

NAZWY I ADRESY W SIECIACH IP PODZIAŁ NA PODSIECI

1. Adres IP

Adresy IP są niepowtarzalnymi identyfikatorami wszystkich stacji należących do intersieci TCP/IP. Stacją może być komputer, terminal, router, a także koncentrator. „Stację” można najprościej zdefiniować jako dowolne urządzenie w sieci, występujące jako przedmiot jednego z trzech działań:

- Uzyskiwania dostępu do innych urządzeń w sieci
- Łączenia się z nim jako udostępnionym składnikiem sieci
- Administrowania niezbędnego dla poprawnego funkcjonowania sieci

Każda stacja wymaga adresu niepowtarzalnego w całej intersieci TCP/IP; żadnej ze stacji nie można przypisać adresu już istniejącego. W światowej sieci, jaką jest Internet, rolę organu przydzielającego adresy IP pełni Internet Assigned Number Authority (IANA – Rada ds. Nadawania Numerów). Określa ona zasady przydzielania adresów.

2. Sposoby zapisywania adresów IP

Każdy z adresów IP jest ciągiem trzydziestu dwóch zer i jedynek. Obecna wersja adresowania IP jest więc nazywana adresowaniem 32-bitowym. Nie jest ono, w gruncie rzeczy, zbyt wygodne. Stąd powszechne używanie notacji dziesiętnej z kropkami.

Na 32-bitowy adres IP składają się 4 oktety. Każdy oktet można zapisać w postaci liczby dziesiętnej.

Przykładowy adres: 01111111 00000000 00000000 00000001
jest zapisywany jako: 127.0.0.1.

Jest to tzw. adres pętli zwrotnej (ang. loopback address), reprezentujący stację lokalną, czyli tę, przy której siedzimy. Jest to adres zarezerwowany i wysyłane doń dane nigdy nie są przekazywane do sieci.

Przekształcenie polega na zapisaniu każdego z oktetów postaci liczby dziesiętnej i wstawieniu pomiędzy nie kropek.

3. Klasy adresów IP

A	0	Sieć	.	Stacja	.	Stacja	.	Stacja
B	10	Sieć	.	Sieć	.	Stacja	.	Stacja
C	110	Sieć	.	Sieć	.	Sieć	.	Stacja
D	1110	Adres multiemisji						
E	11110	Zarezerwowany do użycia w przyszłości						

Rys.: Pięć klas adresów IP

Źródło: Komar, B. (2002). TCP/IP dla każdego. Gliwice: Helion, str. 64

Każda z pięciu klas adresów IP jest oznaczona literą alfabetu: klasa A, B, C, D i E. Każdy adres składa się z dwóch części: adresu sieci i adresu hosta (stacji). Klasy prezentują odmienne uzgodnienia dotyczące liczby obsługiwanych sieci i hostów.

- Adres IP klasy A

Pierwszy bit adresu (8 bajtów) klasy A jest zawsze ustawiony na „0”. Następne siedem bitów identyfikuje numer sieci. Ostatnie 24 bity (np. trzy liczby dziesiętne oddzielone kropkami) adresu klasy A reprezentują możliwe adresy hostów.

Wzorzec binarny tej klasy to: 0#####.

Adresy klasy A mogą mieścić się w zakresie od **1.0.0.1** do **127.255.255.254**.

Każdy adres klasy A może obsłużyć 16777214 ($= 2^{24}-2$) unikatowych adresów hostów.

- Adres IP klasy B

Pierwsze dwa bity adresu klasy B to „10”. 16 bitów identyfikuje numer sieci, zaś ostatnie 16 bitów identyfikuje adresy potencjalnych hostów.

Wzorcem binarnym jest: 10#####.

Adresy klasy B mogą mieścić się w zakresie od **128.0.0.1** do **191.255.255.254**.

Każdy adres klasy B może obsłużyć 65534 ($= 2^{16}-2$) unikatowych adresów hostów.

- Adres IP klasy C

Pierwsze trzy bity adresu klasy C to „110”. Następne 21 bitów identyfikuje numer sieci. Ostatni oktet służy do adresowania hostów.

Wzorzec binarny: 110#####.

Adresy klasy C mogą mieścić się w zakresie od **192.0.0.1** do **223.255.255.254**. Każdy adres klasy C może obsłużyć 254 ($= 2^8 - 2$) unikatowe adresy hostów.

- Adres IP klasy D

Pierwsze cztery bity adresu klasy D to „1110”. Adresy te są wykorzystywane do multicastingu, ale ich zastosowanie jest ograniczone. Adres multicast jest unikatowym adresem sieci, kierującym pakiety do predefiniowanych grup adresów IP. Adresy klasy D mogą pochodzić z zakresu **224.0.0.0** do **239.255.255.254**.

- Adres IP klasy E

Faktycznie – zdefiniowano klasę E adresu IP, ale InterNIC zarezerwował go dla własnych badań. Tak więc żadne adresy klasy E nie zostały dopuszczone do zastosowania w Internecie.

4. Ogólne zasady adresowania IP

Podczas nadawania adresów IP należy przestrzegać następujących reguł:

- Wszystkie stacje w jednym fizycznym segmencie sieci powinny mieć ten sam identyfikator sieci
- Część adresu IP określająca pojedynczą stację musi być odmienna dla każdej stacji w segmencie sieci
- Identyfikatorem sieci nie może być 127 – wartość ta jest zarezerwowana do celów diagnostycznych
- Identyfikator stacji nie może składać się z samych jedynek – jest to adres rozgłaszania dla sieci lokalnej
- Identyfikator sieci nie może składać się z samych zer – jest to oznaczenie sieci lokalnej
- Identyfikator stacji również nie może składać się z samych zer – jest to oznaczenie sieci wskazanej przez pozostałą część adresu i nie może zostać przypisane pojedynczej stacji

5. Specjalne adresy IP

Pewne adresy IP zostały zarezerwowane i nie mogą zostać wykorzystane do oznaczania stacji lub sieci.

- Adresy poszczególnych sieci powstają ze złożenia identyfikatora sieci oraz zer w miejscu identyfikatora stacji.

KLASA	ID SIECI
A	w.0.0.0
B	w.x.0.0
C	w.x.v.0

Rys.: Adresy sieci według klas

- Identyfikatory sieci połączone z binarnymi jedynekami w miejscu identyfikatora stacji są adresami rozgłaszania.

KLASA	ADRES ROZGŁASZANIA
A	w.255.255.255
B	w.x.255.255
C	w.x.v.255

Rys.: Adresy rozgłaszania według klas

- Adres IP 255.255.255.255 jest zarezerwowany jako adres ograniczonego rozgłaszania. Może on zostać użyty zawsze, gdy stacja nie zna jeszcze identyfikatora sieci. Ogólną zasadą konfiguracji routerów jest uniemożliwienie przesyłania tego rozgłoszenia poza lokalny segment sieci.
- Adres sieci 127 jest zarezerwowany dla celów diagnostycznych (tzw. adres pętli zwrotnej).
- Adres IP 0.0.0.0 oznacza „niniejsza stacja”. Wykorzystywany jest jedynie w takich sytuacjach jak uruchomienie klienta DHCP, który nie otrzymał jeszcze własnego adresu IP.

6. Znaczenie masek podsieci

Maska podsieci (ang. SNM — subnet mask) jest wykorzystywana do określania, ile bitów adresu IP wskazuje sieć, a ile stację w tej sieci. Dla adresów klas A, B i C wykorzystywane są maski domyślne

- klasa A – 255.0.0.0
- klasa B – 255.255.0.0
- klasa C – 255.255.255.0

Maska podsieci klasy A mówi, że sieciowa część adresu to pierwsze 8 bitów. Pozostałe 24 bity określają stację w tej sieci. Jeżeli adresem stacji jest 11.25.65.32, to wykorzystanie maski domyślnej określa adres sieci jako 11.0.0.0. Częścią adresu wskazującą stację jest 25.65.32.

Maska podsieci klasy B mówi, że sieć jest określona przez pierwszych 16 bitów adresu. Pozostałe 16 bitów wskazuje konkretną stację. Dla adresu stacji 172.16.33.33, sieć wskazuje adres 172.16.0.0, a składnikiem określającym stację jest 33.33.

Maska podsieci klasy C mówi, że część adresu określająca sieć to pierwsze 24 bity, a pozostałe 8 wskazuje należącą do niej stację. Dla adresu stacji 192.168.2.3 wskazaniem sieci jest 192.168.2.0, zaś składnikiem określającym stację jest 3.

7. Adresy w sieci lokalnej

Trzy następujące pule adresów IP zostały zarezerwowane do użytku w sieciach lokalnych, oddzielonych serwerami proxy lub zaporami firewall:

- Od 10.0.0.0 do 10.255.255.255
- Od 172.16.0.0 do 172.31.255.255
- Od 192.168.0.0 do 192.168.255.255

Celem ich utworzenia było zapewnienie sieciom nie przyłączonym do Internetu puli adresów niewchodzących w konflikt z żadnymi adresami będącymi w użyciu w Internecie.

Sieciom korzystającym z tych pul nie zagraża w razie późniejszego przyłączenia do Internetu, przypadkowy konflikt z inną siecią obecną w Internecie.

Poza zabezpieczeniem przed konfliktem, prywatne adresowanie sieci przyczynia się istotnie do ograniczenia zapotrzebowania na adresy publiczne. Przy wysyłaniu danych z sieci prywatnej do publicznej, pierwotny adres źródłowy zostaje zamieniony na adres zewnętrzny, uzyskany od ISP. Procedury tego rodzaju określane są jako translacja adresów sieciowych (NAT – network address translation).

Adresy NAT mogą być wykorzystywane wyłącznie za zaporami firewall albo serwerami proxy, które ukrywają przed Internetem własne schematy adresowania. Utrudnia to dostęp do sieci osobom nieuprawnionym i umożliwia współużytkowania jednego adresu publicznego przez wiele stacji.

8. Protokół Internetu, wersja 6 (IPv6)

Protokół IPv4 ma już prawie dwadzieścia lat. Od jego początków Internet przeszedł kilka znaczących zmian, które zmniejszyły efektywność IP jako protokołu uniwersalnej przyłączalności. Być może najbardziej znaczącą z tych zmian była komercjalizacja Internetu. Przyniosła ona bezprecedensowy wzrost populacji użytkowników Internetu. To z kolei stworzyło zapotrzebowanie na większą liczbę adresów, a także potrzebę obsługi przez warstwę Internetu nowych rodzajów usług. Ograniczenia IPv4 stały się bodźcem dla opracowania zupełnie nowej wersji protokołu. Jest ona nazywana IP, wersja 6 (IPv6), ale powszechnie używa się również nazwy Następna generacja protokołu Internetu (ang. IPng — next generation of Internet Protocol).

Protokół IPv6 ma być prostą, kompatybilną „w przód” nowelizacją istniejącej wersji protokołu IP. Intencją przyświecającą tej nowelizacji jest wyeliminowanie wszystkich słabości ujawniających się obecnie w protokole IPv4, w tym zbyt małej liczby dostępnych adresów IP, niemożności obsługiwanego ruchu o wysokich wymaganiach czasowych i braku bezpieczeństwa w warstwie sieci.

Dodatkowym bodźcem dla opracowania i rozwoju nowego protokołu IP stało się trasowanie, które w ramach protokołu IPv4 jest skrepowane jego 32-bitową architekturą adresową, dwupoziomą hierarchią adresowania i klasami adresowymi. Dwupoziomowa hierarchia adresowania „host.domena” po prostu nie pozwala

konstruować wydajnych hierarchii adresowych, które mogłyby być agregowane w routerach na skalę odpowiadającą dzisiejszym wymaganiom globalnego Internetu.

Następna generacja protokołu IP – IPv6 – rozwiązuje wszystkie wymienione problemy.

Będzie oferować znacznie rozszerzony schemat adresowania, aby nadążyć za stałą ekspansją Internetu, a także zwiększoną zdolność agregowania tras na wielką skalę.

IPv6 będzie także obsługiwać wiele innych właściwości, takich jak: transmisje audio i/lub wideo w czasie rzeczywistym, mobilność hostów, bezpieczeństwo końcowe (czyli na całej długości połączenia) dzięki mechanizmom warstwy Internetu – kodowaniu i identyfikacji, a także autokonfiguracja i autorekonfiguracja. Oczekuje się, że usługi te będą odpowiednią zachętą dla migracji, gdy tylko staną się dostępne produkty zgodne z IPv6. Wiele z tych rozwiązań wciąż wymaga dodatkowej standaryzacji, dlatego też przedwcześnie byłoby ich obszerne omawianie.

Podstawowe zmiany wprowadzane w nowej edycji protokołu to:

- Rozszerzone możliwości adresowania.
Zwiększona do 128 bitów długość adresów IPv6 spowoduje znaczny wzrost dostępnej ich liczby. Każdy użytkownik Internetu będzie dysponował tyloma adresami, ile dziś jest dostępnych w całej wielkiej sieci.
- Uproszczenie nagłówka IP.
Większość informacji zapisywanych w nagłówku IP zostało określonych jako opcjonalne lub całkowicie usunięte. Przyspiesza to przetwarzanie nagłówka przez stacje odbierające pakiet.
- Zwiększenie elastyczności nagłówka IP.
Nagłówek IP został skonstruowany pod kątem efektywniejszego przekazywania, większej elastyczności w zakresie długości pól opcji i prostszego dołączania w przyszłości nowych opcji. Przez kilka lat pozwoli to nagłówkowi IP zmieniać się wraz z ewolucją protokołu bez konieczności przeprojektowywania całego jego formatu.

- Ulepszona kontrola przepływu.

Datagramy IP będą mogły zawierać zlecenie lepszej jakości usługi. Oznacza to dostarczanie informacji o określonym czasie oraz zdolność żądania minimalnej szerokości pasma lub obsługi w czasie rzeczywistym.

- Zwiększone bezpieczeństwo.

Nagłówek IP będzie zawierał rozszerzenia zapewniające uwierzytelnianie stacji źródłowej i docelowej oraz wyższą gwarancję braku uszkodzeń danych. Zostanie uwzględniona również opcja szyfrowania przesyłanych przez sieć informacji.

Wymienione zmiany protokołu IP powinny istotnie wpłynąć na rozwój Internetu. Przyczynią się one zapewne również do dalszego zwiększania ilości funkcji dostępnych dla aplikacji korzystających z TCP/IP jako podstawowego zestawu protokołów.

9. Literatura

- 9.1. Komar, B. (2002). TCP/IP dla każdego. Gliwice: Helion.
- 9.2. Sportack, M. (1999). Sieci komputerowe – księga eksperta. Gliwice: Helion.
- 9.3. „PC World Kompurer – PRO”. Nr 3/2003.
- 9.4. „Komputer Świat - Expert”. Nr 3/2003 (4).
- 9.5. „PC Format”. Nr 09/2003 (37).
- 9.6. <http://www.siecilokalne.pl>