informatyka+

Algorytmika i programowanie

Bazy danych

Multimedia, grafika i technologie internetowe

Sieci komputerowe

Tendencje w rozwoju informatyki i jej zastosowań

Człowiek – najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

informatyka+

Wszechnica Informatyczna: Sieci komputerowe

Komunikacja w sieciach komputerowych

Dariusz Chaładyniak, Józef Wacnik

Człowiek – najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Komunikacja w sieciach komputerowych

Rodzaj zajęć: Wszechnica Informatyczna
Tytuł: Komunikacja w sieciach komputerowych
Autorzy: dr inż. Dariusz Chaładyniak, mgr inż. Józef Wacnik

Redaktor merytoryczny: prof. dr hab. Maciej M Sysło

Zeszyt dydaktyczny opracowany w ramach projektu edukacyjnego **Informatyka+** — ponadregionalny program rozwijania kompetencji uczniów szkół ponadgimnazjalnych w zakresie technologii informacyjno-komunikacyjnych (ICT).
www.informatykaplus.edu.pl
kontakt@informatykaplus.edu.pl

Wydawca: Warszawska Wyższa Szkoła Informatyki
ul. Lewartowskiego 17, 00-169 Warszawa
www.wwsi.edu.pl
rektorat@wwsi.edu.pl

Projekt graficzny: FRYCZ I WICHA

Warszawa 2010

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Komunikacja w sieciach komputerowych

Dariusz Chaładyniak
Warszawska Wyższa Szkoła Informatyki
dchalad@wwsi.edu.pl

Józef Wacnik
Warszawska Wyższa Szkoła Informatyki
j_wacnik@poczta.wwsi.edu.pl

Streszczenie

W wykładzie są przedstawione podstawowe informacje związane z adresowaniem komputerów w sieciach. Wyjaśnia na czym polega adresowanie fizyczne, a na czym adresowanie logiczne. Prezentuje podstawowe rodzaje transmisji sieciowej (unicast, multicast, broadcast). Wyjaśnia budowę i przeznaczenie protokołów IPv4 oraz IPv6. Omawia adresowanie klasowe (klasy A, B, C, D i E) oraz adresowanie bezklasowe (z wykorzystaniem masek podsieci) z praktyczną interpretacją podziału sieci na podsieci. Omawiane są ponadto trzy wybrane usługi sieciowe, których zrozumienie opiera się na znajomości adresowania IP. Aby móc skorzystać z dowolnych zasobów WWW, musimy mieć publiczny adres IP, który może być współdzielony przez wiele komputerów z zastosowaniem translacji NAT (statycznej lub dynamicznej) lub translacji z przeciążeniem PAT. Adres IP dla naszego komputera może być przypisany ręcznie lub przydzielony dynamicznie poprzez usługę DHCP. Aby przeglądarka internetowa właściwe zinterpretowała adres domenowy, musi być dostępna usługa odwzorowująca ten adres na adres IP zrozumiały dla oprogramowania sieciowego.

Warsztaty są okazją do praktycznego przećwiczenia materiału z wykładu.

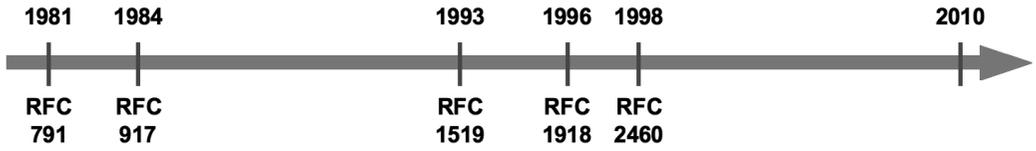
Spis treści

Wykład

Warsztaty

1 WSTĘP DO ADRESOWANIA IP

Rys historyczny



Rysunek 1.
Wybrane fakty związane z adresowaniem IP

W roku 1981 dokumentem RFC nr 791 zdefiniowano ostatecznie protokół IPv4 jako 32-bitową liczbę binarną, zapisywaną w notacji kropkowo-dziesiętnej.

W roku 1984 w dokumencie RFC 917 określono pojęcie adresowania bezklasowego przy użyciu masek podsieci.

W roku 1993 dokumentem RFC 1519 zdefiniowano metodę CIDR (ang. *Classless Inter-Domain Routing*), która upraszcza zapis masek podsieci.

W dokumencie RFC 1918 z 1996 roku zdefiniowano dla każdej z klas (A, B, C) pulę adresów prywatnych. Adresy te mogą być stosowane wewnętrznie (bez możliwości routowania) a dzięki translacji NAT i PAT umożliwiają „wyjście" do Internetu.

W roku 1998 zdefiniowano ostatecznie nowy protokół adresowania hostów w Internecie IPv6 jako 128-bitową liczbę binarną, zapisaną w notacji dwukropkowo-szesnastkowej.

Od roku 1998 następuje sukcesywna implementacja protokołu IPv6.

Organizacje związanie z adresowaniem IP

IETF (ang. *The Internet Engineering Task Force*) – organizacja odpowiedzialna za opracowywanie kolejnych wersji protokołu IP.

IANA (ang. *Internet Assigned Numbers Authority*) – organizacja przydzielająca adresy IP w skali światowej (przejęła obowiązki od **InterNIC** (ang. *Internet Network Information Center*). Założycielem IANA i twórcą systemu numeracji i nazewnictwa adresów internetowych był Jon Postel.

ICANN (ang. *The Internet Corporation for Assigned Names and Numbers*) – instytucja powołana do życia 18 września 1998 roku w celu przejęcia od rządu USA funkcji nadzorowania technicznych aspektów Internetu (przejęcia obowiązków od IANA). Formalnie ICANN jest prywatną organizacją typu non-profit, o statusie firmy zarejestrowanej w stanie Kalifornia, której rząd USA przekazał czasowo prawo nadzoru nad systemem DNS, przydziałem puli adresów IPv4 oraz IPv6 dla tzw. Regional Internet Registries (RIR) oraz rejestracją numerów portów.

Na czym polega adresowanie fizyczne

Adresowanie fizyczne ma miejsce w drugiej warstwie modelu odniesienia ISO/OSI, czyli w warstwie łącza danych. Często adresowanie fizyczne określa się jako adresowanie sprzętowe, gdyż adres fizyczny jest „wypalonym" adresem MAC w układzie ROM (ang. *Read Only Memory*) karty sieciowej (patrz rys. 2).

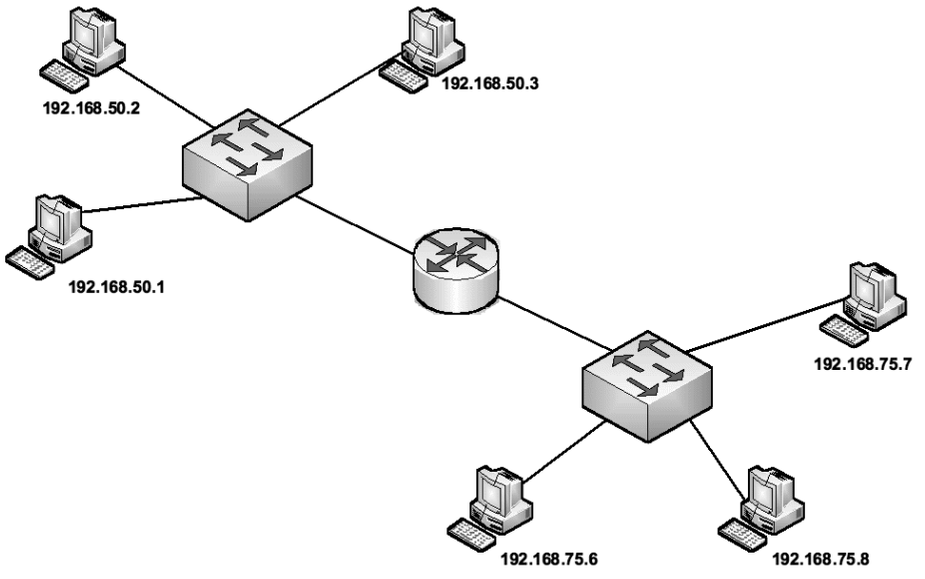
Na czym polega adresowanie logiczne

Adresowanie logiczne występuje w trzeciej warstwie modelu odniesienia ISO/OSI, czyli w warstwie sieciowej. Każdy komputer w sieci Internet ma unikatowy adres IP, którego przydział jest administrowany przez odpowiednie organizacje (IANA, ICANN).

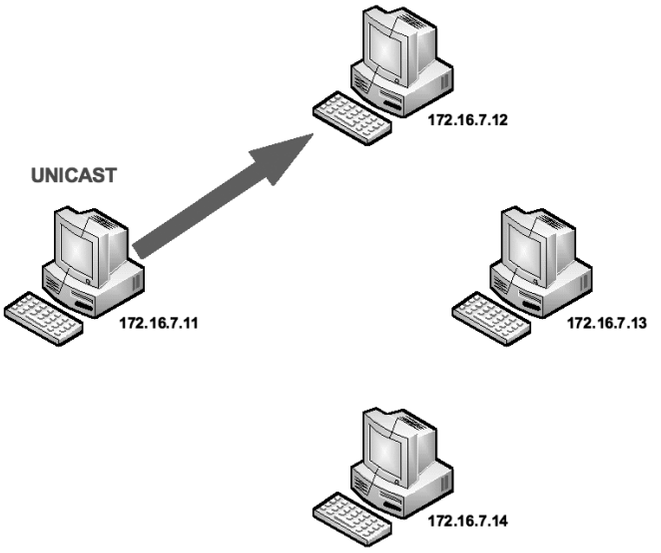
Transmisja unicast

Transmisja unicast (patrz rys. 4) to tryb transmisji, w której przekaz informacji dokonuje się wyłącznie między dwoma dokładnie określonymi komputerami w sieci.

Rysunek 2.
Karty sieciowe



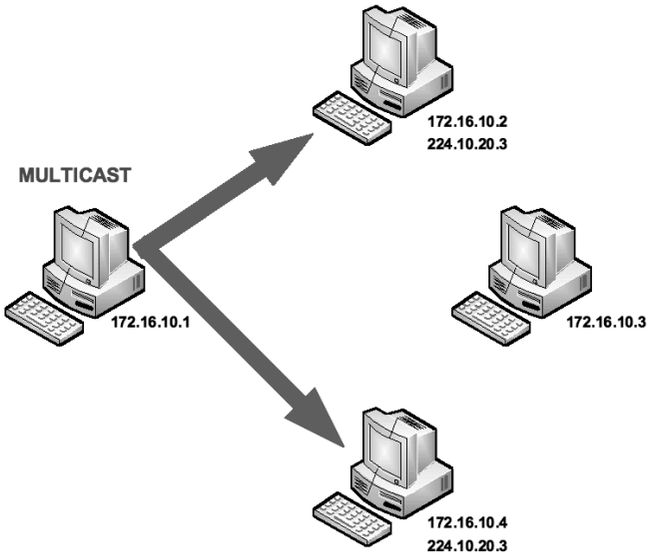
Rysunek 3.
Przykład adresowania logicznego



Rysunek 4.
Transmisja typu unicast

Transmisja multicast

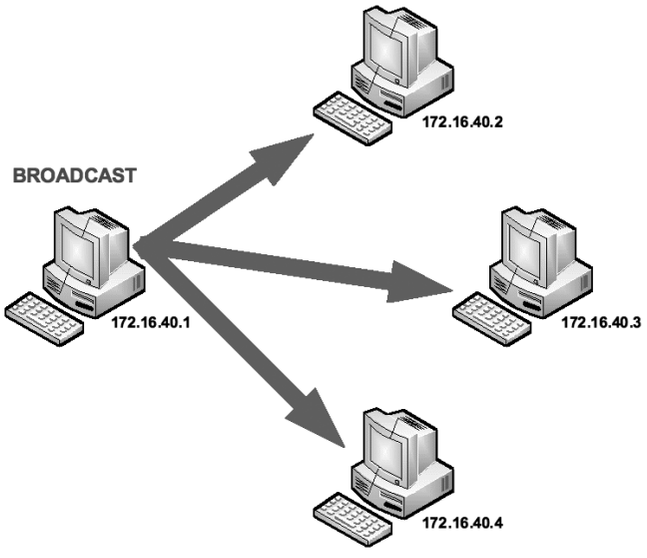
Transmisja multicast (patrz rys. 5) ma miejsce wtedy, gdy jedna stacja (router, węzeł, serwer, terminal) jednocześnie transmituje lub odbiera informacje do/z konkretnie określonej i uprzednio zdefiniowanej grupy innych stacji roboczych lub routerów.



Rysunek 5.
Transmisja typu multicast

Transmisja broadcast

Transmisja broadcast (patrz rys. 6) polega na wysyłaniu pakietów przez jeden port (kanał komunikacyjny), które powinny odbierać wszystkie pozostałe porty przyłączone do danej sieci (domeny rozgłoszeniowej). Pakiet danych, wysyłany do wszystkich stacji sieciowych domeny rozsiewczej, ma adres składający się z samych jedynek.



Rysunek 6.
Transmisja typu broadcast

2. ADRESOWANIE KLASOWE

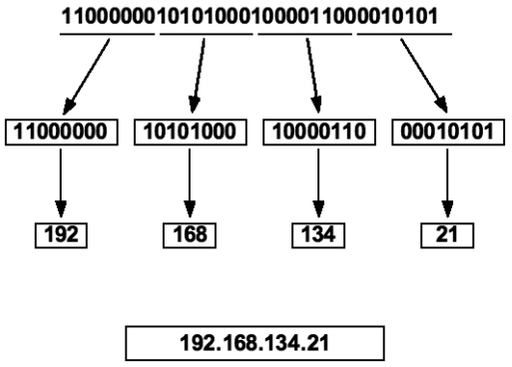
Ewolucja zapisu adresów IPv4

- 10111011011001101110001101111101
- 3144082301
- 3.144.082.301
- 187.102.227.125

Adres IPv4 to 32-bitowa liczba binarna. W początkowym etapie działania sieci komputerowych adresy IP były zapisywane binarnie. Z uwagi, że istniało niewiele hastów system ten był do zaakceptowania. Jednak w miarę zwiększania się liczby hostów w Internecie powyższy system adresowania był bardzo niewygodny. Dlatego postanowiono zapis binarny przekonwertować do systemu dziesiętnego.

Notacja kropkowo-dziesiętna

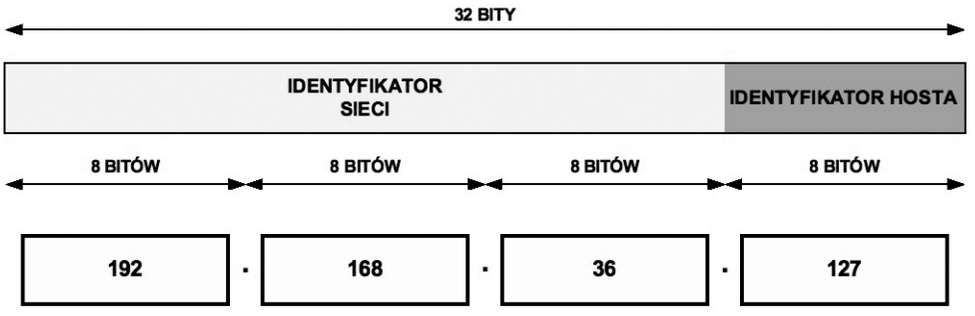
Adres IPv4 składa się z czterech oktetów liczb dwójkowych. Aby ten adres łatwiej zapamiętać, ta 32-bitowa liczba binarna jest zamieniana na cztery grupy liczb dziesiętnych oddzielonych kropkami (patrz rys. 7).



Rysunek 7.
Przykład adresu IP w wersji 4 w notacji kropkowo-dziesiętnej

Format adresu IPv4

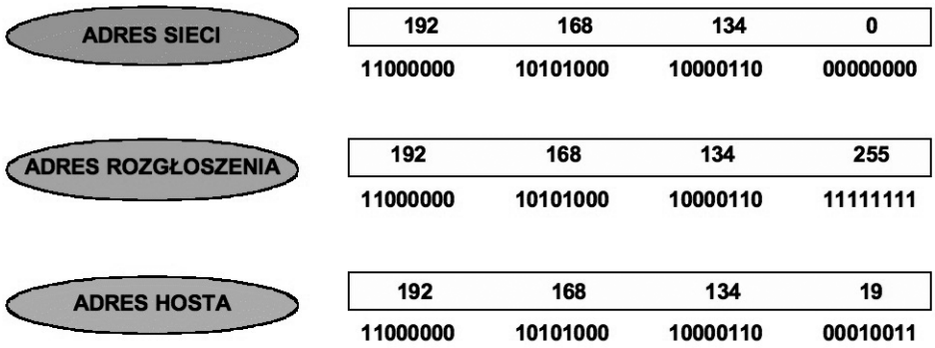
Adres IPv4 jest 32-bitową liczbą binarną konwertowaną do notacji kropkowo-dziesiętnej. Składa się z identyfikatora sieci przydzielonego przez odpowiedni RIR (ang. *Reginal Internet Registries*) oraz identyfikatora hosta (zarządzanego przez administratora sieciowego) (patrz rys. 8).



Rysunek 8.
Format adresu IP w wersji 4

Rodzaje adresów IPv4

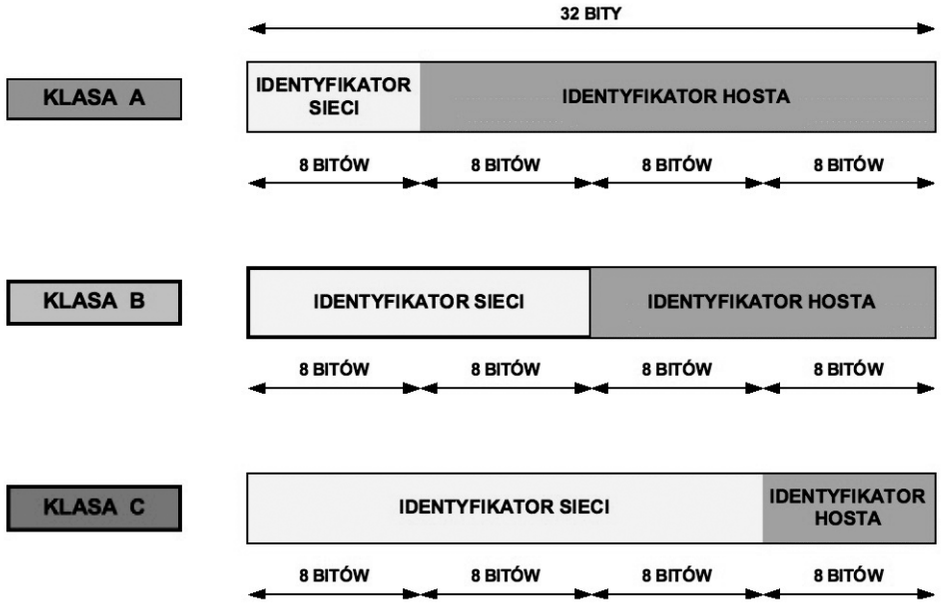
Adres sieci charakteryzuje się tym, że w części hostowej są same zera. **Adres rozgłoszenia** jest rozpoznawalny po tym, że ma same jedynki w części hostowej. **Adres hosta** jest zakresem pomiędzy adresem sieci i adresem rozgłoszenia.



Rysunek 9.
Rodzaje adresów IP w wersji 4

Klasy adresów IPv4

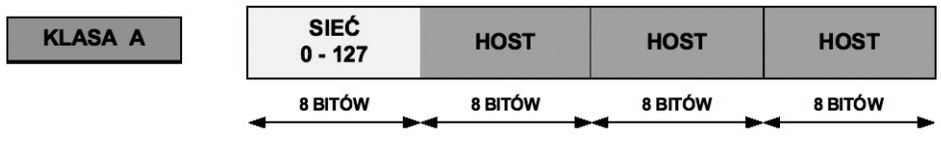
W **adresowaniu klasowym** wyróżniono pięć klas adresowych – A, B, C, D i E. Trzy pierwsze klasy (A, B, C) wykorzystuje się do adresacji hostów w sieciach komputerowych, natomiast klasy D i E są przeznaczone dla specyficznych zastosowań.



Rysunek 10.
Klasy adresów IP w wersji 4

Klasa A

klasa A – pierwszy bit adresu jest równy 0, a następne 7 bitów określa sieć. Kolejne 24 bity wskazują komputer w tych sieciach. Adres rozpoczyna się liczbą między 1 i 127. Można zaadresować 126 sieci (adres 127.x.y.z został zarezerwowany dla celów diagnostycznych jako adres loopback) po 16 777 214 ($2^{24} – 2$) komputerów.



Rysunek 11.
Klasa A

Klasa B

klasa B – dwa pierwsze bity adresu to 1 i 0, a następne 14 bitów określa sieć. Kolejne 16 bitów identyfikuje komputer. Adres rozpoczyna się liczbą między 128 i 191. Można zaadresować 16 384 (2^{14}) sieci po 65 534 ($2^{16} – 2$) komputery.

Rysunek 12.
Klasa B

Klasa C

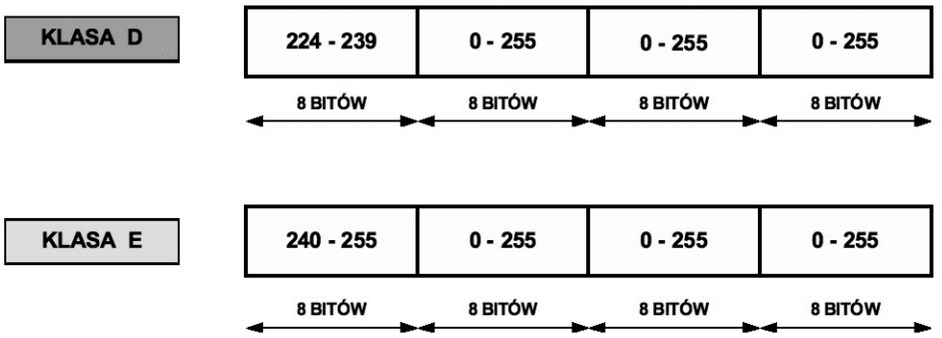
klasa C – trzy pierwsze bity adresu to 1, 1 i 0, a następnych 21 bitów identyfikuje adresy sieci. Ostatnie 8 bitów służy do określenia numeru komputerów w tych sieciach. Adres rozpoczyna się liczbą między 192 i 223. Może zaadresować 2 097 152 (2^{21}) sieci po 254 ($2^8 – 2$) komputery.

Rysunek 13.
Klasa C

Klasa D i E

klasa D – cztery pierwsze bity adresu to 1110. Adres rozpoczyna się liczbą między 224 i 239. Adresy tej klasy są stosowane do wysyłania rozgłoszeń typu multicast.

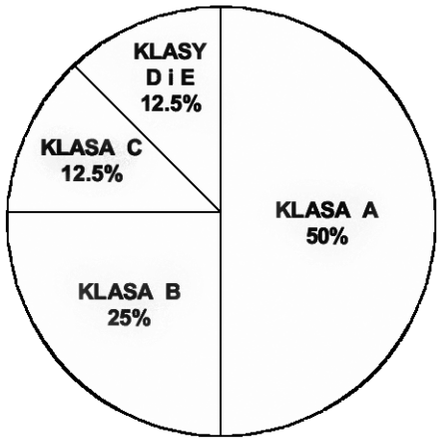
klasa E – cztery pierwsze bity adresu to 1111. Adres rozpoczyna się liczbą między 240 i 255 (adres 255.255.255.255 został zarezerwowany dla celów rozgłoszeniowych). Adresy tej klasy są zarezerwowane dla przyszłych zastosowań.



Rysunek 14.
Klasa D i E

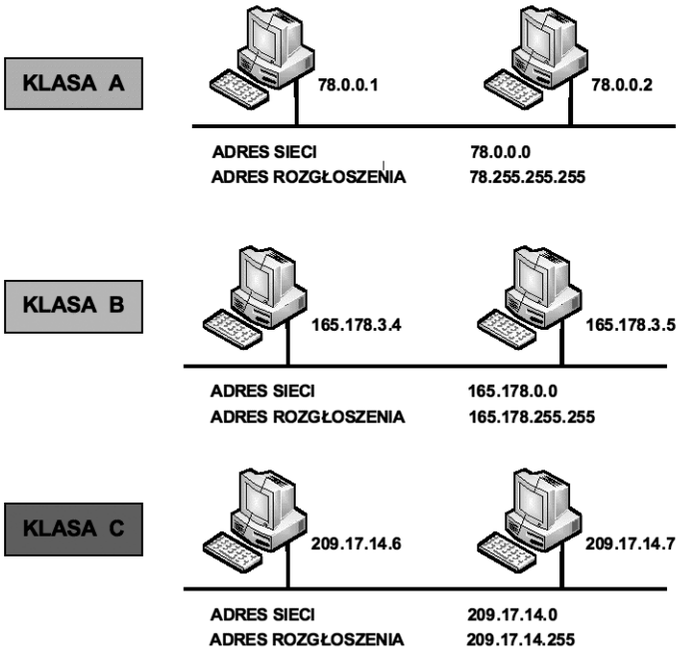
Alokacja adresów IPv4

Do klasy A należy 50% wszystkich dostępnych adresów IPv4, czyli 2 147 483 648 adresów. Na klasę B przypada 25% wszystkich adresów IPv4, co stanowi 1 073 741 824 adresów. Klasa C dostarcza 12.5% całej puli adresów IPv4 i wynosi 536 870 912 adresów. Natomiast w klasach D i E znajduje się również 12.5% wszystkich dostępnych adresów IPv4 – 536 870 912 adresów (patrz rys. 15).



Rysunek 15.
Alokacja adresów IP w wersji 4

Przykłady adresów IPv4



Rysunek 16.
Przykłady adresów IP w wersji 4

Adresy zarezerwowane

Pewne specyficzne adresy IP oraz szczególne ich zakresy są zarezerwowane i ich stosowanie jest w jakimś stopniu ograniczone, głównie do sieci lokalnych LAN.

255.255.255.255 – adres tego typu jest stosowany w wiadomości wysłanej do wszystkich urządzeń i wszystkich sieci (podsieci). Wiadomość taka byłaby niebezpieczna dla funkcjonowania Internetu i dlatego routery nie przełączają takiego pakietu, co ogranicza jego rozprzestrzenianie jedynie do sieci lokalnej. Inną postacią wiadomości wysyłanej do wszystkich urządzeń w danej sieci jest zastosowanie adresu z wartością numeru sieci i wstawienie jedynek na wszystkich pozycjach bitów definiujących hosta. Na przykład, chcąc wysłać wiadomość typu rozgłoszenie do sieci o numerze 135.17.0.0, mającej maskę równą 255.255.0.0, należy wysłać rozgłoszenie pod adresem 135.17.255.255.

0.0.0.0 – taki adres oznacza nieznaną sieć i jest stosowany w metodzie znalezienia bramy dla wyjścia z lokalnej sieci. Adres stosowany przy braku wprowadzonego stałego adresu bramy.

127.0.0.1 – specjalny adres w klasie A stosowany do testowania prawidłowości ustawienia stosu protokołu TCP/IP na lokalnym komputerze (ang. *localhost*). Adres ten jest często określany adresem pętli zwrotnej (ang. *loopback address*). Testowanie tego typu adresu można wykonać w każdym komputerze zawierającym kartę sieciową i polega to na wydaniu polecenia ping i podaniu adresu IP z zakresu między 127.0.0.1 i 127.255.255.254.

3 ADRESOWANIE BEZKLASOWE – MASKI PODSIECI

Wprowadzenie do adresowania bezklasowego

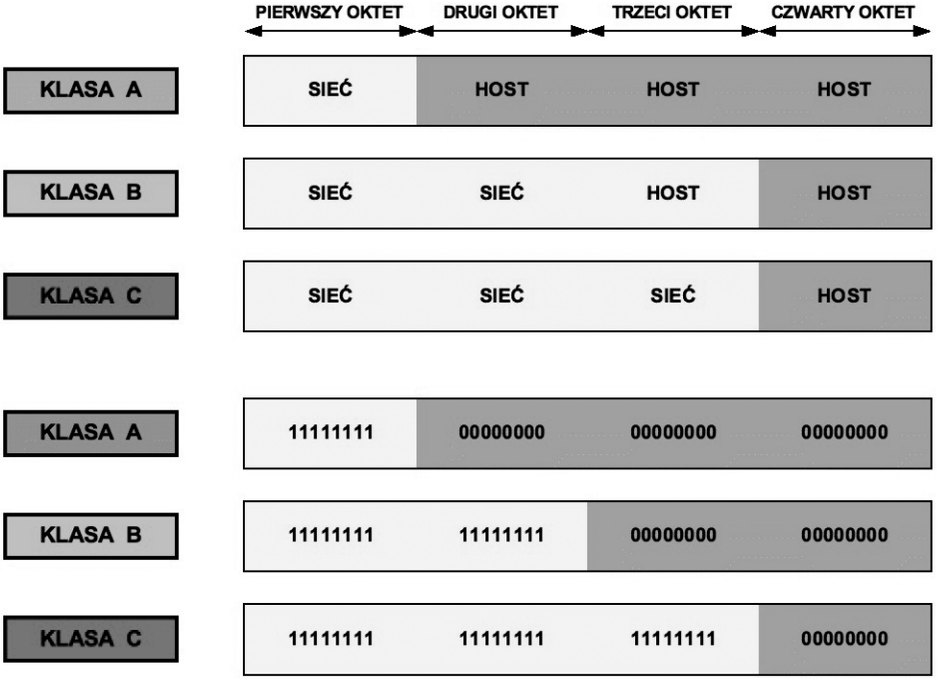
Podział adresów na klasy A, B i C, przy gwałtownym wzroście zapotrzebowania na nie, okazał się bardzo nieekonomiczny. Dlatego obecnie powszechnie jest stosowany model adresowania bezklasowego, opartego na tzw. **maskach podsieci**. W tym rozwiązaniu dla każdej podsieci definiuje się tzw. maskę, mającą podobnie jak adres IPv4 postać 32-bitowej liczby, ale o dosyć szczególnej budowie.

Na początku maski podsieci występuje ciąg jedynek binarnych, po których następuje ciąg samych zer binarnych. Część maski podsieci z samymi jedynkami określa sieć natomiast część maski z zerami określa liczbę sieci do zaadresowania.

Maskę podsieci zapisujemy podobnie jak adres IPv4 w notacji kropkowo-dziesiętnej.

Standardowe maski podsieci w postaci binarnej

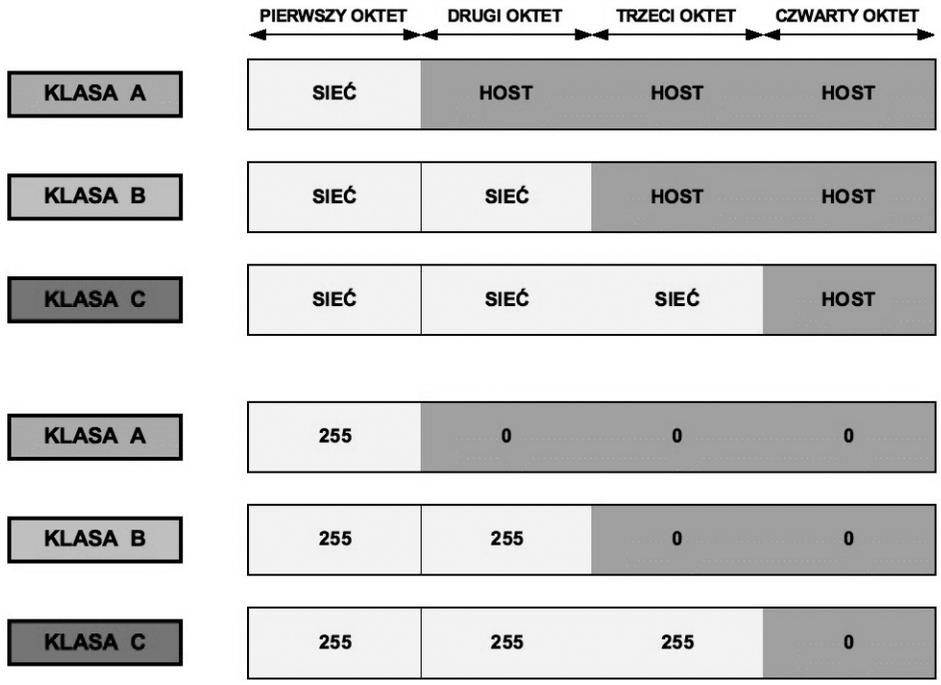
Maski podsieci można zapisywać w notacji binarnej lub dziesiętnej. W przypadku zapisu binarnego (patrz rys. 17), w części identyfikatora sieci występują same jedynki, natomiast w części identyfikatora hosta znajdują się same zera.



Rysunek 17.
Standardowe maski podsieci w zapisie binarnym

Standardowe maski podsieci w notacji dziesiętnej

W przypadku notacji dziesiętnej (patrz rys. 18), maski podsieci w części identyfikatora sieci mają wartość 255 natomiast w części identyfikatora hosta wartość 0. Na przykład standardowa maska podsieci w klasie A – to 255.0.0.0, w klasie B – to 255.255.0.0, a w klasie C – to 255.255.255.0



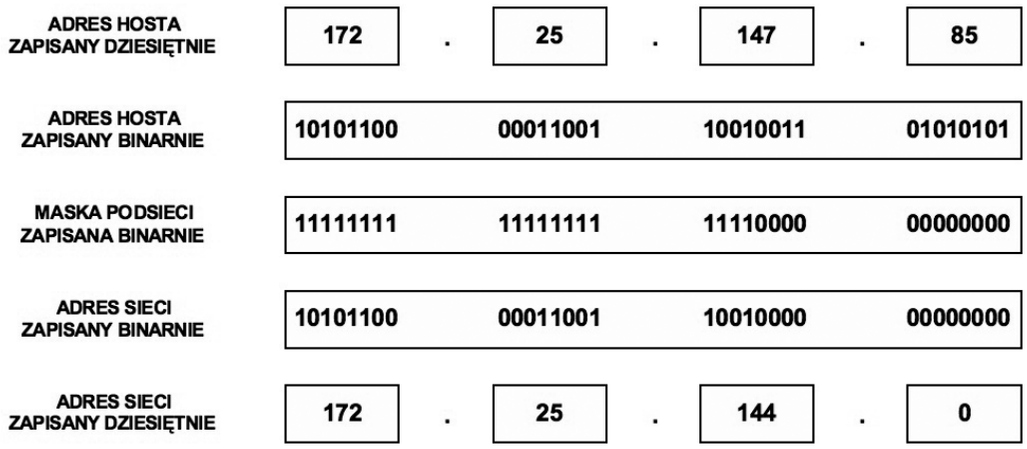
Rysunek 18.
Standardowe maski podsieci w zapisie dziesiętnym

Określanie identyfikatora sieci

Identyfikator sieci jest wykorzystywany do określenia, czy host docelowy znajduje się w sieci lokalnej czy rozległej.

Aby określić sieć, do której należy dowolny adres IPv4, najpierw zamieniamy zapis dziesiętny na binarny, zarówno adresu IP hosta, jak i jego maski podsieci. Następnie używając operacji logicznej koniunkcji AND porównujemy odpowiadające sobie bity IP hosta i maski podsieci. Wynik jest równy 1, gdy oba porównywane bity są równe 1. W przeciwnym wypadku wynik jest równy 0.

Na przykład, jaki jest identyfikator sieci dla hosta o adresie 172.25.147.85 z maską podsieci 255.255.240.0? Odpowiedź: należy zamienić obie liczby na ich binarne odpowiedniki i zapisać jeden pod drugim. Następnie wykonać operację AND dla każdego bitu i zapisać wynik. Otrzymany identyfikator sieci jest równy 172.25.144.0 (patrz rys. 19).



Rysunek 19.
Określanie identyfikatora sieci

4 PODZIAŁ NA PODSIECI

Podział na podsieci z maską 25-bitową

W przypadku maski 25-bitowej zapożyczany jest jeden bit z części hostowej. Można wtedy wydzielić 2 podsieci i dla każdej z nich przypisać po 126 użytecznych adresów IP. Wartość maski podsieci w notacji kropkowo-dziesiętnej w tym przykładzie wynosi 255.255.255.128.

	SIEĆ	SIEĆ	SIEĆ	HOST / PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	10000000
	255	255	255	128

Rysunek 20.
Maska 25-bitowa

Podział na podsieci z maską 26-bitową

Dla maski 26-bitowej zapożyczane są dwa bity z części hostowej. Można wówczas wydzielić 4 podsieci i dla każdej z nich przypisać po 62 użyteczne adresy IP. Wartość maski podsieci w notacji kropkowo-dziesiętnej dla takiego przypadku wynosi 255.255.255.192.

	SIEĆ	SIEĆ	SIEĆ	HOST / PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	11000000
	255	255	255	192

Rysunek 21.
Maska 26-bitowa

Podział na podsieci z maską 27-bitową

Dla maski 27-bitowej zapożyczane są trzy bity z części hostowej. W tym przypadku można wydzielić 8 podsieci i dla każdej z nich zaalokować po 30 użytecznych adresów IP. Wartość maski podsieci w notacji kropkowo-dziesiętnej wynosi 255.255.255.224.

	SIEĆ	SIEĆ	SIEĆ	HOST / PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	11100000
	255	255	255	224

Rysunek 22.
Maska 27-bitowa

Podział na podsieci z maską 28-bitową

Dla maski 28-bitowej trzeba zapożyczyć cztery bity kosztem części hostowej. Można wtedy wydzielić 16 podsieci i dla każdej z nich przypisać po 14 użytecznych adresów IP. Wartość maski podsieci w tym przypadku wynosi 255.255.255.240.

	SIEĆ	SIEĆ	SIEĆ	HOST / PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	11110000
	255	255	255	240

Rysunek 23.
Maska 28-bitowa

Podział na podsieci z maską 29-bitową

W przypadku maski 29-bitowej należy zapożyczyć pięć bitów z części hostowej. Takie rozwiązanie umożliwia wydzielenie 32 podsieci i dla każdej z nich przypisanie po 6 użytecznych adresów IP. Wartość maski podsieci w notacji kropkowo-dziesiętnej wynosi 255.255.255.248.

	SIEĆ	SIEĆ	SIEĆ	HOST / PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	11111000
	255	255	255	248

Rysunek 24.
Maska 29-bitowa

Podział na podsieci z maską 30-bitową

W tym przypadku trzeba zapożyczyć sześć bitów z części hostowej dla podsieci. Umożliwia to wydzielenie aż 64 podsieci, ale dla każdej z nich można przypisać tylko po 2 użyteczne adresy IP. Wartość maski podsieci w notacji kropkowo-dziesiętnej wynosi 255.255.255.252.

	SIEĆ	SIEĆ	SIEĆ	HOST / PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	11111100
	255	255	255	252

Rysunek 25.
Maska 30-bitowa

Podział na podsieci z maską 31-bitową

W przypadku maski 31-bitowej jest zapożyczanych siedem bitów z części hostowej. Co prawda można wydzielić aż 128 podsieci, ale dla każdej z nich niestety nie można przypisać nawet jednego użytecznego adresu IP. Wartość maski podsieci w notacji kropkowo-dziesiętnej wynosi 255.255.255.254.

	SIEĆ	SIEĆ	SIEĆ	HOST / PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	11111110
	255	255	255	254

Rysunek 26.
Maska 31-bitowa

Podział na podsieci z maską 32-bitową

W przypadku maski 32-bitowej zapożyczane są wszystkie osiem bitów z części hostowej. Jest to rozwiązanie nie dające żadnych praktycznych zastosowań. Wartość maski podsieci w notacji kropkowo-dziesiętnej w tym przypadku wynosi 255.255.255.255.

	SIEĆ	SIEĆ	SIEĆ	HOST / PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	11111111
	255	255	255	255

Rysunek 27.
Maska 32-bitowa

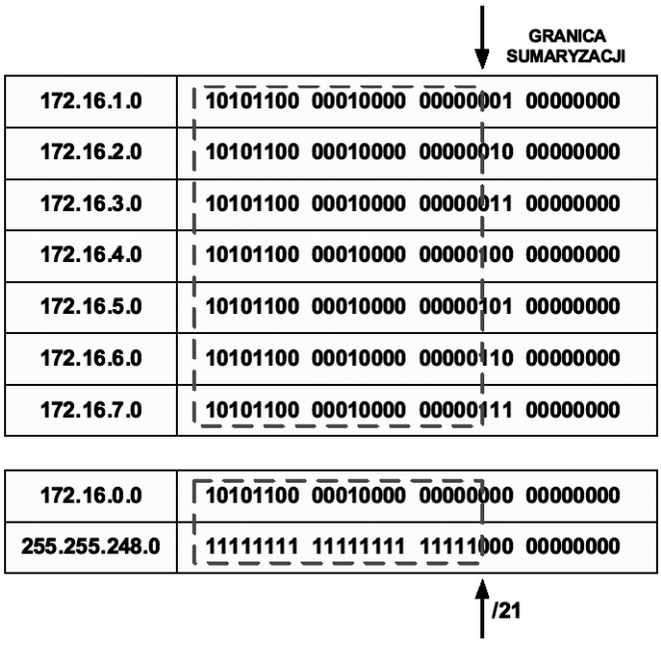
Sumaryzacja tras

Trasa sumaryczna (ang. *summary route*) to pojedyncza trasa używana do reprezentowania wielu tras. Trasy sumaryczne są zbiorem sieci mających ten sam interfejs wyjściowy lub adres IP następnego skoku oraz mogą być podsumowane do jednego adresu sieciowego. Dzięki trasom sumarycznym rozmiar tablic routingu jest mniejszy a proces jej przeszukiwania wydajniejszy. W przykładzie na rys. 28, siedem wpisów o podsieciach (172.16.1.0, 172.16.2.0, 172.16.3.0, 172.16.4.0, 172.16.5.0, 172.16.6.0, 172.16.7.0) w tablicy routingu można zastąpić jednym (172.16.0.0), zmieniając wartość maski podsieci z 255.255.255.0 na 255.255.248.0.

5 TRANSLACJA NAT I PAT

Adresy prywatne

W dokumencie RFC 1918 wyróżniono trzy pule adresów IP przeznaczonych tylko do użytku prywatnego (patrz tab. 1). Adresy te mogą być stosowane tylko i wyłącznie w sieci wewnętrznej. W zależności od tego, jak dużą sieć zamierzamy skonfigurować, wybieramy jedną z klas adresów (A, B lub C). Pakiety z takimi adresami nie są routowane przez Internet.



Rysunek 28.
Przykład sumaryzacji tras

Tabela 1.
Dostępne zakresy prywatnych adresów IP

KLASA	ZAKRES ADRESÓW PRYWATNYCH RFC 1918	STANDARDOWA MASKA PODSIECI	ILOŚĆ SIECI	ILOŚĆ HOSTÓW NA SIEĆ	CAŁKOWITA ILOŚĆ HOSTÓW
A	10.0.0.0 – 10.255.255.255	255.0.0.0	1	16 777 214	16 777 214
B	172.16.0.0 – 172.31.255.255	255.255.0.0	16	65 534	1 048 544
C	192.168.0.0 – 192.168.255.255	255.255.255.0	256	254	65 024

Prywatne adresy IP są zarezerwowane i mogą zostać wykorzystane przez dowolnego użytkownika. Oznacza to, że ten sam adres prywatny może zostać wykorzystany w wielu różnych sieciach prywatnych. Router nie powinien nigdy routować adresów wymienionych w dokumencie RFC 1918. Dostawcy usług internetowych zazwyczaj konfigurują routery brzegowe tak, aby zapobiec przekazywaniu ruchu przeznaczonego dla adresów prywatnych. Zastosowanie mechanizmu NAT zapewnia wiele korzyści dla poszczególnych przedsiębiorstw i dla całego Internetu. Zanim opracowano technologię NAT, host z adresem prywatnym nie mógł uzyskać dostępu do Internetu. Wykorzystując mechanizm NAT, poszczególne przedsiębiorstwa mogą określić adresy prywatne dla niektórych lub wszystkich swoich hostów i zapewnić im dostęp do Internetu.

Wprowadzenie do translacji NAT

Technologia NAT (ang. *Network Address Translation*), zdefiniowana w dokumencie RFC 1631, umożliwia ograniczenie liczby publicznych adresów IP i wykorzystanie prywatnych adresów IP w sieciach wewnętrznych. Te prywatne adresy wewnętrzne są poddawane translacji na adresy publiczne, które mogą być routowane.

Proces zamiany informacji w warstwie sieci modelu odniesienia ISO/OSI, w chwili gdy pakiet przekracza granicę pomiędzy siecią wewnętrzną i zewnętrzną nazywamy **translacją NAT**. W dokumencie RFC 1918 wyróżniono trzy pule adresów IP przeznaczonych tylko do użytku prywatnego (patrz tab. 1). Adresy te mogą być stosowane tylko i wyłącznie w sieci wewnętrznej. W zależności od tego, jak dużą sieć zamierzamy skon-

figurować, wybieramy jedną z klas adresów (A, B lub C). Pakiety z takimi adresami nie są routowane przez Internet.

Operacja ta wykonywana jest przez znajdujące się między sieciami urządzenia, na których działa wyspecjalizowane oprogramowanie obsługujące funkcję NAT, umożliwiające zwiększenie poziomu prywatności w sieci przez ukrycie wewnętrznych adresów IP. Router brzegowy realizuje proces NAT, czyli proces translacji prywatnego adresu wewnętrznego hosta na publiczny adres zewnętrzny, który może być routowany.

Terminologia związana z NAT

Sieć wewnętrzna (ang. *inside network*) – jest to wewnętrzna lokalna sieć komputerowa danej firmy lub przedsiębiorstwa.

Sieć zewnętrzna (ang. *outside network*) – jest to sieć zewnętrzna (np. Internet).

Adres lokalny (ang. *local address*) – jest to adres, za pomocą którego komunikują się hosty w tej samej sieci.

Adres globalny (ang. *global address*) – jest to adres, którego używają hosty z różnych sieci.

Wewnętrzny adres lokalny (ang. *inside local address*) – adres IP przypisany do hosta w sieci wewnętrznej. Najczęściej jest to adres prywatny zgodny ze standardem RFC 1918.

Wewnętrzny adres globalny (ang. *inside global address*) – publiczny adres IP przypisany przez organizację IANA lub dostawcę usług. Adres ten reprezentuje dla sieci zewnętrznych jeden lub więcej wewnętrznych, lokalnych adresów IP.

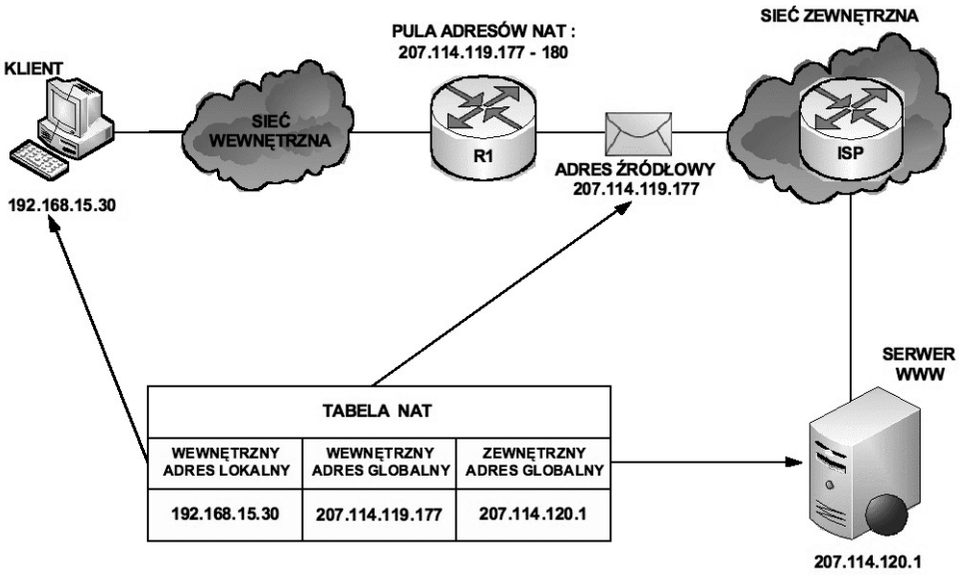
Zewnętrzny adres lokalny (ang. *outside local address*) – publiczny adres IP zewnętrznego hosta, który znany jest hostom znajdującym się w sieci wewnętrznej.

Zewnętrzny adres globalny (ang. *outside global address*) – publiczny adres IP przypisany do hosta w sieci zewnętrznej.

Działanie translacji NAT

Na rysunku 29 jest wyjaśnione działanie usługi NAT):

- Klient o adresie prywatnym 192.168.15.30 (wewnętrzny adres lokalny) zamierza otworzyć stronę WWW przechowywaną na serwerze o adresie publicznym 207.114.120.1 (zewnętrzny adres globalny).



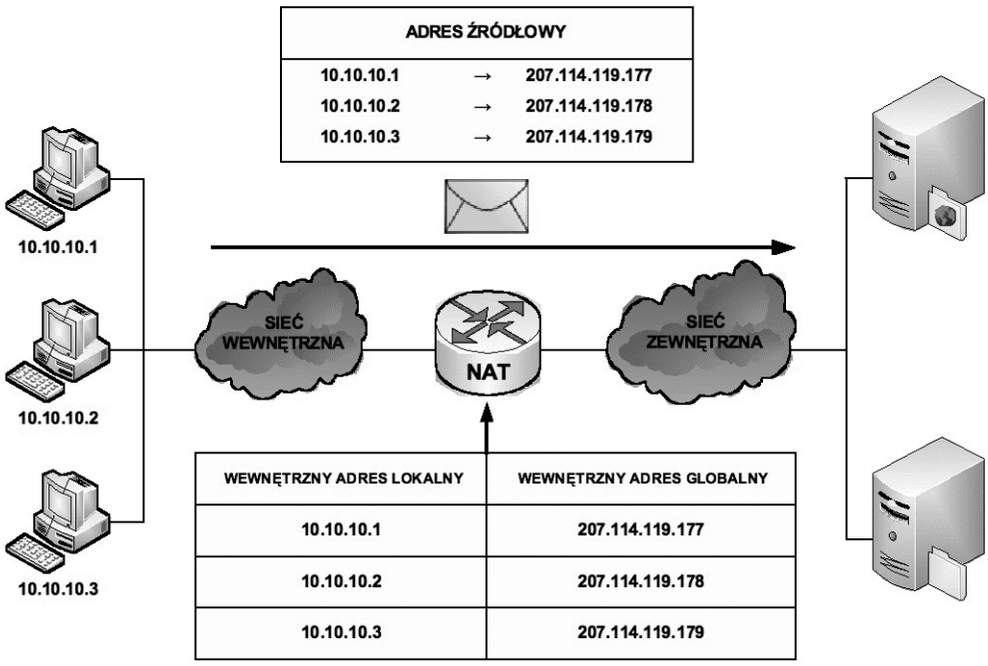
Rysunek 29.
Działanie translacji NAT

- Komputer kliencki otrzymuje z puli adresów przechowywanych na routerze R1 publiczny adres IP (wewnętrzny adres globalny) 207.114.119.177.
- Następnie router ten wysyła pakiet o zmienionym adresie źródłowym do sieci zewnętrznej (router ISP), z której trafia do serwera WWW.
- Kiedy serwer WWW odpowiada na przypisany przez usługę NAT adres IP 207.114.119.177, pakiet powraca do routera R1, który na podstawie wpisów w tabeli NAT ustala, że jest to uprzednio przekształcony adres IP.
- Następuje translacja wewnętrznego adresu globalnego 207.114.119.177 na wewnętrzny adres lokalny 192.168.15.30, a pakiet przekazywany jest do stacji klienckiej.

Statyczna translacja NAT

Statyczna translacja NAT (ang. *static NAT*) umożliwia utworzenie odwzorowania typu jeden-do-jednego pomiędzy adresami lokalnymi i globalnymi pomiędzy sieciami wewnętrzną i zewnętrzną. Jest to szczególnie przydatne w wypadku hostów, które muszą mieć stały adres dostępny z Internetu. Takimi wewnętrznymi hostami mogą być serwery lub urządzenia sieciowe w przedsiębiorstwie. W tym rozwiązaniu administrator ręcznie konfiguruje predefiniowane skojarzenia adresów IP. Ten typ translacji tak naprawdę nie ma nic wspólnego z oszczędzaniem przestrzeni adresowej IP, gdyż każdemu prywatnemu adresowi w sieci wewnętrznej trzeba przypisać adres publiczny w sieci zewnętrznej. Jednakże takie odwzorowanie daje gwarancję, że żaden przesyłany pakiet nie zostanie odrzucony z powodu braku dostępnej przestrzeni adresowej.

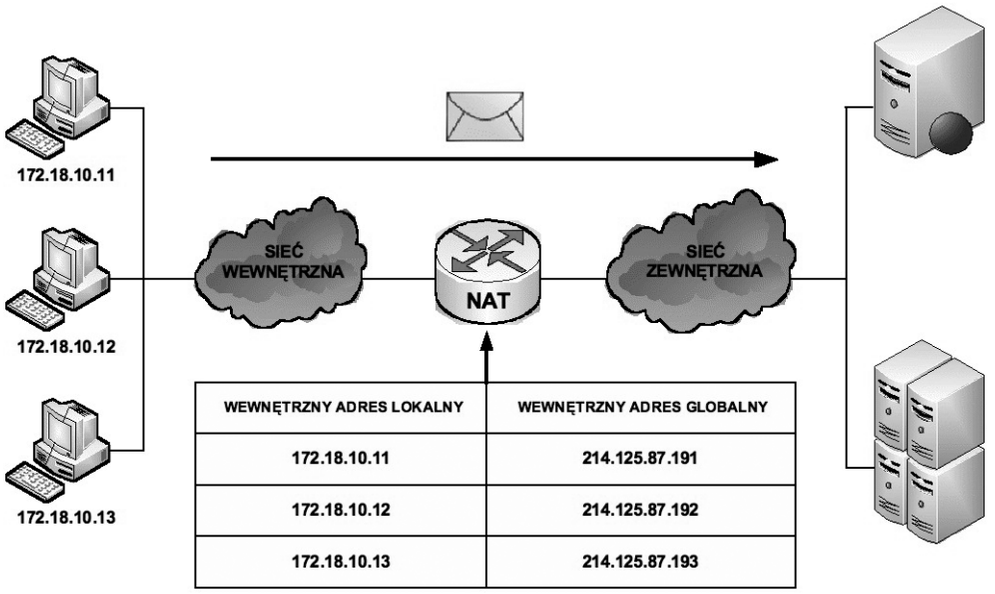
Na rysunku 30 widać, że trzem adresom prywatnym (10.10.10.1, 10.10.10.2, 10.10.10.3) zamapowano trzy adresy publiczne (odpowiednio 207.114.119.177, 207.114.119.178, 207.114.119.179).



Rysunek 30.
Statyczna translacja NAT

Dynamiczna translacja NAT

Dynamiczna translacja NAT (ang. *dynamic NAT*), patrz rys. 31, służy do odwzorowania prywatnego adresu IP na dowolny adres publiczny z uprzednio zdefiniowanej puli. W translacji dynamicznej unikamy stosowania dokładnie takiej samej puli adresów publicznych co prywatnych. Oznacza to, że z jednej strony możemy zaoszczędzić dostępną przestrzeń adresową ale istnieje ryzyko braku gwarancji zamiany adresów w przypadku wyczerpania się puli adresów routowalnych. Z tego powodu na administratorze sieci spoczywa obowiązek zadbania o odpowiedni zakres puli adresów publicznych, aby była możliwa obsługa wszystkich translacji. Ponieważ nie wszyscy użytkownicy sieci komputerowej potrzebują jednoczesnego dostępu do zasobów zewnętrznych, można skonfigurować pulę adresów publicznych mniejszą od liczby adresów prywatnych. Dlatego w tym przypadku unikamy przypisywania wszystkim użytkownikom adresów routowalnych, jak w usłudze translacji statycznej NAT.

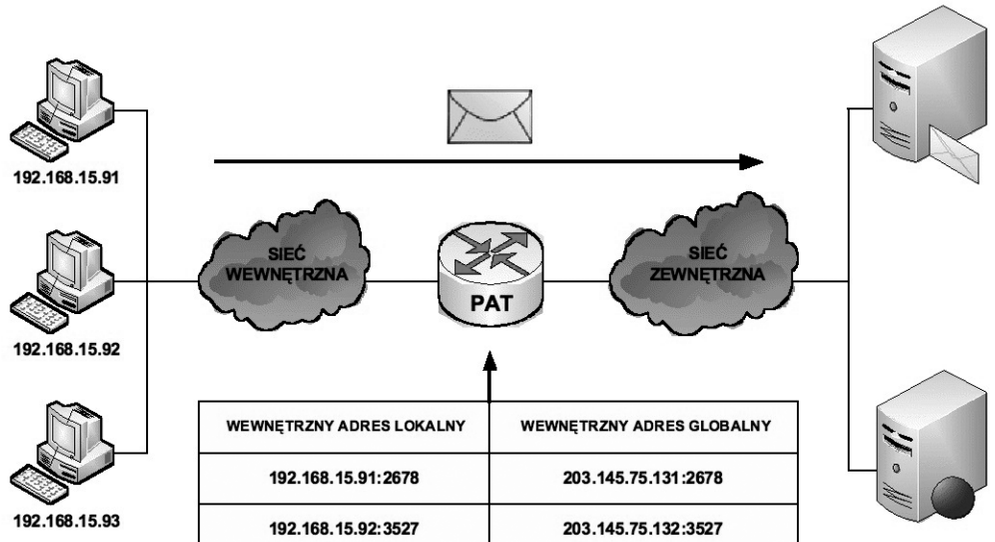


WEWNĘTRZNY ADRES LOKALNY	WEWNĘTRZNY ADRES GLOBALNY
172.18.10.11	214.125.87.191
172.18.10.12	214.125.87.192
172.18.10.13	214.125.87.193

Rysunek 31.
Dynamiczna translacja NAT

Translacja PAT

Translacja PAT (ang. *Port Address Translation*), patrz rys. 32, służy do odwzorowania wielu prywatnych adresów IP na jeden publiczny adres IP. Istnieje możliwość odwzorowania wielu adresów na jeden adres IP, ponieważ z każdym adresem prywatnym związany jest inny numer portu. W technologii PAT tłumaczone adresy są rozróżniane przy użyciu unikatowych numerów portów źródłowych powiązanych z globalnym adresem IP. Numer portu zakodowany jest na 16 bitach. Całkowita liczba adresów wewnętrznych, które mogą być przetłumaczone na jeden adres zewnętrzny, może teoretycznie wynosić nawet 65 536. W rzeczywistości do jednego adresu IP może zostać przypisanych około 4000 portów. W mechanizmie PAT podejmowana jest zawsze próba zachowania pierwotnego portu źródłowego. Jeśli określony port źródłowy jest już używany, funkcja PAT przypisuje pierwszy dostępny numer portu, licząc od początku zbioru numerów odpowiedniej grupy portów (0–511, 512–1023 lub 1024–65535). Gdy zabraknie dostępnych portów, a skonfigurowanych jest wiele zewnętrznych adresów IP, mechanizm PAT przechodzi do następnego adresu IP w celu podjęcia kolejnej próby przydzielenia pierwotnego portu źródłowego. Ten proces jest kontynuowany aż do wyczerpania wszystkich dostępnych numerów portów i zewnętrznych adresów IP.



WEWNĘTRZNY ADRES LOKALNY	WEWNĘTRZNY ADRES GLOBALNY
192.168.15.91:2678	203.145.75.131:2678
192.168.15.92:3527	203.145.75.132:3527
192.168.15.93:7794	203.145.75.133:7794

Rysunek 32.
Translacja PAT

Zalety translacji NAT i PAT

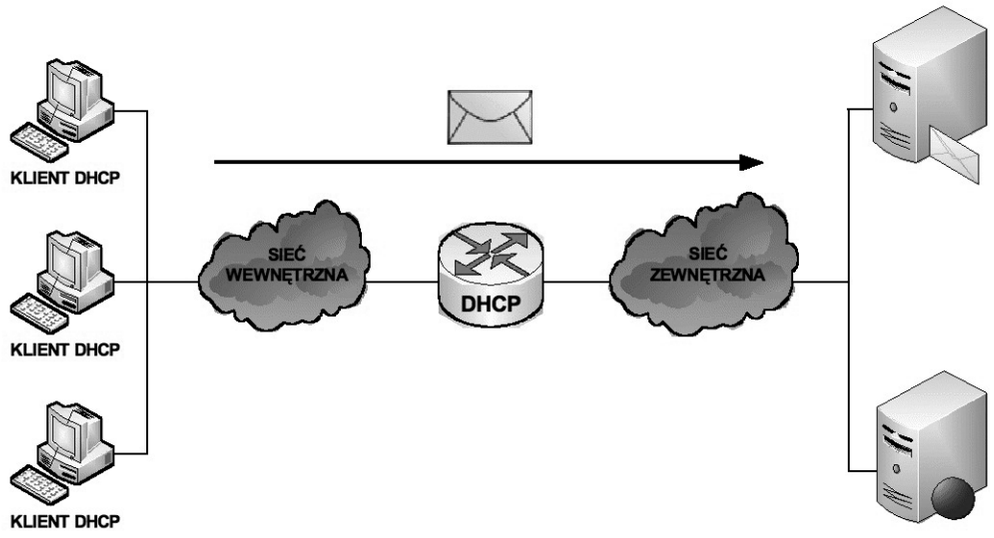
Do głównych zalet translacji adresów prywatnych na publiczne należą:

1. Eliminacja konieczności ponownego przypisania adresów IP do każdego hosta po zmianie dostawcy usług internetowych (ISP). Użycie mechanizmu NAT umożliwia uniknięcie zmiany adresów wszystkich hostów, dla których wymagany jest dostęp zewnętrzny, a to wiąże się z oszczędnościami czasowymi i finansowymi.
2. Zmniejszenie liczby adresów przy użyciu dostępnej w aplikacji funkcji multipleksowania na poziomie portów. Gdy wykorzystywany jest mechanizm PAT, hosty wewnętrzne mogą współużytkować pojedynczy publiczny adres IP podczas realizacji wszystkich operacji wymagających komunikacji zewnętrznej. W takiej konfiguracji do obsługi wielu hostów wewnętrznych wymagana jest bardzo niewielka liczba adresów zewnętrznych. Prowadzi to do oszczędności adresów IP.
3. Zwiększenie poziomu bezpieczeństwa w sieci. Ponieważ w przypadku sieci prywatnej nie są rozgłaszane wewnętrzne adresy ani informacje o wewnętrznej topologii, sieć taka pozostaje wystarczająco zabezpieczona, gdy dostęp zewnętrzny odbywa się z wykorzystaniem translacji NAT.

6 USŁUGA DHCP

Podstawy działania DHCP

Usługa DHCP (ang. *Dynamic Host Configuration Protocol*), patrz rys. 33, działa w trybie klient-serwer i została opisana w dokumencie RFC 2131. Umożliwia ona klientom DHCP w sieciach IP uzyskiwanie informacji o ich konfiguracji z serwera DHCP. Użycie usługi DHCP zmniejsza nakład pracy wymagany przy zarządzaniu siecią IP. Najważniejszym elementem konfiguracji odbieranym przez klienta od serwera jest adres IP klienta. Klient DHCP wchodzi w skład większości nowoczesnych systemów operacyjnych, takich jak systemy Windows, Sun Solaris, Linux i MAC OS. Klient żąda uzyskania danych adresowych z sieciowego serwera DHCP, który zarządza przydzielaniem adresów IP i odpowiada na żądania konfiguracyjne klientów.



Rysunek 33.
Działanie usługi dynamicznego przydzielania adresów IP

Serwer DHCP może odpowiadać na żądania pochodzące z wielu podsieci. Protokół DHCP działa jako proces serwera służący do przydzielania danych adresowych IP dla klientów. Klienci dzierżawią informacje pobrane z serwera na czas ustalony przez administratora. Gdy okres ten dobiega końca, klient musi zażądać nowego adresu. Zazwyczaj klient uzyskuje ten sam adres.

Administratorzy na ogół preferują serwery sieciowe z usługą DHCP, ponieważ takie rozwiązanie jest skalowalne i łatwo nim zarządzać. Konfigurują oni serwery DHCP tak, aby przydzielane były adresy ze zdefiniowanych pul adresów. Na serwerach DHCP mogą być dostępne także inne informacje, takie jak adresy serwerów DNS, adresy serwerów WINS i nazwy domen. W przypadku większości serwerów DHCP administratorzy mogą także zdefiniować adresy MAC obsługiwanych klientów i automatycznie przypisywać dla tych klientów zawsze te same adresy IP.

Protokołem transportowym wykorzystywanym przez protokół DHCP jest UDP (ang. *User Datagram Protocol*). Klient wysyła komunikaty do serwera na port 67. Serwer wysyła komunikaty do klienta na port 68.

Sposoby przydzielania adresów IP

Istnieją trzy mechanizmy przydzielania adresów IP dla klientów:

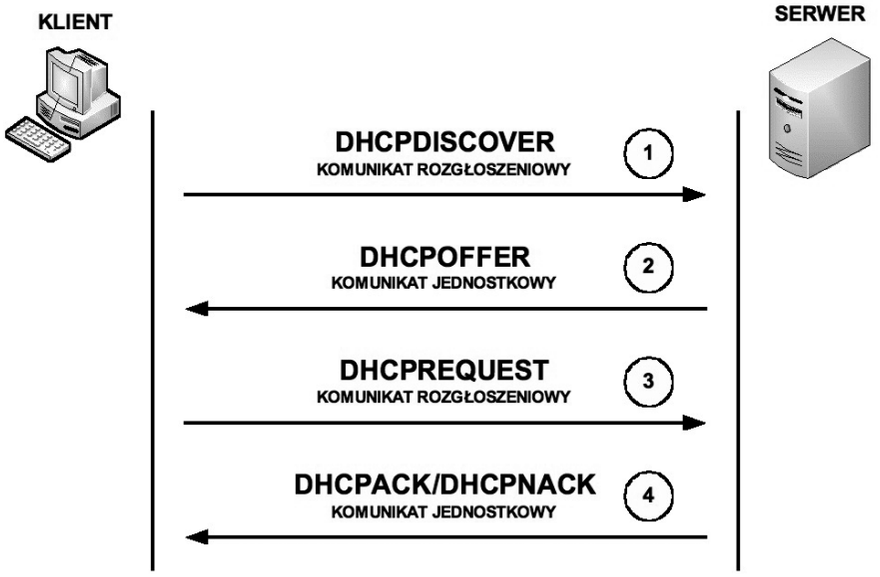
1. **Alokacja automatyczna** – serwer DHCP przypisuje klientowi stały adres IP.
2. **Alokacja ręczna** – adres IP dla klienta jest przydzielany przez administratora. Serwer DHCP przesyła adres do klienta.
3. **Alokacja dynamiczna** – serwer DHCP dzierżawi klientowi adres IP na pewien ograniczony okres czasu.

Serwer DHCP tworzy pule adresów IP i skojarzonych z nimi parametrów. Pule przeznaczone są dla poszczególnych logicznych podsieci IP. Dzięki temu jeden klient IP może uzyskiwać adresy od wielu serwerów DHCP i może być przenoszony. Jeśli klient uzyska odpowiedź od wielu serwerów, może wybrać tylko jedną z ofert.

Wymiana komunikatów protokołu DHCP

W procesie konfiguracyjnym klienta DHCP wykonywane są następujące działania (patrz rys. 34):

1. Na kliencie, który uzyskuje członkostwo w sieci, musi być skonfigurowany protokół DHCP. Klient wysyła do serwera żądanie uzyskania konfiguracji IP. Czasami klient może zaproponować adres IP, na przykład wówczas, gdy żądanie dotyczy przedłużenia okresu dzierżawy adresu uzyskanego wcześniej od serwera DHCP. Klient wyszukuje serwer DHCP, wysyłając komunikat rozgłoszeniowy DHCPDISCOVER.



Rysunek 34.
Wymiana komunikatów protokołu DHCP

2. Po odebraniu tego komunikatu serwer określa, czy może obsłużyć określone żądanie przy użyciu własnej bazy danych. Jeśli żądanie nie może zostać obsłużone, serwer może przekazać odebrane żądanie dalej, do innego serwera DHCP. Jeśli serwer DHCP może obsłużyć żądanie, do klienta wysyłana jest oferta z konfiguracją IP w formie komunikatu transmisji pojedynczej (unicast) DHCPOFFER. Komunikat DHCPOFFER zawiera propozycję konfiguracji, która może obejmować adres IP, adres serwera DNS i okres dzierżawy.
3. Jeśli określona oferta jest odpowiednia dla klienta, wysyła on inny komunikat rozgłoszeniowy, DHCPREQUEST, z żądaniem uzyskania tych konkretnych parametrów IP. Wykorzystywany jest komunikat rozgłoszeniowy, ponieważ pierwszy komunikat, DHCPDISCOVER mógł zostać odebrany przez wiele serwerów DHCP. Jeśli wiele serwerów wyśle do klienta swoje oferty, dzięki komunikatowi rozgłoszeniowemu DHCPREQUEST serwery te będą mogły poznać ofertę, która została zaakceptowana. Zazwyczaj akceptowana jest pierwsza odebrana oferta.
4. Serwer, który odbierze sygnał DHCPREQUEST, publikuje określoną konfigurację, wysyłając potwierdzenie w formie komunikatu transmisji pojedynczej DHCPACK. Istnieje możliwość (choć jest to bardzo mało prawdopodobne), że serwer nie wyśle komunikatu DHCPACK. Taka sytuacja może wystąpić wówczas, gdy ser-

wer wydzierżawi w międzyczasie określoną konfigurację innemu klientowi. Odebranie komunikatu DHCPACK upoważnia klienta do natychmiastowego użycia przypisanego adresu.

Jeśli klient wykryje, że określony adres jest już używany w lokalnym segmencie, wysyła komunikat DHCPDECLINE i cały proces zaczyna się od początku. Jeśli po wysłaniu komunikatu DHCPREQUEST klient otrzyma od serwera komunikat DHCPNACK, proces rozpocznie się od początku.

Gdy klient nie potrzebuje już adresu IP, wysyła do serwera komunikat DHCPRELEASE.

Zależnie od reguł obowiązujących w przedsiębiorstwie, użytkownik końcowy lub administrator może przypisać dla hosta statyczny adres IP dostępny w puli adresów na serwerze DHCP.

7 USŁUGA DNS

Adresy domenowe

Posługiwanie się adresami IP jest bardzo niewygodne dla człowieka, ale niestety oprogramowanie sieciowe wykorzystuje je do przesyłania pakietów z danymi. Aby ułatwić użytkownikom sieci komputerowych korzystanie z usług sieciowych, obok adresów IP wprowadzono tzw. **adresy domenowe** (symboliczne). Nie każdy komputer musi mieć taki adres. Są one z reguły przypisywane tylko komputerom udostępniającym w Internecie jakieś usługi. Umożliwia to użytkownikom chcącym z nich skorzystać łatwiejsze wskazanie konkretnego serwera. Adres symboliczny zapisywany jest w postaci ciągu nazw, tzw. **domen**, które są rozdzielone kropkami, podobnie jak w przypadku adresu IP. Części adresu domenowego nie mają jednak żadnego związku z poszczególnymi fragmentami adresu IP – chociażby ze względu na fakt, że o ile adres IP składa się zawsze z czterech części, o tyle adres domenowy może ich mieć różną liczbę – od dwóch do siedmiu lub jeszcze więcej. Kilka przykładowych adresów domenowych przedstawiono poniżej:

http://www.wwsi.edu.pl
http://www.onet.pl
http://www.microsoft.com
ftp://public.wwsi.edu.pl
http://www.nask.pl
http://www.mf.gov.pl/

Domeny

Odwrotnie niż adres IP, adres domenowy czyta się od tyłu. Ostatni jego fragment, tzw. domena najwyższego poziomu (ang. *top-level domain*), jest z reguły dwuliterowym oznaczeniem kraju (np. .pl, .de). Jedynie w USA dopuszcza się istnienie adresów bez oznaczenia kraju na końcu. W tym przypadku domena najwyższego poziomu opisuje branżową przynależność instytucji, do której należy dany komputer. Może to być:

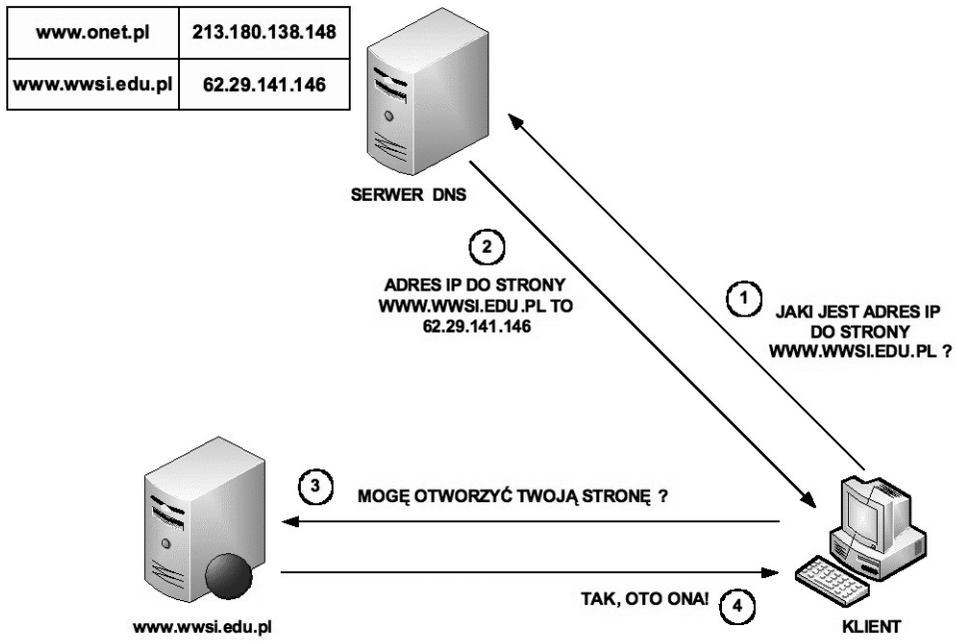
com/co – firmy komercyjne (np. Microsoft, IBM, Intel);
edu/ac – instytucje naukowe i edukacyjne (np. uczelnie);
gov – instytucje rządowe (np. Biały Dom, Biblioteka Kongresu, NASA, Sejm RP);
mil – instytucje wojskowe (np. MON);
org – wszelkie organizacje społeczne i inne instytucje typu *non-profit*;
int – organizacje międzynarodowe nie dające się zlokalizować w konkretnym państwie (np. NATO);
net – firmy i organizacje zajmujące się administrowaniem i utrzymywaniem sieci komputerowych (np. EARN);
biz – biznes;
info – informacje;
name – nazwy indywidualne;
pro – zawody.

Działanie usługi DNS

Działanie usługi DNS sprowadza się do następujących czynności (patrz rys. 35):

1. Klient z przeglądarką internetową pragnie otworzyć stronę www.wwsi.edu.pl przechowywaną na serwerze WWW. Z uwagi, że oprogramowanie sieciowe wymaga adresu IP, klient wysyła zapytanie do serwera DNS o adres IP dla żądanej strony WWW.

2. Serwer DNS na podstawie odpowiednich wpisów w swojej tablicy DNS odsyła klientowi odpowiedź, że stronie www.wwsi.edu.pl odpowiada adres IP w postaci 62.29.141.146.
3. Klient po otrzymaniu właściwego adresu IP wysyła do serwera WWW zapytanie o możliwość otwarcia strony www.wwsi.edu.pl.
4. Serwer WWW po zweryfikowaniu właściwego skojarzenia strony WWW z adresem IP odsyła klientowi zgodę na otwarcie żądanej strony internetowej.



Rysunek 35.
Przykład działania usługi DNS

8. ADRESOWANIE IPV6

Format adresu IPv6

Adres IPv6 początkowo oznaczany był jako IPnG (ang. *IP-The Next Generation*). Adresów IPv6 jest tyle, że można każdemu mieszkańcowi na Ziemi przypisać ich więcej, niż wynosi cała przestrzeń adresowa IPv4. Na każdy metr kwadratowy naszej planety przypada bowiem 665 570 793 348 866 943 898 599 adresów IPv6. IPv6 to 128 bitowy adres, który dzieli się na osiem 16 bitowych bloków:

0010000111011010 0000000011010011 0000000000000000
0010111100111011 0000001010101010 0000000011111111
1111111000101000 1001110001011010

Każdy 16-bitowy blok jest konwertowany do 4-cyfrowego bloku w postaci szesnastkowej i ograniczony dwukropkiem:

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

Adres IPv6 oferuje wiele udoskonaleń w porównaniu z adresowaniem IPv4:

- ulepszone adresowanie,
- uproszczony nagłówek,
- większa mobilność,
- wyższe bezpieczeństwo.

Możliwe uproszczenia zapisu adresu IPv6

ADRES IPv6 ZAPISANY BINARNIE

0010000111011010 0000000011010011 0000000000000000 0010111100111011
0000001010101010 0000000000000000 0000000000000000 1001110001011010

ADRES IPv6 ZAPISANY SZESNASTKOWO

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

ADRES IPv6 – DOPUSZCZALNE UPROSZCZENIA

21DA : D3 : 0000 : 2F3B : 2AA : 0000 : 0000 : 9C5A
21DA : D3 : 0 : 2F3B : 2AA : 0000 : 0000 : 9C5A
21DA : D3 : 0 : 2F3B : 2AA :: 9C5A

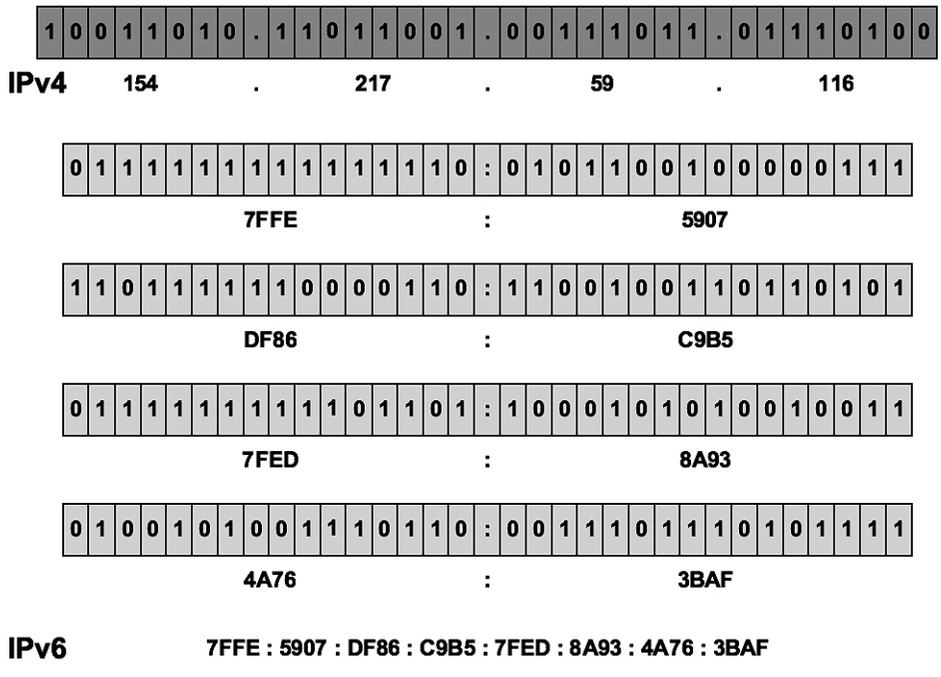
ADRES IPv6 – INNE PRZYKŁADY UPROSZCZEŃ

0ADA : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0009	>>>	ADA :: 9
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001	>>>	:: 1
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000	>>>	::

Rysunek 36.
Przykłady uproszczeń zapisu adresów IPv6

Porównanie adresów IPv4 i IPv6

Adres IPv4 jest adresem 32-bitowym, natomiast adres IPv6 jest adresem 128-bitowym. Adres IPv4 składa się z czterech oktetów liczb binarnych, natomiast adres IPv6 składa się z ośmiu 16-bitowych bloków. Adres IPv4 jest zapisywany w notacji kropkowo-dziesiętnej, natomiast adres IPv6 jest zapisywany w notacji dwu-kropkowo-szesnastkowej. Adres IPv4 daje pulę 4 294 967 296 adresów, natomiast adres IPv6 dostarcza 3.4 x 1038 adresów.



Rysunek 37.
Porównanie zapisu adresów IPv4 i IPv6

9. KONFIGURACJA ADRESÓW IP

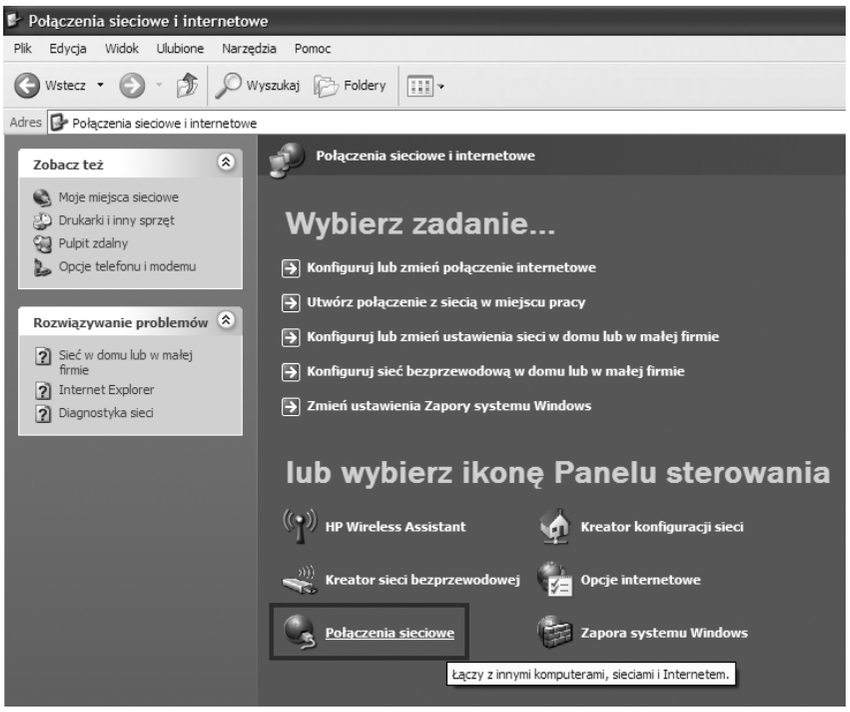
Ręczna konfiguracja adresów IP

Aby ręcznie skonfigurować adresy IP (adres hosta, maska podsieci, brama domyślna, główny serwer DNS, zapasowy serwer DNS) w systemie Windows XP należy wykonać poniższe kroki.

W menu Start wybieramy zakładkę Panel sterowania, i w oknie, które się pojawi (rys. 38) klikamy w kategorię Połączenia sieciowe i internetowe.

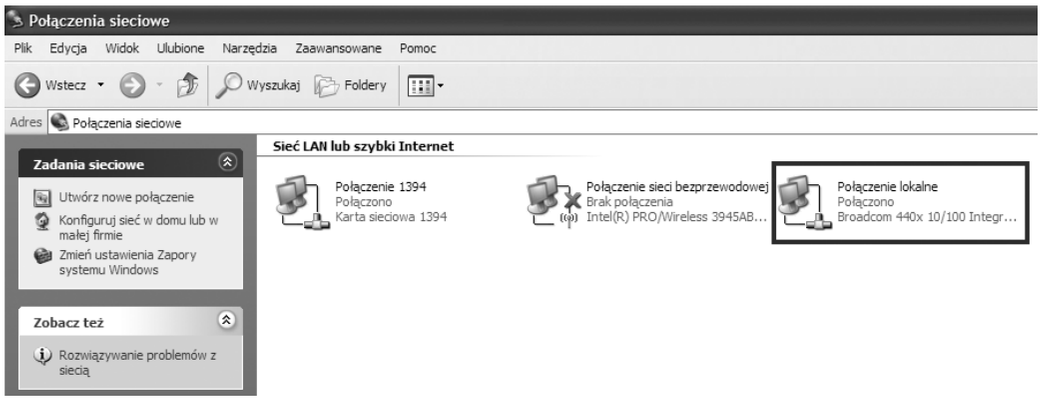
Rysunek 38.
Początek manualnego konfigurowania adresów IP

Z kategorii Połączenia sieciowe i internetowe wybieramy Połączenia sieciowe (patrz rys. 39).



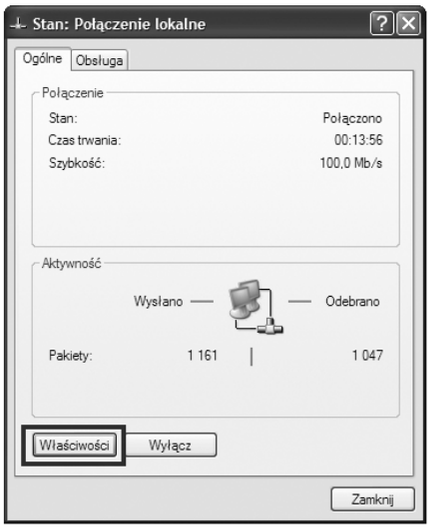
Rysunek 39.
Wybór połączeń sieciowych i internetowych

W kategorii Połączenia sieciowe wybieramy Połączenie lokalne (patrz rys. 40).



Rysunek 40.
Wybór połączenia lokalnego wśród połączeń sieciowych

W oknie, które się ukaże (rys. 41) możemy odczytać: stan połączenia, czas trwania połączenia, szybkość połączenia a także jego aktywność (ilość pakietów wysłanych i odebranych). W oknie tym klikamy na zakładkę Właściwości.



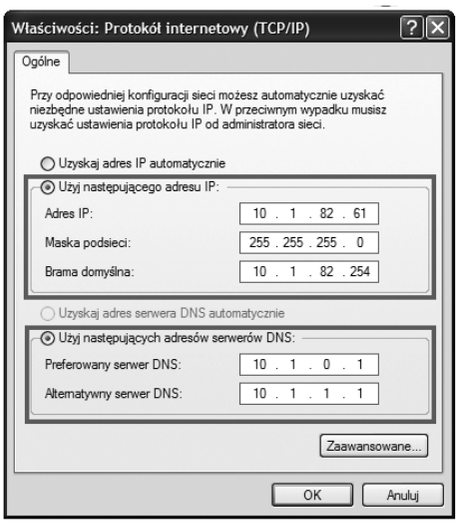
Rysunek 41.
Okno prezentujące stan połączenia lokalnego

W kolejnym oknie, które się (rys. 42), wybieramy składnik Protokół internetowy (TCP/IP) a następnie klikamy w zakładkę Właściwości.

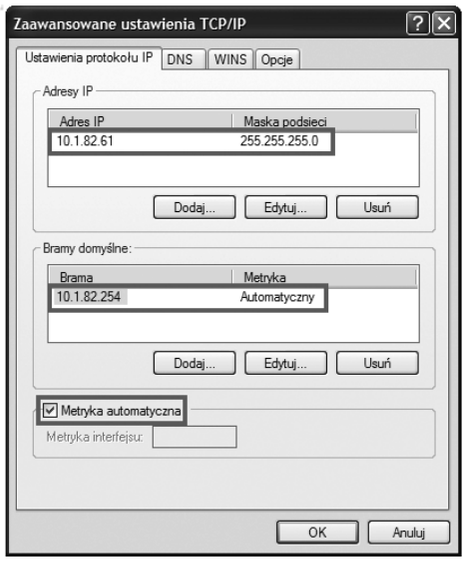
W kolejnym oknie (rys. 43) wybieramy opcję Użyj następującego adresu IP, po czym ręcznie wpisujemy: adres IP hosta, jego maskę podsieci oraz adres bramy domyślnej. W drugiej części okna wybieramy opcję Użyj następujących adresów serwerów DNS, po czym wpisujemy adres IP preferowanego serwera DNS oraz adres IP alternatywnego serwera DNS.

Po kliknięciu w zakładkę Zaawansowane w oknie Właściwości: Protokół internetowy (TCP/IP) otrzymujemy podgląd zaawansowanych ustawień stosu protokołów TCP/IP (patrz rys. 44).

Rysunek 42.
Okno z właściwościami połączenia lokalnego



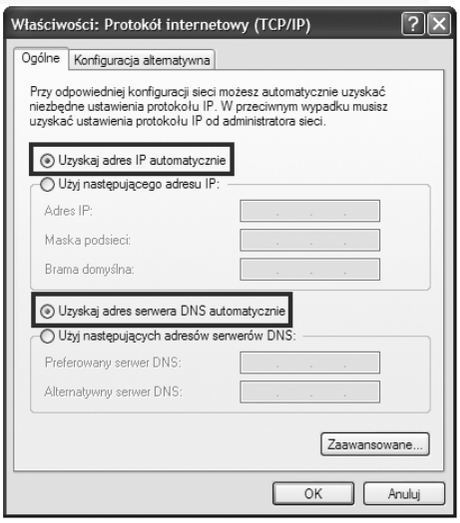
Rysunek 43.
Ręczne wpisanie adresów sieciowych



Rysunek 44.
Efekt wybrania zakładki Zaawansowane w oknie Właściwości Protokołu Internetowego TCP/IP

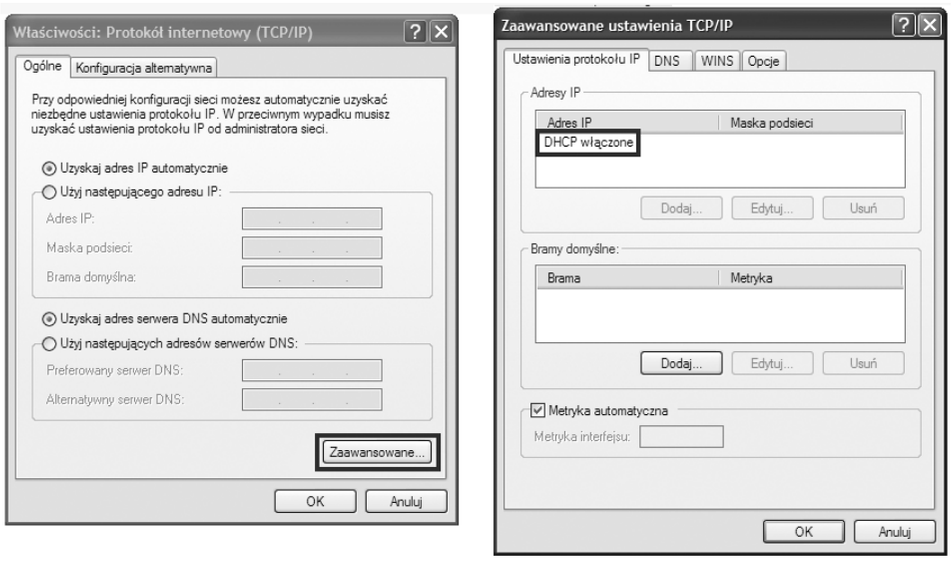
Automatyczna konfiguracja adresów IP

Automatyczna konfiguracja adresów IP przebiega początkowo identycznie, jak w przypadku ręcznego konfigurowania adresów IP, co zilustrowano na rys. 38-42. Dopiero w oknie (rys. 45), które się ukazuje po wybraniu Właściwości w oknie Połączenie lokalne (patrz rys. 42), wybieramy następujące opcje: Uzyskaj adres IP automatycznie oraz Uzyskaj adres serwera DNS automatycznie. W rezultacie zostaną nadane automatycznie następujące adresy IP: adres IP hosta, jego maska podsieci, adres IP bramy domyślnej, adres IP preferowanego serwera DNS oraz adres IP alternatywnego serwera DNS.



Rysunek 45.
Odznaczenie automatycznych wyborów adresów IP

Po kliknięciu w zakładkę Zaawansowane otrzymujemy podgląd zaawansowanych ustawień stosu protokołów TCP/IP, w którym możemy zauważyć, że jest włączony serwer DHCP (patrz rys. 46).

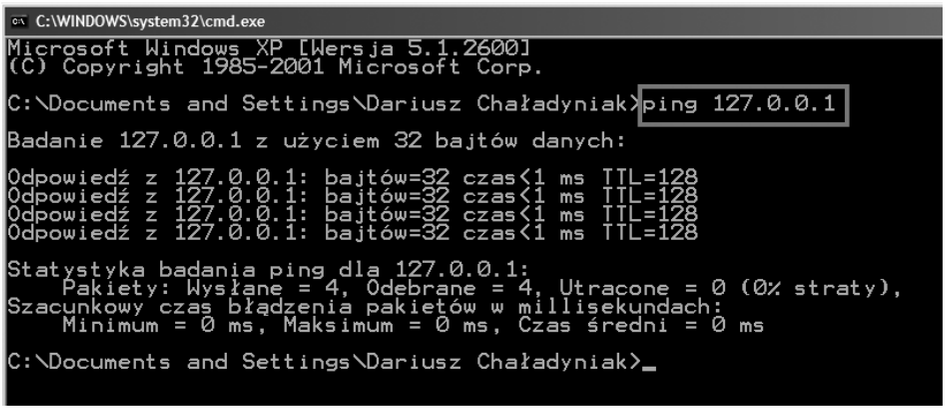


Rysunek 46.
Efekt wybrania zakładki Zaawansowane w oknie Właściwości Protokołu Internetowego TCP/IP

Testowanie konfiguracji protokołu TCP/IP – polecenie ping

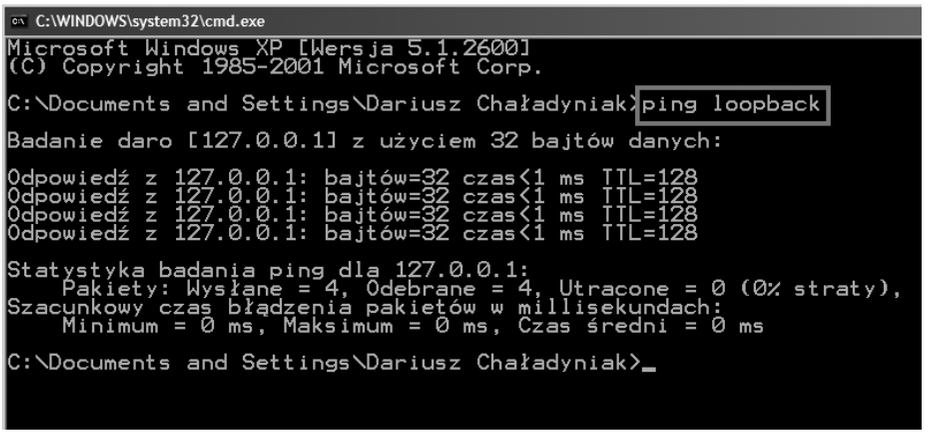
Polecenie **ping** wysyła pakiet do hosta docelowego, a następnie oczekuje na pakiet odpowiedzi tego hosta. Wyniki otrzymane w wyniku stosowania tego protokołu mogą pomóc w ocenie niezawodności ścieżki do hosta, występujących na niej opóźnień oraz tego, czy host jest dostępny i działa. Jest to podstawowy mechanizm testowania. W przykładzie na rys. 47 przedstawiono sytuację, gdy docelowy host (adres pętli zwrotnej)

127.0.0.1 odpowiedział na wszystkie cztery wysłane do niego pakiety. W poleceniu ping jest wykorzystywany protokół ICMP (ang. *Internet Control Message Protocol*).



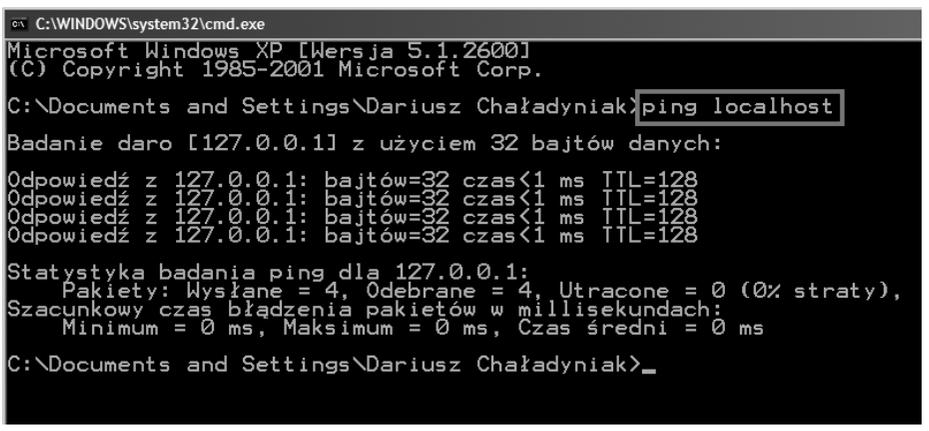
Rysunek 47.
Wydanie polecenia ping 127.0.0.1

Adres pętli zwrotnej można również przetestować poleceniem – ping loopback (rys. 48).



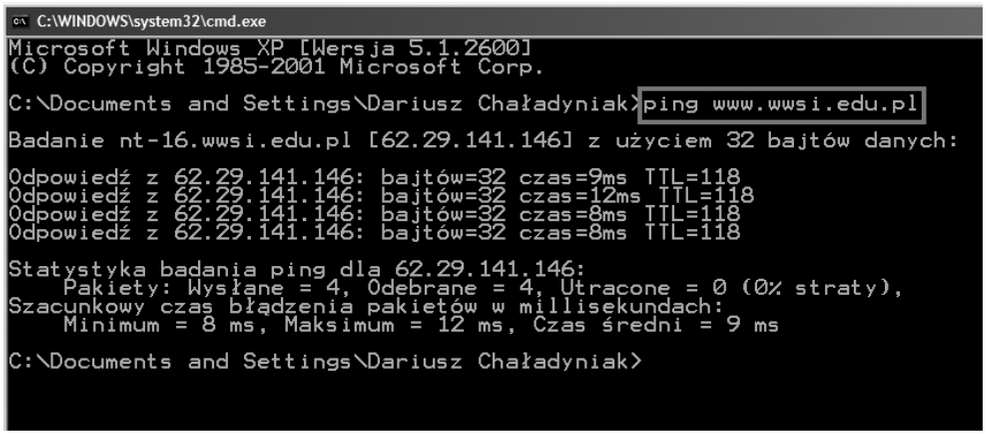
Rysunek 48.
Wydanie polecenia ping loopback

Można użyć również zlecenia jak na rys. 49, ale pod warunkiem, że w katalogu C:/Windows/System32/drivers/etc/ znajduje się plik hosts, w którym jest wpis – 127.0.0.1 localhost.



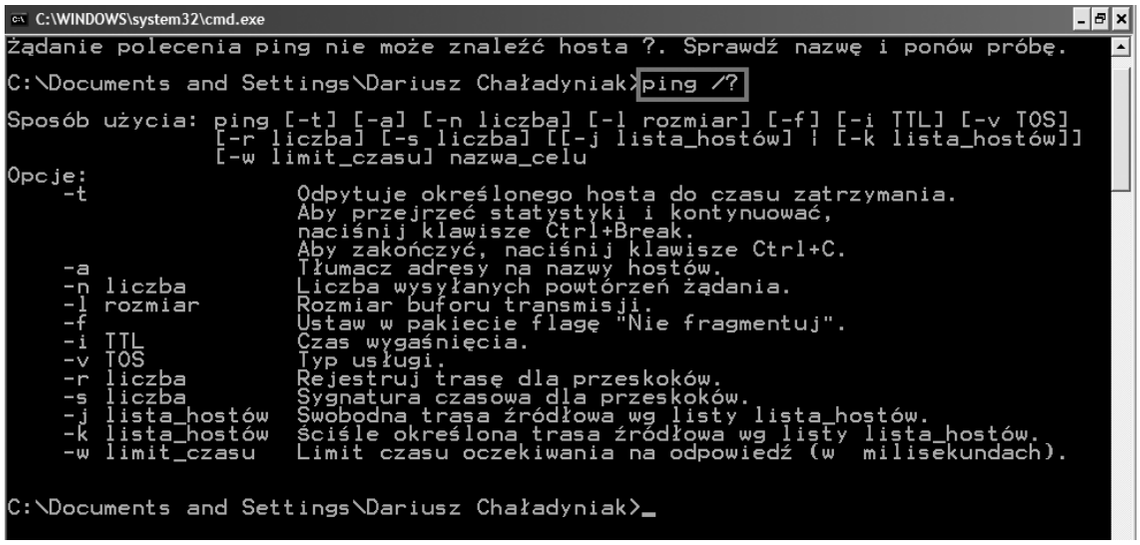
Rysunek 49.
Wydanie polecenia ping localhost

Na rys. 50 pokazano przykład zlecenia ping testującego osiągalność zdalnego hosta w Internecie, w tym przypadku stwierdzono dostępność hosta www.wwsi.edu.pl.



Rysunek 50.
Wydanie przykładowego polecenia ping www.wwsi.edu.pl

Polecenie ping można użyć z wieloma opcjami (patrz rys. 51), w zależności od konkretnych potrzeb np.:
ping –n 10 – liczba wysyłanych powtórzeń żądania – w tym przypadku 10 powtórzeń;
ping –l 1024 – rozmiar buforu transmisji – w tym przypadku 1024 bajtów;
ping –i 128 – czas wygaśnięcia – w tym przypadku 128 (sekund lub liczba przeskoków);
ping –w 500 – limit czasu oczekiwania na odpowiedź – w tym przypadku 500 milisekund.

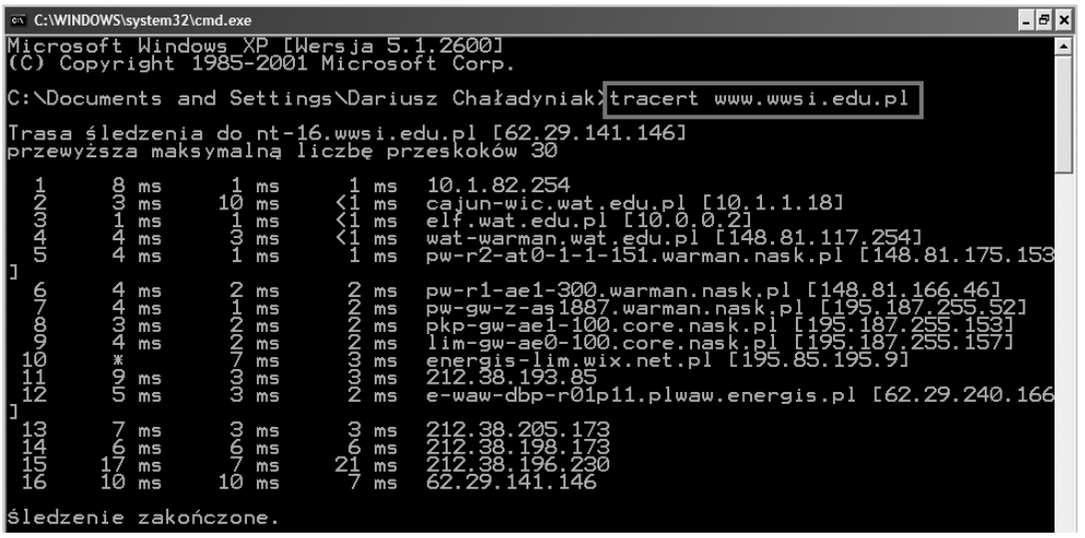


Rysunek 51.
Przykłady możliwych opcji polecenia ping

Testowanie konfiguracji protokołu TCP/IP – polecenie tracert

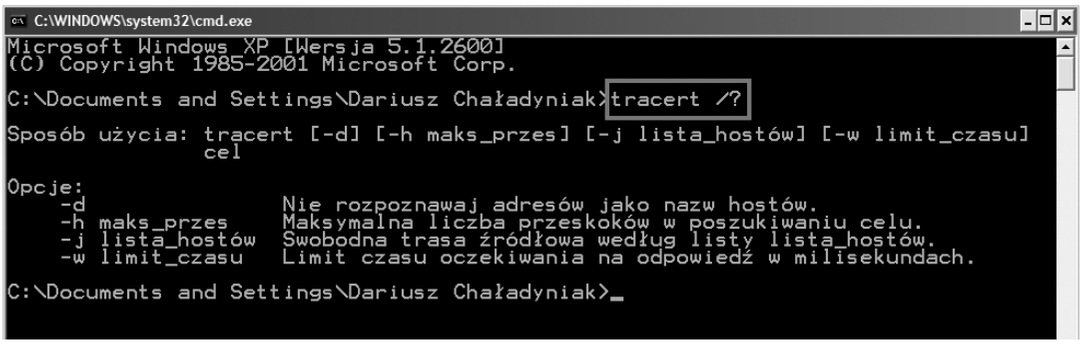
Polecenie **tracert**, umożliwia znalezienie drogi przesyłania danych w sieci i jest podobnie do polecenia ping. Różnica polega na tym, że polecenie ping testuje tylko osiągalność hosta, a polecenie tracert – każdy etap drogi pakietu. W przykładzie na rysunku 52 przedstawiono sytuację, w której śledzona jest ścieżka od lokalnej bramy do hosta www.wwsi.edu.pl.

Polecenie tracert można wydać w z następującymi opcjami (patrz rys. 53):



Rysunek 52.
Wydanie polecenia tracert www.wwsi.edu.pl

tracert –d – nie rozpoznawaj adresów jako nazw hostów;
tracert –h 15 – maksymalna liczba przeskoków w poszukiwaniu celu – w tym przypadku 15 przeskoków;
tracert –j lista_hostów – swobodna trasa źródłowa według listy lista_hostów;
tracert –w 300 – limit czasu oczekiwania na odpowiedź w milisekundach – w tym przypadku 300 milisekund.



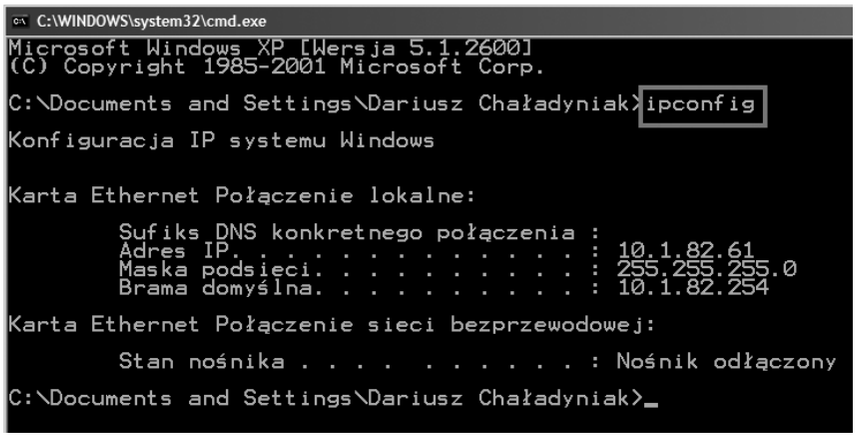
Rysunek 53.
Przykłady możliwych opcji polecenia tracert

Testowanie konfiguracji protokołu TCP/IP – polecenie ipconfig

Polecenie **ipconfig** bez żadnej opcji (patrz rys. 54) służy do wyświetlania podstawowych informacji o adresacji IP: adres IP hosta, jego maskę podsieci oraz adres IP bramy domyślnej (routera).

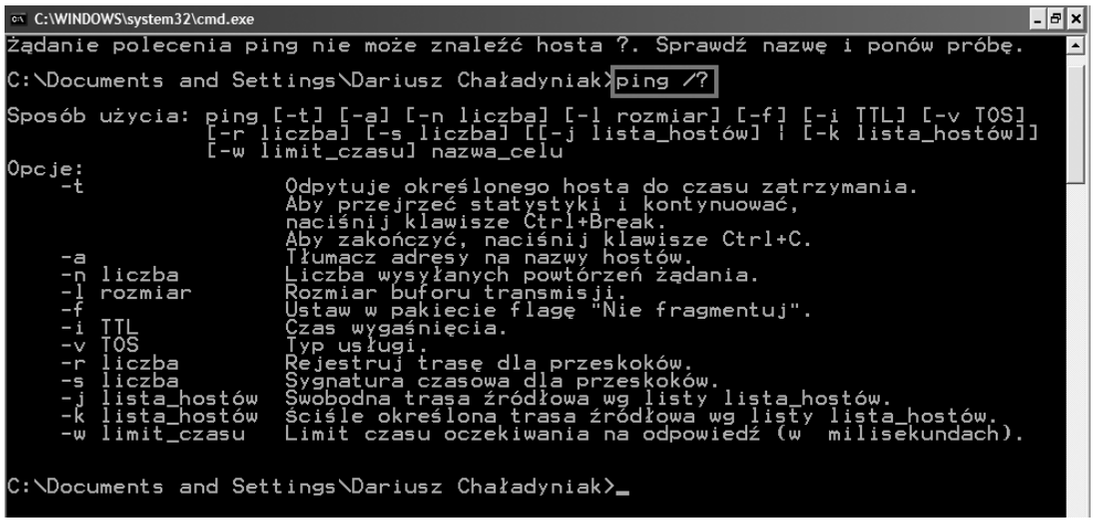
Polecenie ipconfig z opcją all dostarcza dodatkowych informacji o konfiguracji stosu protokołów TCP/IP, np: nazwy kart sieciowych i ich adresy fizyczne (MAC), informację czy serwer DHCP jest włączony czy nie, adres IP serwera DNS i inne (patrz rys. 55).

Inne dodatkowe opcje polecenia ipconfig, to między innymi (patrz rys. 56):
release – zwalnia adres IP dla określonej karty sieciowej;
renew – odnawia adres IP dla określonej karty sieciowej;
flushdns – czyści bufor programu rozpoznającego nazwy DNS;
registerdns – odświeża wszystkie dzierżawy serwera DHCP i ponownie rejestruje nazwy symboliczne DNS;
displaydns – wyświetla zawartość buforu programu rozpoznającego nazwy DNS;



Rysunek 54.
Wydanie polecenia ipconfig

Rysunek 55.
Wydanie polecenia ipconfig z opcją all



Rysunek 56.
Przykłady możliwych opcji polecenia ipconfig

LITERATURA

1. Dye M.A., McDonald R., Rufi A.W., *Akademia sieci Cisco. CCNA Exploration. Semestr 1*, WN PWN, Warszawa 2008
2. Graziani R., Vachon B., *Akademia sieci Cisco. CCNA Exploration. Semestr 4*, WN PWN, Warszawa 2009
3. Komar B., *TCP/IP dla każdego*, Helion, Gliwice 2002
4. Krysiak K., *Sieci komputerowe. Kompendium*, Helion, Gliwice 2005
5. Mucha M. *Sieci komputerowe. Budowa i działanie*, Helion, Gliwice 2003
6. Odom W., Knot T., *CCNA semestr 1. Podstawy działania sieci*, WN PWN, Warszawa 2007

WARSZTATY

Spis treści

Celem warsztatów jest szczegółowe zapoznanie słuchaczy ze strukturą adresacji IPv4 oraz IPv6, wykorzystywanej podczas planowania, wdrażania oraz zarządzania sieciami komputerowymi. Pierwsza część warsztatów jest poświęcona działaniom na liczbach w różnych systemach pozycyjnych (binarnym, dziesiętnym i szesnastkowym), a część druga dotyczy działań na systemie adresowania IPv4 i IPv6 oraz monitorowania i diagnozowania komunikacji w sieciach komputerowych.

1. KONWERSJA MIĘDZY SYSTEMAMI: BINARNYM, DZIESIĘTNYM I SZESNASTKOWYM

Adresy IPv4 komputerów, a ogólniej – urządzeń sieciowych są przedstawiane jako układ czterech liczb w systemie dziesiętnym lub w systemie binarnym (dwójkowym). W systemie IPv6 jest to grupowanie 128-bitowego adresu po 2 bajty i oddzielenie dwukropkiem. Tak wyodrębnione bloki 16-bitowe są konwertowane na postać szesnastkową. Zaczniemy więc zajęcia od przypomnienia, tych systemów oraz algorytmów zamiany liczb między tymi systemami.

Liczbowy system pozycyjny

Systemy dziesiętny i binarny są przykładami systemu pozycyjnego. **System pozycyjny** jest metodą zapisywania liczb w taki sposób, że w zależności od pozycji danej cyfry w ciągu, oznacza ona wielokrotność potęgi pewnej liczby *p* uznawanej za **podstawę** danego systemu. W takiej konwencji zapisu, każda pozycja ma ściśle określoną i niezmienną wagę liczbową. System pozycyjny umożliwia również zapisywanie ułamków, przy czym liczby wymierne składają się albo ze skończonej liczby znaków, albo są od pewnego miejsca okresowe.

Na co dzień stosujemy **system dziesiętny**, zwany także **systemem dziesiątkowym**, czyli o podstawie *p* = 10. W tym systemie, na przykład liczba 539 oznacza:

$539 = 5 \cdot 100 + 3 \cdot 10 + 9 \cdot 1$ czyli $539 = 5 \cdot 10^2 + 3 \cdot 10^1 + 9 \cdot 10^0$.

W informatyce jest stosowany system **dwójkowy**, zwany także **binarnym**, a więc o podstawie 2. Cyframi w tym systemie są 1 i 0 i na przykład, liczba 100101 w systemie binarnym – będziemy ją też zapisywać jako $(100101)_2$ – oznacza:

$1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$

Ten zapis umożliwia obliczenie dziesiętnej wartości tej liczby:

$$(100101)_2 = 1\cdot2^5 + 0\cdot2^4 + 0\cdot2^3 + 1\cdot2^2 + 0\cdot2^1 + 1\cdot2^0 =$$
$$= 1\cdot32 + 0\cdot16 + 0\cdot8 + 1\cdot4 + 0\cdot2 + 1\cdot1 =$$
$$= 37 = (37)_{10}$$

Ogólnie, przy ustalonej podstawie p, liczby w systemie o tej podstawie są zapisywane z wykorzystywaniem cyfr {0, 1, 2, ..., p – 1}. Liczbę w tym systemie, która ma i cyfr, oznaczamy $(c_{i-1}c_{i-2}...c_2c_1c_0)_p$, gdzie c_{i-1}, c_{i-2}, ..., c_2, c_1, c_0 są cyframi tej liczby ze zbioru możliwych cyfr {0, 1, 2, ..., p – 1}. W tym zapisie c_{i-1} jest **najbardziej znaczącą** cyfrą tej liczby, a c_0 jest **najmniej znaczącą cyfrą**. Liczba $(c_{i-1}c_{i-2}...c_2c_1c_0)_p$, ma wartość dziesiętną:

$$(c_{i-1}c_{i-2}...c_2c_1c_0)_p = c_{i-1}\cdot p^{i-1} + c_{i-2}\cdot p^{i-2} + ... + c_2\cdot p^2 + c_1\cdot p^1 + c_0\cdot p^0$$

System pozycyjny o podstawie p charakteryzuje się następującymi cechami, które są uogólnieniem cech systemu dziesiętnego:

- system określa liczba p, będąca podstawą systemu; .
- do zapisu liczb w tym systemie służy p cyfr: 0, 1, 2, ..., p – 1;
- cyfry są ustawiane od najbardziej znaczącej do najmniej znaczącej pozycji; ;
- pozycje cyfr są numerowane od 0 poczynając od prawej strony zapisu, czyli od najmniej znaczącej cyfry;
- każdej pozycji odpowiada waga, równa podstawie systemu podniesionej do potęgi o wartości numeru pozycji;
- cyfry określają, ile razy waga danej pozycji uczestniczy w wartości liczby;
- wartość liczby jest równa sumie iloczynów cyfr przez wagi ich pozycji.

Zaletą systemów pozycyjnych jest łatwość wykonywania nawet złożonych operacji arytmetycznych oraz możliwość zapisu dowolnie dużej liczby.

Ćwiczenie 1. Jaki system zapisu liczb, który znasz bardzo dobrze, nie jest systemem pozycyjnym i dlaczego? Przypomnijmy tylko, że stosowano go w starożytności.

W dalekiej przeszłości, obok systemy dziesiętnego był stosowany powszechnie system **sześć dziesiątkowy**, zwany również **kopowym**. Zapewne wtedy pojawił się pomysł podziału godziny na 60 minut, a minuty na 60 sekund. Podobnie można wnioskować odnośnie miary kata pełnego, która wynosi 360°, czyli 6 x 60.

System binarny, upowszechniony w erze komputerów, ma swoje korzenie w filozoficznym systemie dwóch wartości: dobro i zło, dzień i noc, Ziemia i Niebo, kobieta i mężczyzna itp., powszechnie stosowanym w starożytnych Chinach. Bazując na tej idei, matematyczną wersję systemu dwoistego, jako system binarny, przedstawił Gottfried W. Leibniz w 1703 roku, jednocześnie proponując, jak maja być wykonywane działania.

W informatyce, poza systemem binarnym, są wykorzystywane jeszcze systemy pochodne: ósemkowy, czyli o podstawie 8, i szesnastkowy, czyli o podstawie 16.

W tabeli 2 przedstawiono zapis liczb od 0 do 20 w różnych systemach pozycyjnych, od dwójkowego po szesnastkowy.

Zamiana reprezentacji dziesiętnej na reprezentację w innym systemie

Potrafimy zamienić liczbę dziesiętna na liczbę binarną. Odpowiedni algorytm polega na dzieleniu przez 2.

Ćwiczenie 2. Znajdź reprezentację binarną liczb dziesiętnych: 0, 1, 2, 8, 10, 20, 101, 110, 256, 1024, 10000, 1000000, 1000001.

Łatwo jest uzasadnić poprawność powyższej metody, korzystając z postaci liczby w systemie binarnym. Podobnie, korzystając z zapisu liczby w systemie o podstawie p, łatwo jest uzasadnić poprawność następującego algorytmu, który służy do zamiany liczby dziesiętnej na postać w systemie o dowolnej podstawie p.

Tabela 2.
Liczby w różnych systemach pozycyjnych.

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
10	2	2	2	2	2	2	2	2	2	2	2	2	2	2
11	10	3	3	3	3	3	3	3	3	3	3	3	3	3
100	11	10	4	4	4	4	4	4	4	4	4	4	4	4
101	12	11	10	5	5	5	5	5	5	5	5	5	5	5
110	20	12	11	10	6	6	6	6	6	6	6	6	6	6
111	21	13	12	11	10	7	7	7	7	7	7	7	7	7
1000	22	20	13	12	11	10	8	8	8	8	8	8	8	8
1001	100	21	14	13	12	11	10	9	9	9	9	9	9	9
1010	101	22	20	14	13	12	11	10	A	A	A	A	A	A
1011	102	23	21	15	14	13	12	11	10	B	B	B	B	B
1100	110	30	22	20	15	14	13	12	11	10	C	C	C	C
1101	111	31	23	21	16	15	14	13	12	11	10	D	D	D
1110	112	32	24	22	20	16	15	14	13	12	11	10	E	E
1111	120	33	30	23	21	17	16	15	14	13	12	11	10	F
10000	121	100	31	24	22	20	17	16	15	14	13	12	11	10
10001	122	101	32	25	23	21	18	17	16	15	14	13	12	11
10010	200	102	33	31	24	22	20	18	17	16	15	14	13	12
10011	201	103	34	31	25	23	21	19	18	17	16	15	14	13
10100	202	110	40	32	26	24	22	20	19	18	17	16	15	14

Algorytm: 10 → *p*.
Dane: dziesiętna liczba *n* i podstawa systemu *p*.
Wynik: reprezentacja liczby *n* w systemie przy podstawie *p*.
Dopóki $n \neq 0$, wykonaj następujące dwa kroki:
1. Za kolejną cyfrę od końca (od najmniej znaczącej cyfry) przyjmij resztę z dzielenia *n* przez *p*.
2. Za nową wartość *n* przyjmij całkowity wynik dzielenia *n* przez *p*.

System szesnastkowy, znany również jako system **heksadecymalny**, różni się od systemu, którego używamy na co dzień, ale jest dość popularny w informatyce od dawna, gdyż umożliwia zapisywanie większych liczb na mniejszej przestrzeni. Jego podstawą (bazą) jest liczba 16, a zatem potrzeba 16 znaków na oznaczenie cyfr w tym systemie, za pomocą których można zapisać dowolną liczbę. Za dodatkowe cyfry w tym systemie przyjmuje się litery na oznaczenie „cyfr" większych od 9: 10 → A, 11 → B, 12 → C, 13 → D, 14 → E, 15 → F. A zatem cyframi szesnastkowymi są:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

Liczba $(c_{i-1}c_{i-2}...c_2c_1c_0)_{16}$, gdzie c_i są cyframi szesnastkowymi, ma więc wartość dziesiętną:

$$(c_{i-1}c_{i-2}...c_2c_1c_0)_{16} = c_{i-1}\cdot 16^{i-1} + c_{i-2}\cdot 16^{i-2} + ... + c_2\cdot 16^2 + c_1\cdot 16^1 + c_0\cdot 16^0$$

Ćwiczenie 3. Wyznacz następujące reprezentacje liczb dziesiętnych:
1. 3, 15, 30, 81, 312 w systemie trójkowym
2. 7, 12, 16, 64, 100, 1600 w systemie szesnastkowym.

Zamiana reprezentacji binarnej na dziesiętną

Podaliśmy powyżej, w jaki sposób obliczać wartość dziesiętną liczby binarnej:

$$(100101)_2 = 1\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 = 1\cdot 3^2 + 0\cdot 16 + 0\cdot 8 + 1\cdot 4 + 0\cdot 2 + 1\cdot 1 = 37$$

Istnieje nieco prostszy sposób, bazujący na **schemacie Hornera**. Zobaczmy na przykładzie tej samej liczby, jak to działa:

$$
\begin{aligned}
(100101)_2 &= 1\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 = \\
&= (1\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 0)\cdot 2 + 1\cdot 1 = \\
&= ((1\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 1)\cdot 2 + 0)\cdot 2 + 1 = \\
&= (((1\cdot 2^2 + 0\cdot 2 + 0)\cdot 2 + 1)\cdot 2 + 0)\cdot 2 + 1 = \\
&= (((1\cdot 2 + 0)\cdot 2 + 0)\cdot 2 + 1)\cdot 2 + 0)\cdot 2 + 1 = \\
&= (37)_{10}
\end{aligned}
$$

W ostatnim wzorze widać, że zamieniliśmy liczenie potęg na mnożenie. Z kolei nawiasy pokazują kolejność działań – zauważmy, że działania są wykonywane od najbardziej znaczącego bitu.

Ten przykład możemy uogólnić na następujący algorytm:

Algorytmu: 2 → 10.
Dane: kolejne, od najbardziej znaczącego, bity liczby binarnej: $(c_{i-1}c_{i-2}...c_2c_1c_0)_2$.
Wynik: Wartość dziesiętną z tej liczby obliczamy w następujący sposób:
$z \leftarrow c_{i-1}$; {Ten bit, jako najbardziej znaczący, jest zawsze równy 1.}
Dla $k = i - 2, i - 3,..., 2, 1, 0$ wykonaj:
$z \leftarrow z^*2 + c_k$;
{Innymi słowy, aktualną wartość z pomnóż przez 2 i dodaj kolejny bit.
Kontynuuj aż do wyczerpania bitów.}.

Ćwiczenie 4. Oblicz wartości dziesiętne liczb binarnych otrzymanych w ćwiczeniu 2. Porównaj wyniki z liczbami dziesiętnymi, danymi na początku tamtego ćwiczenia.

Algorytm **2 → 10** może być uogólniony na algorytm ***p* → 10** przez prostą zamianę w ostatnim kroku mnożenia przez 2 mnożeniem przez p.

Ćwiczenie 5. Oblicz wartości dziesiętne liczb reprezentowanych w innych systemach, otrzymanych w ćwiczeniu 3. Porównaj wyniki z liczbami dziesiętnymi, danymi na początku tamtego ćwiczenia.

Konwersja między systemami dziesiętnym i heksadecymalnym
Zamiana (konwersja) liczby dziesiętnej na heksadecymalną odbywa się podobnie, jak zamiana liczb dziesiętnych na postać binarną – daną liczbę dziesiętną dzielimy z resztą przez 16 i zapisujemy kolejno otrzymywane reszty jako cyfry w systemie szesnastkowym. Należy przy tym pamiętać, resztom większym od 9 odpowiadają cyfry będące kolejnymi literami alfabetu, np. resztę 14 zapisujemy jako E. A więc stosujemy w tym przypadku podany powyżej algorytm 10 → p z $p = 16$.

Zamiana liczby szesnastkowej na dziesiętną, czyli obliczanie dziesiętnej wartości liczby szesnastkowej odbywa się również podobnie, jak w przypadku systemu binarnego – w algorytmie 2 → 10 należy w miejsce liczby 2 wstawić liczbę 16.

Ćwiczenie 6. Znajdź liczbę dziesiętną odpowiadającą liczbie heksadecymalnej 4C2H.

Znacznie łatwiejsze jest przechodzenie między systemami binarnym i szesnastkowym, dzięki temu, że podstawa 16 to 2^4, a zatem czterem cyfrom w reprezentacji binarnej, licząc czwórkami od prawej strony, odpowiada jedna cyfra w systemie szesnastkowym. Na przykład, liczbę binarną

10111011011 dzielimy od prawej na bloki złożone z 4 bitów: 101 1101 1011 a następnie czwórki bitów zamieniamy na cyfry szesnastkowe: 5 D B

Ćwiczenie 7. Zapisz liczbę binarną 100101010 w postaci liczby heksadecymalnej i zamień liczbę szesnastkową 4C2H na liczbę binarną.

Dodawanie liczb binarnych

Aby dodać dwie liczby binarne potrzebna jest tabliczka dodawania, czyli wyniki wszystkich możliwych sum dwóch cyfr binarnych. Taka tabliczka ma bardzo prostą postać:

+	0	1
0	0	1
1	1	10

Dodając dwie liczby binarne podpisujemy je jadna pod drugą tak, aby w kolejnych kolumnach znalazły się cyfry stojące na kolejnych pozycjach od prawej. Podobnie jak w systemie dziesiętnym rozpoczynamy od najbardziej prawej kolumny. Sumujemy cyfry w kolumnie zgodnie z podaną wyżej tabelką zapisując wynik pod kreską. Jeśli w kolumnie dodajemy dwie jedynki, to jako wynik piszemy 0 a 1 jest cyfrą przeniesienia na następna pozycję. Jeśli jedna z liczb jest krótsza, w wolne miejsca wpisujemy zera. Na przykład:

```
  1 1              ← cyfry przeniesienia
  110100
+  10101
 1001001
```

Mnożenie liczb binarnych

Mnożenie liczb w układzie dwójkowym jest również bardzo proste, wykonujemy je podobnie jak na liczbach dziesiętnych ale z następująca tabliczka mnożenia.

·	0	1
0	0	0
1	0	1

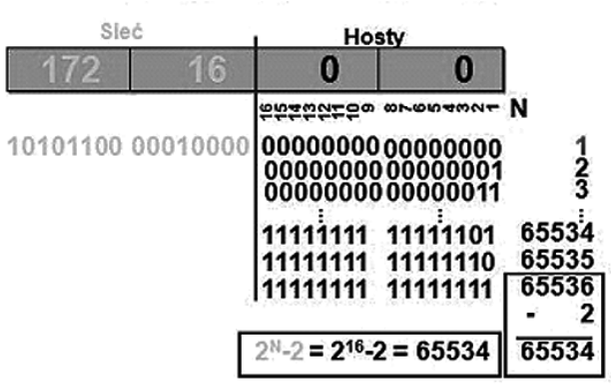
```
    1010
 ·  1010
    0000
   1010
  0000
 1010
 1100100
```

2. DZIAŁANIA NA PRZESTRZENI ADRESOWEJ IPV4

Dla zapewnienia poprawnego sposobu komunikacji pomiędzy urządzeniami w sieci komputerowej, każde z nich musi zostać zdefiniowane w jednoznaczny sposób. Niezbędnym jest również, aby każdy z pakietów tworzonych w warstwie sieciowej podczas komunikacji pomiędzy dwoma hostami zawierał zarówno adres

urządzenia źródłowego jak i docelowego. W przypadku użycia protokołu IPv4 oznacza to, iż oba te 32-bitowe adresy są zawarte w nagłówku warstwy sieciowej. Dla użytkowników sieci, łańcuch 32-bitowy jest trudny do interpretacji i jeszcze trudniejszy do zapamiętania, zatem zwykle prezentujemy adresy IPv4 używając notacji dziesiętnej z kropkami.

Adres sieciowy



Adres sieciowy jest standardowym sposobem odwoływania się do sieci. W przypadku sieci przedstawionej na rysunku powyżej, możemy odwoływać się do niej używając nazwy „sieć 172.16.0.0". Adres sieci jest pierwszym (najniższym) adresem w zakresie adresów związanych z daną siecią. Jest to sposób jednoznacznie określający sieć oraz informujący, iż wszystkie hosty pracujące w sieci 10.0.0.0 będą miały takie same bity w polu sieciowym adresu. W zakresie adresów IPv4 związanych z daną siecią, pierwszy (najniższy) adres jest zarezerwowany dla adresu sieciowego. W adresie tym wszystkie bity w polu hosta mają wartość 0.

Ćwiczenie 8. Wyodrębnij z podanych poniżej adresów, adresy sieci (uwzględniając klasowy schemat adresowania).

192.168.1.212
212.89.73.255
172. 16.0.0
10.10.10.10

Adres rozgłoszeniowy

Adres rozgłoszeniowy IPv4 jest specjalnym adresem występującym w każdej sieci, umożliwiającym jednoczesne komunikowanie się ze wszystkimi hostami w danej sieci. Oznacza to, iż aby wysłać dane do wszystkich urządzeń końcowych w danej sieci, host wysyła pojedynczy pakiet zaadresowany adresem rozgłoszeniowym. Adres rozgłoszeniowy jest ostatnim (najwyższym) adresem w zakresie adresów związanych z daną siecią. Jest to adres, w którym wszystkie bity znajdujące się w polu hosta mają wartość 1. W przypadku sieci 172.16.0.0, adres rozgłoszeniowy będzie miał postać 172.16.255.255. Adres ten określany jest również jako rozgłoszenie skierowane (ang. *directed broadcast*).

Ćwiczenie 9. Wodrębnij z podanych poniżej adresów, adresy rozgłoszeniowe (uwzględniając klasowy schemat adresowania).

198.12.13.254
172.100.0.0
10.255.255.255
1.1.1.255

Operacja koniunkcji (AND)
Aby sprawdzić, w jakiej sieci znajduje się dany adres IP, stosujemy logiczną operację AND do adresu IP i jego maski. Tabelka tej operacji jest taka sama jak w przypadku mnożenia binarnego{

·	0	1
0	0	0
1	0	1

Na przykład, wykonanie operacji AND dla adresu 192.168.1.1 i maski 255.255.255.0 daje następujący wynik:

11000000.10101000.00000001.00000001 (adres 192.168.1.1)
AND
11111111.11111111.11111111.00000000 (maska 24 bitowa)
wynik
11000000.10101000.00000001.00000000 (czyli 192.168.1.0)

Ćwiczenie 10. Wyodrębnij z podanych przykładów, za pomocą operacji AND, adresy sieci:
10.11.125.121/16
172.168.11.12/24
1.1.1.1/8

Adresy hostów
Każde urządzenie końcowe (w rozumieniu sieci komputerowych) musi być jednoznacznie określone za pomocą unikatowego adresu, aby móc dostarczyć do niego wysyłany pakiet. W adresacji IPv4 urządzenia końcowe pracujące w danej sieci, mogą mieć przypisane adresy z zakresu ograniczonego adresem sieciowym oraz rozgłoszeniowym.

Ćwiczenie 11. Oblicz z wykorzystaniem podanych przykładów adresów użyteczne zakresy adresów dla hostów (uwzględniając klasowy schemat adresowania).
192.168.0.0
172.16.0.0
199.199.199.255
10.10.10.10

Ćwiczenie 12. Dla podanych w tabeli adresów należy uzupełnij pozostałe pozycje:

Adres IP	Klasa sieci (podać A lub B lub C)	Adres sieciowy	Adres rozgłoszeniowy	Hosty (podać użyteczny zakres adresów)	Uwagi
11.23.1.1					
128.61.2.100					
202.221.5.64					
192.8.141.2					
130.102.64.17					
256.241.211.13					
127.0.0.1					

Ćwiczenie 13. Projektowanie sieci o określonej liczbie hostów.
Założenia:
– przestrzeń adresowa 172.16.0.0/16
– sieć LAN1: 400 hostów
– siec LAN2: 200 hostów
– siec LAN3 100 hostów
– siec LAN4 100 hostów
– sieć LAN5 60 hostów
– sieć LAN6 20 hostów
– sieć WAN1, 2, 3, są to sieci point-to-point
Zadanie do wykonania: Zaprojektuj schemat adresacji zaczynając od sieci największej a kończąc na najmniejszej, stosując się przy tym do zasady, że powinniśmy zachować jak najwięcej adresów na przyszły rozwój sieci. Określ adresy sieci, maski oraz zakresy dla adresów użytecznych.

Ćwiczenie 14. Projektowanie wymaganej liczby sieci przy opisanej przestrzeni adresowej
Założenia:
– przestrzeń adresowa 192.168.1.0/24
– 5 maksymalnie dużych sieci LAN
– 4 point-to-point sieci WAN
Zadanie do wykonania: Zaprojektuj schemat adresacji zgodnie z wymaganiami. Określ adresy sieci, maski oraz zakresy dla adresów użytecznych.

3 DZIAŁANIA NA PRZESTRZENI ADRESOWEJ IPV6

Protokół **IPv6** to najnowsza wersja protokołu IP, będąca następcą IPv4. Do stworzenia IPv6 przyczyniły się głównie problemy związane z wyczerpywanie się adresów IPv4. Dodatkowymi zamierzeniami było udoskonalenie protokołu IP: eliminacja wad starszej wersji, wprowadzenie nowych rozszerzeń (uwierzytelnienie, zlikwidowanie konieczności stosowania translacji adresów i adresów prywatnych w wielu sieciach, kompresja i inne), zminimalizowanie czynności wymaganych do podłączenia nowego węzła do Internetu. Protokół IPv6 zapewnia większą spójność infrastruktury sieciowej, uproszczenie zasad adresowania, odporność na błędy oraz gotowe mechanizmy bezpieczeństwa.

Struktura przestrzeni adresowej IPv6
Przestrzeń adresowa IPv6 została rozszerzona z 32 do 128 bitów. Tak długi adres byłby trudny do zapisania w sposób znany z IPv4, a tym bardziej do zapamiętania. Aby usprawnić operowanie nowymi adresami, wprowadzono pewne modyfikacje. Adres 128-bitowy grupuje się po 2 bajty i oddziela dwukropkiem. Tak wyodrębnione bloki 16-bitowe konwertuje się na postać szesnastkową. Przykład takiego adresu:

0034:0000:A132:827C:0000:0000:19AA:2837

Aby skrócić taki adres, pomija się zera występujące na początku danego członu:

34:0:A132:827C:0:0:19AA:2837

Chcąc jeszcze bardziej go uprościć, sąsiadujące ze sobą bloki złożone z samych zer zastępuje się dwoma dwukropkami:

34:0:A132:827C::19AA:2837

Tę operację można jednak zastosować tylko raz. Analizator adresu (*parser*) rozdziela adres w miejscu występowania podwójnego dwukropka i wypełnia go zerami do momentu wyczerpania 128 bitów.

Opisane uproszczenia powodują, że adres IPv6 jest bardziej czytelny i mniej podatny na błędy podczas zapisu przez użytkownika. Schemat adresowania IPv6 określono w dokumencie RFC 2373.

Ze względu na długość adresu IPv6 szczególnie ważną funkcję spełniają serwery DNS. Jeżeli nadal chcemy zapisywać adresy URL, podając numer IP, należy umieszczać je w nawiasach kwadratowych. W przeciwnym razie parser URL nie będzie w stanie rozróżnić adresu IP do numeru portu. Przykład:

http:///[34:0:A132:827C::19AA:2837]:80/index.html

Reprezentacja adresu IPv6

Prefiks, czyli część początkową adresu tworzy określona liczba bitów wyznaczona od lewej strony adresu IPv6, które identyfikują daną sieć. Jego tekstowa reprezentacja jest analogiczna do notacji CIDR (ang. *Classless InterDomain Routing*), znanej z IPv4, tj. adres IPv6/długość prefiksu:

0034:0000:A132:827C:0000:0000:19AA:2837/64

gdzie adres węzła to:

0034:0000:A132:827C:0000:0000:19AA:2837

a adres podsieci to:

0034:0000:A132:827C:0000:0000: 0000:0000/64

lub po skróceniu:

34:0:A132:827C::/64

Zarządzanie adresacją IPv6

Adresy zarezerwowane:

– adres nieokreślony 0:0:0:0:0:0:0:0

Informuje o braku adresu. Jest wykorzystywany jako adres źródłowy podczas wysyłania pakietu z hosta, który jeszcze nie zdążył uzyskać swojego adresu.

– adres Loopback 0:0:0:0:0:0:0:1

To adres typu pętla zwrotna, gdzie węzeł wysyła pakiet sam do siebie. Adresy tego typu nie powinny nigdy opuszczać danego węzła, a tym bardziej być przekazywane przez routery.

4 PODSTAWOWE SPOSOBY WERYFIKACJI DZIAŁANIA PROTOKOŁU IP

Ćwiczenie 15. Użycie komendy *ping* i *tracert* – interpretacja wyników obserwacji

Ćwiczenie 16. Użycie komendy *route print* – interpretacja wyników obserwacji

Ćwiczenie 17. Użycie komendy *netstat* – interpretacja wyników obserwacji

W projekcie **Informatyka +**, poza wykładami i warsztatami, przewidziano następujące działania:

- 24-godzinne kursy dla uczniów w ramach modułów tematycznych
- 24-godzinne kursy metodyczne dla nauczycieli, przygotowujące do pracy z uczniem zdolnym
- nagrania 60 wykładów informatycznych, prowadzonych przez wybitnych specjalistów i nauczycieli akademickich
- konkursy dla uczniów, trzy w ciągu roku
- udział uczniów w pracach kół naukowych
- udział uczniów w konferencjach naukowych
- obozy wypoczynkowo-naukowe.

Szczegółowe informacje znajdują się na stronie projektu

www.informatykaplus.edu.pl