Maski o stałej i zmiennej długości (VLSM)

Autor: Natalia Dajniak IVFDS

STRESZCZENIE

Projekt obejmuje wyjaśnienie pojęcia: maska sieciowa, maska o stałej długości, VLSM itp. Na przykładach pokazano podział sieci na podsieci z uwzględnieniem poszczególnych klas (A, B, C), obliczanie optymalnej struktury podziału na podsieci, wziąwszy pod uwagę wymagania związane z liczbą podsieci oraz liczbą hostów przypadających na podsieć, a także, w jaki sposób budować tablicę podsieci. Omówiono także algorytm najdłuższego dopasowania, sposób zespalania tras, wdrażanie VLSM, obliczanie maski podsieci, a także budowania nadsieci w oparciu o klasę C.

Spis treści

1. POJĘCIA

Wraz z rozwojem Internetu nieekonomicznym okazało się przydzielanie adresów wg klas, gdyż dostępne klasy adresów zaczęły się bardzo szybko kurczyć. Wprowadzono system zwany: **bezklasowym rutowaniem międzydomenowym** CIDR (*Classless Inter-Domain Routing*). Pojawiło się też pojęcie **maski sieci**.

Maska sieci stosowana w połączeniu z miejscem docelowym w celu ustalenia, kiedy dana trasa jest wykorzystywana. Na przykład trasa hosta posiada maskę 255.255.255.255, co oznacza, że akceptowane jest tylko dokładne dopasowanie. Trasa domyślna posiada maskę 0.0.0.0, co oznacza, że z tej trasy może korzystać dowolne miejsce docelowe. Maska sieci, gdy jest napisana w systemie dwójkowym, składa się z grupy jedynek, po której następuje grupa zer. Jedynka jest znacząca (musi pasować), a zero jest nieznaczące (nie musi pasować).Maska sieci w tablicy tras działa w sposób podobny do maski podsieci, chociaż jej funkcja nie jest całkiem taka sama. Składa się podobnie jak adres IP z 4 bajtów, używana jest do wydzielenia części adresu odpowiadającej za identyfikację sieci i części odpowiadającej za identyfikację komputera z adresu IP.

Przykład

Adres IP(dziesiętnie):	212.51.219.50
Maska sieci(dziesiętnie):	255.255.255.192
Adres IP(binarnie):	11010100.00110011.11011011.00110010
Maska(binarnie):	11111111.11111111.11111111.11000000
Adres sieci(binarnie):	11010100.00110011.11011011.00000000
Broadcast(binarnie:	11010100.00110011.11011011.00111111
Adres sieci (dziesiętnie):	212.51.219.0
Broadcast (dziesiętnie):	212.51.219.63

Dzięki masce i adresowi IP możemy wyznaczyć adres sieci i adresu rozgłoszeniowego (Broadcast).
Adres sieci tworzymy przepisując niezmienione wszystkie bity adresu IP, dla których odpowiednie bity maski mają wartość jeden. Resztę uzupełniamy zerami.
Adres **broadcast** jest adresem rozgłoszeniowym sieci. Używa się go do jednoczesnego zaadresowania wszystkich komputerów w danej sieci (jest przetwarzany przez wszystkie komputery w sieci). Tworzymy go podobnie do adresu sieci, jednak dopełniamy jedynkami zamiast zerami.
Mając adres sieci i adres broadcast możemy łatwo wyznaczyć możliwy zakres numerów IP komputerów w danej sieci. Dla podanych powyżej adresów sieci i broadcast, komputerów w sieci mogą przyjmować adresy IP od numeru: 212.51.219.1 do 212.51.219.62.
Adres 212.51.219.50 z maską 255.255.255.192 możemy w skrócie zapisać 212.51.219.50/26. W tym przypadku ostatnia liczba oznacza ilość bitów o wartości jeden w masce.

Przy wyznaczaniu zakresu adresów w sieci warto pamiętać, że zakres zaczyna się od liczby nieparzystej a kończy liczbą parzystą. Jeśli wychodzi nam inaczej oznacza to, że obliczenia są błędne.

Maska podsieci(subnet mask) – podobnie jak adres IP, jest 32-bitową liczbą binarną, ale posiada bardzo specyficzny format. Musi ona składać się z grupy jedynek poprzedzającej grupę zer — na przykład 11111111111111110000000000000000. Maski podsieci są zazwyczaj zapi-

sywane albo przy użyciu kropkowej notacji dziesiętnej (255.255.0.0), albo w formacie *ukośnikowym*, gdzie wartość po ukośniku reprezentuje liczbę jedynek (/16).
- w schemacie adresowania protokołu Internet (IP) to zespół wybranych bitów, które identyfikują podsieć. Wszystkie człony podsieci mają tę samą maskę podsieci. Inna nazwa maski podsieci to subnetwork address mask.

Maska adresu podsieci (subnetwork address mask) – wzorzec określający, w jaki sposób adres IP jest podzielony na część określającą podsieć i na część określającą adres konkretnego hosta. Maska sieci to 32-bitowa liczba z jedynkami w miejscu bitów adresu IP określających część sieciową adresu i zerami w miejscu bitów określających część hosta.

Maska adresu(address mask)- część schematu adresowania w protokole między sieciowym (Internet Protocol). Maska adresu, znana też pod nazwą maski podsieci (subnet mask), to grupa bitów, których wartości identyfikują podsieć. Maska adresu upraszcza proces odnoszenia się do członków danej podsieci.

Maska podsieci, podobnie jak adres IP, jest 32-bitową liczbą binarną, ale posiada bardzo specyficzny format. Musi ona składać się z grupy jedynek poprzedzającej grupę zer — na przykład 11111111111111110000000000000000. Maski podsieci są zazwyczaj zapisywane albo przy użyciu kropkowej notacji dziesiętnej (255.255.0.0), albo w formacie *ukośnikowym*, gdzie wartość po ukośniku reprezentuje liczbę jedynek (/16).

([1],[2])

2. MASKA O STAŁEJ DŁUGOŚCI

2.1 Podział na podsieci

Trochę historii....
W 1985r określono, w jaki sposób należy dzielić sieci na podsieci. Procedura podziału została zawartą w dokumencie RFC 950.

Dwupoziomowa hierarchia adresowania IP została zastąpiona trzypoziomową, dzielącą standardowe klasowe pole numeru hosta na numer podsieci oraz numer hosta w tej podsieci.
Bity z adresu hosta są przydzielane adresowi sieci.
Rysunek 2.1.1 przedstawia sieć (*/16*) *klasy B*, w której pięć *bitów podsieci* zostało wziętych z przydziału adresu hosta i dodanych do przydziału adresu sieci, dając większą liczbę sieci z mniejszą liczbą hostów w każdej z nich.

Adres IP	nnnnnnnnnnnnnnn	sssssh	hhhhhhhhhh
Maska podsieci	1111111111111111	11111	00000000000
		Bity podsieci	

Rysunek 2.1.1 Przydzielanie bitów podsieci

Bity podsieci w masce podsieci przybierają wartość binarnej jedynki, ponieważ binarna jedynka została przypisana do bitu adresu sieci, a binarne zero do bitu adresu hosta.
Domyślnie dla sieci *klasy B* maska podsieci wynosi 255.255.0.0 (*/16*), ale zamienia się w 255.255.248.0 (*/21*), kiedy zostaje przydzielonych 5 bitów dla podziału na podsieci.

Przykład:
Istnieje sieć *klasy B* 131.11.0.0. W postaci binarnej dowolny adres w tej sieci to:
10000011 00001011 hhhhhhhh hhhhhhhh,
gdzie `h` oznacza bit adresu hosta.
Aby dokonać dalszego podziału sieci, należy utrzymać tę samą tożsamość sieci, ale wykorzystać niektóre bity (w tym przykładzie 5 bitów) z tożsamości hosta (ID) do utworzenia tożsamości podsieci, w sposób następujący:

```
Adres IP              10000011 00001011 sssssHHH HHHHHHHH
Maska podsieci        11111111 11111111 11111000 00000000
```

gdzie **`s`** oznacza bit maski podsieci.
Jeśli w tym samym segmencie lub podsieci danej sieci są dwa hosty, to muszą one mieć taką samą tożsamość sieci i taką samą tożsamość podsieci. Jeżeli są one w różnych podsieciach, to mają identyczne tożsamości sieci, ale różne tożsamości podsieci.
Przykładowo:

```
Adres IP 1        10000011 00001011 10010011 00100000 (131.11.147.64)
Adres IP 2        10000011 00001011 10010100 00110000 (131.11.148.96)
Maska podsieci    11111111 11111111 11111000 00000000 (255.255.248.0)
```

są w tej samej sieci. Jednak adresy IP:

```
Adres IP 3        10000011 00001011 10011011 00100000 (131.11.153.64)
Adres IP 2        10000011 00001011 10010101 00110000 (131.11.149.96)
Maska podsieci    11111111 11111111 11111000 00000000 (255.255.248.0)
```

są w różnych podsieciach. By dwa adresy mogły być w tej samej sieci, bity, które odpowiadają binarnym jedynkom w masce podsieci, muszą być identyczne dla obu adresów.

2.2 Obliczanie liczby podsieci i hostów

Mając tożsamość sieci i maskę podsieci, ile podsieci możemy utworzyć i ile hostów może rezydować w każdej z podsieci?
Przykładowo wzięto 3 bity podsieci. W adresie IP, bity te mogą przybierać następujące wartości:

```
000
001
010
011
100
101
110
111
```

Należy wykluczyć wartości 000 i 111, gdyż bity podsieci w adresie IP nie mogą być samymi jedynkami ani samymi zerami. Pozostaje sześć wartości (możliwych) dla bitów podsieci.
Ogólnie jest 2^x–2 możliwych podsieci, gdzie *x* to liczba bitów podsieci. W rozpatrzonym wcześniej przykładzie jest 5 bitów podsieci, a więc jest 2^5–2 (tj. 30) podsieci.

Przedstawiony przykład to podzielona na podsieci sieć *klasy B*. Dokładnie te same zasady można zastosować wobec sieci *klasy A* i *klasy C*.

2.3 Obliczanie zakresu adresów IP dla podsieci

Po obliczeniu liczby podsieci oraz liczby hostów na podsieć dla pary typu adres IP — maska podsieci, następny krok to rozpracowanie zakresu adresów IP dla każdej z podsieci. Aby zilustrować tę technikę, wykorzystamy przykład, który rozważyliśmy wcześniej: tożsamość sieci o wartości 131.11.0.0 z maską podsieci o wartości 255.255.248.0 (czasami zapisywaną 131.11.0.0/21).
Stosowane są trzy reguły:

- bity maski podsieci nie mogą być samymi zerami,
- bity tożsamości hosta nie mogą być samymi zerami,
- bity tożsamości hosta nie mogą być samymi jedynkami.

Zatem pierwsza wartość podsieci, jakiej możemy użyć, to 0001, pierwsza tożsamość hosta, jaką możemy określić, to 0000000001, a ostatnia tożsamość hosta, jaką możemy określić, to 11111111110. Dla pierwszej podsieci daje to wartości:

```
Tożsamość sieci                 10000011 00001011 00000000 00000000
(131.11.0.0)
Maska podsieci                  11111111 11111111 11111000 00000000
(255.255.248.0)
Pierwszy adres IP               10000011 00001011 00001000 00000001
(131.11.8.1)
Ostatni adres IP                10000011 00001011 00001111 11111110
(131.11.15.254)
```

W podanym przykładzie zakres adresów IP dla pierwszej podsieci to 131.11.8.1 do 131.11.15.254. Zastosowanie tych samych obliczeń do drugiej podsieci daje zakres od 131.11.16.1 do 131.11.23.254. Tę samą technikę można zastosować wobec dowolnej pary typu tożsamość sieci — maska podsieci; można też wyprowadzić tablicę zakresów podobną do tabeli 1.

Tabela 1.

Podsieć	Zakres adresów
1	131.11.8.1 do 131.11.15.254
2	131.11.16.1 do 131.11.23.254
3	131.11.24.1 do 131.11.31.254
-	- - - - - - - - - - - - - - - - - - -
-	- - - - - - - - - - - - - - - - - - -
30	131.11.240.1 do 131.11.247.254

Inne przykłady podziału sieci na podsieci:
Przykład1.
Podział sieci na dwie podsieci

Dana jest sieć o adresie: 192.168.100.0
Maska sieci to: 255.255.255.0

Zapis bitowy:

11000000.10101000.01100100.00000000 – adres
11111111.11111111.11111111.00000000 – maska

Należy wyznaczyć broadcast poprzez przepisanie wszystkich bitów adresu, dla których bit maski ma wartość 1, wartość 0 w masce uzupełniamy jedynkami.

Stąd 10000000.10101000.01100100.11111111 – Broadcast

192.168.100.255 – jest to adres rozgłoszeniowy sieci – Broadcast, dzięki niemu wiadomo, że adresy w sieci mogą znajdować się w zakresie 1-254
Reasumując
192.168.100.0 – adres sieci
192.168.100.1 - 192.168.100.254 – adresy w sieci
192.168.100.255 – broadcast

Aby dokonać podziału danej sieci na dwie podsieci należy wykorzystać 25 bit adresu.

Maska podsieci to: 255.255.255.128

z tego wynika następujący podział:

192.168.100.0 – adres I podsieci – bit 25 ma wartość 0
192.168.100.1 – 192.168.100.126 – adresy w podsieci
192.168.100.127 - broadcast

192.168.100.128 – adres II podsieci – bit 25 ma wartość 1
192.168.100.129 – 192.168.100.254 – adresy w podsieci
192.168.100.255 – broadcast

Przykład:2.

Podział sieci na cztery podsieci

Dana jest sieć o adresie: 192.168.100.0
Maska sieci to: 255.255.255.128

Zapis bitowy:

11000000.10101000.01100100.00000000 – adres
11111111.11111111.11111111.10000000 – maska

Należy wyznaczyć broadcast poprzez przepisanie wszystkich bitów adresu, dla których bit maski ma wartość 1, wartość 0 w masce uzupełniamy jedynkami.

Stąd 10000000.10101000.01100100.01111111 – Broadcast

192.168.100.127 – Jest to adres rozgłoszeniowy sieci – Broadcast, dzięki niemu wiadomo, że adresy w sieci mogą znajdować się w zakresie 1-126

Reasumując:
192.168.100.0 – adres sieci
192.168.100.1 - 192.168.100.126 – adresy w sieci
192.168.100.127 – broadcast

Aby dokonać podziału danej sieci na cztery podsieci należy wykorzystać 26 i 27 bit adresu

Maska podsieci to: 255.255.255.224

z tego wynika następujący podział

192.168.100.0 – adres I podsieci – bit 25 ma wartość 0, 26 ma wartość 0
192.168.100.1 – 192.168.100.30 – adresy w podsieci
192.168.100.31 - broadcast

192.168.100.32 – adres II podsieci – bit 25 ma wartość 0, 26 ma wartość 1
192.168.100.33 – 192.168.100.62 – adresy w podsieci
192.168.100.63 – broadcast

192.168.100.64 – adres II podsieci – bit 25 ma wartość 1, 26 ma wartość 0
192.168.100.65 – 192.168.100.94 – adresy w podsieci
192.168.100.95 – broadcast

192.168.100.96 – adres II podsieci – bit 25 ma wartość 1, 26 ma wartość 1
192.168.100.97 – 192.168.100.126 – adresy w podsieci
192.168.100.127 – broadcast

Przykład 3.

Dana jest sieć o adresie 172.24.150.192/27. Należy podzielić ją na dwie podsieci.

Zapis bitowy adresu u maski:

101011000.00011000.10010110.11000000 – adres IP
11111111.11111111.11111111.11100000 – maska sieci

Z tych informacji jasno widać, że na adresy komputerów pozostaje 5 bitów adresu. Chcąc dokonać podziału sieci na dwie podsieci należy do ich oznaczenia wykorzystać 28 bit adresu. A co za tym idzie na adresy hostów pozostaną 4 bity adresu.

101011000.00011000.10010110.11000000 – 28 bit adresu wykorzystany do podziału na podsieci

11111111.11111111.11111111.11110000 – maska dla podsieci

Adres pierwszej podsieci to : 172.24.150.192
Broadcast: 172.24.150.207
Zakres adresów: 172.24.150.193 – 172.24.150.206

Adres drugiej podsieci to: 172.24.150.208
Broadcast: 172.24.150.223
Zakres adresów: 172.24.150.209 – 172.24.150.222

2.4Formaty zapisu maski

Chociaż format dziesiętny kropkowy uznawany bywa za „staroświecki”, to jest on nadal formatem często używanym. Zgrabniej jest określić daną sieć jako 195.162.230.0/24 zamiast 195.162.230.0, maska podsieci 255.255.255.0, ale ten drugi format przekłada się bardziej na informacje, które trzeba wpisać w oknach dialogowych konfiguracji. Format dziesiętny kropkowy jest często stosowany w obliczeniach podziału na podsieci, podczas gdy bezklasowe wybieranie trasy (CIDR) i łączenie w nadsieć mogą z powodzeniem korzystać z notacji skróconej. Dobrze jest więc znać obie te konwencje.

Funkcją maski podsieci jest identyfikowanie, która część adresu IP określa sieć, a która część określa hosta. Jedynki określają, że odpowiadające im bity w adresie IP to bity sieci, a zera określają bity hosta. W przypadku tradycyjnego adresowania klasowego, początkowe bity adresu określają klasę adresu, która z kolei określa zakres hosta i sieci. Stąd, kiedy wprowadzano adresy IP oraz adresowanie klasowe, nie zostały zaimplementowane maski sieci.
Jednak analiza początkowych bitów adresu jest nużąca, a maski podsieci upraszczają ten proces. Binarna operacja AND sprawia, że zera w masce podsieci maskują część hosta w adresie IP, pozostawiając tylko te bity, które identyfikują sieć, albo *prefiks sieci*. Adresy *klasy A* (adresy */8*) mają domyślną maskę podsieci */8* (255.0.0.0). *Klasy B* i *C* mają domyślne maski podsieci, odpowiednio, */16* (255.255.0.0) i */24* (255.255.255.0).

Pierwotnie maski podsieci wprowadzono, by ułatwić obliczanie adresu sieciowego. W późniejszym czasie zaczęły być wykorzystywane do innego celu — by dzielić sieci *klasy A*, *B* oraz *C* na mniejsze części za pomocą techniki znanej jako *podział na podsieci*.

([5])

3 MASKA O ZMIENNEJ DŁUGOŚCI

VLSM, czyli maska o zmiennej długości bywa mylona z pojęciem podziału na podsieć, gdyż podział ten polega właśnie na zmianie długości maski podsieci.

Dokonując podziału sieci na podsieci rozbija się ją na segmenty, z których wszystkie są tej samej wielkości. Pojedynczą maskę podsieci, aczkolwiek nie domyślną maskę podsieci, stosuje się wobec całej sieci.

Dokument RFC 1009 (1987r.)określił, w jaki sposób sieć może wykorzystywać więcej niż jedną maskę podsieci, aby implementować segmenty różnej długości. VLSM umożliwia przypisanie danej sieci więcej niż jednej maski, w związku z czym rozszerzone prefiksy sieci różnych segmentów sieci mają różne długości.

Niektóre protokoły routingu, takie jak protokół routingu internetowego w wersji 1 (RIPv1), wymagają jednolitych masek podsieci w obrębie całego prefiksu sieci. RIPv1 pozwala na użycie tylko pojedynczej maski podsieci z każdym z numerów sieci, ponieważ nie zapewnia on informacji o maskach podsieci w ramach swoich komunikatów uaktualnień tablicy tras.

Protokół RIPv2 i protokół otwierania najkrótszej ścieżki w pierwszej kolejności (OSPF) dopuszczają VLSM. Korzyści płynące z przydzielania wielu masek podsieci danemu numerowi IP sieci:

- możliwe jest bardziej wydajne wykorzystanie przydzielonej przestrzeni adresów IP.
- Możliwe jest zespalanie tras, co przyczynia się do znacznego ograniczenia informacji dotyczących routingu w obrębie domeny routingu danej organizacji.

([5])

3.1Wydajne wykorzystanie dostępnej przestrzeni adresowej

Obsługiwanie tylko jednej maski podsieci w obrębie danego prefiksu sieci stwarzało problem związany z koniecznością stałego rozmiaru podsieci. Przykładowo sieć 131.11.0.0/21 zapewnia 30 podsieci, przy czym każda z nich ma 2046 hostów. Podsieć *klasy B* została przydzielona przedsiębiorstwu posiadającemu dwa duże zakłady, z których każdy wymaga około 5 000 adresów IP. Ponadto przedsiębiorstwo ma 25 filii, z których każda wymaga najwyżej 200, a często znacznie mniej, adresów IP.

Oba z tych dużych zakładów potrzebowałyby co najmniej trzech podsieci, a przydzielono by im prawdopodobnie cztery. Oznacza to poważną i być może niepotrzebną, inwestycję w routery. Mogą być inne powody segmentowania sieci liczącej 8 000 użytkowników (jak na przykład ograniczanie ruchu emisji), ale konstruktor sieci powinien mieć wybór określenia najbardziej wydajnej segmentacji, a nie powinien być zmuszony do zastosowania segmentów liczących 2 000 hostów.

Ponieważ każda z filii (po 200 użytkowników każda) musi korzystać z podsieci liczącej 2000 hostów, znaczna liczba adresów jest marnowana. W rzeczywistości przy ośmiu podsieciach już przydzielonych dużym zakładom przedsiębiorstwu nie pozostaje wystarczająco dużo podsieci, aby przydzielić jedną każdej z filii. Dlatego też potrzebuje ono albo drugiej sieci, pomimo że wykorzystuje o wiele mniej adresów IP, niż 65 000, które (teoretycznie) zapewnia jego sieć *klasy B*, albo też musi implementować maskę podsieci */22* (62 podsieci). To drugie rozwiązanie prowadziłoby do jeszcze większej liczby routerów w dużych zakładach oraz do dwukrotnego wzrostu ogłaszanych tras.

Rozwiązanie VLSM polega na określeniu sześciu podsieci */19* o pojemności 2^{13}–2 (tj. 8 190) adresów hostów każda. Dwie z nich mogą zostać przydzielone dużym zakładom, a trzecia może zostać bardziej podzielona przy użyciu maski podsieci */24* — co daje 30 podsieci liczących 254 użytkowników. Przedsiębiorstwu pozostają jeszcze trzy podsieci */19* lub połowa przydzielonej mu przestrzeni adresowej, na przyszły rozwój.

Rysunek 3.1.1 przedstawia tę strategię podziału na podsieci.

30 pod-podsieci

Pod-podsieć /24
254 hosty

6 podsieci szkieletowych

Podsieć /19
8190 hostów

Sieć /16
65 tys. Hostów

Rysunek 3.1.1 Wykorzystywanie VLSM do implementowania wydajnej segmentacji sieci

Rysunek 3.1.1 Wykorzystywanie VLSM do implementowania wydajnej segmentacji sieci

([5])

3.2Algorytm najdłuższego dopasowania

Routery implementują spójny algorytm przekazywania oparty na algorytmie *najdłuższego dopasowania*. Jeżeli wykorzystywany jest VLSM, to większe podsieci (z mniejszymi prefiksami sieci) zostają bardziej podzielone, tworząc mniejsze pod-podsieci (z większymi prefiksami sieci). Mówi się, że pod-podsieci są *bardziej określone*, ponieważ dłuższy prefiks sieci bliżej określa lokalizację danego hosta w sieci.
Na przykład na rysunku 2.2.1 trasa sieciowa do hosta 131.11.97.5 może być określona jako 131.11.0.0/16, 131.11.96.0/19, lub 131.11.97.0/24. Ponieważ te bardziej określone segmenty sieci są podsieciami tych mniej określonych segmentów, host jest na wszystkich trzech trasach.

131.11.97.0./24

131.11.96.0./19

131.11.0.0./16

Host 131.11.97.5

Rysunek 3.2.1 Algorytm najdłuższego dopasowania

Przy użyciu algorytmu najdłuższego dopasowania router przekazujący będzie routował do najbardziej określonej sieci, to jest 131.11.97.0/24. Oznacza to, że host 131.11.97.5 musi być zainstalowany w podsieci 131.11.97.0/24. Gdyby, przez pomyłkę, host ten został podłączony do sieci szkieletowej 131.11.96.0/19, nie udałoby się go nigdy osiągnąć.

3.3Zespalanie tras

Wykorzystując VLSM dzieli się sieć na podsieci o największych wymaganych rozmiarach (podsieci szkieletowe). Następnie należy te podsieci ponownie podzielić już wg określonych potrzeb. Dzięki temu można zebrać i zespolić przestrzeń adresową ograniczając tym samym

ilość informacji dotyczących routingu na najwyższym poziomie oraz ukryć szczegółową strukturę informacji routingu dla jednej z grup podsieci przed inną grupą podsieci.

Przykład:

By podsieci wcześniej rozważanej sieci nie były rozgłaszane wewnętrznie i zewnętrznie przez tablicę tras przedsiębiorstwa należy zastosować rozwiązanie VLSM.
Router A ogłasza w Internecie tylko jedną pozycję sieciową tablicy tras (131.11.0.0/16). *Router B* zespala wszystkie podsieci */24* w jedną tożsamość podsieci */19*, którą ogłasza w sieci szkieletowej organizacji. Prowadzi to do powstania mniejszych tablic tras i zmniejszenia się ruchu ogłoszeń routingu.

131.11.98.0./24

131.11.97.0./24 Router B

131.11.96.0./19 Router A

131.11.0.0./16

131.11.64.0./19

131.11.32.0./19

Rysunek 3.3.1 Zespalanie tras przy użyciu VLSM

3.4Wdrażanie VLSM

Wdrażanie hierarchicznego schematu podziału na podsieci, który zapewnia VLSM wymaga starannego planowania. Należy dokładnie przestudiować plan adresów i upewnić się, że najmniejsze podsieci będą mogły obsługiwać wymaganą liczbę hostów. O ile VLSM jest wdrażany przy użyciu logicznej struktury hierarchicznej — tak, aby plan adresów odzwierciedlał strukturę, albo *topologię* sieci — to adresy z każdej spośród podsieci mogą być zespalane w pojedynczy blok adresowy, który powstrzymuje tablice tras sieci szkieletowej od stawania się zbyt dużymi.
Istnieją trzy warunki zapewniające pomyślne wdrażanie VLSM:

- Protokoły routingu muszą nieść rozszerzone informacje o prefiksach sieci wraz z każdym ogłoszeniem tras. Takie protokoły, jak RIPv2 i OSPF mają tę funkcję.
- Routery muszą implementować algorytm najdłuższego dopasowania.
- Adresy muszą być przydzielone tak, aby miały znaczenie topologiczne, umożliwiając w ten sposób zespalanie tras....

([5])

3.5Opracowywanie maski podsieci

Przy podziale na podsieci wszystkie obliczenia biorą się z liczby bitów podsieci. Normalnie istnieje maksimum wynoszące 8 bitów podsieci. Może być więcej — sieć *klasy B* mogłaby być, przykładowo, podzielona na 510 podsieci liczących po 126 hostów — ale taki poziom podziału jest rzeczą niezwykłą. Bity podsieci nie mogą być samymi jedynkami, ani samymi zerami. Dlatego też może być tylko 1 bit podsieci. Zakres bitów podsieci z praktycznego punktu widzenia wynosi zatem 2 do 8.

Aby opracować maskę podsieci dla danej liczby bitów podsieci, należy wykonać następujące czynności:

1. Określić, czy sieć jest siecią *klasy A*, *B*, czy *C*.
2. Wziąć domyślną maskę podsieci (odpowiednio */8*, */16*, lub */24*) i dodać liczbę bitów podsieci. W ten sposób sieć *klasy B* (*/16*) mająca 3 bity podsieci ma maskę podsieci */19*.
3. Aby obliczyć maskę podsieci w kropkowej notacji dziesiętnej należy wziąć pierwszy oktet zerowy domyślnej maski podsieci. W przypadku *klasy B* (255.255.0.0) jest to trzeci oktet.
4. Przekształcić najbardziej znaczące bity tego oktetu na jedynki, aby pasowały do bitów maski podsieci. To znaczy, jeżeli są 3 bity maski podsieci, to przekształcić 3 pierwsze bity oktetu na jedynki.
5. Obliczyć dziesiętną wartość oktetu, zważywszy, że binarne 10000000 równa się 128, 01000000 równa się 64 i tak dalej.
6. Z tych obliczeń wygenerowana zostanie tabelę 2

Tabela 2. Opracowywanie maski podsieci

Bity podsieci	Maska
2	192
3	224
4	240
5	248
6	252
7	254
8	255

([5])

3.6Obliczanie liczby podsieci

Liczbę podsieci można obliczyć z liczby bitów podsieci. By tego dokonać należy:

1. Obliczyć 2^x, gdzie *x* stanowi liczbę bitów podsieci (2^2=4, 2^3=8, 2^4=16 i tak dalej).
2. Odjąć 2 od każdej z tych liczb.
3. Dołączyć wyniki do tabeli 2, aby wygenerować tabelę 3

Tabela 3. Dodawanie liczby podsieci

Bity podsieci	Maska	Podsieci
2	192	2
3	224	6
4	240	14

5	248	30
6	252	62
7	254	126
8	255	254

3.7 Obliczanie przyrostu

Przyrost to wartością wykorzystywaną do obliczania zakresu adresów w każdej z podsieci. Reprezentuje ona różnicę albo *skok* w obrębie odpowiedniego oktetu, (drugiego w przypadku *klasy A*, trzeciego w przypadku *klasy B*, czwartego w przypadku *klasy C*) pomiędzy adresami początkowymi dla każdej z podsieci.
By obliczyć przyrost należy:

1. Wziąć uprzednio obliczoną wartość oktetu z maski podsieci.
2. Odjąć tę wartość od 256.
3. Dodać wartości przyrostu do tabeli 3, aby wygenerować tabelę 4.

Tabela 4. Dodawanie wartości przyrostu

Bity podsieci	Maska	Podsieci	Przyrost
2	192	2	64
3	224	6	32
4	240	14	16
5	248	30	8
6	252	62	4
7	254	126	2
8	255	254	1

([5])

3.8 Obliczanie liczby hostów na podsieć

Obliczanie liczby hostów na podsieć nie jest czynnością bardzo skomplikowaną, nawet w systemie binarnym. Aby obliczyć liczbę hostów należy:

1. Wziąć liczbę bitów domyślnie przydzielonych tożsamościom hostów (24 dla *klasy A*, 16 dla *klasy B*, 8 dla *klasy C*).
2. Odjąć liczbę bitów podsieci, aby otrzymać wartość *y*.
3. Obliczyć 2^y dla każdego rzędu w tabeli.
4. Odjąć 2 od każdej wartości (ponieważ adresem hosta nie mogą być same jedynki ani same zera).
5. Dodać uzyskane liczby hostów do tabeli 4, aby uzyskać wykres podsieci przedstawiony w tabeli 5 Zazwyczaj nie ma potrzeby dokładnego obliczania liczby hostów powyżej 510; dlatego też stosuje się przybliżenia.

Tabela 5. Wykres podsieci

Bity podsieci	Maska	Podsieci	Przyrost	Hosty *klasy A*	Hosty *klasy B*	Hosty *klasy C*
2	192	2	64	4M	16K	62
3	224	6	32	2M	8K	30
4	240	14	16	1M	4K	14
5	248	30	8	500K	2K	6
6	252	62	4	250K	1K	2
7	254	126	2	130K	510	—
8	255	254	1	65K	254	—

3.9 Dzielenie sieci klasy A na podsieci

Duże przedsiębiorstwa czasem używają sieci *klasy A* (szczególnie 10.0.0.0) w intranetach firmowych. Przykładowe międzynarodowe przedsiębiorstwo wymaga ogólnej liczby 70 podsieci. Chociaż większość z nich będzie względnie małych, dyrekcja przewiduje zapotrzebowanie w wysokości 80 tys. hostów w jednej z nich. Korzysta się ze specyfikacji wewnętrznego adresu intranetowego 10.0.0.0/8 (RFC 1918). Kierownik techniczny chce wiedzieć, czy hosty 10.2.4.213 i 10.6.1.14 będą w tej samej podsieci. Aby zaimplementować wymaganą strukturę podsieci należy:

1. Wybrać liczbę bitów podsieci. Według tabeli 4.6 wybór 7 bitów podsieci daje 126 sieci, co spełnia wymogi i pozostawia miejsce na rozbudowę.
2. Sprawdzić liczbę hostów na podsieć. Sieć *klasy A*, która ma 7 bitów podsieci, dopuszcza 130 tys. hostów na sieć. Spokojnie mieści się to w granicach wymogów.
3. Uzyskać maskę podsieci. Według tabeli 4.6, wartość drugiego oktetu (jako że jest to sieć *klasy A*) wynosi 254. Zatem maska podsieci to 255.254.0.0 (lub */15*).
4. Zastosować przyrost. Według tabeli 4.6 wynosi on 2. Zatem podsieci to 10.2.0.0/15, 10.4.0.0/15, 10.6.0.0/15 i tak dalej.
5. Dodać zakresy adresów hostów. Adresy hostów nie mogą być samymi jedynkami, ani samymi zerami, więc zakresy adresów to 10.2.0.1 do 10.3.255.254, 10.4.0.1 do 10.5.255.254, 10.6.0.1 do 10.7.255.254 i tak dalej.
6. Skontrolować strukturę sieci, którą uzyskano. Host 10.2.4.213 jest w sieci 10.2.0.0, a host 10.6.1.14 jest w sieci 10.6.0.0. A zatem nie są one w tej samej podsieci.

3.10 Dzielenie sieci klasy B na podsieci

Zazwyczaj przedsiębiorstwo, któremu została przydzielona sieć *klasy B* lub zaimplementowało prywatną sieć wewnętrzną *klasy B* w swoim intranecie, potrzebuje podziału na podsieci.
Przykładowe przedsiębiorstwo aktualnie wymaga 28 podsieci w swojej sieci *klasy B*, 155.62.0.0. Obecnie maksymalna liczba hostów w każdej z podsieci wynosi 250 Założono, że liczba ta nie przekroczy 500 w najbliższej przyszłości. Istnieje wymóg, aby hosty 155.62.10.6 i 155.62.15.230 nie dzieliły ze sobą tej samej podsieci. Aby implementować wymaganą strukturę podsieci, należy wykonać następujące czynności:

1. Wybrać liczbę bitów podsieci. Według tabeli 4.6 wybór zarówno 5 bitów podsieci (30 podsieci), jak i 6 bitów sieci (62 podsieci) spełnia wymogi, przy czym druga z opcji daje więcej miejsca na przyszłą rozbudowę.
2. Sprawdzić liczbę hostów na podsieć. Jeżeli wybrano 5 bitów podsieci, to każda z podsieci będzie w stanie pomieścić w przybliżeniu 2 000 hostów. Wybór 6 bitów podsieci ogranicza maksymalną liczbę hostów na podsieć do około 1 000. Obydwie liczby spokojnie mieszczą się w granicach wymogów.

3. Zastosować przyrost. Dla 5 bitów podsieci jest to 8, dla 6 bitów podsieci — 4. Stąd też wybór podsieci to:
- *5 bitów podsieci* — 155.62.8.0/21, 155.62.16.0/21, 155.62.24.0/21 i tak dalej,
- *6 bitów podsieci* — 155.62.4.0/22, 155.62.8.0/22, 155.62.12.0/22 i tak dalej.

4. Zastosować wymóg sformułowany w specyfikacji. Jeżeli wybrano 5 bitów podsieci, to hosty 155.62.10.6 i 155.62.15.230 będą razem w sieci 155.62.8.0/21. Jeżeli jednak wybrano 6 bitów podsieci, to będą one, odpowiednio, w podsieciach 155.62.8.0/22 i 155.62.12.0/22. Dlatego też wybór powinien paść na 6 bitów podsieci.
5. Uzyskać maskę podsieci. Według tabeli 4.6, wartość trzeciego oktetu (jako że jest to sieć *klasy B*) wynosi 252. A zatem maska sieci to 255.255.254.0.0 (lub */22*).
6. Dodać zakresy adresów hostów. Adresy hostów nie mogą być samymi jedynkami, ani samymi zerami, więc zakresy adresów to 155.62.4.1 do 155.62.7.254, 155.62.8.1 do 155.62.11.254, 155.62.12.1 do 155.62.15.254 i tak dalej.

([5])

3.11 Dzielenie sieci klasy C na podsieci

Przykład:
Firma wymaga ogólnej liczby czterech sieci. W żadnej z tych podsieci nigdy nie będzie więcej, niż 20 hostów. Przydzielono klasę C 195.162.230.0/24. By zaimplementować wymaganą strukturę sieciową, należy:

1) Wybrać liczbę bitów podsieci. Wg tabeli 4.6 wybór 3 bitów podsieci daje 6 sieci liczących maksymalnie po 30 hostów. To spełnia wymogi.
2) Uzyskać maskę podsieci. Wg tabeli 4.6, wartość czwartego oktetu (jako że jest to sieć *klasy C*) wynosi 224. Zatem maska podsieci to 255.255.255.224 (lub */27*).
3) Zastosować przyrost. Wg tabeli 4.6 wynosi on 32. A zatem podsieci to 195.162.230.32/27, 195.162.230.64/27, 195.162.230.97/27 i tak dalej.
4) Dodać zakresy adresów hostów. Adresy hostów nie mogą być samymi jedynkami, ani samymi zerami, więc zakresy adresów to 195.162.230.33 do 195.162.230.62, 195.162.230.65 do 195.162.230.94, 195.162.230.97 do 195.162.230.126 i tak dalej.

3.12 Podział segmentu VLSM na podsieci

Dzielenie segmentu na podsieć w przypadku VLSM odbywa się na tych samych zasadach, co podział „zwykły". Podziału można dokonać poprzez granice klas jaki i podziału segmentu.
Przykład:
Zadanie polega na podziale podsieci 155.62.12.0/22 sieci klasy B na największą możliwą liczbę pod-podsieci. Ograniczeniem jest liczba hostów w każdej z podsieci równa 40. Wewnętrzny podział podsieci szkieletowej wymaga, aby został wdrożony VLSM. Wykorzystywany jest protokół routingu niosący rozszerzone informacje o prefiksie sieci wraz z każdym ogłoszeniem trasy oraz routery sieci implementują algorytm najdłuższego dopasowania.
By dokonać dalszej segmentacji podsieci szkieletowej 155.62.12.0/22 należy:

5) Wg tabel 4.6 określić podsieć spełniającą ograniczenie dotyczące liczby hostów (czyli sieć klasy C, ponieważ może mieć ona do 62 hostów).
6) Uzyskać maskę podsieci dla tej podsieci (zatem maska ta określona jest jako 255.255.255.192, lub */26*.)
7) Uzyskać przyrost. Ponieważ przekroczono granicę klas, przyrost ten stosuje się do czwartego oktetu adresu (według tabeli 4.6, przyrost ten wynosi 64)

8) Zastosować przyrost. (Podsieci to 155.62.12.64/26, 155.62.12.128/26, 155.62.12.192/26, 155.62.13.0/26 i tak dalej, aż do 155.62.15.128/26.)
9) Dodać tożsamości hostów. (Daje to zakresy adresów 155.62.12.65 do 155.62.12.126, 155.62.12.129 do 155.62.12.190, 155.62.12.193 do 155.62.12.254, 155.62.13.1 do 155.62.13.62 i tak dalej)
10) By obliczyć maksymalną liczbę pod-podsieci należy od maski pod-podsieci (/26) odjąć maskę podsieci szkieletowej (/22).W dłuższym z tych prefiksów są cztery dodatkowe bity podsieci. Liczba pod-podsieci wynosi zatem 2^4–2, czyli 14.

3.13 Łączenie sieci klasy C w nadsieć

Przy łączeniu w nadsieć należy pamiętać o limicie granicy. Jeżeli zachodzi potrzeba połączenia dwóch sieci *klasy C* w nadsieć, to wartość trzeciego oktetu niższego adresu musi być podzielna przez 2. W przypadku czterech sieci, wartość ta musi być podzielna przez 4 i tak dalej. Sieci muszą być przyległe i poddaje się je łączeniu w nadsieć w grupach po 2, 4, 8, 16 i tak dalej (potęgi liczby dwa).
Przykład:
Mamy cztery sieci klasy C 207.23.68.0 do 207.23.71.0. Należy je połączyć w pojedynczą sieć. Należy sprawdzić, czy jest to możliwe, obliczyć maskę podsieci i zakres adresów.

1) Czy sieci są przyległe? (są przyległe) Czy wartość trzeciego oktetu najniższej sieci (68) jest podzielna przez 4? (jest podzielna) Zatem sieci te mogą zostać połączone.
2) Domyślną maskę podsieci klasy B (/24) należy skrócić o odpowiednią liczbę bitów. By połączyć dwie sieci należy skrócić ja o jeden bit; by połączyć cztery – o dwa bity; by połączyć osiem — należy skrócić ją o trzy i tak dalej. W danym przykładzie skracamy maskę o dwa bity. Stąd maska podsieci to */22* lub 255.255.252.0.
3) A zatem połączona sieć to 207.23.68.0/22. Należy dodać tożsamości hostów, aby otrzymać zakres adresów od 207.23.68.1 do 207.23.71.254.

LITERATURA

[1] S. Siyan Karanijt „Windows NT: TCP/IP” Wyd. Robomatic Wrocław 1998r.

[2] Kosowicz Piotr „Sieci komputerowe: polski i angielski słownik terminologii”

[3] Bartosz Kiziukiewicz „Sieci lokalne” (książka w formie eletronicznej)

[4] Przykłady i informacje zaczerpnięto z internetu m.in.:

http://www.elektronet.gower.pl/pc043.htm

http://www.republika.pl/kmis/adresow.htm

linuxpub.w.interia.pl/dl/sieci.pdf ...

[5] materiały własne