**Разбиение IP-сетей на подсети**

**Введение**

Проектирование, внедрение и управление эффективным планом IP-адресации обеспечивают надёжность и эффективность работы сетей. Это особенно актуально в случаях, когда увеличивается количество узлов сети. Понимание иерархической структуры IP-адреса и того, как изменить иерархию для повышения эффективности маршрутизации, является важной частью планирования схемы IP-адресации.

В исходном IPv4-адресе существует два уровня иерархии: сеть и узел. Эти два уровня адресации делают возможной базовую группировку в сети, которая способствует маршрутизации пакетов в сеть назначения. Маршрутизатор пересылает пакеты, основываясь на сетевой части IP-адреса. После нахождения сети определяется целевое устройство по узловой части адреса.

Однако по мере роста сети во многих организациях, когда к сети подключаются сотни и даже тысячи узлов, двухуровневая иерархия становится неэффективной.

При разделении сети на подсети в иерархию сети фактически добавляются три уровня: сеть, подсеть и узел. При добавлении нового уровня иерархии в IP-сети создаются дополнительные подгруппы. Это позволяет ускорить доставку пакетов и обеспечить дополнительную фильтрацию, способствуя сокращению объёма «локального» трафика.

В этом модуле подробно описывается создание и присвоение адресов IP-сети и подсети с помощью маски подсети.

**Разбиение IP-сетей на подсети**

**Введение**

**Позвоните мне!**

В этой главе вы узнаете, каким образом устройства можно разделить на подсети или небольшие сетевые группы на основе одной крупной сети.

В этом задании по моделированию вам необходимо придумать номер, который вы, возможно, используете ежедневно, например номер своего телефона. После выполнения задания подумайте о том, как телефонную нумерацию можно сравнить с методами, используемыми сетевыми администраторами для идентификации узлов, чтобы эффективно передавать данные.

Письменно ответьте на вопросы, приведённые ниже. Сохраните два раздела в бумажном или электронном виде для последующего обсуждения в аудитории.

* Объясните, как номер вашего мобильного или стационарного телефона разделяется на определяющие группы цифр. В номере вашего телефона используется код города? Идентификатор поставщика услуг? Код города, области или страны?
* Каким образом разделение вашего номера телефона на группы цифр помогает вам созваниваться и общаться с другими людьми?

[Работа в аудитории: позвоните мне! (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.0.1.2%20Call%20Me%21%20Instructions.pdf)

**Разбиение IPv4-сети на подсети**

**Сегментация сети**

Ранее при развёртывании сети организации часто подключали все компьютеры и другие сетевые устройства к одной IP-сети. Всем устройствам в организации назначались IP-адреса с одинаковой сетевой частью. Конфигурация такого типа называется плоской архитектурой сети. В небольшой сети с небольшим количеством устройств плоская архитектура не представляет проблемы. Однако по мере расширения сети с такой конфигурацией могут возникнуть серьёзные трудности.

Подумайте о том, как в сети Ethernet устройства выполняют поиск необходимых служб и устройств с помощью широковещательной рассылки. Как вы помните, широковещательное сообщение доставляется всем узлам данной сети. Протокол DHCP — пример сетевой службы, которая зависит от широковещательной рассылки. Устройства отправляют по сети широковещательные запросы, чтобы определить местонахождение DHCP-сервера. В крупной сети из-за этого может создаваться значительный трафик, который замедлит общую работу сети. Кроме того, поскольку широковещательная рассылка выполняется по всем устройствам, им необходимо принять и обработать трафик, что приводит к повышению требований к обработке. Если устройство должно обработать значительный объём широковещательных рассылок, это может даже привести к замедлению работы устройства. По этой причине более крупные сети необходимо разделить на более мелкие подсети, предназначенные для небольших групп устройств и служб.

Процесс сегментации сети путём разделения её на несколько более мелких сетей называется разбиением на подсети. Эти более мелкие сети называются подсетями. Сетевые администраторы могут группировать устройства и службы в подсети по их географическому местоположению (например, 3-й этаж здания), организационному подразделению (например, отдел продаж) или по типу устройств (принтеры, серверы, глобальная сеть и т.п.) или по другому значимому для сети принципу. Разбиение на подсети может снизить общую нагрузку на сеть и повысить её производительность.

**Примечание**. Подсеть аналогична сети, и оба этих термина можно использовать как синонимы. Большинство сетей сами являются подсетями более крупных блоков адресов.

# Разбиение IPv4-сети на подсети

## Сегментация сети

Маршрутизатор необходим для взаимодействия узлов из разных подсетей. Устройства в сети используют интерфейс маршрутизатора, подключённый к их локальной сети, в качестве шлюза по умолчанию. Трафик, отправляемый на устройство в удалённой сети, будет обработан маршрутизатором и отправлен в направлении сети назначения. Чтобы определить, является ли трафик локальным или удалённым, маршрутизатор использует маску подсети.

В пространстве подсети этот механизм реализуется аналогичным образом. Как показано на рисунке, подсети образуют несколько логических сетей из одного блока адресов или сетевого адреса. Каждая подсеть рассматривается как отдельное сетевое пространство. Устройства в одной подсети должны использовать адрес, маску подсети и шлюз по умолчанию той подсети, которой они принадлежат.

Трафик не может передаваться между подсетями без использования маршрутизатора. У каждого интерфейса маршрутизатора должен быть IPv4-адрес, принадлежащий сети или подсети, к которой подключён этот интерфейс.

# Разбиение IPv4-сети на подсети

## Значимость разбиения IP-сети на подсети

Как показано на рисунке, при планировании подсетей требуется учитывать требования организации к использованию сети и предполагаемую структуру подсетей. Для начала необходимо изучить требования к сети. Это означает, что нужно изучить всю сеть, определить её основные части и разделить их на сегменты. План распределения адресов содержит информацию о требуемом размере подсети, количестве узлов и принципе назначения адресов узлам. Кроме того, необходимо определить узлы, которым нужно выделить статические IP-адреса, и узлы, которые смогут получать сетевые настройки по протоколу DHCP.

Определяя размер подсети, необходимо оценить количество узлов, которым потребуются IP-адреса в каждой подсети в рамках разделённой частной сети. Например, при проектировании сети студенческого городка нужно оценить количество узлов в локальной сети администраторов, в локальной сети преподавателей и в локальной сети учащихся. В домашней сети можно оценить количество узлов в локальной сети жилой зоны и в локальной сети домашнего офиса.

Как уже упоминалось ранее, диапазон частных IP-адресов, используемых в локальной сети, выбирается сетевым администратором, и к выбору этого диапазона следует отнестись с должным вниманием. Необходимо убедиться, что количества адресов будет достаточно для активных в данный момент узлов и для будущего расширения сети. Запомните диапазоны частных IP-адресов:

* 10.0.0.0 с маской подсети 255.0.0.0
* 172.16.0.0 с маской подсети 255.240.0.0
* 192.168.0.0 с маской подсети 255.255.0.0

На основании требований к IP-адресам можно определить диапазон или диапазоны узлов для развёртывания. После разбиения выбранного пространства частных IP-адресов на подсети будут получены адреса узлов, соответствующие требованиям к сети.

Публичные адреса, используемые для подключения к Интернету, обычно выделяются оператором связи. Хотя в данном случае применяются те же принципы разбиения на подсети, это не всегда является обязанностью администратора сети организации.

**Разбиение IPv4-сети на подсети**

**Значимость разбиения IP-сети на подсети**

Определите стандарты присвоения IP-адресов в диапазоне каждой подсети. Например:

* Принтерам и серверам будут назначены статические IP-адреса
* Пользователи будут получать IP-адреса от DHCP-серверов в подсетях /24
* Маршрутизаторам назначаются первые доступные адреса узла в диапазоне.

Два существенных фактора, влияющих на определение необходимого блока частных адресов, — это количество необходимых подсетей и максимальное количество узлов в каждой подсети. Каждый из этих блоков адресов позволит распределить узлы исходя из размера сети, количества узлов, активных в настоящий момент, или добавляемых в ближайшем будущем. Требования к IP-пространству определят диапазон или диапазоны используемых узлов.

В примерах ниже отображено разбиение на подсети на основе блоков адресов с масками подсети 255.0.0.0 и 255.255.255.0, 255.255.0.0.

# Разбиение IPv4-сети на подсети

## Разбиение IPv4-сети на подсети

Каждый сетевой адрес содержит допустимый диапазон адресов узлов. Все устройства, подключённые к одной и той же сети, будут иметь IPv4-адрес узла этой сети, а также общую маску подсети или префикс сети.

Префикс и маска подсети — это разные способы представления одного и того же — сетевой части адреса.

Для создания IPv4-подсетей мы задействуем один или нескольких бит из узловой части в качестве бит сетевой части. Для этого мы расширяем маску подсети. Чем больше заимствовано бит из узловой части, тем больше подсетей можно создать. Для каждого заимствованного бита количество доступных подсетей удваивается. Например, если заимствовать один бит, можно создать две подсети. Для двух бит — 4 подсети, для трёх бит — 8 подсетей и т. д. Однако с каждым заимствованным битом уменьшается количество адресов узлов в каждой подсети.

Биты могут быть заимствованы только из узловой части адреса. Сетевая часть адреса выделяется оператором связи, и изменить её невозможно.

**Примечание**. На рисунках в примерах отображается только последний октет в двоичном формате, поскольку использовать можно только биты из узловой части.

Как показано на рисунке 1, сеть 192.168.1.0/24 имеет 24 бита в сетевой части и 8 бит в узловой части, что обозначено маской подсети 255.255.255.0 или записью с префиксом /24. Без разделения на подсети эта сеть поддерживает работу только с одним интерфейсом локальной сети. Если нужна дополнительная локальная сеть, основную сеть нужно разделить на подсети.

На рисунке 2 в самом старшем разряде (крайний левый бит) заимствуется 1 бит в узловой части, расширяя сеть до 25 бит. При этом создаются две подсети: первая определяется цифрой 0 в заимствованном бите, а вторая — цифрой 1 в заимствованном бите. Для маски подсети обеих сетей используется цифра 1 в заимствованном бите, чтобы показать, что этот бит теперь входит в сетевую часть адреса.

Как показано на рисунке 3, если преобразовать двоичный октет в десятичный формат, мы увидим, что адрес первой подсети — 192.168.1.0, а адрес второй подсети — 192.168.1.128. Поскольку был заимствован бит, маска подсети для каждой подсети будет 255.255.255.128 или /25.

**Разбиение IPv4-сети на подсети**

**Разбиение IPv4-сети на подсети**

В примере выше сеть 192.168.1.0/24 была разделена на две подсети:

192.168.1.0/25

192.168.1.128/25

Обратите внимание, что на рисунке №1 к интерфейсам GigabitEthernet маршрутизатора R1 подключены два сегмента локальной сети. Подсети будут использоваться для сегментов, подключённых к этим интерфейсам. Чтобы выполнять роль шлюза для устройств в локальной сети, каждому из интерфейсов маршрутизатора должен быть назначен IP-адрес в диапазоне допустимых адресов для назначенной подсети. В качестве адреса интерфейса маршрутизатора рекомендуется использовать первый или последний доступный адрес диапазона сети.

Первая подсеть (192.168.1.0/25) используется для сети, подключённой к интерфейсу GigabitEthernet 0/0, а вторая подсеть (192.168.1.128/25) — к интерфейсу GigabitEthernet 0/1. Чтобы назначить IP-адрес каждому из этих интерфейсов, необходимо определить диапазон допустимых IP-адресов для каждой подсети.

Ниже даны рекомендации для каждой из подсетей.

* **Сетевой адрес** — все биты 0 в узловой части адреса.
* **Адрес первого узла** — все биты 0, а также крайний правый бит 1 в узловой части адреса.
* **Адрес последнего узла** — все биты 1, а также крайний правый бит 0 в узловой части адреса.
* **Широковещательный адрес** — все биты 1 в узловой части адреса.

Как показано на рисунке 2, адрес первого узла в сети 192.168.1.0/25 — 192.168.1.1, а адрес последнего узла — 192.168.1.126. На рисунке 3 показано, что адрес первого узла в сети 192.168.1.128/25 — 192.168.1.129, а адрес последнего узла — 192.168.1.254.

Чтобы назначить адрес первого узла в каждой подсети интерфейсу маршрутизатора для этой подсети, используйте команду **ip address** в режиме конфигурации интерфейса, как показано на рисунке 4. Обратите внимание, что для каждой подсети используется маска подсети 255.255.255.128, которая означает, что под сетевую часть адреса отведено 25 бит.

Конфигурация узла для сети 192.168.1.128/25 показана на рисунке 5. Обратите внимание, что IP-адресом шлюза является адрес (192.168.1.129), настроенный на интерфейсе G0/1 маршрутизатора R1, а маской подсети является 255.255.255.128.

# Разбиение IPv4-сети на подсети

## Разбиение IPv4-сети на подсети

**Расчёт подсетей**

Для расчёта количества подсетей используйте следующую формулу:

2^n (где n = количество заимствованных бит)

Как показано на рисунке 1 для примера 192.168.1.0/25, расчёт выглядит следующим образом:

2^1 = 2 подсети

**Расчёт узлов**

Для расчёта количества узлов в одной сети используйте следующую формулу:

2^n (где n = количество бит, оставшихся в узловой части адреса)

Как показано на рисунке 2 для примера 192.168.1.0/25, расчёт выглядит следующим образом:

2^7 = 128

Поскольку для узлов не может использоваться сетевой адрес или широковещательный адрес из подсети, эти два адреса нельзя назначить узлам. Это означает, что в каждой из подсетей можно использовать 126 (128-2) адресов узлов.

Таким образом, в этом примере заимствование одного бита узла для сети приведёт к созданию двух подсетей, в каждой из которых можно назначить 126 узлов.

**Разбиение IPv4-сети на подсети**

**Разбиение IPv4-сети на подсети**

Рассмотрим сетевую инфраструктуру, в которой требуются три подсети.

Если использовать одинаковый блок адресов 192.168.1.0/24, для создания как минимум трёх подсетей необходимо позаимствовать несколько бит из узловой части. Если заимствовать один бит, будут созданы только две подсети. Для создания большего количества подсетей необходимо заимствовать больше бит из узловой части. Рассчитаем количество подсетей, создаваемых при заимствовании двух бит из узловой части по формуле 2^n:

2^2 = 4 подсети

Заимствование двух бит позволяет создать 4 подсети, как показано на рисунке 1.

Как вы помните, маска подсети должна изменяться для отражения заимствованных бит. В этом примере при заимствовании двух бит маска будет расширена на два бита в последнем октете. В десятичном формате маска имеет вид 255.255.255.192, поскольку последний октет в двоичном формате имеет вид 1100 0000.

**Расчёт узлов**

Чтобы рассчитать количество узлов, изучите последний октет. После заимствования двух бит для подсети остаётся 6 бит в узловой части.

Используйте формулу расчёта узлов, как показано на рисунке 2.

2^6 = 64

Не забывайте, что если в узловой части адреса все биты равны 0, то это адрес самой сети, а если все биты равны 1 — широковещательный. Таким образом, в каждой подсети фактически доступно только 62 адреса узлов.

Как показано на рисунке 3, адрес первого узла в первой подсети — 192.168.1.1, а адрес последнего узла — 192.168.1.62. На рис. 4 показаны диапазоны для подсетей от 0 до 2. Помните, что каждый узел должен иметь правильный IP-адрес в диапазоне, определённом для данного сегмента сети. Подсеть, присвоенная интерфейсу маршрутизатора, определит, к какому сегменту относится узел.

На рисунке 5 показан пример конфигурации. В этой конфигурации первая сеть назначена интерфейсу GigabitEthernet 0/0, вторая сеть — интерфейсу GigabitEthernet 0/1, а третья сеть назначена последовательной сети 0/0/0.

Кроме того, согласно общему плану адресации адрес первого узла в подсети назначен интерфейсу маршрутизатора. Узлы в каждой подсети будут использовать адрес интерфейса маршрутизатора в качестве адреса шлюза по умолчанию.

* Для ПК1 (192.168.1.2/26) в качестве адреса шлюза по умолчанию будет использоваться 192.168.1.1 (адрес интерфейса G0/0 маршрутизатора R1).
* Для ПК2 (192.168.1.66/26) в качестве адреса шлюза по умолчанию будет использоваться 192.168.1.65 (адрес интерфейса G0/1 маршрутизатора R1).

**Примечание.** Все устройства в одной и той же подсети будут иметь IPv4-адрес узла из диапазона адресов узлов и использовать одну и ту же маску подсети.

**Разбиение IPv4-сети на подсети**

**Разбиение IPv4-сети на подсети**

Далее рассмотрите сетевую инфраструктуру, в которой требуется пять подсетей, как показано на рисунке 1.

Если использовать одинаковый блок адресов 192.168.1.0/24, для создания как минимум пяти подсетей необходимо позаимствовать несколько бит из узловой части адреса. Заимствование двух битов создаст только четыре подсети, как было показано в предыдущем примере. Для создания большего количества подсетей необходимо заимствовать больше бит из узловой части. Рассчитаем количество подсетей, создаваемых при заимствовании трёх бит из узловой части по формуле:

2^3 = 8 подсетей

Как показано на рисунках 2 и 3, при заимствовании трёх бит создаются 8 подсетей. Если заимствовать три бита, маска подсети будет расширена на 3 бита в последнем октете (/27), что даст маску подсети 255.255.255.224. Все устройства в этих подсетях будут использовать маску подсети 255.255.255.224 (/27).

**Расчёт узлов**

Чтобы рассчитать количество узлов, изучите последний октет. После заимствования трёх бит для подсети остаётся 5 бит в узловой части.

Применим формулу расчёта узлов:

2^5 = 32, но вычтем 2 для всех нулей в узловой части (сетевого адреса) и все единицы в узловой части (широковещательный адрес).

Подсети назначаются сегментам сети, необходимым для топологии, как показано на рисунке 4.

Кроме того, согласно общему плану адресации, адрес первого узла в подсети назначен интерфейсу маршрутизатора, как показано на рисунке 5. Узлы в каждой подсети будут использовать адрес интерфейса маршрутизатора в качестве адреса шлюза по умолчанию.

* Для ПК1 (192.168.1.2/27) в качестве адреса шлюза по умолчанию будет использоваться 192.168.1.1.
* Для ПК2 (192.168.1.34/27) в качестве адреса шлюза по умолчанию будет использоваться 192.168.1.33.
* Для ПК3 (192.168.1.98/27) в качестве адреса шлюза по умолчанию будет использоваться 192.168.1.97.
* Для ПК4 (192.168.1.130/27) в качестве адреса шлюза по умолчанию будет использоваться 192.168.1.129.

# Разбиение IPv4-сети на подсети

## Разбиение IPv4-сети на подсети

В предыдущих примерах мы рассматривали сетевую инфраструктуру, в которой требуются три подсети, и структуру с пятью подсетями. Чтобы создать четыре подсети, мы заимствовали два бита из восьми доступных бит в узловой части с IP-адресом, который имеет маску по умолчанию 255.255.255.0 или префикс /24. Полученная маска подсети имела вид 255.255.255.192, было создано 4 возможных подсети. Применив формулу расчёта узлов 2^6-2, мы определили, что в каждой из этих четырёх подсетей доступно 62 адреса для назначения узлам.

Чтобы создать 5 подсетей, мы заимствовали три бита из восьми доступных бит узловой части с IP-адресом, который имеет маску по умолчанию 255.255.255.0 или префикс /24. После заимствования этих трёх бит из узловой части у нас осталось 5 бит узловой части. Полученная маска подсети имела вид 255.255.255.224, было создано 8 подсетей с 30 адресами узлов в каждой из них.

Рассмотрим крупные организации или комплексы зданий, для сетевых инфраструктур которых требуется 100 подсетей. Как и в предыдущих примерах, для создания 100 подсетей необходимо заимствовать биты из узловой части IP-адреса существующей объединённой сети. Как и раньше, для расчёта количества подсетей необходимо определить количество доступных бит и применить формулу 2^n - 2. Если использовать IP-адрес из последнего примера (192.168.10.0/24), нам доступно 8 бит в узловой части, а для создания 100 подсетей нужно позаимствовать 7 бит.

Рассчитаем количество подсетей, создаваемых при заимствовании семи бит в узловой части: 2^7=128 подсетей.

Однако после заимствования семи бит у нас останется только один бит узла, и если мы применим формулу расчёта узлов, мы получим 0 узлов в этих подсетях. Рассчитаем количество узлов в случае, когда остался только один бит: 2^1=2 и вычтем 2 для сетевого адреса и широковещательного адреса. В результате мы имеем 0 узлов (2^1-2=0).

Если требуется большее количество подсетей, необходимо использовать IP-сеть с большим числом бит в узловой части для заимствования, например IP-адрес с маской подсети по умолчанию /16 или 255.255.0.0. Адреса с диапазоном 128–191 в первом октете имеют маску по умолчанию 255.255.0.0 или /16. Адреса в этом диапазоне имеют по 16 бит в сетевой и узловой части. Биты из этих 16 бит можно использовать для создания подсетей.

Если использовать новый IP-адрес 172.16.0.0/16, для создания как минимум 100 подсетей необходимо позаимствовать несколько бит в узловой части. Начиная с первого слева доступного бита в узловой части, мы будем заимствовать по одному биту за один раз до тех пор, пока не получим количество бит, необходимых для создания 100 подсетей. Позаимствовав один бит, мы создадим 2 подсети, позаимствовав два бита — 4 подсети, 3 бита — 8 подсетей и т.д. Рассчитаем количество подсетей, создаваемых при заимствовании двух бит из узловой части по формуле 7^n:

2^7 = 128 подсетей

Заимствование семи бит позволяет создать 128 подсетей, как показано на рисунке.

Как вы помните, маска подсети должна изменяться для отражения заимствованных бит. В этом примере при заимствовании семи бит маска будет расширена на 7 бит в третьем октете. В десятичном формате маска будет иметь вид 255.255.254.0 или префикс /23, поскольку третий октет в двоичном формате имеет вид 11111110, а четвёртый октет — 00000000. Разделение на подсети будет выполняться в третьем октете с использованием бит в узловой части в третьем и четвёртом октете.

# Разбиение IPv4-сети на подсети

## Разбиение IPv4-сети на подсети

**Расчёт узлов**

Чтобы рассчитать количество узлов, изучите третий и четвёртый октеты. После заимствования семи бит подсети в третьем октете остался один бит в узловой части, а в четвёртом октете — 8 бит в узловой части.

Используйте формулу расчёта узлов, как показано на рисунке 1.

2^9 = 512

Не забывайте, что если в узловой части адреса все биты равны 0, то это адрес самой сети, а если все биты равны 1 — широковещательный. Таким образом, в каждой подсети фактически доступно только 510 адресов узлов.

Как показано на рисунке 2, адрес первого узла в первой подсети — 172.16.0.1, а адрес последнего узла — 172.16.1.254. Помните, что каждый узел должен иметь правильный IP-адрес в диапазоне, определённом для данного сегмента сети. Подсеть, присвоенная интерфейсу маршрутизатора, определит, к какому сегменту относится узел.

**Напоминание.**

Биты могут быть заимствованы только из узловой части адреса. Сетевая часть адреса выделяется оператором связи, и изменить её невозможно. Поэтому организациям, которым требуется значительное число подсетей, необходимо обратиться к своему интернет-провайдеру с просьбой выделить блок IP-адресов, используя маску подсети по умолчанию с числом битов, достаточным для создания требуемого числа подсетей.

# Разбиение IPv4-сети на подсети

## Разбиение IPv4-сети на подсети

Некоторым организациям, например небольшим операторам связи, может потребоваться дополнительное количество подсетей, более чем 100. В качестве примера рассмотрим организацию, которой требуется 1000 подсетей. Как и всегда, для создания подсети нужно позаимствовать биты из узловой части адреса исходной сети. Как и раньше, для расчёта допустимого количества подсетей необходимо определить количество доступных бит в узловой части. В такой ситуации необходимо, чтобы IP-адрес, выделенный интернет-провайдером, имел достаточно бит узлов для расчёта 1000 подсетей. IP-адреса с диапазоном 1–126 в первом октете имеют маску по умолчанию 255.0.0.0 или /8. Это означает, что при разделении на подсети для заимствования доступно 8 бит в сетевой части адреса и 24 бита в узловой части.

Если использовать блок адресов 10.0.0.0/8, для создания как минимум тысячи подсетей необходимо позаимствовать несколько бит из узловой части. Начиная с первого слева доступного бита в узловой части, мы будем заимствовать по одному биту за один раз до тех пор, пока не получим количество бит, необходимых для создания 1000 подсетей. Рассчитаем количество подсетей, создаваемых при заимствовании двух бит из узловой части по формуле 10^n:

2^10 = 1024 подсети

Заимствование десяти бит позволяет создать 1024 подсети, как показано на рисунке 1.

Как вы помните, маска подсети должна изменяться для отражения заимствованных бит. В этом примере при заимствовании десяти бит маска будет расширена на 10 бит в третьем октете. В десятичном формате маска будет иметь вид 255.255.192.0 или префикс /18, поскольку третий октет в двоичном формате имеет вид 11000000, а четвёртый октет — 00000000. Разделение на подсети будет выполняться в третьем октете, но не забывайте о битах из узловой части в третьем и четвёртом октете.

**Расчёт узлов**

Чтобы рассчитать количество узлов, изучите третий и четвёртый октеты. После заимствования десяти бит для подсети в третьем октете осталось 6 бит в узловой части, а в четвёртом октете — 8 бит в узловой части. Всего осталось 14 бит.

Используйте формулу расчёта узлов, как показано на рисунке 2.

2^14 - 2 = 16382

Адрес первого узла в первой подсети — 10.0.0.1, а адрес последнего узла — 10.0.63.254. Помните, что каждый узел должен иметь правильный IP-адрес в диапазоне, определённом для данного сегмента сети. Подсеть, присвоенная интерфейсу маршрутизатора, определит, к какому сегменту относится узел.

**Примечание.** Все устройства в одной и той же подсети будут иметь IPv4-адрес узла из диапазона адресов узлов и использовать одну и ту же маску подсети.

# Разбиение IPv4-сети на подсети

## Определение маски подсети

Принятие решения о том, сколько бит в узловой части заимствовать для создания подсетей, является важным этапом планирования. При планировании подсетей следует рассмотреть два момента: количество адресов узлов, необходимых для каждой сети, и количество требуемых отдельных подсетей. На анимационном представлении показаны возможности подсети для сети 192.168.1.0. Выбор количества бит для идентификатора подсети влияет на количество возможных подсетей и количество адресов узлов в каждой из них.

Обратите внимание на обратную зависимость между количеством подсетей и узлов в них. Чем больше бит заимствовано для создания подсетей, тем меньше останется бит в узловой части и, следовательно, тем меньше узлов будет доступно в каждой подсети. Если требуется больше узлов, значит, нужно больше бит в узловой части, что приводит к уменьшению количества подсетей.

**Количество узлов**

При заимствовании бит для создания нескольких подсетей у вас остаётся достаточно бит в узловой части для самой крупной подсети. Количество адресов узлов, необходимых в самой крупной подсети, определяет, сколько бит нужно оставить в узловой части адреса. Для расчёта количества адресов, которые будут доступны в каждой подсети, используется формула 2^n (где n — количество оставшихся бит в узловой части). Как вы помните, два адреса использовать нельзя, поэтому фактически количество доступных адресов рассчитывается как 2^n-2.

# Разбиение IPv4-сети на подсети

## Определение маски подсети

Иногда требуется конкретное количество подсетей, а количество адресов узлов в каждой подсети менее важно. Например, в организации может потребоваться разделить сетевой трафик согласно внутренней структуре или при настройке сети в подразделении. Например, организация может принять решение объединить в одну сеть все устройства, используемые специалистами технического отдела, а все устройства, используемые руководством, вынести в отдельную сеть. В этом случае количество подсетей имеет более высокий приоритет при определении количества бит для заимствования.

Как вы помните, количество подсетей, создаваемых при заимствовании бит, можно рассчитать по формуле 2^n (где n — количество заимствованных бит). Вычитать какие-либо подсети нет необходимости, так как они все пригодны к использованию.

Ключевым моментом является соотношение количества необходимых подсетей и количества узлов, требуемых для самой крупной подсети. Чем больше бит было заимствовано для создания дополнительных подсетей, тем меньше узлов будет доступно в каждой из подсетей.

# Разбиение IPv4-сети на подсети

## Определение маски подсети

Все сети в организации спроектированы таким образом, чтобы обеспечить работу конечного количества узлов. Для базового разбиения на подсети требуется достаточно подсетей для объединения сетей, что обеспечивает при этом нужное количество адресов в каждой подсети.

В некоторых сетях, таких как каналы сети WAN класса «точка-точка», требуется только два узла. Другие сети, например локальная сеть пользователей в крупном здании или в отделе, могут содержать сотни узлов. Сетевые администраторы должны разработать схему межсетевой адресации, чтобы обеспечить максимальное количество узлов в каждой сети. Количество узлов в каждом подразделении должно иметь запас для увеличения в будущем.

**Определение общего количества узлов**

Сначала оцените общее количество узлов, необходимых для всей корпоративной объединённой сети. Необходимо использовать достаточно крупный блок адресов, который охватывает все устройства во всех корпоративных сетях. К таким устройствам относятся устройства конечных пользователей, сервера, промежуточные устройства и интерфейсы маршрутизатора.

Рассмотрим пример корпоративной сетевой инфраструктуры, которая должна охватывать 123 узлов в пяти офисах (см. рис. 1). В этом примере оператор связи выделил сетевой адрес 172.20.0.0/21 (11 бит в узловой части). Как показано на рисунке 2, этот блок содержит 2,046 адреса узлов, которых хватает для обеспечения потребностей этой сетевой инфраструктуры.

# Разбиение IPv4-сети на подсети

## Определение маски подсети

**Определение количества сетей и их размеров**

Далее следует проанализировать требуемое количество подсетей и количество адресов узлов, необходимых в каждой подсети. Если взять за основу топологию сети, содержащей 5 сегментов ЛВС и 4 соединения между маршрутизаторами, то потребуются 9 подсетей. Самая большая подсеть должна содержать 40 узлов. При проектировании схемы адресации необходимо заранее учесть увеличение как количества подсетей, так и узлов в подсетях.

Сетевой адрес 172.16.0.0/22 имеет 10 битов в узловой части. Поскольку самой крупной подсети требуется 40 узлов, для обеспечения их адресации требуется не менее 6 битов в узловой части. Это число определяется по следующей формуле: 2^6 - 2 = 62 узла. Оставшиеся 4 бита в узловой части можно использовать для создания подсетей. По формуле определения количества подсетей получаем 16 подсетей: 2^4 = 16. Поскольку в нашем примере сетевой инфраструктуры требуются 9 подсетей, это соответствует нашим требованиям и обеспечивает некоторый запас для роста в будущем.

Если заимствовать 4 бита, новая длина префикса будет /26 с маской подсети 255.255.255.192.

Как показано на рисунке 1, длина префикса /26 позволяет определить 16 адресов подсетей. Увеличилась только часть подсети в адресе. Исходные 22 бита сетевого адреса нельзя изменить, а узловая часть будет содержать нулевые биты.

**Примечание**. Обратите внимание, что поскольку часть подсети находится в третьем и четвёртом октетах, одно или два этих значения будут изменяться в адресах подсетей.

Как показано на рисунке 2, исходная сеть 172.16.0.0/22 была единой сетью, в которой используются 10 бит, обеспечивая 1022 пригодных к использованию адресов для назначения узлам. Путём заимствования 4 бит из узловой части можно создать 16 подсетей (от 0000 до 1111). В каждой подсети имеются 6 бит в узловой части или 62 пригодных к использованию адреса узлов.

Как показано на рисунке 3, подсети можно назначить сегментам локальной сети и соединениям между маршрутизаторами.

# Разбиение IPv4-сети на подсети

## Определение маски подсети

Для разбиения на подсеть дан сетевой адрес 192.168.100.0/24. Необходимо составить схему IP-адресации сети, изображённой в топологии. Для каждой локальной сети в сети требуется достаточно пространства минимум для 25 адресов оконечных устройств, коммутатора и маршрутизатора. Для соединения между маршрутизаторами R1 и R2 потребуется по одному IP-адресу на каждом конце канала.

[Packet Tracer: разбиение на подсети, вариант 1 (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.1.4.6%20Packet%20Tracer%20-%20Subnetting%20Scenario%201%20Instructions.pdf)

[Packet Tracer: разбиение на подсети, вариант 1 (PKA)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.1.4.6%20Packet%20Tracer%20-%20Subnetting%20Scenario%201.pka)

# Разбиение IPv4-сети на подсети

## Определение маски подсети

Для разбиения на подсеть дан сетевой адрес 172.31.1.0/24. Необходимо составить схему IP-адресации сети, изображённой в топологии. Требуемые адреса узла для каждого канала сети WAN и локальной сети отмечены в топологии.

[Packet Tracer: разбиение на подсети, вариант 2 (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.1.4.7%20Packet%20Tracer%20-%20Subnetting%20Scenario%202%20Instructions.pdf)

[Packet Tracer: разбиение на подсети, вариант 2 (PKA)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.1.4.7%20Packet%20Tracer%20-%20Subnetting%20Scenario%202.pka)

**Разбиение IPv4-сети на подсети**

**Определение маски подсети**

**В ходе этой работы вам необходимо выполнить следующие задания.**

* Часть 1: определите разбиение на подсети IPv4-адреса
* Часть 2: рассчитайте разбиение на подсети IPv4-адреса

[Лабораторная работа: расчёт IPv4-подсетей](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.1.4.8%20Lab%20-%20Calculating%20IPv4%20Subnets.pdf)

**Разбиение IPv4-сети на подсети**

**Определение маски подсети**

**В ходе этой работы вам необходимо выполнить следующие задания.**

Части 1–5 для каждой топологии сети.

* Определите количество подсетей.
* Разработайте соответствующую схему адресации.
* Присвойте интерфейсам устройств адреса и маски подсетей.
* Проверьте использование доступного пространства сетевых адресов и будущего потенциала роста.

[Лабораторная работа: разбиение топологий сетей на подсети](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.1.4.9%20Lab%20-%20Subnetting%20Network%20Topologies.pdf)

**Разбиение IPv4-сети на подсети**

**Определение маски подсети**

**В ходе этой работы вам необходимо выполнить следующие задания.**

* Часть 1: обзор доступных калькуляторов подсетей.
* Часть 2: расчёт сети с помощью калькулятора подсети.

[Лабораторная работа: изучение калькуляторов подсетей](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.1.4.10%20Lab%20-%20Researching%20Subnet%20Calculators.pdf)

# Разбиение IPv4-сети на подсети

## Преимущества разбиения на подсети с использованием маски переменной длины

В традиционном разбиении на подсети каждой подсети выделяется одинаковое количество адресов. Если все подсети имеют одинаковые требования к количеству узлов, такие блоки адресов фиксированного размера будут эффективными. Однако чаще всего требования отличаются.

Например, в топологии, показанной на рисунке 1, используются семь подсетей: по одной для каждой из четырёх локальных сетей и по одной для каждого из трёх каналов сети WAN между маршрутизаторами. В традиционном разбиении на подсети с указанным адресом 192.168.20.0/24 из узловой части в последнем октете можно позаимствовать три бита, чтобы обеспечить создание семи подсетей. Как показано на рисунке 2, при заимствовании трёх бит можно создать 8 подсетей, а оставшихся пяти бит в узловой части хватит для 30 адресов узлов в каждой подсети. В данной схеме создаются необходимые подсети, и она соответствует требованиям к узлам для самой крупной локальной вычислительной сети.

Хотя это традиционное разбиение на подсети соответствует требованиям самой крупной ЛВС и делит адресное пространство на достаточное количество подсетей, в нём создаётся значительный объём неиспользуемых адресов.

Например, в каждой подсети для каждого из трёх WAN-соединений нужны только два адреса. Поскольку в каждой подсети доступно по 30 адресов, 28 из них не будут использоваться. Как показано на рисунке 3, в результате мы получаем 84 неиспользуемых адреса (28x3).

Кроме того, это ограничивает возможности для будущего роста, сокращая общее количество доступных подсетей. Такое неэффективное использование адресов характерно для традиционного разбиения на подсети с использованием классовых сетей.

Применение традиционной схемы разбиения на подсети в данном варианте является неэффективным и бесполезным. Фактически, этот пример демонстрирует, как в процессе разбиения подсети на несколько подсетей можно максимально задействовать адресное пространство.

Разбиение подсети на несколько подсетей с использованием маски подсети переменной длины (VLSM) позволяет распределять гораздо меньше «лишних» адресов.

# Разбиение IPv4-сети на подсети

## Преимущества разбиения на подсети с использованием маски переменной длины

Обратите внимание, что во всех предыдущих примерах разбиения на подсети ко всем подсетям применялась одна маска подсети. Это означает, что в каждой подсети доступно одинаковое количество адресов узлов.

Как показано на рисунке 1, при традиционном разбиении на подсети создаются подсети одинакового размера. Во всех подсетях в традиционной схеме используется одна маска подсети. Как показано на рисунке 2, VLSM-маска позволяет разделить сетевое пространство на неравные части. VLSM-маска подсети может варьироваться в зависимости от количества бит, которые были заимствованы для конкретной подсети. Эти биты образуют «переменную» часть маски.

VLSM-разбиение на подсети похоже на традиционное тем, что в нём для создания подсетей заимствуются биты. Формулы расчёта количества возможных подсетей и количества узлов в каждой подсети также применимы. Различие состоит в том, что разбиение на подсети выполняется в несколько этапов. При использовании VLSM сеть сначала разбивается на подсети, а затем подсети снова делятся на подсети. Этот процесс может повторяться много раз для создания подсетей различного размера.

# Разбиение IPv4-сети на подсети

## Преимущества разбиения на подсети с использованием маски переменной длины

Чтобы лучше понять процесс применения VLSM, вернёмся к предыдущему примеру.

В предыдущем примере, показанном на рисунке 1, сеть 192.168.20.0/24 была разбита на восемь подсетей равного размера. Семь из восьми подсетей были выделены. Четыре подсети использовались для локальных сетей, а три подсети — для каналов сети WAN между маршрутизаторами. Как вы помните, в подсетях, используемых для каналов сети WAN, были неиспользуемые адреса, так как в этих подсетях нужны только два адреса — по одному для каждого интерфейса маршрутизатора. Чтобы предотвратить неэффективное использование адресов, с помощью VLSM можно создать более мелкие подсети для каналов сети WAN.

Чтобы создать более мелкие подсети для каналов сети WAN, одна из подсетей будет разделена. На рисунке 2 последняя подсеть 192.168.20.224/27 будет дополнительно разбита на подсети.

Как вы помните, если известно требуемое количество адресов узлов, можно использовать формулу 2^n-2 (где n — количество оставшихся бит в узловой части). Чтобы получить два доступных адреса, в его узловой части должны остаться два бита.

2^2 - 2 = 2

Поскольку в адресном пространстве 192.168.20.224/27 имеются 5 бит в узловой части, три бита можно позаимствовать, оставив 2 бита в узловой части.

На данном этапе расчёты в точности совпадают с расчётами при традиционном разбиении на подсети. Биты заимствуются, определяя диапазоны подсетей.

Как показано на рисунке 2, схема VLSM-разбиения на подсети уменьшает количество адресов в каждой подсети до подходящего размера соединений с глобальной сетью. Разбиение подсети 7 для сетей WAN оставляет доступными подсети 4, 5 и 6 для будущих сетей, а также для нескольких других подсетей для сетей WAN.

**Разбиение IPv4-сети на подсети**

**Преимущества разбиения на подсети с использованием маски переменной длины**

При использовании VLSM-подсетей для сегментов ЛВС и сети WAN можно выделить адреса без ненужной избыточности.

Узлам во всех локальных сетях будет присвоен допустимый адрес узла в диапазоне этой подсети и с маской /27. У каждого из четырёх маршрутизаторов будет интерфейс локальной сети с подсетью /27, а также один или несколько последовательных интерфейсов с подсетью /30.

В стандартной схеме адресации IPv4-адрес первого узла в каждой подсети назначается LAN-интерфейсу маршрутизатора. WAN-интерфейсам маршрутизаторов назначаются IP-адреса и маска для подсетей /30.

На рисунках с 1 по 4 показаны конфигурации интерфейсов для всех маршрутизаторов.

Узлы в каждой подсети будут иметь IPv4-адрес из диапазона адресов этой подсети и соответствующую маску. Узлы будут использовать адрес подключённого LAN-интерфейса маршрутизатора в качестве шлюза по умолчанию.

* Узлы здания A (192.168.20.0/27) будут использовать адрес 192.168.20.1 маршрутизатора в качестве шлюза по умолчанию.
* Узлы здания B (192.168.20.32/27) будут использовать адрес 192.168.20.33 маршрутизатора в качестве шлюза по умолчанию.
* Узлы здания С (192.168.20.64/27) будут использовать адрес 192.168.20.65 маршрутизатора в качестве шлюза по умолчанию.
* Узлы здания D (192.168.20.96/27) будут использовать адрес 192.168.20.97 маршрутизатора в качестве шлюза по умолчанию.

**Разбиение IPv4-сети на подсети**

**Преимущества разбиения на подсети с использованием маски переменной длины**

Выделение адресов можно также спланировать с помощью ряда способов. Одним из таких способов является определение доступных и назначенных блоков адресов с помощью схемы VLSM. Этот метод позволяет предотвратить назначение уже выделенных адресов. Например, для сети из предыдущего примера с помощью схемы VLSM можно спланировать назначение адресов.

**Изучение подсетей /27**

Как показано на рисунке 1, при использовании традиционного разбиения на подсети первые семь блоков адресов используются для локальных и глобальных сетей. Как вы помните, по этой схеме были получены 8 подсетей с 30 доступными адресами в каждой из них (/27). Хотя схема подходит для сегментов локальной сети, в сегментах сети WAN будет несколько неиспользуемых адресов.

При проектировании схемы адресации для новой сети блоки адресов можно присвоить таким образом, чтобы сократить до минимума избыточные адреса и объединить неиспользуемые блоки адресов.

**Назначение блоков адресов VLSM**

Как показано на рисунке 2, чтобы более эффективно использовать адресное пространство, для каналов сети WAN были созданы подсети /30. Чтобы объединить неиспользуемые блоки адресов, последняя подсеть /27 была дополнительно разбита на подсети для создания подсетей /30. Первые 3 подсети были назначены каналам сети WAN.

* Диапазон адресов узла .224 /30 от 225 до 226: канал сети WAN между маршрутизаторами R1 и R2.
* Диапазон адресов узла .228 /30 от 229 до 230: канал сети WAN между маршрутизаторами R2 и R3.
* Диапазон адресов узла .232 /30 от 233 до 234: канал сети WAN между маршрутизаторами R3 и R4.
* Диапазон адресов узла .236 /30 от 237 до 238: доступен для использования.
* Диапазон адресов узла .240 /30 от 241 до 242: доступен для использования.
* Диапазон адресов узла .244 /30 от 245 до 246: доступен для использования.
* Диапазон адресов узла .248 /30 от 249 до 250: доступен для использования.
* Диапазон адресов узла .252 /30 от 253 до 254: доступен для использования.

При подобном проектировании схемы адресации остаются три неиспользуемые подсети /27 и пять неиспользуемых подсетей /30.

**Схемы адресации**

**Структурированный проект**

Как показано на рисунке, выделение в корпоративной сети адресного пространства на сетевом уровне необходимо тщательно спроектировать. Адреса не должны назначаться случайным образом. При планировании выделения адресов необходимо рассмотреть три основных момента.

* **Предотвращение дублирования адресов:** каждый узел в сетевой инфраструктуре должен иметь уникальный адрес. Без надлежащего планирования и документирования адрес может быть назначен нескольким узлам, что приведёт к проблемам доступа к сети этих узлов.
* **Предоставление доступа и управление им:** некоторые узлы, такие как серверы, предоставляют ресурсы и внутренним, и внешним узлам. Назначенный серверу адрес 3-го уровня можно использовать для управления доступом к этому серверу. Если адрес назначен случайным образом и нигде не задокументирован, управлять доступом будет сложнее.
* **Мониторинг безопасности и производительности:** аналогичным образом необходимо контролировать безопасность и производительность узлов сети, а также всей сети в целом. В рамках мониторинга сетевой трафик анализируется на наличие адресов, которые генерируют или получают большое число пакетов. При надлежащем планировании и документировании адресации в сети проблемные устройства можно легко обнаружить.

**Назначение адресов в сети**

В сети существуют устройства различных типов, включая следующие:

* Клиентские устройства конечных пользователей
* Серверы и периферийные устройства
* Узлы, доступные из Интернета
* Промежуточные устройства
* Шлюз

При проектировании схемы IP-адресации обычно рекомендуется использовать готовый шаблон назначения адресов каждому типу устройств. Это помогает администраторам добавлять и удалять устройства, фильтровать трафик на основе IP-адресов, а также упрощает документирование.

# Схемы адресации

## Структурированный проект

В план выделения адресов в сети могут входить различные диапазоны адресов во всех подсетях для каждого типа устройств.

**Адреса клиентов**

Из-за сложностей, связанных со статической раздачей адресов, устройства конечных пользователей часто получают адреса динамически по протоколу DHCP. Как правило, использование протокола DHCP — наиболее предпочтительный способ присвоения IP-адресов узлам в крупной сети, поскольку он облегчает работу специалистов службы поддержки и практически устраняет возможность ошибки.

Другое преимущества DHCP состоит в том, что адреса присваиваются узлам временно. Если нам нужно изменить схему разбиения сети на подсети, нет необходимости статически переназначать адреса отдельных узлов. При использовании DHCP потребуется только перенастроить DHCP-сервер, указав новые данные подсети. После этого узлам нужно только автоматически обновить свои IP-адреса.

**Адреса серверов и периферийных устройств**

Всем сетевым ресурсам, таким как сервера или принтеры, следует присвоить статические IP-адреса, как показано на рисунке. Клиентские узлы обращаются к этим ресурсам по IP-адресам конкретных устройств. Поэтому всем серверам и периферийным устройствам нужно назначить предсказуемые адреса.

На серверах и периферийных устройствах концентрируется сетевой трафик. На IPv4-адреса этих устройств отправляется много пакетов, равно как и исходит из них. При мониторинге сетевого трафика с помощью таких средств, как программа Wireshark, администратор сети сможет быстро определять подобные устройства. Использование согласованной системы нумерации упростит идентификацию этих устройств.

**Адреса узлов, доступных из Интернета**

В большинстве сетевых инфраструктур только отдельные устройства доступны за пределами корпоративной сети. Как правило, этими устройствами являются сервера определённого типа. Как и у всех устройств в сети, которые предоставляют сетевые ресурсы, IP-адреса данных устройств должны быть статическими.

В случае серверов, доступных из Интернета, каждому из них должен быть назначен публичный адрес. Кроме того, изменение адреса одного из этих устройств приведёт к тому, что устройство станет недоступным из Интернета. В большинстве случаев эти устройства находятся в сети, где используются частные адреса. Это означает, что маршрутизатор или граничный брандмауэр сети необходимо настроить на преобразование внутреннего адреса сервера в публичный адрес. Из-за такой дополнительной настройки на граничном промежуточном устройстве ещё более важным становится то, чтобы эти устройства имели предсказуемые адреса.

**Адреса промежуточных устройств**

Промежуточные устройства также являются точками концентрации сетевого трафика. Практически весь трафик внутри сети или между сетями проходит через одно из таких промежуточных устройств. Таким образом, на данных сетевых устройствах можно разместить средства управления сетью, её мониторинга и обеспечения безопасности.

Большинство промежуточных устройств имеют адреса 3-го уровня, необходимые для их работы или управления ими. Устройствам, таким как концентраторы, коммутаторы и точки беспроводного доступа для работы в качестве промежуточных устройств IPv4-адреса не нужны. Однако если нам нужно получить доступ к этим узлам для настройки, мониторинга и устранения неполадок сети, эти устройства должны иметь адреса.

Поскольку нам необходимо знать, как связаться с промежуточными устройствами, у таких устройств должны быть предсказуемые адреса. Поэтому их адреса, как правило, назначаются вручную. Кроме того, адреса этих устройств должны принадлежать другому диапазону в блоке адресов, отличному от адреса устройства пользователя.

**Адрес шлюза (маршрутизаторы и брандмауэры)**

В отличие от других упомянутых промежуточных устройств, маршрутизаторы и брандмауэры имеют только по одному адресу на каждом интерфейсе. Каждый интерфейс находится в своей сети и выполняет роль шлюза для узлов в этой сети. Как правило, для интерфейса маршрутизатора используется самый младший или самый старший адрес в сети. Назначение должно быть единообразным во всех сетях организации, чтобы пользователи сети всегда знали шлюз сети независимо от того, в какой подсети они работают.

Интерфейсы маршрутизатора и брандмауэра являются точками концентрации трафика, входящего в сеть и исходящего из неё. Поскольку узлы в каждой сети используют интерфейс маршрутизатора или брандмауэра в качестве исходящего шлюза, через такие интерфейсы проходит большое количество пакетов. Таким образом, эти устройства могут играть важную роль в системе безопасности сети, фильтруя пакеты на основе IP-адресов источника и/или назначения. Объединение различных типов устройств в группы логической адресации повышает эффективность назначения адресов и работы этой фильтрации пакетов.

**Схемы адресации**

**Структурированный проект**

**В ходе этой работы вам необходимо выполнить следующие задания.**

* Часть 1: разработайте схему разбиения сети на подсети
* Часть 2: выполните настройку устройств
* Часть 3: проверьте и устраните неполадки в сети

[Лабораторная работа: разработка и внедрение структуры адресации IPv4-сети, разделённой на подсети](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.2.1.3%20Lab%20-%20Designing%20and%20Implementing%20a%20Subnetted%20IPv4%20Addressing%20Scheme.pdf)

**Схемы адресации**

**Структурированный проект**

**В ходе этой работы вам необходимо выполнить следующие задания.**

* Часть 1: изучите требования к сети
* Часть 2: разработайте схему адреса маски подсети переменной длины (VLSM)
* Часть 3: проведите и настройте IPv4-сети

[Лабораторная работа: разработка и внедрение структуры адресации VLSM](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.2.1.4%20Lab%20-%20Designing%20and%20Implementing%20a%20VLSM%20Addressing%20Scheme.pdf)

# Схемы адресации

## Структурированный проект

Дан сетевой адрес, по которому необходимо разработать схему адресации VLSM для сети, показанной на приложенной топологии.

[Packet Tracer: разработка и внедрение структуры адресации VLSM (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.2.1.5%20Packet%20Tracer%20-%20Designing%20and%20Implementing%20a%20VLSM%20Addressing%20Scheme%20Instruct.pdf)

[Packet Tracer: разработка и внедрение структуры адресации VLSM (PKA)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.2.1.5%20Packet%20Tracer%20-%20Designing%20and%20Implementing%20a%20VLSM%20Addressing%20Scheme.pka)

# Особенности проектирования IPv6-сети

## Разбиение IPv6-сети на подсети

Разбиение IPv6-сети на подсети подразумевает использование другого подхода, чем разбиение на подсети IPv4-сети. Основная причина заключается в том, что в IPv6 заложено огромное количество адресов. Поэтому разбиение на подсети полностью отличается от разбиения IPv4-сетей. Пространство IPv6-адресов разбивается не с целью экономии адресов, а для обеспечения иерархической логической структуры сети. Если IPv4-сети разбиваются на подсети в основном для борьбы с нехваткой адресов, то целью разбиения IPv6-сети на подсети является создание иерархии адресов на основе количества маршрутизаторов и обслуживаемых ими сетей.

Как вы помните, блок IPv6-адресов с префиксом /48 содержит 16 бит идентификатора подсети, как показано на рисунке 1. Разбиение на подсети с использованием 16 бит идентификатора подсети даёт 65 536 возможных подсетей /64. Поэтому нет необходимости заимствовать биты из идентификатора интерфейса или узловой части адреса. Каждая IPv6-подсеть /64 содержит примерно 18 квинтиллионов адресов, что, как очевидно, гораздо больше, чем когда-либо понадобится в одном сегменте IP-сети.

Подсети, созданные из идентификатора подсети, легко представить, поскольку не нужно выполнять преобразование в двоичный формат. Чтобы определить следующую доступную подсеть, достаточно рассчитать следующее шестнадцатеричное число. Как показано на рисунке 2, необходимо применить расчёт части идентификатора подсети в шестнадцатеричной системе счисления.

Префикс глобальной маршрутизации является одинаковым для всех подсетей. Для каждой подсети увеличивается только четырёхразрядный байт идентификатора подсети.

# Особенности проектирования IPv6-сети

## Разбиение IPv6-сети на подсети

Когда на выбор доступно 65 000 подсетей, задачей сетевого администратора становится проектирование логической структуры адресов в этой сети.

Как показано на рисунке 1, в примере топологии потребуются подсети для каждой локальной сети, а также для канала сети WAN между маршрутизаторами R1 и R2. В отличие от примера для IPv4-сети IPv6-сеть с подсетью канала сети WAN не будет разбиваться на подсети. Хотя при этом могут остаться неиспользуемые адреса, что не является проблемой для IPv6-сетей.

Как показано на рисунке 2, для данного примера будут выделены пять IPv6-подсетей с идентификаторами подсети от 0001 до 0005. Каждая подсеть /64 предоставит гораздо больше адресов, чем может когда-либо понадобиться.

Как показано на рисунке 3, каждому сегменту ЛВС и каналу сети WAN назначается подсеть /64.

Аналогично настройке IPv4, на рисунке 4 показано, что каждый интерфейс маршрутизатора был настроен как находящийся в другой IPv6-подсети.

# Особенности проектирования IPv6-сети

## Разбиение IPv6-сети на подсети

В IPv6-сетях по аналогии с заимствованием бит из узловой части IPv4-адреса можно позаимствовать биты из идентификатора интерфейса для создания дополнительных IPv6-подсетей. Как правило, это делается по соображениям безопасности, чтобы уменьшить число узлов в подсети и создавать дополнительные подсети.

При расширении идентификатора подсети путём заимствования бит из идентификатора интерфейса рекомендуется создавать подсеть на границе полубайта. Полубайт — это 4 бита или одна шестнадцатеричная цифра. Как показано на рисунке, префикс подсети /64 расширяется на четыре бита или один полубайт до подсети /68. Это позволяет уменьшить размер идентификатора на 4 бита (с 64 до 60).

Разбиение на подсети по границе полубайта имеет значение только для масок подсетей, выровненных по полубайту. Начиная с /64, масками подсети, выровненными по полубайту, будут являться маски /68, /72, /76, /80 и т. д.

Разбиение на подсети по границе полубайта позволяет создать подсети с использованием дополнительного шестнадцатеричного значения. В этом примере новый идентификатор подсети состоит из пяти шестнадцатеричных значений в диапазоне от 00000 до FFFFF.

Можно создать подсеть в пределах полубайта, используя шестнадцатеричную цифру, однако это не рекомендуется и, кроме того, в этом нет необходимости. Разбиение на подсети в пределах полубайта сводит на нет преимущества быстрого определения префикса из идентификатора интерфейса. Например, если используется длина префикса /66, первые два бита были бы частью идентификатора подсети, а вторые два бита — частью идентификатора интерфейса.

# Особенности проектирования IPv6-сети

## Разбиение IPv6-сети на подсети

Системный администратор хочет, чтобы вы назначили пять подсетей IPv6 /64 для сети, показанной в топологии. Ваша задача — определить IPv6-подсети, присвоить IPv6-адреса для маршрутизаторов и настроить компьютеры для автоматического получения IPv6-адресации. В итоге вы должны проверить связь между IPv6-узлами.

[Packet Tracer: внедрение схемы адресации IPv6-сети с разделёнными подсетями (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.3.1.4%20Packet%20Tracer%20-%20Implementing%20a%20Subnetted%20IPv6%20Addressing%20Scheme%20Instructions.pdf)

[Packet Tracer: внедрение схемы адресации IPv6-сети с разделёнными подсетями (PKA)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.3.1.4%20Packet%20Tracer%20-%20Implementing%20a%20Subnetted%20IPv6%20Addressing%20Scheme.pka)

**Заключение**

**Заключение**

**Можете мне позвонить?**

**Примечание**. Это задание можно выполнять самостоятельно или в группах с использованием программы Packet Tracer.

Вы настраиваете выделенную схему адресации компьютерам в больничных палатах. Коммутатор будет располагаться в центре сети в кабинете главной медсестры, так как во все пять палат будет заведён сетевой кабель, чтобы пациенты могли подключиться к встроенным в стену портам RJ-45. Разработайте физическую и логическую топологию сети для одного из шести этажей, используя следующие требования к схеме адресации.

* Есть шесть этажей с пятью палатами на каждом из них. Всего необходимо тридцать подключений. В каждой палате должна быть точка подключения к сети.
* В данной схеме должно быть предусмотрено разделение на подсети.
* Для выполнения адресации используйте один маршрутизатор, один коммутатор и пять узловых пунктов.
* Убедитесь, что все компьютеры можно подключить к внутренним службам больницы.

Сохраните копию схемы, чтобы позже показать её группе или другим учащимся. Будьте готовы объяснить, каким образом будут реализованы разбиение на подсети, одноадресная, многоадресная и широковещательная рассылка, а также для каких целей можно будет использовать предложенную вами схему адресации.

[Работа в аудитории: можете мне позвонить? (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.4.1.1%20Can%20You%20Call%20Me%20Now.pdf)

# Заключение

## Заключение

Будучи техническим специалистом, который знаком с внедрением адресации IPv4 и IPv6, вы теперь готовы приступить к работе с существующей сетевой инфраструктурой и на практике применить свои знания и умения для завершения конфигурации. Сетевой администратор уже настроил некоторые команды на маршрутизаторах. **Не удаляйте и не изменяйте эти конфигурации**. Ваша задача — подготовить схему адресации IPv4 и IPv6, реализовать её и проверить сетевые подключения.

[Packet Tracer: отработка комплексных практических навыков (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.4.1.2%20Packet%20Tracer%20-%20Skills%20Integration%20Challenge%20Instructions.pdf)

[Packet Tracer: отработка комплексных практических навыков (PKA)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/9.4.1.2%20Packet%20Tracer%20-%20Skills%20Integration%20Challenge.pka)

# Заключение

## Заключение

Как показано на рисунке, процесс сегментации сети для её разделения на несколько более мелких сетей называется разбиением на подсети.

Каждый сетевой адрес содержит допустимый диапазон адресов узлов. Все устройства, подключённые к одной и той же сети, будут иметь IPv4-адрес узла этой сети, а также общую маску подсети или префикс сети. Узлы могут напрямую обмениваться трафиком, если они находятся в одной подсети. Трафик не может передаваться между подсетями без использования маршрутизатора. Чтобы определить, является ли трафик локальным или удалённым, маршрутизатор использует маску подсети. Префикс и маска подсети — это разные способы представления одного и того же — сетевой части адреса.

Для создания IPv4-подсетей мы задействуем один или нескольких бит из узловой части в качестве бит сетевой части. Два существенных фактора, которые влияют на определение блока IP-адресов с помощью маски подсети, — это количество необходимых подсетей и максимальное количество узлов, которое должно быть в подсети. Между количеством подсетей и узлов в них существует обратная зависимость. Чем больше бит заимствовано для создания подсетей, тем меньше останется бит в узловой части и, следовательно, тем меньше узлов будет доступно в каждой подсети.

Для расчёта количества адресов, которые будут доступны в каждой подсети, используется формула 2^n (где n — количество оставшихся бит в узловой части). Однако в этом диапазоне сетевой адрес и широковещательный адрес недоступны для использования, поэтому количество доступных адресов рассчитается по формуле 2^n-2.

Разбиение подсети на несколько подсетей или использование маски подсети переменной длины (VLSM) предназначены для того, чтобы избежать создания ненужных адресов.

Разбиение IPv6-сети на подсети подразумевает использование другого подхода, чем разбиение на подсети IPv4-сети. Пространство IPv6-адресов разбивается не с целью экономии адресов, а для обеспечения иерархической логической структуры сети. Если IPv4-сети разбиваются на подсети в основном для борьбы с нехваткой адресов, то целью разбиения IPv6-сети на подсети является создание иерархии адресов на основе количества маршрутизаторов и обслуживаемых ими сетей.

Для обеспечения наилучшего использования схемы IP-адресации требуется тщательное планирование. В процессе планирования адресов необходимо учитывать размер, расположение, использование и требования к доступу.

После установки IP-сети её необходимо протестировать для проверки подключений и производительности.