

Тема № 2: IP АДРЕСАЦИЯ

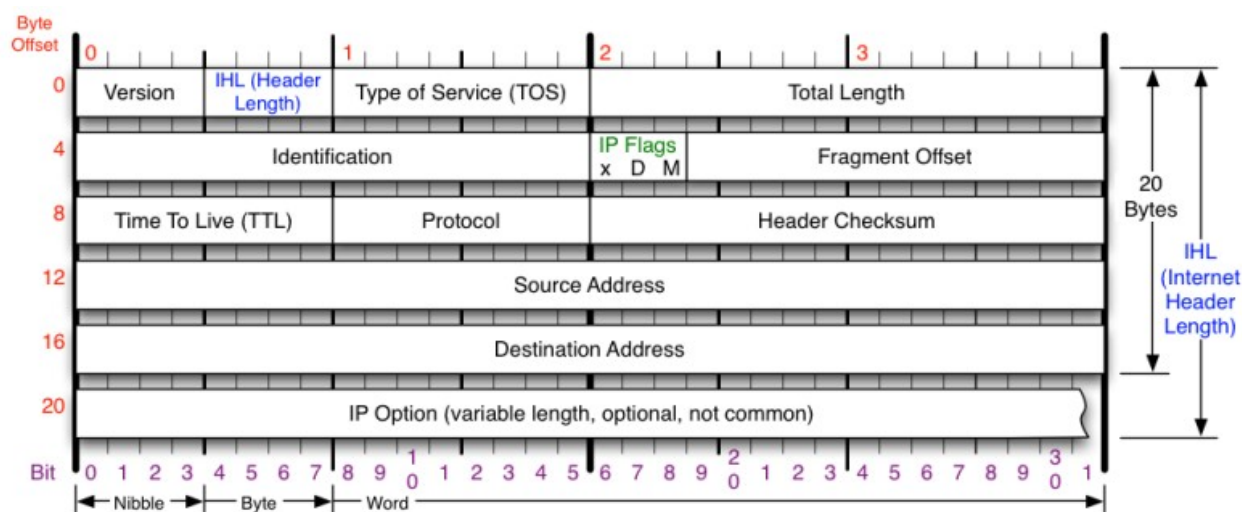
IP адресът представлява логически адрес на конкретен възел от мрежата. За да се осъществи връзка между две крайни устройства, те трябва да имат уникални адреси (в мрежата).

IP адресът се присвоява на мрежовия интерфейс на крайното устройство. Много често в сървърите се монтират повече от една мрежова карта (NIC), като всяка карта има собствен, уникален IP адрес.

NIC притежават:

- работни станции;
- сървъри;
- мрежови принтери;
- IP телефони.

Във всеки изпратен по мрежата пакет има записани в неговата заглавна част (IP header) IP адресът на изпращача и IP адресът на получателя на пакета.



Version Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.	Protocol IP Protocol ID. Including (but not limited to): 1 ICMP 17 UDP 57 SKIP 2 IGMP 47 GRE 88 EIGRP 6 TCP 50 ESP 89 OSPF 9 IGRP 51 AH 115 L2TP	Fragment Offset Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.	IP Flags x D M x 0x80 reserved (evil bit) D 0x40 Do Not Fragment M 0x20 More Fragments follow
Header Length Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.	Total Length Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.	Header Checksum Checksum of entire IP header	RFC 791 Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

СТРУКТУРА НА IP АДРЕСА

IP адресът представлява серия от 32 двоични бита (0 или 1), което го прави трудно разбираем даже и ако битовете се групират в групи (4 групи) по 8 бита, наречени октети. За улесняване на разбираемостта на IP адресите, всеки октет се записва с

неговото десетично представяне (точково-десетичен запис):

dec:	192	168	1	5
bin:	110000000	10101000	00000001	00000101

Структурата на 32 битовия IP адрес е описана в мрежовия протокол IPv4 – **RFC 791**; IPv6 – **RFC 2460**; **RFC 6144 – Framework for IPv4/IPv6 Translation**. Все още 32 битовият протокол IPv4 е най-разпространеният протокол за адресация в Internet.

Всеки октет на мрежовия адрес се състои от 8 бита, като всеки бит има своята стойност. И 4-те групи от октети имат един и същ набор от стойности. Значението на най-десният бит в октета е 1, а значението на останалите битове, отляво надясно е 2, 4, 8, 16, 32, 64 и 128.

128	64	32	16	8	4	2	1
-----	----	----	----	---	---	---	---

За да определим стойността на октета, трябва да съберем стойностите на позициите, в които има двоична единица. При извършване на това събиране в сила са следните правила:

1. В събирането не участват позициите, в които има 0;
2. Ако всичките осем бита имат стойност 0 (00000000), тогава стойността на октета е 0;
3. Ако всичките осем бита имат стойност 1 (11111111), тогава стойността на октета е 255;
4. Ако стойностите на осемте бита са различни, например 00100101, тогава стойността на октета е 39 (32 + 4 + 2 + 1):

128	64	32	16	8	4	2	1
0	0	1	0	0	1	1	1
		32			4	2	1

Стойността на всеки октет се намира в диапазона от 0 до 255.

ФОРМАТ НА IP АДРЕС

Логическият IP адрес представлява йерархична система и се състои от две части – първата част от него идентифицира мрежата като цяло, а втората идентифицира конкретният възел в нея. Първата част се нарича мрежова част (net_ID), а втората – хост част (host_ID).

net_ID + host_ID = 32 bits

10000011	01101100	01111010	11001100
8 бита	8 бита	8 бита	8 бита

131	108	122	204
8 бита	8 бита	8 бита	8 бита

Пример на IP адрес от клас C: 192.168.18.57

Първите три октета образуват мрежовата част (192.168.18), а последният октет (.57) – идентифицира възела в нея.

Такава система се нарича **йерархична адресация**, защото мрежовата част от адреса идентифицира мрежата, в която се намират всички възли (хостове). На маршрутизаторите е нужно да знаят само пътя до мрежата, но не и разположението на отделните възли в нея.

Друг пример за йерархична мрежа е телефонната мрежа:

359-2-1234567

359 – код на държавата;

2 – код на града;

1234567 – телефонен номер.

359 и 2 идентифицират мрежата (на телефонния оператор), а 1234567 е локалният номер на телефона.

При IP адресацията, в една физическа мрежа може да съществуват няколко логически мрежи.

Възлите с еднаква мрежова част (например, 192.168.18) могат да обменят информация помежду си, но не могат да обменят с други възли (с друга мрежова част, например 192.168.5), без да използват маршрутизация.

КЛАСОВЕ IP МРЕЖИ И МРЕЖОВИ МАСКИ ПО ПОДРАЗБИРАНЕ

IP мрежите се разделят на следните класове:

- A – комерсиална мрежа;
- B – комерсиална мрежа;
- C – комерсиална мрежа;
- D – за multicast (многоадресно) (примерно мултимедия);
- E – за експериментални цели.

Мрежа клас A:

net_ID – само един октет;

host_ID – цели три октета.

Мрежи от клас A се дават само на големи организации. Броят на възлите в такава мрежа е 2^{24} . Мрежовата маска на мрежите от такъв клас е 255.0.0.0, а самата мрежова маска се състои от 24 бита.

Мрежа клас B:

net_ID – два октета;

host_ID – два октета.

Мрежовата маска по подразбиране се състои от 16 бита: 255.255.0.0. Броят на възлите в такива мрежи е $2^{16} = 65536$ възела. Мрежи от такъв клас обикновено се раздават на средноголеми организации.

Мрежа клас C:

net_ID – три октета (8 бита);

host_ID – един октет (24 бита).

В мрежи от такъв клас може да има $2^8 = 256$ адреса. Мрежовата маска по подразбиране е 255.255.255.0. Използват се за малки по размер мрежи.

Мрежа клас D:

1	1	1	0					2	3	4
net_ID				host_ID						

Мрежа клас E:

1	1	1	1					2	3	4
net_ID				host_ID						

Класът на мрежата може да се определи по значението на нейния първи октет.

Клас мрежа	Мрежи	Битове в първия октет
A	1-127	<u>0</u> 0000000 – <u>0</u> 1111111
B	128-191	<u>10</u> 000000 – <u>10</u> 111111
C	192-223	<u>110</u> 00000 – <u>110</u> 11111
D	224-239	<u>1110</u> 0000 – <u>1110</u> 1111
E	240-255	<u>1111</u> 0000 – <u>1111</u> 1111

Подчертаните битове от първия октет не се променят. Броят на мрежите от съответния клас се определя от броя на битовете, които могат да бъдат променяни в първия октет. За мрежите от клас A те са 7 бита, от което следва, че броят мрежи е $2^7 = 128$ (от 1 до 127). За клас B – $2^6 = 64$ (от 128 до 191), за клас C – $2^5 = 32$ (от 192 до 223), за клас D и E – $2^4 = 16$ (от 224 до 239 и от 240 до 255).

RFC 6890 (Special-Purpose IP Address Registries) прави "карта" на адресните сегменти (IPv4 и IPv6) за специално използване.

10.0.0.0/8; 172.16.0.0/12 и 192.168.0.0/16 са блокове от адреси, предназначени за употреба в частни мрежи и са документирани в [\[RFC1918\]](#). Както е описано в този документ (RFC 1918), адресите от тези блокове не може да бъдат използвани в публични мрежи. Тези адреси могат да бъдат използвани без да има нужда от съгласуване с IANA или някой Internet регистратор.

Класовата адресация не позволява рационалното използване на ограничени ресурс от уникални IP адреси, тъй като не позволява използването на различни мрежови маски на подмрежи. При нея се използва **фиксирана** мрежова маска, което позволява идентифицирането на класа мрежа по първия байт от адреса (но само при класовата адресация).

БЕЗКЛАСОВА IP АДРЕСАЦИЯ (CIDR – Classless Inter-Domain Routing)

При безкласовата IP адресация се използват мрежови маски с променлива дължина

(VLSM – Variable Length Subnet Mask), което позволява по-рационалното управление на адресното пространство на мрежата.

Общо адреси	Битове в host_id	префикс	клас	Десетична мрежова маска
1	0	/32		255.255.255.255
2	1	/31		255.255.255.254
4	2	/30		255.255.255.252
8	3	/29		255.255.255.248
16	4	/28		255.255.255.240
32	5	/27		255.255.255.224
64	6	/26		255.255.255.192
128	7	/25		255.255.255.128
256	8	/24	1C	255.255.255.0
512	9	/23	2C	255.255.254.0
1024	10	/22	4C	255.255.252.0
2048	11	/21	8C	255.255.248.0
4096	12	/20	16C	255.255.240.0
8192	13	/19	32C	255.255.224.0
16384	14	/18	64C	255.255.192.0
32768	15	/17	128C	255.255.128.0
65536	16	/16	1B	255.255.0.0
131072	17	/15	2B	255.254.0.0
262144	18	/14	4B	255.252.0.0
524288	19	/13	8B	255.248.0.0
1048576	20	/12	16B	255.240.0.0
2097152	21	/11	32B	255.224.0.0
4194304	22	/10	64B	255.192.0.0
8388608	23	/9	128B	255.128.0.0
16777216	24	/8	1A	255.0.0.0
33554432	25	/7	2A	254.0.0.0
67108864	26	/6	4A	252.0.0.0
134217728	27	/5	8A	248.0.0.0
268435456	28	/4	16A	240.0.0.0
536870912	29	/3	32A	224.0.0.0
1073741824	30	/2	64A	192.0.0.0

2147483648	31	/1	128A	128.0.0.0
4294967296	32	/0	256A	0.0.0.0

Предназначение на мрежовата маска – **определя каква част от IP адреса се отнася за net_ID и каква част – за host_ID.**

Маската се сравнява с мрежата побитово, отляво надясно. В мрежовата маска единиците отговарят на мрежовата част, а нулите – на адреса на възела.

Изпращайки пакет по мрежата, крайното устройство сравнява мрежовата маска със своя IP адрес и IP адреса на получателя. Ако битовете на мрежовата част съвпадат, значи и двата адреса (на изпращача и на подателя) се намират в една и съща мрежа и пакета се доставя локално. Ако не съвпадат, изпращащият възел изпраща пакета на интерфейса на локалния маршрутизатор за изпращане в друга мрежа.

Брой възможни мрежови адреси – взимат се отредените за host_id битове и с тях се повдига 2 на съответната степен. Например, за host_id са отделени 6 бита, тогава възможните мрежови адреси в такава мрежа (/26) е $2^6 = 64$.

Максималният брой мрежови адреси е $2^8 = 256$. От него трябва да извадим два адреса – частта, в която host_id се състои само от 0 се използва за идентификатор на мрежата и не се присвоява на конкретен възел от мрежата.

Частта, в която host_id се състои само от единици се използва за broadcast разпращане до всички адреси. Този адрес също не се присвоява на конкретни възли от мрежата.

По този начин възможният брой използвани адреси в една мрежа е $256 - 2 = 254$.

ПУБЛИЧНИ И ЧАСТНИ АДРЕСИ

Поради ограничения ресурс от 32-битови IP адреси съществува опасност от тяхното изчерпване. Едно от решенията за намаляване на тази опасност е резервирането на част от адресите за вътрешна употреба в отделните организации.

RFC 1918 регламентира това резервиране. Запазени са няколко диапазона адреси от мрежи, клас А, В и С.

А – запазена е една мрежа от клас А – 10.0.0.0;

В – запазени са 16 мрежи от клас В – 172.16.0.0 – 172.31.0.0;

С – запазени са 256 мрежи от клас С – 192.168.0.0 – 192.168.255.0

Частните адреси позволяват на възлите от мрежата да обменят данни помежду си без да използват **уникални** IP адреси. Частните адреси **не се маршрутизират** в Internet.

Съществуват и частни адреси за диагностика на устройствата. Наричат се **адреси за обратна връзка (loopback address)**. За такива адреси е запазена мрежата 127.0.0.0 от клас А.

ЗАДАЧИ:

Задача 1: Определете от кой клас са следните адреси:

1. 127.0.0.1 - А
2. 201.13.123.245 - С

3. 226.4.37.105 - D
4. 103.24.254.0 - A
5. 10.234.17.25 - A
6. 154.12.255.255 - B
7. 13.13.13.13 - A
8. 204.0.3.1 - C
9. 193.256.1.16 - C
10. 194.87.45.0 - C
11. 195.34.116.255 - C
12. 161.23.45.305 - nonexisted address

Кой от тези адреси може да се ползва като постоянен адрес на възел в Internet?

Всички без 1, 6, 10 и 12:

1 – loopback адрес;

10 – идентификатор на мрежа, не се присвояват на крайни устройства;

6 – broadcast адрес;

12 – такъв адрес не съществува, последният октет е извън обхвата 0-255.

Задача 2: Възел в мрежата има адрес 198.65.12.67, мрежовата маска е 255.255.255.240. Определете адреса на подмрежата. Какъв е максималният брой адреси в тази (под)мрежа?

Започва се от маската – 255.255.255.240 отговаря на префикс /28 – взети са 4 бита от host_id => имаме 16 мрежи с 16 адреса във всяка мрежа:

198.65.12.0-198.65.12.15 – Ist subnet;

195.65.12.16-198.65.12.31 – IInd subnet;

198.65.12.32-198.65.12.47 – IIIrd subnet;

198.65.12.48-192.168.12.63 – IVth subnet;

198.65.12.64-192.65.12.79 – Vth subnet

Следователно адресът 198.65.12.67 попада в петата подмрежа. Мрежовият адрес на тази мрежа е 198.65.12.64/28. Максималният брой възли в тази мрежа е $2^4 - 2 = 16 - 2 = 14$.

Сравняваме двоично само последния октет от адреса с последния октет от мрежовата маска:

67 – 01000011

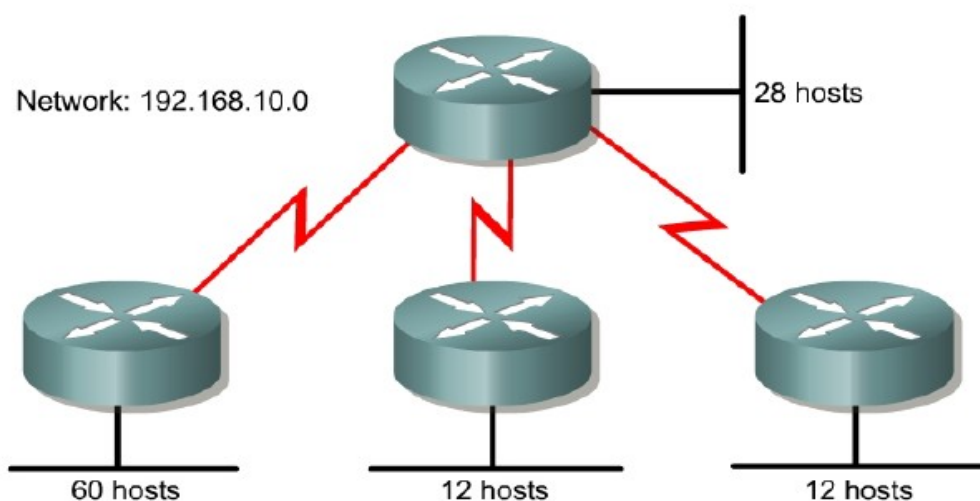
240 – 11110000

64 – 01000000

→ мрежовият адрес е 198.65.12.64/28

sipcalc 108.65.12.67/28

host address: 198.65.12.67
network address: 192.168.12.64
network mask: 255.255.255.240
network mask (bits): 28
network mask (hex): FFFFFFF0
broadcast address: 192.65.12.79
addresses in network: 16
network range: 192.65.12.64-192.65.12.79
usable addresses: 192.65.12.65-192.65.12.78

Задача 3:

Имате мрежата на горната фигура. Отпуснат ви е IPv4 адресния блок 192.168.10.0/24. Как ще разпределите адресното пространство така, че да имате възможно най-оптимално използване на IP адресите?

(Заб. Тук можеш да посочиш различни префикси и различен брой мрежовите сегменти и хостове в тях)

Задача 4:

В Интернет пространството трябва да рекламирате префиксите 62.44.120.0/24, 62.44.121.0/24, 62.44.122.0/24 и 62.44.123.0/24. Как можете да представите тези 4 префикса само с един, за да не хабите честотна лента по линията към съседния рутер. (тук имаме супернетване, отг. е 62.44.120.0/22)

(Може да се посочи и пример с префикси 62.44.110.0/24, 62.44.111.0/24, ... 62.44.117.0/24 – 62.44.110.0/21)

Задача 5:

IP мрежата 62.44.109.0/24 е разделена на 4 подмрежа. Кой е първият (последният, бродкаст и т.н.) използваем (хост) адрес на втората (3-та, 4-та) подмрежа?

IPv6

IPv6 не е обратно съвместим с IPv4, необходими са промени в мрежови устройства и

услуги. Според RFC 4291: адресното пространство от 32-битово става 128-битово: 2^{32} (4.3×10^9) с/у 2^{128} (3.4×10^{38}). Автоконфигуриране. RFC 4862 дефинира автоматично (plug-and-play) присвояване на адрес без помощта на DHCP сървър като в IPv4.

Цели на протокола IPv6 – същите като на протокола IPv4: присъединяване на адреси към мрежовите устройства; маршрутизиране на пакетите в мрежата; други) какви други :))

За разлика от протокола IPv4, в който се използва десетична нотация на записване на мрежовите адреси, в шестата версия на протокола IP за избягване на объркване се използва по-различна нотация. За разделител между отделните части на адреса се използва :, а не .. Също така не се използва десетичен запис на числата, а шестнадесетичен.

Структура на хедъра в IPv6

Version (4)	Traffic Class (8)	Flow Label (20 bits)	
Payload length (16)		Next Header (8)	Hop Limit (8)
Source Address (128 bits)			
Destination Address (128 bits)			

traffic class (заменя IPv4 ToS);

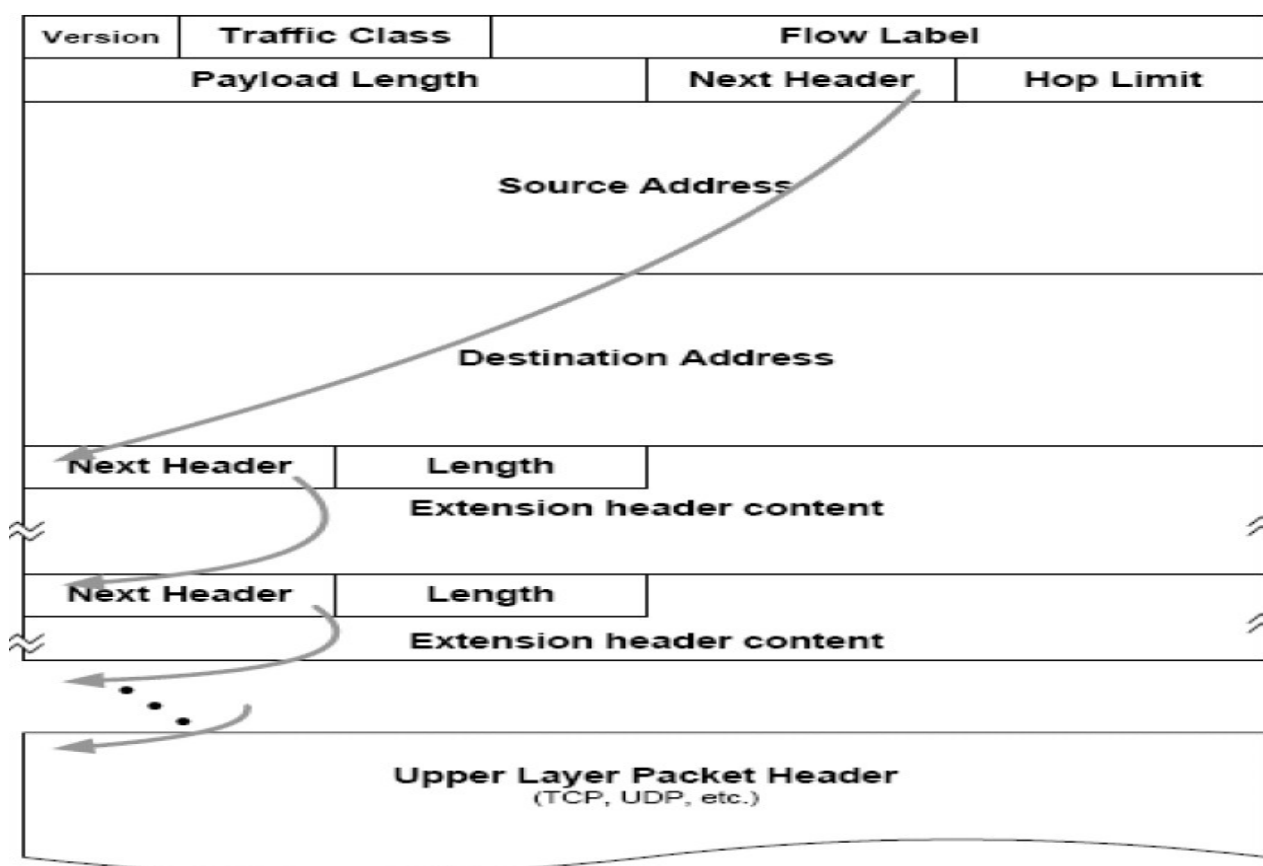
flow label (ново QoS management);

payload length (до 64KB);

next header (заменя IPv4 protocol);

hop limit (заменя IPv4 TTL).

Разширение на хедъра в IPv6



Extension Header	Type	Remarks
Hop-by-hop Options	0	used for options that apply to intermediate routers
Routing	43	used for source routing
Fragment	44	processed only by the final recipient
Destination Options	60	used for options that apply only for the final recipient
Authentication header (AH)	51	used for IPsec integrity protection
Encapsulating Security Payload (ESP)	50	used for IPsec integrity and confidentiality protection
Mobility	135	used for managing mobile IPv6 bindings

В IPv6 фрагментирането на пакетите става още при източника.

В IPv4 рутерът фрагментира пакета, когато MTU на следващия канал е по-малък. Ако отсреща не се възстанови оригиналният пакет, сесията се разваля.

В IPv6 всеки хост използва Path Maximum Transmission Unit (PMTU) Discovery, за да

научи размера на MTU по пътя, за да не се налага фрагментиране.

IPv6 адресиране

2001:0db8:9095:02e5:0216:cbff:feb2:7474

8 групи с по 4 шестнадесетични числа

Мрежовият префикс (RFC 4291) е аналогичен на означението с "/" на SM в IPv4:

IPv6 address/prefix length

Например адрес с 32-bit мрежов префикс:

2001:0db8:9095:02e5:0216:cbff:feb2:7474/32

32-битов мрежов префикс

48-битов мрежов префикс

64-битов мрежов префикс

Запис на IPv6 адреси

2001:DB8:0:0:8:800:200C:417A unicast

FF01:0:0:0:0:0:0:101 multicast

0:0:0:0:0:0:0:1 loopback

0:0:0:0:0:0:0:0 unspecified

Се представят:

2001:DB8::8:800:200C:417A

FF01::101

::1

::

ПРАВИЛНО представяне на 60-bit префикс:

2001:0DB8:0000:CD30:0000:0000:0000:0000/60

2001:0DB8::CD30:0:0:0/60

2001:0DB8:0:CD30::/60

НО

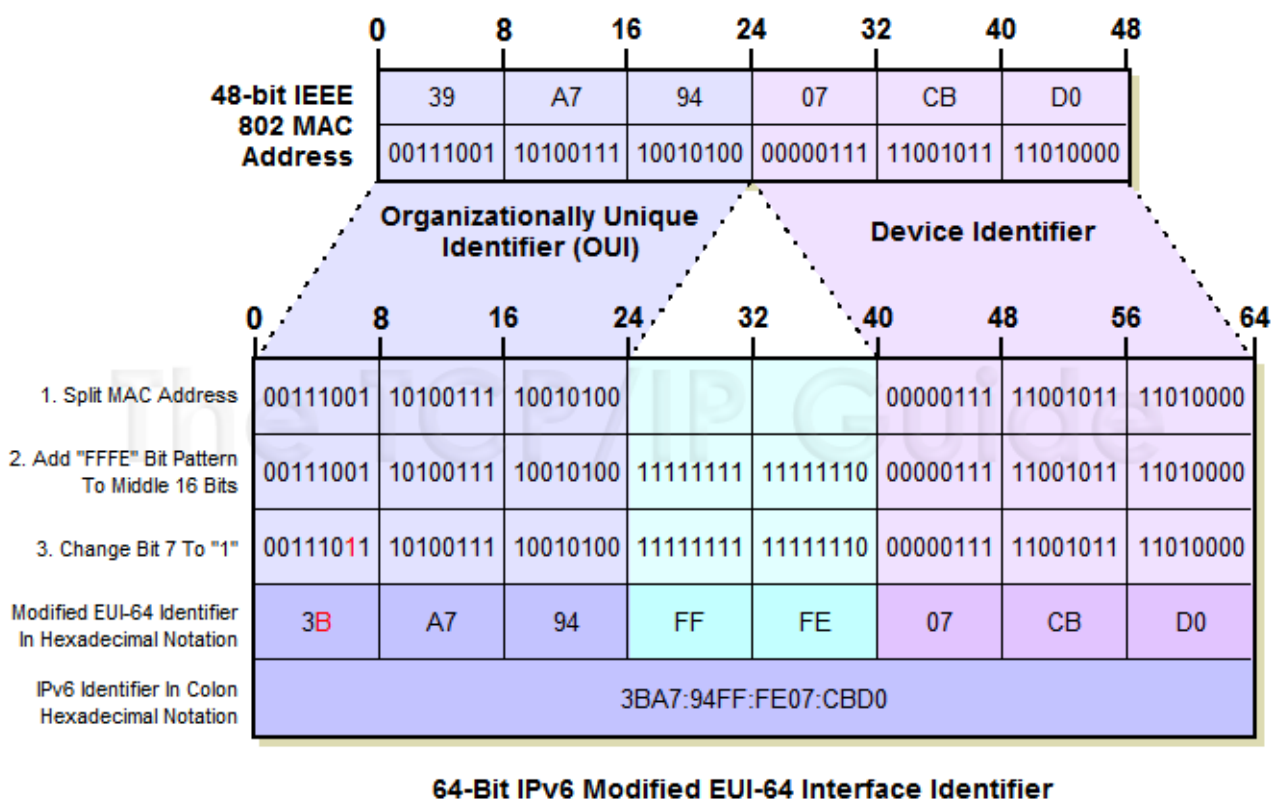
2001:0DB8::CD30::/60

е НЕПРАВИЛНО

Защо няма Broadcast адреси?

Interface ID

EUI-64 формат:



<https://tools.ietf.org/html/rfc4291>:

"u" bit според IEEE EUI-64 терминологията (глобално/локално администриране) при формиране на IEEE EUI-64 идентификатори - Modified EUI-64 format, се усдтановява от 0 в 1.

С **ip a** да им се покаже Link-local и global scope адреси.

Да се покаже и обясни команда **ip neighbor** и ролята на ICMPv6. Neighbor Discovery (ND) и Router Discovery (RD) в IPv6 заместват ARP. По този механизъм се открива и PMTU. Както и автоконфигурирането – Stateless получаването на IPv6 адреси. Да се каже нещо и за **radvd**.

Структура на адрес от протокола IPv6 – състои се от 8 hextets за разлика от 4-те октета при четвъртата версия на протокола. Адресът е разделен с : на групи числа в интервала 0000-FFFF (0-65535) за разлика от протокола IPv4, където октетите съдържат числата от 0 до 255 (00-FF). Типичният вид на един адрес от шестата версия на протокола има следния вид:

2001:05c0:9168:0000:0000:0000:0000:0001/128

При записването на тези адреси е допустимо:

1. премахването на водещата 0 от съответната група – например 05c0 може да бъде записано като 5c0;
2. веднъж и само веднъж в целия адрес може да бъде заменена група от последователни 0000 със символа „::“ – например 0000:0000:0000:0000 да бъде изписана като ::

Горният адрес 2001:05c0:9168:0000:0000:0000:0001/128 със спазване на горните правила може да бъде записан като 2001:5c0:9168::1/128.

Други примери за подобно изписване:

ПРАВИЛНО представяне на 60-bit префикс:

2001:0DB8:0000:CD30:0000:0000:0000:0000/60

2001:0DB8::CD30:0:0:0/60

2001:0DB8:0:CD30::/60

Префиксът /128 също като префикса /32 в четвъртата версия на протокола се използва за определяне на net_ID и host_ID частта от адреса.

От шестата версия на протокола са премахнати някои функции, усложняващи работата на маршрутизаторите:

1. маршрутизаторите повече не са длъжни да фрагментират пакетите, а просто ги отхвърлят с ICMP съобщение за надвишаване на MTU. Фрагментацията е възможна по инициатива на предаващата страна и е нейна грижа. Използва се технологията [Path MTU discovery](#) за предварително определяне на маршрута, по който ще минат пакетите до получателя им;
2. от IP заглавието на протокола е изключена контролната сума, която е приета, че е излишна при наличието на контролни суми в каналните (ethernet) и транспортни (TCP и UDP) протоколи.

Подобрения спрямо IPv4:

1. При скоростни мрежи е възможно поддръжката на огромни пакети (jumbograms) с размер до 4 gb;
2. TimeToLive (TTL) е преименуван на HopLimit;
3. Поява на етикети на потоци и класове на трафик (свързано е с QoS);
4. Поява на многоадресно (multicast) изпращане на пакети.

АВТОКОНФИГУРИРАНЕ

При първоначалната инициализация на мрежовия интерфейс, на него се дава локален IPv6 адрес, състоящ се от префикс fe80::/10 и идентификатор на интерфейса, разположен в младшата част на адреса. Като идентификатор на интерфейса се използва 64 битовия, разширен уникален идентификатор EUI-64, асоцииран често с MAC адреса на интерфейса. Локалният IPv6 адрес действителен само в границите на ethernet сегмента и основно се използва за обмяна на пакети по протокола ICMPv6.

За получаване на друг адрес, възелът може да изпрати ICMPv6 съобщение „Router Solicitation“ до груповия (multicast) адрес на маршрутизатора, който отговаря с ICMPv6 съобщение „Router Advertisement“, съдържащо информация за мрежовия

префикс, за адреса на шлюза (gateway), за адресите на рекурсивните DNS сървъри, за MTU и още други параметри. На основата на тази информация и обединявайки мрежовия префикс и идентификатора на интерфейса, възелът избира нов адрес. За защита на персонални данни, идентификатора на интерфейса може да бъде заменен с псевдослучайно число.

За по-голям административен контрол може да бъде използван и протокола DHCPv6, позволяващ даването на конкретен адрес на конкретен възел.

ЕТИКЕТ НА ПОТОК (FLOW LABELS)

Позволява значително опростяване на процедурата на маршрутизация на еднородни потоци от пакети.

Поток – последователност от пакети, изпратени до определен адресат. Предполага се, че всички пакети от този поток ще бъдат обработени по определен начин, който се задава в допълнителните заглавия на пакета.

Допустимо е съществуването на повече от един поток между изпращача и получателя. Етикета се присвоява от възела, който изпраща пакета и представлява 20-битово псевдослучайно число. Всички пакети от един поток трябва да имат еднакви етикети, обработвани от маршрутизатора.

КЛАСОВЕ ТРАФИК

Клас на трафика	Предназначение
0	Нехарактеризиран трафик
1	Запълващ трафик (мрежови новини)
2	Несъществен информационен трафик (email)
3	резерв
4	Съществен трафик (FTP, HTTP, NFS)
5	резерв
6	Интерактивен трафик (telnet, X-terminal, SSH)
7	Управляващ трафик (маршрутна информация, SNMP)

ТИПОВЕ IPv6 АДРЕСИ

- unicast – адресират само един интерфейс, който получава само пакети, адресирани до него
- anycast – синтактично не се различават от unicast адресите, но адресират група от интерфейси. Пакет, изпратен на такъв адрес, ще се получи на най-близкия по метрика интерфейс. Този тип адреси се използват

изключително от маршрутизатори;

- multicast – също адресират група от интерфейси. Пакет, изпратен до такъв адрес, ще се получи на **ВСИЧКИ** интерфейси, присъединени към групата за много адресно разпространяване.

Задачи по IPv6

1. Напишете коректните съкращения за IPv6 адресите:

2001:0d02:0000:0000:0014:0000:0000:0095

2001:0d02:0000:0000:0014:0000:0000:0095

2001:0d02:0000:0000:0014:0000:0000:0095

2. Имате MAC адрес на интерфейс wlan0 = 00:0e:2e:d1:ab:15 или 00-0C-27-A2-13-1B. Какъв ще бъде Host ID на IPv6 link local адреса на интерфейс wlan0 в двата случая?

3. Как би изглеждал IPv6 адреса 2001:4b58:acad:252::2e в разгърнат вид?