Sieć komputerowa

Siecią komputerową nazywamy system informatyczny składający się z dwóch lub więcej komputerów połączonych w celu wymiany danych między nimi. Sieć przewodowa może być zbudowana z wykorzystaniem urządzeń takich jak koncentratory, mosty lub/i przełączniki. Dwa ostatnie typy urządzeń (mosty i przełączniki) stosowane są do podziału sieci na segmenty. Urządzenia te służą do przekazywania informacji między segmentami, oraz ich separacji – dzięki tej funkcjonalności dane przesyłane w obrębie danego segmentu nie wydostają się poza ten segment, a dane zaadresowane do komputera znajdującego się w innym segmencie zostają wysłane tylko do tego segmentu. Zasady działania mostów (przełączników) opisuje standard RFC 802.1D.

Komputery należące do jednego segmentu współdzielą to samo medium transmisyjne. Może to prowadzić do tzw. kolizji występujących wtedy, gdy dwa lub więcej komputerów z tego samego segmentu wysyła dane w tej samej chwili. Transmisja danych nie dochodzi wówczas do skutku, a w segmencie rozchodzi się sygnał kolizji. Sygnał ten nie wydostaje się poza segment, w którym kolizja wystąpiła. Z tego powodu segmenty sieci komputerowej nazywane są niekiedy domenami kolizyjnymi. Istnieją mechanizmy, które w zależności od rodzaju sieci zapobiegają kolizjom (CSMA/CA), albo – w przypadku ich wystąpienia – zapewniają powtórzenie nieudanej transmisji (CSMA/CD). Komunikacja w obrębie sieci przebiega na bazie adresów sprzętowych.

Adresy sprzętowe

Adresy sprzętowe, zwane też adresami fizycznymi, adresami MAC (ang. Media Access Control), lub adresami warstwy łącza danych modelu OSI (ang. data link layer) służą do identyfikowania hostów w komunikacji wewnątrzsieciowej. Zwyczajowo, adresy MAC są zapisywane w postaci sześciu dwucyfrowych liczb szesnastkowych oddzielonych dwukropkami. Pierwsze trzy liczby oznaczają producenta interfejsu sieciowego (z wyjątkiem adresów broadcast i multicast), natomiast ostatnie trzy identyfikują interfejs danego producenta. Adres taki może być typu unicast, multicast, albo broadcast. Adres unicast identyfikuje pojedynczy komputer, multicast – grupę komputerów (np. realizujących określoną usługę), broadcast – wszystkie komputery w danej sieci. Adres MAC typu broadcast to ff:ff:ff:ff:ff:ff, natomiast adresy MAC typu multicast zawierają się w przedziale 01:80:c2:00:00:00 – 01:80:c2:ff:ff:ff. Dane z adresem docelowym broadcast trafiają są do

wszystkich komputerów w segmencie lokalnym oraz pozostałych segmentach, dane z adresem multicast – do komputerów w segmencie lokalnym oraz do tych segmentów, w których znajdują się komputery należące do danej grupy multicast. Uwaga, dane z adresami multicast z przedziału 01:80:c2:00:00:00 – 01:80:c2:00:00:0f nie są przekazywane (przez mosty lub przełączniki) do innych segmentów, zatem trafiają tylko do komputerów w segmencie lokalnym. Należy podkreślić, że adresy sprzętowe umożliwiają przesyłanie danych tylko w obrębie jednej sieci, nie jest natomiast możliwe przesłanie danych między różnymi sieciami w oparciu o same adresy fizyczne.

Adresy logiczne

Służą do identyfikacji hostów w komunikacji międzysieciowej. Adresy logiczne umożliwiają przesłanie danych między różnymi sieciami. Urządzenia łączące dwie lub więcej sieci noszą nazwę routerów. Analizują one adresy logiczne i zajmują się przekazywaniem danych między sieciami w sytuacji, gdy host docelowy znajduje się w innej sieci niż host źródłowy. Router posiada po jednym interfejsie do każdej z podłączonych do niego sieci. Na podstawie adresu logicznego hosta docelowego i tabeli routingu, zwanej też tabelą trasowania, router wysyła dane bezpośrednio do tego hosta (jeśli host znajduje się w jednej z przyłączonych do routera sieci), albo do jednego z routerów sąsiednich, czyli takiego, który ma interfejs do jednej z przyłączonych do routera sieci.

System adresacji IP (wersja IPv4)

Jest to system adresacji logicznej stosowany jeszcze w przeważającej części Internetu. Każdy komputer podłączony do (publicznego) Internetu musi mieć unikalny adres IP. W najczęściej stosowanym zapisie adres IP składa się z czterech liczb dziesiętnych z przedziału od 0 do 255 oddzielonych kropkami. W pewnych sytuacjach stosuje się również zapis binarny (dwójkowy) i heksadecymalny (szesnastkowy). Przykładem adresu IP jest 10.1.1.20. Ten sam adres w zapisie dwójkowym to 00001010.00000001.00000001.00010100. Adres IP składa się z dwóch części – sieciowej i hostowej. Pierwsza z nich identyfikuje sieć, natomiast druga – hosta w danej sieci. Podział na część sieciową i hostową jest realizowany przy pomocy tzw. maski, która jest ciągiem 32 bitów składającym się z samych jedynek po lewej i z samych zer po prawej stronie. Przykładem maski jest adres 11111111.11111111.11110000.00000000 (w zapisie binarnym) lub 255.255.240.0 (w zapisie dziesiętnym). Liczbę jedynek występujących w postaci binarnej maski nazywamy jej długością. Maska określa, które bity adresu tworzą

jego część sieciową, a które hostową. Mianowicie, część sieciową adresu tworzą te bity, które w masce są jedynkami, a część hostową – te, które w masce są zerami. W powyższym przykładzie część sieciowa adresu składa się z pierwszych 20 bitów, natomiast hostowa – z pozostałych 12 bitów.

Maska służy do określenia sieci, w której znajduje się host o danym adresie IP, a konkretnie do określenia adresu i rozmiaru tej sieci. Adres sieci uzyskujemy w wyniku boolowskiego pomnożenia kolejnych bitów adresu przez odpowiednie bity maski. Ta operacja nazywa się nakładaniem maski na adres. W naszym przykładzie adres sieci to 10.1.0.0. Adres ten powstał z pomnożenia kolejnych bitów adresu 10.1.1.20 przez odpowiadające im bity maski 255.255.240. Ilustruje to poniższy rysunek.

Adres binarnie:	Adres dziesiętnie:
00001010.00000001.00000001.00010100	10.1.1.20
Maska binarnie:	Maska dziesiętnie:
11111111.11111111.11110000.00000000	255.255.240.0
Adres sieci binarnie:	Adres sieci dziesiętnie:
00001010.00000001.00000000.00000000	10.1.0.0

Z kolei rozmiar sieci to liczba wszystkich adresów w danej sieci, Jest ona równa 2^n, gdzie n jest liczbą bitów części hostowej. Z kolei maksymalna liczba interfejsów, które można umieścić w danej sieci wynosi 2^n – 2 (zapis x^n oznacza x do potęgi n). Może się wydawać, że liczba ta powinna być równa rozmiarowi sieci, ale dwa adresy mają specjalne znaczenie. Adres IP zawierający w części hostowej same zera (w zapisie binarnym) jest adresem całej sieci, natomiast adres zawierający w części hostowej same jedynki jest tzw. adresem broadcast. Służy on do adresowania informacji przeznaczonej dla wszystkich komputerów w danej sieci, a nie tylko dla jednego z nich. Jest to tzw. broadcast skierowany (inny rodzaj adresu broadcast jest omówiony w dalszym ciągu). Pakiet z takim adresem docelowym może być przekazywany przez routery. Każdy z pozostałych 2^n – 2 adresów jest tzw. adresem unicast, tzn. służy do adresowania informacji przeznaczonej dla jednego, określonego tym adresem komputera.

Maska nie była potrzebna, kiedy przynależność komputera do sieci była określana tylko na podstawie tzw. klasy, do której należał dany adres. Jednak wraz z rozwojem Internetu

wprowadzono możliwość podziału pełnej sieci na podsieci, przy zastosowaniu maski dłuższej niż domyślna dla pełnej sieci. Zasady takiego podziału opublikowano w dokumencie RFC 950. Maska stała się wówczas nieodłącznym atrybutem adresu, ponieważ nie sam adres IP, ale dopiero para składająca się z adresu IP i maski daje pełną informację o logicznej lokalizacji komputera. Poniższa tabela przedstawia podział przestrzeni adresowej IPv4 na klasy.

Klasy adresów IPv4

Klasa	Pierwszy bajt adresu	Liczba sieci danej klasy	Część sieciowa	Część hostowa	Maska domyślna	Liczba adresów unicast w sieci
A	1-126 (127)	126 (127)	1 oktet	3 oktety	255.0.0.0	2^24 – 2
B	128-191	2^6*2^8 = 2^14	2 oktet	2 oktety	255.255.0.0	2^16 – 2
C	192-223	2^5*2^16 = 2^21	3 oktety	1 oktet	255.255.255.0	2^8 – 2 = 254
D	224-239	Adresy typu multicast				
E	240-255	Zarezerwowane dla uprawnionych podmiotów				

Uwaga 1: Do adresowania komputerów są używane adresy z pierwszych trzech klas, czyli klas A, B i C. Adresy z pozostałych klas mają inne przeznaczenie.

Uwaga 2: Formalnie, adresy z pierwszym bajtem równym 127 należą do klasy A, ale nie są one używane do adresowania rzeczywistych interfejsów sieciowych. Za ich pomocą adresowany jest tzw. interfejs pętli zwrotnej (ang. loopback interface) używany w sytuacjach, gdy komputer (a ściślej – oprogramowanie realizujące protokół IP) wysyła informację do samego siebie.

Uwaga 3: Adres 255.255.255.255 (formalnie należący do klasy E) to tzw. broadcast globalny. Pakiet z tym adresem docelowym jest przeznaczony dla wszystkich komputerów w sieci lokalnej, ale nie jest przekazywany przez routery do innych sieci, czym różni się funkcjonalnie od broadcastu skierowanego.

Uwaga 4: Pakiety z adresami multicast z zakresu 224.0.0.0 – 224.0.0.255 nie są przekazywane (przez routery) do innych sieci, zatem trafiają tylko do komputerów w sieci lokalnej (porównaj z analogiczną uwagą dotyczącą adresów MAC typu multicast).

Publiczne i prywatne adresy IPv4

Pewne grupy adresów IPv4 są wydzielone jako tzw. adresy prywatne. Adresy te są stosowane w sieciach prywatnych oddzielonych od publicznego Internetu specjalnymi bramkami (ang. gateway). Na tych bramkach jest wykonywana tzw. translacja adresów. W pakiecie wysyłanym z sieci prywatnej do publicznego Internetu bramka zamienia prywatny adres źródłowy (adres komputera źródłowego w sieci prywatnej) na publiczny adres źródłowy (adres bramki od strony Internetu publicznego). W pakiecie przysyłanym z publicznego Internetu do sieci prywatnej bramka zamienia publiczny adres docelowy (adres bramki od strony Internetu publicznego) na prywatny adres docelowy (adres komputera docelowego w sieci prywatnej).

Grupy adresów prywatnych (określone w dokumencie RFC 1918)

10.0.0.0 - 1 sieć klasy A
od 172.16.0.0 do 172.31.0.0 - 16 sieci klasy B
od 192.168.0.0 do 192.168.255.0 - 256 sieci klasy C

Adresy z powyższych grup nie mogą być nadawane komputerom podłączonym do publicznego Internetu. Służą one do adresowania komputerów w tzw. sieciach prywatnych, które nie wchodzą w skład publicznego Internetu, ale są z nim pośrednio połączone przez tzw. bramki internetowe. Na bramkach tych działają mechanizmy translacji adresów umożliwiające obustronną komunikację między komputerami z sieci prywatnej, a tymi z publicznego Internetu.

Podział sieci danej klasy na podsieci

Sieci klas A, B i C mogą być dzielone na równe rozmiarowo podsieci. W celu podzielenia sieci danej klasy na podsieci wydłuża się jej maskę domyślną o pewną liczbę bitów – k. Skutkuje to wydzieleniem 2^k grup adresów (podsieci) takich, że adresy każdej grupy są jednakowe w części sieciowej, różnią się między sobą w części hostowej, pierwszy z nich ma same zera (w zapisie binarnym) w części hostowej, a ostatni ma same jedynki (w zapisie binarnym) w części hostowej.

Tabela podziału sieci klasy C na równe podsieci

Liczba podsieci	Maska podsieci	Liczba bitów maski	Adresy podsieci	Zakresy dostępnych adresów unicast	Adres broadcast
2^1 = 2	255.255.255.128	24 + 1 = 25	w.x.y.0 w.x.y.128	w.x.y.1 - w.x.y.126 w.x.y.129 - w.x.y.254	w.x.y.127 w.x.y.255
2^2 = 4	255.255.255.192	24 + 2 = 26	w.x.y.0 w.x.y.64 w.x.y.128 w.x.y.192	w.x.y.1 –w.x.y.62 w.x.y.65 - w.x.y.126 w.x.y.129 - w.x.y.190 w.x.y.193 - w.x.y.254	w.x.y.63 w.x.y.127 w.x.y.191 w.x.y.255
2^3 = 8	255.255.255.224	24 + 3 = 27	w.x.y.0 w.x.y.32 w.x.y.64 w.x.y.96 w.x.y.128 w.x.y.160 w.x.y.192 w.x.y.224	w.x.y.1 - w.x.y.30 w.x.y.33 - w.x.y.62 w.x.y.65 - w.x.y.94 w.x.y.97 - w.x.y.126 w.x.y.129 - w.x.y.158 w.x.y.161 - w.x.y.190 w.x.y.193 - w.x.y.222 w.x.y.225 - w.x.y.254	w.x.y.31 w.x.y.63 w.x.y.95 w.x.y.127 w.x.y.159 w.x.y.191 w.x.y.223 w.x.y.255

Metoda VLSM (Variable Length Subnet Mask – RFC 1009)

Sieć danej klasy można również podzielić na podsieci o różnej wielkości. W tym celu stosowana jest tzw. metoda VLSM (ang. Variable Length Subnet Mask). Nazwa metody bierze się stąd, że do wydzielenia poszczególnych podsieci używa się masek o różnych długościach. Taki sposób podziału jest niezbędny w sytuacjach, kiedy metoda podziału na równe podsieci nie może być zastosowana ze względu na wymagania odnośnie rozmiarów poszczególnych podsieci. Załóżmy, że chcemy podzielić sieć klasy C o adresie 192.168.1.0 na

cztery podsieci, do których ma należeć odpowiednio 100, 50, 25 i 20 komputerów. Metoda podziału na równe podsieci nie ma w tym przypadku zastosowania, ponieważ nie da się umieścić 100 adresów unicast w podsieci o rozmiarze 64, która powstaje z podziału sieci klasy C na 4 równe części. Problem ten daje się jednak rozwiązać, jeśli do podziału sieci wyjściowej zastosujemy maski o różnych długościach – 25, 26 i dwa razy po 27 bitów. Oto tabela przedstawiająca rozwiązanie:

Numer podsieci	Maska podsieci	Adres podsieci	Zakres dostępnych Adresów unicast	Adres broadcast
1	255.255.255.128	192.168.1.0	192.168.1.1 – 126	192.168.1.127
2	255.255.255.192	192.168.1.128	192.168.1.129 – 190	192.168.1.191
3	255.255.255.224	192.168.1.192	192.168.1.193 – 222	192.168.1.223
4	255.255.255.224	192.168.1.224	192.168.1.225 – 254	192.168.1.255

Powyższy podział zrealizowany metodą podziału odcinka:

[0----------127][128----------191][192-----223][224-----255]

Uwaga: Każda z podsieci wydzielonych metodą VLSM musi być podsiecią powstałą z równego podziału. W powyższym przykładzie pierwsza podsieć, czyli 192.168.1.0/25, jest pierwszą podsiecią powstałą z podziału na 2 równe podsieci, druga podsieć jest trzecią powstałą z podziału na 4 równe podsieci, a dwie ostatnie podsieci to siódma i ósma powstałe z podziału na 8 równych podsieci. Przy podziale metodą VLSM istotna jest kolejność wydzielania podsieci. Wynika to z faktu, że nie każdy adres z całej sieci może być adresem podsieci z niej wydzielanej. W powyższym przykładzie nie można zamienić kolejnością pierwszej i drugiej podsieci. Po takiej zamianie druga podsieć miałaby adres 192.168.1.64 i 25-bitową maskę, ale nie byłaby to podsieć powstała z równego podziału sieci 192.168.1.0 na dwie części. Ilustruje to poniższy rysunek.

[0----------63][64----------191][192-----223][224-----255]

Widać na nim, że grupa adresów 192.168.1.64/25 nie jest ani podsiecią 192.168.1.0/25 ani 192.168.128/25, które to podsieci powstają z równego podziału na dwie części. Poza tym,

grupa adresów powstała z nierównego podziału musi być siecią IP. Grupa 192.168.1.64/25 nie jest siecią IP, ponieważ pierwszy adres grupy, czyli 192.168.1.0 1000000 (ostatni oktet zapisany binarnie, spacja oddziela część sieciową od hostowej) nie ma samych zer w części hostowej. Dzieląc sieć na podsieci metodą VLSM należy przestrzegać następującej zasady: w zapisie bitowym adres podsieci musi mieć same zera w części hostowej. Wynika z niej, że podsieć może być „odsunięta" od początku całej sieci tylko o całkowitą wielokrotność swojego rozmiaru.

Zadanie do samodzielnego rozwiązania

Podzielić pełną sieć klasy C o adresie w.x.y.0 na trzy jak najmniejsze podsieci w taki sposób, aby w pierwszej podsieci można było umieścić 30, w drugiej 60, a w trzeciej 120 komputerów.

Wskazówka: kolejne podsieci muszą mieć adresy w.x.y.0 albo w.x.y.32 (pierwsza), w.x.y.64 (druga), oraz w.x.y.128 (trzecia).

Złe rozwiązanie:
[0-------- 31][32----------95][96----------223]
Adres 2 grupy: w.x.y.00 100000 <- jedynka w części hostowej
Adres 3 grupy: w.x.y.0 1100000 <- jedynki w części hostowej

Dwa dobre rozwiązania:
[0--------31][--------][64----------127][128----------255]
Adres 1 grupy: w.x.y.000 00000 <- same zera w części hostowej
Adres 2 grupy: w.x.y.01 000000 <- same zera w części hostowej
Adres 3 grupy: w.x.y.1 0000000 <- same zera w części hostowej

[--------][32--------63][64----------127][128----------255]
Adres 1 grupy: w.x.y.001 00000 <- same zera w części hostowej
Adres 2 grupy: w.x.y.01 000000 <- same zera w części hostowej
Adres 3 grupy: w.x.y.1 0000000 <- same zera w części hostowej

CIDR (Classless Inter-Domain Routing – RFC 1517...1520)

Jest to wydzielanie bloków adresów będących (w nawiązaniu do podziału na klasy) podsieciami, całymi sieciami lub sieciami zagregowanymi (nadsieciami). Blok taki jest oznaczany przez w.x.y.z/d gdzie w.x.y.z jest początkowym adresem bloku, a zarazem adresem podsieci, całej sieci, lub sieci zagregowanej, natomiast d jest liczbą bitów maski dzielącej adresy bloku na część sieciową i hostową. Maksymalna liczba adresów unicast w takim bloku wynosi 2^d–2. Pierwszy adres bloku składa się z samych zer w części hostowej i jest adresem sieci, a ostatni składa się z samych jedynek w części hostowej i jest adresem broadcast w danej sieci.

Przykładowa agregacja czterech sieci klasy C do jednej sieci bezklasowej

Weźmy następujące 4 sieci klasy C: 192.168.0.0, 192.168.1.0, 192.168.2.0, 192.168.3.0
W każdej z powyższych sieci są 254 adresy unicast, łacznie 1016 adresów unicast.
Wypiszmy po kolei wszystkie adresy z tych 4 sieci z maską domyślną skróconą o 2 bity:

192.168.0—0 00.0—0 <- pierwszy adres 1 podsieci
…
192.168.0—0 00.1—1 <- ostatni adres w 1 podsieci
192.168.0—0 01.0—0 <- pierwszy adres w 2 podsieci
…
192.168.0—0 01.1—1 <- ostatni adres w 2 podsieci
192.168.0—0 10.0—0 <- pierwszy adres w 3 podsieci
…
192.168.0—0 10.1—1 <- ostatni adres w 3 podsieci
192.168.0—0 11.0—0 <- pierwszy adres w 4 podsieci
…
192.168.0—0 11.1—1 <- ostatni adres w 4 podsieci

Powyższe 1024 adresy tworzą sieć IP, ponieważ spełniają odpowiednie warunki, czyli są to kolejne adresy, ich liczba jest potęgą dwójki, a pierwszy adres ma w zapisie binarnym same zera w części hostowej.

Adres CIDR sieci zagregowanej: 192.168.0.0/22
Maska sieci zagregowanej zapisana binarnie: 1—1.1—1.11111100.0—0
Maska sieci zagregowanej zapisana dziesiętnie: 255.255.252.0
Zakres adresów unicast: 192.168.0.1 – 192.168.3.254 (1022 adresy)
Adres broadcast w sieci zagregowanej: 192.168.3.255

Adresy 192.168.1.0, 192.168.2.0, 192.168.3.0, oraz 192.168.0.255, 192.168.1.255, 192.168.2.255 mogą być nadawane komputerom w sieci zagregowanej, natomiast przy zachowaniu podziału na klasy są odpowiednio adresami drugiej, trzeciej i czwartej sieci, oraz adresami broadcast w pierwszej, drugiej i trzeciej sieci.

Uwaga 1: Nie każdy adres sieci klasy A, B lub C może być początkowym adresem bloku CIDR.

Przykład niepoprawnie określonego bloku CIDR

Przykładowo, następujących ośmiu sieci klasy C: 192.168.4.0,…,192.168.11.0 nie można połączyć w sieć IP. Powstałby wtedy blok adresów o adresie 192.168.4.0/21 (8 sieci klasy C łączymy skracając domyślną maskę o 3 bity, czyli skracając ją z 24 do 21 bitów). Żeby blok był siecią IP, to pierwszy adres bloku musi mieć same zera (w zapisie binarnym) w części hostowej, czyli na ostatnich 11 bitach. Tymczasem w zapisie dwójkowym adres 192.168.4.0 przedstawia się następująco: 11000000.10101000.00000 100.00000000, więc jedenasty bit, licząc od prawej strony, jest jedynką, co przeczy powyższej zasadzie. Poprawnie natomiast jest określony blok 192.168.8.0/21 reprezentujący sieć zagregowaną z ośmiu sieci klasy C o adresach 192.168.8.0,...,192.169.15.0, a także blok 192.168.4.0/22 reprezentujący sieć zagregowaną z czterech sieci klasy C o adresach 192.168.4.0,...,192.168.7.0.

Uwaga 2: Sposób adresowania metodą CIDR jest w istocie zerwaniem z podziałem na klasy (stąd określenie „classless” – oznaczające „bezklasowy”). Przy zachowaniu podziału na klasy przykładowy adres 192.168.0.0/22 jest niepoprawny, ponieważ 192.168.0.0 jest adresem sieci klasy C albo jej podsieci, w której mogą być maksymalnie 254 adresy unicast, natomiast liczba adresów unicast w bloku 192.168.0.0/22 wynosi 1022 (2^10 – 2).