Adresacja w sieciach

Protokół IPv4

- Protokół IPv4 został szczegółowo opisany w dokumencie RFC 791. Sam protokół IP został opracowany do działania w sytuacjach ekstremalnych, np. w trakcie wojny. W normalnych warunkach jego funkcja sprowadza się do wyboru optymalnej trasy i przesyłania nią pakietów. W przypadku wystąpienia awarii, na którymś z połączeń protokół będzie próbował dostarczyć pakiety trasami alternatywnymi (nie zawsze optymalnymi). Protokół IP jest podstawowym protokołem przesyłania pakietów w Internecie.
- Protokół IP jest protokołem bezpołączeniowym. Oznacza to, że w celu przesłania pakietów nie jest nawiązywane połączenie z hostem docelowym. Pakiety mogą być przesyłane różnymi trasami do miejsca przeznaczenia, gdzie są następnie składane w całość. Podobna zasada działa przy przesyłaniu listów tradycyjnym systemem pocztowym. Tutaj również w momencie wysyłania listu adresat nie musi potwierdzać, że przesyłkę odbierze.
- Do przesyłania danych protokół IP używa specjalnego formatu pakietu. Pakiet ten składa się z nagłówka pakietu oraz danych do przesłania. Zgodnie z zasadą przesyłania strumieniowego dane protokołu IP są danymi pochodzącymi z wyższych warstw modelu ISO/OSI. Dane te są następnie enkapsulowane do postaci pakietu IP. Przy przejściu do warstwy łącza danych pakiet IP jest enkapsulowany do postaci ramki Ethernetowej.

Pakiet IPv4

+	Bity 0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Wersja	Długość nagłówka	Typ usługi	Całkowita długość	
32	Numer identyfikacyjny			Flagi	Kontrola przesunięcia
64	Czas życia pakietu (TTL)		Protokół warstwy wyższej	Suma kontrolna nagłówka	
96	Adres źródłowy IP				
128	Adres docelowy IP				
160	Opcje IP				Uzupełnienie
192	Dane				

- Poszczególne pola pakietu mają następujące znaczenie:
- wersja (VERS) - pole 4-bitowe określające typ protokołu IP. Jeśli jest tam wpisana wartość 4 oznacza to wersję czwartą protokołu. Jeśli jest tam wartość 6 oznacza to IPv6..
- długość nagłówka (HLEN) - pole 4 bitowe określające długość datagramu wyrażoną jako wielokrotność słów 32 bitowych.
- typ usługi (TOS ang. Type-of-Service) - 8-bitowe pole określające poziom ważności jaki został nadany przez protokół wyższej warstwy. Znaczenie poszczególnych bitów tego pola jest następujące:
  - pierwsze 3 bity: wartość 0 - stopień normalny, wartość 7 - sterowanie siecią
  - czwarty bit - O - prośba o krótkie czasy oczekiwania
  - piąty bit - S - prośba o przesyłanie danych szybkimi łączami
  - szósty bit P - prośba o dużą pewność przesyłania danych
  - bity 6, 7 nieużywane
- całkowita długość - pole 16-bitowe. Długość całego pakietu wyrażona w bajtach.
  - W celu uzyskania długości pola danych należy odjąć od długości całkowitej długość nagłówka.
  - Wartość minimalna wynosi 576 oktetów zaś maksymalna 65535 oktetów, tzn. 64 kB Identyfikacja - 16 bitowe pole używane do określania numeru sekwencyjnego bieżącego datagramu.
- Znaczniki - 3 bitowe pole. Pierwszy najbardziej znaczący ma zawsze wartość 0. Kolejne znaczące bity sterują fragmentacją
  - 0- oznacza, czy pakiet może zostać podzielony na fragmenty,
  - 1 - nie może być podzielony.

  Trzeci bit oznacza: ostatni pakiet powstały w wyniku podzielenia (jeśli ma wartość 1) lub pakiet ze środka 0.

- Przesunięcie fragmentu - 13-bitowe pole służące do składania fragmentów datagramu.
- Czas życia (TTL, ang. Time To Live) - 8-bitowe pole określające liczbę routerów (przeskoków), przez które może być przesłany pakiet. Wartość tego pola jest zmniejszana przy przejście przez każdy router na ścieżce. Gdy wartość tego pola wynosi 0, wtedy pakiet taki jest odrzucany. Zasada ta pozwala na stosowanie mechanizmów zapobiegających zapętlaniu się tras routingu.
- Protokół - 8-bitowe pole określające, który z protokołów warstwy wyższej odpowiada za przetworzenie pola Dane.
- Suma kontrolna nagłówka - 16-bitowe pole z sumą kontrolną nagłówka pozwalającą stwierdzić, czy nie nastąpiło, naruszenie integralności nagłówka. Ze względu na fakt, że każdy router dokonuje zmian w nagłówku musi ona być przeliczona na każdym z routerów.
- Adres IP nadawcy - 32-bitowe pole z adresem IP nadawcy pakietu
- Adres IP odbiorcy - 32-bitowe pole z adresem IP odbiorcy pakietu
- Opcje - pole to nie występuje we wszystkich pakietach.
- Uzupełnienie (Wypełnienie) - pole to jest wypełnione zerami i jest potrzebne, żeby długość nagłówka była wielokrotnością 32 bitów (patrz-> Długość nagłówka) Dane - pole od długości do 64kB zawierające dane pochodzące z wyższych warstw.

Opcje w IPv4

Bajt kodu w polu opcje

Klasa opcji	Numer opcji	Długość	Opis
0	0	-	Koniec listy opcji-używane,gdy opcje nie kończą się wraz z końcem nagłówka
0	1	-	Brak przypisanej funkcji, służy do wyrównania bajtów w liście opcji
0	2	11	Ograniczenia związane z bezpieczeństwem i obsługą
0	3	zmienna	Zapisuj trasę - do śledzenia trasy
0	7	zmienna	Identyfikator strumienia - przestarzałe
0	8	4	Rygorystyczne trasowanie według nadawcy
0	4	zmienna	Używana do zapisywania czasów wzdłuż trasy pakietów

Protokół w IPv4

- W zależności od tego jaki protokół uformował pole danych oraz jaki powinien je przetworzyć w nagłówku pakietu musi być to zaznaczone.
- Polem odpowiedzialnym za identyfikację właściwego protokołu jest pole „Protokół”.
- Wartości wpisane w pole „protokół” nagłówka IP mają następujące znaczenie:
  - 1 - ICMP (ang. Internet Control Message Protocol) - protokół komunikacyjny sterowania siecią Internet
  - 2 - IGMP (ang. Internet Group Message Protocol) - protokół zarządzania grupami Internetowymi
  - 6 - TCP - (ang. Transmission Control Protocol) - protokół sterujący transmisją
  - 8 - EGP - (ang. Exterior Gateway Protocol) - zewnętrzny protokół bramowy
  - 17 - UDP - (ang. User Datagram Protocol) - protokół datagramów użytkownika

Protokół ICMP

- protokół IP nie sprawdza, czy dane dotarły do adresata. Rolę sprawdzania, czy pakiety docierają do adresata pełnią protokoły wyższych warstw.
- W ramach warstwy sieciowej sprawdzaniem dostępności sieci docelowej zajmuje się protokół ICMP (ang. Internet Control Message Protocol). Jego zadaniem nie jest rozwiązywanie problemów z zawodnością IP, ale zgłaszanie braku łączności. Protokół ten został zdefiniowany w dokumencie RFC 792.
- Komunikaty ICMP wysyłają zwykle bramy lub hosty. Najczęstsze powody wysyłania tych komunikatów to:
  - zbytnie obciążenie routera lub hosta
  - wysyłany jest komunikat ICMP, że należy zwolnić prędkość przesyłania komunikatów, bo host nie nadąża je przetwarzać
  - router lub host znajduje lepszą trasę - może wtedy wysłać do źródła komunikat o lepszej trasie
  - host docelowy jest nieosiągalny - wtedy ostatnia brama wysyła komunikat ICMP o niedostępności adresata i przesyła go do hosta źródłowego
  - pole TTL pakietu jest równe 0 - wtedy router może wysłać komunikat ICMP do źródła i odrzuca pakiet.

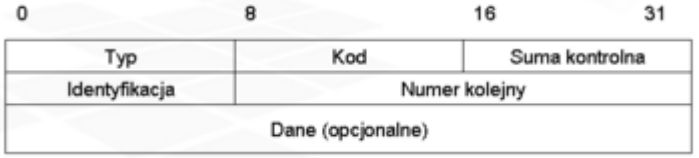
Dostarczanie komunikatu ICMP

- Jak zostało to pokazane na rysunku, sam komunikat ICMP jest przesyłany w datagramie IP. Komunikat ICMP składa się z nagłówka ICMP oraz danych ICMP. Warto przy tym zauważyć, że ze względu na zawodny charakter protokołu IP w momencie zaginięcia datagramu przenoszącego komunikat ICMP nie zostanie to zdiagnozowane. Wysyłanie komunikatów o błędach powodowałoby występowanie znacznego ruchu w sieci.

Format komunikatu ICMP

- Najważniejsze dane przesyłane w komunikacie ICMP zawarte są w polach TYP i KOD. Zatem wszystkie wersje komunikatów ICMP musza zawierać pola: Typ, Kod, Suma kontrolna. Znaczenie poszczególnych bajtów jest następujące:

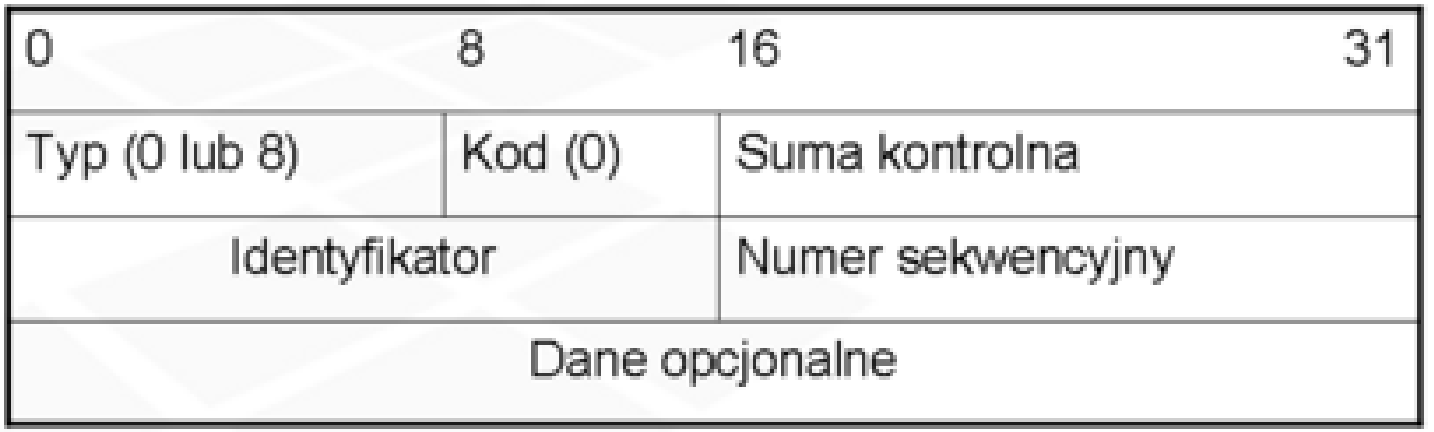
  Pole Typ: 0 - odpowiedź z echem (ang. Echo Reply) 3 - odbiorca nieosiągalny (ang. Destination Unreachable). 4 - zmniejszenie szybkości nadawania - tłumienie źródła (ang. source quench) 5 - zmiana trasowania - przekierowanie (ang. redirect). 8 - prośba o echo (ang. echo request) 9 - rozgłaszanie routera (ang. router advertisement) 10 - wywołanie routera (ang. router solicitation) 11 - przekroczenie TTL (ang. Time Exceeded) 12 - kłopot z parametrami datagramu 13 - prośba / żądanie o wysłanie znacznika czasu (ang. timestamp request) 14 - odpowiedź na prośbę / żądanie o wysłanie znacznika czasu (ang. timestamp reply) 15 - prośba o informację 16 - odpowiedź z informacją 17 - prośba o maskę adresu 18 - odpowiedź z maską adresu 30 - Traceroute 31 - błąd konwersji datagramu (ang. Datagram Conversion Error) 32 - przekierowanie hosta mobilnego (ang. Mobile Host Redirect) 33 - IPv6 Where-Are-You 34 - IPv6 Here-I-Am 35 - prośba o zarejestrowanie urządzenia mobilnego (ang. Mobile Registration Request) 36 - odpowiedź na prośbę o zarejestrowanie urządzenia mobilnego (ang. Mobile Registration Reply) 37 - żądanie nazw domeny (ang. Domain Name Request) 38 - zwrot nazwy domeny (ang. Domain Name Reply) 39 - SKIP Algorithm Discovery Protocol 40 - Photuris, Security Failures
- W zależności od wartości występującej w polu Typ, wartość pola Kod może zawierać różne liczby. Najczęściej spotykane wartości par Typ, Komunikat zostaną przedstawione na następnych slajdach.
- Następujące wartości pola Typ są zarezerwowane : 1,2,7,19 (zarezerwowane dla bezpieczeństwa), 20-29, 41-255.



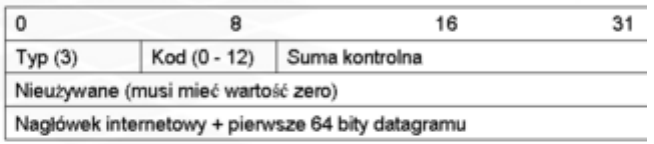
Nagłówek ICMP

Echo request i echo response

- W przypadku komunikatu ICMP typu żądanie echa (ang. echo request) i odpowiedzi z echem (ang. echo reply) wartości pola typ wynoszą odpowiednio 8 albo 0. Wartość pola Kod w obu przypadkach wynosi 0.
- Tego typu komunikaty ICMP są wykorzystywane przez podstawowe programy testujące, takie jak ping czy traceroute.



- Przy próbach wysyłania pakietów do miejsca przeznaczenia może wystąpić szereg błędów związanych z np. z uszkodzeniem łącza, błędnym adresem docelowym, nieznaną lokalizacją, itd. W takich przypadkach router, który wykryje problem wysyła komunikat o niedostępnym adresacie (ang. destination unreachable) w postaci przedstawionej na rysunku.
- W zależności od przyczyny błędu w polu „Kod” pojawiają się wartości liczbowe powiązane z następującymi usterkami:
  - 0 - sieć niedostępna
  - 1 - host niedostępny
  - 2 - protokół niedostępny
  - 3 - port niedostępny
  - 4 - niezbędna fragmentacja, ustawiona wartość DF
  - 5 - nie powiodło się określenie trasy przez nadawcę (ang. source route)
  - 6 - nieznana sieć docelowa
  - 7 - nieznany host docelowy
  - 8 - host źródłowy odizolowany
  - 9 - komunikacja z siecią docelową zablokowana przez administratora
  - 10 - komunikacja z hostem docelowym zablokowana przez administratora
  - 11 - sieć niedostępna dla tego typu usługi
  - 12 - host niedostępny dla tego typu usługi
- Komunikat o niedostępnym adresie wysyłany jest również w przypadku, gdy przesyłany pakiet musi zostać podzielony na mniejsze datagramy, np. przy przesyłaniu z sieci typu Token Ring do sieci Ethernet, a znacznik w nagłówku pakietu nie pozwala na taką fragmentację. Wysyłany jest wtedy kod błędu o wartości 4.



0	8	16	31
Typ (3)	Kod (0 - 12)	Suma kontrolna	
Nieużywane (musi mieć wartość zero)			
Nagłówek internetowy + pierwsze 64 bity datagramu			

Inne typy i kody komunikatów ICMP

- Typ 12 Błąd ten oznacza, że jest problem związany z parametrem (ang. parameter problem).
  - Jeśli pole „Kod” ma wartość 0, to wartość w polu „Wskaźnik” wskazuje numer oktetu nagłówka datagramu, w którym występuje błędna wartość parametru.
- Typ 5 – zmiana trasowania / przekierowanie
  - Kod 0 dla sieci
  - Kod 1 dla hosta
  - Kod 2 dla typu usługi i sieci
  - Kod 3 dla typu usługi hosta

Inne typy i kody komunikatów ICMP

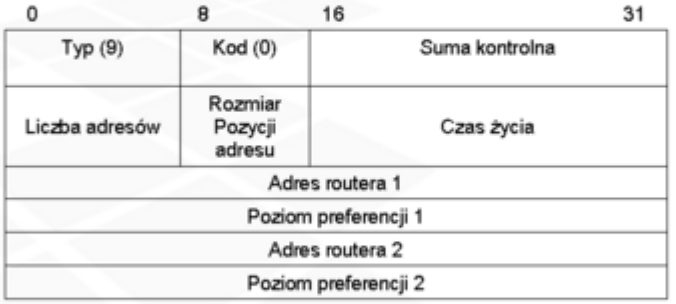
- Typ 13 i 14 ICMP żądanie / prośba wysłania znacznika czasowego (ang. timestamp request) o wartości pola Typ równej 13. W odpowiedzi na taką prośbę wysyłany jest komunikat odpowiedzi o wartości pola Typ równej 14. Pola kodu w przypadku obu typów komunikatów są równe 0
- Komunikaty **żądanie / prośba o przesłanie informacji** (ang. information request) oraz odpowiedź na żądanie przesłania informacji (ang. information reply) zostały zaprojektowane z myślą o przesyłaniu numerów IP. W zależności od tego czy jest to prośba o informację, czy też odpowiedź na tę prośbę pole **Typ ma wartości: 15 lub 16**. W przypadku obu typów komunikatów wartości pola „**Kod" wynoszą 0**.W praktyce obecnie nie są wykorzystywane, gdyż informacje takie są przesyłane w sposób bardziej dogodny przez protokoły takie jak BOOTP, RARP czy też DHCP. Protokoły służące uzyskiwaniu adresów zostaną omówione w kolejnym module poświęconym automatycznemu uzyskiwaniu adresów IP.

Inne typy i kody komunikatów ICMP

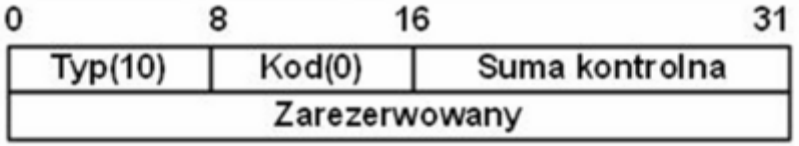
- Komunikat ICMP typu **żądanie maski adresowej** oraz **odpowiedź** na żądanie maski adresowej mają odpowiednio wartości pól **Typ** wypełnione liczbami **17 i 18**. Komunikaty te służą określeniu przez hosta jego maski adresowej.

IRDP: Komunikaty ICMP umożliwiające wykrywanie routera

- ICMP Router Discovery Messages (RFC 1256):
  - Rozgłaszanie routera (ang. router advertisement)



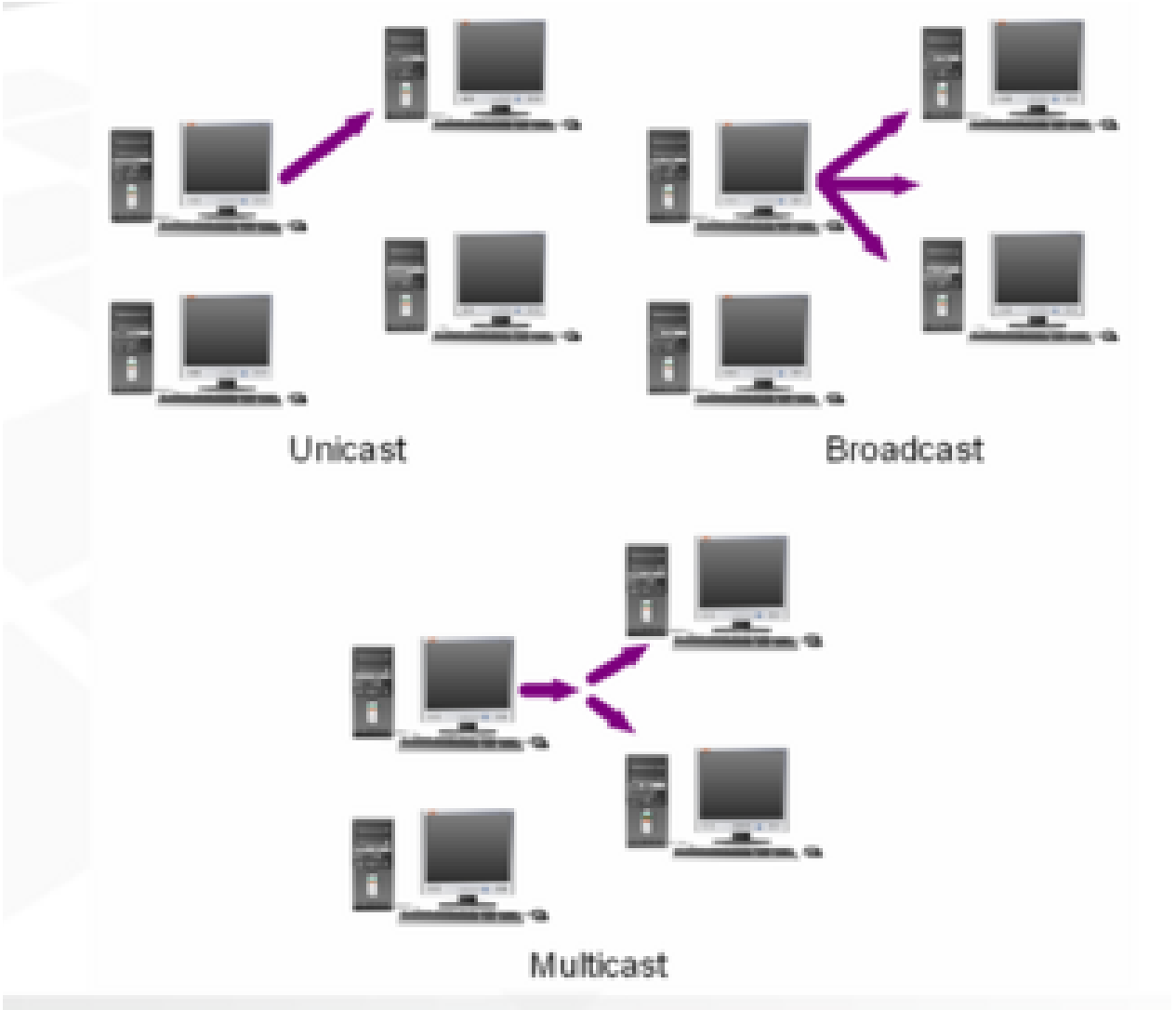
  - Wywołanie routera (ang. router solicitation)



Protokół IGMP

- Protokół zarządzania grupami internetowymi IGMP (ang. Internet Group Menagement Protocol) został opracowany z myślą o dogodnej komunikacji urządzeń sieciowych przy pomocy transmisji grupowych. Standard tego protokołu został opublikowany w dokumencie RFC 1112 pod koniec lat 90-tych XXw.
- Działanie takie jest możliwe, dzięki transmisjom grupowym (ang. multicasting). W tym typie transmisji pakiety wysyłane są na adres grupowy IP. Routery wiedzą, które komputery znajdują się w grupie obsługiwanej przez daną aplikację. Pozwala to na jednokrotne wysłanie określonych danych do wszystkich hostów z danej grupy. Jest to działanie bardziej efektywne niż transmisje kierowane (ang. unicasting), czy też wysyłanie poprzez adres rozgłoszeniowy (ang. broadcasting).

Typy transmisji danych



IGMP

- Hosty, które chcą się przyłączyć do danej grupy wysyłają komunikat IGMP Host Membership Report. Przyłączenie się klienta do danej grupy składa się z dwóch procesów:
  - host powiadamia router o tym, że chce się przyłączyć do danej grupy
  - host wiąże w sposób dynamiczny IP z adresem grupowym, który jest zarezerwowany dla danej aplikacji oraz z zarezerwowanym adresem Ethernetowym
- Opuszczenie danej grupy odbywa się poprzez wysłanie komunikatu IGMP Explicit Leave. Host powinien powiadomić lokalne routery o zamiarze opuszczenia grupy poprzez wysłanie właśnie takiego komunikatu.

- Routery okresowo sprawdzają czy w dalszym ciągu istnieje potrzeba przesyłania pakietów na adres grupowy. Kontrola taka odbywa się poprzez wysłanie zapytania przy użyciu adresu grupowego przeznaczonego dla wszystkich hostów (224.0.0.1). Pakiety które są wysyłane pod ten zarezerwowany numer IP mają ustawione pole TTL na wartość jeden, dzięki temu nie są rozsyłane dalej przez inne routery. W odpowiedzi hosty powinny przesłać pakiet raportu z adresem takim jaki jest zarezerwowany dla tej grupy. Po sprawdzeniu, które z grup jeszcze istnieją routery będą przesyła tylko pakiety dla funkcjonujących grup, natomiast pakiety z adresem grupowym będą odrzucane przez router.

IGMP: struktura pakietu

W nagłówku pakietu IGMP przesyłane są następujące pola:

Wersja - 4b - wersja pakietu IGMP Typ - 4b - typ komunikatu. Wartości tam zapisane oznaczają odpowiednio;

```
1 - zapytanie o przynależność hosta
2 - raport o przynależności hosta
Nie używane - 8b - pole nie wykorzystywane
Suma kontrolna - 16b - pole wykorzystywane do przesyłania liczby umożliwiającej sprawdzenie
integralności pakietu
Adres grupy - 32b - gdy pakiet jest przesyłany w celu zapytania o przynależność hosta, to
pole to jest puste. Gdy host odpowiada raportem o przynależność do grupy, to w polu tym
przesyłany jest adres rozsyłania grupowego konkretnej grupy.
```

Konieczność adresacji

- W przypadku sieci komputerowych, podobnie jak w przypadku tradycyjnych sposobów komunikacji, istnieje potrzeba określenia miejsca przeznaczenia, do którego powinna zostać wysłana porcja danych. Można to przyrównać do wysyłania listu do znanej nam (lub nieznanej) osoby. W obu przypadkach należy określić adres miejsca przeznaczenia. W przypadku tradycyjnego systemu pocztowego na kopercie wpisywane są dane adresata. Zwykle też podawane są dane nadawcy, w celu komunikacji zwrotnej. Oba adresy powinny być unikalne w innym przypadku korespondencja mogłaby nie trafiać do adresatów.
- Również analogicznie jak w tradycyjnej poczcie pakiety transportowane są do określonej sieci, w której router jest odpowiednikiem urzędu pocztowego. Router decyduje również do którego hosta adresuje ramkę z danym pakietem, podobnie jak listonosz, który przynosi przesyłki do konkretnego adresata.

Adresacja w sieciach

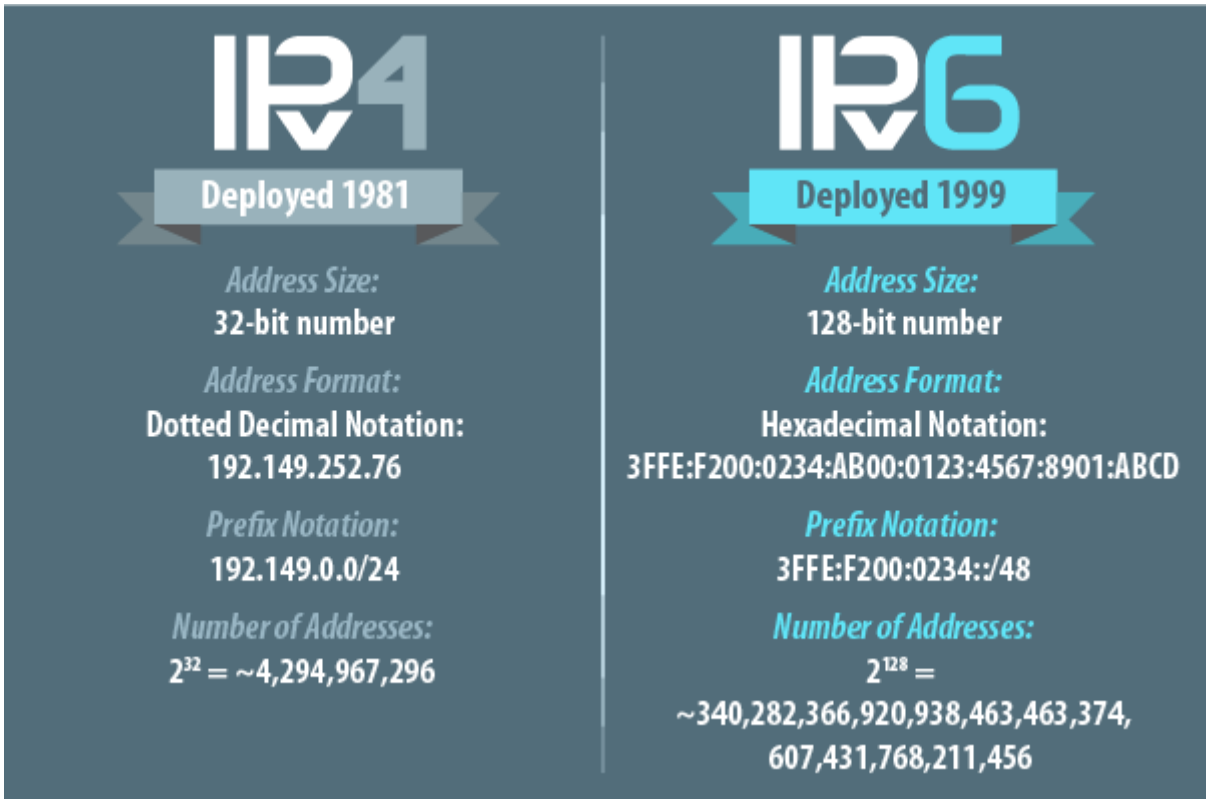
- Analogicznie w sieciach komputerowych stosuje się adresację wymaganą przez stosowane protokoły. W zależności od rozpatrywanych warstw modelu ISO/OSI można wyróżnić adresację na poziomie warstwy łącza danych (L2) oraz adresację na poziomie warstwy sieci (L3). Pierwsza z nich dotyczy adresacji fizycznej interfejsu sieciowego, tzw. **adres MAC** (Media Access Control). Druga z nich odnosi się do adresacji logicznej **adres IP**.

Przydzielanie adresów

- Podobnie jak w przypadku rzeczywistych adresów tak samo w przypadku adresów IP musi być zapewniona ich unikalność.
- Przydzielaniem adresów zajmują się powołane do tego celu organizacje:
  - Pierwotnie zajmował się tym Internet Network Information Center (InterNIC). Organizacja ta obecnie nie istnieje.
  - Internet Assigned Numbers Authority (IANA).

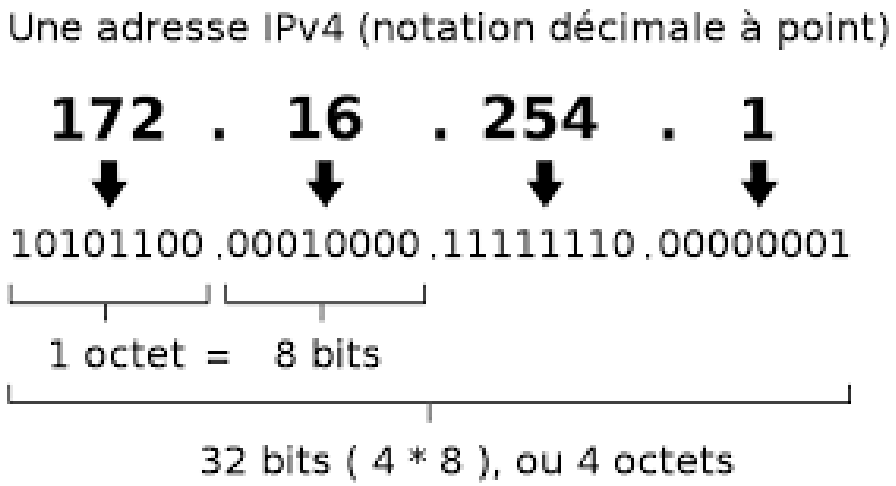
Wersje adresacji

- IPv4 – 32 bity adresu – dostępnych adresów 2^{32}
- IPv4 – 128 bitów adresu – dostępnych adresów 2^{128}



Struktura adresacji IPv4

- W przypadku adresacji IP adres składa się z części bitów przeznaczonych
  - na identyfikację sieci, do której został przypisany dany interfejs hosta
  - pozostałej liczby bitów przeznaczonych na adresację hosta w danej sieci.



Maska

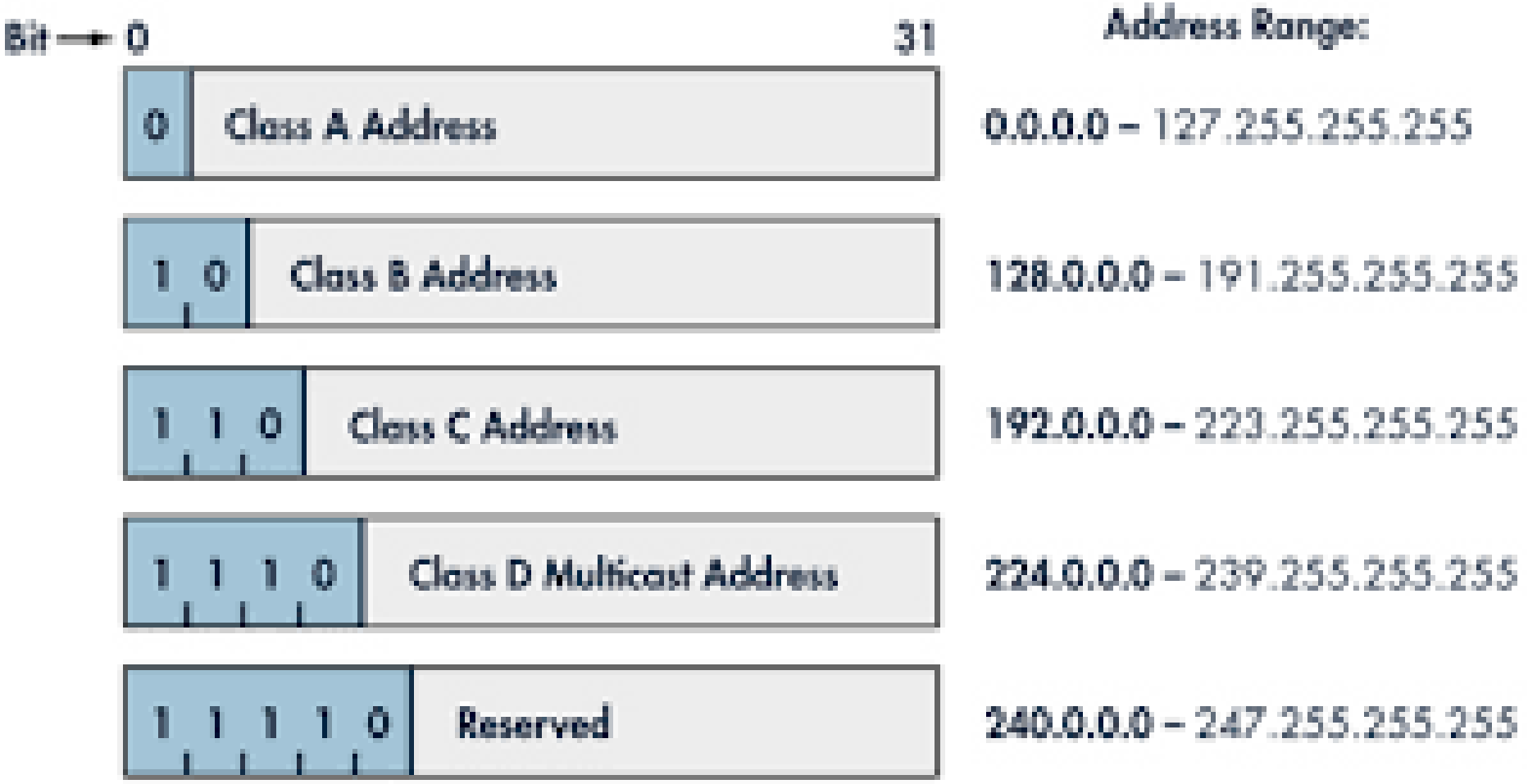
- W przypadku IPv4 część adresu przeznaczona na identyfikator sieci jest zależna od długości maski sieciowej.
- Maska ta służy do wyznaczania adresu sieciowego, który jest (musi być) taki sam dla wszystkich interfejsów znajdujących się w tej samej podsieci.
- Netmaska podobnie jak adres IPv4 składa się z 32 bitów.

CIDR	Maska	Liczba dostępnych adresów hostów
/1	128.0.0.0	2147483646
/2	192.0.0.0	1073741822
/3	224.0.0.0	536870910
/4	240.0.0.0	268435454
/5	248.0.0.0	134217726
/6	252.0.0.0	67108862
/7	254.0.0.0	33554430
/8	255.0.0.0	16777214
/9	255.128.0.0	8388606
/10	255.192.0.0	4194302
/11	255.224.0.0	2097150
/12	255.240.0.0	1048574
/13	255.248.0.0	524286
/14	255.252.0.0	262142
/15	255.254.0.0	131070
/16	255.255.0.0	65534
/17	255.255.128.0	32766
/18	255.255.192.0	16382
/19	255.255.224.0	8190
/20	255.255.240.0	4094
/21	255.255.248.0	2046
/22	255.255.252.0	1022
/23	255.255.254.0	510
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/29	255.255.255.248	6

Formy adresacji IP

- Adresacja klasowa
- Adresacja bezklasowa
-
-
- Podział na notację klasową i bezklasową wynika ze stosowania numerów IPv4 i odpowiadających im netmasek. W przypadku notacji klasowej numery IP jak i maski mają ściśle określone zakresy. W przypadku adresacji bezklasowej dozwolonym numerom IPv4 mogą być przypisane dowolne (dozwolone) netmaski.

Podział adresów IPv4 na klasy

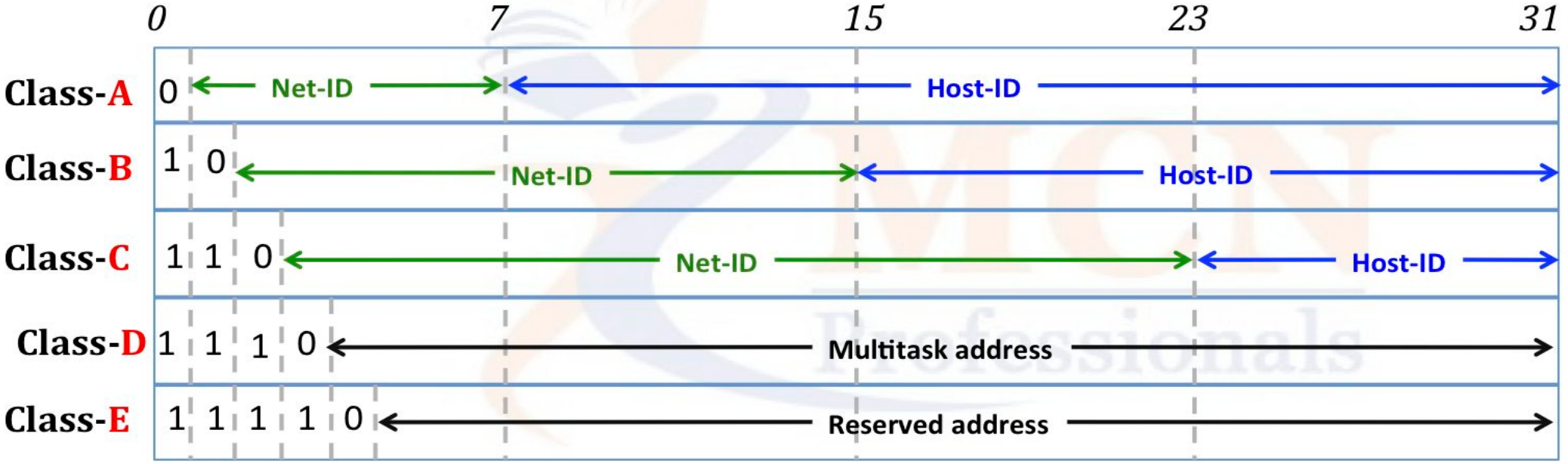


Klasa IPv4

- Klasa A została przeznaczona dla dużych organizacji z bardzo dużą liczbą hostów. Pula adresowa sieci zawiera się w przedziale 1-126 i stanowi połowę wszystkich dostępnych adresów.
- Klasa B została przeznaczona dla dużej liczby organizacji z dużą liczbą hostów. Numery sieci w tej klasie zawierają adresy od 128 do 191, stąd dostępna liczba adresów stanowi 25 procent całej puli adresowej.
- Klasa C była zaplanowana przede wszystkim dla małych organizacji z liczbą hostów nie przekraczającą kilkuset sztuk.
- Klasa D służy do rozsyłania grupowego pakietów przy pomocy adresów IPv4. Klasa E została zarezerwowana przez IETF dla celów badawczych.
- Jak się później okazało podział ten nie pozwalał na efektywne zarządzanie pulą adresów.

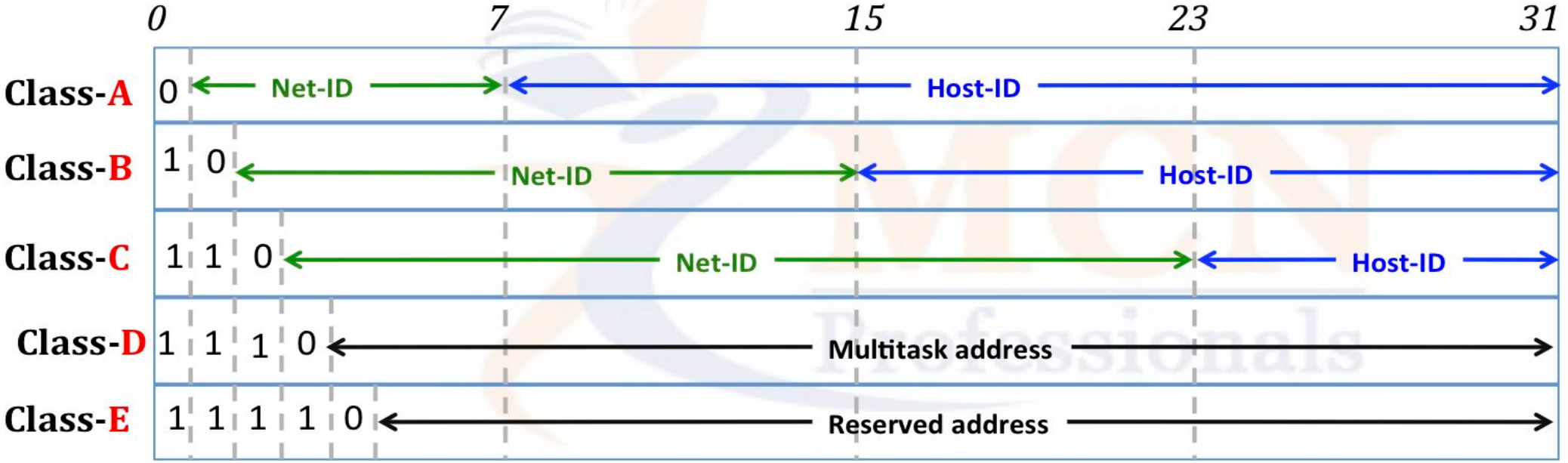
KLASA A

- W klasie A tylko 8 bitów zostało przeznaczone na adresację sieci.
- Pierwszy najbardziej znaczący bit ma zawsze wartość 0, zatem do dyspozycji na numerację sieci klasy A pozostaje 2^7 adresów.
- Dzięki temu zakres adresów pierwszego oktetu zawiera się w przedziale od 0 do 126.
- Adres zaczynający się od 127 został zarezerwowany na adres pętli zwrotnej



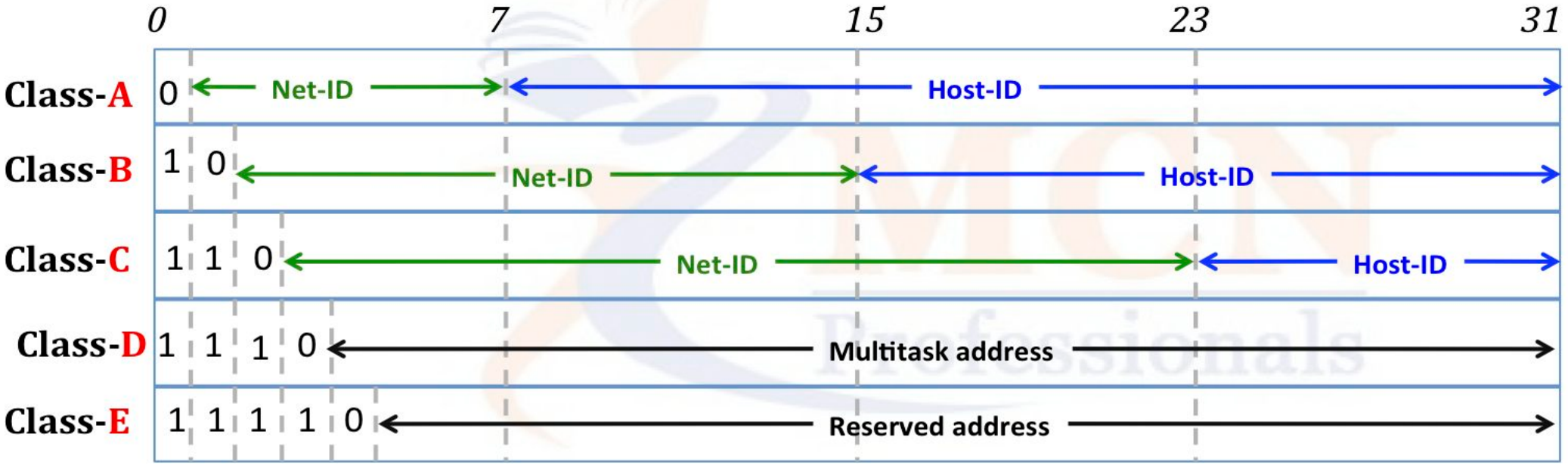
KLASA A

- W sieci tej klasy pozostałe 24 bity są przeznaczone na część identyfikującą hosty.
- Daje to przestrzeń adresową ponad 16 milionową (16.777.216)
- Standardowa (naturalna) maska dla sieci tej klasy to 255.0.0.0



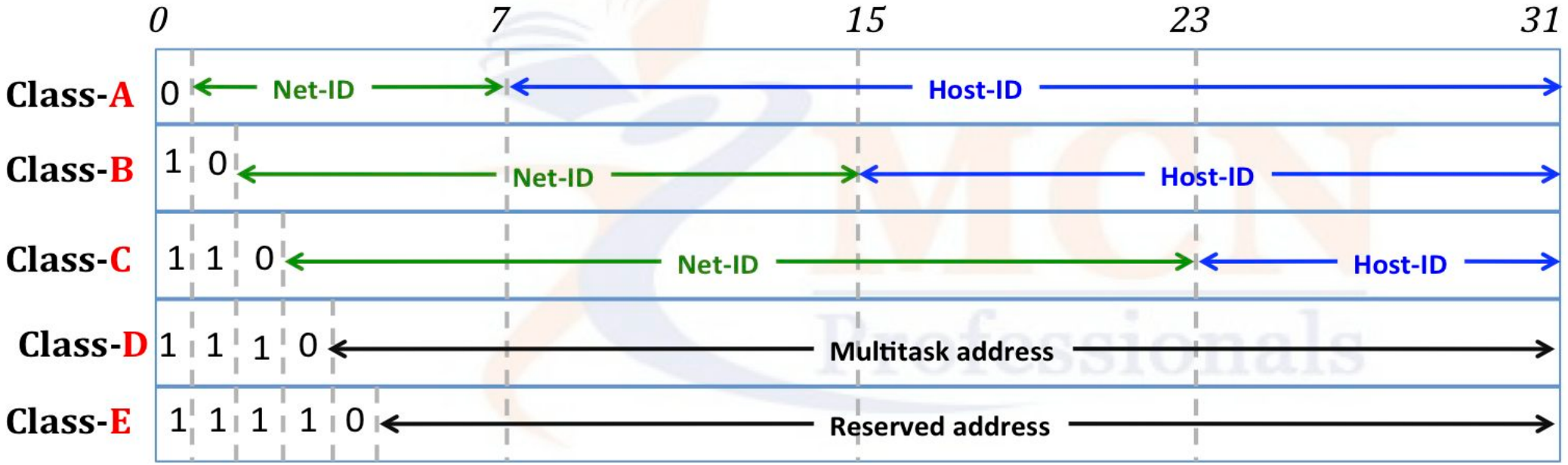
KLASA B

- W klasie B 16 bitów zostało przeznaczone na adresację sieci.
- Pierwsze dwa najbardziej znaczące bity mają wartość 10. Dzięki temu zakres adresów pierwszego oktetu zawiera się w przedziale od 128 do 191.
- Zatem na zaadresowanie sieci pozostaje 14 bitów, co daje 16384 (2^{14}) adresów
- W sieci tej klasy pozostałe 16 bitów przeznaczone są na część identyfikującą hosty.
- Daje to przestrzeń adresową umożliwiającą wykorzystanie ponad 65 tysięcy adresów sieciowych (65536).
- Standardowa (naturalna) maska sieciowa dla tej klasy wynosi: 255.255.0.0



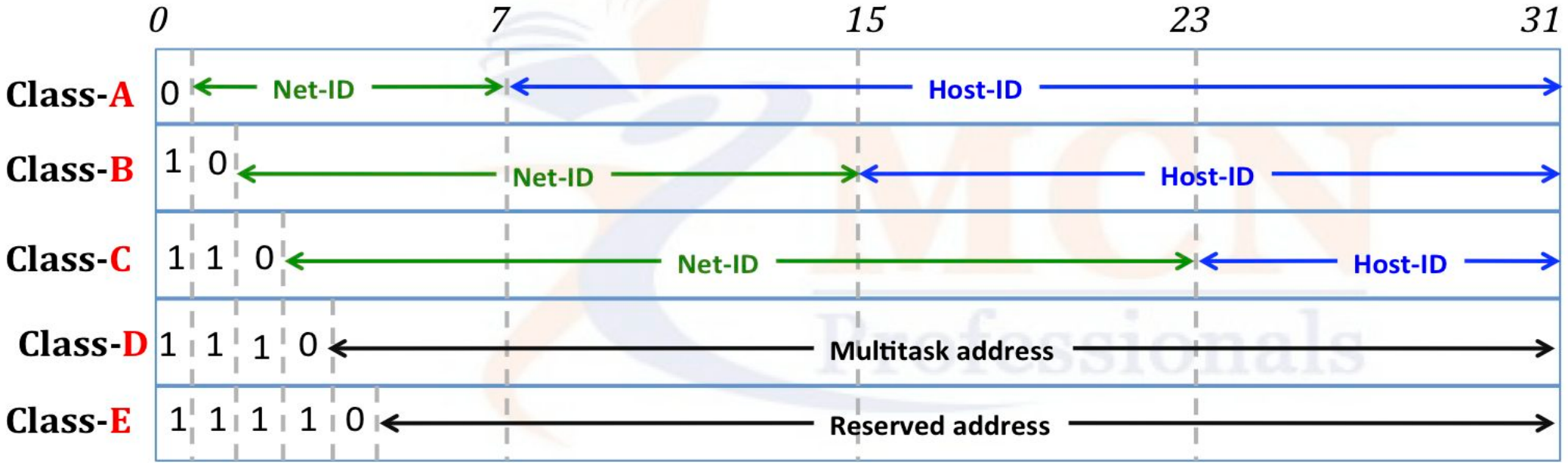
KLASA C

- W klasie C 24 najbardziej znaczące bity zostały przeznaczone na adresację sieci.
- Pierwsze trzy najbardziej znaczące bity mają wartość 110.
- Dzięki temu zakres adresów pierwszego oktetu zawiera się w przedziale od 192 do 223.
- Daje to razem 2097152 (2^21) adresów przeznaczonych na identyfikację sieci.
- W sieci tej klasy pozostałe 8 bitów przeznaczone są na część identyfikującą hosty.
- Daje to przestrzeń adresową umożliwiającą zaadresowanie małych sieci składających z się z nie więcej niż 256 adresów.
- Standardowa (naturalna) maska sieciowa dla tej klasy wynosi: 255.255.255.0



KLASA D

- Klasa adresów D została zarezerwowana na potrzeby rozsyłania grupowego.
- Jest to bardziej efektywny sposób przesyłania danych do hostów niż rozgłaszanie poprzez adres 255.255.255.255.
  - Ten ostatni sposób wymaga przetwarzania pakietów przez wszystkie hosty w domenie rozgłoszeniowej. Związane jest to z niepotrzebnym nakładem obliczeń. Zamiast tego można wykorzystywać adresację grupową, gdzie tylko określone hosty będą otrzymywały pakiety, które muszą przetworzyć.
- Przykładem takich pakietów są pakiety wysyłane przez protokoły rotingu:
  - RIPv2 wysyła uaktualnienia na adres 224.0.0.9
  - OSPF - wysyła pakiety „Hello" na adres 224.0.0.5



Zasady adresowania IPv4

- Z puli dostępnych wartości adresów część wartości jest wyłączona z adresów, które mogą być nadawane hostom.
- Jednym z takich ograniczeń jest adres postaci 127.x.x.x. Został on zarezerwowany na potrzeby pętli zwrotnej.
- Kolejnym ograniczeniem jest adres, w którym identyfikator hosta składa się z liczb 255. Wynika, to z założenia, że ten rodzaj adresu przeznaczony jest do rozsyłania komunikatów typu broadcast.
- Identyfikator hosta nie może składać się z samych zer, gdyż jest to adres sieci, w której znajduje się host.
- Aby spełniony był warunek unikalności całych adresów IP, identyfikator hosta nie może powtórzyć się w sieci.

Użyteczna liczba hostow

- 2^n-2
- Pierwszy adres hosta – zarezerwowany na identyfikator sieci
- Ostatni adres hosta – zarezerwowany na adres rozgłoszeniowy - broadcastowy

Ograniczenia klasowego IPv4

- Protokół IPv4 został zaprojektowany na początku lat 80-tych XX w.
- W tamtym czasie spełniał on w wystarczającym stopniu wymagania co do liczby adresów niezbędnych do obsłużenia połączonych w sieci urządzeń.
- **Jednak wraz z rozwojem sieci komputerowych wzrasta zapotrzebowanie na adresy IP.**
- Potrzeba co raz większej liczby adresów wymusiła potrzebę zarządzania dostępną pulą adresów.
- **Problem ten szczególnie dotyczył adresów klasy C**, która zakładała przydzielanie całej puli składającej się z **255 adresów**. W przypadku, gdy sieć ta posiadała zaledwie kilkanaście hostów pozostałe ponad dwieście było niewykorzystanych.
- „rozrzutność” dotyczyła sieci klasy A, czy też B. Sytuacja odwrotna występowała w przypadku organizacji z dużą liczbą hostów. W tym przypadku istniała potrzeba używania większej puli adresów. W obu przypadkach wiązało się to z nieefektywnym wykorzystaniem przydzielonych adresów.
- Dodatkowym problemem były duże tablice routingu i związane z tym długie czasy przesyłania pakietów w sieciach.

Rozwiązanie problemu niedobory adresów IPv4

- Ze względu na zmniejszającą się pulę dostępnych adresów podejmowane były różne kroki w celu rozwiązania tego problemu.
- Tworzenie podsieci (1985)
- Tworzenie podsieci o zróżnicowanej długości adresów (1987)
- Bezklasowy routing między-domenowy – CIDR (1993)
- Wydzielenie prywatnych adresów sieciowych
- Translacja adresów sieciowych
- Automatyczne przydzielanie adresów.

•Tworzenie podsieci (1985)

- Jednym ze sposobów, zaproponowanym w 1985 roku, było tworzenie podsieci.
- Zakres adresów hostów w danej sieci był dzielony na mniejsze podsieci z mniejszą liczbą hostów, w każdej z nowo utworzonych.
- Metoda ta wymagała „pożyczenia” bitów z części adresu przeznaczonej dla identyfikacji hosta dla zaadresowania podsieci.

•Tworzenie podsieci o zróżnicowanej długości adresów (1987)

- Innym sposobem rozwiązania problemu brakujących adresów było, zaproponowanie w dokumencie RFC 1009 (w 1987 roku), tworzenie podsieci o zróżnicowanej długości masek adresów (ang. Variable Length Subnet Masks (VLSM).
- Przydzielona danej organizacji pula adresów jest następnie dzielona wewnątrz niej na mniejsze porcje.
- Podział ten jest następnie niewidoczny z zewnątrz sieci danej organizacji.

•Bezklasowy routing między-domenowy – CIDR (1993)

- Jeszcze inne rozwiązanie polegało na wprowadzeniu bezklasowego routingu międzydomenowego - CIDR (ang. Classless Inter-Domain Routing).
- Metoda CIDR podobnie jak metoda VLSM pozwala na podział puli adresów na mniejsze porcje. Przy czym w odróżnieniu do metody VLSM, metoda CIDR polega na podziale puli dostępnych adresów przez Internet Registry dla dostawcy Internetu (ISP) najwyższego poziomu, poprzez poziom pośredni niski, aż do odbiorcy usług Internetowych.
- W metodzie CIDR informacje na temat masek sieci są przekazywane przez poszczególne routery w trakcie aktualizacji tablic routingu.

•Wydzielenie prywatnych adresów sieciowych

- Kolejnym sposobem, który może być stosowany w sieciach lokalnych jest mechanizm adresów prywatnych.
- Nie wymaga on praktycznie żadnych nakładów poza wyborem numeracji.
- Pakiety pochodzące z takich adresów będą odfiltrowywane przez routery.
- **Dokument RFC 1918 podaje trzy pule adresów prywatnych, po jednej dla poszczególnych klas A,B,C**. Pakiety z adresami prywatnymi nie są przepuszczane przez routery sieciowe.
  - W klasie A są to adresy z zakresu 10.0.0.0 - 10.255.255.255
  - W klasie B do dyspozycji jest pula adresów 172.16.0.0 - 172.31.255.255
  - W klasie C są to adresy 192.168.0.0 192.168.255.255

- Dodatkowo stosując netmaski i zmiennej długości (VLSM) można te pule zmniejszać lub też zwiększać w zależności od potrzeb.

•Translacja adresów sieciowych - NAT

- W przypadku adresów prywatnych, aby była możliwa komunikacja w Internecie, wprowadzono mechanizm tłumaczenia adresów prywatnych na publiczne, tzw. NAT (ang. Network Address Translation).
- Dzięki temu organizacjom wystarczy pojedynczy publiczny adres IP, w przypadku braku serwerów WWW, pocztowych i innych.

Adresacja IPv6

- Protokół IPv4 jest w dalszym ciągu powszechnie wykorzystywany pomimo niedoskonałości tego rozwiązania.
- Prace nad nowszą wersją protokołu IPv6 trwają od kilku lat.
- Jednym z ważniejszych argumentów przemawiających za potrzebą migracji do nowszej wersji protokołu jest zapotrzebowanie na dużą liczbę adresów Internetowych.
- Innym powiązanym z poprzednim, wymaganiem jest potrzeba zapewnienia ustalonych parametrów transmisji dla ruchu multimedialnego. Technologie wprowadzane coraz powszechniej: telefonia IP, telewizja cyfrowa, wideo na życzenie itp. wymagają stałych parametrów przesyłania.
- Innym, równie istotnym, wymogiem jest kwestia autoryzacji nadawcy, która nie była możliwa w IPv4.
- Te oraz inne niewymienione czynniki bardzo istotnie przemawiają za szybką migracją do IPv6, który również bywa nazywany protokołem następnej generacji IPNG (IP Next Genaration).

- Warto podkreślić fakt, że zmiana protokołu warstwy sieciowej modelu ISO (protokołu warstwy Internetowej stosu protokołów TCP/IP) nie powoduje potrzeby dostosowywania protokołów pozostałych. Część z dostawców Internetu (ISP) oferuje już dostęp do IPv6. Ze względu na fakt, że w dalszym ciągu powszechnie używany jest IPv4, to ruch IPv6 jest tunelowany w starszej wersji protokołu (IPv6-in-IPv4). Protokół IPv6 opisują dokumenty RFC 1883 oraz RFC 1884.
- Jedną z podstawowych zalet, chociaż nie najważniejszą, jest liczba dostępnych adresów w nowej wersji protokołu.
- Ze względu na to, że do zapisania adresu w IPv6 użytych jest 128 bitów, to dostępna pula wynosi ok. $3,4x10^{38}$ adresów.
- W przeliczeniu na powierzchnię Ziemi daje to ok. $6,7x10^{17}$/mm^2. W ten sposób zapotrzebowanie na pulę adresów dla nowych rozwiązań sieciowych powinno zostać spełnione.

Budowa datagramu IPv6

Bity	0-3	4-7	8-11	12-15	16-19	20-23	24-27	28-31
0	Wersja	Priorytet		Etykieta przepływu				
32	Długość danych				Następny nagłówek		Limit przeskoków	
64	Adres źródłowy (128 bitów)							
96								
128								
160								
192	Adres docelowy (128 bitów)							
224								
256								
288								

IPv6 – nagłówki rozszerzające

- Ważną cechą, która umożliwia szybsze przesyłanie pakietów przez routery jest możliwość dołączania nagłówków rozszerzających.
- Jest to możliwe, dzięki polu „Następny nagłówek” (ang. Next header). Nagłówek ten jest umieszczany w pakiecie za nagłówkiem podstawowym, a przed nagłówkiem warstwy transportowej. Nagłówki te powinny występować w określonej kolejności natomiast nie ma ograniczenia co do ich liczby. Nagłówki te zastępują pola opcjonalne w IPv4. Dzięki zastosowaniu tego mechanizmu możliwe jest, m.in. uwierzytelnianie pakietów.
- Wśród zdefiniowanych nagłówków dodatkowych można wymienić: Hop-by-hop options header Destinations options header-1 Source routing header Fragmentation header Authentication header IPv6 encryption header Destination option header-2

Adresy IPv6

- Jedną z najważniejszych i bardzo istotną zmianą w stosunku do IPv4 jest przeznaczenie większej liczby bitów na określenie adresu.
- Rozwój metod komunikacji (GPRS, EDGE, UMTS) oraz wprowadzanie na rynek nowych urządzeń z funkcją komunikacji sieciowej wymusza zastosowanie efektywniejszych metod przesyłania datagramów. Jednym z bardziej istotnych elementów jest możliwość nieograniczonego przydzielania adresów IP.
- Zwiększenie przestrzeni adresowej z 2^32 (IPv4) do 2^**128** (IPv6) oznacza przyrost możliwych do przypisania adresów z ok. 4,3x10^9 do ok. 3,4x10^38.
- Adres IPv6 zapisywany jest postaci **heksadecymalnej**.
- Preferowany jest zapis, w którym co 16 bitów (4 cyfry heksadecymalne) wstawiany jest separator w postaci dwukropka. 0432:5678:abcd:00ef:0000:0000:1234:4321.
- Notacja pozwala opuszczać wiodące zera, zatem adres ten można zapisać również jako: 432:5678:abcd:ef:::1234:4321
- Specyfikacja pozwala również w przypadku występowania mieszanej infrastruktury (IPv6 z Ipv4) na podkreślenie tego faktu poprzez zapis ostatnich 32 bitów podobnie jak to było zapisywane w wersji IPv4, np.: 0:0:0:0:0:0:13.1.68.3 0:0:0:0:0:FFFF:129.144.52.38 lub wersji skróconej: 13.1.68.3 FFFF:129.144.52.38
- Ze względu na fakt, że spora część ruchu odbywa się w dalszym ciągu w oparciu o IPv4 pakiety IPv6 są tunelowane wewnątrz IPv4.

IPv6 typy adresów

- Wartym podkreślenia jest fakt, że w IPv6 nie ma adresów rozgłoszeniowych (ang. broadcastowych). Ich funkcje w pełni zastąpiły adresy rozsyłania grupowego.
- W specyfikacji RFC 1884 wymienione są 3 typy adresów:
  - kierowanego (ang. Unicast) - identyfikator pojedynczego interfesju. Pakiety wysyłane na ten adres trafiają do określonego w nim hosta
  - uniwersalnego (ang. Anycast) - identyfikator zbioru interfejsów, które zwykle należą do różnych węzłów sieci. Pakiet wysłany na ten adres jest dostarczany tylko na jeden z interfejsów z tego zbioru. Zwykle jest to adres interfejsu najbliższego w rozumieniu metryki
  - grupowego (ang. Multicast) - podobnie jak w przypadku poprzednim: identyfikator jest przypisany do zbioru interfejsów. Pakiet zawierający ten adres jest dostarczany na każdy z interfejsów należących do zbioru.

IPv6 specjalne pule adresów

- Wśród adresów IPv6 są pewne specjalne pule adresów. Część z nich zostanie wymieniona poniżej
- ::/128 – adres zerowy, wykorzystywany tylko w oprogramowaniu.
- ::1/128 – adres pętli zwrotnej, zapisany inaczej: 0:0:0:0:0:0:0:1 (odpowiednik 127.0.0.1 z IPv4).
- ::/96 – adresy kompatybilne z adresem IPv4 hosta korzystającego z IPv6 i IPv4.
- ::ffff:0:0/96 – adresy kompatybilne z adresem IPv4 hosta korzystającego wyłącznie z IPv4, część adresu (32 najmniej znaczące bity) jest taka sama jak w IPv4
- fe80::/10 – adresy typu "link-local" wykorzystywane wewnątrz sieci lokalnych, w procesie autokonfiguracji.
- ff00::/8 – adresy multicast