INFORMATYKA – MÓJ SPOSÓB NA POZNANIE I OPISANIE ŚWIATA

PROGRAM NAUCZANIA INFORMATYKI Z ELEMENTAMI PRZEDMIOTÓW MATEMATYCZNO-PRZYRODNICZYCH

Informatyka – poziom rozszerzony

Podstawy adresowania IP w sieciach komputerowych

Dariusz Chaładyniak

Człowiek - najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Tytuł: ***Podstawy adresowania IP w sieciach komputerowych***

Autor: ***Dariusz Chaładyniak***

Redaktor merytoryczny: ***prof. dr hab. Maciej M. Sysło***

Materiał dydaktyczny opracowany w ramach projektu edukacyjnego
Informatyka – mój sposób na poznanie i opisanie świata. Program nauczania informatyki z elementami przedmiotów matematyczno-przyrodniczych

www.info-plus.wwsi.edu.pl

infoplus@wwsi.edu.pl

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

Projekt graficzny: *Marzena Kamasa*

Warszawa 2013

Człowiek - najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

SCENARIUSZ TEMATYCZNY

PODSTAWY ADRESOWANIA IP W SIECIACH KOMPUTEROWYCH

INFORMATYKA – POZIOM POZIOM ROZSZERZONY

OPRACOWANY W RAMACH PROJEKTU:

INFORMATYKA – MÓJ SPOSÓB NA POZNANIE I OPISANIE ŚWIATA.

PROGRAM NAUCZANIA INFORMATYKI

Z ELEMENTAMI PRZEDMIOTÓW MATEMATYCZNO-PRZYRODNICZYCH

Streszczenie

Scenariusz przedstawia podstawowe informacje związane z adresowaniem komputerów w sieciach: na czym polega adresowanie fizyczne, a na czym adresowanie logiczne. Prezentuje podstawowe rodzaje transmisji sieciowej (unicast, multicast, broadcast). Materiał zawiera informacje dotyczące budowy i przeznaczenia 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. Zostają tu wprowadzone trzy wybrane usługi sieciowe, których zrozumienie opiera się na podstawowej wiedzy związanej z adresowaniem 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.

Czas realizacji

5 x 45 minut

Tematy lekcji:

1. Adresowanie klasowe (1 x 45 minut)
2. Adresowanie bezklasowe (2 x 45 minut)
3. Wybrane usługi sieciowe związane z adresacją IP (2 x 45 minut)

LEKCJA NR 1

TEMAT: Adresowanie klasowe

Streszczenie

Lekcja obejmuje następujące treści:

- Organizacje związane z adresowaniem IP
- Adresowanie fizyczne
- Rodzaje transmisji IP
- Format adresu IPv4
- Rodzaje adresów IPv4
- Klasy adresów IPv4
- Adresy zarezerwowane

Podstawa programowa

Etap edukacyjny: IV, przedmiot: informatyka (poziom rozszerzony)

Cele kształcenia – wymagania ogólne

I. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem, wykorzystanie sieci komputerowej; komunikowanie się za pomocą komputera i technologii informacyjno-komunikacyjnych.

Treści nauczania – wymagania szczegółowe

1. Korzystanie z sieci komputerowej. Uczeń:
   3) przedstawia warstwowy model sieci komputerowych, określa ustawienia sieciowe danego komputera i jego lokalizacji w sieci, opisuje zasady administrowania siecią komputerową w architekturze klient-serwer, prawidłowo posługuje się terminologią sieciową, korzysta z usług w sieci komputerowej, lokalnej i globalnej, związanych z dostępem do informacji, wymianą informacji i komunikacją.

Cel

Uświadomienie uczniom na czym polega adresowanie IP, jakie są klasy oraz rodzaje adresów IP oraz jakie są typy transmisji.

Słowa kluczowe

adres hosta, adres IPv4, adres IPv6, adres rozgłoszenia, adres sieci, adresowanie fizyczne, adresowanie logiczne, adresowanie klasowe (klasa A, B, C, D, E), transmisja broadcast, transmisja multicast, transmisja unicast

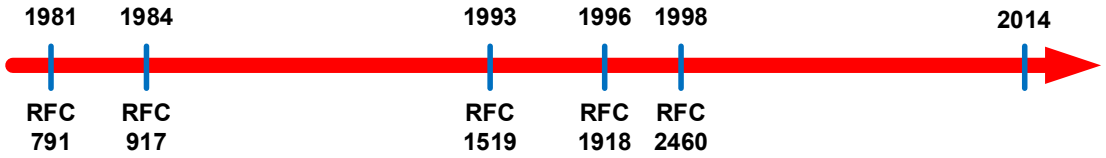
Co przygotować

- Skorzystać z literatury wymienionej w scenariuszu (opcjonalnie)
- Prezentacja 1 – Adresowanie IP

- Zadania 1

MATERIAŁ TEORETYCZNY

Rys historyczny



Rysunek 1. Wybrane fakty istotnie związane z adresowaniem IP

W roku 1981 dokumencie RFC nr 791 zdefiniowano ostatecznie protokół IPv4 jako 32-bitowa liczba binarna, zapisywana w notacji kropkowo-dziesiętnej. W roku 1984 w dokumencie RFC 917 określono pojecie 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 wydanym w roku 1996 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-bitowa liczba binarna, zapisywana 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 całego systemu numeracji i nazewnictwa adresów internetowych był Jon Postel.
- **ICANN** (ang. The Internet Corporation for Assigned Names and Numbers) – instytucja ta została powołana do życia 18 września 1998 roku w celu przejęcia od rządu USA funkcji nadzorowania technicznych aspektów Internetu (przejęcia obowiązków od IANA).

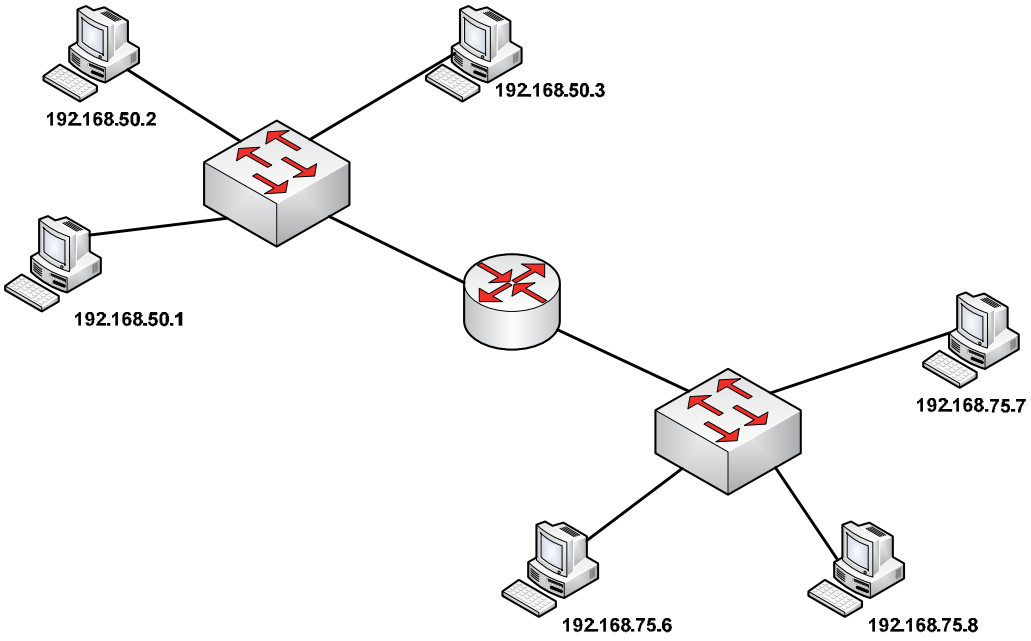
Formalnie ICANN jest prywatną organizacją typu non-profit o statusie firmy zarejestrowanej w stanie Kalifornia, której rząd USA przekazał czasowo prawo nadzoru nad systemem DNS, przydziałem puli adresów IPv4 oraz IPv6 dla tzw. *Regional Internet Registries* (RIR) oraz rejestracją numerów portów.

Na czym polega adresowanie fizyczne

Rysunek 2. Karty sieciowe

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). Adres MAC składa się z 48 bitów i zapisywany jest przeważnie szesnastkowo.

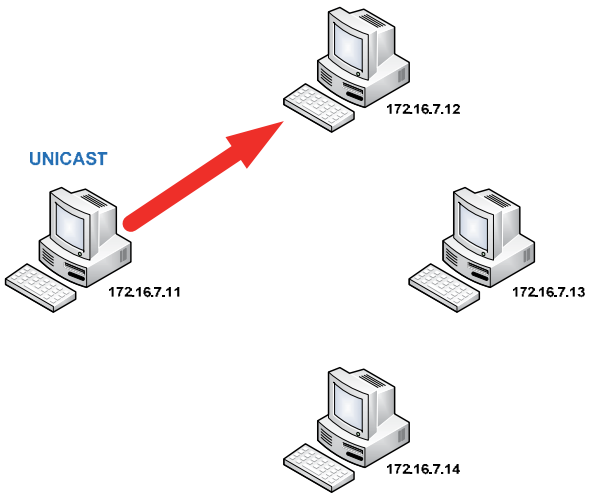
Na czym polega adresowanie logiczne



Rysunek 3. Przykład adresowania logicznego

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).

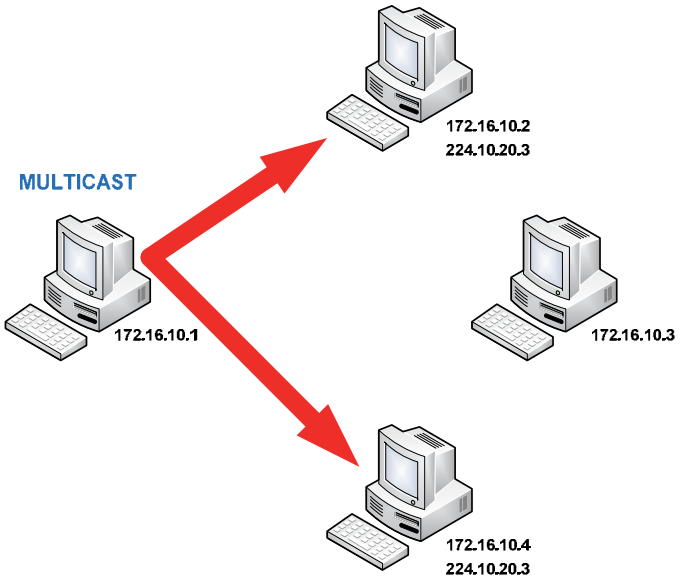
Transmisja unicast



Rysunek 4. Transmisja typu unicast

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

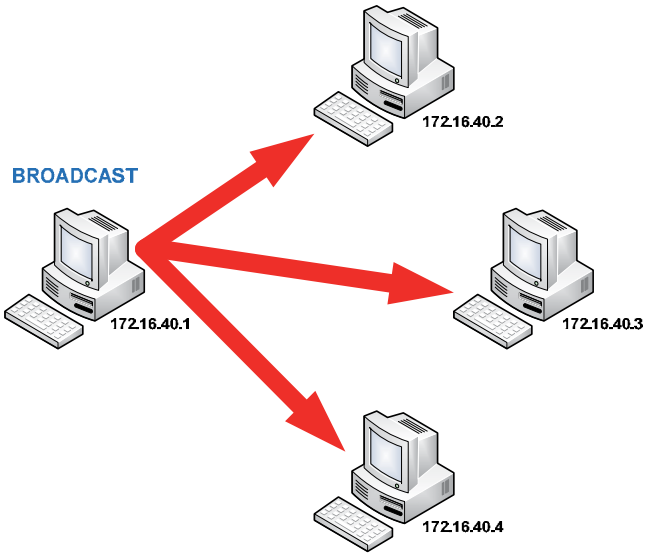
Transmisja multicast



Rysunek 5. Transmisja typu multicast

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

Transmisja broadcast



Rysunek 6. Transmisja typu 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.

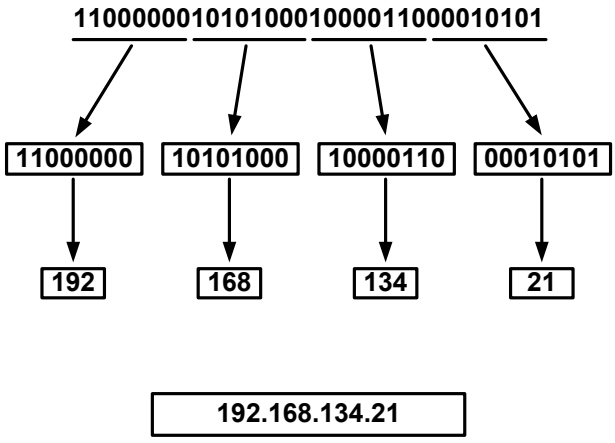
Ewolucja zapisu adresów IPv4

- 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 zapisywane były binarnie. Z uwagi na fakt, że istniało niewiele hostów system ten był do zaakceptowania. Jednak w miarę zwiększania się ilości hostów w Internecie powyższy system adresowania był bardzo niewygodny. Dlatego postanowiono zapis binarny przekonwertować do systemu dziesiętnego.

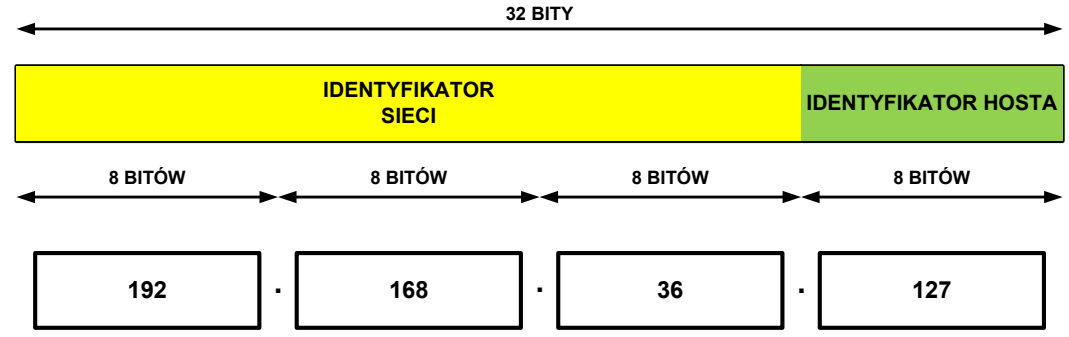
Notacja kropkowo-dziesiętna



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

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).

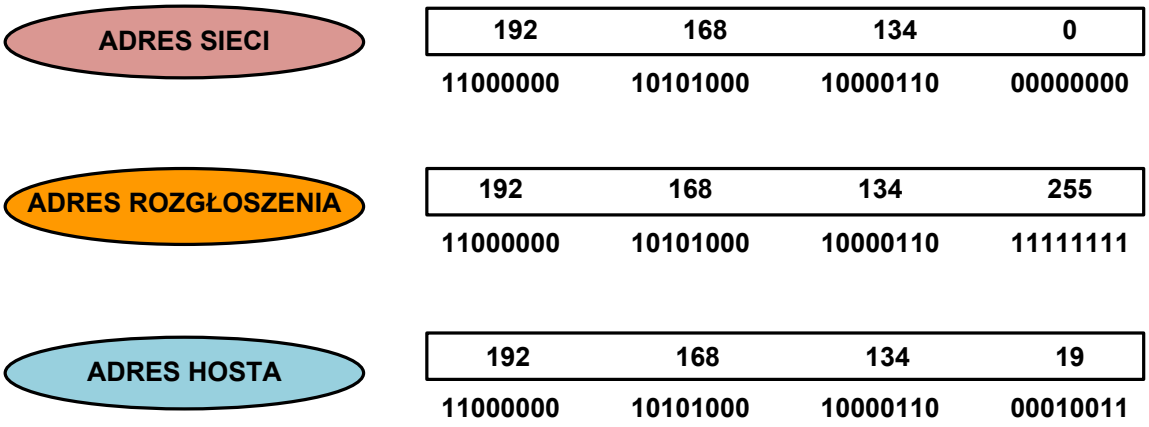
Format adresu IPv4



Rysunek 8. Format adresu IP w wersji 4

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

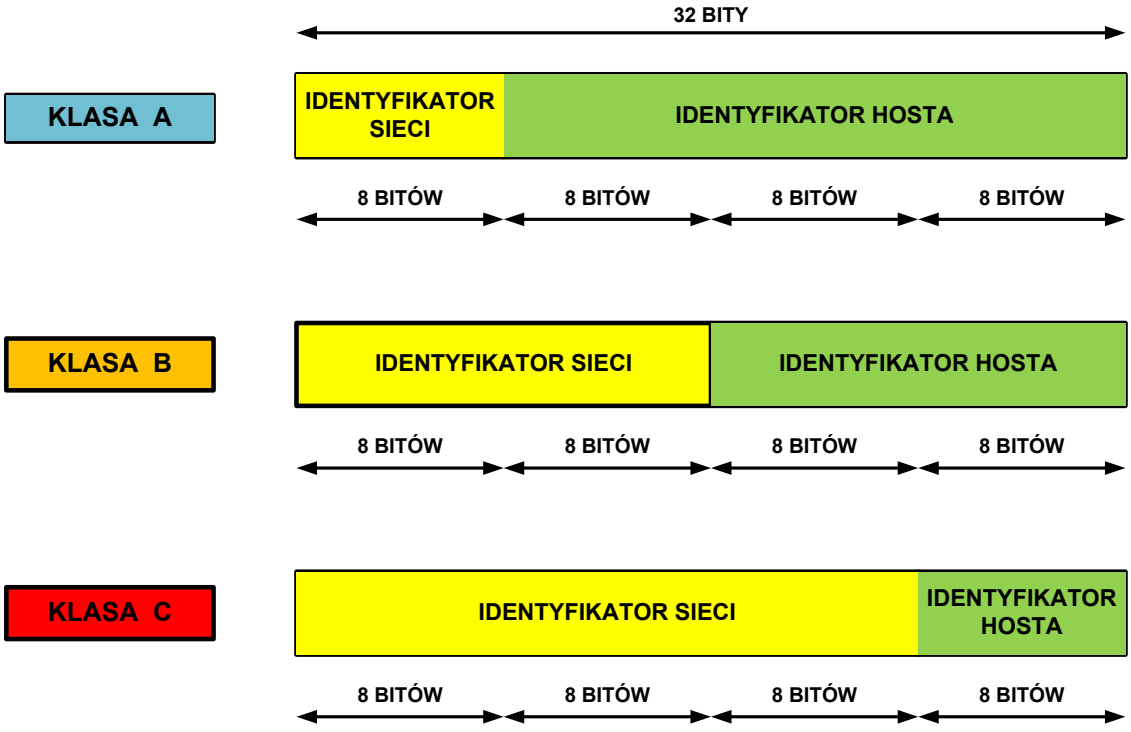
Rodzaje adresów IPv4



Rysunek 9. Rodzaje adresów IP w wersji 4

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

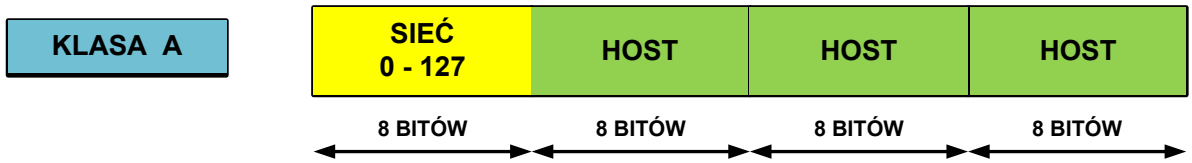
Klasy adresów IPv4



Rysunek 10. Klasy adresów IP w wersji 4

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.

Klasa A



Rysunek 11. Klasa A

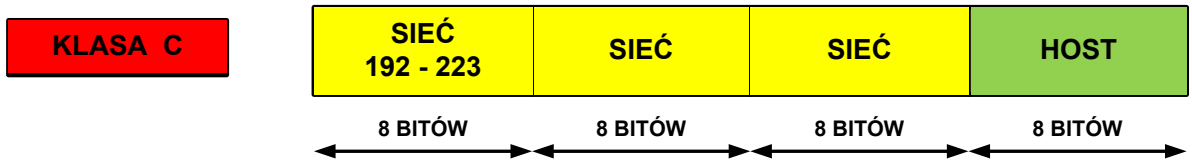
klasa A – pierwszy bit adresu jest równy 0, a następne 7 bitów określa sieć. Kolejne 24 bity wskazują komputer w tych sieciach. Adres rozpoczyna się liczbą między 0 i 127. Można zaadresować 126 użytecznych sieci (sieć 0.0.0.0 oraz 127.0.0.0 zostały zarezerwowane dla specjalnych celów) po 16 777 214 (2^24 – 2) komputerów.

Klasa B

Rysunek 12. 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.

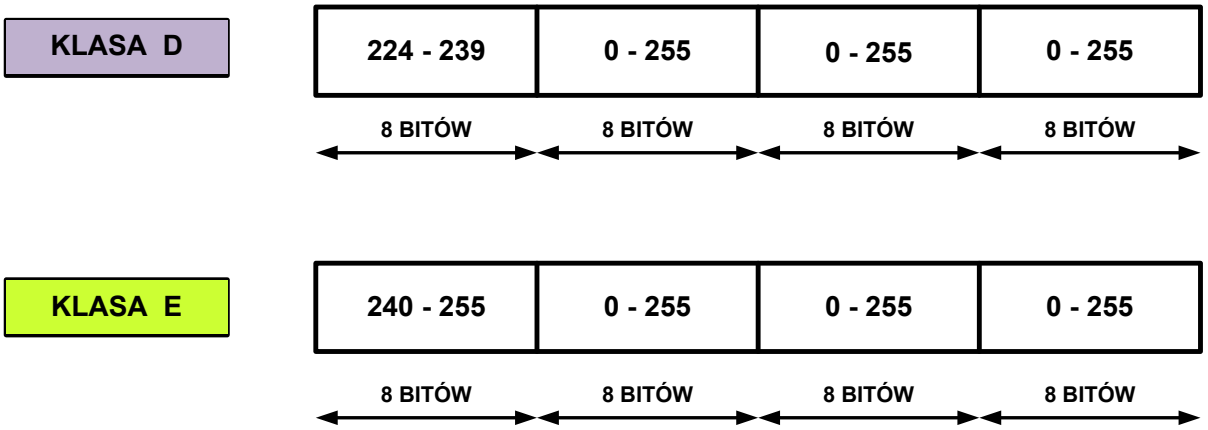
Klasa C



Rysunek 13. 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.

Klasa D i E

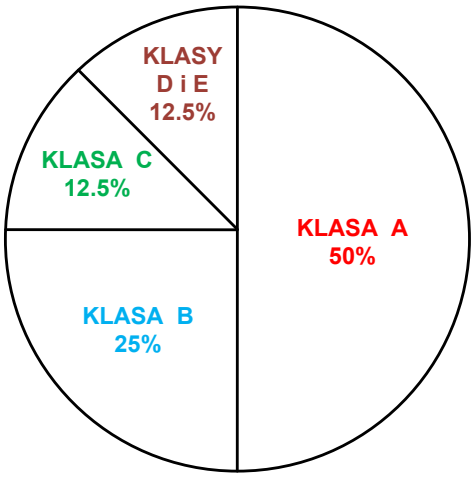


Rysunek 14. Klasa D i E

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.

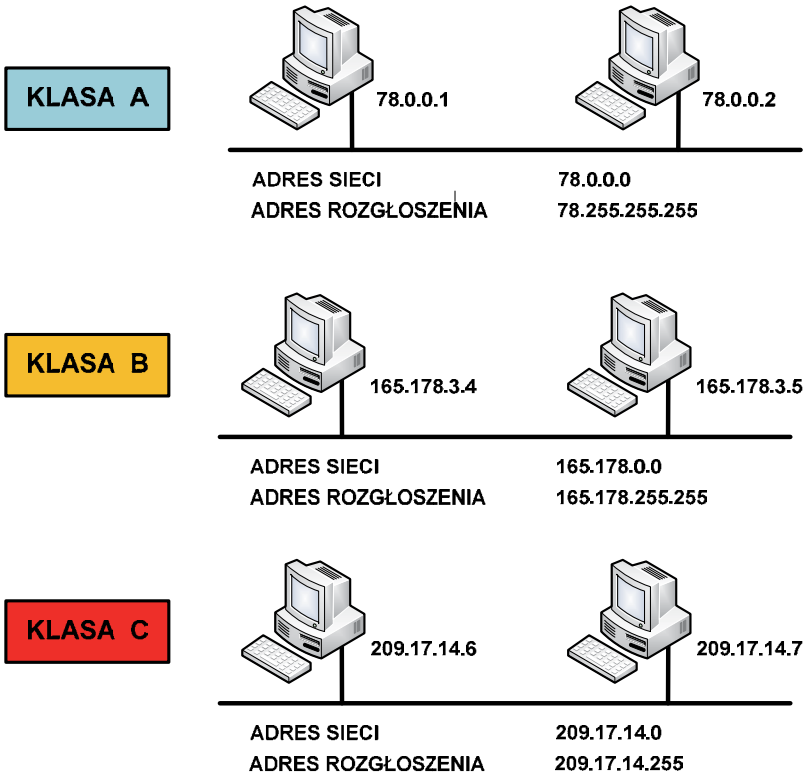
Alokacja adresów IPv4



Rysunek 15. Alokacja adresów IP w wersji 4

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).

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 zastosowanie jest w jakimś stopniu ograniczone. Ograniczenie to polega na ich zastosowaniu jedynie w lokalnych sieciach LAN.

255.255.255.255 – ten adres 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 (*localhost*). Adres ten jest często określany adresem pętli zwrotnej (*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.

Literatura

1. Dye M. A., McDonald R., W. Rufi A., *Akademia sieci Cisco. CCNA Exploration. Semestr 1*, Wydawnictwo Naukowe PWN, Warszawa, 2008
2. Halska B., Bensel P., *Projektowanie lokalnych sieci komputerowych i administrowanie sieciami, Część 1*, Helion, Gliwice, 2012
3. Halska B., Bensel P., *Projektowanie lokalnych sieci komputerowych i administrowanie sieciami, Część 2*, Helion, Gliwice, 2012

Przebieg zajęć

Wprowadzenie (10 minut)

Omówienie wprowadzenia teoretycznego do niniejszej lekcji, przy użyciu przygotowanej prezentacji.

Praca indywidualna lub w zespołach (30 minut)

Praca indywidualna lub zespoły dwuosobowe.

Uczniowie wykonują ćwiczenia, korzystając w razie potrzeby z treści wprowadzenia teoretycznego do niniejszej lekcji.

Dyskusja podsumowująca (5 minut)

Omówienie rezultatów pracy – efektów wykonania ćwiczeń.

Sprawdzenie wiedzy

Ćwiczenie 1.1

Ćwiczenie 1.2

Ćwiczenie 1.3

Ćwiczenie 1.4

Dostępne pliki

1. Prezentacja 1 – Adresowanie IP
2. Ćwiczenia 1.1-1.4 (Zadania 1)

LEKCJA NR 2

TEMAT: Adresowanie bezklasowe

Streszczenie

Lekcja omawia następujące treści:

- Standardowe maski podsieci
- Określanie identyfikatora sieci
- Podział sieci na podsieci
- Sumaryzacja tras
- Format adresu IPv6

Podstawa programowa

Etap edukacyjny: IV, przedmiot: informatyka (poziom rozszerzony)

Cele kształcenia – wymagania ogólne

I. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem, wykorzystanie sieci komputerowej; komunikowanie się za pomocą komputera i technologii informacyjno-komunikacyjnych.

Treści nauczania – wymagania szczegółowe

1. Korzystanie z sieci komputerowej. Uczeń:
   3) przedstawia warstwowy model sieci komputerowych, określa ustawienia sieciowe danego komputera i jego lokalizacji w sieci, opisuje zasady administrowania siecią komputerową w architekturze klient-serwer, prawidłowo posługuje się terminologią sieciową, korzysta z usług w sieci komputerowej, lokalnej i globalnej, związanych z dostępem do informacji, wymianą informacji i komunikacją.

Cel

Wyjaśnienie uczniom, co to jest maska podsieci oraz jak można dzielić sieć na podsieci, a także wyjaśnić schemat adresowania IPv6.

Słowa kluczowe

adres hosta, adres IPv4, adres IPv6, adres rozgłoszenia, adres sieci, aaska podsieci

Co przygotować

- Skorzystać z literatury wymienionej w scenariuszu (opcjonalnie)
- Prezentacja 2 – Adresowanie IP

- Zadania 2

MATERIAŁ TEORETYCZNY

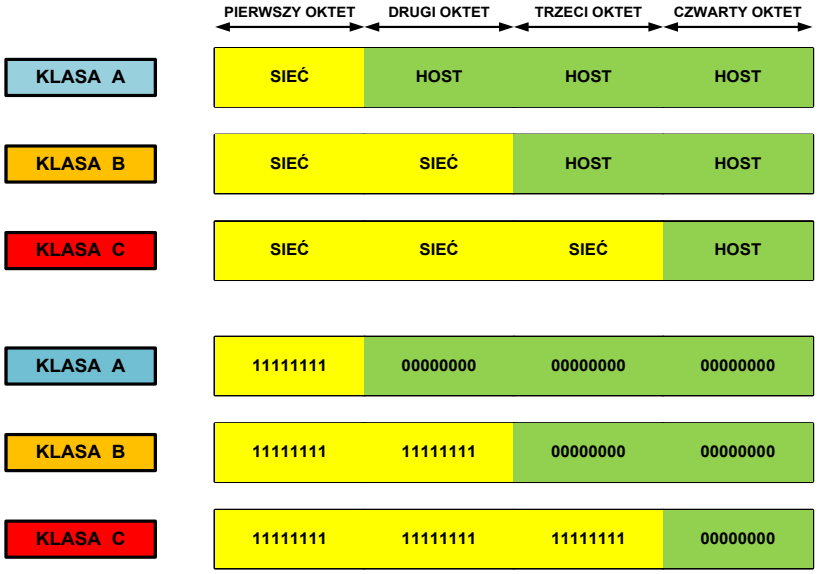
Wprowadzenie do adresowania bezklasowego

Przy gwałtownym wzroście zapotrzebowania podział adresów na klasy A, B i C okazał się bardzo nieekonomiczny. Dlatego obecnie powszechnie stosowany jest 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 oznacza liczbę możliwych do zaadresowania hostów.

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

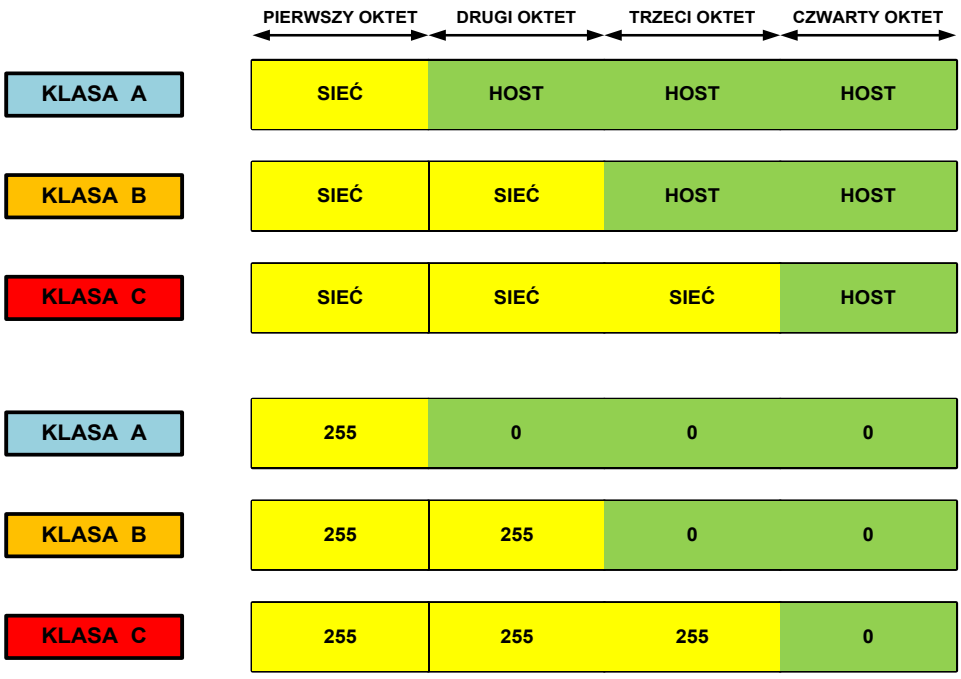
Standardowe maski podsieci w postaci binarnej



Rysunek 17. Standardowe maski podsieci w zapisie binarnym

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.

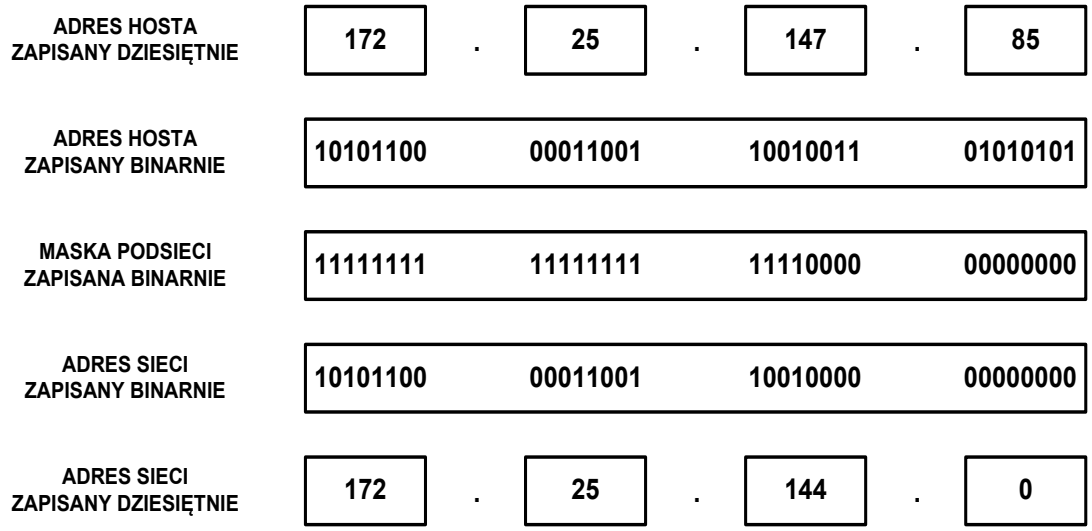
Standardowe maski podsieci w notacji dziesiętnej



Rysunek 18. Standardowe maski podsieci w zapisie dziesiętnym

W przypadku notacji dziesiętnej (patrz rys. 18) maski podsieci w części identyfikatora sieci mają wartość 255, a 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.

Określanie identyfikatora sieci



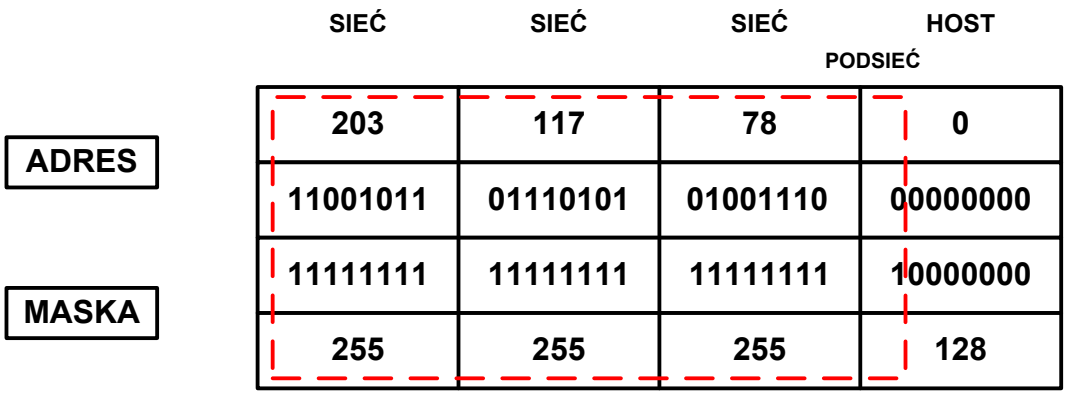
Rysunek 19. Określanie identyfikatora sieci

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 pytanie: Jaki jest identyfikator sieci dla hosta o adresie 172.25.147.85 z maską podsieci 255.255.240.0, odpowiedź brzmi: 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).

Podział na podsieci

Podział na podsieci z maską 25-bitową



Rysunek 20. Maska 25-bitowa

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.

Podział na podsieci z maską 26-bitową

	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

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.

Podział na podsieci z maską 27-bitową

	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

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.

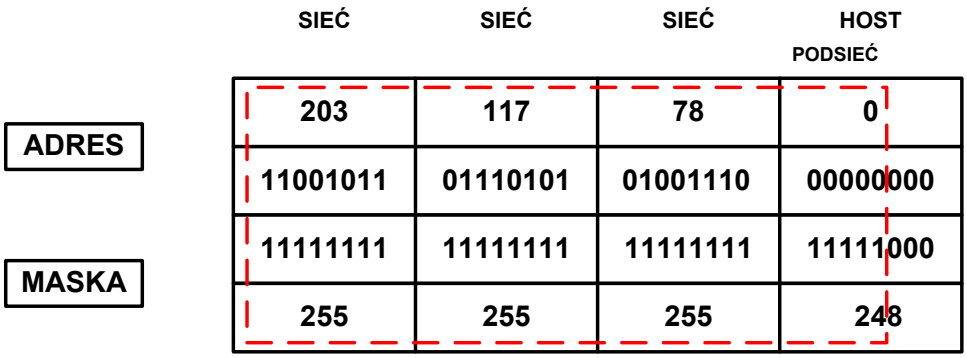
Podział na podsieci z maską 28-bitową

	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

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.

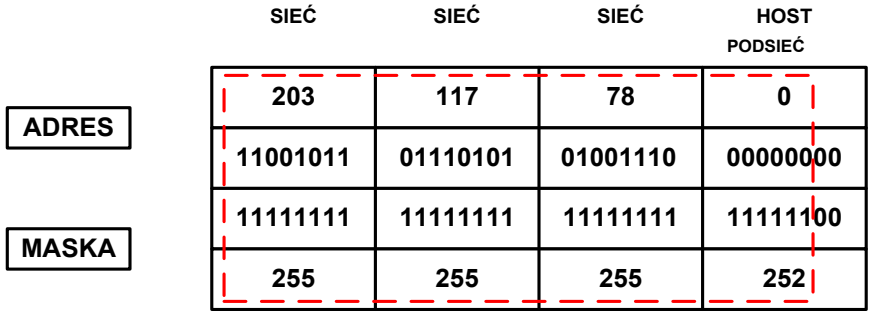
Podział na podsieci z maską 29-bitową



Rysunek 24. Maska 29-bitowa

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.

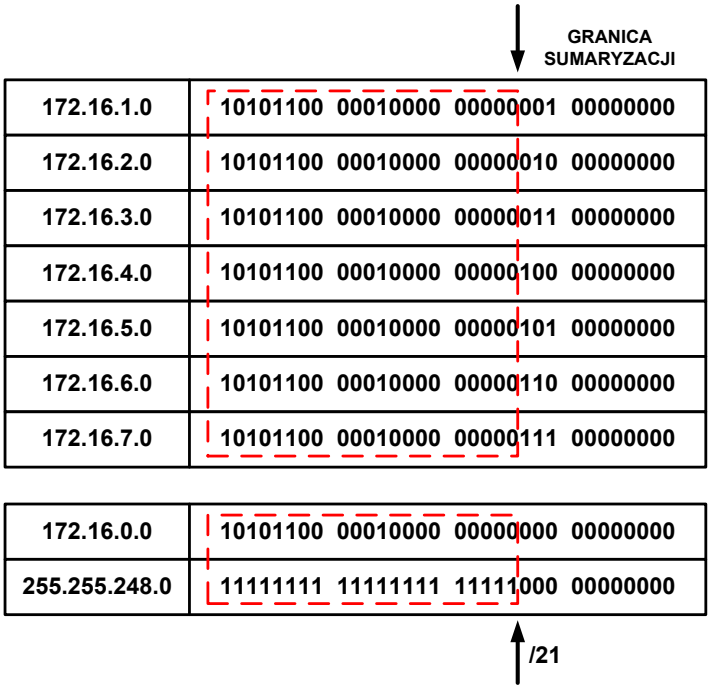
Podział na podsieci z maską 30-bitową



Rysunek 25. Maska 30-bitowa

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.

Sumaryzacja tras



Rysunek 26. Przykład sumaryzacji 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 powyższym przykładzie 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 (patrz rys. 26).

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 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 konwertowany jest 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

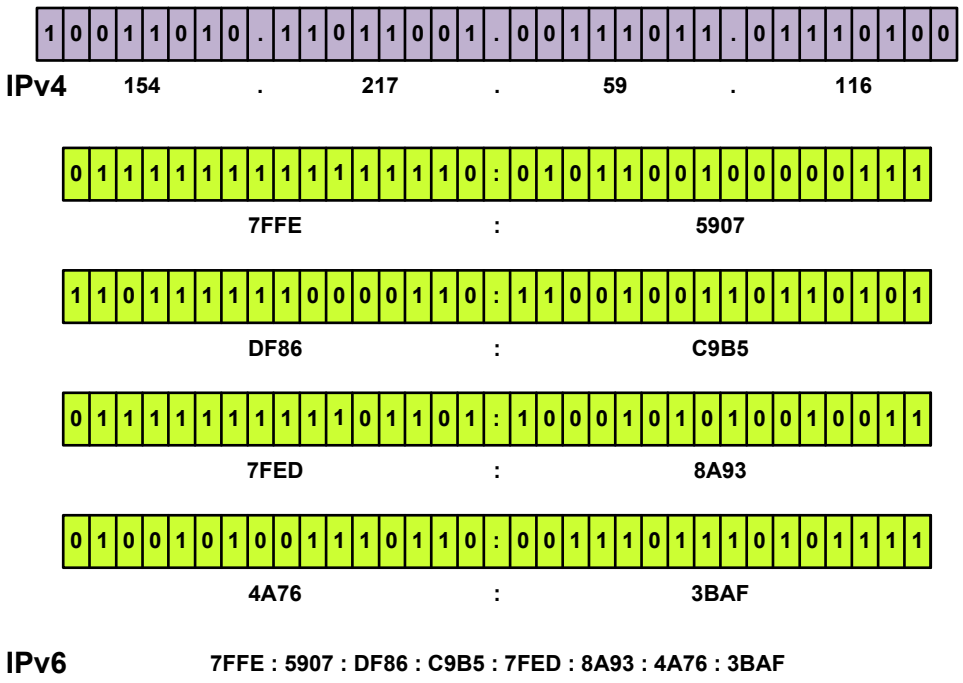
21DA : D3 : 0000 : 2F3B : 2AA : 0000 : 0000 : 9C5A
21DA : D3 : 0 : 2F3B : 2AA : 0000 : 0000 : 9C5A
21DA : D3 : 0 : 2F3B : 2AA :: 9C5A

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 27. Przykłady uproszczeń zapisu adresów IPv6

Porównanie adresów IPv4 i IPv6



Rysunek 28. Porównanie zapisu adresów IPv4 i IPv6

Adres IPv4 jest adresem 32-bitowym, natomiast adres IPv6 – 128-bitowym. Adres IPv4 składa się z czterech oktetów liczb binarnych, natomiast adres IPv6 składa się z ośmiu 16-bitowych bloków. Adres IPv4 zapisywany jest w notacji kropkowo-dziesiętnej, natomiast adres IPv6 zapisywany jest w notacji dwu-kropkowo-szesnastkowej.

Adres IPv4 daje pulę 4 294 967 296 adresów, natomiast adres IPv6 dostarcza 3.4 x 1038 adresów.

Literatura

1. Dye M. A., McDonald R., W. Rufi A., *Akademia sieci Cisco. CCNA Exploration. Semestr 1*, Wydawnictwo Naukowe PWN, Warszawa, 2008
2. Halska B., Bensel P., *Projektowanie lokalnych sieci komputerowych i administrowanie sieciami, Część 1*, Helion, Gliwice, 2012
3. Halska B., Bensel P., *Projektowanie lokalnych sieci komputerowych i administrowanie sieciami, Część 2*, Helion, Gliwice, 2012

Przebieg zajęć

Wprowadzenie (2 x 10 minut [po 10 minut na początku każdej lekcji])

Omówienie wprowadzenia teoretycznego do niniejszej lekcji, przy użyciu przygotowanej prezentacji.

Praca indywidualna (2 x 30 minut [po 30 minut na początku każdej lekcji])

Uczniowie wykonują ćwiczenia, korzystając w razie potrzeby z treści wprowadzenia teoretycznego do niniejszej lekcji.

Dyskusja podsumowująca (2 x 5 minut [po 5 minut na koniec każdej lekcji])

Omówienie rezultatów pracy – efektów wykonania ćwiczeń.

Sprawdzenie wiedzy

Ćwiczenie 2.1

Ćwiczenie 2.2

Ćwiczenie 2.3

Ćwiczenie 2.4

Ćwiczenie 2.5

Ćwiczenie 2.6

Dostępne pliki

1. Prezentacja 2
2. Ćwiczenie 2.1-2.6 (Zadania 2)

LEKCJA NR 3

TEMAT: Wybrane usługi sieciowe związane z adresacją IP

Streszczenie

Treść lekcji obejmuje następujące zagadnienia:

- Statyczna translacja NAT
- Dynamiczna translacja NAT
- Translacja PAT
- Podstawy działania DHCP
- Wymiana komunikatów DHCP
- Adresy domenowe
- Działanie usługi DNS

Podstawa programowa

Etap edukacyjny: IV, przedmiot: informatyka (poziom rozszerzony)

Cele kształcenia – wymagania ogólne

I. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem, wykorzystanie sieci komputerowej; komunikowanie się za pomocą komputera i technologii informacyjno-komunikacyjnych.

Treści nauczania – wymagania szczegółowe

1. Korzystanie z sieci komputerowej. Uczeń:
   3) przedstawia warstwowy model sieci komputerowych, określa ustawienia sieciowe danego komputera i jego lokalizacji w sieci, opisuje zasady administrowania siecią komputerową w architekturze klient-serwer, prawidłowo posługuje się terminologią sieciową, korzysta z usług w sieci komputerowej, lokalnej i globalnej, związanych z dostępem do informacji, wymianą informacji i komunikacją.

Cel

Wyjaśnienie zasad działania wybranych usług sieciowych (NAT, PAT, DHCP, DNS) związanych z adresowaniem IP.

Słowa kluczowe

usługa sieciowa DHCP, usługa sieciowa, adres globalny, adres lokalny, sieć wewnętrzna, sieć zewnętrzna, wewnętrzny adres globalny, wewnętrzny adres lokalny, zewnętrzny adres globalny, zewnętrzny adres lokalny

Co przygotować

- Skorzystać z literatury wymienionej w scenariuszu (opcjonalnie)
- Prezentacja 3 – Adresowanie IP

- Zadania 3
- Test sprawdzający wiedzę ze wszystkich lekcji

- Film 1 – Podstawy adresowania IP.avi

MATERIAŁ TEORETYCZNY

Adresy prywatne

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

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.

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 wewnętrzne adresy 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. Operacja ta wykonywana jest przez znajdujące się między sieciami urządzenia, na których działa wyspecjalizowane oprogramowanie obsługujące funkcję NAT, pozwalające na 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*) – wewnętrzna lokalna sieć komputerowa danej firmy lub przedsiębiorstwa.

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

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

Adres globalny (ang. *global address*) – tego adresu używają hosty z różnych sieci.

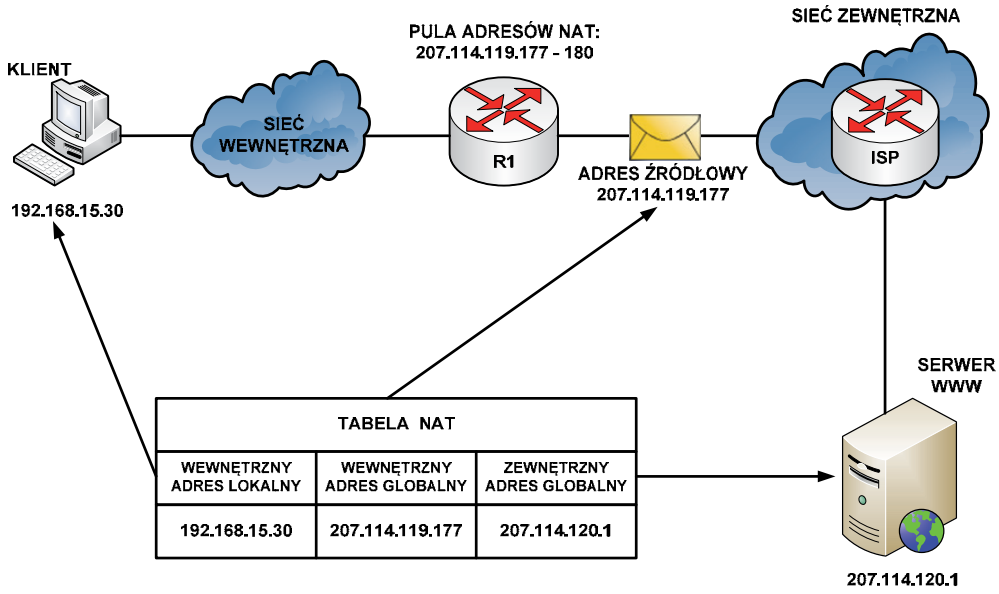
Wewnętrzny adres lokalny (ang. *inside local address*) – adres IP przypisany do hosta w sieci wewnętrznej. Najczęściej jest to adres prywatny zgodny ze standardem RFC 1918.

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

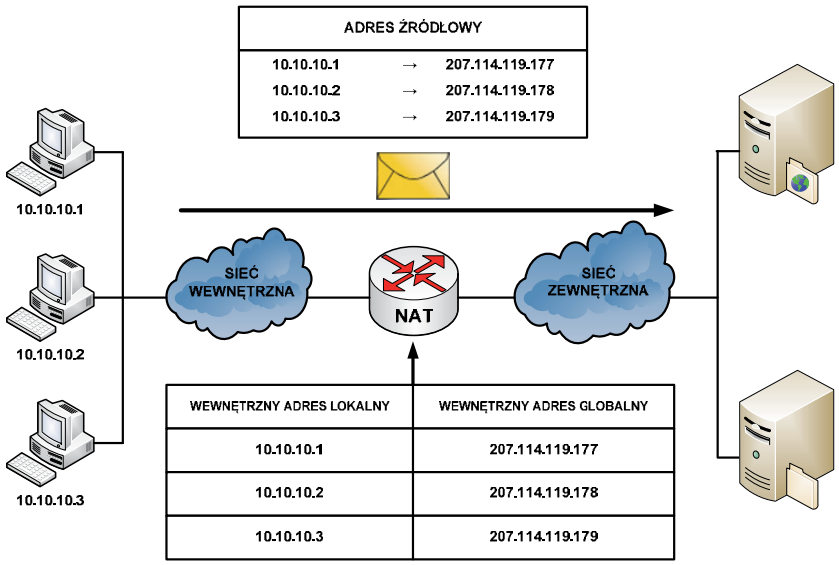


Rysunek 29. Działanie translacji NAT

Na rysunku 29 wyjaśniono 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).
- 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

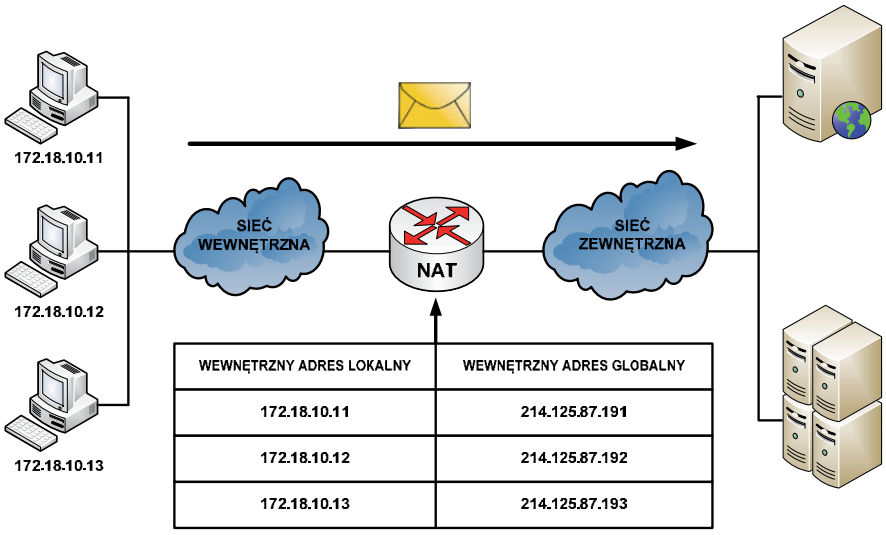


Rysunek 30. Statyczna translacja NAT

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 widzimy, 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).

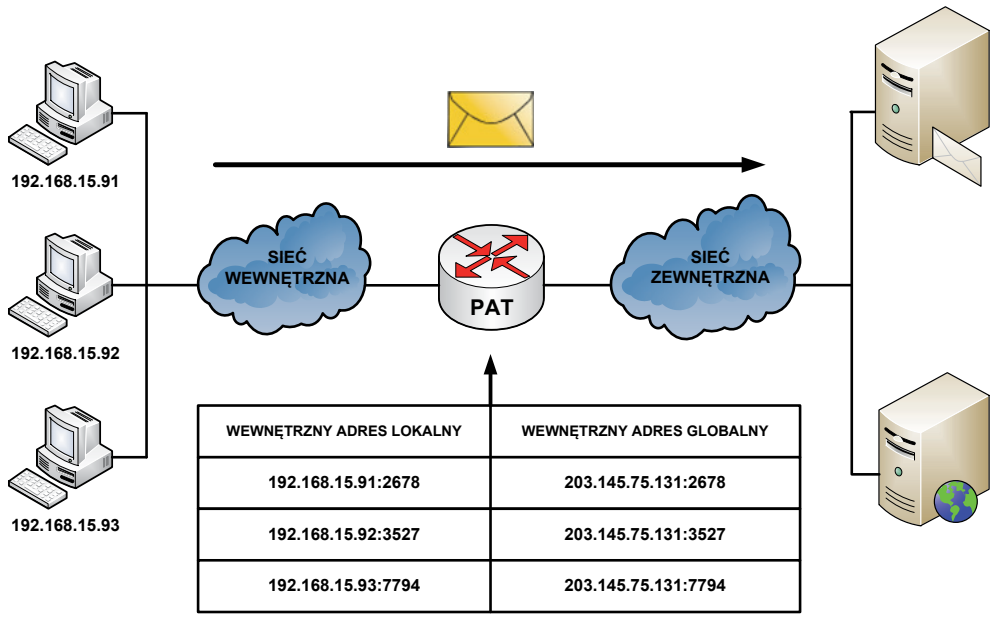
Dynamiczna translacja NAT



Rysunek 31. Dynamiczna translacja NAT

Dynamiczna translacja NAT (ang. *dynamic NAT*) – 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 administratora sieci spada obowiązek zadbania o odpowiedni zakres puli adresów publicznych, aby możliwa była 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.

Translacja PAT



Rysunek 32. Translacja PAT

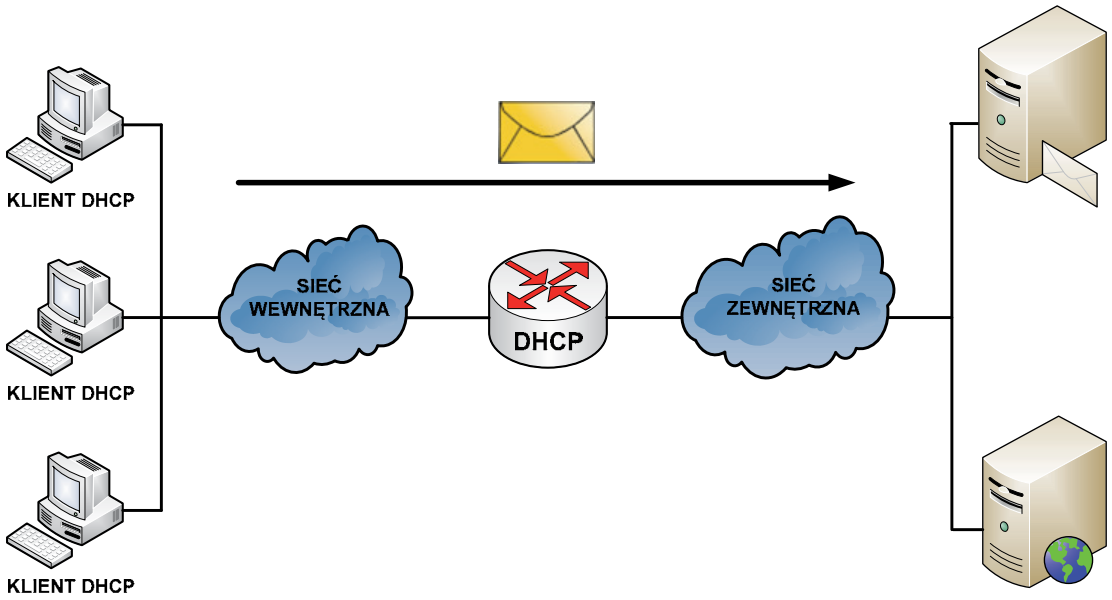
Translacja PAT (ang. *Port Address Translation*) – rys. 32 – służy do odwzorowania wielu prywatnych adresów IP na jeden publiczny adres IP. Istnieje możliwość odwzorowania wielu adresów na jeden adres IP, ponieważ z każdym adresem prywatnym związany jest inny numer portu. W technologii PAT tłumaczone 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 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.

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 wypadku 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.

Podstawy działania DHCP



Rysunek 33. Działanie usługi dynamicznego przydzielania adresów IP

Usługa DHCP (ang. *Dynamic Host Configuration Protocol*) – 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.

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 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 zdefi-

niowanych pul adresów. Na serwerach DHCP mogą być dostępne także inne informacje, takie jak adresy serwerów DNS, adresy serwerów WINS i nazwy domen. W wypadku 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. Klient wysyła komunikaty do serwera na port 67. Serwer wysyła komunikaty do klienta na port 68.

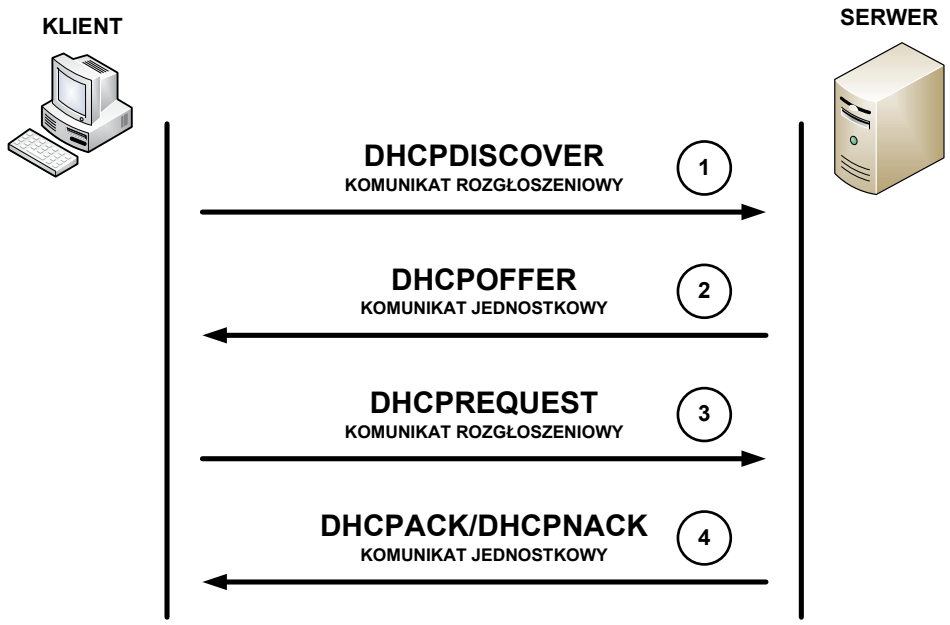
Sposoby przydzielania adresów IP

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 czas.

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



Rysunek 34. 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.
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 żąda-

nie dalej, do innego serwera DHCP. Jeżeli natomiast 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 serwer 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.

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 niedające się zlokalizować w konkretnym państwie (np. NATO);

net – firmy i organizacje zajmujące się administrowaniem i utrzymywaniem sieci komputerowych (np. EARN);

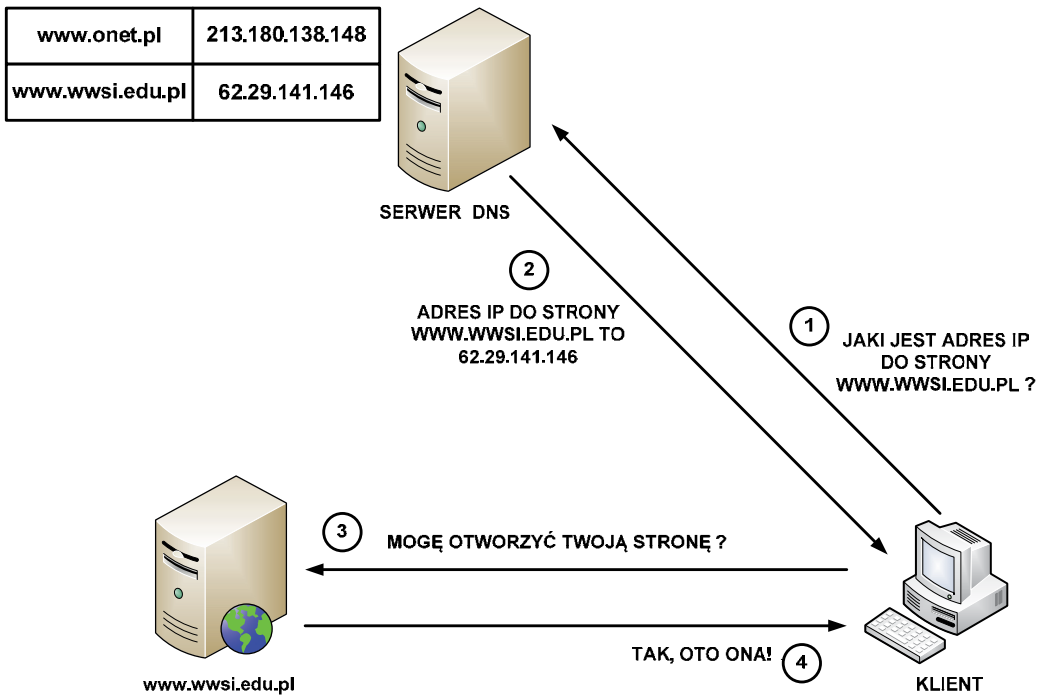
biz – biznes;

info – informacje;

name – nazwy indywidualne;

pro – zawody.

Działanie usługi DNS



Rysunek 35. Przykład działania usługi DNS

Działanie usługi DNS sprowadza się do następujących kolejnych 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 dla strony www.wwsi.edu.pl odpowiada adres IP o wartości 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.

Literatura

1. Dye M. A., McDonald R., W. Rufi A., *Akademia sieci Cisco. CCNA Exploration. Semestr 1*, Wydawnictwo Naukowe PWN, Warszawa, 2008
2. Halska B., Bensel P., *Projektowanie lokalnych sieci komputerowych i administrowanie sieciami, Część 1*, Helion, Gliwice, 2012
3. Halska B., Bensel P., *Projektowanie lokalnych sieci komputerowych i administrowanie sieciami, Część 2*, Helion, Gliwice, 2012

Przebieg zajęć

Wprowadzenie (2 x 10 minut [po 10 minut na początku każdej lekcji])

Omówienie wprowadzenia teoretycznego do niniejszej lekcji, przy użyciu przygotowanej prezentacji.

Praca indywidualna (2 x 30 minut [po 30 minut na początku każdej lekcji])

Uczniowie wykonują ćwiczenia, korzystając w razie potrzeby z treści wprowadzenia teoretycznego do niniejszej lekcji, tekst wprowadzenia teoretycznego, nagrania multimedialnego.

Dyskusja podsumowująca (2 x 5 minut [po 5 minut na koniec każdej lekcji])

Omówienie rezultatów pracy – efektów wykonania ćwiczeń.

Sprawdzenie wiedzy

Ćwiczenie 3.1

Ćwiczenie 3.2

Ćwiczenie 3.3

Ćwiczenie 3.4

Ćwiczenie 3.5

Ćwiczenie 3.6

Test wiedzy na zakończenie wszystkich lekcji.

Zaliczenie testu wiedzy w przypadku co najmniej połowy poprawnych odpowiedzi.

Dostępne pliki

1. Prezentacja – Adresowanie IP lekcja 3.ppt
2. Ćwiczenie 3.1-3.6 (Zadania 3)
3. Film 1 – Podstawy adresowania IP.avi
4. Test wiedzy

Człowiek - najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego