Поняли ведущие умы, что использовать классовые сети не удобно и нужно от них отказываться. Это привело к созданию бесклассовой адресации и маскам переменной длины, о чем мы ниже поговорим. Но перед этим пару слов о видах IP-адресов. Несмотря на то, что переход от классовой адресации к бесклассовой предполагал экономию IP-адресов, на деле эта проблема все равно решалась не полностью. Все упиралось в саму технологию IPv4. Объясним почему. Выше говорилось, что длина IP адреса равна 32 бита. Каждый бит может принимать значение 0 или 1, то есть два значения. Соответственно, чтобы вычислить все комбинации, надо возвести 2 в 32-ую степень. Получаем 4294967296 адресов. Если вычесть отсюда зарезервированные для специальных нужд и прочего, то останется примерно 4.2 млрд. адресов, когда на Земле проживает около 7.3 млрд. человек. Поэтому ведущие умы быстро просекли эту фишку и начали искать решение. Они решили выделить некое адресное пространство, которое будет использоваться только в пределах локальной сети и не будет использоваться в Интернете. Это разделило адреса на 2 лагеря: белые или публичные (англ. public) и серые или частные (англ. private).

Приведем диапазон адресов, которые выделены под локальные сети:

1. 10.0.0.0 — 10.255.255.255 с маской 255.0.0.0 (или кратко 10/8).
2. 172.16.0.0 — 172.31.255.255 с маской 255.240.0.0 (или кратко 172.16/12).
3. 192.168.0.0 — 192.168.255.255 (или кратко 192.168/16).

Если честно, мало где применяется адресация 172.16.X.X. Обычно в корпоративной среде всегда используется 10.X.X.X, а в домах/квартирах и мелких офисах 192.168.X.X.

Теперь обратим внимание на очень важную вещь, которую многие путают. Не путайте классовую адресацию и диапазон частных адресов. Очень много людей наступают на эти грабли и свято верят, что диапазон частных адресов 10.0.0.0 — 10.255.255.255 — это диапазон A класса.

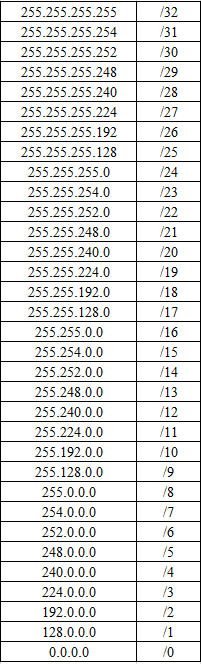
Разобрались, что такое частные адреса или private адреса. Но это еще не все. Есть еще список зарезервированных адресов, которые не могут светиться в Интернете. По ним написана целая документация на IETF. Имеется документ, где можно прочитать оригинал ([ссылка](https://tools.ietf.org/html/rfc3330)). Кратко опишем часто встречающиеся.

1. 0.0.0.0/8 — диапазон адресов, используемый хостами для самоидентификации. Обычно это можно увидеть, когда хост пытается получить IP-адрес от DHCP сервера. Так как изначально у него нету IP-адреса, то в поле источника он вставляет адрес из данного диапазона.
2. 127.0.0.0/8 — loopback или localhost адреса. Это IP-адреса, используемые компьютером, чтобы обратиться к самому себе. Очень полезно для проверки работы TCP/IP. Дело в том, что независимо от наличия соединения с Интернетом или локальной сетью, адреса из этого пула должны всегда пинговаться. Если этого не происходит, значит система накрылась или накрывается медным тазом.
3. 169.254.0.0/16 — link-local address или локальные адреса. Автоматически используются хостами при отсутствии DHCP-сервера или его недоступности. Это позволяет быстро организовать локальную сеть и проверить работу узлов. Однако данный пул адресов не маршрутизируется. Следовательно, выйти в Интернет с них не получится.
4. 224.0.0.0/4 — блок адресов, зарезервированный под многоадресную рассылку или multicast. Для тех, кто хочет побольше узнать про multicast, ([ссылка](https://tools.ietf.org/html/rfc3171)).

**Бесклассовая адресация (англ. Classless Inter-Domain Routing или CIDR)**.

Описана была в стандарте RFC1519 в 1993 году. Она отказалась от классовых рамок и фиксированной маски. Адреса делятся только на публичные и зарезервированные, о которых написано выше. Если в классовой адресации маска нарезалась единой для всех подсетей, то в бесклассовой — у каждой подсети может быть своя маска. На теории все хорошо и красиво, но нет ничего лучше, чем практика.

В качестве шпаргалки приведем список всех возможных масок.



Представим ситуацию. Вам выдали сеть 192.168.1.0/24 и поставили следующие условия:

1) Подсеть на 10 адресов для гостей.  
2) Подсеть на 42 адреса для сотрудников.  
3) Подсеть на 2 адреса для соединения 2 маршрутизаторов.  
4) Подсеть на 26 адресов для филиала.

Ок. Данная маска показывает, что в нашем распоряжении находятся 256 адресов. По условию эту сеть надо каким-то образом разделить на 4 подсети. Давайте попробуем. 256 очень хорошо делится на 4, давая в ответе 64. Значит один большой блок в 256 адресов можно поделить на 4 равных блока по 64 адреса в каждом. И все было бы прекрасно, но это порождает большое число пустых адресов. Для сотрудников, которым нужно 42 адреса, ладно, может в дальнейшем компания еще наймет. Но вот подсеть для маршрутизаторов, которая требует всего 2 адреса, оставит 60 пустых адресов. Да, вы можете сказать, что это private адреса, и кому дело до них. А теперь представьте, что это публичные адреса, которые маршрутизируются в Интернете. Их и так мало, а тут мы еще будем их отбрасывать. Это не дело, тем более, когда мы можем гибко управлять адресным пространством. Поэтому возвращаемся к примеру, и нарежем подсети так, как нам нужно.

Итак, какие подсети должны быть нарезаны, чтобы вместились все адреса, заданные по условию?!

1) Для 10 хостов, наименьшей подсетью будет блок из 16 адресов.

2) Для 42 хостов, наименьшей подсетью будет блок из 64 адресов.

3) Для 2 хостов, наименьшей подсетью будет блок из 4 адресов.

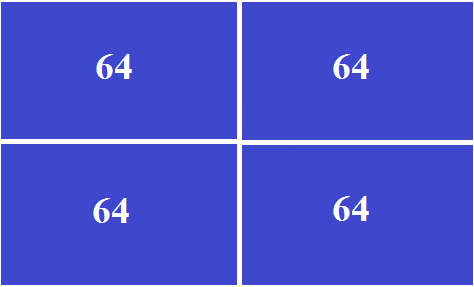
4) Для 26 хостов, наименьшей подсетью будет блок из 32 адресов.

Понимаю, что не все могут с первого раза в это вникнуть, и в этом нет ничего страшного. Все люди разные и по-разному воспринимают информацию. Для полноты эффекта покажем деление на картинке.

Вот у нас блок, состоящий из 256 адресов.



После деления на 4 части получается следующая картинка.



Выше мы выяснили, что при таком раскладе адреса используются не рационально. Теперь обратите внимание, как стало выглядеть адресное пространство после нарезки подсетей разной длины.



Как видите, в свободном доступе осталось куча адресов, которые мы в дальнейшем сможем использовать. Можно посчитать точную цифру. 256 — (64 + 32 + 16 + 4) = 140 адресов.

Вот столько адресов мы сэкономили. Двигаемся дальше и ответим на следующие вопросы:

— Какими будут сетевые и широковещательные адреса?

— Какие адреса можно будет назначить хостам?

— Как буду выглядеть маски?

Механизм деления на подсети с разной маской получил название **VLSM (от англ. Variable Length Subnet Mask)** или **маска подсети переменной длины**. Начинайте адресацию с самой большой подсети. Иначе вы можете попасть на то, что адреса начнут перекрываться. Поэтому сначала планируйте сеть на бумаге. Нарисуйте ее, изобразите в виде фигур, просчитайте вручную или на калькуляторе и только потом переходите настройке в боевых условиях.

Итак, самая большая подсеть состоит из 64 адресов. С нее и начнем. Первый пул адресов будет следующий:

* Адрес подсети — 192.168.1.0.
* Широковещательный адрес — 192.168.1.63.
* Пул адресов для назначения хостам от 192.168.1.1 до 192.168.1.62.

Теперь выбор маски. Тут все просто. Отнимаем от целой сети нужный кусок и полученное число записываем в октет маски. То есть 256 — 64 = 192 => маска 255.255.255.192 или /26.

Дальше идет подсеть поменьше. Состоит она из 32 адресов. Если первая заканчивалась на .63, то эта будет начинаться с .64:

* Адрес подсети — 192.168.1.64.
* Широковещательный адрес — 192.168.1.95.
* Пул адресов для назначения хостам будет от 192.168.1.65 до 192.168.1.94.
* Маска: 256 — 32 = 224 => 255.255.255.224 или /27.

3-я подсеть, которая предназначена для филиала, начнет старт с .96:

* Адрес подсети — 192.168.1.96.
* Широковещательный адрес — 192.168.1.111.
* Пул адресов для назначения хостам будет от 192.168.1.97 до 192.168.1.110.
* Маска: 256 — 16 = 240 => 255.255.255.240 или /28.

Ну и для последней подсети, которая уйдет под интерфейсы, соединяющие роутеры, будет начинаться с .112:

* Адрес подсети — 192.168.1.112.
* Широковещательный адрес — 192.168.1.115.
* Разрешенными адресами будут 192.168.1.113 и 192.168.1.114.
* Маска: 256 — 4 = 252 => 255.255.255.252 или /30.

Адрес 192.168.1.115 является последним используемым адресом. Начиная с 192.168.1.116 и до .255 свободны.

Вот таким образом, при помощи VLSM или масок переменной длины, мы экономно создали 4 подсети с нужным количеством адресов в каждой.

**Задача №3**

Разделите сеть 192.168.1.0/24 на 3 разные подсети. Найдите и запишите в каждой подсети ее адреса, широковещательный адрес, пул разрешенных к выдаче адресов и маску. Указываю требуемые размеры подсетей:

1) Подсеть на 120 адресов.

2) Подсеть на 12 адресов.

3) Подсеть на 5 адресов.