHHHHH, to będzie można stworzyć 4 podsieci (CLP) o adresach:

00, 01, 10, 11

Tylko podsieci 01 i 10 będą mogły być wykorzystanie, a więc nie spełni to warunków zadania.

Jeśli pożyczyć 3 bity: SSSHHHHH, to można stworzyć ELPS = 2^3-2=6 efektywnych podsieci (całkowita ilość podsieci CLP=2^3=8).

Tak wyznaczona maska podsieci przyjmie postać:

11111111.11111111.11111111.11100000

co po zamianie na system dziesiętny odpowiada wartości 255.255.255.224 (/27)

Tak skonstruowana maska spełni warunki zadania (potrzebnych jest 5 efektywnych podsieci).

2. Kolejnym etapem jest określenie zakresu adresów podsieci i zakresu adresów hostów.

   Skoro z czwartego oktetu adresu pożyczone zostały 3 bity na zaadresowanie podsieci, to pozostałe 5 bitów (SSSHHHHH) wykorzystane zostanie na obliczenie zakresu adresów poszczególnych podsieci.

   $$Z=2^H=2^5=32$$

   Ponieważ każda podsieć musi mieć swój adres podsieci i adres rozgłoszeniowy, to na zaadresowanie hostów pozostanie:

   $$EAH=2^H-2=2^5-2=30$$

   Efektywnych adresów hostów – EAH

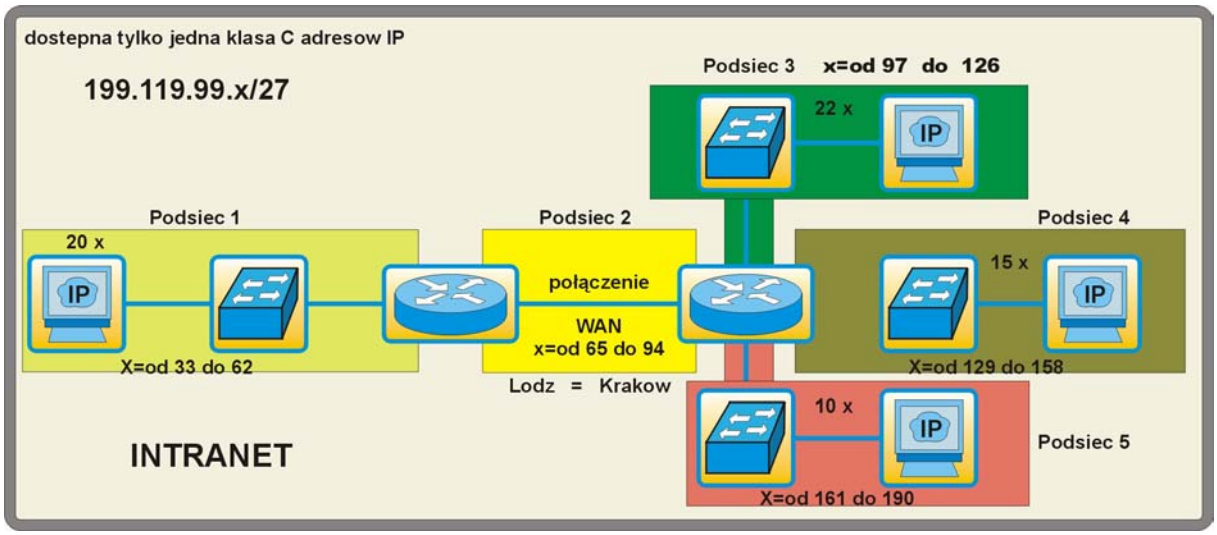
3. Zestawiając wyniki można stwierdzić, że maska 255.255.255.224 (/27) podzieli sieć na 8 podsieci (6 efektywnych). Każda podsieć będzie miała zakres 32 adresów, z czego dla hostów przewidzianych jest 30 adresów:

Tab. 15. Podział sieci klasy C na 8 podsieci (6 efektywnych podsieci)

L.P	Adres podsieci	Adresy hostów (30)	Adres rozgłoszeniowy	Uwagi
Związana z CLP	Związany z wyznaczonym zakresem Z. Pierwszy adres zakresu	Związane z EAH. Adresy pomiędzy pierwszym i ostatnim adresem zakresu Z	Związany z wyznaczonym zakresem Z. Ostatni adres zakresu	
1	199.119.99.0	199.119.99.1 – 199.119.99.30	199.119.99.31	adres całej sieci
2	199.119.99.32	199.119.99.33 – 199.119.99.62	199.119.99.63	do wykorzystania
3	199.119.99.64	199.119.99.65 – 199.119.99.94	199.119.99.95	do wykorzystania
4	199.119.99.96	199.119.99.97 – 199.119.99.126	199.119.99.127	do wykorzystania
5	199.119.99.128	199.119.99.129 – 199.119.99.158	199.119.99.159	do wykorzystania
6	199.119.99.160	199.119.99.161 – 199.119.99.190	199.119.99.191	do wykorzystania
7	199.119.99.192	199.119.99.193 – 199.119.99.222	199.119.99.223	do wykorzystania później
8	199.119.99.224	199.119.99.225 – 199.119.99.254	199.119.99.255	adres rozgłoszeniowy całej sieci

Zakres 1 (adres całej sieci) i 8 (adres rozgłoszeniowy całej sieci) nie są do wykorzystania. Zakres 7 do wykorzystania w późniejszym czasie. Maksymalna liczba hostów dla każdej podsieci: 30 (efektywne adresy IP w każdej podsieci, EAH).

Rozdział adresów IP został przedstawiony na rysunku 12.



Rys. 12. Rozkład adresów IP w pięciosegmentowej sieci klasy C.

Jak widać, istnieje pokaźna ilość adresów, które nie mogą być wykorzystane do adresowania hostów. Przy podziale sieci na 8 podsieci dla hostów dostępnych jest tylko 6*30=180 adresów IP z puli 254. Dodatkowo traci się znaczną ilość adresów na połączeniach punkt-punkt pomiędzy routerami (potrzebne są tylko dwa adresy IP, a pula ma ich 30).

Kiedy dzieli się sieci na podsieci istnieje czasami konieczność oznaczenia, w której podsieci pracuje urządzenie, któremu nadano już adres IP (przykład 2). Bardzo często okazuje się, że administrator pomylił się i urządzenie ma przyznany nieprawidłowy adres IP (adres podsieci, adres broadcastowy podsieci lub adres z całego pierwszego i ostatniego zakresu adresów podsieci).

Przykład 2

W pewnym przedsiębiorstwie drukarce przydzielono adres 192.168.5.125 /29. Obliczyć, do której podsieci należy drukarka. Podać adres podsieci, zakres adresów hostów podsieci oraz adres rozgłoszeniowy podsieci. Czy adres jest prawidłowy?

1. W pierwszej kolejności trzeba zapisać adres hosta i adres maski w postaci binarnej

H: 11000000.10101000.00000101.01111101

S: 11111111.11111111.11111111.11111000 (29 jedynek)

2. Aby wyznaczyć adres podsieci, do której należy drukarka, należy dokonać operacji logicznego iloczynu (AND) adresu hosta i maski

Tab. 16. Operacja logicznego iloczynu – sposób liczenia

H	0	1	0	1
S	0	0	1	1
Wynik operacji AND	0	0	0	1

```
   11011110.11101101.00000101.01111101
   11111111.11111111.11111111.11111000
AND_____________________ _____________
   11011110.11101101.00000101.01111000
```

Obliczony w ten sposób adres podsieci należy zamienić na postać dziesiętną: 192.168.5.120.

Skoro 192.168.5.120 jest adresem klasy C, to maska /29 oznacza, że pożyczonych zostało 5 bitów (trzy pierwsze oktety – 24 bity są domyślną maska podsieci klasy C) na zaadresowanie podsieci. Do zaadresowania hostów pozostały 3 bity, więc w podsieci może być nie więcej niż EAH=2^3-2= 6 hostów (SSSSSHHH).

Aby łatwo policzyć adres rozgłoszeniowy tej podsieci należy wykonać operację logiczną NOT na masce, a następnie na uzyskanej wartości operację OR z adresem podsieci.

S	0	1
Wynik operacji NOT	1	0

H	0	1	0	1
S	0	0	1	1
Wynik operacji OR	0	1	1	1

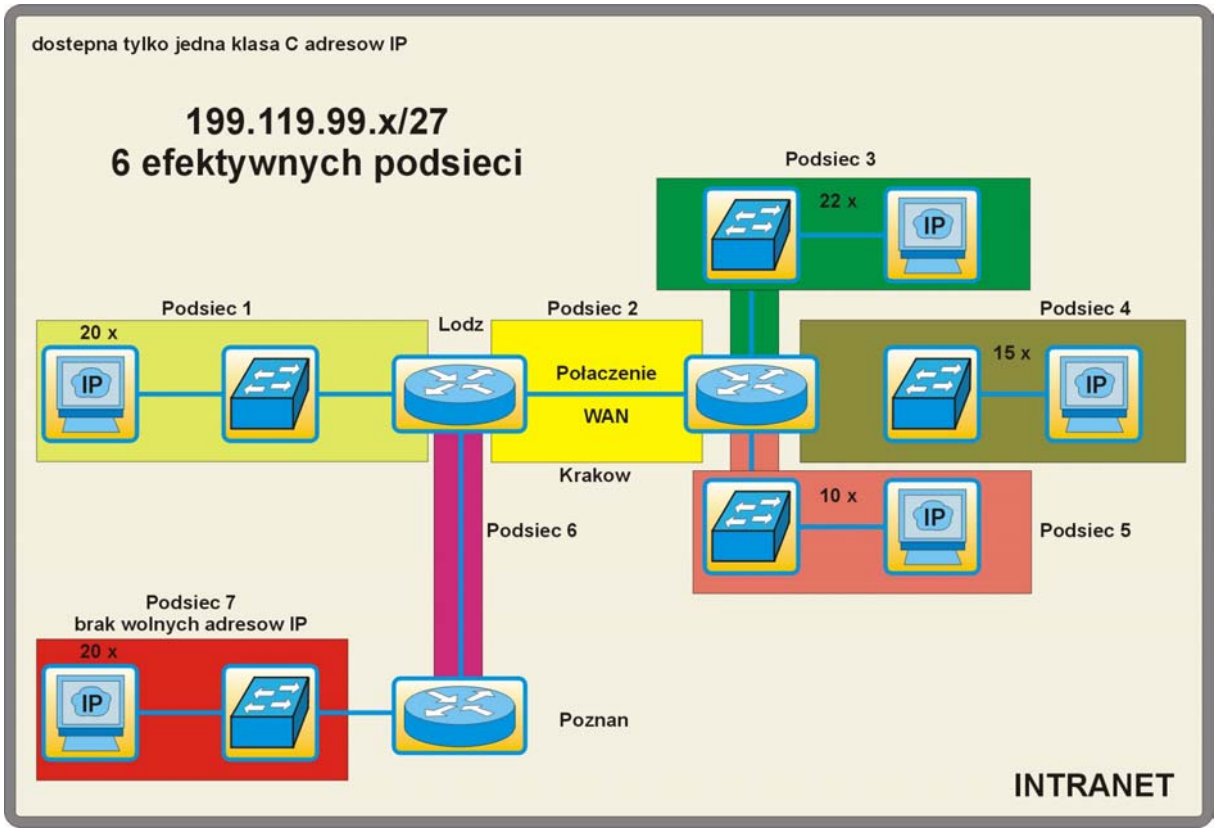
```
   11011110.11101101.00000101.01111000
   00000000.00000000.00000000.00000111
OR _____________________________________
   11011110.11101101.00000101.01111111
```

Zestawiając informacje można zapisać:

Adres IP drukarki: 192.168.5.125
Maska podsieci: 255.255.255.248
Adres podsieci: 192.168.5.120
Adres rozgłoszeniowy: 192.168.5.127 (liczone z zakresu $Z=2^3=8$)
Zakres adresów hostów podsieci: 192.168.5.121-192.168.5.126
Adres prawidłowy (mieści się w zakresie adresów hostów i nie należy ani do pierwszej, ani do ostatniej podsieci).

6. VLSM (Variable-Length Subnet Masks) – podsieci o zmiennej długości

Można sobie wyobrazić sytuację, kiedy sieć ulega rozwojowi i konieczne jest dołączenie kolejnego segmentu sieci, tak jak na rysunku 13.



Rys. 13. Schemat rozbudowy przykładowej sieci.

Korzystając z tabeli 17, okaże się, że brakuje adresów IP dla hostów podsieci 7. Widać również, że połączenia pomiędzy routerami Lodz i Krakow oraz Lodz i Poznan wykorzystują tylko po dwa adresy IP – traci się 56 adresów IP z podsieci 2 i 6.

Gdyby podzielić podsieć na pod-podsieci, może się okazać, że zaoszczędzone zostaną kolejne adresy IP.

Wybierając zakres 3 (tab. 17) dostępne są następujące adresy IP:

Tab. 17.

Numer podsieci	Adres podsieci	Zakres adresów hostów	Adres broadcastowy podsieci
3	199.119.99.64	199.119.99.65 – 199.119.99.94	199.119.99.95

Kiedy przyjrzeć się masce sieci z przykładu 1:

255.255.255.224 (/27)
11111111.11111111.11111111.11100000

okazuje się, że dostępnych jest 5 bitów (zera w masce), które mogą być użyte do kolejnego podziału podsieci. Jeżeli „pożyczyć" 3 bity, to można będzie utworzyć 2^3=8 pod-podsieci. Każda pod-podsieć będzie obejmowała cztery adresy (2^2), z czego dwa będą mogły być wykorzystane do adresowania połączeń miedzy routerami (punkt-punkt).

Dla podsieci 3 maska ulegnie więc zmianie: 11111111.11111111.11111111.11111100 (/30)

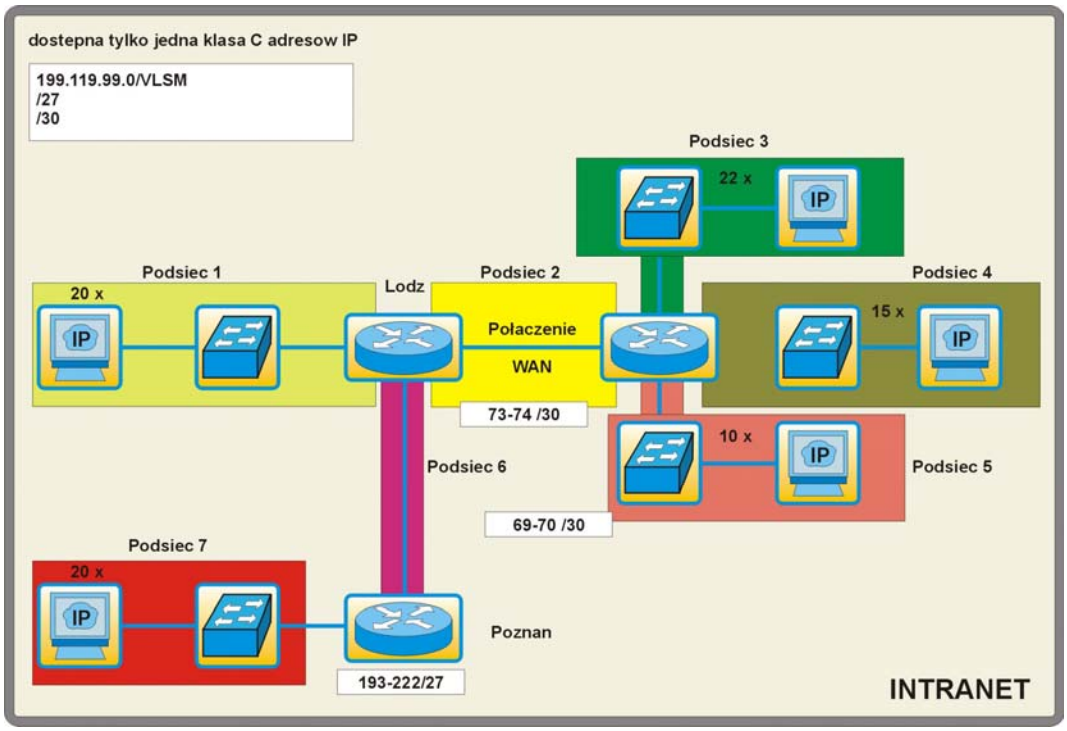
Wyniki takiego podziału podsieci 3 przedstawione są w tabeli 18 (dla ułatwienia ominięte zostały pierwsze trzy, niezmienne oktety adresu: 199.119.99.x).

Tab. 18. Pod-podsieci zakresu 199.119.99.64 – 199.119.99.95

Numer pod-podsieci	Adres pod-podsieci	Dostępne adresy hostów	Adres broadcastowy pod-podsieci	Zastosowanie
3a	64	65, 66	67	Adres całej podsieci
3b	68	69, 70	71	połączenie punkt-punkt podsieci 2
3c	72	73, 74	75	połączenie punkt-punkt podsieci 3
3d	76	77, 78	79	Wolne
3e	80	81, 82	83	Wolne
3f	84	85, 86	87	Wolne
3g	88	89, 90	91	Wolne
3h	92	93, 94	95	Adres rozgłoszeniowy całej podsieci

Używając techniki VLSM, można więc podzielić sieć na podsieci o zmiennej długości. Są to podsieci, które nie zawierają jednakowej ilości hostów.

Schemat sieci po rozbudowie przedstawiono na rysunku 14:



Rys. 14. Przydział adresów IP / VLSM dla siedmiu podsieci

7. CIDR (Classless InterDomain Routing)

CIDR – bezklasowy routing międzydomenowy – jest kolejną techniką stosowaną w celu lepszego zarządzania adresami IP. W CIDR adres sieci jest oznaczany poprzez maskę sieci. Adres sieci to ta część adresu IP, dla której maska sieci ma ustawione bity na 1. Adres hosta to ten obszar adresu IP, dla którego maska sieci ma ustawione bity na 0. CIDR umożliwia trasowanie pakietów w zagregowanych (połączonych) kilku kolejnych sieciach. Przykładowo, kilka kolejnych sieci, np. klasy C, może zostać połączonych są w jedną, bezklasową przestrzeń adresową. Taka przestrzeń nazwana jest supersiecią. W przestrzeni takiej nie obowiązuje podział na klasy adresów (classless).

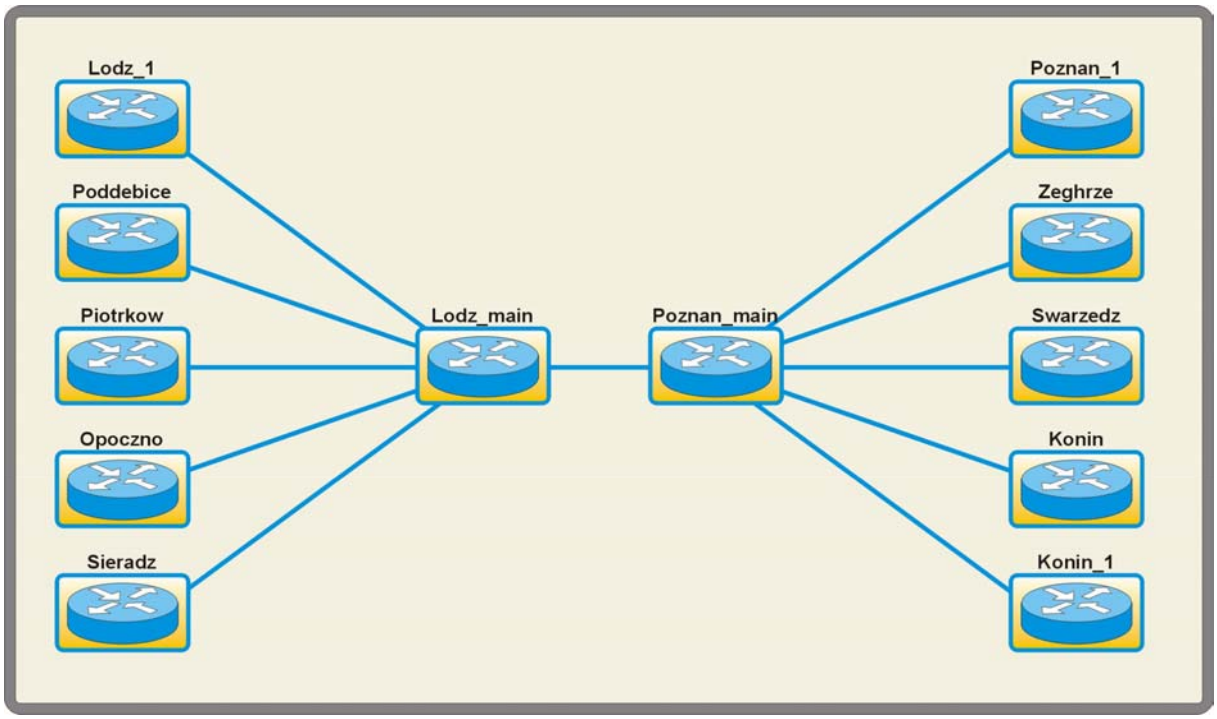
Jeśli przedsiębiorstwo potrzebuje 1000 adresów, to należy wyznaczyć liczbę bitów, która umożliwia zaadresowanie 1000 hostów (2^{10}=1024). Dziesięć bitów będzie więc używane w części przeznaczonej na adresowanie hostów, a 22 określać będą adres sieci.

11111111.11111111.11111100.00000000

Zakładając, że adresem początkowym zakresu jest 193.13.12.0 z maską /22 (255.255.252.0) można wyznaczyć adres końcowy zakresu (broadcast): 193.13.15.255 (razem 1024 adresów). Adresy dostępne dla hostów to zakres od 193.13.13.1 do 193.13.16.254.

Dzięki CIDR oraz VLSM możliwa jest tez agregacja tras. Ma to na celu zmniejszenie ilości wpisów w tablicach routingu routerów.

Na rysunku 15 przestawiony jest schemat sieci, gdzie pomiędzy routerami Lodz_main i Poznan_main następuje koncentracja ruchu, a tablice routingu są rozbudowane.



Rysunek 15. Schemat sieci

Adresy IP sieci obsługiwanych przez poszczególne routery przedstawione są w tabeli 19:

Tab. 19

Lodz_1	192.168.1.0 /24	Poznan_1	10.1.0.0 /16
Poddebice	192.168.2.0 /24	Zegrze	10.5.0.0 /16
Piotrkow	192.168.3.0 /24	Swarzedz	10.77.0.0 /16
Opoczno	192.168.4.0 /24	Konin	10.80.0.0 /16
Sieradz	192.168.5.0 /24	Konin_1	10.125.0.0 /16

Każda sieć i podsieć wymaga odpowiedniego wpisu do tablicy routingu routerów Lodz_main i Poznan_main. W omawianym przykładzie spowoduje to wygenerowanie dużej ilości takich wpisów w tych routerach. Zamiast pięciu wpisów, można zredukować ich liczbę do jednego.

W tym celu trzeba wyznaczyć trasę sumaryczną (część wspólną adresów). Dokonuje się tego, używając postaci binarnej adresów. W obszarze, gdzie adres nie ulega zmianie, ustawia się bity maski na 1. Dla lewej gałęzi sieci:

	Pierwszy oktet	**Drugi oktet**	**Trzeci oktet**	**Czwarty oktet**
192.168.1.0 /24	11000000	10101000	00000001	00000000
192.168.2.0 /24	11000000	10101000	00000010	00000000
192.168.3.0 /24	11000000	10101000	00000011	00000000
192.168.4.0 /24	11000000	10101000	00000100	00000000
192.168.5.0 /24	11000000	10101000	00000101	00000000
Trasa sumaryczna i maska	11000000 11111111 255	10101000 11111111 255	00000000 11111000 248	00000000 00000000 0
	192.168.0.0 /21			

Tak zagregowana trasa obejmować będzie adresy sieci od 192.168.0.0 do 192.168.7.0.

Dla prawej gałęzi sieci:

	Pierwszy oktet	**Drugi oktet**	**Trzeci oktet**	**Czwarty oktet**
10.1.0.0 /16	00001010	00000001	00000001	00000000
10.5.0.0 /16	00001010	00000101	00000010	00000000
10.77.0.0 /16	00001010	01001101	00000011	00000000
10.80.0.0 /16	00001010	01010000	00000100	00000000
10.125.0.0 /16	00001010	01111101	00000101	00000000
Trasa sumaryczna i maska	00001010 11111111 255	00000000 10000000 128	00000000 00000000 0	00000000 00000000 0
	10.0.0.0 /9			

Trasa sumaryczna obejmować będzie sieci od 10.0.0.0 do 10.127.0.0.

Opracowano wiele kalkulatorów, które ułatwiają przeliczanie adresów IP. Freeware'owe kalkulatory mogą być pobrane ze np. stron Famatechu (www.radmin.com) oraz www.solarwinds.net.

Podsumowanie

Stosowanie odpowiednich technik administrowania adresami IP spowodowało, że groźba wyczerpania się adresów IPv4 oddaliła się. Techniki te w pewien sposób zatrzymały rozwój i implementację protokołu IPv6. W chwili obecnej (2004) adresowanie hostów za pomocą adresów tzw. nowej generacji (IPv6) ma zastosowanie, ale raczej do celów testowych.