Podstawy działania wybranych usług sieciowych

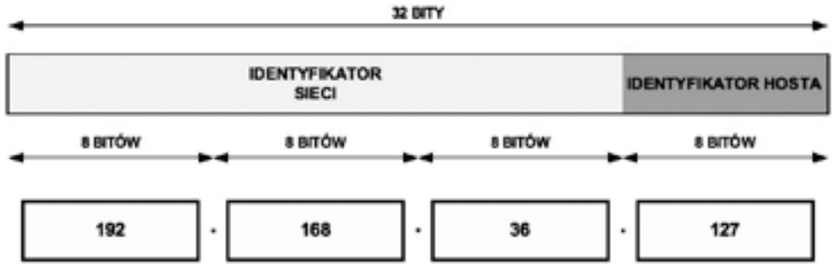
Dariusz Chaładyniak
Warszawska Wyższa Szkoła Informatyki
dchalad@wwsi.edu.pl

Streszczenie
Istnieje wiele dostępnych usług sieciowych, z których możemy korzystać, gdy mamy komputer wpięty do sieci komputerowej. Wykład omawia trzy wybrane usługi sieciowe, których zrozumienie opiera się na podstawowej wiedzy związanej z adresowaniem IP. Aby móc korzystać 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 właściwie zinterpretowała adres domenowy, musi być dostępna usługa odwzorowująca ten adres na adres IP zrozumiały dla oprogramowania sieciowego.

Spis treści

1 PODSTAWY ADRESOWANIA IPV4

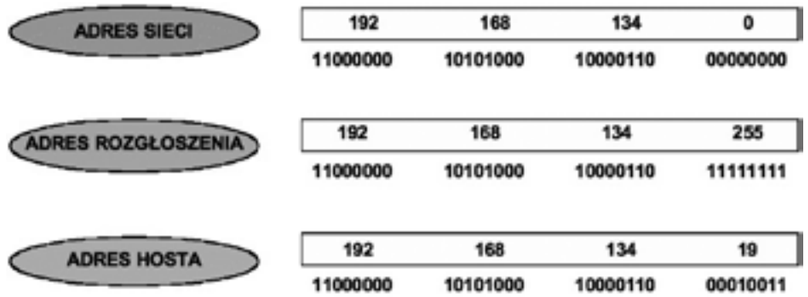
Format adresu IPv4



Rysunek 1.
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 Registry*) oraz identyfikatora hosta (zarządzanego przez administratora sieciowego).

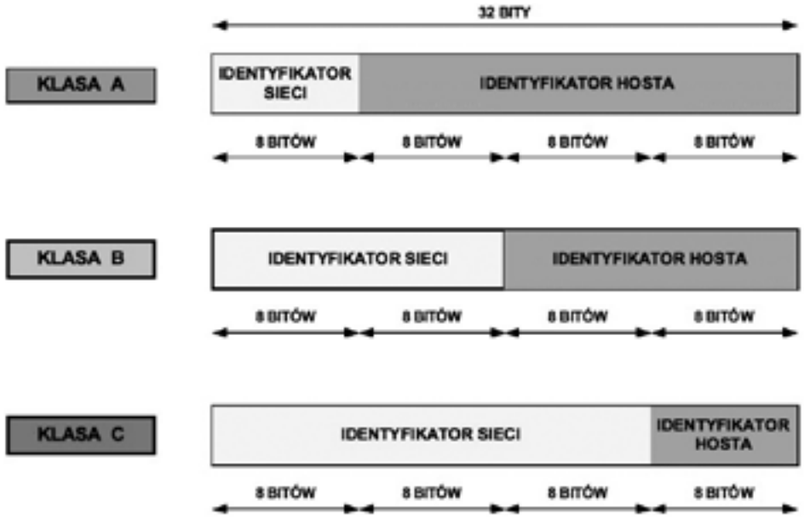
Rodzaje adresów IPv4



Rysunek 2.
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 ma same jedynki w części hostowej. **Adres hosta** jest zakresem pomiędzy adresem sieci i adresem rozgłoszenia.

Klasy adresów IPv4
W adresowaniu klasowym wyróżniono pięć klas adresowych – A, B, C, D i E. Trzy pierwsze klasy – A, B i C – wykorzystuje się do adresacji hostów w sieciach komputerowych, natomiast klasy D i E są przeznaczone dla specyficznych zastosowań.



Rysunek 3.
Klasy adresów IP w wersji 4

Adresowanie klasowe

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 4.
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 5.
Klasa B

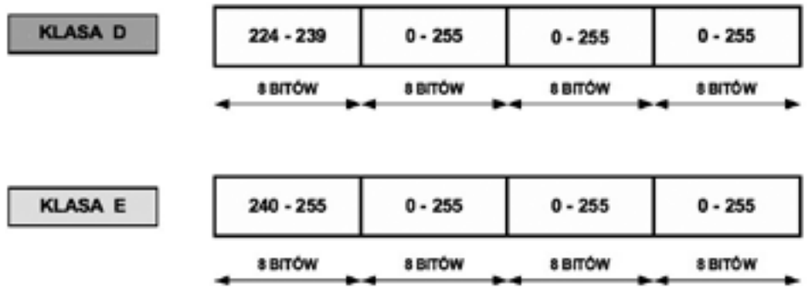
Klasa C

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 6.
Klasa C

Klasy 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.



Rysunek 7.
Klasy D i E

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.

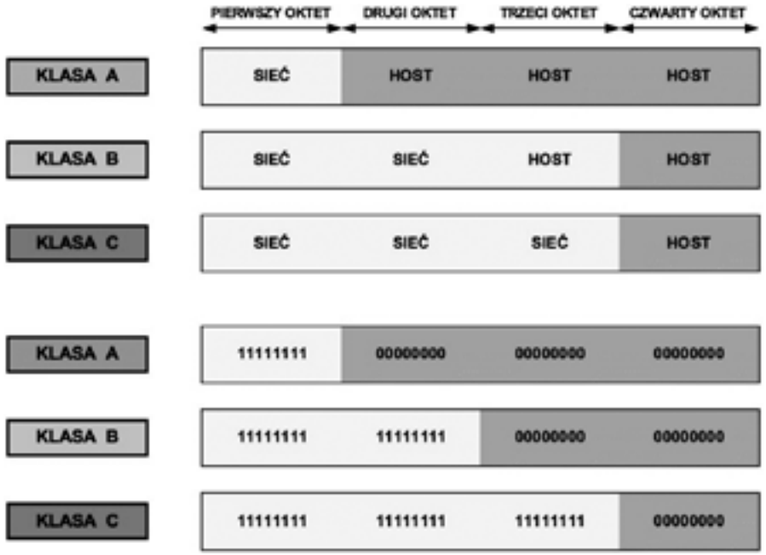
Wprowadzenie do adresowania bezklasowego

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 możliwych do zaadresowania hostów. Maskę podsieci zapisujemy podobnie jak adres IPv4 w notacji kropkowo-dziesiętnej.

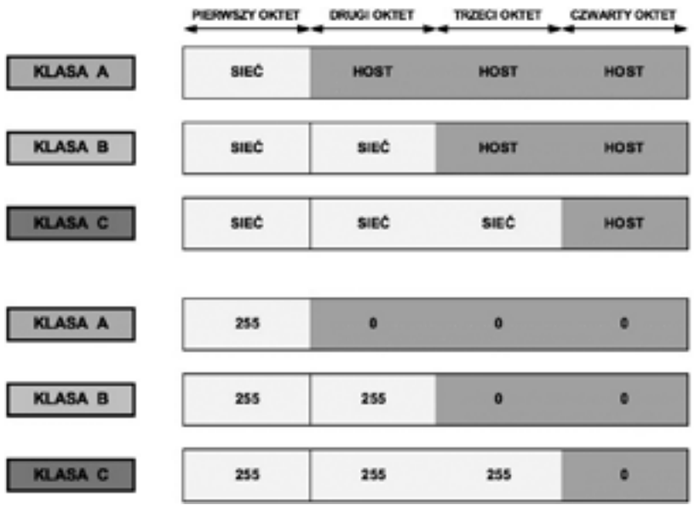
Maski podsieci można zapisywać w notacji binarnej lub dziesiętnej. W przypadku zapisu binarnego, w części identyfikatora sieci występują same jedynki, natomiast w części identyfikatora hosta znajdują się same zera.

Standardowe maski podsieci w postaci binarnej



Rysunek 8.
Standardowe maski podsieci w zapisie binarnym

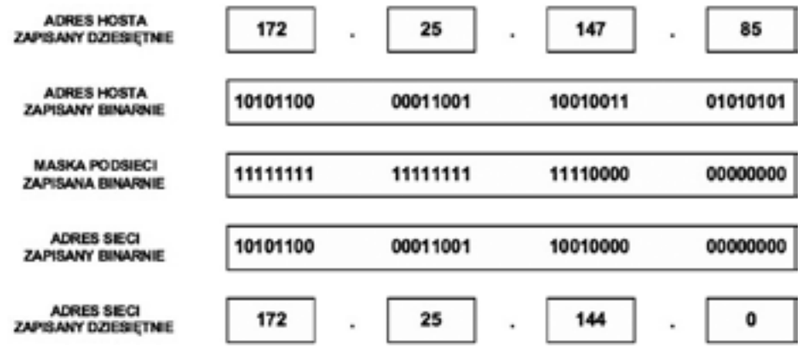
Standardowe maski podsieci w notacji dziesiętnej



Rysunek 9.
Standardowe maski podsieci w zapisie dziesiętnym

W przypadku notacji dziesiętnej, 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.

Określanie identyfikatora sieci



Rysunek 10.
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.

2 USŁUGA NAT I PAT

Adresy prywatne

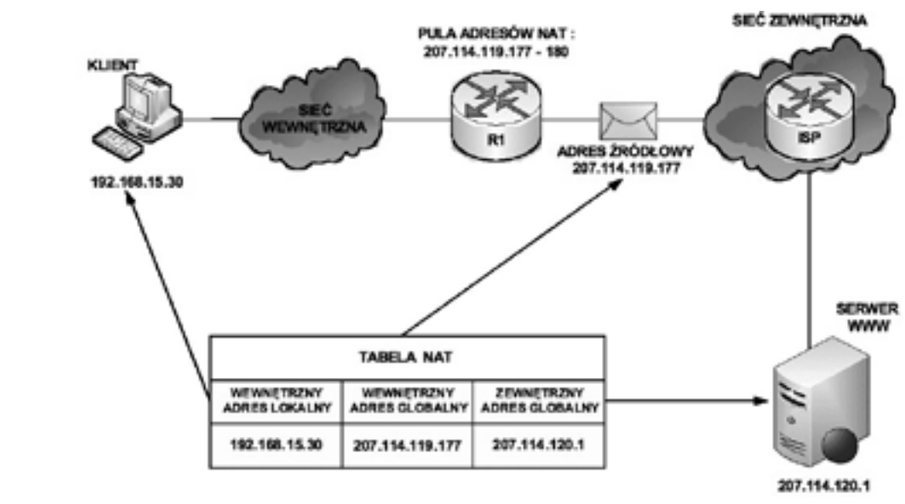
W dokumencie RFC 1918 wyróżniono trzy pule adresów IP przeznaczonych tylko do użytku prywatnego. Adresy te mogą być stosowane tylko i wyłącznie w sieci wewnętrznej. W zależności od tego, jak dużą sieć zamierzamy skonfigurować, wybieramy jedną z klas adresów (A, B lub C). Pakiety z takimi adresami nie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

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.

Działanie translacji NAT



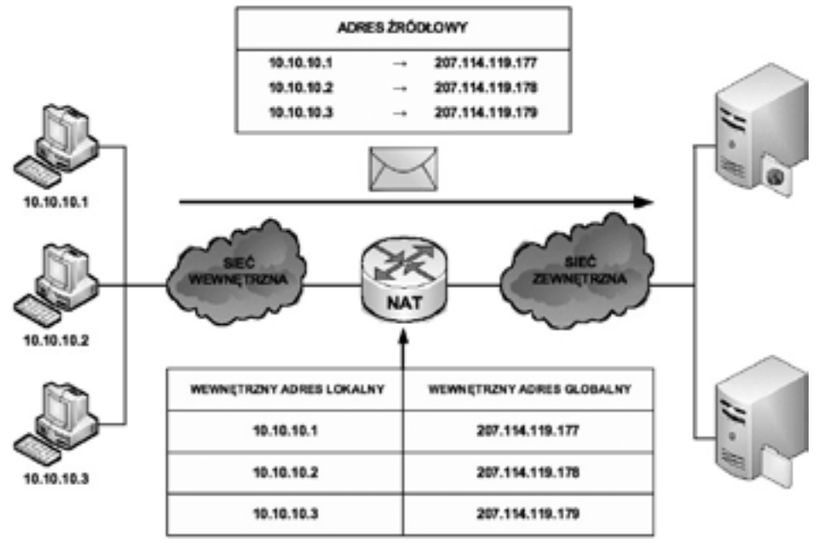
Rysunek 11.
Działanie translacji NAT

Na rysunku 11 wyjaśnione jest działanie usługi NAT (ang. *Network Address Translation*):

- 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 12.
Statyczna translacja NAT

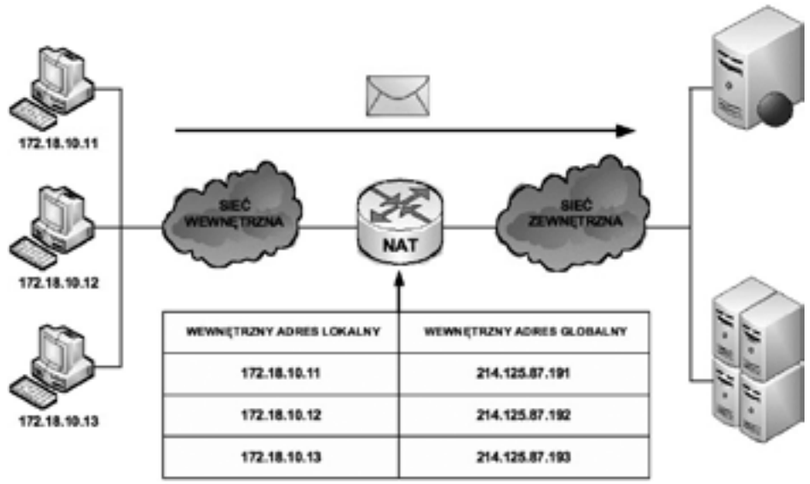
Statyczna translacja NAT (ang. *static NAT*) umożliwia utworzenie odwzorowania typu jeden-do-jednego pomiędzy adresami lokalnymi i globalnymi pomiędzy sieciami wewnętrzną i zewnętrzną. Jest to szczególnie przydatne w przypadku hostów, które muszą mieć stały adres dostępny z Internetu. Takimi wewnętrznymi 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 12 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).

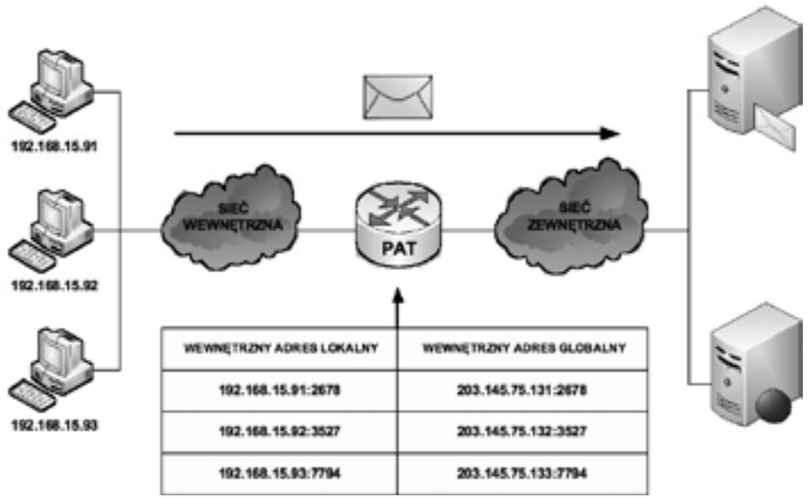
Dynamiczna translacja NAT

Dynamiczna translacja NAT (ang. *dynamic NAT*) (patrz rysunek 13) 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 możliwa była obsługa wszystkich możliwych 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.



Rysunek 13.
Dynamiczna translacja NAT



Rysunek 14.
Translacja PAT

Translacja PAT

Translacja PAT (ang. *Port Address Translation*) (patrz rysunek 14) 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.

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 adresó 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.

3 USŁUGA DHCP

Podstawy działania DHCP

Usługa DHCP (ang. *Dynamic Host Configuration Protocol*) 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 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: adresy serwerów DNS, adresy serwerów WINS i nazwy domen. W większości serwerów DHCP administratorzy mogą także zdefiniować adresy MAC obsługiwanych klientów i automatycznie przypisywać tym klientom zawsze te same adresy IP.

Rysunek 15.
Działanie usługi dynamicznego przydzielania adresów 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 klientom:

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

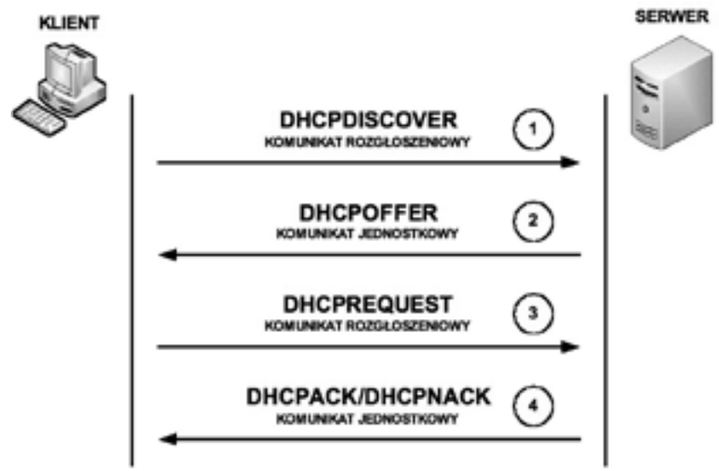
Serwer DHCP tworzy pule adresów IP i skojarzonych z nimi parametrów. Pule przeznaczone są dla poszczególnych logicznych podsieci IP. Dzięki temu jeden klient IP może uzyskiwać adresy od wielu serwerów DHCP i może być przenoszony. Jeśli klient uzyska odpowiedź od wielu serwerów, może wybrać tylko jedną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

Wymiana komunikatów protokołu DHCP

W procesie konfiguracji klienta DHCP wykonywane są następujące działania:

1. Na kliencie, który uzyskuje dostęp do 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 od serwera DHCP wcześniej. 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 żądanie dalej, do innego serwera DHCP. Jeśli serwer DHCP może obsłużyć żądanie, do klienta jest wysyłana oferta z konfiguracją IP w postaci 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.



Rysunek 16.
Wymiana komunikatów protokołu DHCP

4. Serwer, który odbierze sygnał DHCPREQUEST, publikuje określoną konfigurację, wysyłając potwierdzenie w postaci 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.

Automatyczna konfiguracja adresów IP

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

- Klikamy przycisk Start, a następnie wybieramy zakładkę Panel sterowania. W oknie, które się pojawi (rys. 17), klikamy w kategorię Połączenia sieciowe i internetowe.

Rysunek 17.
Początek automatycznego konfigurowania adresów IP

- Z kategorii Połączenia sieciowe i internetowe wybieramy Połączenia sieciowe (patrz rys. 18).

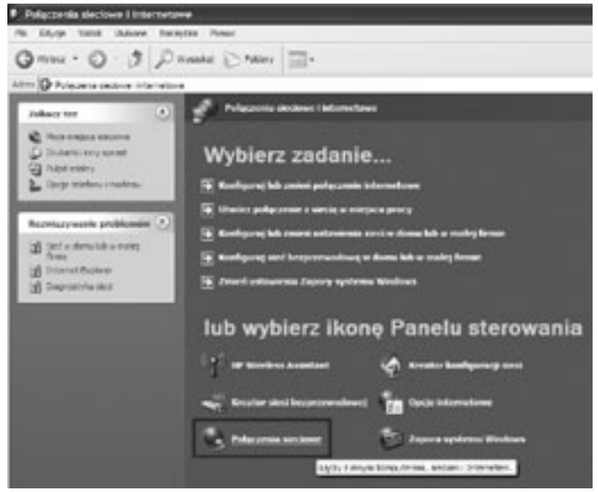
- W kategorii Połączenia sieciowe wybieramy Połączenie lokalne (patrz rys. 19).

- W oknie na rysunku 20 jest ukazany podgląd stanu Połączenia lokalnego, z którego możemy odczytać: stan połączenia, czas trwania połączenia, szybkość połączenia, a także jego aktywność (liczbę pakietów wysłanych i odebranych). W oknie tym klikamy na zakładkę Właściwości.

- Po wybraniu zakładki Właściwości ukazuje nam się kolejne okno (rys. 21), w którym wybieramy składnik Protokół internetowy (TCP/IP), a następnie klikamy w zakładkę Właściwości.

- Po wybraniu składnika Protokół internetowy (TCP/IP) i kliknięciu w zakładkę Właściwości otwiera się okno (rys. 22), w którym wybieramy następujące opcje: Uzyskaj adres IP automatycznie oraz Uzyskaj adres serwera DNS automatycznie. Po wybraniu tych opcji 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.

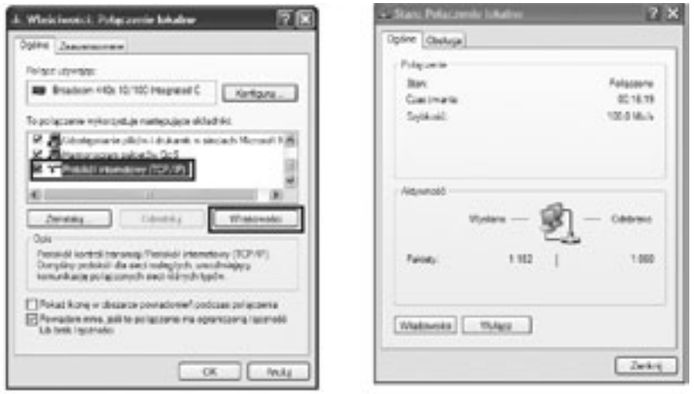
- Po kliknięciu w zakładkę Zaawansowane w oknie Właściwości: Protokół internetowy (TCP/IP) otrzymujemy podgląd w zaawansowane ustawienia stosu protokołów TCP/IP, w którym możemy zauważyć, że jest włączony serwer DHCP (patrz rys. 23).



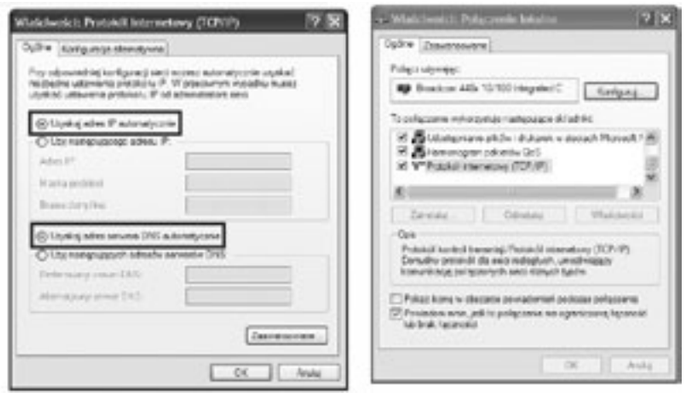
Rysunek 18.
Wybór wśród połączeń sieciowych i internetowych

Rysunek 19.
Wybór połączenia lokalnego wśród połączeń sieciowych

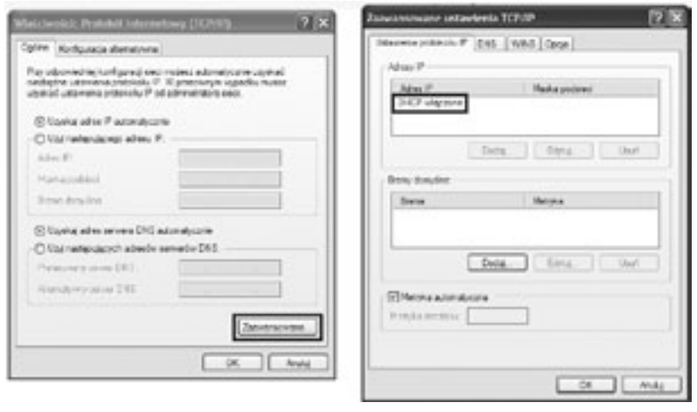
Rysunek 20.
Okno ukazujące stan połączenia lokalnego



Rysunek 21.
Okno z właściwościami połączenia lokalnego

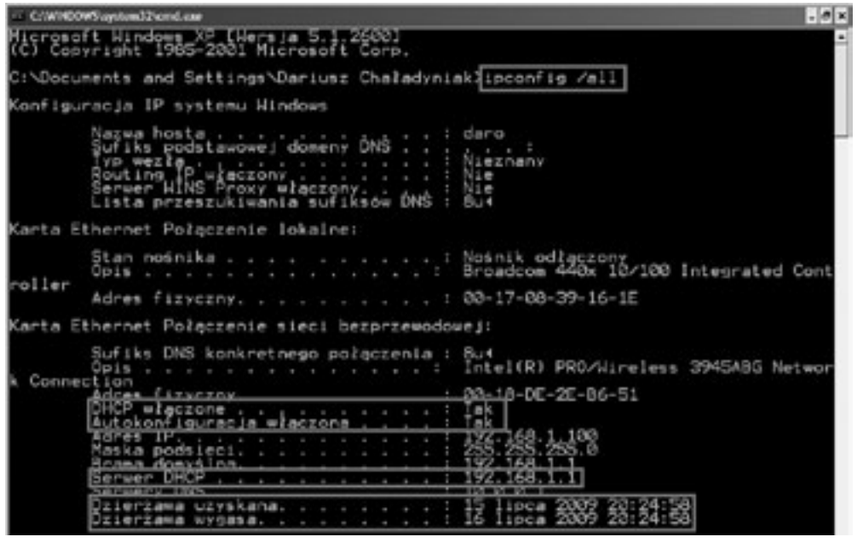


Rysunek 22.
Odznaczenie automatycznych wyborów adresów IP



Rysunek 23.
Efekt wybrania zakładki Zaawansowane w oknie Właściwości Protokołu internetowego TCP/IP

Testowanie konfiguracji usługi DHCP



Rysunek 24.
Testowanie konfiguracji usługi DHCP

Aby przetestować konfigurację usługi DHCP wydajemy polecenie ipconfig z opcją all. W wyniku jego wykonania otrzymujemy informację, czy usługa DHCP jest włączona i czy włączona jest jej autokonfiguracja. Ponadto otrzymujemy informację o adresie IP serwera DHCP (w tym przypadku – 192.168.1.1) oraz daty: uzyskania dzierżawy usługi DHCP i jej wygaśnięcia (rys. 24).

4 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:
http://www.wwsi.edu.pl
http://www.onet.pl
http://www.microsoft.com
ftp://public.wwsi.edu.pl

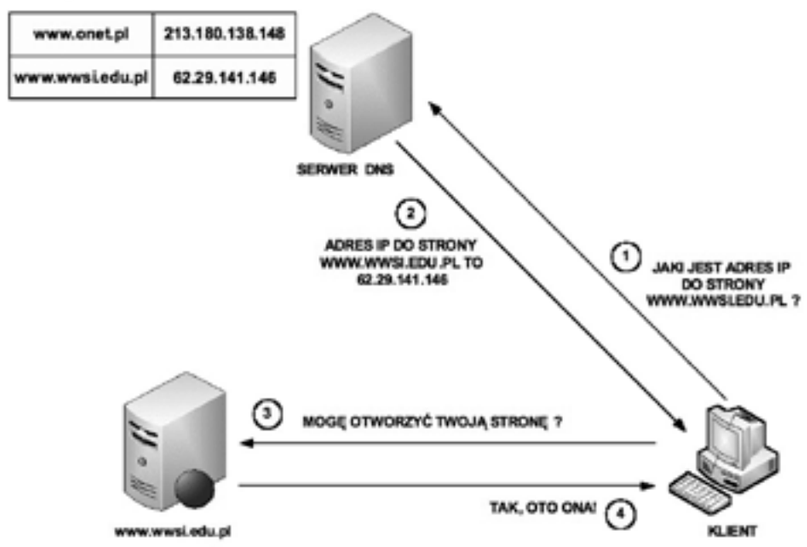
http://www.nask.pl
http://www.mf.gov.pl/

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 25.
Przykład działania usługi DNS

Działanie usługi DNS sprowadza się do następujących kolejnych czynności (patrz rys. 25):

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 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., Rufi A.W., *Akademia sieci Cisco. CCNA Exploration. Semestr 1*, Mikom, Warszawa 2008
2. Graziani R., Vachon B., *Akademia sieci Cisco. CCNA Exploration. Semestr 4*, Mikom, 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*, Mikom, Warszawa 2007