

Тема 14. Протоколът IP

- ТСР/IP
- IP адрес
- Класове IP Адреси
- Правила при IP адресирането
- Мрежова маска
- CIDR
- Частни адресни пространства
- Служебни адресни пространства
- Подмрежово маскиране
- Въпроси и задачи

ТСР/IP

ТСР/IP е основният мрежов протокол, който се използва в глобалната мрежа Интернет. ТСР/IP е съвкупност от два протокола, които работят в различни слоеве на мрежовия модел OSI – това са ТСР (в транспортния слой) и IP (в мрежовия слой). Основно функциите на двата протокола се свеждат до транспортиране на данните между мрежовите устройства.

За да може информацията в мрежата да достигне успешно до получателя е необходимо всяко устройство в мрежата да има свой уникален адрес. Този адрес се обозначава като **IP адрес**.

IP адрес

IP (Internet Protocol) адресът е логически адрес, който се присвоява на всеки хост в мрежата. Един хост може да има няколко мрежови карти (няколко интерфейса). Всеки от тези интерфейси притежава собствен IP адрес. Например, всеки компютър притежава loopback интерфейс, чийто IP адрес е 127.0.0.1.

Хост, който има реален IP адрес има достъп до всички услуги в Интернет, също така може да предлага услуги. Достъп до Интернет може да се извършва чрез посредник (програма [proxy](#) или [NAT](#)). Единствено посредникът има реален адрес, другите хостове имат [частни IP адреси](#). В този случай потребителите могат да ползват, но не могат да предлагат интернет услуги. За разпределянето на адресите в глобалната мрежа Интернет отговаря американската организация IANA (Internet Assigned Numbers Authority). В рамките на една локална мрежа, IP адресите трябва да са уникални. Компютрите в локалните мрежи, не представляващи част от Интернет, трябва да използват частни IP адреси.

Забележка:

Всеки доставчик на Интернет услуги (ISP) също предоставя на своите клиенти реален IP адрес. Този адрес може да се присвоява на компютър, притежаващ интернет достъп или на друг компютър/устройство. Например, клиентите на BTC ADSL се свързват към ADSL модема/рутера чрез локалната мрежа. Единствено рутерът има реален IP адрес. Компютърът (или компютрите), които имат достъп до Интернет имат локални (частни) IP адреси – ако вътрешният адрес на рутера е 192.168.1.1, то на останалите компютри адресите ще бъдат: 192.168.1.2, 192.168.1.3, ...

Какво ще се случи, ако две устройства имат еднакви IP адреси? Виж: [Конфликт на IP адреси](#)

IPv4 адрес

Всеки IP адрес се представя вътрешно в компютъра като двоично число. При **IPv4** протоколът се използва 32 битово адресиране. Тъй като двоичният запис е по-труден за възприемане, IP адресът се представя в десетично-точков формат. 32 битовият адрес се записва като поредица от четири 8 битови числа (октети). Всеки един от тези октети може лесно да се преобразува в десетично число. След това октетите се разделят с точка.

Например IP адресът

11000000 10101000 00000000 00000001

се записва като 192.168.0.1.

Числата в октетите могат да бъдат от 0 до 255 (2^8-1). Четирите октета се обозначават като **w.x.y.z**. За едно 32 битово число възможните комбинации са 2^{32} или 4 294 967 296 на брой компютри могат да се включат в една мрежа.

Компютър с нулев адрес (не асоцииран с IP адрес) се изписва като:
0.0.0.0

Специалният loopback адрес, означаващ „този компютър“ е:
127.0.0.1

IPv6 адрес

При протоколът **IPv6** се използва 128 битов адрес. Това е нов стандарт за адресиране, нарича се още Интернет протокол от следващо поколение IPng (**IP Next Generation**). Адресът от версия 6 се представя като осем 16 битови двоични числа. 16 битовите числа се записват в шестнадесетична бройна система и се разделят помежду си с двоеточия.

Например
1080:0:0:0:800:0:417A

е запис на IP адрес при протокола **IPv6**. Нулите могат да не се изписват:
1080::800:0:417A

Компютър с нулев адрес се изписва като:
::

Специалният loopback адрес, означаващ „този компютър“ е:
::1

При 128 битовия адрес възможните комбинации са 2^{128} .

IP адресиране

IP адресът е съвкупност от две части – адрес на мрежата, в която е включено устройството и адрес на самото устройство. Например в IPv4¹ адреса 74.125.39.147 първите три октета идентифицират *адреса на мрежата*. Последното число е *адреса на компютъра*. Всички компютри включени в тази подмрежа ще имат един и същ мрежови адрес (74.125.39).

$$\underbrace{74.125.39}_{\text{мрежови адрес}} . \underbrace{147}_{\text{адрес на компютъра}}$$

При изпращане на съобщение в Интернет до компютър с IP адрес 74.125.39.147 първата задача на мрежовите протоколи е да транспортират данните до подмрежата с адрес 74.125.39. След като пакетите с информация се "доставят" до тази мрежа се извършва вътрешно маршрутизиране, така че те да достигнат до компютър с адрес 147.

В разгледания пример първите три октета са за мрежовия адрес. Това обаче не винаги е така. Частта за мрежовия адрес и частта за адреса на компютъра се определят от *класа на IP адреса*.

Класове IP Адреси

При 32 битовото адресиране възможните комбинации от адреси са 2^{32} . Но на практика не всички адреси се използват. При IP адресирането са дефинирани 5 множества от IP адреси, които са известни като **класове**. При първите 3 класа, IP адресът включва мрежова част (N – net) и част за устройството (H – host).

Клас	w	x	y	z
Клас А	0 N N N N N N N N	H H H H H H H H	H H H H H H H H	H H H H H H H H
Клас В	1 0 N N N N N N N	N N N N N N N N	H H H H H H H H	H H H H H H H H
Клас С	1 1 0 N N N N N N	N N N N N N N N	N N N N N N N N	H H H H H H H H
Клас D	1 1 1 0	Multicast адрес		
Клас E	1 1 1 1 0	Резервирани за бъдещо използване		

Табл. 14-1. 32-битови IP адреси от различен клас мрежа

¹ IPv6 адресите се състоят от две части: 64-битова маршрутизираща част, следвана от 64-битов идентификатор на хоста.

Клас А

Мрежова част - заделен е един октет. Мрежовият адрес започва задължително с 0 (в двоична бройна система), като по този начин възможните числа са 2^7 или 128. Два адреса са забранени за използване – 0 и 127. Така допустимите стойности за мрежови адрес са 126 на брой.

Част за устройството – остават три октета за адреса на устройството (24 бита). Възможните стойности са $2^{24} = 16\,777\,216$. От тях първият и последният адрес не се използват. Остават общо 16 777 214 адреса. Това е и броят на устройствата, които могат да се включват в мрежа от Клас А.

Клас В

Мрежова част – включва два октета. Мрежовият адрес започва задължително с 10 при неговото двоично представяне, при което стойностите на първия октет могат да бъдат в диапазона 128 – 191. За представяне на мрежовия адрес остават 14 бита. Възможните стойности за мрежови адреси са $2^{14} = 16\,384$.

Част за устройството – остават два октета или 16 бита - $2^{16} = 65\,536$ възможни стойности. От тях два адреса са забранени – първият и последният. Остават допустими 65 534 на брой адреси за устройства.

Клас С

Мрежова част – състои се от три октета или 24 бита. Първите 3 знака на първия октет са 110, което определя и стойностите на първия октет да бъдат в диапазона между 192 и 223. Остават 21 бита за представяне на мрежовия адрес. Броят на възможните мрежи от Клас С е $2^{21} = 2\,097\,152$.

Част за устройството – остава 1 октет (8 бита) – $2^8 = 256$ на брой възможни стойности. Първият и последният адрес са забранени за използване. Така остават 254 на брой възможни устройства за свързване в мрежа от Клас С.

Клас D

Адресите от клас D са резервирани за multicast използване и не могат да се използват за присъединяване на адреси на устройства. Първият октет започва с 1110 в двоичен код и съответно стойностите на първия октет са в диапазона 224 – 239. Останалите 28 бита се използват за идентифициране на multicast групата.

Клас E

Адресите от този клас са експериментални и не се използват за публични цели. Първият октет започва с 1111 в двоичен вид, при което стойностите за първия октет са между 240 и 255.

Клас	Водещи битове	Начален адрес	Краен адрес	CIDR запис	Подразбираща се мрежова маска
Клас А	0	0.0.0.0	127.255.255.255	/8	255.0.0.0
Клас В	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
Клас С	110	192.0.0.0	223.255.255.255	/24	255.255.255.0
Клас D (multicast)	1110	224.0.0.0	239.255.255.255	/4	
Клас E (reserved)	1111	240.0.0.0	255.255.255.255	/4	

Табл. 14-2. Класове IP адреси

Правила при IP адресирането

- Всички устройства от един и същ физически мрежови сегмент трябва да имат еднакъв мрежови адрес;
- Всяко устройство от един мрежови сегмент трябва да има уникален адрес;

- Мрежовият адрес не може да бъде 127 – този адрес е запазен за loopback функции;
- Мрежовият адрес в двоичен вид не може да съдържа само единици – този адрес е запазен за broadcast функции;
- Адресът на устройството не може да съдържа само единици. Тези адреси са запазени за broadcast функции;
- Мрежовият адрес в двоичен вид не може да съдържа само нули. Този адрес означава цялата локална мрежа;
- Адресът на устройството не може да съдържа само нули. Когато частта за устройството съдържа само нули, а мрежовата част число различно от нула, тогава адресът като цяло се използва за обозначаване на локалната мрежа.

Мрежова маска

Определя кои битове от IP адреса са за мрежовата част и кои за адреса на устройството. По подразбиране за клас А, В и С се използват следните подмрежови маски:

Клас А – 255.0.0.0
 Клас В – 255.255.0.0
 Клас С – 255.255.255.0

Подмрежовата маска на клас А означава, че първите 8 бита определят мрежовата част, а останалите 24 са за частта на устройството.

Когато *устройство А* изпраща информация до *устройство В* в мрежата, *устройството А* използва подмрежовите маски, за да определи дали *устройството В* е в локалната или в друга мрежа. При това се извършват следните операции от *устройство А*:

1. Изпълнява се операция "логическо И" над две двоични числа – IP адреса на *устройство А* и подмрежовата маска на *устройство А*. Като резултат се получава мрежовия адрес на *устройство А*.
2. Същите изчисления се извършват и с IP адреса на *устройство В* и подмрежовата маска на *устройство В*. Като резултат се получава мрежовия адрес на *устройство В*.
3. Сравняват се двата мрежови адреса.
4. Ако те съвпадат, от гледна точка на *устройство А*, то двете устройства се намират физически в една и съща мрежа и ще комуникират директно.
5. Ако не съвпадат, то устройствата са в различни мрежови сегменти.

Пример:

Устройство А е с IP адрес 192.168.1.5, устройство В – съответно 192.168.2.6. Устройство А желае да изпрати информация до устройство В. Подмрежовите маски и на двете устройства са 255.255.0.0. Дали двете устройства ще комуникират директно или ще използват маршрутизатор?

IP адресът 192.168.1.5 представен в двоичен вид се записва така:

11000000 10101000 00000001 00000101

IP адресът 192.168.2.6 съответно изглежда така:

11000000 10101000 00000010 00000110

От устройство А се изпълнява операцията "логическо И" над следните операнди:

IP адрес на устройство А	11000000 10101000 00000001 00000101
Подмрежова маска на устройство А	11111111 11111111 00000000 00000000
Операция логическо И	11000000 10101000 00000000 00000000

За устройство В резултатът е следния:

IP адрес на устройство В	11000000 10101000 00000010 00000110
Подмрежова маска на устройство В	11111111 11111111 00000000 00000000
Операция логическо И	11000000 10101000 00000000 00000000

Двата резултата за устройства А и В съвпадат, т.е. мрежовите адреси са еднакви. Следователно устройствата са в една локална мрежа и ще комуникират директно помежду си.

CIDR

CIDR (*Classless Inter-Domain Routing*) е метод на представяне на мрежовата и хост частта от IP адреса. Приема се нотация за изписване на мрежов адрес – CIDR блок. При този запис след мрежовия адрес се поставя наклонена черта и се изписват броя на битовете в мрежовия адрес. Примерно: 192.168.0.0/16 е еквивалентно на мрежа 192.168.*.* маска 255.255.0.0. За да се използва метода е необходимо всички маршрутизиращи протоколи да пренасят информация освен за мрежовите адреси, така и за дължината на мрежовата част. При това става възможно да се адресират всички възможни IP адресни комбинации, премахва се разделянето на адресите на класове, премахва се понятието мрежова маска. В IPv6 мрежова маска не се дефинира като понятие, използва се единствено CIDR запис.

[Виж в Уикипедия](#)

Частни адресни пространства

Стандартът RFC 1819 определя следните групи IP адреси за устройства включени в локална мрежа:

CIDR блок адреси	Описание	Начален адрес	Краен адрес	Брой хостове
10.0.0.0/8	Клас А мрежа	10.0.0.0	10.255.255.255	16 777 214
172.16.0.0/12	16 клас В мрежи	172.16.0.0	172.31.255.255	1 048 574
192.168.0.0/16	256 клас С мрежи	192.168.0.0	192.168.255.255	65 534

Табл. 14-3. RFC 1819 - Частни адресни пространства

При конфигуриране на устройствата в една локална мрежа се препоръчва използването на тези IP адреси, за да не се влиза в конфликт с адресите на устройствата включени в глобалната мрежа Интернет. Адресите от тези групи не се използват в Интернет.

Служебни адресни пространства

Служебните IP адреси не са адреси на устройства включени в мрежата. Те са резервирани за следните цели:

- *мрежови адреси*. Представяват съвкупност от адреса на мрежата и нули за адреса на устройството.

Клас	Мрежови адрес
А	w . 0 . 0 . 0
В	w . x . 0 . 0
С	w . x . y . 0

Табл. 14-4. Мрежови адреси по клас

- *broadcast адреси*. Включват адреса на мрежата и единици за адреса на устройството.

Клас	Мрежови адрес
А	w . 255 . 255 . 255
В	w . x . 255 . 255
С	w . x . y . 255

Табл. 14-5. broadcast адреси по клас

IP адресът 255.255.255.255 е запазен като limited broadcast address. Използва се, когато устройството не знае мрежовия адрес. Обикновено маршрутизаторите са програмирани така, че да не пропускат този адрес извън мрежовия сегмент.

- *мрежовият адрес 127* е резервиран за loopback функции. Единственият IP адрес в този мрежови сегмент е '127.0.0.1'.
- *IP адресът 0.0.0.0* е запазен за обозначаване на компютър, който все още не е получил IP адрес.

Следващата таблица описва служебните адресни пространства, както са дефинирани в RFC 3330. Частните адресни пространства се включват и в тази област.

CIDR блок адреси	Описание	Референция
0.0.0.0/8	Нулева мрежа	RFC 1700, стр.4
10.0.0.0/8	Частно адресно пространство	RFC 1918
14.0.0.0/8	Публични мрежи за данни	RFC 1700, стр.181
24.0.0.0/8	Мрежи за кабелни телевизии	
39.0.0.0/8	Експериментални	RFC 1797
127.0.0.0/8	Loopback – всеки пакет изпратен към тази мрежа се връща на хоста. Единственият адрес, който се използва е 127.0.0.1/32	RFC 1700, стр.5
128.0.0.0/16	Резервирани (IANA)	
169.254.0.0/16	Използва се за автоконфигурация на IP адрес при отсъствие на DHCP сървър.	
172.16.0.0/12		RFC 1918
191.255.0.0/16	Резервирани (IANA)	
192.0.0.0/24	Резервирани (IANA)	
192.0.2.0/24	Документация и примери	
192.88.99.0/24	Преобразуване на IPv6 в IPv4	RFC 3068
192.168.0.0/16		RFC 1918
198.18.0.0/15	Network benchmark tests	RFC 2544
223.255.255.0/24	Резервирани (IANA)	
224.0.0.0/4	Multicasts (Клас D мрежа)	RFC 3171
240.0.0.0/4	Резервирани (Клас E мрежа)	
255.255.255.255	Broadcast	RFC 1700, стр.4

Табл. 14-6. RFC 3330 Служебни адресни пространства

Подмрежово маскиране

Ефективното използване на ограничения брой IP адреси в IPv4 налага да се използват мрежови маски, различни от подразбиращите се за класа мрежа. При използване на подмрежово маскиране частта от IP адреса за адрес на устройство се разделя на част за подмрежа и част за устройствата. На Фиг. 14-1 е показана мрежовата маска по подразбиране (default subnet mask) за мрежа клас B. Намалявайки частта за устройството с 8 бита се създава подмрежова част от

адреса. Комбинацията от мрежовата и подмрежовата част се наричат разширен мрежов префикс (представка).



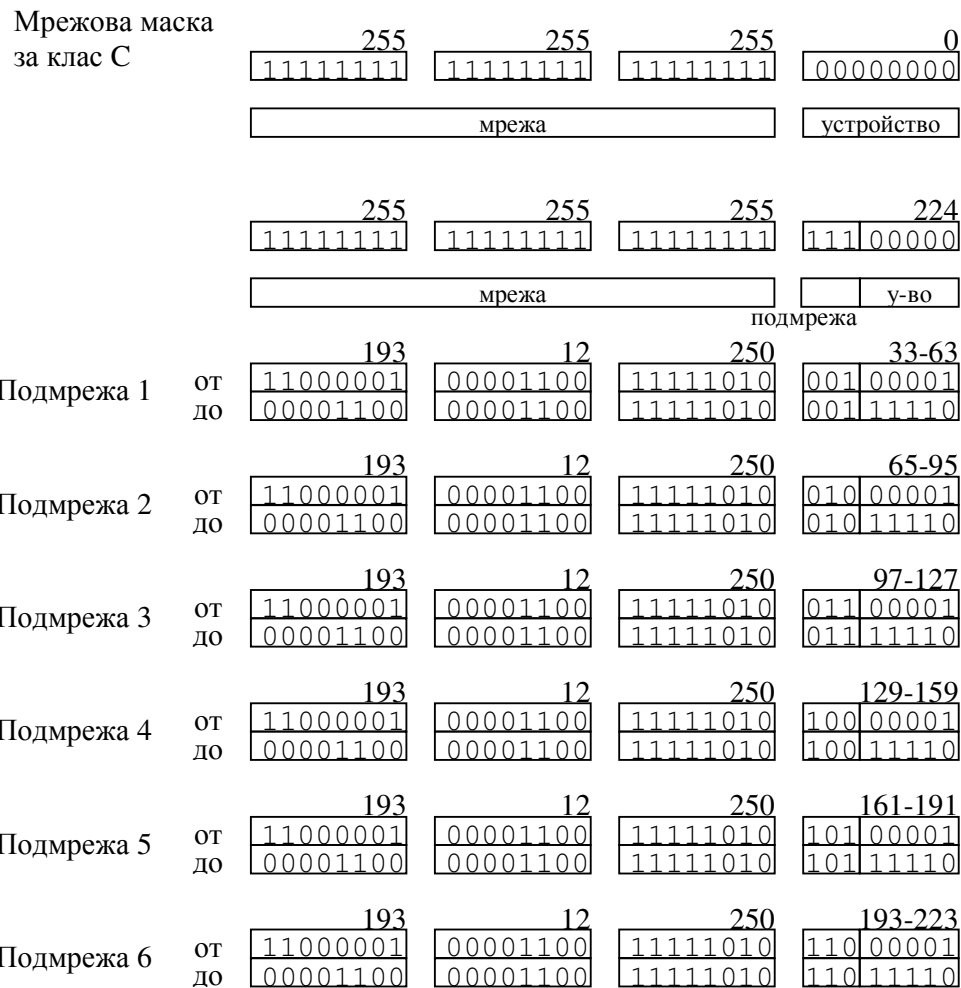
Фиг. 14-1

Разширяване на мрежовата част

При добавяне на битове към мрежовата маска, диапазонът с адреси се разделя на няколко по-малки диапазона. Броят на хостовете в подмрежа е степен на числото 2 (2, 4, 8, ...). Ако използваме цял октет от IP адреса за подмрежа (8 бита), би трябвало да можем да създадем 256 подмрежи. Това обикновено не е така, защото не всички комбинации са допустими. IP адресите с комбинацията от битове '1' в мрежовата и подмрежовата част се използват за broadcast, а адресите със стойност на битовете '0' – за мрежови адреси. Така, при N бита за подмрежова маска, броят на подмрежите е $2^N - 2$.

Пример:

Фирма, получава от доставчика си на Интернет мрежа клас C: '193.12.250.*', маска '255.255.255.0'. Във фирмата има 4 отдела със самостоятелни локални мрежи, като очакваният брой потребители, на които ще бъдат необходими реални IP адреси в следващите няколко години е 25. За 4 броя подмрежи трябва да се определи броя на битовете, които ще се използват за подмрежова част. При 2 бита, възможните подмрежи са 2 – недостатъчно, при 3 бита са 6 – следователно ще се използват три бита за подмрежа. С останалите 5 бита от IP адреса (за номер на устройство), броят на компютрите в подмрежите определяме по формулата $2^N - 2$, за N=5 това са 30 компютъра. Това удовлетворява зададения максимален брой на компютрите (25 по условие).



Фиг. 14-2

Разширяване на мрежовата част

Резултат:

Мрежата от 254 възможни реални IP адреса се раздели на 6 сегмента от по 30 хоста = 180 адреса. Остават 74 неизползваеми IP адреса. Използваната мрежова маска е: '255.255.255.224'. Създават се подмрежите:

№	от адрес	до адрес
1	193.12.250.33	193.12.250.63
2	193.12.250.65	193.12.250.95
3	193.12.250.97	193.12.250.127
4	193.12.250.129	193.12.250.159
5	193.12.250.161	193.12.250.191
6	193.12.250.193	193.12.250.223

Табл. 14-7. Подмрежи

От примера се вижда, че при този начин на подмрежово маскиране се губи възможността за използване на голям брой адреси. Съвременните маршрутизатори, използвани от доставчиците на интернет услуги използват маршрутни протоколи, изпращащи мрежовата маска при разпространяването на маршрутизиращата информация. Това позволява използването на адреси със стойност на подмрежовата част 0 и стойност за номер на устройство 0.

Въпроси и задачи

1. Определете класа на IP адресите от Табл. 14-8

IP адрес	Клас на IP адрес
132.97.3.11	
127.0.0.1	
224.12.34.56	
128.11.22.33	
10.1.2.3	
223.255.255.223	

Табл. 14-8

Определяне на класа IP адреси

2. Какъв е мрежовия адрес на устройство с IP адрес 201.200.200.15 с подмрежова маска по подразбиране?
3. Кои множества IP адреси са резервирани за използване в локална мрежа?
4. Какви преимущества има IPv6 в сравнение с IPv4?
5. При мрежа с адрес 10.0.0.0/8, колко бита ще бъдат необходими за създаване на 100 подмрежи? Каква ще бъде мрежовата представка за тези подмрежи?
6. Попълнете липсващата информация:
Начален адрес: 200.200.64.1
Краен адрес: ---- . ---- . ---- . ----
Подмрежова маска: 255.255.252.0